



Doc. 300.1.3

Date: 30.5.19

# Feedback Report from EEC experts

- **Higher education institution:**  
EUROPEAN UNIVERSITY CYPRUS
- **Town:** NICOSIA
- **Program of study (Name, ECTS, duration, cycle)**  
**In Greek:** ΑΣΦΑΛΕΙΑ ΚΥΒΕΡΝΟΧΩΡΟΥ, 90 ECTS,  
18 μήνες, (Μεταπτυχιακό)  
**In English:** CYBERSECURITY, 90 ECTS, 18 months,  
(Master of Science)
- **Language of instruction:** English
- **Program's status**  
**New program:**    
**Currently operating:** .....

The present document has been prepared within the framework of the authority and competencies of the Cyprus Agency of Quality Assurance and Accreditation in Higher Education, according to the provisions of the “Quality Assurance and Accreditation of Higher Education and the Establishment and Operation of an Agency on Related Matters Laws of 2015 and 2016” [N. 136 (I)/2015 and N. 47(I)/2016].

## A. External Evaluation Committee (EEC)

<i>Name</i>	<i>Position</i>	<i>University</i>
Benny Pinkas	Professor	Bar Ilan University
Bracha Shapira	Professor	University of the Negev
Georgios Kambourakis	Associate Professor	University of the Aegean
Iordanis Kavathatzopoulos	Professor	Uppsala University

## B. Guidelines on content and structure of the report

- *The EEC based on the external evaluation report (Doc.300.1.1) and the Higher Education Institution's response (Doc.300.1.2), must justify whether actions have been taken in improving the quality of the programme of study in each assessment area.*
- *Below each assessment area the EEC must circle the degree of compliance.*

The School of Sciences of European University Cyprus wishes to express its sincere gratitude to the *External Evaluation Committee (EEC)* for the evaluation of the postgraduate program: **Cybersecurity (MSc) – Distance Learning (DL)**. It is with great pleasure that we noted the positive feedback of the *EEC* and we appreciate its insightful and critical recommendations which provided us the opportunity to improve the quality and implementation of the program. In the pages that follow we have responded to all recommendations for improvement provided by the *EEC* and we provide all information and the accompanying documents explaining the actions taken to ensure that the proposed program is of high quality and addresses all *EEC* recommendations.

## 1. Study program and study program's design and development (ESG 1.1, 1.2, 1.8, 1.9)

### **EEC Comments:**

#### **Findings:**

*The study program is designed to provide the students with a high-level introduction to the field of cyber security. The program is composed of six compulsory courses, in addition to either a thesis or three additional courses. The courses cover relevant areas, but most of them only give a high level theoretical/survey perspective, and there is a lack of courses that give the students a hands on experience.*

#### **Strengths:**

*The courses in the program introduce the students to most of the topics that are relevant for Cybersecurity.*

#### **Areas of improvement and recommendations:**

*The study program does not give the students the practical knowledge to start working in the area. It is true that an academic program is not intended to give practical knowledge that is usually learned in professional courses about specific tools or procedures, but it is essential that the students learn the basic skills of analyzing and solving problems in the related field. In particular, our opinion is that the following intended learning outcomes listed in the Application for Evaluation, are not met:*

- *Gain expertise in both theory and practice of Cybersecurity*
- *Design and implement networked, software and distributed systems with Cybersecurity in mind*
- *Secure both clean and corrupted systems, protecting personal data, securing simple computer networks, and safe Internet usage*
- *Incorporate approaches for incident analysis and response*
- *Incorporate approaches for risk management and best practices*

*In the context of cyber security, the best way to ensure that students learn about the practice and implementation, is through hands-on programming exercises. Even in theoretical courses such exercises can verify that the students understand the material. Also, this*

familiarizes the students with challenges that occur in the real world. Even if the students work as managers, or only oversee work that is done by external contractors and suppliers, it is essential that they understand what these suppliers are doing.

In the proposed program, programming exercises are given in the course on Ethical Hacking and Penetration Testing (CS607). We strongly recommend that the students will also need to do hands-on programming exercises in the Network security course (CS603), and at least one such exercise in the cryptography course (CS602). It would be useful to add such exercises to other courses, as well. The courses describe the basic knowledge in the areas that they cover, and in general do not cover the most up-to-date research results. This is to a large extent expected since the students need to learn the basics first. Also, most of the teaching staff is not involved in active research in the areas of cyber security. However, it is highly preferred that each course will describe in the last weeks some up-to-date advanced material.

The study program contains a thesis. The committee has examined several theses from the Information Systems masters program, and thesis topics for the cyber security program. The theses include a literature survey and a limited analysis of it. Few of the suggested topics require any implementation work, and most of the suggested topics are too general. (See our recommendation in Section 2.)

The web information about the conventional cyber security masters program describes all general information about the program, but does not give detailed information about the courses. In particular, with regards to the distant program, and if it is accepted that the program needs to contain substantially more programming exercises (which might be challenging to some students), then this should be presented to the students before registering to the program.

### **EUC reply:**

In order to enhance the program's quality by upgrading the practical knowledge to be acquired by students and by encouraging the analytical and problem-solving skills that students will acquire from it, hands-on exercises were added to the following courses:

- CYS603 Communications and Network Security (see attached Study Guide, pp. 25, 35, 46, 47, 59, 71, 53, 79).

- CYS604 Cryptography (see attached Study Guide pp.13, 66, 89, 100, 112, 139)
- CYS606 Cybersecurity Architecture and Operations (see attached Study Guide page 10)

In addition, as indicated by *EEC*, CYS607 Ethical Hacking and Penetration Testing and CYS625 Incident Response and Forensic Analysis courses, already included hands-on exercises (see for your convenience, attached Study Guides: pp. 21, 26, 31, 34, 43, 50 for CYS607; pp. 16, 27, 36, 48, 51 for CYS625). Please also see in Appendix B listed samples of assignments that include hands-on programming exercises.

Based on the recommendations of *EEC*, with the changes we have applied to the program as a whole, we believe that the learning outcomes listed below are now fulfilled, and a brief explanation is provided for each case below:

- *"Gain expertise in both theory and practice of Cybersecurity"*: as mentioned above, practical exercises have been infused in most of the courses (namely, CYS603, CYS604, CYS606)
- *"Design and implement networked, software and distributed systems with Cybersecurity in mind"*: courses comprising the Cybersecurity (MSc) program are formed in such a way to allow students to have a holistic view of Cybersecurity and design, implement and infuse Cybersecurity in networks formation and software creation.
- *"Secure both clean and corrupted systems, protecting personal data, securing simple computer networks, and safe Internet usage"*: CYS607 Ethical Hacking and Penetration Testing course, aims to provide students the opportunity to effectively use different tools and techniques of ethical hacking to protect and secure systems and networks, and more specifically to critically evaluate security techniques used to protect system and user data. Along with CYS624 Data Privacy in the era of Data Mining and AI and CYS603 Communications and Network Security, students will be able to categorise and point out aspects of network security (wired, wireless and mobile) and the importance of data gathering, as well as the protection of such data that will lead students to achieve the learning outcome as proposed.
- *"Incorporate approaches for incident analysis and response"*: The course CYS625 Incident Response and Forensic Analysis aims to explain the principles and legal aspects of incident response and forensic analysis and appreciate where these principles should be applied. Further, it aims to apply the core concepts, knowledge and practice of digital forensic methodology to computer crime investigation and describe forensic investigation approaches and the most up-to-date incident investigation techniques from an incident response perspective, including live analysis.

- *Incorporate approaches for risk management and best practices:* We have incorporated the main approaches for risk management and best practices in a number of weeks throughout the CYS623 Study Guide. See for instance, Week 2 “Cyber Security Standards and Best Practices”, Week 8 “Risk Assessment Approaches”, and in Individual Assignment Week 8.

Additionally, some courses have been enhanced with up-to-date advanced materials, as recommended by the *EEC*. Specifically, courses now include recent Cybersecurity events and their related impact, as well as which controls fail to adequately protect against the related threats (CYS606, CYS607). Moreover, CYS623 content was updated to include the latest developments of the European Union Agency for Network and Information Security (ENISA) and the Cybersecurity Framework of the National Institute of Standards and Technology (NIST), as well as latest recommendations and high priorities, amongst other advanced and current methodologies of internationally recognized institutions.

Regarding the theses examined by the *EEC*, it is important to note that these concern the existing program of Information Systems (MSc). We have, however, taken *EEC*'s recommendations into serious consideration and we have updated our perspective as to how to improve the thesis topics in the Cybersecurity (MSc) program. Please refer to Appendix C for some new Master Thesis topics that will be assigned to the Cybersecurity (MSc) program which are more demanding as anticipated by the *EEC*. Moreover, given that this specific observation of the *EEC* was identified by the Department of Computer Science and Engineering itself as well, the Department has decided to revise its overall regulations on the types of Master's Theses it will accept. Each thesis will now lead to a measurable result, such as solving an actual industry problem, or producing part of an article that is submitted for publication. While the Department is still in deliberation about the specifics, we totally agree with the *EEC* that the Master's thesis topics should provide something more than the development of simple applications or surveys. With this in mind, we aim to establish before the beginning of next semester our Master's Thesis Guide for all the Master's theses produced in the Department. Given the short timeframe to respond to this Evaluation Report, the Department may provide its Master's Thesis Guide to the Cyprus Agency of Quality Assurance and Accreditation in Higher Education before the beginning of the coming academic year.

As far as the program profile, description of courses, learning outcomes and all relevant information, we would like to inform the *EEC* that these are available to all existing and prospective students, graduates, other stakeholders and the public as soon as a program receives accreditation. This is an obligation for every program of study upon receiving accreditation. For instance, as indicated at the time of the *EEC* visit, information about the conventional Cybersecurity (MSc) program appear on the University's website at:

[https://www.euc.ac.cy/easyconsole.cfm/id/176/dep/167/program\\_id/187](https://www.euc.ac.cy/easyconsole.cfm/id/176/dep/167/program_id/187). When visiting the link, you may see a brief description of the program along with the program outline and curriculum. To get detailed information about each course, the visitor can click on each course code and see the course syllabus of the selected course. We endorse with the EEC's recommendation to exemplify the description text of the existing conventional Cybersecurity (MSc) program which as you might see at the same link above it has been edited and now has as follows on the University's website:

*"The Master degree in Cybersecurity that spans over the core areas of cyber security, embraces technical subjects and at the same time aspects of law and social sciences, risk management and cryptography giving students an excellent basis for a future career in the Cybersecurity field. MCYS curriculum covers, cryptography, network and web security, law, ethics, and privacy, cyber offense and cyber defence, governance, policy and compliance, ethical hacking techniques and penetration testing and incident response and forensic analysis. Courses include coursework in the field of Cybersecurity by granting them access to state-of-the-art technology labs to strengthen their practical understanding of the concepts discussed. It also gives students the opportunity to work on a master thesis in a more dedicated manner."*

When the distance education Cybersecurity (MSc) program will be accredited, a new separate page will be created with a concise description of the program, and a detailed description of what the program offers and its aims and requirements. No information may be provided for a program before it has been officially accredited by the Cyprus Agency of Quality Assurance and Accreditation in Higher Education.

**Please circle one of the following for:**

**Study programme and study programme's design and development**

**Non-compliant**

**Partially compliant**

**Substantially compliant**

**Fully compliant**

## 2. Teaching, learning and student assessment (ESG 1.3)

### **EEC Comments:**

#### **Findings**

The program includes 6 courses and some elective courses that cover the main topics in cyber security. The materials are quite basic and provide merely an introduction to cyber security. The University has 6200 students and maintains 90 programs, thus it is difficult to maintain expertise in every program of study. The structure of the courses and the assessments is quite similar for all the courses. There is a limited number of (~6) lectures given by the teacher. The materials are recorded and uploaded to the e-learning platform (Blackboard) and are available for the students in an asynchronous manner. There are basic self-assessment questions (~2) for every week of study and typically, some mandatory assignments, individual or group based. There is a final exam. Typically, the assignments are 50% of the final grade and the final exam is 50%, meaning that it is required to have minimal knowledge in order to receive credit for a course. The overall learning process seems to be organized. The information about the assessment is provided in the syllabi, and so are the learning outcomes, and the detailed content of the course. However, the assignments are very basic, and do not require too much learning effort from the students. The assignments conform with the low-demanding declared learning outcomes of the courses. For example, the CYS607 course on ethical hacking and penetration testing, the learning outcomes require the students to be able to describe ways to conduct hacking but not to actually be able to perform them, as could be expected. Thus, in accordance with that, the assignments don't require more than a basic technical effort from the students. Also the time load for the students that is allocated by the teachers seems to be far higher than our estimated actual. Each syllabus includes a bibliography, but it is not always relevant to the course content, or does not reflect the latest state of the art materials. For example, the research methods course content is mainly about statistics and design of experiments, but the bibliography consists of a book on research methods in cyber security, which is not really covered in the course. As another example, the course CYS624 which teaches privacy in the era of big data is based on papers dated to 2011 (the latest) and does not discuss GDPR. A last example of this situation is the absence of a reference to the ISO/IEC 27000 family of standards in course CYS602. As for students' support during a course and the teacher's availability, the teachers reported about their intensive communication with the

*students, and the students that we met reported that they receive all the support they need.*

### Strengths

- *The teachers seem to be dedicated to their jobs and good teachers (even if they are not the best experts in their fields).*
- *The institution is very responsive to their students.*
- *The students seem very satisfied with the institution and their studies. Note that no student enrolled to the conventional Cybersecurity program was present in the corresponding meeting hour.*
- *The institution seems to be very organized, the syllabi are very informative and includes all the required assessment parts.*

### Areas of improvement and recommendations

- *The assignments are not demanding enough, especially for the technical courses. They don't reflect the time load that is allocated to them and do not always meet the objective of the courses.*
- *The content of the courses does not reflect the state of the art in the corresponding field.*
- *Some courses seem to cover too many topics and this may result in poor learning outcomes.*
- *Some courses present considerable overlap with others.*
- *Course CYS622 entitled "Current trends in Cybersecurity" seems to be too general to be included in the list of elective courses.*
- *Course CYS624 lacks a discussion on major anonymity networks, including Tor and I2P.*
- *The quality of the theses is very low, they are not research theses, but rather technical projects that do not seem to qualify for 30 credit points.*
- *The presentation (defence) of the thesis should be done in face-to-face manner and not via the use of teleconferencing software.*
- *Students should be actively involved in research activities either in the context of their thesis or via their participation to research projects as assistants.*
- *The balance between the exam and the assignments allows students that receive illegitimate help from others to get credit for courses with minimal knowledge.*
- *Where possible, assessment should be carried out by more than one examiner.*

### Recommendations

- *Update the assignments to be more demanding to include technical, practical and cognitive challenges*
- *Update the content of the course to reflect the state of the art in the field of interest.*
- *Cybersecurity is a constantly changing field, hence the courses should be updated on a continuous basis.*
- *Revise the method of defining a thesis and apply more demands on theses towards subjects that require more than the development of simple applications or shallow surveys.*
- *Change the balance of the final grade by putting more emphasis on the exams.*

### EUC reply:

The national regulations define the balance between exams and assignments 50% - 50% (see <http://www.kysats.ac.cy/index.php/el/genikes-plirofories/spoudes-ex-apostaseon>). This ratio is implemented for all EUC Distance Education programs of study. In the Distance Education Cybersecurity (MSc) more specifically, the 50% for assignments is divided into 20% individual work, 20% group work and 10% activities. The activities listed on the Study Guides that were submitted to *EEC*, are showing only the 10% of the marked activities per course. These activities, as indicated by the same regulations of the Cyprus Agency of Quality Assurance and Accreditation in Higher Education aim to provide self-evaluation/assessment opportunities and structure to the students. The aim of these assignments, marked with 10% of the total final mark, is to provide the opportunity to the student to self-regulate her/his learning. Additional to these activities there are other marked *Assignments* carrying 40% of the student's final mark. These are not shown on the Study Guides, given that they are assigned by each instructor. The *EEC* did not have thus the opportunity to review such assignments. These assignments have much higher complexity (including technical, practical and cognitive challenges) and require much more effort and time from students to be completed. In Appendix B you can find example of such assignments.

In addition, the learning outcomes listed in the course syllabi have been reviewed, in order to higher the requirements as per *EEC*'s comments, to match the time-load required for the successful completion of the course, and depict the practical aspect added to the courses as mentioned in Section 1. As far as the bibliography, the bibliography section of each syllabus has been carefully reviewed so that it is updated and thus reflect the latest state of the art materials. Moreover, overlapping has been observed into courses and more specifically in the courses CYS603, CYS604, CYS607, as discussed during *EEC*'s on-site visit. Despite that some

overlapping will always exist in Cybersecurity courses due to its interdisciplinary and multifaceted nature, we have carefully observed the overlapping areas to ensure they will be studied in a different way/angle according to the aim and specific learning outcomes of each course.

As far as the course CYS622, this has been renamed to *Special Cybersecurity Topics*. The aim of this elective course is to provide the opportunity to the program to offer to students additional contemporary or more specific topics to those covered by the existing courses in the program. As you might see in the new syllabus we prepared, the course provides space for such an approach. You may also refer to the attached sample syllabus and Study Guide which demonstrate how this course might be approached in the offering of the program.

Regarding the course CYS624, we have conformed with the EEC's recommendations and thus the bibliography is updated, and the content has changed to discuss GDPR, anonymity networks and ethical considerations. In addition, CYS602 Introduction to Cybersecurity course content has been improved to include reference to the ISO/IEC 27000 family of standards.

Face to face manner for Thesis defence is of course an option, especially for conventional studies and for local students. This, however, has a number of shortcomings for Distance Education programs and students who do not reside close to the university offering a distance education program (especially students that live in abroad). The Cyprus Agency of Quality Assurance and Accreditation in Higher Education thus does not foresee for an on-situ thesis defence procedure. As such, our university (as others in Cyprus) conducts an open to all the academic community defence procedure by sharing a Blackboard web-link which is sent to students and staff in a given program of study in order to have the ability to attend the defence. In this way the procedure is aligned to the open character of the defence.

Students are expected to be actively involved in research activities in the context of their master's thesis as mentioned in Section 1 as well. Moreover, through the [CERIDES](http://www.cerides.euc.ac.cy) ([www.cerides.euc.ac.cy](http://www.cerides.euc.ac.cy)) Center of Excellence of our University, certain calls are announced per semester for MCYS students wishing to be further involved in research activities.

Blackboard Platform operates Turnitin system as a plagiarism control system which aims to ensure academic integrity and this is used by all distance education instructors in all distance education programs of study.

**Please circle one of the following for:**

**Study programme and study programme's design and development**

**Non-compliant**

**Partially compliant**

**Substantially compliant**

**Fully compliant**

### 3. Teaching Staff (ESG 1.5)

#### EEC Comments:

##### Current state and deficiencies

Five out of seven members of the teaching staff are special scientists (1) or special teaching personnel (4). So, in total, 5 of 7 do not hold a permanent position in the hosting institution. The coordinator of the proposed program is at the Lecture rank with rather limited experience in the field. It is expected that such a position is allocated to permanent experienced personnel who is at the rank of full professor or associate professor. With reference to their CVs, most of the teaching staff is not very much security-oriented. They mostly publish in journals/conferences that lie outside the field of information security and privacy enhancing technologies. Also, the research profile of the teaching staff is rather weak, i.e., only two of them have more than 250 citations (264) as reported by Google scholar, and almost all of them do not present a strong research record, namely publishing frequently in prestigious international journals and/or conference proceedings. The EEC found some discrepancies between what is reported in the 3rd column of Table 3 (“discipline/specialization”) of the proposal and the specialization of each of them as given in their personal page, and their scientific profile in general. The number of 12 teaching hours per week per each member of the teaching staff is rather high. This may result in poor results in conducting equally important tasks including scientific research and the writing/participation of/in research projects. In the latter cases, a member of the teaching staff may be allowed to teach 3 to 6 hours less, but the way the missing hours are compensated by the department and the university in general is not defined. According to the curriculum of each lesson and the meeting with the teaching staff, a limited number of lectures per course is delivered by industry specialists. However, there is no evidence or reference of inviting recognized visiting professors in the field of Cybersecurity to deliver lectures, seminars, etc. The ECC also underlines the absence of summer schools organized by the department in the field of Cybersecurity and privacy enhancing technologies.

##### Suggestions

- The department should consider ways of reducing the teaching workload of the teaching staff and focus on strengthening and easing the research activities of the teaching personnel, e.g., by granting awards and additional funding for doing research of high quality.

- *The department should recruit permanent high-ranked personnel, i.e., at least one more associate professor and 2 assistant professors who have a solid academic background and are actively working on the area of Cybersecurity.*
- *The curriculum of each course should include lectures delivered by experts in the field of interest.*

*Also, the department should consider the possibility of organizing summer schools and workshops in the area of Cybersecurity and privacy enhancing technologies.*

#### **EUC reply:**

Three (3) out of seven members of the teaching staff are full-time faculty of EUC (as shown in Table 4 in the application) and four (4) are scientific collaborators. According to CY.Q.A.A. the coordinator of a program needs to be a full-time faculty of the institution of not a specific rank (<http://www.dipae.ac.cy/index.php/en/news-and-events/announcements/13-dipae-el/dipael/anakoinoseis/180-2018-10-25-syntonistes-programmaton-spoudon>). This can change with the three new openings for full-time faculty in the rank of professor, associate professor and assistant professor which the University has already advertised based on the EEC's recommendations. The three new academic positions are in the area of Cybersecurity with a requirement of strong research background, in an attempt to enhance the research profile of the MCYS teaching personnel. The link for EUC's website and the respective vacancies is: <https://www.euc.ac.cy/en/school-of-sciences-vacancies/department-of-computer-sciences-and-engineering--academic-positions>. In Appendix A you can also find the newspaper announcement. As in all hiring procedures at the EUC, the applicants research profile and activities are taken as prime consideration for hiring purposes. The University through its Charter and its Research Policy provides strong incentives to faculty to carry out quality research that will lead to publications in prestigious international journals and therefore high citations. According to the University's Research Policy (see Appendix D), each teaching personnel involved in research or having a number of publications/conferences presentations, is entitled teaching load reduction per academic semester/year. Based on this Research Policy, a full-time Faculty member can teach as low as 6 hours per week. If a member of the teaching staff takes advantage of the teaching load reduction scheme, then part-time personnel is hired to cover the missing hours for as long as needed. Moreover the university offers internal grants for research and funds for papers publication fees and conferences presentations. In addition, promotion in rank is achieved by demonstrating such a strong publication record.

It is also noted that two of the faculty members teaching in the program, namely Dr. Danidou and Dr. Kiourmourtzis were and currently are actively involved in EU funded research projects in the areas of Cybersecurity. As an example some projects are: PrEsto Cloud (H2020), AsgardWeb (H2020), ARCADIA (H2020) and others.

In a number of courses there are invited lectures by industry specialists related to Cybersecurity. These lectures are explicitly stated in the Study Guides, and in the case of the conventional MCYS program, we have successfully implemented many invited lectures. Particularly, we have invited the Commissioner for Personal Data Protection who discussed GDPR issues as well data protection in a business context with students. Moreover, other good existing examples are the Standards Officer from the Cyprus Organisation for Standardisation, and an expert advisor in the fields of Enterprise Risk Management, Compliance, Physical and Information Security and Organisational Resilience. However, as per *EEC*'s recommendation, we will also invite visiting professors from the Cybersecurity field to deliver lectures, seminars, etc, as well as to conduct on an annual basis webinars of contemporary Cybersecurity topics.

Regarding the suggestion for organising summer schools, this can be considered taking in account the needs and demands of the first cohort of students. The Department considers this recommendation as of high value and quality for the overall experience the students will gain by deciding to pursue the Cybersecurity (MSc).

**Please circle one of the following for:**

**Study programme and study programme's design and development**

*Non-compliant*

*Partially compliant*

*Substantially compliant*

*Fully compliant*

#### 4. Students (ESG 1.4, 1.6, 1.7)

##### **EEC Comments:**

###### *Findings*

*The students are accepted to the program if they have a CS or relevant degree from any accredited program from anywhere in the world. Also, as reported by the administrative and teaching staff, students from other disciplines may be accepted after taking some fundamental courses. It was not clear what fundamentals are required and what other disciplines are at all considered. The administrative staff declared that the students do not pay extra fees for the fundamentals courses.*

*As reported, the dropout rate is very low, which is very untypical to Computer Science degrees. The reasons for that can come from the good support that the students receive or/and from the not very demanding program. We believe that both reasons apply here.*

*The program outcome does not fully comply with the declared learning outcome (as discussed in part 1). The students should receive a correct description of the actual outcome of the program.*

*The students seem to be very satisfied from the communication with the teaching staff, the support they receive, and from the teaching evaluation procedure. They reported that teachers that are found to be incapable by the students are fired. The extent of considering student's desires is even a bit exaggerated to the level that they affect the program of study and professional decisions. For example, the teaching staff describe a case where a fundamental course was cancelled being not popular among the students.,*

*It is noted that the institution just transformed its teaching evaluation procedure to an automatic process for better efficiency.*

*The students receive an M.Sc degree in cyber security from the School of Sciences with supplements that comply with the EU regulations.*

*The institution reported of very high employability of their graduates in the market, however, since this is a new distant learning program, and*

*the relevant conventional program does not yet have graduates, it is impossible to assess the level of employability of the graduates.*

### Strengths

- Good communication between the students and the teaching staff
- Good support for students
- Good teaching evaluation procedure

### Areas of improvement and recommendations

- Unclear and not sufficiently regulated admission process.
- Unmet learning outcome and objectives of the program
- The program is not demanding enough

### Recommendations

- Clarify the criteria for acceptance to the program
- Adjust the declared learning outcome to the actual content of the courses.
- Higher the requirements, do not consider all students requests about courses

### EUC reply:

The content of the courses has been revised to reach higher standards as per EEC's comments and the bibliographies have been updated. Thus, the learning outcomes have been revised, were necessary, to match these changes and higher the requirements of the courses. By adding new content in the courses, we aimed at improving the quality of the program as a whole and make it more demanding for our students.

As far as the student admissions criteria. These are as follows:

#### **General admissions criteria for master's programs of study:**

- A recognized Bachelor's degree or its equivalent.

- Proficiency in English. Applicants must submit proof of English proficiency. This must consist of at least one of the following:

- a. Proof that undergraduate instruction and coursework has been done in English
- b. The Test of English as a Foreign Language (TOEFL) examination with a minimum score of 550 (paper-based total) or 213 (Computer based total).
- c. IELTS with a score of 6.5 or English GCSE (GCE) O' Level with "C" or above.

In cases that the above English language requirements cannot be met for practical reasons, a student shall take the English Placement Test of the University. The minimum level for the student to be admitted to a post-graduate program is ENL102-Advanced English.

**Specific admissions criteria for the Cybersecurity (MSc) program of study:**

- An undergraduate (Bachelor's) degree in Computer Science, Computer Engineering, Information Systems, Electronic Engineering or a related field from an accredited college, university, or higher education institution  
Or
- An undergraduate (Bachelor's) from a variety of backgrounds related to computer science and electronic engineering, such as mathematics, branches of engineering, and related disciplines which can be considered eligible upon completion of foundation courses on Cybersecurity. For these applicants who cannot proceed directly to the program of study, the Program Committee will decide, on an individual basis, which foundation courses these applicants will be required to take among the following:
  - ECE210 - Computer Organization and Architecture
  - CSE300 - Data Communications and Computer Networks
  - CSE320 - Operating Systems

Upon evaluation of the assigned foundation courses, the applicants will then be formally accepted to the Cybersecurity (MSc) program.

All eligible applications will be evaluated by the Evaluation Committee of the Program that will rank the candidates based on:

- Grade Point Average (GPA) of their undergraduate degree
- Working experience in the relevant field.

The Evaluation Committee of the Program reserves the right to conduct interviews when necessary, request additional information and to adopt any additional criteria it may deem necessary.

Regarding the dropout rates of relevant programs of the Cybersecurity (MSc) program, for the undergraduate program of Computer Science numbers range from 9.28 – 19.09 and for postgraduate programs range from 5.56 – 14.29.

On other comments of the *EEC* provided in this section:

- The material of the courses has been revised as to meet the learning outcomes of the program. The program will be more demanding after adopting the *EEC*'s suggestions.
- Student's suggestions are considered as the Cyprus Agency of Quality Assurance and Accreditation in Higher Education requests their representation in various committees such as in the Program Evaluation Report Committees. In no case though, the students have the primary and sole role in decision-making processes regarding the University's programs of study and implementation.

**Please circle one of the following for:**

**Study programme and study programme's design and development**

**Non-compliant**

**Partially compliant**

**Substantially compliant**

**Fully compliant**

## 5. Resources (ESG 1.6)

### EEC Comments:

#### Findings

*The program under evaluation is a distant learning program, thus the physical facilities at the institution are not relevant besides the distant learning platform that is described in section 6.*

*In addition, access to materials of the library is granted through open access via VPN and the library is taking part of the national project that unites all high academic institutions in Cyprus into one non-profit organization that has an agreement with a great number of major publishers to provide access to students to relevant academic resources.*

*As for the labs, physical labs are of course not mandatory, the teaching staff reported that they use virtual machines for technical practice which seems rather adequate for the program at hand.*

#### *Strengths*

*NA*

#### *Areas of improvement and recommendations*

*NA*

### EUC reply:

*NA*

Please circle one of the following for:

**Study programme and study programme's design and development**

**Non-compliant**

**Partially compliant**

**Substantially compliant**

**Fully compliant**

## 6. Additional for distance learning programs (ALL ESG)

### **EEC Comments:**

*EUC is an established university with several years of experience in providing distance education. In order to grow as a small university in a very small country, EUC has to expand internationally. A way to achieve this is by offering courses that satisfy the need of education in Cybersecurity for students anywhere in the world.*

*The proposed course of Cybersecurity can rely on EUC's previous experience on Distance Learning courses. The needed technical infrastructure is already there as well as the teaching staff that has the skills to teach in distance learning courses. A special Distance Learning Unit is there to prepare and support teachers and students as well as to coordinate technical procedures and equipment. A conventional course on Cybersecurity is given so there are experienced teachers available in this special subject.*

*The philosophy of the proposed Distance Education Cybersecurity (MSc) program is a more on the cooperation mainly between individual student and teacher and not between students, except in the cases of group-work. A stronger cooperation model would imply the introduction of peer-reviewing of individual assignments and thesis.*

*The focus of Distance Learning Unit and the courses and support it provides seems to be more focused on technical infrastructure issues and on course procedures in distance learning rather on the pedagogical challenges of this kind of education.*

### **EUC reply:**

In the conventional MCYS program, we have applied during the last semester the peer-reviewed system to enhance the cooperation of individual students. We plan to take this further and apply the peer-review systems for individual assignments in the DL Master in Cybersecurity program as well. Additionally, to enhance the cooperation between students, we already apply forums and group activities.

Distance Education has a concrete pedagogical model adapted to the special characteristics of DL students and based on three fundamental elements

- resources, collaboration and guidance - that all advocate in students' achievements. Teaching methodology is based both on student-centered approach and on high-tech material use. The teacher's primary role is to coach and facilitate student learning and the overall comprehension of material as well. Web-based learning such as virtual laboratories, case studies, group discussion,



brainstorming, audio-visual presentation, individual assignments, seminars, quiz, group project are of significant use.

**Please circle one of the following for:**

**Study programme and study programme's design and development**

*Non-compliant*      *Partially compliant*      *Substantially compliant*      *Fully compliant*

**7. Additional for doctoral programs (ALL ESG)**

N/A

**8. Additional for joint programs (ALL ESG)**

N/A

**C. Conclusions and final remarks**

*EEC's* comments gave us the opportunity to improve our program and raise the requirements to make it more demanding for our students.

Overall, we have completed the following changes to meet *EEC's* comments:

1. The learning outcomes of the courses have been changed, where necessary, to be more focused and demanding.
2. The Study Guides submitted to *EEC* included a number of graded activities, but not the actual assignments. Please refer to Appendix B to see more specific assignments and to judge the level of complexity.
3. Hands-on programming exercises were added to a number of courses, to enhance the learning experience of students (see Section 1 above)
4. The bibliography of each course was updated to include up-to-date material.
5. We have taken *EEC's* comments into consideration and thesis topics will be from now on more demanding, and will end-up to research results. Students will also be involved in research, through the Centre for Risk and Decision Sciences (CERIDES) and the funded projects it participates and submits.
6. The syllabi have been revised to meet the specific comments received by *EEC*.
7. New hirings have been announced to address the comment of enhancing research in the field of Cybersecurity.

Taking this chance to refer to any changes to the program, please note upon the program's accreditation, the following course codes will be used.

Course codes		
CYS600	Introduction to Cybersecurity	10
CYS615	Communications and Network Security	10
CYS625	Cryptography	10
CYS630	Cybersecurity Policy, Governance, Law and Compliance	10
CYS645	Cybersecurity Architecture and Operations	10
CYS655	Ethical Hacking and Penetration Testing	10
CSE600	Research Methods	10
CYS670	Special Cybersecurity Topics	10
CYS675	Cybersecurity Risk Analysis and Management	10
CYS680	Data Privacy in the era of Data Mining and AI	10
CYS685	Incident Response and Forensic Analysis	10
CSE670	Master Thesis	30

**The EEC must provide constructive conclusions and final remarks**

#### A. Signatures of the EEC

Name	Signature

Date: .....

**Appendix A: Academic Vacancy**

**Appendix 8: Samples of Assignments**

**Appendix C: Sample Theses Topics**

**Appendix D: Research Policy**



**European  
University Cyprus**

**Appendix A: Academic Vacancy**

**Appendix B: Samples of Assignments**

**Appendix C: Sample Theses Topics**

**Appendix D: Research Policy**

## Appendix A



**European University Cyprus** | **School of Sciences**

**THE** UNIVERSITY  
UNIVERSITY  
RANKINGS  
2019 TOP 301+



### Academic Vacancies

The School of Sciences, department of Computer Science and Engineering of European University Cyprus, is seeking to recruit faculty members in the discipline of **Cybersecurity** at any academic rank for the following specialization areas:

▶ Machine Learning

▶ Penetration Testing

▶ Digital Forensics

▶ Network Security

---

**Number of positions:**  
One faculty member in the rank of Associate Professor or Professor  
Two faculty members in the rank of Lecturer or Assistant Professor

---

**Candidates should submit the following documents:**

▶ Letter of interest

▶ Curriculum Vitae

▶ Proof of qualifications

▶ Two reference letters

---

**Application process:**  
Applications submitted electronically to the Human Resource Department  
Email: [hrm@euc.ac.cy](mailto:hrm@euc.ac.cy) by **Monday, 1st of July 2019**  
Tel: +357 22713061

More information about the required documents on our website: [www.euc.ac.cy](http://www.euc.ac.cy)

**European University Cyprus**  
6 Diogenes Street, Engomi, Nicosia  
P.O.Box 22006, 1516 Nicosia, Cyprus  
Tel: +357 22713000  
Fax: +357 22713172

## Appendix B

### CYS604 Assignment - Vulnerability scanning (20 points)

In most cases, your local network consists of you ADSL modem that is an all-in-one box with the modem, firewall, router, switch, firewall and a wireless Access Point (AP) similar to one presented in **Error! Reference source not found..**

In this assignment, you are requested to conduct an Internal and External vulnerability scanning in your home network. In an internal vulnerability scanning, you will have to discover all the hosts in your home network and discover any open ports of all the devices that are connected to your home router. To do so, you will need to use nmap and perform a number of different scans for TCP and UDP. You have to take screenshots as a proof of your work and explain your findings.

In an external vulnerability scanning, you can use a number of tools that are already provided to you in the Lab sessions. You need to find your ip address and choose some of the tools to run external scanning to your router. Again, you will need to take screenshots as a proof of your work and explain your findings.

Firewall settings: Open your network firewall and make sure that DMZ is not enabled. Explain the meaning of the DMZ and make sure that you have not running services inside the DMZ unless it is necessary. You will need to take screenshots as a proof of your work and explain your findings.

All the above results with explanations of the tools you have used will be submitted as a report.

In addition to this, you are requested to present your work in the classroom and get ready to provide explanations on your work, at the end of the course.

### CYS604 Group Assignment: Packet Inspection with Wireshark (20 points)

Wireshark is a free and open source packet analyzer. In your home computer use Wireshark to capture packets that are destined to and sourced from your computer. We suggest you to capture the packets over the time of few seconds.

A quick tutorial on how to install and capture packets is provided in this [link](#).

After you run Wireshark and capture a number of packets examine the following:

1. Identify your internal IP address by running either *ipconfig* (Windows) or *ifconfig* (Linux).
2. Check all the TCP and UDP packets and identify the source and the destination address.
3. Identify the port number for each packet for both TCP and UDP.
4. Check to see known vulnerabilities associated with the specific port numbers by using an online Database (<https://www.speedguide.net/ports.php> ).

5. Identify either the source or destination of each TCP and UDP packet by using an online [IP Lookup Tool](#).

Take some screenshots to prove your findings, report the results and provide justification of your findings.

## CYS604 Individual Assignment (20 points)

The individual assignment includes solving questions related to the syllabus covered in this course. The questions can vary from practical ones, to essay style questions asking to use your current skills in order to describe existing cryptography protocols.

In addition, there will be one exercise asking to implement using any programming language, one of the protocols already taught in the course.

This assignment counts 20% of the final course mark.

You will need approximately 20 hours to solve this Individual Assignment.

## CYS604 Exercise 10.5

Using your preferred programming language, develop a simple implementation of the Diffie-Hellman key-exchange protocol.

## **Appendix C**

### **Title: Critical Infrastructure Interoperability and Cyber Attacks**

Description: In most modern countries around the world, infrastructures like water distribution systems, transportation and electricity grids are controller with a number of microcontrollers (PLCs), sensors and actuators. In order to achieve the best possible outcome, these equipment exchanges information using industrial protocols. Unfortunately, some of those protocols are not secure and might pose a huge risk to the most vital aspect of a functioning country/city.

In this thesis you should provide a survey of such protocols in critical infrastructure, describing their restrictions and limitations. Choose a number of incidents that have already happened, with an in-depth analysis of each incident indicating how they attackers achieved their goal and how they could have been prevented.

Develop a penetration testing tool or use existing penetration testing tools & libraries in order to develop an automated test that a user can use in order to examine for vulnerabilities of an interconnected infrastructure.

### **Title: Cyber Security in Organizations**

Description: The majority of organizations is highly depended on computers and networking in order to complete everyday tasks. Several of those computers and networks are either not protected from attacks or the staff using them is not trained to distinguish between legit and non-legit actions.

In this thesis you should provide a survey of cyber attacks in organizations around the world, describing how they attackers gained access to the system/network.

Develop a sophisticated phishing attack that can be used by the organizations against their employees. The outcome of the attack will indicate if the employees are educated in order to distinguish between legit and non-legit actions

### **Title: Malware Study In A Sandboxed Environment**

Description: The scope of this thesis will be separated into two distinct phases, concerning the study of malicious software (i.e. malware). Originally, the student will have to perform a literature review on existing approaches for malware analysis, so as to understand how such an activity is performed and study possible assumptions and limitations. While, on the next phase, a practical study must be performed to existing malicious softwares. More specifically, the student must setup an isolated (sandboxed) environment, that will be used for the malware analysis, in accordance with the already studied frameworks and approaches.

**Title: Phishing Campaigns: A Thorough Study**

Description: The scope of this thesis includes the study of known phishing attacks and approaches. By that, the student will be able to understand how an attacker develops, launches and exploits such attacks, by using existing tools and mechanisms. In addition, the thesis will include the practical implementation of such an attack, on a predefined controlled environment, so as to imitate the actions of a real attacker and depict how an attack could be utilized and how to protect against it.

## **Appendix D**



# **RESEARCH POLICY**

September 2018

# Table of Contents

## INTRODUCTION

10

<b>1. EUC RESEARCH ETHICS POLICY</b>	<b>11</b>
1.1 <u>SCOPE AND PURPOSE</u> .....	11
1.2 <u>GENERAL PRINCIPLES</u> .....	12
1.3 <u>THE DEFINITION OF HUMAN-RELATED RESEARCH</u> .....	12
1.4 <u>VULNERABLE PARTICIPANTS</u>	6
1.5 <u>THE LEGAL FRAMEWORK, THE ROLE OF PROFESSIONAL ASSOCIATIONS AND RESEARCH COUNCILS</u> .....	13
<b>2. GOOD RESEARCH PRACTICES / CODE OF ETHICAL CONDUCT IN RESEARCH</b>	<b>13</b>
2.1 <u>CODE OF ETHICAL CONDUCT IN RESEARCH</u> .....	13
2.2 <u>OPENNESS IN RESEARCH</u> .....	14
2.3 <u>INTEGRITY</u> .....	14
2.4 <u>MISCONDUCT IN RESEARCH</u> .....	14
<b>3. INTELLECTUAL PROPERTY POLICY</b>	<b>15</b>
3.1 <u>INTRODUCTION</u> .....	15
3.2 <u>DEFINITIONS</u> .....	15
<b>3.3 INTELLECTUAL PROPERTY REGULATIONS</b>	<b>16</b>
3.3.1 <u>Responsibility</u> .....	16
3.3.2 <u>Identification of IP (including duty of confidentiality)</u> .....	16
3.3.3 <u>Coverage of the Regulations</u> .....	19
3.3.4 <u>Exceptions to the Regulations</u> .....	20
3.3.5 <u>Disclosure of IP</u> .....	20
3.3.6 <u>Ownership of IP</u> .....	21
3.3.7 <u>Modus Operandi for Commercial Exploitation of the IPR</u> .....	21
3.3.8 <u>IPR protection</u> .....	22
3.3.9 <u>Revenue Sharing Mechanism</u> .....	23
3.3.10 <u>Leaving the EUC</u> .....	23
3.3.11 <u>Applications to use the EUC's IP</u> .....	23
3.3.12 <u>Breach of the Regulations</u> .....	23
3.3.13 <u>Discretion to assign/licence back</u> .....	23
3.3.14 <u>Amendments to the Regulations</u> .....	24
3.3.15 <u>Death</u> .....	24
3.3.16 <u>Disputes</u> .....	24
<b>4. OFFICES, COMMITTEES AND CENTRES FOR RESEARCH</b>	<b>25</b>
4.1 <u>VICE RECTOR FOR RESEARCH AND EXTERNAL AFFAIRS</u> .....	25
4.2 <u>SENATE RESEARCH COMMITTEE</u> .....	25
4.3 <u>RESEARCH FOUNDATIONS AND CENTRES</u> .....	25
4.4 <u>RESEARCH OFFICE</u> .....	25
<b>5. RULES GOVERNING EXTERNAL RESEARCH PROGRAMS</b>	<b>26</b>
5.1 <u>SUGGESTED PROCEDURE FOR SUBMITTING AND IMPLEMENTING A FUNDED RESEARCH PROJECT</u> .....	26
5.1.1 <u>SUBMISSION OF RESEARCH PROPOSALS</u> .....	26
5.1.2 <u>PROJECT IMPLEMENTATION</u> .....	26

<b>5.1.3 FINANCIAL ISSUES CONCERNING EXTERNALLY FUNDED RESEARCH PROJECTS .....</b>	<b>27</b>
<b>5.1.4 UNIVERSITY RESEARCH FUND</b>	<b>28</b>
<b>6. RULES GOVERNING INTERNAL RESEARCH AWARDS</b>	<b>28</b>
<b>6.1 PURPOSE .....</b>	<b>28</b>
<b>6.2 ELIGIBILITY FOR THE AWARDS .....</b>	<b>29</b>
<b>6.3 APPLICATION PROCEDURE.....</b>	<b>29</b>
<b>7. TEACHING HOURS REDUCTION FOR RESEARCH PURPOSES</b>	<b>29</b>
<b>7.1 AWARD OF A THR FOR PARTICIPATION IN RESEARCH PROJECTS.....</b>	<b>29</b>
<b>7.2 AWARD OF A THR FOR WRITING A BOOK .....</b>	<b>30</b>
<b>7.3 AWARD OF A THR BY ACCUMULATION OF POINTS .....</b>	<b>30</b>
<b>8. EQUIPMENT ACQUIRED THROUGH INTERNAL AND EXTERNAL FUNDING</b>	<b>31</b>
<b>8.1 EQUIPMENT ACQUIRED THROUGH UNIVERSITY FUNDS.....</b>	<b>31</b>
<b>8.2 EQUIPMENT PURCHASED THROUGH EXTERNAL FUNDING .....</b>	<b>31</b>
<b>8.3 PROVISION OF COMPUTING EQUIPMENT BY MIS .....</b>	<b>32</b>
<b>9. POLICY ON RESEARCH STAFF</b>	<b>25</b>
<b>9.1 Introduction.....</b>	<b>25</b>
<b>9.2 Definitions of Roles.....</b>	<b>25</b>
<b>9.3. Procedures for Appointment.....</b>	<b>30</b>
<b>9.4 Honorary Research Staff.....</b>	<b>31</b>
<b>9.5 Intellectual Property Rights.....</b>	<b>32</b>
<b>9.6 Involvement of Research Staff.....</b>	<b>32</b>
<b>APPENDIX A:</b>	
40	
<b>APPENDIX B:</b>	
40	
<b>APPENDIX C:</b>	
43	
<b>APPENDIX D:</b>	
44	
<b>D1. POINTS ACCUMULATION FROM RESEARCH .....</b>	<b>44</b>
<b>D2. POINTS ACCUMULATION FROM RESEARCH / DEPARTMENT OF ARTS.....</b>	<b>47</b>

## **Introduction**

Within the framework of further contribution to the research community, the mission of the European University Cyprus (from now on referred to as the University or EUC) is to develop a pioneering and innovative research infrastructure with the objective of generating new knowledge. The university focuses on both fundamental and applied research and wherever possible the commercial application or exploitation of the research results.

The policy is guided by the following broad objectives:

- 1) The establishment of an interdisciplinary approach for researchers with attractive conditions for accessible movement among institutions, disciplines, sectors and countries, without financial and administrative obstacles.
- 2) The creation of state of the art research infrastructures, including research centres, foundations, units and/or laboratories, which are integrated and networked and accessible to research teams from across the EUC.
- 3) Introduction of a simple and harmonized regime for intellectual property rights in order to enhance the efficiency of knowledge transfer, in particular between public research and industry.
- 4) Optimization of research programs and priorities, for example by developing joint principles for the administration of European, national and regional funding programs.
- 5) The strengthening of international cooperation enabling faculty and other scholars in the world to participate in various research areas, with special emphasis on developing multilateral initiatives to address global challenges.
- 6) The transfer of research-based knowledge to EUC students

Research is conducted by faculty members, research associates/research personnel and PhD students either on their own or within the framework of external (national, European, international) and internal funding programs that are launched by the University.

The Research Policy provides a code of conduct for research and is intended for all staff, including people with honorary positions, faculty members, special teaching personnel, scientific collaborators, special scientists, research associates, and students carrying out research at or on behalf of the University.

All groups mentioned above must familiarize themselves with the Research Policy to ensure that its provisions are observed.

# **EUC Research Ethics Policy**

## **1.1 Scope and Purpose**

1. The aim of the EUC Research Ethics policy is to promote and encourage a high quality research and enterprise culture, with the highest possible standards of integrity and practice. The policy applies to all academic, contract research and administrative staff, all research students, as well as undergraduate and masters students who are undertaking research. In short, the policy applies to all disciplines and research activities within the University, or sub-contracted on its behalf.
2. All staff and students are expected to act ethically when engaged in University business. Any research involving animals, human participants, human tissue or the collection of data on individuals requires ethical consideration. While particular attention must be paid to the interests of potentially vulnerable groups, such as children, the University recognises that it has a duty of care towards all members of the wider community affected by its activities. The University also recognises that it has a duty of care to its own staff, and that this includes the avoidance of harm to those undertaking research.
3. The University will establish a framework for research ethics governance in which its Research Ethics Committee will have a central approval, monitoring and training role. The University will establish a Research Ethics Committee with representatives from all the Schools. The Research Ethics Committee will put in place the procedures needed to obtain approval.

It is, however, recognised that it may not always be appropriate or practicable for ethical approval to be sought from the Research Ethics Committee especially when it comes to short or undergraduate projects. Normally undergraduate or taught projects will not require clearance from the Research Ethics Committee and the matter can be dealt with at School and/or Department level. However, when active intervention is involved whether physically invasive or psychologically intrusive the Research Ethics Committee will need to be consulted. In particular, university staff has an obligation to ensure that not only their own research but any undergraduate or masters student research conducted under their supervision is ethically sound. Where research projects are subject to external approval, the School or Department responsible must ensure that this approval is sought and given. Where approval for a project has been given by a Research Ethics Committee at another university, as may be the case with a collaborative project, the EUC Research Ethics Committee must be provided with proof of this.

4. For some research projects it may be necessary to obtain the approval of the Cyprus National Bioethics Committee. Researchers should consult directly with the Cyprus National Bioethics Committee. Contact details and more information on the approval process can be found on <http://www.bioethics.gov.cy> .

## **1.2 General Principles**

1. The EUC Research Ethics Policy is based on widely accepted principles and practices governing research involving human participants. The key elements are:
  - Minimal risk of harm to participants and researchers;
  - Potential for benefit to the society;
  - Maintenance of the dignity of participants;
  - Minimal risk of harm to the environment;
  - Voluntary informed consent by participants, or special safeguards where this is not possible;
  - Transparency in declaring funding sources;
  - Confidentiality of information supplied by research participants and anonymity of respondents;
  - Acknowledgement of assistance;
  - Appropriate publication and dissemination of research results;
  - Independence and impartiality of researchers.

## **1.3 The Definition of Human-Related Research**

1. All human-related research which includes one or more of the following require ethical assessment and approval at the appropriate level:
  - Direct involvement through physically invasive procedures, such as the taking of blood samples
  - Direct involvement through non-invasive procedures, such as laboratory-based experiments, interviews, questionnaires, surveys, observation
  - Indirect involvement through access to personal information and/or tissue
  - Involvement requiring consent on behalf of others, such as by parents for a child participant

## **1.4 Vulnerable Participants**

1. Some participants may be particularly vulnerable to harm and may require special safeguards for their welfare. In general, it may be inappropriate for undergraduates to undertake research projects involving such participants.

- 
2. Particularly vulnerable participants might be:
  - Infants and children under the age of eighteen
  - People with physiological and/or psychological impairments and/or learning difficulties.
  - People in poverty
  - Relatives of sick, or recently—deceased, people

## **1.5 The Legal Framework, the Role of Professional Associations and Research Councils**

1. All research undertaken under the auspices of EUC must meet statutory requirements. Of particular relevance is the Bioethics Law (N.150 (I)/2001 and 53 (I)/2010), the Data Protection Law (2001), the Patients Protection Law (2005), and all those laws that create the legal framework for the Cyprus National Bioethics Committee.
2. Researchers in particular disciplines should comply with any research ethics guidelines set out by their professional associations.
3. Research Councils, charitable trusts and other research funding bodies in most cases require an undertaking from grant applicants that research proposals involving human participants have been approved by the University Research Ethics Committee or another appropriate body. Some also require audited compliance with their guidelines.

## **Good Research Practices / Code of Ethical Conduct in Research**

### **Code of ethical conduct in research**

Scholarly inquiry and the dissemination of knowledge are central functions of the University. They can be carried out only if faculty and research personnel abide by certain rules of conduct and accept responsibilities stemming from their research. And they can only be carried out if faculty and research personnel are guaranteed certain freedoms. The University expects that faculty and research personnel will be bound by the following research practices:

All faculty and research personnel are free to choose any research matter, to receive support from any legitimate source, and to create, analyse and derive their own findings and conclusions.

Research methods, techniques, and practices should not violate any established professional ethics, or infringe on health, safety, privacy and other personal rights of human beings and/or animals.

The above principles define the university's role with respect to research carried out on its premises. They are set forth to reinforce, and not diminish each faculty and research personnel's personal responsibilities toward their research, and to assure that each faculty and research personnel's source of funding and research applications are consistent with moral and societal conscience.

### **Openness in research**

The University recognizes and supports the need for faculty and research personnel to protect their own rights, be they academic or intellectual property rights. Even so, the University encourages all faculty and research personnel to be as open as possible when discussing their research with other researchers and the public. This aims at the dissemination of research performed in the University to enhance the international research community's knowledge and understanding.

### **Integrity**

Faculty and research personnel must be honest about their research and in their review of research coming from other researchers. This applies to all types of research work, including, but not limited to, analysing data, applying for funding, and publishing findings. The contributions of all involved parties should be acknowledged in all published forms of findings.

Faculty and research personnel are liable to the society, their professions, the University, their students and any funding agency that may fund their research. For this reason, faculty and research personnel are expected to understand that any form of plagiarism, deception, fabrication or falsification of research results are regarded as grave disciplinary offences managed by procedures described in detail in Section 2.4.

Any real or potential conflict of interest should be reported by faculty and research personnel to any affected party in a timely manner in all matters concerning research and peer review. According to the United States National Institute of Health "Conflict of interest occurs when individuals involved with the conduct, reporting, oversight, or review of research also have financial or other interests, from which they can benefit, depending on the results of the research." (<http://www.nih.gov>).

### **Misconduct in research**

Misconduct in research may involve Fabrication, Falsification, or Plagiarism in proposing, performing, or reviewing research, or in reporting research results. To prove that there has been misconduct in research, the following conditions must be met: The performance of said research has significantly deviated from accepted practices used in the field that the research was performed, and there was intention in the misconduct by the researcher(s).

Any allegations about misconduct in research will be investigated by the University thoroughly, through a special committee formed as described in the University Charter, Annex 11, Article VII.

# **Intellectual Property Policy**

## **Introduction**

The EUC is dedicated to teaching, research, and the extension of knowledge to the public. Faculty, research personnel, and students at the University, hereafter referred to as "University Employees," recognize as two of their major objectives the production of new knowledge and the dissemination of both old and new knowledge. Because of these objectives, the need is created to encourage the production of creative and scholarly works and to develop new and useful materials, devices, processes, and other inventions, some of which may have potential for commercialization.

The University acknowledges the need for an Intellectual Property Rights (IPR) policy, which will promote the University's reputation as socially relevant, leading research and teaching organisation and will directly contribute to the financial position of the EUC if its commercial value is realised.

The policy is based on the principles that will govern the ownership rights emanating from research of and/or materials produced by the EUC's members of staff and students, and to establish objectively fair and equitable criteria for the transfer of knowledge. The EUC thus aims to provide support services to promote the creation of Intellectual Property (IP) whilst seeking to maximise the commercial exploitation of the resulting IPR.

Intellectual Property includes, but is not limited to, patents, registered designs, registered trademarks and applications and the right to apply for any of the foregoing, copyright, design rights, topography rights, database rights, brands, trademarks, utility model rights, rights in the nature of copyright, knowhow, rights in proprietary and confidential information and any other rights in inventions.

The EUC acknowledges that registration and commercial exploitation of Intellectual Property is often a long and costly process that is justified once it is ascertained that there exists a business case for such registration and exploitation. It is known that in practice, only a small number of works can be commercially exploited in a viable manner, depending on the nature and marketability of the work in question.

## **Definitions**

For the purposes of this Policy:

**Creator** - "Creator" shall mean, employees of EUC, a student, non-employees contracted to EUC for contracts and services, or a member of a Visiting Teaching Staff involved in the production of Disclosable Work.

**Disclosable Work** – "Disclosable Work" shall mean such work that is novel, original, and/or important and is likely to bring impact and enhance the Creator's reputation. This work is characterised by the IP rights it generates.

Intellectual Property Policy – “IP Policy” is the name of the policy described here that outlines the regulations of the EUC in regard to disclosure and exploitation of Intellectual Property Rights (IPR).

Organisation – “Organisation” for the purpose of this document is the European University Cyprus (EUC).

Intellectual Property Adjudication Committee – is the name of the committee established to resolve disputes over interpretation or claims arising out of or relating to this policy, or dispute as to ownership rights of Intellectual Property under this policy.

Office of the Vice Rector for Research and External Affairs – is the office within the EUC responsible for the development of and enacting this IP Policy and is the interface between the EUC and the Technology Transfer Facility.

Technology Transfer Facility – “TTF” for the purpose of this policy, is the relevant body responsible for Technology Transfer support in Cyprus.

### **3.3 Intellectual Property Regulations**

#### **Responsibility**

1. The IP Policy acknowledges that all members of staff and students have responsibilities with regard to IPR arising from and/or used by them in the course of their teaching/employment.
  2. The IP Policy also recognises that all members of staff and students require

support and assistance to help them to meet their responsibilities and this will be provided by the Office of the Vice Rector for Research and External Affairs and, subsequently, by the Technology Transfer Facility.

#### **Identification of IP (including duty of confidentiality)**

1. It is expected that identification will take place when employees, students, or members of staff are involved in creating and developing IP. Much of the IP which will be created by the EUC’s employees may be anticipated prior to its creation depending on the nature of the project in question and outputs and results that are expected to be generated. Examples of such outputs which are likely to have potential IP rights arising include (but are not limited to):
  - Inventions (whether or not patentable);
  - Methodologies;
  - Software;
  - Databases;
  - Educational/training materials and tools;
  - Modelling tools;
  - Solutions to technical problems; and

- Design/artistic products.
2. A Summary of the main classes of IPR is listed below:

### Patent

A registered patent provides a time-defined (up to 20 years) geographically defined monopoly right to exploit a new commercially valuable invention or process. The basis of the permission to exploit is that the invention's working is disclosed, although patenting is not possible if there has been ANY prior disclosure of the invention. Patents are governed by Cyprus Law or EU Law such as the New Patent Law of Cyprus (Law No. 16(I)/1998).

### Copyright

This time-limited right (which varies between 25 and 70 years according to the material) arises automatically on the physical creation (not the idea) of software, original literary, dramatic, artistic or musical work, and in recorded (e.g. film) or published (e.g. layout) derivations. Use of the © mark and owner's name and date is the internationally recognised way of alerting the public to the copyright ownership but the protection (the right to preventing unauthorised copying) exists regardless. Copyright is governed by the Copyright Law, 59/76.

Copyright may be assigned to a third party, but until that point or until a licence is agreed it remains the property of the Creator, unless s/he creates the work 'in the course of his/her employment', in which case it is the property of the employer.

### Moral rights

All European countries recognise an author's moral rights. In Cyprus, there are two moral rights: the right of paternity and the right of integrity. These rights relate to the reputation or standing of the creator in the eyes of fellow human beings. To infringe a moral right involves denigrating or harming the author's reputation. The right of integrity means the creator has the right to object to derogatory treatment of his/her work. Basically, this means changing it in a way that affects the nature of the work without permission. Moral rights can be waived (i.e. the author chooses not to exercise the rights) or they can be bequeathed. They cannot be assigned.

### Performing rights

Creators of copyright works have the right to protect the physical form in which those works are created – words on the page, pigment on a canvas, or the clay or metal of a sculpture. Performers such as teachers, actors, musicians and dancers also enjoy protection of their performance, especially when recorded on film, video, tape, CD, or in other form.

Performing rights may affect the multimedia elements of online courseware, as well as the Creator's copyright in the material itself.

### Database Right

This time-limited (15 years) right arises without registration to protect the compilers of non-original information from losing the benefit of their work through unauthorised copying or re-use.

### Industrial Designs

There is automatic time-limited (15 years) protection (the right to prevent unauthorised copying) for unregistered designs, provided authorship can be proved, under the Legal Protection of Industrial Designs and Models Law 4(I)/2002. This design right covers "the appearance of the whole or a part of a product resulting from the features of, in particular, the lines, contours, colours, shape, texture and/or materials of the product itself and/or its ornamentation" on condition of novelty of the design.

On registration under Legal Protection of Industrial Designs and Models Law, the designer of the new pattern or shape which has aesthetic appeal (can be 2 or 3 dimensional) acquires a monopoly right of commercialisation for a maximum of 25 years from the filing of the application, divided into 5 periods of 5 years.

An unregistered community design (UCD) gives its owner the right to prevent unauthorised copying of their design throughout the European Union. It is not a monopoly right and lasts for 3 years from the date on which the design was first made available to the public within the Community.

### Domain Names

Registering a domain name for Internet use gives a right to use the domain name typically for a period of two years, registered with bodies like ICANN internationally and the University of Cyprus in Cyprus. Owners of trademarks can have established rights to domain names.

### Trade Marks

Registering a trade mark under the Cyprus Trade Marks Law, Chapter 268, gives a monopoly right for the use of graphically distinct trading identification signs. Unregistered trade marks have some protection through court actions against "passing off" (piracy), provided that their use has not lapsed for a period of 5 years. Cyprus legislation is fully harmonised with EU Standards applicable in trade mark protection.

3. EUC's members of staff and students undertake to keep confidential and not disclose any confidential information, data, materials, knowhow, trade secrets or any other IP, to any unauthorised third party and shall also undertake to keep such information secure and strictly confidential both during the course of

research activity, be it of an Academic or Collaborative/Contract nature, and also on and following completion thereof.

4. Any breach of this confidentiality and non-disclosure obligation constitutes a serious breach and may lead to disciplinary action and does not prejudice the rights of the EUC to file any action for damages or any other rights available at law.

## **Coverage of the Regulations**

1. Whom does this IP Policy apply to?
  - Employees:  
By persons employed by the EUC in the course of their employment.
  - Students:  
By student members in the course of or incidentally to their studies at EUC.
  - Non-employees contracted to the EUC:  
By persons engaged by EUC under contracts for services during the course of or incidentally to that engagement.
2. Sabbatical, Seconded, Visiting Academics and others:  
By other persons engaged in study or research in the University who, as a condition of their being granted access to the EUC's premises or facilities, have agreed in writing that this Part shall apply to them.
3. Participation of the EUC members of staff/employees and or students in Collaborative and/or Contracted Research.  
The preparation and negotiation of any IP agreements or contracts involving the allocation of rights in and to IP will be undertaken by a competent person authorised for this purpose by the EUC.  
Issues that will be addressed in such agreements include, but will not always be limited to:
  - ownership of Foreground IP;
  - licences to Foreground IP for uses outside the project;
  - ownership of Background IP;
  - licences to use Background IP in the project or activity in question and in relation to the use of the Foreground IP arising from such project or activity;
  - allocation of rights to use or commercialise IP arising from any such project or activity and the sharing of revenues; and
  - publications arising from the relevant project or activity and the rights arising from such projects or activities.The terms of such agreements may be subject to negotiation.

## **Exceptions to the Regulations**

1. Unless specifically commissioned, typically the EUC will NOT claim ownership of copyright in certain types of Disclosable Work described in this policy as "Creator Copyright Works":
  - artistic works;
  - text and artwork for publication in books;
  - articles written for publication in journals;
  - papers to be presented at conferences;
  - theses and dissertations;
  - oral presentations at conferences;
  - posters for presentation at conferences; and
  - musical scores.
2. Where IP has been generated under the exception clause of this regulation, the EUC may assign the copyright to the Creator.
3. Students – undergraduate and/or postgraduate.

## **Disclosure of IP**

1. All persons bound by these Regulations are required to make reasonably prompt written disclosure to the EUC's Office of the Vice Rector for Research and External Affairs at the outset of the work or as soon as they become aware of it (by completion of the Invention Disclosure Form, the information required for which is provided in Appendix B):
  - any IP of potential commercial value arising from their work;
  - the ownership by a third party of any IP referred to or used for their work;
  - any use to be made of existing EUC IP during their work;
  - any IP which they themselves own which is proposed to be used by the EUC.
2. Creators shall keep all Disclosable Work confidential and avoid disclosing this prematurely and without consent;
3. Only disclose any Disclosable Work and the IP relating to it in accordance with the EUC's policy and instructions;
4. Seek EUC's consent to any publication of information relating to any Disclosable Work;
5. Creators must NOT:
  - i. apply for patents or other protection in relation to the Disclosable Work; and
  - ii. use any Disclosable Work for their own personal and/or business purposes and/or on their own account.

## **Ownership of IP**

1. Ownership of IP created by an individual who is an employee is generally determined by considering:
  - Who created the IP?
  - Was the IP created in the course of the Creator's employment?
  - Are there any contractual conditions that affect ownership?
2. Assignment of ownership rights  
Generally, the Creator of IP is its legal owner. From the EUC's point of view, the most important exception to this is the general rule that IP is owned by a person's employer where the IP is created as part of, or through the auspices of, the person's employment.
3. The EUC claims ownership of all the Intellectual Property specified in section 2.2, which is devised, made or created by those specified in section 3 and under the exceptions to the regulations in Section 4. It also includes but is not limited to the following:
  - i. Any work generated by computer hardware/software owned/operated by the EUC.
  - ii. Any work generated that is patentable or non-patentable.
  - iii. Any work generated with the aid of the EUC's resources and facilities including but not limited to films, videos, field and laboratory notebooks, multimedia works, photographs, typographic arrangements.
  - iv. Any work that is registered and any unregistered designs, plant varieties and topographies.
  - v. Any University commissioned work generated. Commissioned work is defined as work which the EUC has specifically employed or requested the person concerned to produce, whether in return of special payment or not and whether solely for the University or as part of a consortium.
  - vi. Know-how and information related to the above
  - vii. Any work generated as a result of the teaching process including but not limited to teaching materials, methodologies and course outlines.
  - viii. Material produced for the purposes of the design, content and delivery of an EUC course or other teaching on behalf of the school, whether used at the school's premises or used in relation to a distance learning and/or e-learning project. This type of material includes slides, examination papers, questions, case studies, and assignments ("course materials").
  - ix. Material for projects specifically commissioned by the EUC
  - x. All administrative materials and official EUC documents, e.g. software, finance records, administration reports, results and data.

## **Modus Operandi for Commercial Exploitation of the IPR**

1. The EUC is entitled to commercially exploit any result obtained under its aegis (unless this entitlement is relinquished). The Office of the Vice Rector for Research and External Affairs has the responsibility for administration of Disclosures and will

work with the TTF of Cyprus, which has responsibility for commercialisation of Disclosures. As guidance to the commercialisation process, the EUC/TTF will follow a standard process, graphically presented in Appendix A.

2. The Creator/s shall notify the Office of the Vice Rector for Research and External Affairs of all IP which might be commercially exploitable and of any associated materials, including research results, as early as possible in the research project. This notification shall be effected by means of an Invention Disclosure Form (contents as noted in Appendix B). In case of doubt as to whether research is commercially exploitable or otherwise, the Creator/s undertake/s to seek the advice of Cyprus Central TTF.
3. The Office of the Vice Rector for Research and External Affairs shall immediately acknowledge receipt of the Disclosure Form. In consultation with the TTF and the Creator/s, shall decide whether the EUC and the TTF has an interest to protect and exploit the relevant IPR.
4. The TTF shall communicate the decision in writing to the Office of the Vice Rector and the Creator/s by not later than three months from the date of receipt of the Invention Disclosure Form. If the EUC and TTF decide to protect and exploit the IPR, it is understood that:
  - the Creator/s shall collaborate with the EUC and the TTF, to develop an action plan for the protection and commercial exploitation of the IP;
  - the TTF in collaboration with the Creator/s shall ensure that third party rights are not infringed in any way through the process; and
  - the EUC/TTF shall seek to protect the right of the Creator/s to use the said IP for strictly non-commercial purposes.
5. Should the EUC and TTF decide that there is no interest in protecting and exploiting the relevant IPR, or should it fail to inform the Creator/s about its decision within the stipulated time, the EUC may assign all its rights, title and interest in such IP to the Creator/s concerned, whilst the EUC retains the right to use the said IP in whichever manifestation for strictly non-commercial purposes.
6. The Creator/s SHALL NOT enter into any sponsorships or commercial agreements with third parties related to their research at EUC without prior written authorisation by the Office of the Vice Rector for Research and External Affairs. This said, it is understood that consent shall generally be granted to Creator/s for such requests as long as the IPRs of the EUC are safeguarded; otherwise the claims on IPR expected by the third party must be agreed upon explicitly upfront.

## **IPR protection**

1. Some forms of IP require active steps to be taken to obtain protection (e.g.: patents, registered trademarks and registered designs). Other forms of IP rights are protected on creation (e.g. Copyright, EU Database Rights) but still require appropriate management in order to maximise the protection available. Best practices in patent protection require that all materials made publicly available by any employees, members of staff and/or students should include a copyright notice.

2. Any decisions relating to the registration of any IP rights such as making an application for a patent or a registered trade mark or a registered design (including any decisions to continue or discontinue any such application) should be made in consultation with the Office of the Vice Rector for Research and External Affairs and the TTF. The IP registration process can be very expensive and IP protection costs should not be incurred without appropriate consideration of how such costs will be recovered.

### **Revenue Sharing Mechanism**

The EUC's employees and students can benefit from the Revenue Sharing Scheme if their work generates income for the EUC. The scheme is presented in Appendix C. Note that such revenue to be shared is typically calculated after deduction of all costs incurred by the EUC and TTF in developing, protecting, exploiting, and marketing the Disclosable Work and the Intellectual Property it contains.

### **Leaving the EUC**

Cessation of employment, under normal circumstances, will not affect an individual's right to receive a share of revenue. Exceptions to this rule include: cessation of employment due to disciplinary actions.

### **Applications to use the EUC's IP**

1. The EUC may be willing to consider requests from its staff and/or students for a licence to use specific IP, owned by EUC for their use although the terms and decision to grant any such licences is a decision wholly made by the EUC.
2. Applications for such licence should be made in writing to the Office of the Vice Rector for Research and External Affairs.

### **Breach of the Regulations**

1. Breach of the regulations listed in this Policy may be a disciplinary matter for the EUC's staff and students under the normal procedures.
2. The EUC shall consider all avenues available to it, including legal action if necessary, in respect to persons bound by these regulations who acted in breach of them.

### **Discretion to assign/licence back**

1. If the EUC does not wish to pursue the commercialisation of any Intellectual Property or does not wish to maintain an interest in the IPR, it has the right to assign such IPR rights to the Creator/s of the IPR by entering into an agreement to enable the IP to be used by the Creators. This will generally only be granted

where there is clear evidence that the IP provides no other benefit to the EUC and is not related to other IP, which the EUC has an interest in.

However, the EUC shall not assign its IP if they consider that the commercialisation of the IP could potentially bring harm to the name of the EUC. Decisions regarding potential harm will be taken by the Research Ethics Committee of EUC.

2. Requests for any transfer of rights from the EUC to another party with rights should be made in the first instance to the Vice Rector for Research and External Affairs.

## **Amendments to the Regulations**

These Regulations may be amended by the Senate of the EUC on the recommendation of the Vice Rector for Research and External Affairs.

## **Death**

In the event of a researcher's death, the entitlement shall continue for the benefit of his or her estate.

## **Disputes**

1. Any question of interpretation or claim arising out of or relating to this policy, or dispute as to ownership rights of intellectual property under this policy, will be settled by submitting to the EUC's Intellectual Property Adjudication Committee a letter setting forth the grievance or issue to be resolved. The committee will review the matter and then advise the parties of its decision within 60 days of submission of the letter.
2. The Intellectual Property Adjudication Committee will consist of a chair who is a member of the tenured faculty, at the rank of either a Professor or an Associate Professor, one member of the faculty from each School, at the rank of either Assistant Professor or Associate Professor or Professor, an individual from the EUC with knowledge of Intellectual Property and experience in commercialisation of Intellectual Property, and two other members representing, respectively, the EUC administration, and the student body. The chair will be appointed by the Vice Rector for Research and External Affairs, with the advice and consent of the Senate Research Committee, and the remaining members of the committee will be appointed: the faculty members, each by their School's Council, the administration representative by the University Council or its designee, and the student representative by the Student Union.

The committee will use the guidelines set forth in this policy to decide upon a fair resolution of any dispute.

3. Any disputes regarding the revenue distribution from the exploitation of Disclosable Works will be dealt with in accordance with the EUC's normal member of staff or student dispute procedures as outlined in the contractual terms of conditions.

4. The Parties shall attempt to settle any claim, dispute or controversy arising in connection with this Policy, including without limitation any controversy regarding the interpretation of this Policy, through consultation and negotiation in good faith and spirit of mutual cooperation. Where such claims or disputes cannot be settled amicably, they may be taken to court.
5. This Agreement shall be governed by, and construed in accordance with the laws of Cyprus.

## **Offices, Committees and Centres for Research**

### **Vice Rector for Research and External Affairs**

The Vice Rector for Research and External Affairs (from now on referred to as the Vice Rector) is the person responsible for representing the University on research matters and enhancing activities related to research within the University. Moreover the Vice Rector facilitates and supports, when asked by faculty or research members, all research activities, including the implementation of research projects, the organization of scientific conferences and the establishment of research units/labs. In addition, the Vice Rector is responsible for the smooth implementation of the University's Research Policy.

### **Senate Research Committee**

The administration of the research activity is facilitated by the Senate Research Committee of the University. The Committee composition is prescribed in the University Charter and the Committee is accountable to the Senate of the University.

### **Research Foundations and Centres**

Research is carried out in university departments, research foundations, and centres. The Senate suggests to the University Council the formation of new foundations and research centres or the discontinuation of existing ones, if necessary.

The University Council approves the establishment of these foundations and research centres. Separate regulations are issued for the establishment of University research centres. Detailed description of the mission, area of specialization, and operation of each foundation or research centre is given in a separate document.

### **Research Office**

Detailed description of the mission, area of specialization, and operation of the Research Office is given in a separate document.

# **Rules Governing External Research Programs**

## **Suggested procedure for submitting and implementing a funded research project**

The following rules apply for externally funded research projects:

### **5.1.1 Submission of research proposals:**

Faculty and research personnel that are interested in submitting a proposal or participate in a proposal for ANY kind of externally funded research project (commercial, consultancy, RPF, European etc) should consult and get the approval of the EUC Research Office. The formal procedures developed by the Research Office pertaining to the development of a research proposal and to participation in a research project should be followed in all cases. Given that in all research and consulting application forms a budget also needs to be prepared, the budget will be developed in collaboration with the EUC Research Office, sharing their expertise with the faculty and research personnel and advising them accordingly about the cost models and cost categories used in each case. This procedure should make sure that the proposal satisfies all the necessary criteria of the particular research call.

The final approval for financial and administrative issues of proposals or projects will be signed by the legal representative of EUC.

### **5.1.2 Project implementation**

The formal procedures developed by the Research Office pertaining to the administration of a research project should be followed in all cases.

In the case where a project is awarded, a copy of the contract and all the original receipts, invoices, contracts and other accounting documents regarding expenses of the project will be maintained by the EUC Research Office without any additional remuneration or personnel costs added to the budget of a project. The researcher/s involved in an externally funded project are responsible for submitting all receipts, invoices, contracts and other accounting documents relevant to their project to this department. No payment will be processed before the submission of the aforementioned documents to the Research Office.

Timesheets should be kept for all projects. These will be used as the basis for calculating the money to be paid to researchers for all types of projects. The EUC Research Office will assist researchers to calculate the hourly and daily rate for each staff member.

The researcher must also inform the Chief Financial Officer of the University, through the EUC Research Office, in order to create a separate ledger (account)

in the University's Accounts Department. After completion of the project, the Accounts Department will keep the file on record for 5 years or more if needed by the contractual agreement.

The EUC Research Office should keep a file with all the details concerning the project. The file must be made available to the Senate Research Committee upon request.

### **5.1.3 Financial issues concerning externally funded research projects**

All incoming funds for the execution of a project are deposited in a separate account (ledger) of the University and all necessary expenses with their receipts relating to the project are paid/signed by the Vice Rector for Research and External Affairs, the CFO and the CEO of the University.

The time spent by faculty and research personnel on national, European or international research projects is, with rare exceptions, an eligible cost for inclusion in a project budget at a level which reflects the time to be spent by faculty and research personnel on the project and the employer's cost. These are real project costs and their inclusion in project budgets is strongly required.

Salary payments to faculty and research personnel will be paid out regularly by the Accounts department upon the project coordinator's request to the Research Office and provided that the allocated amount for the previous period has been received from the funding agency and all reporting requirements for the previous period to the funding agency have been met.

In cases of delay in receiving the predetermined instalment, the University will grant to the researcher the required funds (not his/her compensation/remuneration but costs such as equipment, consumables, traveling) to initiate the research, provided that a copy of the contract and all necessary documentation had been submitted to the Research Office.

Employment of additional temporary staff, budgeted for completion of the research project, will be the responsibility of the project coordinator. The remuneration for temporary staff will depend on the corresponding budget of the project and the possible allocation of funds for this purpose.

Subcontracting activities within the framework of a research project will be the responsibility of the project coordinator. These activities should be in alignment with the corresponding budget of the project, the grant rules, and the EUC subcontracting policy.

In the case where a faculty or research personnel fails to complete a research project due to failure to meet his/her contractual obligations, or if it is clear that there was an intention of misconduct and there are financial damages laid upon

the University relating to this event, the faculty or research personnel is liable to pay these damages. This will not be applied in cases such as health problem, etc, where there is clearly not an intention of misconduct.

#### **5.1.4 University research fund**

All funds allocated for research from externally-funded research projects, the University as well as funds offered for research purposes from third parties will be deposited in the University Research Fund. Recommendations for the allocation of funds are made by the Senate Research Committee and are subject to the final approval of the Management of the University. These funds can be used to finance such activities as:

- (a) Participation of academic researchers in conferences, seminars, and meetings to co-ordinate activities, which are needed for submission of external programs.
- (b) The administration costs associated with providing support services to academic researchers.
- (c) Organisation of training seminars for the faculty and research personnel of the University; these seminars shall be organized if and only will help/assist and/or facilitate researchers to enhance and further develop their knowledge in subjects related to their research fields and help them design and implement research projects.
- (d) Purchase of software, hardware and equipment that are needed by faculty and research personnel for research projects.
- (e) The funding for the University's Internal Research Awards such as PhD scholarships
- (f) Development of Infrastructure related to the research activity of the University.
- (g) Funding of the activities of the Research Office of the University.

## **6 Rules Governing Internal Research Awards**

The University's "Internal Research Awards" (IRA) are launched on an annual basis by the Senate Research Committee, are announced by the Vice Rector for Research & External Affairs and financed by the University Research Fund and external sponsors as described in Section 5.1.4 above.

#### **6.1 Purpose**

IRAs are awarded to EUC faculty in order to pursue research and other creative work. IRAs provide support for exploratory research projects which might result in proposals submitted for external funding or in creative work that is likely to enhance the recognition of the faculty and research personnel and the University at large.

IRAs may be used for funding travel, equipment, supplies, PhD student assistants' scholarships, student assistants, research assistants and other expenses. Funding for this program comes from the University Research Fund.

## **6.2 Eligibility for the awards**

All full-time faculty members of the University who have the rank of Assistant Professor or higher are eligible to apply for the awards. Specific eligibility criteria may apply for each type of award.

## **6.3 Application Procedure**

The Vice Rector for Research and External Affairs initiates the selection process by issuing a call for proposals. The deadline for the submission of proposals will be announced. Application materials will be available from the office of the Vice Rector for Research and External Affairs and the proposals will be submitted electronically to the office of the Vice Rector.

# **7 Teaching Hours Reduction for Research Purposes**

The University rewards members of staff who excel in research by awarding them Teaching Hours Reduction (THR). A THR may be awarded if the member of staff fulfils the conditions in one or more of the three schemes outlined below.

A member of staff may be awarded a THR under more than one of the schemes described below if he/she is eligible. The minimum teaching per semester can be reduced down to 6 hours per week based on the accumulated research load reduction hours. An exemption may be considered for Deans and Chairs.

All allocations of THR under the three schemes outlined below will be made after a recommendation of an ad-hoc committee chaired by the Vice Rector for Research and External Affairs. The committee will take into account scheduling constraints and other considerations for the sustainable development of research activity at the university. The committee will meet at an appropriate time in each semester in order to make the THR allocations in time for the preparation of the schedule of classes for the next semester.

## **7.1 Award of a THR for participation in research projects**

Members of staff are eligible to apply for a Teaching Hours Reduction (THR) when conducting funded research for the full duration and until the completion of relevant funded projects. Should their application meets with success, funded project coordinators are entitled to a three-hour teaching reduction per semester for the whole duration of the project, whereas research partners are eligible for a THR equivalent to at least one third of the duration of the project.

Based on the policy of the University with regard to THR requests, Faculty, research and Other Teaching Personnel (OTP) members are expected to submit a written request to the Chairperson of his/her Department before the beginning of the academic year/semester. The Chairperson will process the THR request by way of making a relevant recommendation to the Dean of School. The Dean will then forward his/her recommendation to the Vice Rector for final approval. After the deadline expires, applications for teaching hours reduction will not be accepted.

The deadlines for submitting a request for teaching load reduction per semester are the following:

For the Fall Semester: 1st of May

For the Spring Semester: 31st of October

If a research proposal was awarded a grant after the special case of approval of a research/grant proposal (i.e. RPF, EU etc) while an academic year is in progress, a THR request should be submitted and be approved prior to the beginning of the next semester, during which the teaching load reduction will be applied. The research project should commence at least one month before the beginning of the next semester for the THR to be awarded.

## **7.2 Award of a THR for writing a book**

A three-hour teaching reduction per semester will be awarded for the purpose of writing a book upon submission of a publishing contract by a reputable publisher. A total of two THR allocations (maximum 6 credits) will be made under the scheme for each book contract. The same deadlines and application procedure apply as in the scheme described in section 7.1.

## **7.3 Award of a THR by accumulation of points**

A third scheme for the award of a THR takes into account the research activity of members of staff and the points they have accumulated according to the tables given in Appendix D. A THR of 3 hours per week is awarded to faculty members once they accumulate 100 (one hundred) points and the same number of points are automatically deducted from his/her accumulated total. Points accumulated over time but not utilized by a member of staff will simply remain at his/her disposal.

Note that members of staff may consider the year 2016 as the starting point for calculating points accumulated through research. The calculation of points will be valid after it has been approved by the Dean of the School and the Vice Rector for Research and External Affairs.

## **8 Equipment Acquired through Internal and External Funding**

### **8.1 Equipment acquired through University funds**

All equipment that has been acquired through funds that come directly through the university's funds (internal research grants, university research funds) will belong solely to the University and will be used by the faculty and research personnel's affiliated department or lab, according to the affiliation used by said faculty and research personnel in the funded research proposal and/or project. The faculty and research member is entitled to use the equipment throughout the duration of the funded project and this remains within the research unit/laboratory once the project is completed, or within the faculty member's department, under his/her direct supervision if s/he does not belong to a unit / lab. Any required maintenance of the equipment should be undertaken by the University.

### **8.2 Equipment purchased through external funding**

Equipment (software and hardware) is often provided in full or partly in the budget of proposals for external funding to enable the faculty and research member to carry out research effectively. This kind of equipment (computers, projectors, software programs, fax and printing machines, etc.) is the property of the University but remains in the faculty or research personnel's research unit/laboratory or when this is not applicable in his/her department, under his/her supervision. The faculty member is entitled to use the equipment throughout the duration of the externally funded project. When faculty or research personnel who have had externally funded research projects leave the University, the status of any equipment purchased remains a property of the unit/lab or department that the faculty or research personnel belonged.

Any required maintenance of the equipment should again be undertaken by the University.

In the unlikely event that a faculty or research personnel obtains equipment via external funding that is not processed through the University's budget, the status of the equipment should be negotiated with the Vice Rector to determine ownership and responsibility for repair and replacement. Faculty or research personnel are encouraged to seek outside funding to upgrade, or replace their research equipment.

The Research Office is committed to working with faculty or research personnel to develop proposals for research and teaching equipment. Equipment grants usually require an institutional match, and faculty or research members are advised to consult with the Research Office and the Director of MIS early in the process about this matter. The MIS should be able to help faculty or research personnel to identify the best hardware and software products and estimate costs for proposal budgets.

### **8.3 Provision of computing equipment by MIS**

The MIS department supplies desktop office computers, computer teaching labs, copy and printing machines and other types of equipment needed for research (software and hardware). The Director of the MIS department is responsible for keeping the University's inventory records and adjust these in the case of equipment purchases or wearing out of equipment (being fully depreciated).

## **9 Policy on Research Staff**

### **9.1 Introduction**

Academic Research Staff are EUC contract employees hired to work on EUC research activities as defined below. As EUC employees, Academic Research Staff are subject to all policies and procedures related to EUC employment, and receive all benefits implied by the employment law.

### **9.2 Definitions of Roles**

The following positions for research staff are being described in the following sections:

- Research Associate
- Research Fellow
- Senior Research Fellow
- Honorary Research Staff

#### **9.2.1 Job Description for the Position of Research Associate**

##### **9.2.1.1 Overall Role**

For researchers who are educated to first degree level (and Master's degree) and who possess sufficient breadth or depth of knowledge in the discipline of research methods and techniques to work within their own area. Role holders who gain their doctorate during the course of employment will normally be recommended for promotion to Research Fellow, if this is appropriate for the duties and responsibilities of the post.

As a team member of the Research Laboratory/Program the Research Associate will contribute quality research outputs and conceptual support to projects. With the guidance of the supervisor/program leader, and within the bounds of the Research Laboratory/Program mandate, the Research Associate will:

##### **9.2.1.2 Key Responsibilities**

- Conceptualize and conduct short-term experiments and research activities in support of broadbased/longitudinal research projects, ensuring consistency with established

methodological approaches and models, adherence to project timelines, and completeness of documentation;

- Conduct studies of related literature and research to support the design and implementation of projects and development of reports, ensuring conceptual relevance, comprehensiveness, and currency of information;
- Write and publish articles in peer-reviewed journals that highlight findings from research and experimental activities ensuring consistency with the highest standards of academic publication and showcasing the Centre's/Program's scientific leadership;
- Communicate to Program/Project team developments/progress and results of research activities ensuring that relevant information and issues in the implementation of projects/experiments are captured in as comprehensive and timely manner as possible;
- Develop collaborative links with core scientific personnel in related program areas to gain exposure to, and build knowledge on experimental/research activities and approaches, in order to subsequently improve conceptual development and implementation of existing programs;
- Utilize appropriate and current techniques/protocols in experimental laboratory management to ensure integrity and security of experimental process, comprehensive documentation, and replicability of experimental procedures;
- Design and organize databases along project frameworks and experimental research design that support overall research management, including the monitoring and evaluation of project inputs, actions, and outcomes, as well as the subsequent integration of these databases to other databanks;
- Identify areas of improvement within the research structure using integrated management approaches in pursuit of capacity building/strengthening and the preservation of scientific rigor in research studies.
- To contribute to the design of a range of experiments/fieldwork/research methodologies in relation to the specific project that they are working on
- To set up and run experiments/fieldwork in consultation with the Principal Investigator, ensuring that the experiments/fieldwork are appropriately supervised and supported. To record, analyse and write up the results of these experiments/fieldwork.
- To prepare and present findings of research activity to colleagues for review purposes.
- To contribute to the drafting and submitting of papers to appropriate peer reviewed journals.
- To prepare progress reports on research for funding bodies when required.
- To contribute to the preparation and drafting of research bids and proposals.
- To contribute to the overall activities of the research team and department as required.
- To analyse and interpret the results of their own research

### **9.2.1.3 Skills and Qualifications**

Education: Level Bachelor and/or Master's in the Program Area

Experience and Skills:

Basic research skills and knowledge of research techniques

Ability to analyse and write up data

Ability to present and communicate research results effectively to a range of audiences

#### **9.2.1.4 EUC Pertaining Benefits**

Researchers will have access to facilities which are necessary and appropriate for the performance of their duties.

- Desk, Telephone line and PC
- MS Office, SPSS, Email and Printing Rights
- Business Cards with the University Emblem and the Research Laboratory they belong to
- Full access to the library

All researchers must receive the same forms of employment documentation as other academic-related staff of the University:

- a formal contract signed by the relevant appointing authority;
- written confirmation of any changes in the terms of employment;
- job description or the generic description of the role and, where appropriate, a list of expected research goals;
- further to the completion of the contract, researchers are responsible for returning in good condition all the equipment as well as business cards that have been provided to them

### **9.2.2 Job Description for the Position of Research Fellow**

#### **9.2.2.1 Overall Role**

A Research Fellow is a researcher with some research experience and who has typically been awarded a doctoral degree. A Research Fellow will often have supervisory responsibilities for more junior researchers and will often lead a team of researchers to achieve a research project's aims. They will initiate, develop, design and be responsible for the delivery of a program of high quality research and may have full authority over several phases of project work.

#### **9.2.2.2 Key Responsibilities**

- Design, Conceptualize and conduct short-term experiments and research activities in support of broadbased/longitudinal research projects, ensuring consistency with established methodological approaches and models, adherence to project timelines, and completeness of documentation;
- Supervise and Conduct studies of related literature and research to support the design and implementation of projects and development of reports, ensuring conceptual relevance, comprehensiveness, and currency of information;
- Write and publish articles in peer-reviewed journals that highlight findings from research and experimental activities ensuring consistency with the highest standards of academic publication and showcasing the Centre's/Program's scientific leadership;
- Take the lead within the team and communicate to Program/Project team developments/progress and results of research activities ensuring that relevant

information and issues in the implementation of projects/experiments are captured in as comprehensive and timely manner as possible;

- Develop collaborative links with core scientific personnel in related program areas to gain exposure to, and build knowledge on experimental/research activities and approaches, in order to subsequently improve conceptual development and implementation of existing programs;
- Utilize appropriate and current techniques/protocols in experimental laboratory management to ensure integrity and security of experimental process, comprehensive documentation, and replicability of experimental procedures;
- Design and organize databases along project frameworks and experimental research design that support overall research management, including the monitoring and evaluation of project inputs, actions, and outcomes, as well as the subsequent integration of these databases to other databanks;
- Identify areas of improvement within the research structure using integrated management approaches in pursuit of capacity building/strengthening and the preservation of scientific rigor in research studies.
- Develop research objectives, projects and proposals.
- Conduct individual or collaborative research projects.
- Identify sources of funding and contribute to the process of securing funds.
- Act as principal investigator on research projects.
- Manage and lead a team of researchers to achieve the aims of a research project.
- Oversee and appropriately supervise and support the research activities (experiments, fieldwork etc.) of a research program/project.
- Ensure that research results are recorded, analysed and written up in a timely fashion.
- Manage research grants in accordance with EUC Financial Regulations and the conditions of the funding body (e.g. EU, RPF etc.)
- Prepare and present findings of research activity to colleagues for review purposes.
- Submit papers to relevant peer reviewed journals and attend and present findings at relevant conferences.
- Prepare progress reports on research for funding bodies when required
- Participate in and develop external networks, for example to identify sources of funding or to build relationships for future research activities

### **9.2.2.3 Skills and Qualifications**

Education: Level PhD in the Program Area

Experience: at least 1-3 years relevant experience.

The candidate must possess sufficient specialist knowledge in the specific discipline to develop research programs and methodologies.

### **9.2.2.4 EUC Pertaining Benefits**

Researchers will have access to facilities which are necessary and appropriate for the performance of their duties.

- Desk, Telephone line and PC

- MS Office, SPSS, Email and Printing Rights
- Business Cards with the University Emblem and the Research Laboratory they belong to
- Full access to the library

All researchers must receive the same forms of employment documentation as other academic-related staff of the University:

- a formal contract signed by the relevant appointing authority;
- written confirmation of any changes in the terms of employment;
- job description or the generic description of the role and, where appropriate, a list of expected research goals;
- further to the completion of the contract, researchers are responsible for returning in good condition all the equipment as well as business cards that have been provided to them

### **9.2.3 Job Description for the Position of Senior Research Fellow**

#### **9.2.3.1 Overall Role**

A Senior Research Fellow is an experienced researcher holding a leadership role in a research group/centre/institute. Post-holders are expected to undertake the role of Principal Investigator on major research projects, exhibit a strong reputation for independent research, and provide academic leadership. They are also expected to support the management activity of the relevant School/Research Centre, and contribute to the delivery of the School's/ Centre's/Laboratory's research strategy.

#### **9.2.3.2 Key Responsibilities**

- Supervise postgraduate research students
- Contribute to the development of research strategies for the relevant School/Centre/Laboratory.
- Define research objectives and questions
- Develop proposals for research projects which will make a significant impact by leading to an increase in knowledge and understanding
- Actively seek research funding and secure it as far as it is reasonably possible
- Generate new research approaches
- Review and synthesise the outcomes of research studies
- Interpret findings obtained from research projects and develop new insights
- Contribute generally to the development of thought and practice in the field
- Provide academic leadership to those working within research areas - for example, by co-ordinating the work of others to ensure that research projects are delivered effectively and to time
- Contribute to the development of teams and individuals through the appraisal system and providing advice on personal development
- Act as line manager (e.g. of research teams)
- Act as a personal mentor to peers and colleagues

- Provide advice on issues such as ensuring the appropriate balance of research projects, appointment of researchers and other performance related issues
- Identify opportunities for strategic development of new projects or other areas of research activity and contribute to the development of such ideas

### ***9.2.3.3 Skills and Qualifications***

Education: Level PhD in the Program Area

Experience: at least 7-10 years relevant experience. Significant post-qualification research experience with a track record of high-quality publications.

Experience of successful supervision of students

Experience in a leadership role in a Research Group/Centre or Laboratory

### ***9.2.3.4 EUC Pertaining Benefits***

Researchers will have access to facilities which are necessary and appropriate for the performance of their duties.

- Desk, Telephone line and PC
- MS Office, SPSS, Email and Printing Rights
- Business Cards with the University Emblem and the Research Laboratory they belong to
- Full access to the library

All researchers must receive the same forms of employment documentation as other academic-related staff of the University:

- a formal contract signed by the relevant appointing authority;
- written confirmation of any changes in the terms of employment;
- job description or the generic description of the role and, where appropriate, a list of expected research goals;
- further to the completion of the contract, researchers are responsible for returning in good condition all the equipment as well as business cards that have been provided to them

## **9.3. Procedures for Appointment**

### ***9.3.1 Selection and Search Procedures***

As a general rule, an appointment to the Academic Research Staff requires a search for a suitable candidate. Searches are initiated with a written vacancy announcement, such as in relevant professional journals or other publications.

The text for the announcement should be sent to the Office of the Vice Rector of Research and External Affairs and the Office of the Director of Human Resources, clearly describing the terms of employment, length of employment, identity and duration of funding sources contributing to his or her salary and line manager (the person the researcher will be

reporting to). The text should be advertised for a reasonable amount of time. A copy of a current CV, a cover letter and at least one recommendation should be sought for. A short list of the potential candidates will be created based on merit and the top part of the list will be called for a structured interview with the line manager. At the end of the procedure, the line manager will report back to the Office of the Vice Rector of Research and External Affairs and the Office of the Director of Human Resources, the name(s) of the proposed Researcher.

### ***9.3.2 Criteria for the Appointment to Rank of Research Associate***

Minimum qualifications as described in Section 9.2.1.

### ***9.3.3 Criteria and Procedures for the Promotion to the Rank of Research Fellow***

A Research Associate may, during the course of his/her appointment obtain, his/her PhD. In such cases, the employee (provided that he/she fulfills the work experience as described in Section 9.2.2) is promoted to the rank of Research Fellow. If the funding source that sponsors the program the researcher is assigned to accounts for a pay rise this is immediately applied.

## **9.4 Honorary Research Staff**

The work of Research Centers is enhanced by the involvement and collaboration in the Research Centers' activities of personnel who are not employees of the University. To recognise the association, EUC may confer an honorary title to such individuals during the period of their association. An honorary title may not be conferred on an employee of EUC.

The title to be conferred will depend on the level of distinction and qualification of the candidate. Applications should come from the Dean of the School with:

- a copy of the person's CV
- a citation that should include:
  - a description of contributions to teaching
  - research being undertaken with academic staff as evidenced by joint publications/research projects and research grants or contracts being held jointly or a significant involvement in industry/academic joint activities within the College
  - rationale for offering the association
  - the start date and end date of the association

Honorary titles are intended to recognise ongoing attachments and are awarded for a fixed term, normally up to three years in the first instance. No monetary honorarium is associated with the offer.

The honorary research titles that can be awarded are:

#### **9.4.1 Honorary Principal Research Fellow**

Will have made an outstanding contribution to teaching and research

#### **9.4.2 Honorary Senior Research Fellow**

Extensive research experience required, the quality of which is determined by refereed publications, invitations to speak at conferences, hold an established national reputation and a known or developing international reputation. Have the ability to attract significant external research funding. Will usually lead a team of other research staff, possibly drawn from several disciplines

#### **9.4.3 Honorary Research Fellow**

Proven ability of high quality research, evidenced by authorship of a range of publications. Capable of attracting external research funding. May be required to undertake project management and/or supervise teams and other research staff; expected to provide expert advice and guidance to others

#### **9.4.4. Honorary Research Associate**

Required to produce independent original research and to take initiatives in planning of research.

### **9. 5 Intellectual Property Rights**

All IP generated throughout the employment of an Academic Research Staff Member belongs to EUC. In such cases that the Researcher is employed in a project that assigns explicit IP rights (e.g. an EU funded project) then the rules as set out by the funding agency are followed.

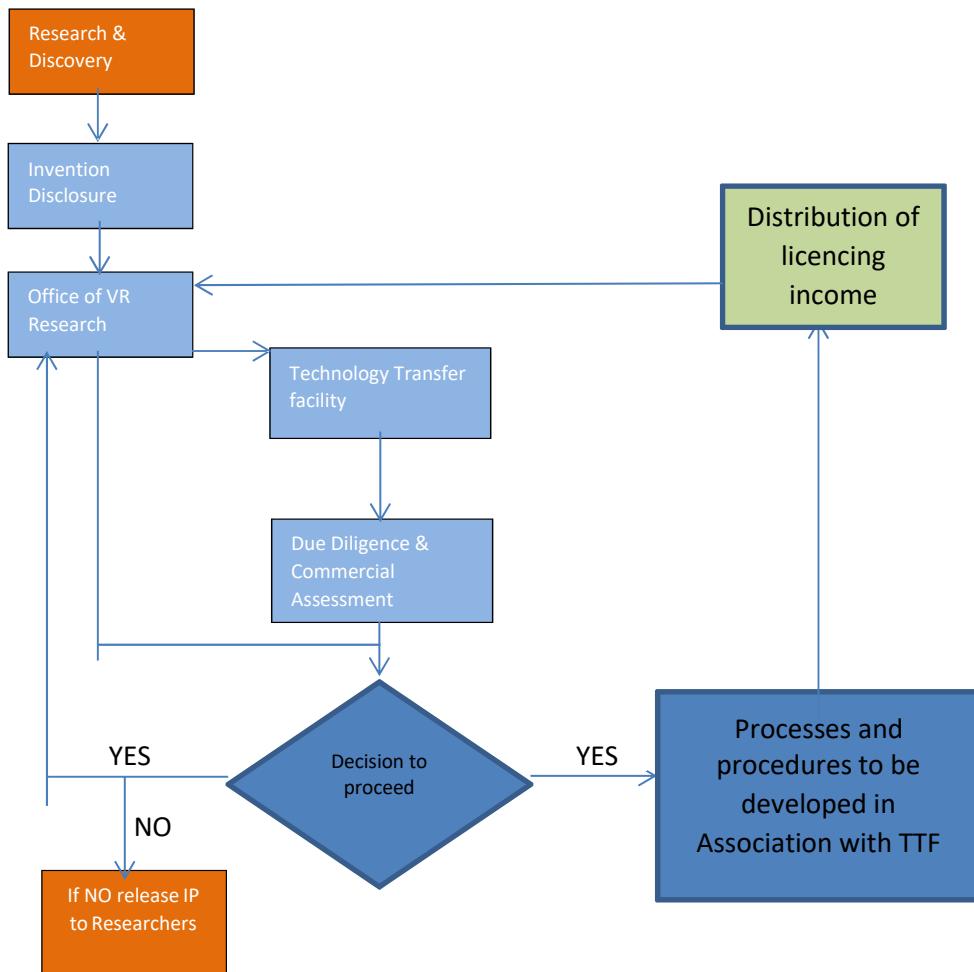
Honorary Research Staff may be required to assign the rights to any IP they create in the course of their academic activities to EUC. EUC may have obligations to organisations which are funding the research (e.g. an EU funded project) in question which it will not be able to honour without such an assignment of rights being in place. Associates are treated as if they were EUC Employees for the purposes of revenue sharing.

### **9.6 Involvement of Research Staff**

Wherever possible, Academic Research staff should be encouraged to take part in university decision making processes, for example by inclusion in relevant departmental committees. Where appropriate, researchers should be included at University level, for example as representatives in working groups and staff consultation exercises.

## Appendix A:

### A Technology Transfer Process Map – to be completed when the TTF has been established.



## Appendix B:

### Invention Disclosure Guidelines

#### **Invention Disclosure Form - Example**

An Invention Disclosure Form (IDF) is designed to determine the basic facts relating to an invention, design, or copyright material. It is a way of capturing an invention and establishing who the inventors are, what the invention is, who is funding it, what the anticipated product/ market is and initiate Intellectual Property (IP) due diligence.

Information on the following aspects of an invention should be included in an Invention Disclosure Form.

1. Descriptive Title of the Invention.
2. Who was involved? Please specify for each individual who contributed, invented or authored (if software):
  - a. Their names and if any are foreign nationals;
  - b. Who their employer is; are any contracts or arrangements in place?
  - c. What they contributed to the development of the technology (e.g. came up with the original idea; designed experiments; carried out experimental work; wrote code)
3. Detail of your invention:
  - a. What do you think your invention is?
  - b. What will your invention be used for?
  - c. What are the advantages of your invention and how does it improve on the present situation?
  - d. What is new about your invention?
  - e. How and why does it work? What is the science behind the invention
  - f. Are there any other uses of the invention?
4. Interest from external organisations and their details.
5. Information on published literature (including patents) relevant to your invention?
6. When and where the invention was first conceived?
7. What are your future plans for developing the technology?
8. Who have you told about the invention, when and where?
9. When did you first describe the invention in writing or electronically?
10. Publications, abstracts, conferences to date.
11. Publication and conference plans.
12. Funding information (comprehensive), e.g including third party support, Material Sales or Transfers, patient consents.  
For inventions that include software, please provide the following additional information.
13. Application name and version number.
14. For source code developed by the researchers identified in question 2 above, include: source files used, programming languages, development tools, copyright protection in source code.
15. For new versions, include: source files changed, added or removed since the previous version, documentation required for others to use, if the source files have been distributed outside the university, and in what form, and are the source files

available as a web-download – inc. URL and terms under which the download is available.

16. For other source files or libraries that are required to build the software application (external software), list the following: all external software required to use the application; who owns that software, how was the software obtained, licence terms or FOSS – name of the licence.

## **Appendix C:**

### **Suggested Revenue Sharing Scheme**

The EUC will share royalty income with employees and/or students involved in producing Disclosable Work whose exploitation generates revenue for the EUC. Payments are made at the Organisation's sole discretion, but the EUC will normally share royalty income in accordance with the table below. This may be either as a lump sum or as royalty income over a period of time.

**Table C1**

<b>Net Revenue</b>	<b>Allocated to the Creator/s</b>	<b>Allocated to the EUC Central Budget</b>	<b>Allocated to the Creator/s School of Study or Department Budget</b>	<b>Allocated to Support the TTF</b>
100%	50%	20%	20%	10%

## **Appendix D**

### **D1. Points accumulation from Research**

Table D1 details the evaluation categories which will be used for the calculation of research points allocated to EUC researchers. The table has been constructed taking into account the following:

1. The points awarded are based on the evaluation of research accomplishments, not on the estimation / calculation of hours spent during the implementation of a research activity.
2. A research accomplishment is any research-related activity which strengthens the research portfolio and enhances the research esteem of a researcher in particular, and the EUC in general
3. It is apparent that specific research accomplishments cannot be evaluated in a similar manner across the range of research disciplines. Therefore, the following table is implicitly “averaging” the weight of these accomplishments, so that the scheme can be operational and fair.
4. The term “national”, when used in association with a conference, refers to one which is local in nature (i.e. only researchers from Cypriot Universities and other Cypriot research establishments participated in it).
5. The term “international”, when used in association with a conference, refers to one which is international in nature (i.e. researchers from Universities and other research establishments from at least two countries participated in it).
6. The term “national”, when used in association with a publication refers to one published by a Cypriot university or other Cypriot academic publishing house.
7. The term “international”, when used in association with a publication refers to one published by an international university or other international academic publishing house.

Where a publication of any type (conference, journal, book chapter, monograph, textbook, book, or other) concerns two or more authors, the following points’ calculation rules will apply: For cases up to (and including) two (2) authors, full points are awarded to the author in consideration. For each additional co-author (three (3) authors or more), a deduction of 2 points will be implemented on the full points’ allocation for the category considered. The minimum points that an author will be awarded cannot be smaller than 50% of the full points’ allocation for the category considered.

**Table D1**

Points	Conferences	Journals	Books	Research Projects	Other*
5	1. Presentation of poster / article in national conference (refereed) 2. Presentation as invited keynote speaker (refereed national conference)			1. Unsuccessful submission of funded research proposal in national / international organization (research partner)	Member of scientific / conference organizing committee (national / international)
10	1. Presentation of refereed poster / article in international conference (refereed) 2. Presentation as invited keynote speaker (refereed international conference) 3. Editor of national conference proceedings (refereed)	1. Publication of refereed journal article (journal not in ISI / Scopus / ACM / IEEE/etc.) 2. Editor of refereed journal special issue (journal not in ISI / Scopus / ACM / IEEE/etc.)	Publication of refereed book chapter (national)	1. Unsuccessful submission of funded research proposal in national organisation (project coordinator)	General Chair or Program Chair of refereed national conference
15	1. Editor of international conference proceedings (refereed)		Publication of refereed book chapter (international)	1. Unsuccessful submission of funded research proposal in international organization (project coordinator)	General Chair or Program Chair of refereed international conference

**Table D1 (continues)**

Points	Conferences	Journals	Book Chapters / Editors	Research Projects	Other*
20		1. Editor of refereed journal special issue (journal in ISI / Scopus / ACM / IEEE/etc.)	Editor of refereed book / book series		
25		1. Publication of refereed journal article (journal in ISI / Scopus / ACM / IEEE/etc.)			

\* For these categories only 50% of the points will be accumulated

## **D2. Points accumulation from Research / Department of Arts**

Due to the nature of the research conducted in the Department of Arts, Table D2 has been produced to address the research output of the Department. For all other research outputs such as journal papers, conferences, books, etc. the European University Cyprus’ “Points’ accumulation” table given in section D1 must be followed.

**Table D2**

Point s	Other				
	Performance /Exhibition (Artist)		Creative works		Workshop/Seminars/Festivals /Competitions/Broadcasts/Residencies
	Music	Graphic Design	Music	Graphic Design	
5	Performance - National level (partial performance )	Participation in local group exhibition	Composition for up to 4 musicians		<ul style="list-style-type: none"> <li>National Performance or Broadcast of a composition/arrangement</li> <li>Adjudication of Competition</li> <li>Invited workshop / art lecture in national conference/festival</li> </ul>
10	Performance - International level (partial performance )	Participation in international group exhibition	Composition from 5-10 musicians	Publication design (national/international) - booklets covers	<ul style="list-style-type: none"> <li>International Performance or Broadcast of a composition/arrangement</li> <li>Competition Finalist</li> <li>Invited workshop / art lecture in international conference/festival</li> <li>Invited Artist (Workshop)</li> </ul>
15	Performance - National level (entire concert) Performance with Large Ensemble	Editor of exhibition catalogue (national/international)	Composition for 10 musicians and above	Publication design (international) - books and exhibition catalogues	<ul style="list-style-type: none"> <li>Competition Winner</li> <li>Invited Artist (Festival – duration more than three days)</li> </ul>
20	Performer – International level (entire concert)	Participation in national solo exhibition	Composition for Symphonic Orchestra	Commissioned work by government/museum/other cultural institution	Participation in funded international residency
25		Participation in international solo exhibition	Publication of a composition (Score/CD) by an International Music Publishing House		



## **SYLLABI**

**“CYBERSECURITY (M.Sc.)”**

Course Title	Introduction to Cybersecurity			
Course Code	CYS602			
Course Type	Compulsory			
Level	Master (2 <sup>nd</sup> cycle)			
Year / Semester	1 <sup>st</sup> Year / 1 <sup>st</sup> Semester			
Teacher's Name	Dr Pericles Leng-Cheng			
ECTS	10	Lectures / week	None	Laboratories / week
Course Purpose and Objectives	This course introduces the fundamental concepts and terminology of cybersecurity as a whole, and functions as a short introduction to the large number of cybersecurity topics that are covered within this MSc course.			
Learning Outcomes	<p>Upon successful completion of this course students should be able to:</p> <ul style="list-style-type: none"> <li>• Describe the meaning and position of fundamental cybersecurity concepts and terminology</li> <li>• Explain the position of the different topics within cybersecurity and how they fit into a comprehensive cybersecurity model</li> <li>• Classify and describe different cybersecurity components and how they contribute to effective defence</li> <li>• Classify and describe different potential routes for cyber attacks.</li> <li>• Understand the importance and application of IT law and cybersecurity certification</li> </ul>			
Prerequisites	None	Co-requisites	None	

Course Content	<p><u>Introduction:</u> Refresh on fundamental networking principles and devices and distributed systems, the context within which cybersecurity (or lack thereof) can be present. Network structure and ways of communication.</p> <p><u>History of cybersecurity:</u> important attacks and consequences. Related history (e.g. the important role of cryptography and cryptanalysis in World War II, etc.)</p> <p><u>Current importance of cybersecurity,</u> given the connectedness of most of our daily lives. Analysis of critical infrastructures and the position of critical information infrastructures within these – importance of the protection of such systems for the smooth operation of essential services in all areas of life. The network as a route for cyberattacks, how the network can be protected, vulnerabilities, threats.</p> <p><u>Asset protection</u> (including data) as a valuable business operation and its contribution to business survivability.</p> <p><u>Main principles of cybersecurity</u> – confidentiality, integrity, availability and combinations thereof, resulting in other important cybersecurity concepts and services – accountability, non-repudiation, authenticity, resilience, business continuity and disaster recovery, audit, cybercrime, data / system / network forensics, cyberdefence.</p> <p><u>Introduction to the phases of cybersecurity</u> – Identify, Protect, Detect, Respond, Recover.</p> <p><u>Applicable cybersecurity and IT law</u> Software licensing, Data privacy and security, Electronic signatures, Legal and regulatory risks, cyberattacks, digital forensics, liability issues, trust. Introduction to ISO/IEC 27001 Information security management.</p> <p><u>Introduction to other courses in this MSc</u> (to aid selection of the elective courses).</p> <p>Introduction to specific cybersecurity topics – database security, secure software development, malware analysis, etc.</p> <p><u>Business case study and lecture:</u> Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on usual network attacks and methods for protection.</p>
Teaching Methodology	Distance Learning

Bibliography	<p><i>“Introduction to Computer Networks and Cybersecurity”</i>, by Chwan-Hwa (John) Wu and J. David Irwin</p> <p><i>“Cybersecurity Foundations: An Interdisciplinary Introduction Hardcover”</i>, by Lee Mark Zeichner</p> <p>“Management of Information Security” by Michael E. Whitman, Herbert J. Mattord</p> <p>“CISSP Guide to Security Essentials” By Peter Gregory</p> <p>“Principles of Information Security” by Michael E. Whitman, Herbert J. Mattord</p> <p><i>IEEE/ ACM/ Elsevier/ Springer Journals and Magazines</i></p> <p>(ISC)<sup>2</sup>, ISACA, and other cybersecurity websites</p>			
Assessment	<p>Examinations</p> <table border="1"> <tr> <td>50%</td> </tr> <tr> <td>50%</td> </tr> <tr> <td>100%</td> </tr> </table> <p>On-going evaluation</p>	50%	50%	100%
50%				
50%				
100%				
Language	English			

Course Title	Communications and Network Security				
Course Code	CYS603				
Course Type	Compulsory				
Level	Master (2 <sup>nd</sup> cycle)				
Year / Semester	1 <sup>st</sup> Year / 1 <sup>st</sup> Semester				
Teacher's Name	Dr George Kiourmourtzis				
ECTS	10	Lectures / week	None	Laboratories / week	None
Course Purpose and Objectives	This course introduces fundamental concepts of communications and network security, particularly in the context of internal and external threats to the operation of the network and to the devices that are attached to it.				
Learning Outcomes	<p>Upon successful completion of this course students should be able to:</p> <ul style="list-style-type: none"> <li>• Describe the underlying principles of networking layers, architecture, topologies, protocol stacks, and separation of duties.</li> <li>• Explain the basic types of networking device, both logical and physical.</li> <li>• Analyse networking methods and applications in practical systems.</li> <li>• Classify and describe different types of wired network attacks.</li> <li>• Classify and describe different types of wireless network attacks.</li> <li>• Describe and evaluate methods and devices used to protect networks.</li> </ul>				
Prerequisites	None	Co-requisites	None		
Course Content	<p><u>Introduction:</u> Refresh on fundamental networking principles and devices, OSI and TCP/IP models. Different types of networking areas – WAN, LAN, MAN, PAN, wireless and mobile systems.</p> <p><u>Principles:</u> the network as a route for cyberattacks, how the network can be protected, vulnerabilities, threats.</p> <p><u>Network Attacks:</u> scanning, malware, (D)DoS, route poisoning, MAC spoofing, sniffing, authentication attacks, man-in-the-middle, session takeover, wiretaps, MAC table flooding, ARP poisoning, ICMP attacks,</p>				

	<p>DNS poisoning, smurf and fraggle attacks, phishing, spam, war-dialling, methods to prevent the network attacks that have been covered (within the discussion of each attack type).</p> <p><u>Wireless Attacks:</u> Encryption and key management vulnerabilities, wireless sniffing, war-driving, mobile/cellular cell spoofing, eavesdropping, mobile phone attacks, methods to prevent the network attacks that have been covered (within the discussion of each attack type).</p> <p><u>General protection, prevention and detection:</u> Firewalls and packet filtering, demilitarized zones (DMZ), intrusion detection and prevention systems, IPsec, VLANs and network zoning, MAC access control, network authentication, system hardening, encryption, authentication, universal threat management (UTM), web filtering, honeypots, awareness.</p> <p>Network management as an effective information-gathering tool and starting point for comprehensive protection mechanisms, use of network and asset management tools to ensure uniform conformity to relevant cybersecurity standards and policies.</p> <p>Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on usual network attacks and methods for protection.</p>			
Teaching Methodology	Distance Learning			
Bibliography	<p><i>“Computer Networking: A Top-Down Approach (7th Edition), by Jim Kurose and Keith Ross.</i></p> <p><i>“Guide to Computer Network Security, 4th Edition”, by Joseph Migga Kizza</i></p> <p><i>“Network Security Essentials: Applications and Standards”, Sixth Edition, by William Stallings</i></p> <p><i>IEEE/ ACM/ Elsevier/ Springer Journals and Magazines</i></p>			
Assessment	<p>Examinations</p> <table border="1" style="float: right; margin-left: 10px;"> <tr><td>50%</td></tr> <tr><td>50%</td></tr> <tr><td>100%</td></tr> </table> <p>On-going evaluation</p>	50%	50%	100%
50%				
50%				
100%				
Language	English			

Course Title	Cryptography			
Course Code	CYS604			
Course Type	Compulsory			
Level	Master (2 <sup>nd</sup> cycle)			
Year / Semester	1 <sup>st</sup> Year / 1 <sup>st</sup> Semester			
Teacher's Name	Dr Philippos Isaia			
ECTS	10	Lectures / week	None	Laboratories / week
Course Purpose and Objectives	This course introduces fundamental concepts of cryptography and its uses in cyber and information security. Beyond the basic uses for keeping information secret and the different methods available, additional forms, such as hashes, digital signatures, non-repudiation and steganography, are introduced.			
Learning Outcomes	<p>Upon successful completion of this course students should be able to:</p> <ul style="list-style-type: none"> <li>• Describe the underlying principles of cryptography, clear text, plain text, algorithms, and keys.</li> <li>• Explain the different kinds of encryption methods (symmetric, asymmetric) and the differences between them.</li> <li>• Classify and describe a number of different encryption algorithms and the way that they work.</li> <li>• Describe the mathematical principles behind encryption and the mathematical properties of ciphertext.</li> <li>• Describe and evaluate different methods used to crack encryption.</li> <li>• Explain the different uses of encryption methods and the security objectives that they meet.</li> </ul>			
Prerequisites	None	Co-requisites	None	

Course Content	<p><u>Introduction:</u> History of cryptography, early forms, cryptosystem strength, Caesar cipher, one time pad, steganography.</p> <p><u>Principles:</u> basic cryptographic functions – substitution ciphers and transposition ciphers, symmetric and asymmetric algorithms, block and stream ciphers, hybrid systems.</p> <p><u>Symmetric systems:</u> DES, 3-DES, AES, IDEA, Blowfish, RC4-5-6, Twofish, Serpent, others, uses and cryptographic services provided.</p> <p><u>Asymmetric systems:</u> Diffie-Hellman algorithm, RSA, El Gamal, Elliptic Curve systems, zero knowledge proof, SSL/TLS, PGP, S/MIME, Bitcoin.</p> <p><u>Public key systems:</u> one-way algorithms, public and private keys, public key infrastructure, certificate and trust authorities, distributed trust systems.</p> <p><u>Other cryptographic services:</u> message and file integrity, hashing, digital certificates, digital signatures, key management.</p> <p><u>Attacks:</u> known and chosen plaintext attacks, ciphertext attacks, analytical attacks, frequency analysis, statistical attacks, social engineering attacks.</p> <p>Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the uses of cryptography in real systems.</p>
Teaching Methodology	Distance Learning
Bibliography	<p><i>“Introduction to Modern Cryptography, Second Edition (Chapman &amp; Hall/CRC Cryptography and Network Security Series)”,</i> by Jonathan Katz and Yehuda Lindell</p> <p><i>“Understanding Cryptography: A Textbook for Students and Practitioners”,</i> by Christof Paar and Jan Pelzl</p> <p><i>“Applied Cryptography: Protocols, Algorithms and Source Code”,</i> by Bruce Schneier</p> <p><i>“Modern Cryptanalysis: Techniques for Advanced Code Breaking”,</i> by Christopher Swenson</p> <p><i>IEEE/ ACM/ Elsevier/ Springer Journals and Magazines</i></p>

Assessment	Examinations On-going evaluation	<table border="1"><tr><td>50%</td></tr><tr><td>50%</td></tr><tr><td>100%</td></tr></table>	50%	50%	100%
50%					
50%					
100%					
Language	English				

Course Title	Cybersecurity Policy, Governance, Law and Compliance				
Course Code	CYS605				
Course Type	Compulsory				
Level	Master (2 <sup>nd</sup> cycle)				
Year / Semester	1 <sup>st</sup> Year / 2 <sup>nd</sup> Semester				
Teacher's Name	Dr Yianna Danidou				
ECTS	10	Lectures / week	None	Laboratories / week	None
Course Purpose and Objectives	This course provides an overview of the broad and constantly emerging field of cybersecurity policy, governance, law and compliance. The importance of the role of security policy is discussed.				
Learning Outcomes	<p>Upon successful completion of this course, students should be able to:</p> <ul style="list-style-type: none"> <li>• State and identify concepts relating to organizational cybersecurity policy, governance mechanisms, applicable legislation and compliance requirements for information security.</li> <li>• State and interpret the different components of a comprehensive organizational cybersecurity policy.</li> <li>• State and interpret the role of security policy within an organization and its position with relation to other controls within a comprehensive cybersecurity environment.</li> <li>• Describe the role of corporate governance with regards to cybersecurity, and the business reasons for implementing a cybersecurity function.</li> <li>• Recognize and explain major applicable legislation and regulatory framework (local, European, international).</li> <li>• Define, explain and exemplify compliance requirements in relation to cybersecurity, information security, data protection (privacy, anonymity) and critical information infrastructure protection.</li> </ul>				
Prerequisites	None	Co-requisites	None		

Course Content	<p><b>Introduction:</b> Concepts of cybersecurity, its relationship with network and information security, cybercrime, cyberdefence, and related definitions. Concepts of policy, governance, related law and compliance, and the relationships between them.</p> <p><b>Principles:</b> Information security components and concepts, confidentiality, integrity, availability.</p> <p><b>Policy:</b> definition, role of policy in an organization, statement of management purpose and organizational objectives, description of organizational approach, standards, baselines, guidelines, procedures.</p> <p><b>Governance:</b> Role of cybersecurity and information security in the organization, levels of responsibility, the different personnel roles: information owner, information custodian, administrator, solution provider, change control, human resources, user. Certification and accreditation.</p> <p><b>Law:</b> Relevant laws and legal/regulatory frameworks on the national, European and international level. Different types of law related to cyberattacks – computer as the means, computer as a victim. Problems of jurisdiction, borderless nature of cybercrime, relevance and importance of data protection and privacy, investigations.</p> <p><b>IT and Law:</b> Introduction, Terminology, and the Nature of Cyberspace and Threats. Cyber-regulation and cyber-regulatory theory. Cyberproperty and Intellectual Property. Cyber-rights, Speech Harm, Crime and Control. Roles of International Law, the State, and the Private Sector in Cyberspace. Authentication and Identity Management. Speech, Privacy and Anonymity in Cyberspace. Trust.</p> <p><b>Compliance:</b> Reasons for specific cybersecurity legislation beyond cybercrime, compliance requirements, self-assessment, auditing principles, audit process.</p> <p>Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on reasons behind and expected benefits of compliance requirements and on recent/future developments.</p>
Teaching Methodology	Distance Learning
Bibliography	<p><i>“Security Risk Management: Building an Information Security Risk Management Program from the Ground Up”, by Evan Wheeler</i></p> <p><i>“Information Security Governance: A Practical Development and Implementation Approach”, by Krag Brotby</i></p>

	<p><i>“Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats”, by Scott E. Donaldson</i></p> <p><i>“Cyber Security and IT Infrastructure Protection”, by John R. Vacca</i></p> <p><i>IEEE/ ACM/ Elsevier/ Springer Journals and Magazines</i></p>			
Assessment	<p>Examinations</p> <p>On-going evaluation</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr><td>50%</td></tr> <tr><td>50%</td></tr> <tr><td>100%</td></tr> </table>	50%	50%	100%
50%				
50%				
100%				
Language	English			

Course Title	Cybersecurity Architecture and Operations				
Course Code	CYS606				
Course Type	Compulsory				
Level	Master (2 <sup>nd</sup> cycle)				
Year / Semester	1 <sup>st</sup> Year / 2 <sup>nd</sup> Semester				
Teacher's Name	Dr Nikos Tsalis				
ECTS	10	Lectures / week	None	Laboratories / week	None
Course Purpose and Objectives	<p>This course introduces the fundamental security principles of confidentiality, integrity, availability, as well as related security services such as accountability, non-repudiation, authentication, etc. The whole operational environment is described, with reference to ongoing security processes such as user provisioning, vulnerability management, penetration testing, exercising, change management, incident response, risk assessment and others. The five phases of cybersecurity are discussed here – Identify, Protect, Detect, Respond, Recover.</p>				
Learning Outcomes	<p>Upon successful completion of this course students should be able to:</p> <ul style="list-style-type: none"> <li>• Identify the various components of a comprehensive cybersecurity architecture within an organization.</li> <li>• Describe and classify controls that meet specific control objectives and to treat identified risks.</li> <li>• Explain in detail the basic security principles of confidentiality, integrity and availability, as well as related security services such as accountability, non-repudiation, authentication, etc.</li> <li>• Describe the five phases of cybersecurity operations: Identify, Protect, Detect, Respond, Recover.</li> <li>• Describe and evaluate the processes of vulnerability management, penetration testing, exercising, change management, incident response, and others.</li> <li>• Classify and describe a number of different effects of main cybersecurity controls on the operational environment, e.g. access control.</li> <li>• Evaluate and select appropriate architectural and operational options according to the organizational risk environment.</li> </ul>				

Prerequisites	None	Co-requisites	None
Course Content	<p><u>Introduction:</u> Definition of security objectives: confidentiality, integrity, availability, accountability non-repudiation, authentication.</p> <p><u>Processes:</u> User provisioning, access control, vulnerability management, penetration testing, exercising, change management, incident response, others.</p> <p><u>Phases:</u> Phases of cybersecurity operations, in relation to the before and after of an incident: Identify, Protect, Detect, Respond, Recover.</p> <p><u>Identify:</u> Identification of organizational assets, threats, vulnerabilities and risks (details in risk assessment course), vulnerability management (open databases, CVE, etc.) as an essential process.</p> <p><u>Protect:</u> Selection and evaluation of controls to meet control objectives and risks identified, application and monitoring of controls, control lists (ISO 27002, COBIT 5, SANS 20 Critical Controls, Australia DSD Top Mitigations, etc), defense-in-depth considerations, penetration testing, BCP and DRP testing, system hardening.</p> <p><u>Detect:</u> Detection of cybersecurity incidents as they occur, evaluation of impacts, log analysis, IDS/IPS, attack vector analysis, SIEM (security incident and event management), indicators of compromise (IOC).</p> <p><u>Respond:</u> Incident triage and response, CERT/CSIRTs, triggering and implementation of business continuity and disaster recovery plans, corrective controls.</p> <p><u>Recover:</u> Orderly and planned return to prior operational status and capabilities, lessons learned, evaluation of corrective controls and supporting processes.</p> <p><u>Specific cybersecurity operations topics:</u> Database security, secure software development, mechanisms for ensuring the security of information at rest, in transit, and during processing, side-channel considerations.</p> <p><u>Business case study and lecture:</u> Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the practicalities of cybersecurity operations in real environments.</p>		

Teaching Methodology	Distance Learning						
Bibliography	<p><i>Farwell, J.P., Roddy, V.N., Chalker, Y. and Elkins, G.C. The Architecture of Cybersecurity: How General Counsel, Executives, and Boards of Directors Can Protect Their Information Assets. University of Louisiana at Lafayette.</i></p> <p><i>Santos, O., Developing Cybersecurity Programs and Policies. Pearson.</i></p> <p><i>“Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”, by Thomas A. Johnson (Editor)</i></p> <p><i>“The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)”, by Anne Kohnke and Dan Shoemaker</i></p> <p><i>ISO 27002:2013 - Information technology – Security techniques – Code of practice for information security management</i></p> <p><i>IEEE/ ACM/ Elsevier/ Springer Journals and Magazines</i></p>						
Assessment	<table border="1"> <tr> <td>Examinations</td> <td>50%</td> </tr> <tr> <td>On-going evaluation</td> <td>50%</td> </tr> <tr> <td></td> <td>100%</td> </tr> </table>	Examinations	50%	On-going evaluation	50%		100%
Examinations	50%						
On-going evaluation	50%						
	100%						
Language	English						

Course Title	Ethical Hacking and Penetration Testing			
Course Code	CYS607			
Course Type	Compulsory			
Level	Master (2 <sup>nd</sup> cycle)			
Year / Semester	1 <sup>st</sup> Year / 2 <sup>nd</sup> Semester			
Teacher's Name	Dr Nikos Tsalis			
ECTS	10	Lectures / week	None	Laboratories / week
Course Purpose and Objectives	<p>The objective of this course is to provide a detailed introduction into the world of ethical hacking and to understand its usefulness to organizations in practical terms. Hacking concepts, tools and techniques, and countermeasures are covered, along with how penetration testing fits into a comprehensive cybersecurity regime. Beyond the confines of ethical hacking, this course covers aggressive hacking techniques that are essential knowledge for professionals who need to be able to defend against such advanced attacks.</p>			
Learning Outcomes	<p>Upon successful completion of this course students should be able to:</p> <ul style="list-style-type: none"> <li>• Define the different types of hacking and its legal and illegal uses in the cybersecurity world</li> <li>• Identify and evaluate the different type of hacking attacks and how these attacks proceed</li> <li>• Explain the principles of vulnerability research</li> <li>• Describe the different phases of ethical hacking and select appropriate techniques depending on the assignment.</li> <li>• Define, describe and perform the different kinds of penetration testing – black box, grey box, white box.</li> <li>• Make effective use of penetration testing related tools</li> <li>• Define which tool is more effective at each step of a penetration testing project</li> </ul>			
Prerequisites	None	Co-requisites	None	

Course Content	<p><u>Introduction:</u> Definition of ethical hacking and penetration testing, position within a comprehensive cybersecurity posture, applicable national and international laws, difference between ethical (white hat), non-ethical (black hat) and grey hat hackers, vulnerability research and zero-day vulnerabilities.</p> <p><u>Hacking phases:</u> The five phases of hacking – reconnaissance, scanning, gaining access, maintaining access, covering tracks.</p> <p><u>Reconnaissance:</u> Discovery of target information, footprinting, competitive intelligence, social engineering, Google hacking, website footprinting, email tracking</p> <p><u>Scanning:</u> TCP flags, ping sweeps, connect scans, TCP flag manipulation, SYN scans, IDLE scans, scanning tools, banner grabbing, vulnerability scanning, ip spoofing, enumeration techniques and tools</p> <p><u>Gaining and maintaining access:</u> password cracking, dictionary attacks, brute force attacks, hashing attacks, privilege escalation, executing applications, malware (viruses, worms, trojans, rootkits, spyware, botnets), lalware detection and anti-malware software, DoS/DDoS, network sniffing, MAC, ARP and DNS attacks, session hijacking, web application attacks, SQL injection, wireless network and mobile device attacks, cryptanalysis and related attacks.</p> <p><u>Covering tracks:</u> Rootkits, disabling auditing, clearing logs, anonymisers, proxies, hiding files, track covering tools</p> <p><u>Practical penetration testing:</u> Penetration testing methodology, ethical considerations, assignments and contracts, reporting, relationship to audits and audit techniques.</p> <p>Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the practicalities and challenges of penetration testing.</p>
Teaching Methodology	Distance Learning
Bibliography	<p><i>Kim, P. The Hacker Playbook 3: Practical Guide to Penetration Testing.</i></p> <p><i>Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G. and Williams, T. Gray hat hacking: the ethical hacker's handbook. McGraw-Hill Education.</i></p>

	<p><i>“Hacking: The Art of Exploitation, 2nd Edition”, by Jon Erickson</i></p> <p><i>“Social Engineering: The Art of Human Hacking”, by Christopher Hadnagy and Paul Wilson</i></p> <p><i>IEEE/ ACM/ Elsevier/ Springer Journals and Magazines</i></p>			
Assessment	<p>Examinations</p> <p>On-going evaluation</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr><td>50%</td></tr> <tr><td>50%</td></tr> <tr><td>100%</td></tr> </table>	50%	50%	100%
50%				
50%				
100%				
Language	English			

Course Title	Research Methods in Cybersecurity			
Course Code	CYS621			
Course Type	Optional			
Level	Master (2 <sup>nd</sup> Cycle)			
Year / Semester	2 <sup>nd</sup> Year / 3 <sup>rd</sup> Semester			
Teacher's Name	Dr George Christou			
ECTS	10	Lectures / week	none	Laboratories / week
Course Purpose and Objectives	The student acquires the necessary skills to enable the successful completion of scientific experiments and their analysis. Established research methods for independent research are introduced using methodical processes.			
Learning Outcomes	<p>Upon successful completion of this course students should be able to:</p> <ul style="list-style-type: none"> <li>• Explain the scientific method</li> <li>• Discuss the various types of research</li> <li>• Assess data through descriptive statistics</li> <li>• Create correct scientific experiments</li> <li>• Propose critical analyses of data based on statistical tests</li> <li>• Explain correlation and regression evidence as part of the analysis of an experimental result</li> </ul>			
Prerequisites	None	Required	None	
Course Content	<p>The nature of research:  Definitions and types of research; research process; types of research methods; feasibility and value; Statistical and qualitative techniques for data analysis; use of appropriate software</p> <p>Descriptive Statistics:  Frequency Distributions; Proportions and Percentages; Nominal, Ordinal and Interval Data;  Cumulative Distributions; Cross-Tabulations; Mode, Median, and Mean; Range, Variance and Standard Deviation; Graphical Representations</p> <p>Probability and the Normal Curve:  Probability; Probability Distributions; Characteristics of the Normal Curve; Random Sampling; Sampling Error; Sampling Distribution of</p>			

	<p>Means; Standard Error; Confidence Intervals; The t Distribution; Proportions; Generalizing From Samples to Populations</p> <p>Decision Making</p> <p>The Null Hypothesis; The Research Hypothesis; Levels of Significance; Standard Error; Two Sample Tests of Proportions; Analysis of Variance; The Sum of Squares; The F Ratio; Nonparametric Tests; The Chi-Square Test; The Median Test</p> <p>Association Methods</p> <p>Correlation; Strength and Direction of Correlation; Curvilinear Correlation; Correlation Coefficient; Pearson's Correlation Coefficient; The Regression Model; Regression and Pearson's Correlation; Spearman's Rank-Order Correlation Coefficient; Goodman's and Kruskal's Gamma; stration: Goodman's and Kruskal's Gamma.</p> <p>Program-specific content</p> <p>As this course is taught in a variety of Master's programs offered by the department of Computer Science, the last part of the course will discuss specific research methods for each discipline. The specific topics will be provided by the instructor of the course according to the specific needs of the audience.</p>							
Teaching Methodology	Distance Learning							
Bibliography	<p>Edgar, T. W. and Manz, D. O. Research Methods for Cyber Security. Cambridge, MA: Syngress.</p> <p>Argyrous, G. Statistics for Research: with a guide to SPSS. Los Angeles, CA: Sage.</p> <p>King, R. S. Research Methods for Information Systems, Dallas, TX: Mercury Learning &amp; Information</p> <p>Cohen, P. R. Empirical Methods for Artificial Intelligence, Cambridge, MA: The MIT Press.</p>							
Assessment	<table border="1"> <tr> <td>Examinations</td> <td>50%</td> <td rowspan="3"></td> </tr> <tr> <td>On-going evaluation</td> <td>50%</td> </tr> <tr> <td></td> <td>100%</td> </tr> </table>	Examinations	50%		On-going evaluation	50%		100%
Examinations	50%							
On-going evaluation	50%							
	100%							
Language	English							

Course Title	Special Cybersecurity Topics							
Course Code	CYS622							
Course Type	Elective							
Level	Master (2 <sup>nd</sup> cycle)							
Year / Semester	1 <sup>st</sup> /2 <sup>nd</sup> or 2 <sup>nd</sup> /3 <sup>rd</sup>							
Instructor	TBA							
ECTS	10	Lectures/ week	3 Hours/14 weeks	Labs / week	N/A			
Course Aims	The aim of the course is the presentation and critical discussion of contemporary theoretical views, trends and practices that affect the theory and practice of Cybersecurity.							
Learning Outcomes	Upon completion of the course, students are expected to be able to respond to the objectives of the course content as this will be designed by the corresponding instructor at the time. Please see attached a possible such syllabus (see also its Study Guide)							
Pre-requisites	None	Co-requisites	None					
Course Content	The exact course content will be based on the special scientific interests of and the needs of the students and might focus on a variety of topics in the field of Cybersecurity. In each case the appropriate teaching and learning methodologies will be applied as well as the appropriate assessment methods and activities. It is requested that the instructor will submit a detailed course outline and the respective study guide of the course on the particular semester s/he will offer the course.							
Teaching Methodology	Distance Learning							
Literature	Literature and reading material will be selected by the instructor on the basis of the content of the course as this will be designed for the particular semester.							
Assessment	Examinations On-going evaluation			50%				
				50%				
				100%				
Language	English							

## **SAMPLE SYLLABUS**

Course Title	Contemporary Issues or Special Topics in Cybersecurity				
Course Code	CYS6...				
Course Type	Elective				
Level	Master (2 <sup>nd</sup> cycle)				
Year / Semester	2 <sup>nd</sup> Year / 3 <sup>rd</sup> Semester				
Teacher's Name	Dr Philippos Isaia				
ECTS	10	Lectures / week	None	Laboratories / week	None
Course Purpose and Objectives	<p>The objective of this course is to provide the student with a comprehensive view of the current state of cybersecurity – major incidents and statistics, recent developments in law, policies, national and European strategies, privacy considerations, new technologies, Safer Internet and the various related professional certifications that are available. Also to provide insight from the organizations and a market perspective of cybersecurity as a critical factor of business growth and economic development. Finally to present the emerging cybersecurity ecosystem and need to keep up to technological developments and threats.</p>				
Learning Outcomes	<p>Upon successful completion of this course students should be able to:</p> <ul style="list-style-type: none"><li>• Identify and define the current events in cybersecurity</li><li>• Describe the various statistics available on cybersecurity and successful attacks around the world</li><li>• Explain recent developments in national, European and international cybersecurity laws and policies</li><li>• Define and describe recent developments in the European area and the impact that these may have on the way cybersecurity operations are conducted</li><li>• Define and describe the different parts of national and European cybersecurity strategy and how they lead to a holistic approach to the response to cybersecurity threats</li><li>• Identify and describe recent developments in the privacy area, and how it is related to and can be protected by proactive cybersecurity operations</li></ul>				

	<ul style="list-style-type: none"> <li>• Identify and describe emerging technologies in the cybersecurity field and their applications</li> <li>• Understand the principles of Safer Internet awareness and how cyber awareness becomes a critical factor of vulnerability for cybersecurity on individual or organizational level.</li> <li>• Define and describe the various professional certifications that are available in the area of cybersecurity and network and information security, and how they are applicable to different parts of a comprehensive cybersecurity architecture and related operations</li> </ul>		
Prerequisites	None	Co-requisites	None
Course Content	<p><u>Introduction:</u> The pace of current developments in cybersecurity and the way that they can influence cybersecurity architecture and operations in organizations and governments. Statistics and major cyber attacks / incidents in recent years.</p> <p><u>Law and Policy:</u> Recent developments in law and policies at the national, European and international level. How these developments can impact the way that cybersecurity operations are conducted. Rising importance of privacy and associated policies. Implications of the expanding usage of cloud services.</p> <p><u>Strategy:</u> National (including Cyprus) and European cybersecurity strategies, how they fit together, national and international cooperation, common and special threats, differences between national and organizational strategies, connections to the areas of cybercrime, cyberdefence and related external affairs. Critical Information Infrastructure Protection.</p> <p><u>Cybersecurity as a factor of growth and the Cybersecurity Ecosystem:</u></p> <p>The importance of cybersecurity for businesses and organizations in general and the interrelations with the other policies. How cybersecurity is a factor of growth and economic development of a business or a whole country.</p> <p>The Cybersecurity ecosystem is in constant evolution and a professional needs to make sure keeping up with it. As cybersecurity as a field has grown in scope and influence, it has effectively become an 'ecosystem' of multiple players, all of whom either participate in or influence the way the field develops and/or operates. It is crucial for those players to collaborate and work together to enhance the security posture of communities, nations and the globe, and security consultants have an</p>		

	<p>important role to play in facilitating this goal, in order to achieve a collaborative security in cyberspace.</p> <p><u>Emerging technologies:</u> Emerging technologies, both in the cybersecurity and in other technological domains, implications on current cybersecurity practices, penetration of technologies that are vulnerable to cyber attacks in all aspects of daily life, implications on vital societal functions.</p> <p><u>Safer Internet:</u> national, European and international efforts in the Safer Internet area, importance of cyber awareness raising for both of these areas, importance and effects of a high level of cyber safety awareness on individual or organizational level, links and effects to other cybersecurity awareness raising initiatives, Better Internet for children as a key for an innovating society.</p> <p><u>Professional Certifications:</u> Introduction to the different information security and cybersecurity professional certifications that are available, importance of their combination with academic qualifications, areas of specialization, additional cybersecurity areas covered.</p> <p>Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the latest developments in the cybersecurity area and their related implications.</p>						
Teaching Methodology	Distance Learning						
Bibliography	<p>National, European and international cybersecurity strategy, policy and legal documents</p> <p>IEEE Journals, Magazines and Websites</p> <p>(ISC)<sup>2</sup> Journals, Magazines and Websites</p> <p>ISACA Journals, Magazines and Websites</p> <p>Other professional certification information sources</p>						
Assessment	<table border="1"> <tr> <td>Examinations</td> <td>50%</td> </tr> <tr> <td>On-going evaluation</td> <td>50%</td> </tr> <tr> <td></td> <td>100%</td> </tr> </table>	Examinations	50%	On-going evaluation	50%		100%
Examinations	50%						
On-going evaluation	50%						
	100%						
Language	English						

Course Title	Cybersecurity Risk Analysis and Management			
Course Code	CYS623			
Course Type	Optional			
Level	Master (2nd cycle)			
Year / Semester	2 <sup>nd</sup> Year / 3 <sup>rd</sup> Semester			
Teacher's Name	Dr George Kiourmourtzis			
ECTS	10	Lectures / week	None	Laboratories / week
Course Purpose and Objectives	<p>This course introduces the fundamental concepts of cybersecurity risk analysis and management, as well as its position as the foundation for cybersecurity protective mechanisms. It covers a wide range of principles and processes related to risk management, and sets the scene for the development of comprehensive cybersecurity controls to protect an organization's assets according to the risk appetite of senior management.</p>			
Learning Outcomes	<p>Upon successful completion of this course students should be able to:</p> <ul style="list-style-type: none"> <li>• Describe the underlying principles of risk analysis and management and the purpose and benefits behind such activities</li> <li>• Explain the terms used, such as risk, analysis, management, vulnerability, threats, actors, impact, risk matrix, etc.</li> <li>• Recognise the difference between vulnerabilities and threats.</li> <li>• Classify and describe a number of different risk assessment/management methodologies.</li> <li>• Classify and describe different assets and their values (including tangible and intangible assets).</li> <li>• Identify and explain various threat sources and the impacts that their materialization may manifest.</li> <li>• Describe the risk management process, as it pertains to the protection of assets.</li> <li>• Evaluate and select appropriate risk treatment options according to the combination of impacts and probabilities that the risk analysis has produced.</li> </ul>			
Prerequisites	None	Co-requisites	None	

Course Content	<p><b>Introduction:</b> Definition of cybersecurity risk and associated terminology, the position of risk analysis and management in relation to the other components of a cybersecurity programme.</p> <p><b>Principles:</b> Assets, vulnerabilities, threats, threat actors, likelihood. Management of risks compared to simple acceptance. Risk treatment options: avoidance, mitigation, transfer, acceptance.</p> <p><b>Assets:</b> Tangible and intangible assets in the cyber world (hardware / software / data, classification, criticality based on the importance and value to organization (not just monetary), dependencies, potential for critical national infrastructure.</p> <p><b>Vulnerabilities:</b> Sources of cyber vulnerability, complexity of modern software, attack surface of modern systems, development of software for functionality and not with security considerations, existing known and zero-day system vulnerabilities, vulnerability databases and open information.</p> <p><b>Threats:</b> Cyber threat categorization, sources, motivation, type, technical vs. non technical (e.g. attacks to cooling systems to disrupt cyber systems), threat actors, exploitation of cyber vulnerabilities leading to impact and associated likelihood.</p> <p><b>Risk analysis:</b> Risk as a combination of possible impact of a threat exploiting a vulnerability and the probability of such an impact occurring, evaluation of cyber risks, categorization, qualitative and quantitative risk analysis, pre-requisites for meaningful quantitative cyber risk assessment, methodologies, risk register.</p> <p><b>Risk management:</b> Risk evaluation and associated selection of risk treatment options, effects and selection of risk avoidance, mitigation, transfer, acceptance (or a combination thereof), risk management as an iterative process, risk profile stemming from modifications in an organisation's environment, building an organisation's cybersecurity control environment from the results of risk analysis, introduction to basic cybersecurity controls.</p> <p>Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the practical uses challenges of risk analysis and management in real environments.</p>
Teaching Methodology	Distance Learning

Bibliography	<p><i>“Effective Cybersecurity: A Guide to Using Best Practices and Standards 1st Edition</i>, by Willian Stallings</p> <p><i>“Cyber-Risk Management” by Atle Refsdal, Bjørnar Solhaug, Ketil Stølen</i></p> <p><i>“Security Risk Management: Building an Information Security Risk Management Program from the Ground Up”,</i> by Evan Wheeler</p> <p><i>“How to Measure Anything in Cybersecurity Risk”,</i> by Douglas W. Hubbard and Richard Seiersen</p> <p><i>“The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)”,</i> by Anne Kohnke and Dan Shoemaker</p>						
Assessment	<table border="1"> <tr> <td>Examinations</td> <td>50%</td> </tr> <tr> <td>On-going evaluation</td> <td>50%</td> </tr> <tr> <td></td> <td>100%</td> </tr> </table>	Examinations	50%	On-going evaluation	50%		100%
Examinations	50%						
On-going evaluation	50%						
	100%						
Language	English						

Course Title	Data Privacy in the era of Data Mining and AI				
Course Code	CYS624				
Course Type	Optional				
Level	Master (2 <sup>nd</sup> cycle)				
Year / Semester	2 <sup>nd</sup> Year / 3 <sup>rd</sup> Semester				
Teacher's Name	Dr Yianna Danidou				
ECTS	10	Lectures / week	None	Laboratories / week	None
Course Purpose and Objectives	<p>The objective of this course is to provide a comprehensive overview of growing data privacy threats to future communication technologies and Internet of Things (IoT) applications such as the Smart Grid and Smart Cities, e-Health and Wireless Sensor Technologies. Recent advances in the technical ICT fields of pervasive communications, combined with the science of big data mining and machine learning, are continuously transforming the way we interact with each other, with physical devices and infrastructures. Such technologies are becoming more tightly intertwined with our daily activities and we are becoming more integrated into the cyber-physical systems that surround us. The positive (economic) impact on society of such advances is enormous; however, big data information flows exposes important privacy details of our daily lives and our behavioural patterns. Such information may potentially be abused for purposes ranging from digital identity theft to targeted marketing, or discrimination based on medical history or other digital footprints, leading to fundamental privacy concerns.</p> <p>On this basis, the objectives of this course further include: a) Understanding interdisciplinary aspects of data handling and cyber security solutions: ultimately, this involves modelling and defining the trade-off between privacy and utility in information sharing IoT scenarios, in a mathematically rigorous way. b) Familiarise with fundamental data mining and machine learning algorithms with a focus on their application as privacy-invasive technologies. c) Learn how to develop application-specific privacy enhancing techniques, including security layers such as intrusion detection, privacy-by-design methods, and privacy-aware sensing.</p>				
Learning Outcomes	<p>Upon successful completion of this course students should be able to:</p> <ul style="list-style-type: none"> <li>• Discuss privacy-by-design principles.</li> <li>• Get an overview of EU legislative and business regulatory aspects of data handling.</li> </ul>				

	<ul style="list-style-type: none"> <li>• Use cyber security protocols to engineer holistic data privacy system solutions.</li> <li>• Apply fundamental data mining and activity recognition algorithms to run privacy-invasive security tests.</li> <li>• Understand the principles of differential privacy and implement privacy-preserving algorithms.</li> <li>• Design privacy solutions for IoT scenarios, including Smart Grid, Smart Cities and wearable sensor technologies.</li> </ul>		
Prerequisites	None	Co-requisites	None
Course Content	<p><u>IoT scenarios and privacy concerns:</u> Smart meter data collection, wearable and smartphone mobile sensing technologies, data handling and data linking potential risks and system-level analysis.</p> <p><u>Mathematical privacy metrics and privacy invasion tools:</u> relative entropy, mutual information, cluster classification, regression analysis, residual features, activity recognition, non-intrusive appliance load monitoring, exploratory data mining, differential privacy and atypicality.</p> <p><u>Cyber-security privacy protection solutions:</u> anonymisation with trusted third party, data aggregation, data splitting, secure multi-party communication protocols, homomorphic encryption, zero-proof cryptosystem, data obfuscation, physical behaviour optimisation. Anonymity networks (e.g. Tor and I2P), ethics</p> <p><u>Information-theoretic privacy preserving techniques:</u> privacy-utility trade-off optimisation, privacy-aware data sensing, lossy data compression, rate-distortion function, differentially private billing. General Data Protection Regulation (GDPR)</p> <p><u>Standardisation, regulatory and business aspects:</u> consent-based approaches, ethical aspects of data collection, access control restrictions, business requirements and risks. ISO/IEC 27001 family of standards.</p> <p>Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the practical privacy scenarios and IoT considerations.</p>		
Teaching Methodology	Distance Learning		
Bibliography	<p><i>Keith M Martin, Everyday Cryptography: Fundamental Principles and Applications. Oxford University Press.</i></p> <p><i>Brij Bhooshan Gupta, Quan Z. Sheng, Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices.</i></p>		

	<p><i>R. Mendes and J. P. Vilela, "Privacy-Preserving Data Mining: Methods, Metrics, and Applications," in IEEE Access, vol. 5, pp. 10562-10582.</i></p> <p><i>Clarence Chio, David Freeman, Machine Learning and Security: Protecting Systems with Data and Algorithms.</i></p> <p><i>Dua, S. and Du, X., Data mining and machine learning in cybersecurity. Auerbach Publications</i></p> <p><i>IEEE/ ACM/ Elsevier/ Springer Journals and Magazines</i></p>						
Assessment	<table border="1"> <tr> <td>Examinations</td> <td>50%</td> </tr> <tr> <td>On-going evaluation</td> <td>50%</td> </tr> <tr> <td></td> <td>100%</td> </tr> </table>	Examinations	50%	On-going evaluation	50%		100%
Examinations	50%						
On-going evaluation	50%						
	100%						
Language	English						

Course Title	Incident Response and Forensic Analysis				
Course Code	CYS625				
Course Type	Optional				
Level	Master (2 <sup>nd</sup> cycle)				
Year / Semester	2 <sup>nd</sup> Year / 3 <sup>rd</sup> Semester				
Teacher's Name	Dr Olga Angelopoulou				
ECTS	10	Lectures / week	None	Laboratories / week	None
Course Purpose and Objectives	<p>The objective of this course is to introduce concepts and techniques related to the topics of incident response and forensic analysis. An incident is a matter of when, not if, a compromise or violation of an organization's security will happen. Today's cyber threats have become very complex and require additional resources and skills to mitigate detect analyze and respond to. The uniqueness and complexity of these threats is often beyond the capabilities of ordinary IT teams. Detecting these incidents therefore requires additional skills such as forensics, malware analysis and threat detection which help decipher how these threats operate and therefore how they can be prevented and mitigated. Forensic analysis techniques are introduced, along with standard tools that are used to carry out computer forensic investigations, with emphasis on digital evidence acquisition, handling and analysis in a forensically sound way.</p>				
Learning Outcomes	<p>Upon successful completion of this course students should be able to:</p> <ul style="list-style-type: none"> <li>• Define and describe the main phases of incident response</li> <li>• Evaluate incident data and indicators of compromise (IOC) to determine the correct responses to an incident</li> <li>• Identify different kinds of attacks methods to counter their effects</li> <li>• Describe the different phases of incident response – preparation, identification, containment, eradication, recovery, follow-up</li> <li>• Explain the principles of evidence collection and the chain of custody</li> <li>• Identify and evaluate key forensic analysis techniques</li> <li>• Describe the application of such techniques to real situations and the connection with incident response</li> </ul>				

	<ul style="list-style-type: none"> <li>Describe the ways in which cybercrime investigations use forensic analysis and legal issues regarding evidence collection.</li> </ul>		
Prerequisites	None	Co-requisites	None
Course Content	<p><b>Introduction:</b> Definitions of incident response and forensic analysis, relation of incident response to the rest of cybersecurity operations, incident response phases - preparation, identification, containment, eradication, recovery, follow-up, indicators of compromise (IOC), forensic analysis as an incident response tool and as support for cybercrime investigations, cybersecurity forensics principles.</p> <p><b>Preparation:</b> Policies and procedures, incident workflows, guidelines, incident handling forms, principles of malware analysis, log analysis, threat intelligence, vulnerability management, penetration testing, digital forensics, incident ticketing systems, incident documentation templates.</p> <p><b>Identification:</b> Detection, incident triage, information gathering and reporting, incident classification, indicators of compromise (IOC).</p> <p><b>Containment:</b> Damage limitation, network segment isolation, system isolation, forensic backup and imaging, use of write blockers, temporary fixes, malware spread limitation.</p> <p><b>Eradication:</b> Actual removal and restoration of affected systems, removal of attack artifacts, scanning of other systems to ensure complete eradication, use of IOCs on other systems and local networks, cooperation with forensic analysis to understand the attack fully.</p> <p><b>Recovery:</b> Test and validate systems before putting back into production, monitoring of system behavior, ensuring that another incident will not be created by the recovery process.</p> <p><b>Follow-up:</b> Documenting lessons learned, preparatory activities for similar future incidents, technical training, process improvement.</p> <p><b>Digital Forensics Investigation Process:</b> Applicable laws, investigation methodology, chain of custody, evidence collection, digital evidence principles, rules and examination process, first responder procedures.</p> <p><b>Technical forensics tools and techniques:</b> Hard disks, removable media and file systems, Windows forensics, duplication/imaging of</p>		

	<p>forensic data, recovering deleted files and hidden or deleted partitions, steganography and image forensics, log analysis, password crackers, network device forensics, packet capture analysis, email tracking, mobile forensics, investigation of attacks, common tools (EnCase, FTK, etc.)</p> <p>Business case study and lecture: Lecture by invited experts from the cybersecurity industry, including law enforcement. Discussion normally focuses on the practicalities and challenges of incident response and the ways in which forensic analysis contributes to successful cybercrime prosecutions.</p>			
Teaching Methodology	Distance Learning			
Bibliography	<p><i>"Incident Response &amp; Computer Forensics, Third Edition"</i> by Jason T. Lutgens and Matthew Pepe</p> <p><i>"Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder"</i>, by Don Murdoch</p> <p><i>"Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response"</i>, by Leighton Johnson</p> <p><i>"The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics"</i>, by John Sammons</p> <p><i>"Digital Forensics with Open Source Tools"</i>, by Cory Altheide and Harlan Carvey</p> <p><i>"Digital Forensics Processing and Procedures"</i>, by David Lilburn Watson and Andrew Jones</p> <p>IEEE Journals and Magazines</p>			
Assessment	<p>Examinations On-going evaluation</p> <table border="1"> <tr> <td>50%</td></tr> <tr> <td>50%</td></tr> <tr> <td>100%</td></tr> </table>	50%	50%	100%
50%				
50%				
100%				
Language	English			

Course Title	Master Thesis			
Course Code	CYS695			
Course Type	Compulsory (for students choosing the Master Thesis) Optional (for students choosing the elective courses)			
Level	Master (2 <sup>nd</sup> cycle)			
Year / Semester	2 <sup>nd</sup> Year / 3 <sup>rd</sup> Semester			
Teacher's Name	Dr George Christou			
ECTS	30	Lectures / week	None	Laboratories / week
Course Purpose and Objectives	<p>The course's purpose is to provide guidance on how to write a successful Master's Thesis. It aims to provide skills in research methods, regardless of the student's subfield of study (as long as it is in the general field of Computer Science). It also aims to equip the student with the tools required to manage a project as large as a Master's thesis, through providing project management techniques. Finally, it aims to prepare the student for independent work as a recipient of a Master's degree.</p>			
Learning Outcomes	<p>Upon successful completion of this course students should be able to:</p> <ul style="list-style-type: none"> <li>• Demonstrate written and oral technical research skills.</li> <li>• Select and justify a research topic, and use various resources to carry out a literature search.</li> <li>• Design, execute, interpret and report results from empirical research projects.</li> <li>• Manage a project and explain the relevant techniques and tools needed in order to complete it successfully on time and within budgeted resources.</li> <li>• Identify real-world problems to which academic concepts and methods can be realistically applied to improve or resolve the problem situation.</li> <li>• Select and use effectively the methods and techniques appropriate for particular cases, and plan and manage their work.</li> <li>• Evaluate a proposed solution and prove its worth to the client.</li> <li>• Critically evaluate the project and the proposed solution, as well as recognize and describe legal, social or ethical obligations stemming from the project.</li> </ul>			
Prerequisites	Consent of Instructor	Co-requisites	None	

Course Content	<p><b>Part A: Research Methods:</b></p> <p>The nature of research: Definitions and types of research; research process; topic selection and scope; feasibility and value.</p> <p>The literature search: Sources of information; differentiating between types of sources; primary, secondary and tertiary sources; using the library and digital databases to conduct efficient literature reviews; searching the Internet; role of the supervisor.</p> <p>Project management: Methods, techniques and tools for research design, and data collection.</p> <p>Analysis and synthesis: Statistical and qualitative techniques for data analysis; use of appropriate software. Reliability and validity of research projects.</p> <p>Presentation of research findings: Project structure; conventions on citation and quotations; style of writing a report.</p> <p><b>Part B: Thesis:</b></p> <p>The student selects a topic from the Thesis Topics Catalogue which becomes available on the first day of the first week of the semester. Students receive the catalogue via a personal email sent to them by the course instructor, and they are also available on the departmental website. Once the students receive the topics, they have two weeks (by the second Friday of the semester) to choose a topic. Topics are assigned on a First-Come, First-Served basis, given that the students have passed all the pre-requisite courses for a specific topic. Once a topic is selected and agreed upon with the associated supervisor, the course follows the weekly breakdown structure as that is provided in the study guide. See Master Thesis study guide for further details.</p> <p>The specific deliverables for each individual's project must be discussed and decided upon in consultation with the academic and industrial supervisors. The roles and responsibilities are outlined below:</p> <p><b>Student:</b></p> <ul style="list-style-type: none"> <li>• To identify and scope a suitable problem</li> <li>• Explain the value of the research</li> <li>• To plan and control the project</li> </ul>
----------------	---

	<ul style="list-style-type: none"> <li>• To carry out the necessary work</li> <li>• To review and evaluate the work done</li> <li>• To prepare and present the project deliverables</li> <li>• To initiate and maintain contact with the academic supervisor</li> </ul> <p><b>Academic Supervisor:</b></p> <ul style="list-style-type: none"> <li>• To comment on the suitability of the selected project</li> <li>• To discuss the mapping of the project onto the course requirements</li> <li>• To discuss and approve the intended deliverables</li> <li>• To suggest starting points for consideration of background research</li> <li>• To discuss the nature of the thesis and comment on early drafts</li> <li>• To provide advice on issues associated with the project such as design, implementation, and proof of concept as appropriate.</li> <li>• To attend any presentation or demonstration of the project</li> </ul> <p><b>Program-specific content</b></p> <p>As this course is taught in a variety of Master's programs offered by the department of Computer Science, the last part of the course will discuss specific research methods for each discipline. The specific topics will be provided by the instructor of the course according to the specific needs of the audience.</p>
Teaching Methodology	Distance Learning
Bibliography	<p>Any material suitable for the subfield in which the student is undertaking the thesis will be specified by the instructor.</p> <p>Howard, K. &amp; Sharp, J.A., The Management of a Student Research Project, Gower</p> <p>Turk, C. &amp; Kirkman, J., Effective Writing: Improving Scientific, Technical and Business Communication, Chapman &amp; Hall</p> <p>J. Zobel., Writing for Computer Science, Springer.</p> <p>W. Navidi, Statistics for Engineers and Scientists, McGraw-Hill Science/Engineering/Math; Latest Edition.</p>



	30%	60 marks
	• Novelty. Does the work improve significantly the current state of the art?	
	30%	60 marks
	• Ability to critically review the project and assess its implications for future work in view of the project recommendations and conclusions	
	10%	20 marks
	• Project Management: Ability to plan and control the project	
	10%	20 marks
	<u>100%</u>	<u>200 marks</u>
	In addition students are reminded about presentation issues: Is the document format (including spelling) of good quality? Is it well organized into appropriate sections? Is the style of language used appropriate for an academic report?	
	<b>ASSESSMENT:</b>	
	Written Thesis: 80%	
	Oral Presentation 20%	
Language	English	



**FORM: 200.1.3**

## **STUDY GUIDE**

**Course : CYS602 - Introduction to Cybersecurity**

## Course Information

<b>Institution</b>	European University Cyprus		
<b>Programme of Study</b>	Cybersecurity (MSc)		
<b>Course unit</b>	CYS602	Introduction to Cybersecurity	
<b>Level</b>	<i>Undergraduate</i>		<i>Postgraduate</i>
		<i>Master</i>	<i>PhD</i>
		√	
<b>Language of Instruction</b>	English		
<b>Teaching Methodology</b>	Distance Learning		
<b>Course Type</b>	<i>Compulsory</i>		<i>Optional</i>
	√		
<b>Number of Group Consultation Meetings/ Web-Conferences/ Lectures</b>	<i>Total</i>	<i>Face to Face</i>	<i>Web-Conferences</i>
	14	1	13
<b>Number of Activities/ Assignments</b>	4		
<b>Final Assessment</b>	<i>Assignments</i>		<i>Final Examinations</i>
	50 %	50 %	
<b>Number of Credits (ECTS)</b>	10		

<b>Study Guide drafted by</b>	Dr Pericles Leng Cheng
<b>Editing and final approval of Study Guide by</b>	Dr Yianna Danidou

## COURSE CONTENTS

		Page
	Introductory Notes	4
	First Group Consultation Meeting	5
1	Week 1 – Technology and cybercrime	7
2	Week 2 – Cryptography	12
3	Week 3 – Introduction to information security and the need for security	17
4	Week 4 – Access control and Physical and Environmental security	21
5	Week 5 – Security Technology: Intrusion Detection and Prevention Systems, and Other Security Tools	27
6	Week 6 – Network vulnerability assessment	31
7	Week 7 – Contingency Planning and Networking Incident Response	35
8	Week 8 – Business Continuity and Disaster Recovery Planning	39
9	Week 9 – Cybersecurity and IT Law	42
10	Week 10 – Ethics	45
11	Week 11 – Invited lectures	47
12	Week 12 – Invited lectures	49
13	Week 13 – Invited lectures	49
14	Revision and Final Examination	50

## INTRODUCTORY NOTES

The CYS602 course is the first core course of the program. Students that begin their journey to becoming cybersecurity experts must have a good understanding of all the areas that encompass the security operations of an organization. This course will introduce students to the current trends in cybersecurity, starting with cryptography and then analyzing the different tools that are used to secure an organization.

This course introduces students to concepts and tools used to establish a secure network, monitor the operations of the network and also reacting to any possible threats that may try to impact the operations of the organization. The course begins with an explanation of cryptography, one of the main pillars of security and then moves on to access control and physical security leading up to intrusion prevention and intrusion detection systems. Students also learn how to plan for possible threats and how to ensure business continuity during a disaster.

Students are required to attend bi- weekly virtual classes to submit discussion posts, reading assignment case studies, media content review and exams.

On successful completion, the student will have the knowledge and skills to:

- Display a comprehensive understanding of cybersecurity and why it is imperative in an organization;
- Explain how cryptography works and how it is used to ensure the Confidentiality, Integrity and Accountability of data;
- Evaluate network access control methods and physical and environmental security policies;
- Describe how Intrusion Detection Systems and Intrusion Prevention Systems work;
- Understand the relationship between data, ethics, and IT law; and
- be able to critically assess their own work and education in the area of cybersecurity. In particular, course assignments will emphasize researcher and practitioner reflexivity, allowing students to explore their own social and ethical commitments as future cybersecurity experts.

## 1st GROUP CONSULTATION MEETING

### Programme Presentation

Leading companies today are rethinking the role of information security in their organizations. They realize that in a digital world, cybersecurity is the key to safeguarding their most precious assets—intellectual property, customer information, financial data, and employee records, among others. But far more than a defensive measure, companies also know that cybersecurity can better position their organization with business partners, customers, investors, and other stakeholders.

The European cybersecurity market is about 25% (i.e. about €17bln) of the world market (estimated at €70bln in 2015), with an average yearly growth slightly larger than 6%, when the world market is growing at about 10%/year. Recent study compiled by Europe's cybersecurity industry leaders pointed out that Europe is in danger of falling behind in the international digital economy field.

The Master in Cybersecurity is a cutting-edge program, designed for those wishing to develop a career as a cyber-security professional, or to take a leading technical or managerial role in an organization critically dependent upon data and information communication technology. Students will develop an advanced knowledge of information security and an awareness of the context in which information security operates in terms of safety, environmental, social and economic aspects. They will gain a wide range of intellectual, practical and transferable skills, enabling them to develop a flexible professional career in IT.

Key elements of this postgraduate degree are: the *real life experience* given by the opportunity to apply their theoretical knowledge through specialized virtual and remote security laboratories in which they will be able to carry out activities such as reconnaissance, network scanning and exploitation exercises, and investigate the usage and behavior of security systems such as Intrusion Detection and Prevention Systems thus becoming confident in the practical application of the latest tools; the *high-level insight* that will enhance student's ability to research and design creative cyber security solutions to address business problems; *hands-on skills* through experimentation with security techniques, cryptographic algorithms, cyber forensics building an ethical hacking environment; and *flexibility* since students will also be able to choose either the completion of a Master thesis or to complete a Research methods course and two elective courses.

Students undertake modules to the value of 90 ECTS credits.

## COURSE PRESENTATION THROUGH THE STUDY GUIDE

This study guide has been prepared collectively by the academic staff teaching in the program of study this course belongs to and by the Distance Education Unit Director. The guide has been approved by the relevant Department Chair and the Distance Education Unit Director. The study guide is based on the syllabus and learning material (provided through the online learning platform) of the course CYS601. The guide consists of a basic tool of the learning process for this course and it has been designed to use it along with the course learning material. The aim of this guide is to direct students on how to use the learning material of this course in order to understand and comprehend it. The guide aims to provide the necessary support needed for distance learning. The guide is continuously updated to keep in accord with the course learning material and to meet the aim of the course. Although the study guide provides extensive information related to the course, it does not substitute in any way the learning material provided on the learning platform. It is imperative that the studying of the learning material and executing the rest of the activities of the course (e.g. attending online lectures, completing coursework) are very important for the successful completion of the course.

This guide consists of a number of units, divided in 13 weeks, each one comprised of the summary and introductory remarks, aim, learning outcomes, keywords, required learning material, recommended further learning material, self-assessment activities and expected time for self-study. At the end of this study guide, students can find suggested solutions and proposed answers to all the self-assessment activities of this guide. It is very important that students carry out the suggested self-assessment activities because it will assist them to understand in a practical way the theoretical material they study for this course. In addition, the self-assessment activities help to motivate and encourage students to carry out their self-study and to develop their analytical and critical thinking skills. The self-assessment activities together with the model answers to the self-assessment activities serve as a kind of a self-assessment for students. The expected time for self-study of each unit includes the expected time spent on studying the learning material and carrying out the self-assessment activities of each unit. The expected time for self-study does not include the expected time for attending online lectures, coursework preparation, final examination preparation, and final examination itself.

### Recommended time for the student to work

Approximately 5 hours to review the study guide

# TECHNOLOGY AND CYBERCRIME

1<sup>st</sup> Week

## Summary

In this meeting the students will learn the basics of cyberattacks. Students need to understand how technology affects everyday life and how attackers can use the power and vulnerabilities of technology to perform attacks on systems. There are different types of people committing cyberattacks and there are a number of different cyberattacks, so the students need to learn all about the who, what and why of cyberattacks.

## Introductory Remarks

Students will become familiarized with the Security Operations Centers (SOC) what kinds of education and certifications may lead to a career working for such an organization.

The first part of the lecture will discuss the targets that attackers will focus on such as hijacking people, ransoming companies or even targeting nations.

Types of Attackers		
Attacker	Skill Level	Motivation
Hacker	High	Improve Security
Cracker	High	Harm Systems
Script Kiddie	Low	Gain Recognition
Spy	High	Earn Money
Employee	Varies	Varies
Hacktivist	Varies	Promote cause
Cyberterrorist	High	Support Ideology

Information Security © 2006 Eric Vanderburg

Figure 1. Types of attackers

Attackers may fall in one of several categories depending on their expertise as depicted in Figure 1. Amateurs, or script kiddies for example, are individuals that can use ready made tools to launch attacks even though they have little or no skills. These types of attackers may be simply curious about how attacks happen, or just want to show off their skills but even these attackers can cause serious harm to individuals or organizations. Hacktivists on the other hand are attackers that have

a specific agenda and that is to protest against political and social ideas. These attackers try to expose sensitive information and disrupt the normal operation of the government or organization they are targeting using tools such as Distributed Denial of Service (DDoS) attacks. Another group of attackers can launch attacks simply for financial gain. These attackers try to gain access to bank accounts, personal information or anything else that can get them some kind of financial gain. Finally, some attackers may be sponsored by an organization or government to gain access to politically sensitive information, or industrial espionage.

Now that a lot of our devices are always connected to the Internet there is a large pool of devices that an attacker may utilize to attack a system. Not knowing how each Internet of Things (IoT) device works in our environment causes holes in our security that one may exploit.

How can someone measure the financial impact of a cyberattack? This is a question that is extremely hard to answer given the fact that information is difficult to quantify. An article in Forbes estimates that around 400 billion dollars are lost annually to cyberattacks.

Information that attackers may try to extract include Personally Identifiable Information (PII) or Personal Health Information (PHI). In addition to personal information, attackers target organizations to access company sensitive data that may lead to a loss of competitive advantage by the company. Attackers may also influence politics and threaten national security by attacking government-controlled devices.



Figure 2. The makings of a Cybercrime

In Figure 2, one can see the steps that could lead to a cybercrime being committed. An unsuspecting target may be tricked into installing certain malicious software in his computer which can then allow an attacker to gain control of the targeted system and ultimately gain access to the data stored on the device.

Security Operation Centers (SOC) are groups of people that use formal, structured and disciplined approaches to confront cyberattacks in an organization. The main parts of a SOC are the people in the center, the processes they follow to handle a cyberattack and the technology they can utilize in their response to the attacks. People are broken down into tiers from Tier 1 who is an alert analyst responsible for spotting the alerts and verifying the validity of an attack, tier 2 who investigates attacks even further to ascertain their impact and advise on actions to be taken and tier 3 who is the expert in a specific area of the attacks and can hunt for potential threats.

There are a number of security certifications that a cybersecurity expert can get to increase knowledge on the subject. CISCO CCNA Cyber Ops, CompTIA Cybersecurity Analyst, (ISC)<sup>2</sup> Information Security Certification, Global Information Assurance Certification (GIAC) and more.

## Aim/Objectives

The aim of this chapter is to introduce students to the different types of cybercrimes, the different attackers that may launch an attack and the motivations behind the attackers. The students will also learn what is a Security Operations Center and how becoming educated in Cybersecurity can help them get a job in such a center or in the cybersecurity branch of a large organization.

## Learning Outcomes

By the end of this week the students should be able to:

- Classify the various types of cybersecurity attacks
- Identify the types of cybersecurity attackers
- Learn how to analyze previous attacks and identify attack characteristics such as the type of attack, the attacker profile, the motivation behind the attack and the final outcome of the attack

## Key Words

Amateur attackers	Hacktivists	Organized Crime Groups
State sponsored attackers	Terrorists	Cyberespionage
Cyberwarfare	Personally identifiable information	Personal health information
Security Operations Center (SOC)	Cybercrime	

## Annotated Bibliography

### Basic

Chapter 1 of Cybercrime and Digital Forensics: An Introduction by Thomas J. Holt, Adam M. Bossler

An introduction to how technology has affected human behavior, how technology can be used in criminal investigation and how cybercrimes occur across the world.

### Supplementary

Top hacker shows us how it's done | Pablos Holman | TEDxMidwest

(<https://youtu.be/hqKafI7Amd8>)

All your devices can be hacked - Avi Rubin

(<https://www.youtube.com/watch?v=BHHCvcCUOWU>)

Example of a hijacked video feed. (<https://www.youtube.com/watch?v=zcmmFQGxMNU>)

## Self-Assessment Exercises

### Exercise 1.1

Perform a search for high profile attacks, analyze the attacks based on victims, tools used, targeted systems, motivation for the attack and the final outcome of the attack.

## **Recommended time for the student to work**

15 hours

# CRYPTOGRAPHY

2<sup>nd</sup> Week

## Summary

When the Internet was first developed data security was not the main concern. Nowadays where data is extremely sensitive and operation critical it is important to understand how to protect them using various techniques. Securing the infrastructure devices can be done through the use of AAA, ACLs, firewalls, IPS and other techniques. After securing the devices it is important to start considering how to secure the data that is being transmitted over the network. The four main elements that are addressed when talking about data security are: confidentiality, data integrity, origin authentication and non-repudiation. Figure 3 below shows what each element guarantees.

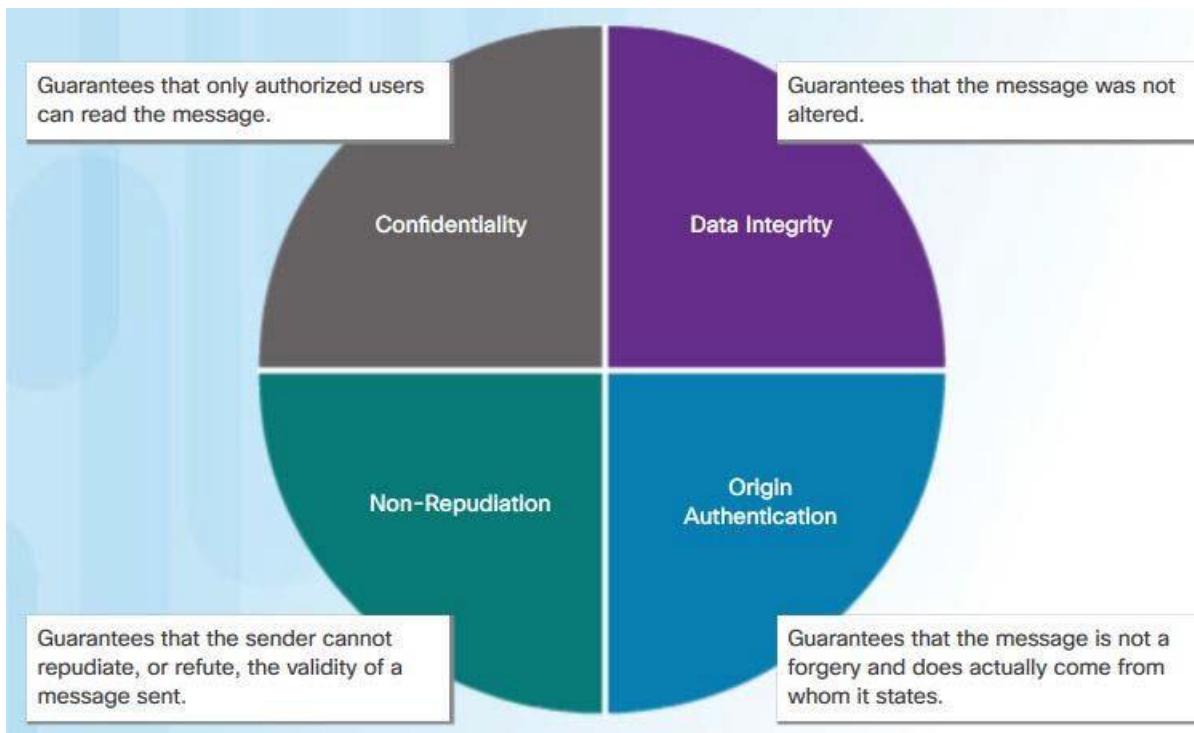


Figure 3. The four elements of data security

## Introductory Remarks

Cryptography is the process of developing new algorithms that can generate codes that can encrypt data. The opposite of this is cryptanalysis which is the process of developing algorithms to break the codes and decrypt the data.

In old encryption algorithms the algorithm had to be kept secret in order for the encryption to be safe. This meant that if anyone could get hold of the algorithm then the data could be decrypted. Nowadays the algorithm is available for everyone to see but the important part of the encryption is the secret key that is used in the algorithm. Two terms that can characterize keys are the key length which specifies how large the key is and the second is the keyspace which signifies the number of possibilities that are generated by a specific key length. For example, a 2 bit key length can generate 4 codes whereas a 40 bit key length can generate 1.099.511.627.776 codes. The bigger the key the better the encryption but that leads to longer processing times which may impact performance.

To handle integrity and authenticity of data the most common techniques are using cryptographic hash functions such as MD5 and SHA. These hash functions can ensure that the data that was transmitted is actually the same as the one the sender intended to send and that it was not changed during the transmission.

The method used to ensure confidentiality is encryption. Encryption can be symmetric or asymmetric. In symmetric encryption both ends of the communication use a shared key that they use to encrypt and decrypt the communication. In asymmetric encryption each end uses different keys to encrypt and decrypt data. Examples of asymmetric encryption protocols include Internet Key Exchange (IKE), Secure Socket Layer (SSL), Secure Shell (SSH) and Pretty Good Privacy (PGP).

The Public Key Infrastructure uses trusted third-party certificate authorities (CA) to confirm the authenticity of keys. Every organization that needs secure connections can ask a CA to generate a public key and a private key. The end-device that keeps the private key and the public key is given to everyone. Anyone encrypting data with the public key can only be decrypted by the private key while anything encrypted by the private key can be decrypted by anyone with the public key. This serves as a start of communication with the one end encrypting a secret key using the public key of the server. The server decrypts the secret key with its private key and then encrypts a message with the secret key and sends it to the initiator of the communication. After

this exchange the two ends now share a common secret which can be used for symmetric encryption.

## Aim/Objectives

The aim of this week is to introduce the student to ways to encrypt data. In previous weeks the student learned how to harden device security using different techniques and now the student needs to ensure that the traffic that moves through the network is protected. Students learn about confidentiality, integrity, non-repudiation and authentication and then learn how to use encryption and hashing methods to ensure those elements are established.

## Learning Outcomes

By the end of this week the students should be able to:

- Understand what confidentiality, integrity, non-repudiation and authentication are and how they affect data communication
- Identify methods that can be used to encrypt and decrypt data using symmetric and asymmetric algorithms
- Discuss how Public Key Infrastructure works

## Key Words

Shared key	Symmetric encryption	Asymmetric encryption
PKI	DH	MD5
SHA	CA	IKE
SSH	SSL	PGP

## Annotated Bibliography

### Basic

Chapter 8 of Principles of Information Security by Michael E. Whitman, Herbert J. Mattord

An overview of the fundamentals of cryptography, the different cipher models and cryptographic algorithms, and a description of the protocols used in secure communications.

## Self-Assessment Exercises

### Exercise 2.1

#### Creating Codes

Secret codes have been used for thousands of years. Ancient Greeks and Spartans used a scytale (rhymes with Italy) to encode messages. Romans used a Caesar cipher to encrypt messages. A few hundred years ago, the French used the Vigenère cipher to encode messages. Today, there are many ways that messages can be encoded.

### Exercise 2.2

#### Encrypting and Decrypting Data Using OpenSSL

In this lab, you will complete the following objectives:

Encrypting Messages with OpenSSL

Decrypting Messages with OpenSSL

### Exercise 2.3

#### Encrypting and Decrypting Data Using a Hacker Tool

In this lab, you will complete the following objectives:

Setup Scenario

Create and Encrypt Files

Recover Encrypted Zip File Passwords

#### Examining Telnet and SSH in Wireshark

### Exercise 2.4

#### Certificate Authority Stores

In this lab, you will complete the following objectives:

Certificates Trusted by Your Browser

Checking for Man-In-Middle

## **Recommended time for the student to work**

15 hours

# INTRODUCTION TO INFORMATION SECURITY AND THE NEED FOR SECURITY

3<sup>rd</sup> Week

## Summary

One of the first things that a cybersecurity expert needs to learn is how attackers try to infiltrate networks and what tools they use to perform their attacks. This will allow them to learn how to prevent such attacks in the future. To better understand network security one must know terms such as threats, vulnerabilities, exploits and risks. Cybersecurity experts need to learn how to manage risk through risk acceptance, avoidance, limitation and transfer.

## Introductory Remarks

Understanding the background of hackers is important so that one can identify the reasons why a hacker is attacking a specific network and what are the expectations from that attack. Hackers can be simple script-kiddies that just want to see if they can penetrate a network, or hacktivists who want to protest against a government or organization by attacking their networking resources. But attackers may also be cybercriminals whose agenda is based on financial reasons either by them acquiring money through buying and selling information stolen from victims or by being hired by criminal organizations to execute the network attacks.

The number of tools that hackers use are numerous but most of them fall in the following categories:

- Password crackers
- Wireless hacking
- Network scanning
- Packet crafting
- Packet sniffers
- Rootkit detectors
- Fuzzers

Attacks may be categorized in the following areas:

- Eavesdropping
- Data modification
- IP address spoofing
- Password-based
- Denial-of-Service
- Man-in-the-Middle
- Compromised key
- Sniffer attack

The main types of cyberattacks can be seen in Figure 4. Malware which is short for malicious software that can infect an end device is a term encompassing the three most prominent types of attacks, namely viruses, trojans and worms. Viruses are malicious software that execute harmful code on the end device, a trojan is a program that is disguised as a valid application that runs harmful code when executed. A worm is similar to a virus with the added advantage that it can replicate itself from one device to another without user interaction. By infecting an end device hackers can modify data and then request payment to revert the data to its original format making those attacks ransomware. Other types of malware include spyware, adware, scareware, phishing and rootkits.

Other than malware attacks, network attacks include reconnaissance attacks, access attacks and Denial-of-Service (DoS) attacks. Reconnaissance attacks are based on gathering information that can be helpful in attacking a network. Access attacks try to exploit known vulnerabilities in systems to gain access to a networking device and DoS attacks try to bring the network down by making its resources unavailable to valid users of the system.

Other than malware attacks, network attacks include reconnaissance attacks, access attacks and Denial-of-Service (DoS) attacks. Reconnaissance attacks are based on gathering information that can be helpful in attacking a network. Access attacks try to exploit known vulnerabilities in systems to gain access to a networking device and DoS attacks try to bring the network down by making its resources unavailable to valid users of the system.

## Types of malware

These are the main types of malware that can be found across the web.

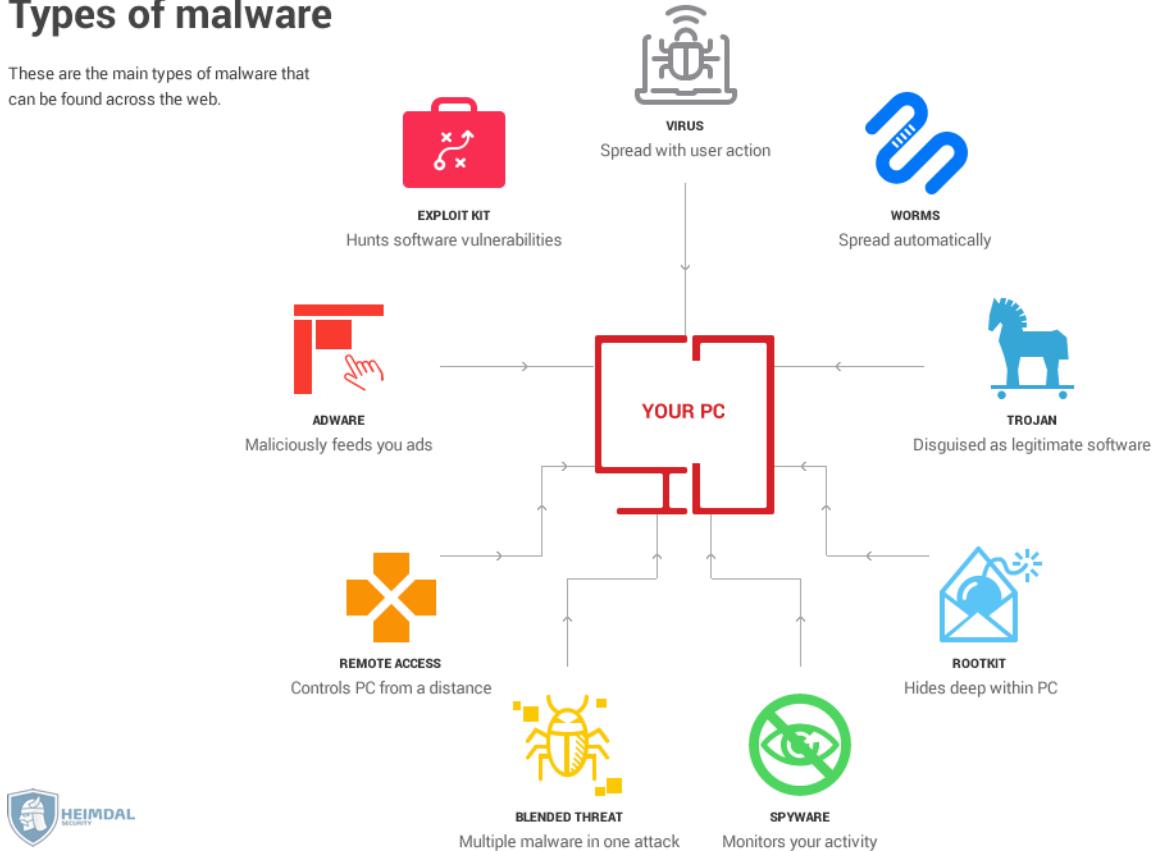


Figure 4. Types of Cyberattacks

## Aim/Objectives

In this week students begin to learn how attackers try to infiltrate networks and end-devices through the use of various hacking tools. The students learn how these tools work and understand the need to recognize the type of attack in order to be able to apply the best countermeasures for that attack.

## Learning Outcomes

By the end of this week the students should be able to:

- Understand the need for Information Security in a networked environment
- Understand how attackers use tools to attack end-devices and network devices
- Identify the types of attacks

- Identify the various types of malware

## Key Words

Script-kiddies	Hacktivists	Cybercriminals
Threat	Malware	Reconnaissance
DoS	DDoS	Virus
Trojan	Worm	

## Annotated Bibliography

### Basic

Chapter 1 and 2 of Principles of Information Security by Michael E. Whitman, Herbert J. Mattord  
Introduction to the history of information technology and an overview of the need for cybersecurity. The second chapter describes the threats and attacks that can cause damage to an organization.

## Self-Assessment Exercises

### Exercise 3.1

Lab - Anatomy of Malware

In this lab, you will research and analyze some recent malware.

### Exercise 3.2

Lab – Social Engineering

In this lab, you will research examples of social engineering and identify ways to recognize and prevent it.

## Recommended time for the student to work

15 hours

# **ACCESS CONTROL AND PHYSICAL AND ENVIRONMENTAL SECURITY**

**4<sup>th</sup> Week**

## **Summary**

Before tackling the security of a network, a cybersecurity expert needs to ensure that the physical and environmental security of the organization is in place. The most secure network in the world is vulnerable if there is not control over who enters the network room. In this week, students learn the basics of access control and how to physically protect systems from malicious attacks as well as learning how to protect the systems from adverse environmental conditions.

## **Introductory Remarks**

While the cybersecurity analyst can secure the intermediary devices and the transmission of data within the network the biggest problem in the security of a network is the endpoint security. Endpoints are the devices that the employees use to access various resources and since the user may not be experts in security they are more vulnerable to attacks that target them. Spam and malware has increased dramatically over the last few years and this can lead to security breaches in organizations.

The first step in securing the endpoint is the installation of antivirus or antimalware software. These types of software can recognize malicious code either through signatures that are distributed by the vendor, heuristic identification of features shared by malware or by analysis of suspicious behavior. Another way is by installing a host-based firewall to enhance the already configured firewall device in the network. An end user can also install security suites that include anti-virus, anti-malware programs, host-based firewalls and other capabilities to secure the end device.

Additional appliances can also be added in the network to protect end users. These devices can be Advanced Malware Protection (AMP), Email Security Appliances (ESA), Web Security Appliances (WSA) and Network Admission Control (NAC).

Host-Based Intrusion Detection Systems (HIDS) can monitor and report on system configuration and application activity. In this way the system can alert cybersecurity professionals of any

suspicious behavior within the host device. HIDS can determine suspicious behavior using anomaly-based testing compared to a baseline model, and policy-based detection that is based on violation of rules.

As the figure below shows the attack surface is continuously expanding bringing more threats to the devices.

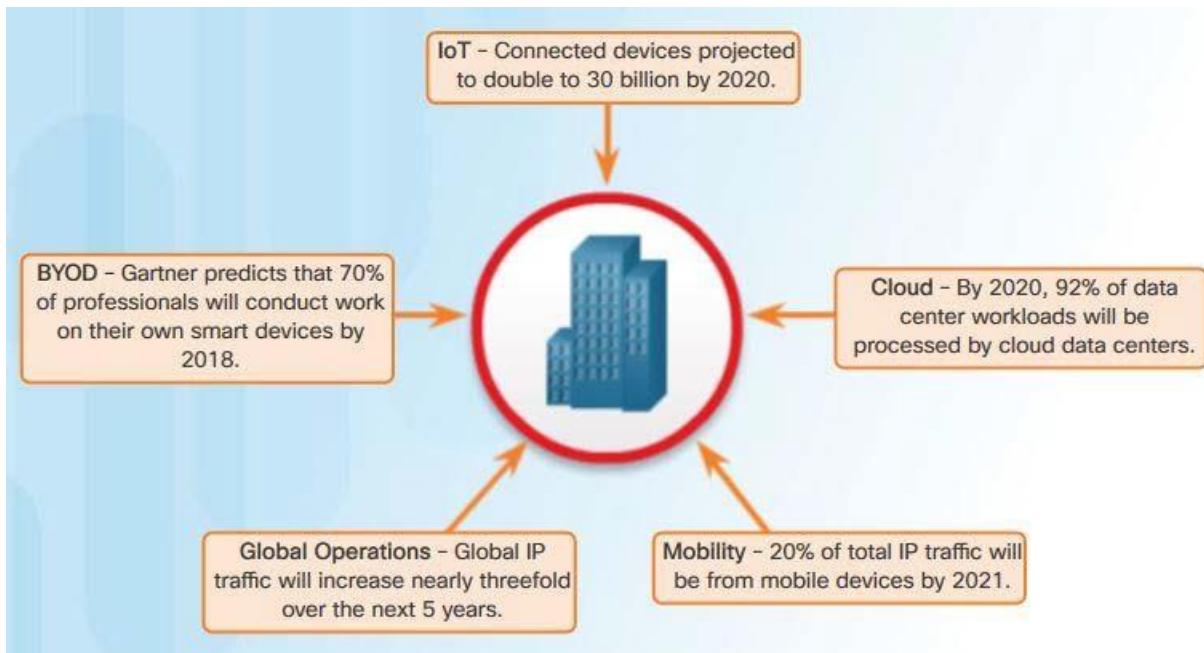


Figure 5. The expanding attack surface

To ensure the security of the network the cybersecurity expert needs to profile both the network and the servers of the organization. This can provide a baseline which will inform the analyst when it detects a network anomaly.

The Common Vulnerability Scoring System (CVSS) is a vendor-neutral framework that weighs risks providing scores for the risk inherent in a vulnerability. CVSS metrics include criteria such as the attack vector, complexity, required privileges, user interaction and scope. The system measures impact metrics based on the confidentiality impact, the integrity impact and the availability impact.

## Most Cyber Attacks Are An Inside Job

Cyber attacks by origin of attacker (2015)

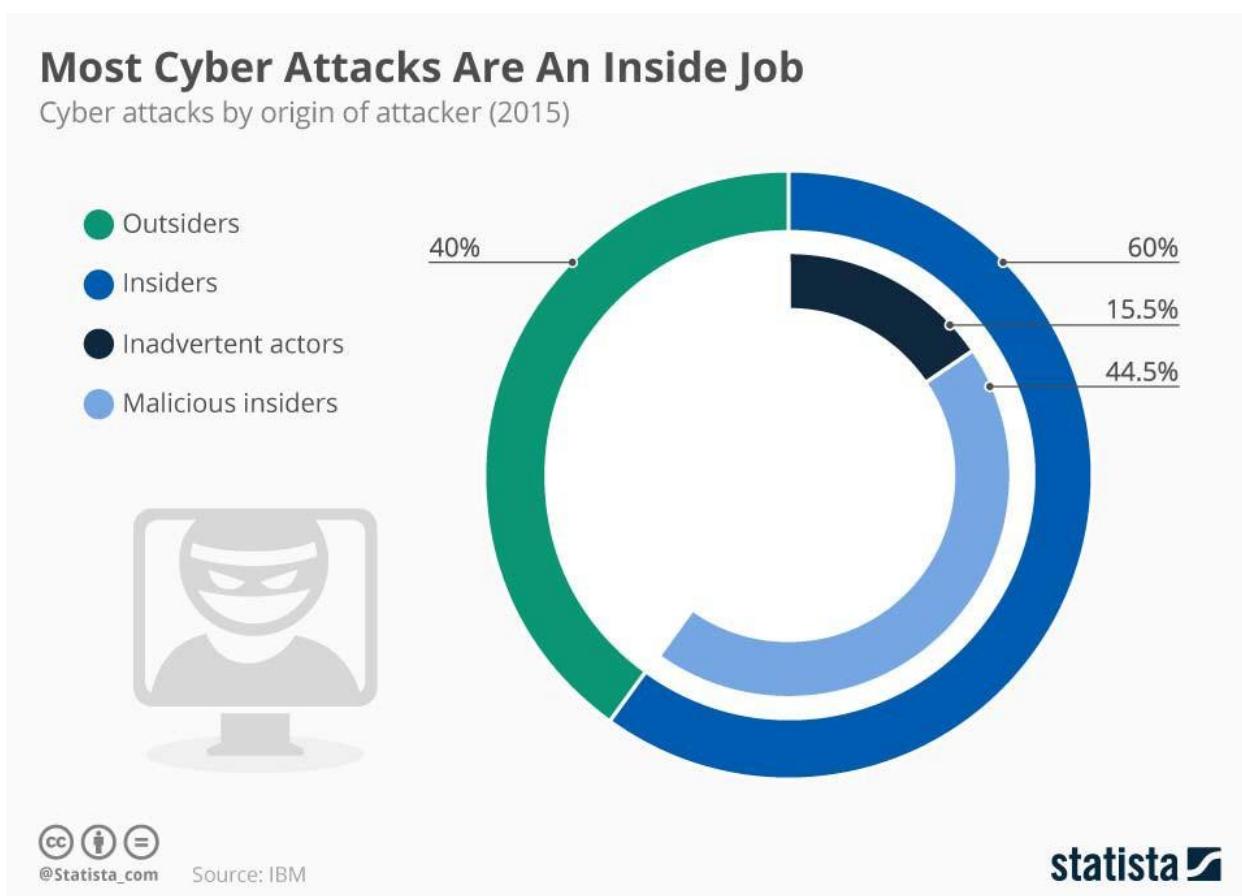


Figure 6. Cyber attacks by origin of attacker

Network Access Control (NAC) allows a security expert to control the access to various areas within the network for the numerous devices that are requesting access to the resources. Figure 6 shows that as much as 60% of the malicious attacks in an organization are actually performed from within the company rather than from the outside. This means that it is of the utmost importance to secure access to resources within the organization as much as from the outside of the organization. As Figure 7 shows, it is imperative for the security of a network to allow only authorized devices to access resources and every endpoint device needs to be compliant with the security policy of the organization to be allowed to access the resources.

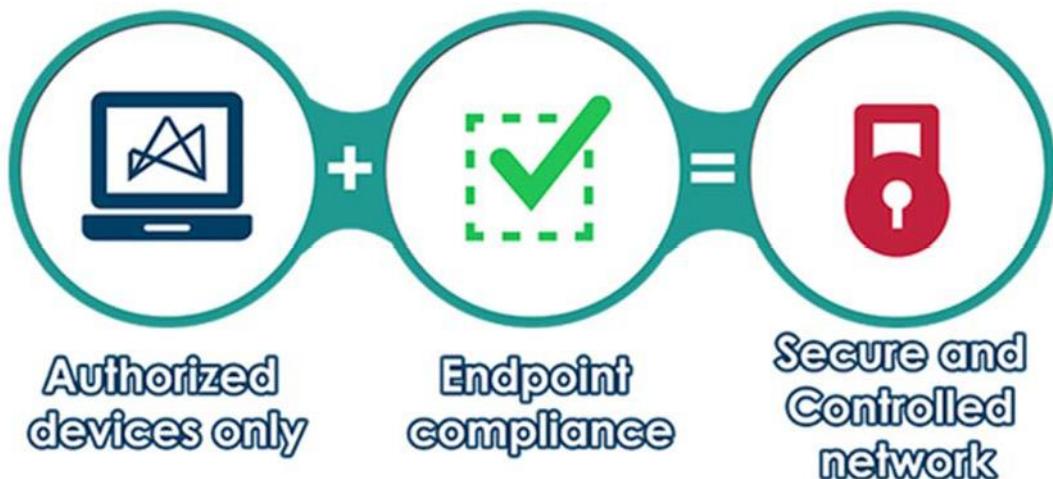


Figure 7. Network Access Control

Even if the network access is controlled it is important to also control physical access to important parts of the organizational infrastructure. Physical access control includes the use of card readers and biometric readers to grant access to secure resources and every secure location requires certain security devices to be in place such as alarm systems, security cameras and electromagnetic interference barriers. Figure 8 shows a number of physical security options for the perimeter of the secure area, the buildings and finally the computer room that contains the restricted resources.

Perimeter	Buildings	Computer room
<ul style="list-style-type: none"> <li>• Security staff around the clock</li> <li>• Facility setback requirements</li> <li>• Barriers</li> <li>• Fencing</li> </ul>	<ul style="list-style-type: none"> <li>• Alarms</li> <li>• Security operations center</li> <li>• Seismic bracing</li> <li>• Security cameras</li> </ul>	<ul style="list-style-type: none"> <li>• Two-factor access control: biometric and card readers</li> <li>• Cameras</li> <li>• Days of backup power</li> </ul>

Figure 8. Physical access security

Another major part of physically securing sensitive resources is environmental security. In most cases devices with sensitive information are placed in secure locations with limited access. This does not mean that the systems are completely immune from malicious attacks. Environmental conditions may influence the operation of these devices leading to loss of data or disruption of

service depending of the situation. Air conditioning must keep the temperature of the computer room in a specific level reducing overheating in devices and humidity must also be controlled to ensure no static electricity from dry environments or high humidity situations. Uninterruptible Power Supplies (UPS) must also ensure the continuous provision of clean, conditioned electrical power to all devices and the ability to safely shutdown devices in the case of a long blackout.

## Aim/Objectives

In this week, the students learn about network access control systems and also how to implement physical and environmental security policies in the organization and especially on restricted resources within the organization. Students understand the need for access control in the organization, and how they can implement policies to ensure the security of sensitive information.

## Learning Outcomes

By the end of this week the students should be able to:

- Understand the need for securing sensitive information
- Describe how network access control works and how it helps in securing network resources
- Identify physical vulnerabilities and how they can secure them
- Recognize the need for environmental controls in secure locations
- Identify ways in which to ensure environmental conditions

## Key Words

Access Control	NAC	Physical controls
Environmental controls		

## Annotated Bibliography

### Basic

Chapter 9 of Principles of Information Security by Michael E. Whitman, Herbert J. Mattord

A description of physical security access controls, fire security and safety, environmental security and remote computing security.

## Activity (5 points)

Pick a security tool and analyze how it works and what kinds of attacks it can stop. You should also list a number of examples where the tool has been successfully or unsuccessfully used during a real-life attack and why it worked or did not work.

## Recommended time for the student to work

20 hours

## **SECURITY TECHNOLOGY: INTRUSION DETECTION AND PREVENTION SYSTEMS, AND OTHER SECURITY TOOLS**

**5<sup>th</sup> Week**

### **Summary**

After learning about the various attacks that threat actors may use to compromise a system, it is important to learn how to defend against those attacks. A Cybersecurity analyst must be able to identify the assets of the organization, the vulnerabilities of those assets and the threats that those assets can have. A good cybersecurity expert needs to have an up-to-date asset inventory with important information such as the location of the assets, information about the asset itself and who can gain access to the asset. Looking at the assets, the analyst needs to identify what the possible vulnerabilities of the system are, who might want to compromise the asset, and what are the consequences if that asset is compromised. Typical threats may include insider attacks, internal system compromise, data center destruction, stolen customer data, fake transactions, or data input errors.

### **Introductory Remarks**

When identifying the threats, the cybersecurity analyst must begin to view the network and start building a defense starting from the edge routers, then the firewalls and finally the internal routers. A common analogy of cybersecurity is like an onion where each layer of the onion is a security layer. Nowadays though and due to the increasing number of networked devices, the system can no longer be represented as an onion with the sensitive data hidden under many layers but as an artichoke where one can remove a few leaves and have access to sensitive data.

## The different types of cyber attacks

Cyber crime worldwide cost \$400 billion in 2015 and is forecast to reach \$2 trillion in 2019\*

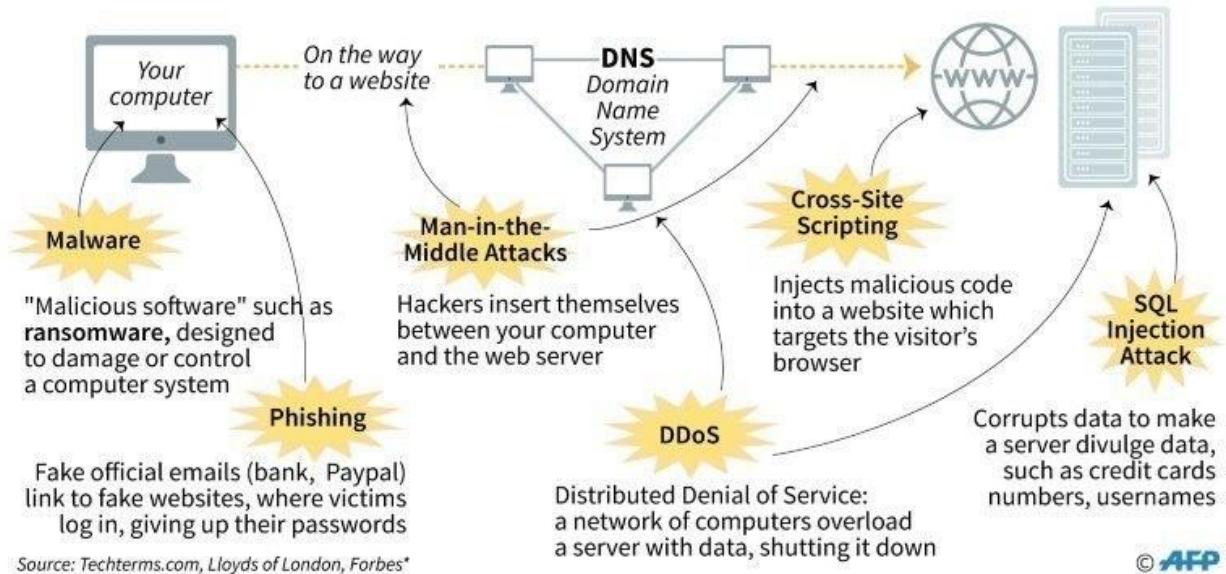


Figure 9. The different types of cyber attacks

Another important security aspect is the definition of security policies. Three types of policies are the company policies which describe the rules of conduct for both employees and employers, employee policies that define information about the employees and their benefits, and finally security policies which define the security objectives of a company and the rules and behaviors of the users and administrators of the system. A security policy shows that the organization is committed to security, sets the rules for expected behavior by its users, ensures consistency in operations, software and hardware acquisition, defines consequences of violations and gives security personnel the support of the management. A security policy may include identification and authentication policy, password policies, acceptable use policy (AUP), remote access policy, network maintenance policy and incident handling policy. Since a lot of organizations are now allowing employees to use their own devices in the company network, a new Bring Your Own Device (BYOD) policy has to be implemented in the security policy.

Cybersecurity experts need to adhere to the CIA triad which defines the Confidentiality, Integrity and Availability components. Confidentiality states that only authorized people or services may access sensitive data, integrity states that the data is protected from unauthorized alteration and availability says that data should always be available to authorized users.

AAA is a framework that defines the Authentication, Authorization and Accounting of systems. Authentication can be local or server based and it is used to authenticate the user using usernames and passwords. Authorization is the definition of what the currently authenticated user may perform on the system and accounting is the ability to keep a log of all the events so that they can later be used in auditing the system.

A cybersecurity analyst needs to always be up to date with the latest attacks and vulnerabilities and to do so one has to be part of a series of security organizations. These organizations include the Computer Emergency Response Team (CERT), the SysAdmin, Audit, Network, Security (SANS) institute and the International Information Systems Security Certification Consortium (ISC)<sup>2</sup>.

Two important security tools are Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS). IPS devices are placed between the edge router and the main internal router and monitor all traffic as it goes through to the network. If a malicious signature is identified the IPS system will take actions to ensure that the network is safe from the attack. In the case of the IDS device, the traffic is monitored but no action is taken. Rather the data is mostly used to keep a log file of an attack to identify how the network was attacked and what the attacker executed.

## Aim/Objectives

Students begin delving into the processes of securing the infrastructure of an organization. Students learn the basics of intrusion detection and intrusion prevention technologies as well as other tools that can help them in developing a secure infrastructure in the organization.

## Learning Outcomes

By the end of this week the students should be able to:

- Identify the three parts of a network: end-devices, intermediary devices and media
- Understand how routers can forward packets towards the destination using IP addresses
- Understand how switches can direct frames from one port to another based on information stored in the CAM table
- Recognize the different types of media used in network communication such as copper cabling, fire optic cabling and wireless communication
- Recognize various security devices and services such as firewalls, VPNs and ACLs

## Key Words

Routers	Switches	Access Points
Firewalls	VPN	CAM
ACL	IPS	IDS
SNMP	Netflow	

## Annotated Bibliography

### Basic

Chapter 7 of Principles of Information Security by Michael E. Whitman, Herbert J. Mattord

This chapter examines the use of Intrusion Prevention and Intrusion Detection Systems and other security tools that can be used to secure a network.

### Supplementary

Video Tutorial - Wireless Communications

Video Tutorial - Security Devices

## Self-Assessment Exercises

### Exercise 5.1

Examine the differences of an IPS and an IDS both in the placement of the device in the network and the capabilities of each device. Describe the advantages and disadvantages of each device.

## Recommended time for the student to work

15 hours

## NETWORK VULNERABILITY ASSESSMENT

6<sup>th</sup> Week

### Summary

Due to the proliferation of networks in our everyday life network attacks are more frequent and more disruptive. Network attacks require a more in-depth analysis which may require the use of specific networking tools. These tools may record network traffic, bandwidth usage and resource access. A network administrator needs to identify the network's normal behavior so that when something out of the ordinary happens then an alert can be generated to inform the cybersecurity expert of an attack. Two ways in which traffic can be monitored are Network Test Access Points (TAPs) and Switch Port Analyzers (SPANs). A TAP receives all network traffic while it is traversing from one networking device to another. SPANs can duplicate traffic destined for a specific port to another port that may have a packet sniffer to monitor the traffic.

### Introductory Remarks

Common monitoring tools include Wireshark, TCPdump, NetFlow and Security Information and Event Management Systems (SIEM) (Figure 10). Cybersecurity experts need to understand how to use all of the information gathered through the monitoring tools and thus knowing what the normal and abnormal behavior of the network would look like.

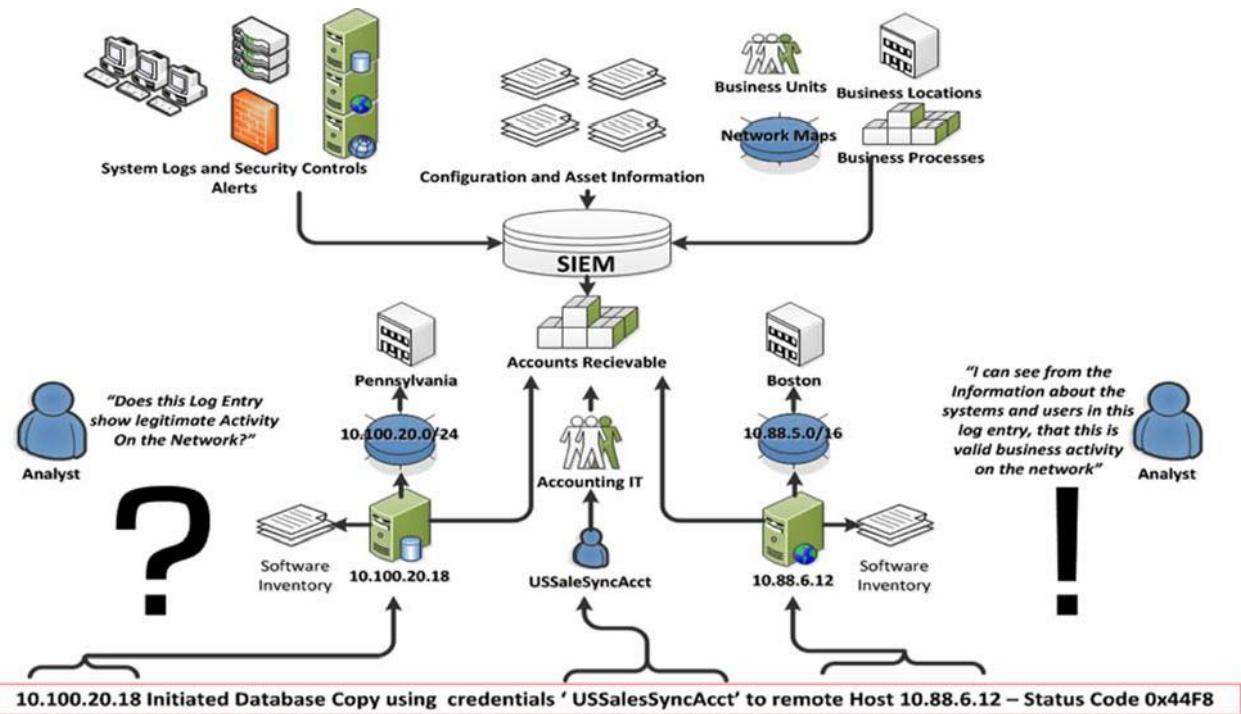


Figure 10. SIEM implementation

The Internet Protocol (IP) was developed to as a connectionless, best effort protocol with no tracking or flow management. Those tasks fall into the transport layer protocols. IP has a number of vulnerabilities such as ICMP attacks, DoS attacks, DDoS attacks, Address Spoofing attacks, Man-in-the-Middle attacks and finally Session Hijacking. ICMP attacks allows attackers to launch reconnaissance or scanning attacks to learn more information about the network they are trying to target. ICMP can also be used to launch Denial-of-Service (DoS) attacks by sending maliciously formatted packets which can crash or slow down a target device, or by overwhelming the traffic towards the target thus reducing the ability of valid users to access the target device. Distributed Denial-of-Service attacks are similar to DoS attacks but are of a more distributed nature with attack nodes being spread out on the network. DDoS attacks include amplification and reflection attacks. Amplification attacks send a message to compromised hosts and all those hosts amplify the message that then goes to the target machine. Reflection attacks receive messages that have the target machine IP address as the source and therefore they send their replies to that machine causing the target machine to slow down because it needs to process all those messages. Address spoofing attacks require the attacker to fake an address in such a way so as to gain access to data that would otherwise only go to the intended destination.

The transport layer is also vulnerable to attacks. A common TCP attack is the TCP SYN Flood attack where an attacker will send a large number of TCP SYN packets with random addresses

and the target device tries to complete the three-way handshake but is never able to do so. Other attacks include the TCP Reset attack and TCP Session Hijacking attack. UDP attacks are based on the fact that UDP traffic is unencrypted allowing an attacker to modify the data and rewrite the checksum making the modified packet seem legitimate.

Other types of attacks include the ARP Cache poisoning attack (Figure 11), DNS tunneling attacks, and DHCP Starvation and Spoofing attacks.

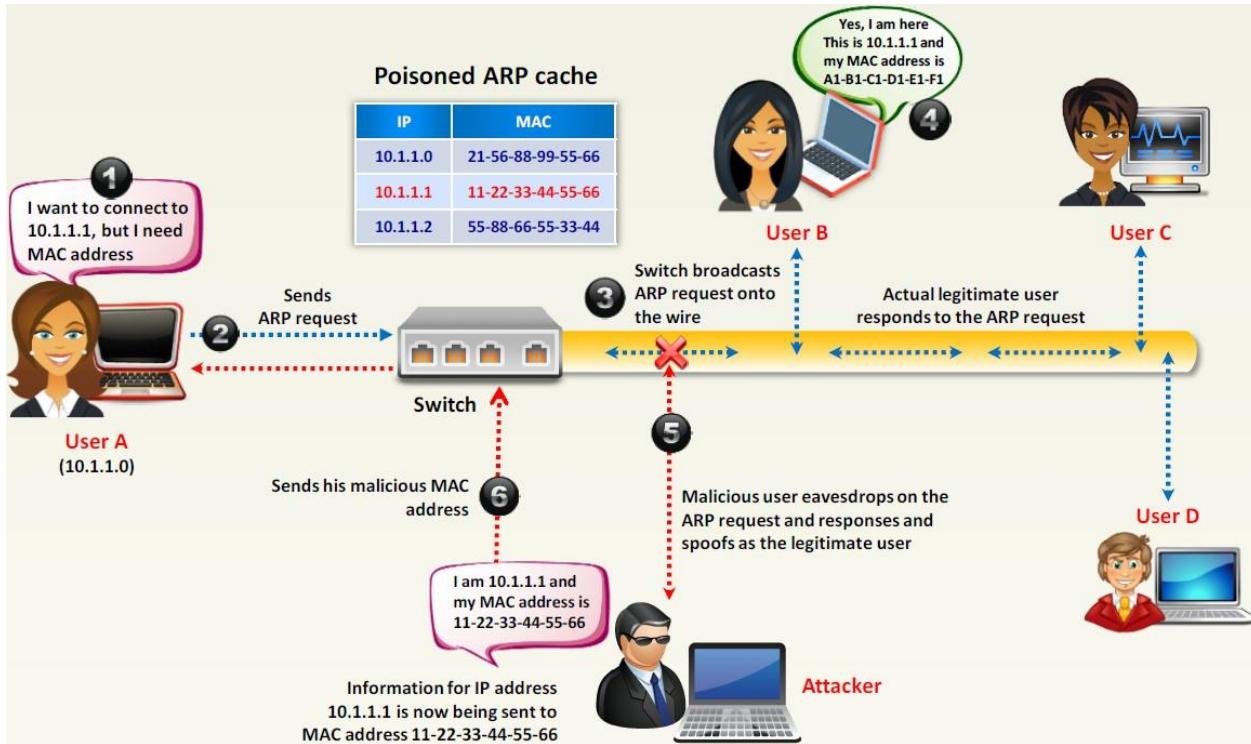


Figure 11. ARP poisoning attack

Moving to a higher abstraction layer, attackers may perform web-based attacks on HTTP and HTTPS web services through compromised web pages. Email attacks are also frequent with attachment-based attacks, email spoofing attacks, spam attacks, open mail relay server attacks and homoglyphs. Databases exposed to the web are also vulnerable to attacks through command injection, SQL injection, and Cross-Site Scripting attacks.

## Aim/Objectives

This week aims to teach students the tools that can help them assess the vulnerability of a network. Tools such as Wireshark, TCPdump, NetFlow and Security Information and Event

Management Systems (SIEM) can be utilized to monitor the network and identify possible security holes that may open the network to malicious users.

## Learning Outcomes

By the end of this week the students should be able to:

- Understand the depth of tools that threat actors can utilize to attack a device
- Identify attacks on the Internet Protocol layer
- Identify attacks on the Transport layer
- Identify attacks on the Application layer
- Use tools to monitor traffic and examine attack patterns

## Key Words

TAP	SPAN	NetFlow
SIEM	Spoofing	3-way handshake
Cache poisoning	Hijacking	

## Annotated Bibliography

### Basic

Chapter 10 of Principles of Information Security by Michael E. Whitman, Herbert J. Mattord

This chapter deals with implementing information security and describes the information security technical and non-technical aspects.

## Self-Assessment Exercises

### Exercise 6.1

Utilize the Wireshark tool to capture a log of normal traffic and try to identify the various areas that could be vulnerable to attack by a malicious user.

## Recommended time for the student to work

15 hours

# CONTINGENCY PLANNING AND NETWORKING INCIDENT RESPONSE

7<sup>th</sup> Week

## Summary

After learning how to secure a network it is important to plan ahead for emergencies. A cybersecurity expert needs to be able to follow predefined steps that can help in mitigating the impact of a threat to the network either from natural disasters or from man-made threats.

## Introductory Remarks

Contingency planning (CP) is the process of a-priori determining how to minimize the impact of threats to information security resources. A good plan needs to prepare the network for threats, react to them and ultimately recover from those threats. The four main components of CP are:

- Business Impact Analysis (BIA)
- Incident Response Plan (IR Plan)
- Disaster Recovery Plan (DR Plan)
- Business Continuity Plan (BC Plan)

Business Impact Analysis must first determine the business processes of the organization and the recovery criticality of these processes. In addition, the BIA needs to identify resource requirements and recovery priorities for system resources. After the BIA is established then the IR plan needs to be developed to document the actions that the organization needs to take while an incident is occurring. Having a Disaster Recovery plan allows the organization to be prepared for a future disaster by gaining control of the impact of an incident and quickly recovering from the incident. Finally, the BC plan ensures that critical business functions can continue if a disaster occurs. Figure x represents the steps taken from the time a disaster occurs in the organization up until the business continuity is established.

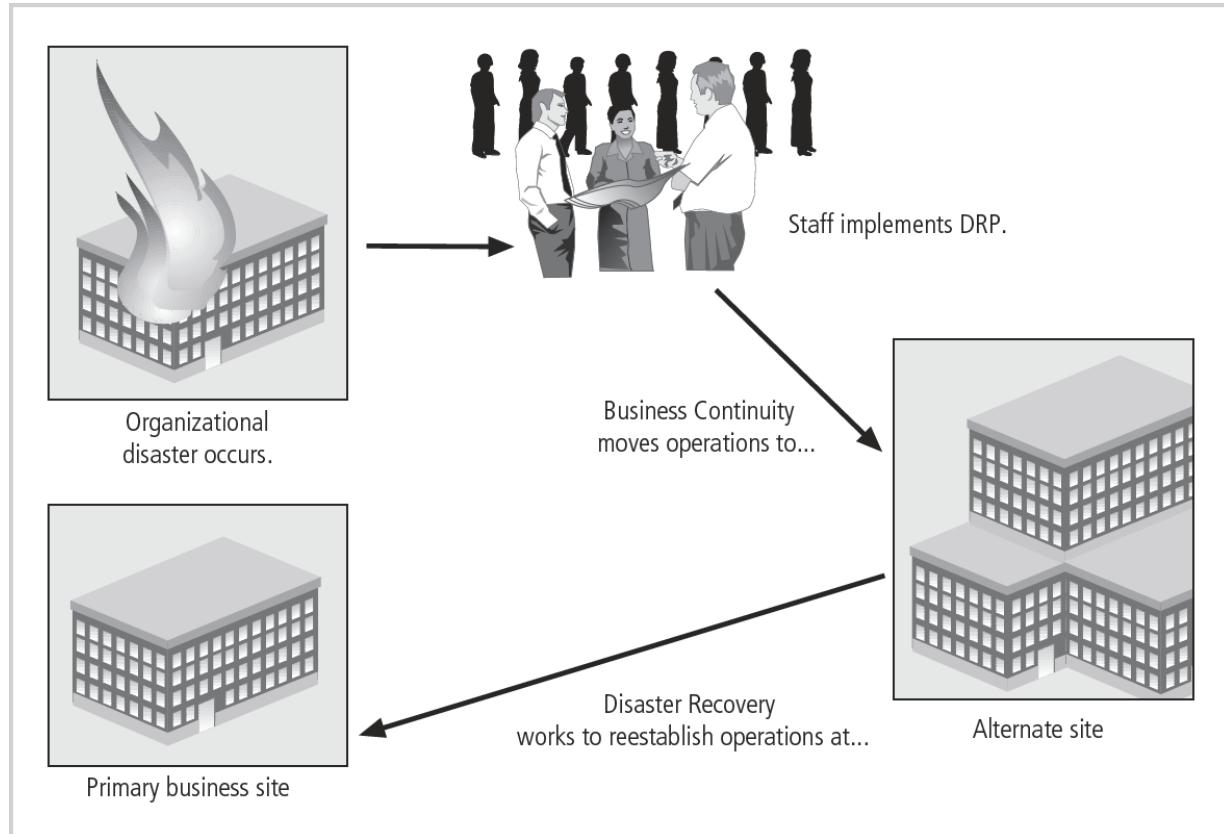


Figure 12. Move from disaster recovery to business continuity

In a networked environment a cybersecurity experts needs to determine the strategies that can help in contingency planning and business continuity for the organization with respect to networked devices and data. A cybersecurity expert needs to establish strong backup strategies and data recovery procedures to protect against threats to stored information.

Another area that helps in contingency planning is the establishment of Service Level Agreements (SLAs). SLAs are contractual documents between the organization and its vendors to ensure that the service level provided by a certain vendor is always guaranteed. An example of an SLA is a cloud service availability of 99.9 percent uptime or better.

## Aim/Objectives

The aim of this week is to introduce students to the notion of contingency planning to protect an organization from possible disasters. The students learn about the different plans that needs to

be established to have a formalized set of processes that can quickly help the organization recover from the disaster.

## Learning Outcomes

By the end of this week the students should be able to:

- Describe the importance of contingency planning and business continuity
- Identify the four pillars of contingency planning: business impact analysis, incident response plan, disaster recovery plan and business continuity
- Understand how to protect stored data and how to recover the data in case of a disaster
- Establish plans for preparing for a disaster, managing an ongoing disaster and establishing business continuity after the disaster
- Use tools such as backup and recovery solutions, and Service Level Agreement to ensure business continuity

## Key Words

Contingency	Business Impact Analysis	Incident Response
Disaster Recovery	Business Continuity	SLA
Backup	Recovery	

## Annotated Bibliography

### Basic

Chapter 6 of CISSP Guide to Security Essentials By Peter Gregory

This chapter introduces the student to contingency planning and business continuity by providing a clear understanding of all the processes involved and the tools that can help in getting business-critical functions working as soon as possible after a disaster.

## **Individual Assignment (20 points)**

Individual assignment – Perform a case-study analysis of a company and how it incorporates cybersecurity tools to protect its sensitive information. Your analysis should include an overview of the organization, the security policy, and the tools employed to protect the organization and its resources.

## **Recommended time for the student to work**

35 hours

# BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING

8<sup>th</sup> Week

## Summary

While talking about contingency planning one of the main areas is business continuity after a disaster. Disasters can be natural or man-made and both can affect the operations of a business. This makes it extremely important to establish the business continuity of the organization.

## Introductory Remarks

Natural disasters include geological, meteorological or health disasters, while man-made disasters can be labor, socio-political or even material disasters such as fires, or even power failures. All of these disasters may affect businesses by causing damage to facilities and equipment, delays to deliveries, supplies or even casualties of company employees.

Business Continuity (BCP) and Disaster Recovery (DRP) plans support the Availability of data in the CIA security pillar. BCP ensures that critical operations of the organization can continue working while DRP ensures that systems are assessed, repaired and eventually restored if they were damaged during a disaster. Through BCP and DRP, businesses can reduce the risk associated with disasters, can improve processes, organizational maturity, availability and reliability and can also gain a marketplace advantage.

In order for an organization to reduce the impact of a disaster it needs to ensure that the equipment can withstand disasters. Organizations need to setup better fire detection and suppression and contingency plans to ensure that the critical operations are up and running in the shortest period.

The first part of building a plan is performing a Business Impact Assessment. In this assessment the cybersecurity expert needs to survey all the critical processes that need to be protected. The expert needs to perform threat and risk analyses and also develop different metrics that can help in establishing a baseline of operations. Metrics include the Maximum Tolerable Downtime (MTD) for each business process and the measurable costs of each process downtime. All these information can help in determining the criticality analysis. In the criticality analysis processes are

ranked based on certain criteria and the most critical processes are the ones that most of the planning will occur. Business continuity and Disaster recovery plans are established for the most critical processes and then staff is trained in the operation of the contingency plans.

## Aim/Objectives

Cybersecurity experts needs to be able to identify the most critical processes of the organization and then develop business continuity and disaster recovery plans to make sure that the organization can survive a disaster. In this week students learn how to measure the criticality of processes and how to develop plans and train staff to handle the disasters.

## Learning Outcomes

By the end of this week the students should be able to:

- Identify various types of natural and man-made disasters
- Establish a business continuity plan
- Implement a disaster recovery plan
- Classify business processes based on their criticality measure

## Key Words

BCP	DRP	MTD
CIA	Mitigation	Downtime
Metrics	Criticality	

## Annotated Bibliography

### Basic

Chapter 4 of CISSP Guide to Security Essentials By Peter Gregory

This chapter introduces the student to business continuity and disaster recovery planning. The chapter discusses ways of measuring the criticality of processes and how to protect the most critical processes in an organization.

## **Individual Assignment (20 points)**

Individual assignment – Identify one cybersecurity breach that has occurred in the past five years and then after examining the contingency and disaster recovery plans write a new disaster recovery plan that would be better suited than the one deployed in the event. In the end discuss the changes in the plans and how these can help mitigate the disaster in a better way.

## **Recommended time for the student to work**

15 hours

# CYBERSECURITY AND IT LAW

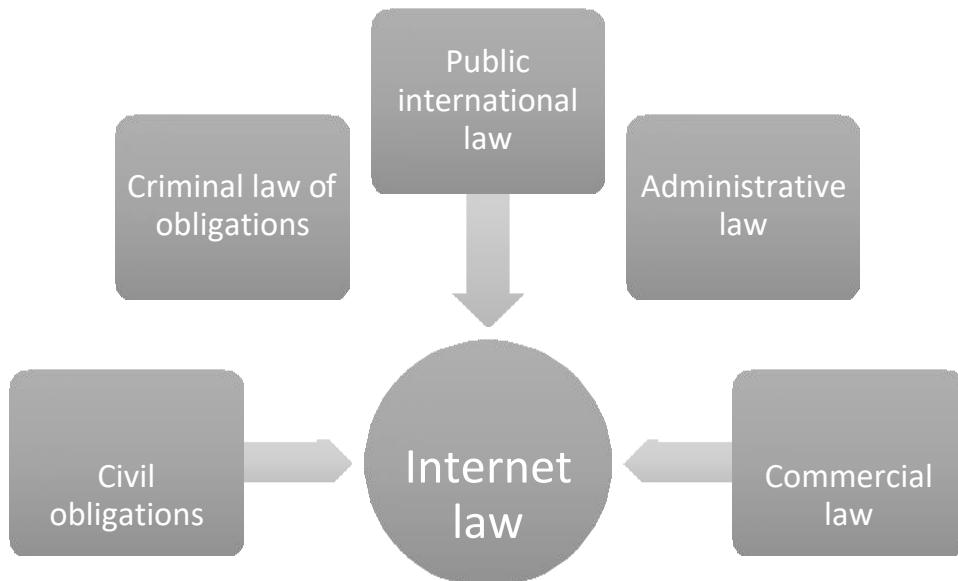
9<sup>th</sup> Week

## Summary

One of the biggest concerns of a cybersecurity expert is the integration of cybersecurity and the applicable law that governs and protects the people and the organization. The various parts that are involved in IT law include Software licensing, Data privacy and security, Electronic signatures, Legal and regulatory risks, cyberattacks, digital forensics, liability issues, trust.

## Introductory Remarks

Cybersecurity experts need to be able to secure the organization's sensitive data and ensure that the data has not been altered or deleted without prior authentication. Users need to use electronic signatures to ensure the non-repudiation of the document. Using e-signatures one can ensure that the person that signed it approves of the information contained within the document and that the context has not been altered without the knowledge of the signer.



A cyber security expert must also be up to date with any legal and regulatory issues that may be involved in the operations of the organization. Experts must be able to protect the personal data

of users such as the IP address of the devices as well as any communication and surveillance that may occur within the company. Other areas that need to be examined are cybercrime legal frameworks, copyright law enforcement, judiciary issues and criminal internet law.

Currently the General Data Protection Regulation (GDPR) is one of the most important directives with regards to personal data protection. When a processor such as a legal person, a public authority, and agency or any other body processes personal data then the controller of that data is liable to the regulation of the protection of the data. Personal data means any information that relates to an identified or identifiable natural person. The regulation may not apply in cases of national security, defense, personal activities, open access or pseudoanonymization. A video camera for example that is used within a household is legal but if it points outside and records a public space then that is a violation of the directive.

Another major cybersecurity certification that is needed by a lot of large companies is the ISO/IEC 27000 - Information security management systems. ISO/IEC 27000 defines a group of standards that help organizations in designing and implementing a secure information asset infrastructure and procedures.

## Aim/Objectives

The aim of this chapter is to introduce the student to the legal framework that exists to protect the persons and the organizations. Students learn about personal data protection laws, software copyright laws and other issues that may impact the operation of an organization.

## Learning Outcomes

By the end of this week the students should be able to:

- Identify applicable cybersecurity and IT laws
- Understand software licensing issues
- Identify data protection laws and how they are enforced
- Discuss legal and regulatory risks, liability issues and trust issues

## Key Words

IT law	Cybercrime	Software licensing
Data protection	e-signature	Forensics
Liability	Trust	

## Annotated Bibliography

### Basic

Chapter 2 of Management of Information Security by Michael E. Whitman, Herbert J. Mattord

This chapter discusses the laws and ethics related to IT and the compliance with accordance to these laws.

## Activity (5 points)

Select one of the European Cybersecurity Laws and analyze them taking into considerations what they are trying to protect, the methodology of the law and how it safeguards persons or resources. You should also present possible case studies of the law and how it was implemented.

## Recommended time for the student to work

20 hours

## ETHICS

10<sup>th</sup> Week

### Summary

Ethics is another aspect of protection that needs to be identified and regulated in an organization. An organization may gather personal data so that it can make better decisions, but the use of such data may impede the privacy of a person.

There are a number of privacy laws that aim in protecting the individuals such as the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA).

### Introductory Remarks

HIPPA is an important privacy law in that it improves the portability of insurance coverage, and reduces fraud, waste and abuse of health insurance and healthcare delivery. FERPA protects students from disclosing educational records without prior consent by the student but also provides the parents with rights to access their child's educational record. In a similar way, COPPA allows parents control over the collection, use and disclosure of their child's personal information on the Internet.

One of the areas that data privacy may be impeached is in electronic surveillance. The Omnibus Crime Control and Safe Streets Act, also known as the wiretap act allows state and federal law enforcement officials to wiretap and eavesdrop if a warrant is issued.

Some of the key privacy and anonymity issues include camera surveillance, vehicle event data recorder or stalking apps. Camera surveillance is used to deter crime and terrorist activities but citizens have criticized this as a violation of civil liberties. Vehicle event data recorder (EDR) records a few seconds of video footage before and after an accident occurs that is strong enough to deploy the airbags of the car. Finally, stalking apps are applications loaded onto the telephone of a user to monitor the location and other activities on the phone. It is illegal to install software on a person's phone without their consent.

## Aim/Objectives

Students learn about various laws that are in place for the protection of people and also learn about the ethical issues that are associated with the collection and processing of personal data.

## Learning Outcomes

By the end of this week the students should be able to:

- Define laws that are in place to protect privacy of an individual
- Identify ethical concerns related to the collection of data in various occasions

## Key Words

HIPAA	FERPA	COPPA
Wiretap act	ECPA	GDPR

## Annotated Bibliography

### Basic

Chapter 6 of CISSP Guide to Security Essentials By Peter Gregory

A chapter describing the legal, regulations, investigations and compliance issues related to Information Security and also a description of the (ISC)<sup>2</sup> Code of ethics.

## Recommended time for the student to work

15 hours

## INVITED LECTURES

11<sup>th</sup> Week

### Summary

In an effort to help students learn about the status of Cybersecurity in Cyprus, the course will endeavor to invite high caliber individuals with a proven background in Cybersecurity. Such individuals can help students understand the area they are studying and may provide important input on their studies and future as cybersecurity experts.

### Introductory Remarks

One such person is the Head of Cyprus Policy Cybersecurity Crime Unit.

### Aims/Objectives

In this week the aim of the course is to introduce students to experts in the field of cybersecurity in Cyprus and learn more about real life experiences and receive advise from such notable personalities.

### Learning Outcomes

By the end of this week the students should be able to:

- Understand the status of cybersecurity in Cyprus
- Identify personalities in Cyprus that are involved in cybersecurity
- Learn more about the area from leading experts

### Group Assignment (20 points)

Students should form groups and develop a security policy for a fictional company taking into consideration all the information learned in this course. The security policy should take into account the effective laws and ethical considerations of the organization and specify the tools that will be used to enforce the security policy in the organization.

## **Recommended time for the student to work**

35 hours

## INVITED LECTURES

12<sup>th</sup> & 13<sup>th</sup> Week

### Summary

In an effort to help students learn about the status of Cybersecurity in Cyprus, the course will endeavor to invite high caliber individuals with a proven background in Cybersecurity. Such individuals can help students understand the area they are studying and may provide important input on their studies and future as cybersecurity experts.

One such person is the Head of Cyprus Policy Cybersecurity Crime Unit.

### Aim/Objectives

In this week the aim of the course is to introduce students to experts in the field of cybersecurity in Cyprus and learn more about real life experiences and receive advise from such notable personalities.

### Learning Outcomes

By the end of this week the students should be able to:

- Understand the status of cybersecurity in Cyprus
- Identify personalities in Cyprus that are involved in cybersecurity
- Learn more about the area from leading experts

### Recommended time for the student to work

30 hours (15 hours/week)

## **REVISION AND FINAL EXAMINATION**

The final exam will contain multiple choice questions and open-ended questions that will examine the student's understanding of the various topics discussed in this course. The questions will determine if the student was able to grasp the concepts presented and if the student can apply those concepts in different scenarios.

### **Recommended time for the student to work**

40 hours

**Date/Time of Final Exam: TBD**



**FORM: 200.1.3**

## **STUDY GUIDE**

**Course: CYS603 - Communications and Network Security**

## Course Information

<b>Institution</b>	European University Cyprus		
<b>Programme of Study</b>	Cybersecurity (MSc)		
<b>Course unit</b>	CYS603	Communications and Network Security	
<b>Level</b>	<i>Undergraduate</i>	<i>Postgraduate</i>	
		<i>Master</i>	<i>PhD</i>
		√	
<b>Language of Instruction</b>	English		
<b>Teaching Methodology</b>	Distance Learning		
<b>Course Type</b>	<i>Compulsory</i>		<i>Optional</i>
	√		
<b>Number of Group Consultation Meetings/ Web-Conferences/ Lectures</b>	<b>Total</b>	<b>Face to Face</b>	<b>Web-Conferences</b>
	14	1	13
<b>Number of Activities/ Assignments</b>	4		
<b>Final Assessment</b>	<i>Assignments</i>		<i>Final Examinations</i>
	50 %		50 %
<b>Number of Credits (ECTS)</b>	10		

<b>Study Guide drafted by</b>	Dr George Kioumourtzis
<b>Editing and final approval of Study Guide by</b>	Dr Yianna Danidou

## COURSE CONTENTS

		Page
	Introductory Notes	4
	First Group Consultation Meeting	5
1	Week 1 – Introduction to Computer Networking	7
2	Week 2 - Computer Network Security Fundamentals	13
3	Week 3 - Security in Wireless Networks and Devices	19
4	Week 4 - Cyber Crimes and Hackers	26
5	Week 5 - Computer Network Security Protocols	31
6	Week 6 – Authentication	36
7	Week 7 - Malicious Software	41
8	Week 8 - Computer Network Vulnerabilities	48
9	Week 9 - Scripting and Security	55
10	Week 10 - Cloud Computing Technology and security	60
11	Week 11 – Internet of Things (IoT) security	65
12	Week 12 – Intrusion Detection and Prevention	72
13	Week 13 - Protecting measures - Firewalls	81
14	Revision and Final Examination	86
	Indicative answers to Self-Assessment Exercises	87

## INTRODUCTORY NOTES

The ‘Communications and Network Security’ course is a fundamental course with a special position among the other courses in the Cybersecurity master program.

The Study Guide, a tool that is necessary and useful for students, especially in those cases where the training material is not written with the methodology of open and distance learning, encourages and facilitates the study and understanding of the issues addressed by the thematic module. In addition, through self-assessment exercises, it stimulates and encourages work at home, provides incentives for further study, and contributes to the development of your critical thinking. The Study Guide is structured on a weekly basis and includes a summary and some very brief introductory remarks, purpose and expected outcome, key words - basic concepts, annotated literature, recommended student's time, self-assessment exercises, critical thinking and case studies, with indicative answers in the end, aiming at a more meaningful understanding of the content, terms and concepts that each unit deals with. The recommended weekly working time includes, apart from the study, the follow-up of teleconferences and OSS, bibliography search, two weekly exercises, etc. Although it is self-evident, it should be noted that the study guide does not substitute to the minimum the educational material on the platform that the student needs to read carefully and assimilate in order to be able to meet the requirements of the program and to successfully complete the thematic module them.

## 1st GROUP CONSULTATION MEETING

### Programme Presentation

Leading companies today are rethinking the role of information security in their organizations. They realize that in a digital world, cybersecurity is the key to safeguarding their most precious assets—intellectual property, customer information, financial data, and employee records, among others. But far more than a defensive measure, companies also know that cybersecurity can better position their organization with business partners, customers, investors, and other stakeholders.

The European cybersecurity market is about 25% (i.e. about €17bln) of the world market (estimated at €70bln in 2015), with an average yearly growth slightly larger than 6%, when the world market is growing at about 10%/year. Recent study compiled by Europe's cybersecurity industry leaders pointed out that Europe is in danger of falling behind in the international digital economy field.

The Master in Cybersecurity is a cutting-edge program, designed for those wishing to develop a career as a cyber-security professional, or to take a leading technical or managerial role in an organization critically dependent upon data and information communication technology. Students will develop an advanced knowledge of information security and an awareness of the context in which information security operates in terms of safety, environmental, social and economic aspects. They will gain a wide range of intellectual, practical and transferable skills, enabling them to develop a flexible professional career in IT.

Key elements of this postgraduate degree are: *the real life experience* given by the opportunity to apply their theoretical knowledge through specialized virtual and remote security laboratories in which they will be able to carry out activities such as reconnaissance, network scanning and exploitation exercises, and investigate the usage and behavior of security systems such as Intrusion Detection and Prevention Systems thus becoming confident in the practical application of the latest tools; the high-level insight that will enhance student's ability to research and design creative cyber security solutions to address business problems; hands-on skills through experimentation with security techniques, cryptographic algorithms, cyber forensics building an ethical hacking environment; and flexibility since students will also be able to choose either the completion of a Master thesis or to complete a Research methods course and two elective courses.

Students undertake modules to the value of 90 ECTS credits.

## COURSE PRESENTATION THROUGH THE STUDY GUIDE

This course is compulsory with a special position among the other courses in the Cybersecurity master program. This course takes a detailed look at the network security. The main objective of this course is to understand the various network technologies, how these technologies expose security vulnerabilities and what are the security measures and configurations to be taken to increase security. We start our study with a review of main network technologies and the fundamental knowledge for network security. Wireless technologies will be discussed and the needed configurations that are required for maximum security will be described. The discovery of network vulnerabilities across the entire network by using security hacking techniques and vulnerability scanning are analysed.

We will overview how cybercrime is evolving and what are currently the cyber-attacks with the highest impact. We will study the most important secure protocols in the TCP-/IP protocol stack. Then we will discuss the authentication methods and how they are used to increase security. Next, we will see the various categories of malicious software (malware).

We will investigate the network and computer vulnerabilities in week eight in which you will be run a practical assignment in your home network to get a deeper understanding on the topic. Next, we will see how scripting enabled the rapid growth of the Internet but introduced a number of security concerns. In weeks tenth and eleventh will discuss the security concerns in emerging technologies such as Cloud Computing and Internet of Things (IoT).

We will also discuss what are the protective measures that system and network administrators put in place to harden the network from internal and external threats. You will get a deeper understanding on how we can monitor the network and identify malware and other threats by using packet inspection tools such as Wireshark. Finally, the various types of firewalls that are available will be explained and analysed.

Upon successful completion of this course students should be able to:

- Describe the underlying principles of networking layers, architecture, topologies, protocol stacks, and separation of duties.
- Explain the basic types of networking device, both logical and physical.
- Analyse networking methods and applications in practical systems.
- Classify and describe different types of wired network attacks.
- Classify and describe different types of wireless network attacks.
- Describe and evaluate methods and devices used to protect networks.

## Recommended time for the student to work

Approximately 5 hours for the study guide

# INTRODUCTION TO COMPUTER NETWORKING

1<sup>st</sup> Week

## Summary

We will start our course this week with a short refresh of computer networking technologies. We will revisit the both wired and wireless technologies and the TCP/IP protocol stack.

## Introductory Remarks

Today's Internet is arguably the largest engineered system ever created by mankind, with hundreds of millions of connected computers, communication links, and switches; with billions of users who connect via laptops, tablets, and smartphones; and with an array of new Internet-connected devices such as sensors, Web cams, game consoles, picture frames, and even washing machines.

Given that the Internet is so large and has so many diverse components and uses, is there any hope of understanding how it works? Are there guiding principles and structure that can provide a foundation for understanding such an amazingly large and complex system?

And if so, is it possible that it actually could be both interesting and fun to learn about computer networks? Fortunately, the answers to all of these questions is a resounding YES! Indeed, the aim of this week is to provide you with a modern introduction to the dynamic field of computer networking, giving you the principles and practical insights, you'll need to understand not only today's networks, but tomorrow's as well.

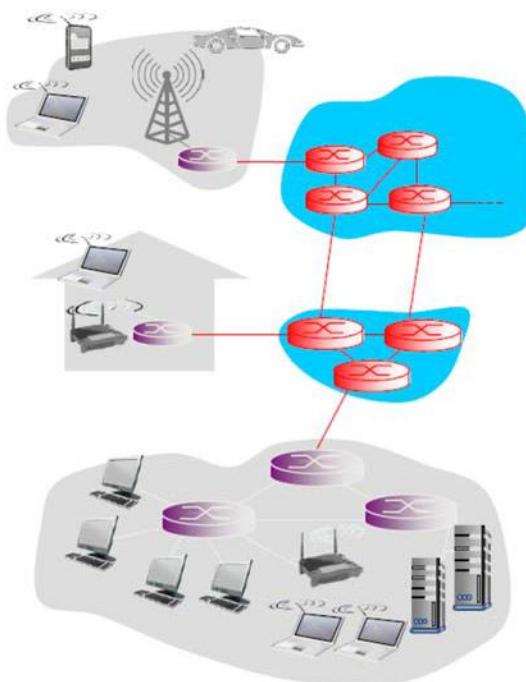


Figure 1 – Core network

We will present in this first week a broad overview of computer networking and the Internet. Our goal here is to paint a broad picture and see the forest through the trees. We'll cover a lot of ground in this introductory week and discuss a lot of the pieces of a computer network, without losing sight of the big picture.

We'll structure our overview of computer networks in this week as follows. After introducing some basic terminology and concepts, we'll first examine the basic terms and technologies in data networking. We will investigate the **OSI** and **TCP/IP layer stack** and how the various network components are communicating with the use of protocols.

We will review the various network technologies such as wired and wireless networks. We will understand the difference between wireless and mobility and how mobility affects the network performance. We'll understand that the Internet is a “**network of networks**”, and we'll learn how these networks connect with each other

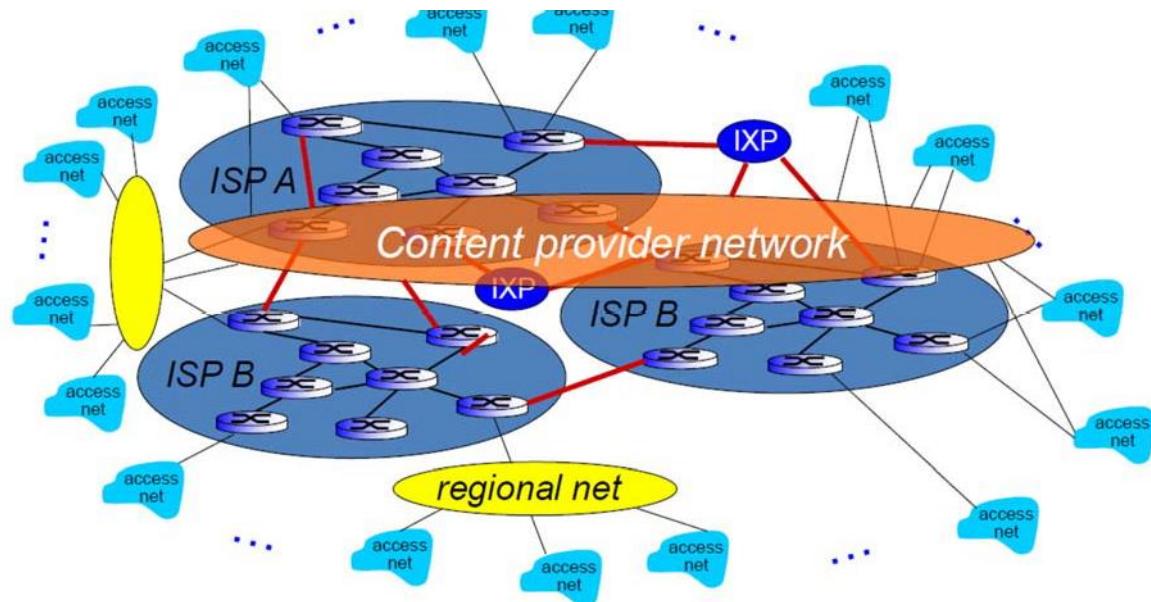
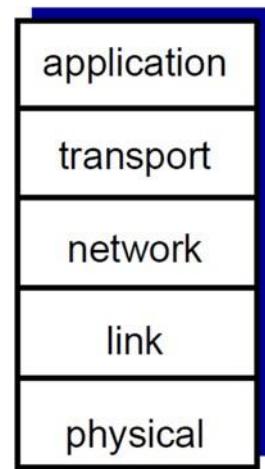


Figure 2 – Internet: Network of networks

In wireless networking We can identify the following elements:

- **Wireless hosts.** As in the case of wired networks, hosts are the end-system devices that run applications. A wireless host might be a laptop, palmtop, smartphone, or desktop computer. The hosts themselves may or may not be mobile.
- **Wireless links.** A host connects to a base station (defined below) or to another wireless host through a wireless communication link. Different wireless link technologies have different transmission rates and can transmit over different distances.
- **Base station.** The base station is a key part of the wireless network infrastructure. Unlike the wireless host and wireless link, a base station has no obvious counterpart in a wired network. A base station is responsible for sending and receiving data (e.g., packets) to and from a wireless host that is associated with that base station.

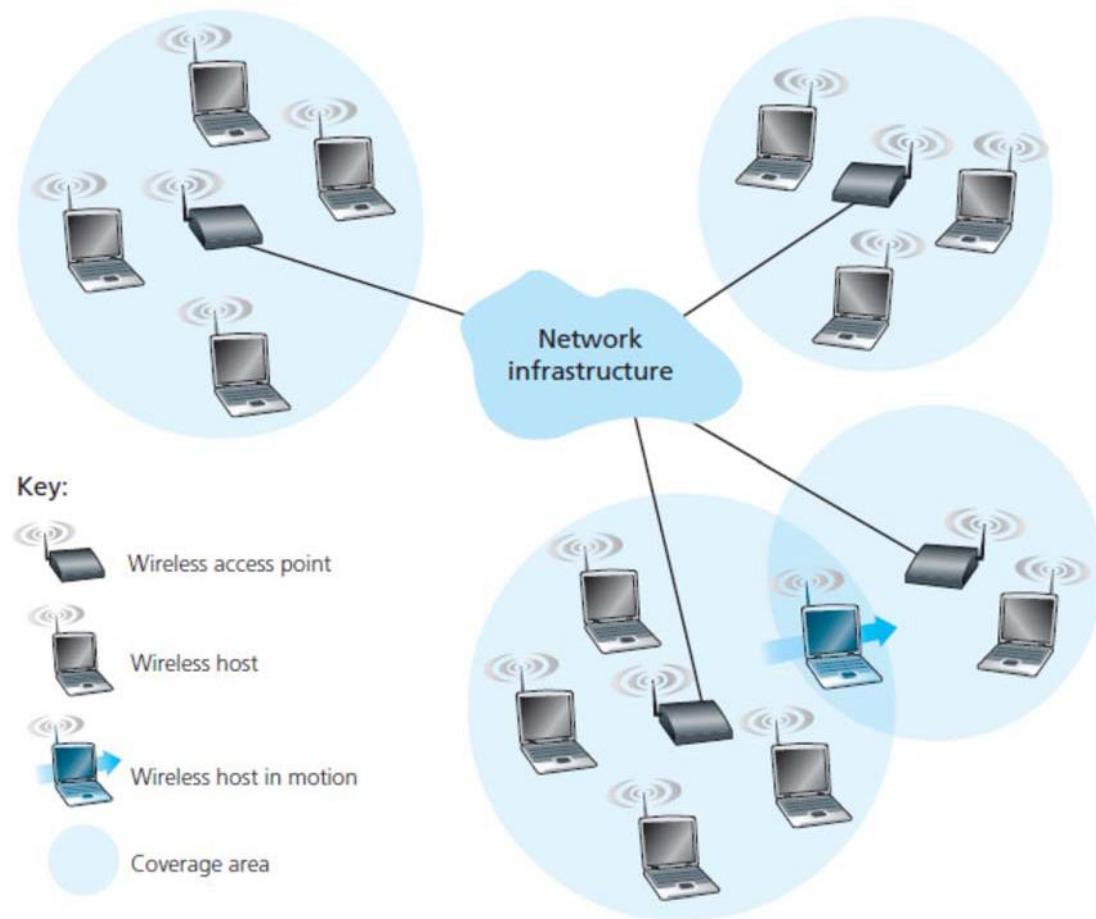


Figure 3 – Elements of a wireless network.

## Aim/Objectives

The scope of this week is to introduce the students with the fundamental knowledge in computer networking, the understanding of the TCP/IP models and the different types of networking areas. Today's networking and internet are based on the communication of the various protocols in the TCP/IP stack via well-defined protocols. Layered approach in data networks provide the necessary abstraction level so that the various network components can communicate in a structured, manageable and efficient manner. One fundamental principle for the today's internet structure is related to packet encapsulation mechanisms. Wireless and mobility are two terms that are used interchangeably. The students will understand that the main challenges in today's wireless communications are related to mobility as hosts moving from one location to another and they need to keep their connectivity during the handover procedure from one access point to another. Students will also need to understand the different types of wireless networks and the ongoing efforts to merge all wireless networks.

## Learning Outcomes

Upon successful completion of this course, students should be able to:

- State and identify concepts relating to data communications, communication protocols and layered protocol architectures.
- State and interpret protocol communication standards like OSI/RM and TCP/IP as used in computer networking and internetworking.
- Describe different network topologies, physical components and their characteristics.
- Recognize and explain data transmission fundamentals and types of media (both wired and wireless).
- Identify computer network models.
- Define, explain and exemplify concepts related to Local Area Networks (both wired and wireless), their topologies and protocols, their types and transmission technologies.

## Key Words

TCP/IP	encapsulation	Wireless networks
router	IPv6	TCP Congestion control
switch	protocols	Mobile networks

## Annotated Bibliography

## **Basic**

Computer Networking A Top-Down Approach, 6th Edition, Kurose, Ross, Available online at:

[https://www.bau.edu.jo/UserPortal/UserProfile/PostsAttach/10617\\_1870\\_1.pdf](https://www.bau.edu.jo/UserPortal/UserProfile/PostsAttach/10617_1870_1.pdf)

This first week is based on the above eBook that is freely available on line and it is offered to students for free. There are two unique characteristics in this book—its top-down approach and its focus on the Internet. The field of networking is now mature enough that a number of fundamentally important issues can be identified. For example, in the transport layer, the fundamental issues include reliable communication over an unreliable network layer, connection establishment/ teardown and handshaking, congestion and flow control, and multiplexing. Two fundamentally important network-layer issues are determining “good” paths between two routers and interconnecting a large number of heterogeneous networks. In the link layer, a fundamental problem is sharing a multiple access channel.

This text identifies fundamental networking issues and studies approaches towards addressing these issues. The student learning these principles will gain knowledge with a long “shelf life”—long after today’s network standards and protocols have become obsolete, the principles they embody will remain important and relevant. The combination of using the Internet to get the student’s foot in the door and then emphasizing fundamental issues and solution approaches will allow the student to quickly understand just about any networking technology.

The student is not requested to study the whole book that is not practical. As this week is a refreshment of existing knowledge in computer network it is enough for the student to read this week presentations and concentrate on the high-level concepts. In a future second time or any other time the student can revisit the book for more detailed information on specific technologies and protocols.

## **Supplementary**

Power point presentation slides available in the platform

Video: [The evolution of the internet | Tech Histories](#)

Video: [UDP and TCP: Comparison of Transport Protocols](#)

Video: [Wireless Networking](#)

## **Suggestions for further reading**

[The evolution of Internet](#)

This article gives elaborates on the evolution of the Internet and how is turning from a decentralised architecture to a centralised one.

#### [A brief history of the internet](#)

This article gives a brief history on the evolution of the Internet.

### **Self-Assessment Exercises**

#### **Exercise 1.1**

List some of the most important protocols in the TCP/IP layer stack

#### **Exercise 1.2**

Define the elements that constitute a wireless network

### **Recommended time for the student to work**

15 hours

# COMPUTER NETWORK SECURITY FUNDAMENTALS

2<sup>nd</sup> Week

## Summary

In this second week, we will discuss about the fundamentals of networking security. We will see on which way can we guarantee security provided that proper protection mechanisms are in place.

## Introductory Remarks

Security is a continuous process of protecting an object from unauthorized access. It is as state of being or feeling protected from harm. That object in that state may be a person, an organization such as a business, or property such as a computer system or a file. Security comes from secure which means, according to Webster Dictionary, a state of being free from care, anxiety, or fear [1]. An object can be in a physical state of security or a theoretical state of security. In a physical state, a facility is secure if it is protected by a barrier like a fence, has secure areas both inside and outside, and can resist penetration by intruders. This state of security can be guaranteed if the following four protection mechanisms are in place: deterrence, prevention, detection, and response [1, 2].

- **Deterrence** is usually the first line of defense against intruders who may try to gain access. It works by creating an atmosphere intended to frighten intruders. Sometimes this may involve warnings of severe consequences if security is breached.
- **Prevention** is the process of trying to stop intruders from gaining access to the resources of the system. Barriers include firewalls, demilitarized zones (DMZs), and the use of access items like keys, access cards, biometrics, and others to allow only authorized users to use and access a facility.
- **Detection** occurs when the intruder has succeeded or is in the process of gaining access to the system. Signals from the detection process include alerts to the existence of an intruder. Sometimes, these alerts can be real time or stored for further analysis by the security personnel.
- **Response** is an aftereffect mechanism that tries to respond to the failure of the first three mechanisms. It works by trying to stop and/or prevent future damage or access to a facility.



Figure 4 – Cybersecurity protection mechanisms.

The areas outside the protected system can be secured by wire and wall fencing, mounted noise or vibration sensors, security lighting, closed-circuit television (CCTV), buried seismic sensors, or different photoelectric and microwave systems [1]. Inside the system, security can be enhanced by using electronic barriers such as firewalls and passwords.

Digital barriers—commonly known as firewalls, discussed in detail in Week 4—can be used. Firewalls are hardware or software tools used to isolate the sensitive portions of an information system facility from the outside world and limit the potential damage by a malicious intruder.

A theoretical state of security, commonly known as pseudosecurity or security through obscurity (STO), is a false hope of security. Many believe that an object can be secured as long as nobody outside the core implementation group has knowledge about its existence. This security is often referred to as “bunk mentality” security.

This is virtual security in the sense that it is not physically implemented like building walls, issuing passwords, or putting up a firewall, but it is effectively based solely on a philosophy. The philosophy itself relies on a need-to-know basis, implying that a person is not dangerous as long as that person doesn't have knowledge that could affect the security of the system like a network, for example.

In real systems where this security philosophy is used, security is assured through a presumption that only those with responsibility and who are trustworthy can use the system and nobody else needs to know. So, in effect, the philosophy is based on the trust of those involved assuming that they will never leave. If they do, then that means the end of security for that system.

Although its usefulness has declined as the computing environment has changed to large open systems, new networking programming, and network protocols, and as the computing power available to the average person has increased, the philosophy is in fact still favored by many agencies, including the military, many government agencies, and private businesses.

In either security state, many objects can be thought of as being secure if such a state, a condition, or a process is afforded to them. Because there are many of these objects, we are going to focus on the security of a few of these object models. These will be a computer, a computer network, and information.

## Aim/Objectives

The scope of this week is to introduce the student with the fundamental knowledge of network security. However, before we talk about network security, the students need to understand the concept of security and its main elements. That is true as students even computer scientists do not always have any previous background in security, which is a different discipline. Therefore, it is essential for the student to grasp the meaning of security and how the main security principles apply in network security. At the European level, the European Union works on a number of fronts to promote cyber resilience across the European Union.

In this week, the students will be also able to identify the various elements related to computer, network and information security. The main pillars of the security requirements triage that is confidentiality, integrity and availability will be analysed and the students will be able to apply this knowledge in the next weeks when working on more technical issues in network security.

In addition to this the students will be introduced with the concept of security standards and how these standards can be applied to increase the resilience and the security in data networks.

## Learning Outcomes

Upon successful completion of this course, students should be able to:

- State and identify the concept of security.

- Identify the concepts of computer security, network security and information security.
- Distinguish between computer, network and information security
- State the importance of security standards
- Understand the importance of best practices.
- Make use of the required resources for securing the computer networks.

## Key Words

Computer security	Network security	Information security
Access control	Authentication	Confidentiality
Integrity	Nonrepudiation	Security standards

## Annotated Bibliography

### Basic

Guide to Computer Network Security, 4th Edition, Joseph Migga Kizza, 2017, DOI 10.1007/978-3-319-55606-2

The book is venturing into and exposing all sorts of known security problems, vulnerabilities, and dangers likely to be encountered by the users of these devices. In its own way, it is a pathfinder as it initiates a conversation toward developing better tools, algorithms, protocols, and best practices that will enhance the security of systems in the public commons, private and enterprise offices, and living rooms and bedrooms where these devices are used. It does this comprehensively in six parts and 26 chapters. Part I gives the reader an understanding of the working of and the security situation of the traditional computer networks. Part II builds on this knowledge and exposes the reader to the prevailing security situation based on a constant security threat. It surveys several security threats. Part III, the largest, forms the core of the guide and presents to the reader most of the tools, algorithms, best practices, and solutions that are currently in use. Part IV goes beyond the traditional computer network as we used to know it to cover new systems and technologies that have seamlessly and stealthily extended the boundaries of the traditional computer network. Systems and other emerging technologies including virtualization, cloud computing, and mobile systems are introduced and discussed. A new Part V ventures into wireless and other technologies creeping into the last mile creating a new security quagmire in the home computing environment and the growing home hotspots. Part VI, the last part, consists of projects.

Available to all EUC students via the <https://www.openathens.net/> service.

Related link: <https://www.springer.com/gp/book/9783319556055>

This week is based on the above eBook and more specifically in Chapter 2 pages 41-57. This chapter provides a simplified approach and presents the main concepts in computer security.

### **Supplementary**

Power point presentation slides available in the platform

### **Suggestions for further reading**

1. Standardisation activities take place in international, national, and industry-based forums. Within Europe the three European Standards Organizations, CEN, CENELEC, and ETSI cooperate to try and minimize the amount of duplication of standards. Read more in ENISA [Cybersecurity standards and certification report](#).
2. Certification, as a conformity assessment activity against specified requirements, is performed and attested by a third party. These requirements are derived from technical standards or legislation, as in the case of certification under GDPR, where the secondary EU legislation provides the normative framework as a basis for the assessment requirements. The outcome of a successful certification (process) is a certificate (thus a document), and/or a seal, that attests that the applicant organisation meets the requirements (substantive and procedural) specified in the certification scheme and provided in technical standards or legislation. In the near future, it is also possible that such requirements, originating from GDPR provisions, are also provided in technical standards. Read more in ENISA [Recommendations on European Data Protection Certification](#) report.

## **Self-Assessment Exercises**

### **Exercise 2.1**

What are the four protection mechanisms in place to guarantee security in computer networks?

### **Exercise 2.2**

What is the meaning of Information security?

## **Recommended time for the student to work**

15 hours



## SECURITY IN WIRELESS NETWORKS AND DEVICES

3<sup>rd</sup> Week

### Summary

This week we will discuss wireless technologies and networking and we will focus on the security challenges in wireless networks. We will investigate the vulnerabilities in wireless networks, and the security measures we need to take to safeguard them.

### Introductory Remarks

Wireless technology is a relatively new technology that started mid in the 20th century. The rapid technological developments of the last 20 years have seen wireless technology as one of the fastest developing technologies of the communication industry. Because of its ability and potential to make us perform tasks while on the go and bring communication in areas where it would be impossible with the traditional wired communication, wireless technology has been embraced by millions. There are varying predictions all pointing to a phenomenal growth of the wireless technology and industry.

To meet these demands and expectations, comprehensive communication infrastructure based on several types of wireless network technologies has been developed. The various wireless technologies can be classified as i) Wireless PAN (Personal Area Networks), ii) Wireless LAN (Local Area Networks), iii) Wireless MAN (Metropolitan Area Networks), iv) Mobile cellular Networks, v) 4G, LTE (Long Term Evolution, and vi) 5G (proposed—rollout by 2020).

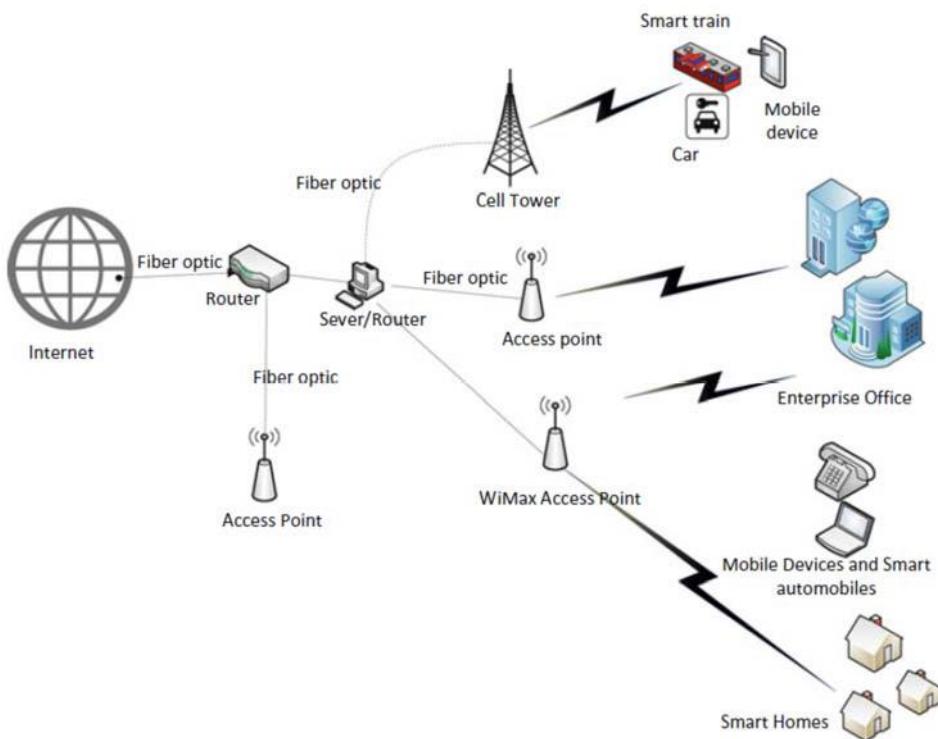


Figure 5 – A typical wireless broadband network.

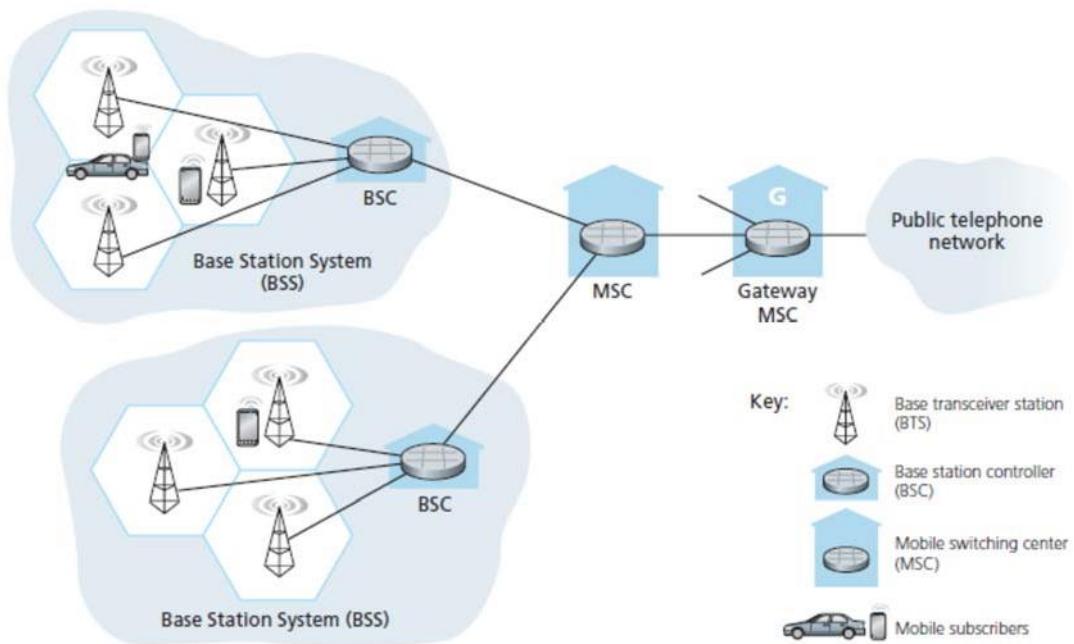


Figure 6 – Components of the GSM 2G cellular network architecture.

Security in Wi-Fi and WiMAX networks is addressed by a special working group (IEEE 802.16 Working Group) that has designed several security protocols to safeguard and protect both users and providers. The evolving security architecture consists of the following five components:

- **Security associations**: A context to maintain the security state relevant to a connection between a base station (BS) and a subscriber station (SS).
- **Certificate profile**—X.509 to identify communication parties to each other.
- **PKM authorization**—authorization protocol to distribute an authorization token to an authorized SS.
- **Privacy and key management**—a protocol to rekey the security association (SA).
- **Encryption**—payload field encryption using Data Encryption Standard (DES) algorithm in the Cipher Block Chaining (CBC) mode of operation in 802.16d, DES-CBC, and Advanced Encryption Standard-Counter with Cipher Block Chaining-Message Authentication Code (AES-CCM) in 802.16e.

In the area of mobile cellular networks, the cellular **wireless application protocol** (WAP) stack was dictated by the mobility of users and their need to have access to information services, including the Internet and the Web. WAP works with all wireless technologies such as GSM, CDMA, and TDMA and is based on Internet technologies such as XML, HTML, IP, and HTTP.

Standard	Publication year	Range	Frequency	Goals	Security
802.16	2002		10–66 GHz	Original standard, line of sight, fixed-fixed point wireless	None
802.16a	2003		2–11 GHz	Added non-line of sight extension. Now supplanted by the 802.16d variant	None
802.16d	2004		2–11 GHz	Supports fixed and nomadic access in line of sight and non-line of sight environments	3DES for authorization key (AK), DES for traffic encryption key (TEK), X.509
			10–66 GHz		
802.16e	2006		2–6 GHz	Optimized for dynamic mobile radio channels, provides support for handoffs and roaming	AES-CCM Extensible Authentication Protocol (EAP)

Table 1 - The security and functional evolution of the IEEE 802.16 standard.

However, Wireless networks are inherently insecure. This problem is compounded by the untraceable hackers who use invisible links to victimize WLANs and the increasing number of fusions between LANs and WLANs, thus adding more access points (the weak points) to the perimeters of secure networks. One can classify the security concerns in the following areas: Identity in WLANs, Lack of Access Control Mechanism, Lack of Authentication Mechanism in 802.11, Lack of a WEP Key Management Protocol, Insertion Attacks, Interception and Monitoring Wireless Traffic Attacks, Simple Network Management Protocol (SNMP) Community Words, Client-Side Security Risk, Risks Due to Installation, Jamming, Client-to-Client Attacks, Parasitic Grids.

All the above along with best practices for Wi-Fi Security will be studied. We will also conduct a number of practical exercises to investigate **Wi-Fi weaknesses** and security testing.

Security, however, in wireless networks requires a thorough understanding of the working of wireless devices and networks. In our first week we made an introduction in computer and wireless networking. However, it is strongly recommended to review the related chapters and reading materials for the student to refresh the concepts and knowledge in wireless networking.

## Aim/Objectives

The scope of this week is for the student to understand the security issues related to wireless technologies. WLAN security concerns will be presented, and the student will be familiar with the main vulnerabilities that the wireless networks expose. Our scope is not to analyse all these vulnerabilities, and the security measures we need to take to safeguard our wireless network. Best practices for wireless security will provide the student with a better understanding of what others have done and how can we get an advantage of additional measures. The student will be also provided with additional resources for reading based mainly on ENISA current publications. At the same time the student is given a number of free tools in order to obtain by his own a deeper understanding on this subject by contacting practical exercises related to Wi-Fi weaknesses and security testing.

## Learning Outcomes

Upon successful completion of this course, students should be able to:

- Identify the various types of wireless technologies
- Define the Types of Wireless Broadband Networks
- Recall the security concerns in wireless networks
- Report the vulnerabilities in wireless networks

- Define best practices for Wi-Fi security

## Key Words

IEEE802.11x protocols	Wireless Local Networks	4G (LTE)
5G	Authentication Mechanism	Wi-Fi weaknesses
Parasitic Grids	Best Practices	WiMAX

## Annotated Bibliography

### Basic

Guide to Computer Network Security, 4th Edition, Joseph Migga Kizza, 2017, DOI 10.1007/978-3-319-55606-2, Available to all EUC students via the <https://www.openathens.net/> service that is available to all EUC students. Related link: <https://www.springer.com/gp/book/9783319556055>

This week is based on the above eBook and more specifically in Chapter 18 pages 397-426. This chapter provides an overview of all wireless technologies deployed today from Wi-Fi to new initiative of 5G that is expecting to be operational by 2020. The wireless network vulnerabilities are discussed along with the security measures to safeguard these networks. In addition to this, additional questions, practical exercises and self-study concludes this sixth week.

### Supplementary

Power point presentation slides available in the platform

A security researcher discovered and disclosed a serious vulnerability affecting the Wi-Fi Protected Access II – WPA2 protocol, which is used by all modern, protected Wi-Fi enabled devices. The vulnerability enables an attacker to modify the protocol's handshake, which can essentially lead to intercepting the internet traffic of a Wi-Fi network -and depending on the network configuration, it is also possible to inject and/or manipulate data, without owning or breaking its password security. The vulnerability is serious, has a very big attack surface but it also has its limitations: it cannot be performed remotely. Read more for [An overview of the Wi-Fi WPA2 vulnerability](#) in ENISA.

Video: [Understanding WEP, WPA, and WPA2](#)

### Suggestions for further reading

## **1. Wireshark - Brief description**

Wireshark is a free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on Linux, OS X, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows. There is also a terminal-based (non-GUI) version called TShark. Wireshark, and the other programs distributed with it such as TShark, are free software, released under the terms of the GNU General Public License.

Website: <https://www.wireshark.org/>

Price: Free (possibly needing to add additional network cards at around €50 each or the AirPcap USB doble for wireless networks, if required, at around \$700 each).

Dependencies: It can be installed on single machines. In machines where the network card is also active, it is recommended to use Wireshark with an additional network card that is able to operate in promiscuous mode. Additionally, AirPcap needs to be bought if required for wireless network sniffing, for the best results in terms of packet analysis. Wireless traffic for other purposes can also be captured through regular 802.11 wireless cards.

2. As mobile technologies evolve so does the threat landscape. Early generations of mobile networks 2G/3G rely on SS7 and its IP Version SIGTRAN, a set of protocols designed decades ago, without giving adequate effect to modern day security implications. Nobody at that time envisioned the scale that mobile networks could reach in the future, so trust and security were not issues. Nonetheless at the moment we are still using this legacy set of protocols to assure the interconnection between providers. The industry and security research community has started covering the topic, by providing good practices and necessary tools. But still, a lot more has to be done. Basic security measures seem to be implemented by more mature providers, but these measures assure only a basic protection level. More efforts need to be made so that an optimal protection level is achieved. Read more in ENISA report on [Signalling Security in Telecom SS7/Diameter/5G](#)

## **Self-Assessment Exercises**

### **Exercise 3.1**

What are the five components that constitute the evolving security architecture?

### **Exercise 3.2**

Suppose you are in charge of information security in a large organization where the value of data justifies strong protection in the hybrid network resulting from both LAN and WLAN. What are these additional security measures, and how would you go about implementing them?

#### **Recommended time for the student to work**

15 hours

## CYBER CRIMES AND HACKERS

4<sup>th</sup> Week

### Summary

This week we will discuss about cybercrimes and how they are executed. Cybercrimes are evolving and the whole nature of cyber-attacks has been changes over the last years. Attacks that are more sophisticated and now targeting to organisations and national institutions whereas at the same time the trends of cybercrime span from simple hacking attempts to ransom to political movements and espionage.

### Introductory Remarks

The greatest threats to the security, privacy, and reliability of computer networks and other related information systems in general are **cybercrimes committed by cybercriminals**, but most importantly **hackers**. Judging by the damage caused by past cybercriminal and hacker attacks to computer networks in businesses, governments, and individuals, resulting in inconvenience and loss of productivity and credibility, one cannot fail to see that there is a growing community demand to software and hardware companies to create more secure products that can be used to identify threats and vulnerabilities, to fix problems, and to deliver security solutions.

Industry and governments around the globe are responding to these threats through a variety of approaches and collaborations such as:

- Formation of organizations, such as the Information Sharing and Analysis Centers (ISACs).
- Getting together of industry portals and ISPs on how to deal with distributed denial-of-service attacks including the establishment of Computer Emergency Response Teams (CERTs).
- Increasing the use of sophisticated tools and services by companies to deal with network vulnerabilities. Such tools include the formation of Private Sector Security Organizations (PSSOs) such as SecurityFocus, Bugtraq, and the International Chamber of Commerce's Cybercrime Unit.
- Setting up national strategies similar to the US National Strategy to Secure Cyberspace, an umbrella initiative of all initiatives from various sectors of the national critical infrastructure grid and the Council of Europe Convention on Cybercrimes.

According to the director of the US National Infrastructure Protection Center (NIPC), cybercrimes present the greatest danger to e-commerce and the public in general [1]. The threat of crime using the Internet is real and growing, and it is likely to be the scourge of the twenty-first century. **A cybercrime is a crime like any other crime, except that in this case, the illegal act must involve a connected computing system either as an object of a crime, an instrument used to commit a crime, or a repository of evidence related to a crime.** Alternatively, one can define a cybercrime as an act of unauthorized intervention into the working of the telecommunication networks and/or the sanctioning of an authorized access to the resources of the computing elements in a network that leads to a threat to the system's infrastructure or life or that causes significant property loss.

Both the International Convention of Cyber Crimes and the European Convention on Cyber Crimes have outlined the list of these crimes to include the following:

- Unlawful access to information
- Illegal interception of information
- Unlawful use of telecommunication equipment
- Forgery with use of computer measures
- Intrusions of the public switched and packet network
- Network integrity violations
- Privacy violations
- Industrial espionage
- Pirated computer software
- Fraud using a computing system
- Internet/e-mail abuse
- Using computers or computer technology to commit murder, terrorism, pornography, and hacking

Because for any crime to be classified as a cybercrime, it must be committed with the help of a computing resource, as defined above, cybercrimes are executed in one of two ways: **penetration** and **denial-of-service** attacks.

Let us see now, who are these people behind network attacks. The word **hacker** has changed meaning over the years as technology changed. Currently, the word has two opposite meanings. One definition talks of a computer enthusiast as an individual who enjoys exploring the details of computers and how to

stretch their capabilities, as opposed to most users who prefer to learn only the minimum necessary. The opposite definition talks of a malicious or inquisitive meddler who tries to discover information by poking around [2].

Before acquiring its current derogatory meaning, the term hacking used to mean expert writing and modification of computer programs. Hackers were considered people who were highly knowledgeable about computing; they were considered computer experts who could make the computer do all the wonders through programming. Today, however, hacking refers to a process of gaining unauthorized access into a computer system for a variety of purposes, including the stealing and altering of data and electronic demonstrations.

**How hackers prepare their attacks and what methodology the used?** Hackers are often computer enthusiasts with a very good understanding of the working of computers and computer networks. They use this knowledge to plan their system attacks. Seasoned hackers plan their attacks well in advance, and their attacks do not affect unmarked members of the system. To get to this kind of precision, they usually use specific attack patterns of topologies. Using these topologies, hackers can select to target one victim among a sea of network hosts, a subnet of a LAN, or a global network. The attack pattern, the topology, is affected by the following factors and network configuration:

- Equipment availability—This is more important if the victim is just one host. The underlying equipment to bring about an attack on only one host and not affect others must be available. Otherwise, an attack is not possible.
- Internet access availability—Similarly, it is imperative that a selected victim host or network be reachable. To be reachable, the host or subnet configuration must avail options for connecting to the Internet.
- The environment of the network—Depending on the environment where the victim host or subnet or full network is, care must be taken to isolate the target unit so that nothing else is affected.
- Security regime—It is essential for the hacker to determine what type of defenses are deployed around the victim unit. If the defenses are likely to present unusual obstacles, then a different topology that may make the attack a little easier may be selected.

Most system attacks take place before even experienced security experts have advance knowledge of them. Most of the security solutions are best practices as we have so far seen, and we will continue to

discuss them as either preventive or reactive. An effective plan must consist of four components: **prevention, detection, analysis and response.**

## Aim/Objectives

The objective of this section is to look into the meaning of cybercrime and the evolution of network attacks over the years. It is important to understand that cybercrime is a crime like any other crime and both the International Convention of Cyber Crimes and the European Convention on Cyber Crimes have outlined the list of these crimes. Another objective is for the student to be able to define the pattern that most attacks follow and name the main components of security solutions and best practices.

## Learning Outcomes

Upon successful completion of this course, students should be able to:

- Provide the definition of cybercrime
- List the various types of cybercrime
- Explain the pattern of a cyber-attack
- Explain what is the Distributed Denial of Service (DDoS)
- State the various Types of Hackers
- Define and explain the ways that cybercrimes are executed
- State the Hacker Motives

## Key Words

Cybercrime	hacker	penetration
prevention	detection	analysis and response

## Annotated Bibliography

### Basic

Guide to Computer Network Security, 4th Edition, Joseph Migga Kizza, 2017, DOI 10.1007/978-3-319-55606-2, Available to all EUC students via the <https://www.openathens.net/> service that is available to all EUC students. Related link: <https://www.springer.com/gp/book/9783319556055>

This week is based on the above eBook and more specifically in Chapter 5 pages 105-130. This chapter provides an insight on cyber-crimes, the various network attacks and how we are dealing with the rising of cybercrimes.

## **Supplementary**

Power point presentation slides available in the platform.

Video: High Tech Hackers Documentary - Modern Day Hacking Today 2017 - [Cyber Crime Biography](#)

Looking back at the first six months of 2018, there have not been as many government leaks and global ransomware attacks as there were by this time last year, but that's pretty much where the good news ends. Corporate security is not getting better fast enough, critical infrastructure security hangs in the balance, and state-backed hackers from around the world are getting bolder and more sophisticated.

[Here](#) are the big digital security dramas that have played out so far in 2018.

## **Suggestions for further reading**

[1] Cybercrime threat “real and growing” <http://news.bbc.co.uk/2/hi/science/nature/978163.stm>

[2] Glossary of vulnerability testing terminology <http://www.ee.oulu.fi/research/ouspg/sage/glossary/>

## **Self-Assessment Exercises**

### **Exercise 4.1**

Give the definition of cybercrime.

### **Exercise 4.2**

What were the most serious cybercrimes the previous year? What was their effect?

## **Activity**

### **Recommended time for the student to work**

15 hours

## COMPUTER NETWORK SECURITY PROTOCOLS

5<sup>th</sup> Week

### Summary

This week we will discuss network security protocols and how they apply to the whole TCP/IP stack. Different protocols provide different level security from the Application layer down to physical layer. Our scope is not to analyse in details the functionality of each one protocol; that will require a separate course, but to scratch on the basic functionality of these protocols and their level of the protection they offer.

### Introductory Remarks

The rapid growth of the Internet and corresponding Internet community has fueled a rapid growth of both individual and business communications leading to the growth of e-mail and e-commerce. In fact, studies now show that the majority of the Internet communication content is e-mail content. The direct result of this has been the growing concern and sometimes demand for security and privacy in electronic communication and e-commerce. Security and privacy are essential if individual communication is to continue and e-commerce is to thrive in cyberspace.

The call for and desire for security and privacy has led to the advent of several proposals for security protocols and standards. Among these are Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols, secure IP (IPsec), Secure HTTP (S-HTTP), secure e-mail (PGP and S/MIME), DNDSEC, SSH, and others. Before we proceed we'd better visit our first week so as to refresh our knowledge and understanding of the network protocol stack.

We will discuss these protocols and standards within the framework of the network protocol stack as follows:

- **Application-level security:** (for TCP/IP) and application and presentation (for ISO)—RADIUS, TACACS, PGP, S/MIME, S-HTTP, HTTPS, SET, SSH, and Kerberos
- **Transport-level security:** (for TCP/IP) and session and transport (for ISO)—SSL and TLS
- **Network-level security:** for both TCP/IP and ISO—PPTP, L2TP, IPsec, and VPNs

- **Physical link-level security:** (for TCP/IP) and data link and physical (for ISO)— packet filters, NAT, CHAP, and PAP.

An association between security protocols and TCP/IP layers is illustrated in Figure 7

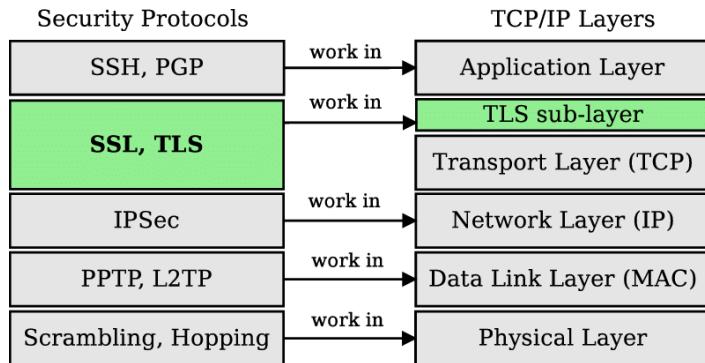


Figure 7 – The security-related protocols associated with the TCP/IP protocol stack.

#### Application-Level Security

All the protocols in the application layer reside on both ends of the communication link. They are all communication protocols ranging from simple text to multimedia including graphics, video, audio, and so on.

#### Security in the Transport Layer

Although several protocols can be found in the transport layer, we are only going to concentrate on two: Secure Socket Layer (SSL) and Transport Layer Security (TLS). Currently, however, these two are no longer considered as two separate protocols but one under the name SSL/TLS, after the SSL standardization was passed over to IETF, by the Netscape consortium, and Internet Engineering Task Force (IETF) renamed it TLS.

#### Security in the Network Layer

The dominant technologies in this layer are the IPsec and VPN. **IPsec** is a suite of authentication and encryption protocols developed by the Internet Engineering Task Force (IETF) and designed to address the inherent lack of security for IP-based networks. IPsec, unlike other protocols, is a very complex set of protocols described in a number of RFCs including RFC 2401 and 2411. It runs transparently to transport layer and application layer protocols which do not see it. Although it was designed to run in the new version of the Internet Protocol, IP version 6 (IPv6), it has also successfully run in the older IPv4.

A **VPN** is a private data network that makes use of the public telecommunication infrastructure, such as the Internet, by adding security procedures over the unsecure communication channels. The security procedures that involve encryption are achieved through the use of a tunneling protocol. There are two types of VPNs: remote access which lets single users connect to the protected company network and site-to-site which supports connections between two protected company networks. In either mode, VPN technology gives a company the facilities of expensive private leased lines at much lower cost by using the shared public infrastructure like the Internet.

## Aim/Objectives

The scope of this week is for the student to understand that security protocols apply to the whole TCP/IP stack. Different protocols provide different lev security from the Application layer down to physical layer. Our scope is not to analyse in details the functionality of each one protocol; that will require a separate course, but to scratch on the basic functionality of these protocols and their level of the protection they offer. The knowledge on security protocols is essential for the student to obtain a holistic understanding of network security.

## Learning Outcomes

Upon successful completion of this course, students should be able to:

- Define the most important security protocols of each one layer in the TCP/IP stack.
- Explain the main features of the Transport Layer Security (TLS)
- Express the differences between SSL and S-HTTP
- Express the benefits of IPsec
- State the IPsec Issues
- Define the various types of Virtual Private Networks (VPNs)
- Explain the differences between SSL and S-HTTP

## Key Words

Secure Socket Layer (SSL)	Transport Layer Security (TLS)	secure IP (IPsec)
Secure HTTP (S-HTTP)	secure e-mail (PGP and S/MIME)	Application-level security
Transport-level security	Network-level security	Physical link-level security

## Annotated Bibliography

### Basic

Guide to Computer Network Security, 4th Edition, Joseph Migga Kizza, 2017, DOI 10.1007/978-3-319-55606-2, Available to all EUC students via the <https://www.openathens.net/> service that is available to all EUC students. Related link: <https://www.springer.com/gp/book/9783319556055>

This week is based on the above eBook and more specifically in Chapter 17 pages 365-396. This chapter provides a detailed guidance on the various security protocols in the whole TCP/IP stack. After a short introduction the security protocols are introduced starting from the Application layer. Secure HTTP (S-HTTP), Secure/Multipurpose Internet Mail Extension (S/MIME), Kerberos and others are described and explained. At the transport layer Secure Socket Layer (SSL), and Transport Layer Security (TLS) are explained. Network layer-based protocols such as Internet Protocol Security (IPsec) are described along with the main differences between IPv4 and IPV6 in relation to security. Point-to-Point Protocol (PPP) and other physical layer protocols are introduced and in this way this chapter covers the whole protocol stack. Self-assessment exercises and self-study concludes this fifth week.

### Supplementary

Power point presentation slides available in the platform

Tutorial: [Introduction to Network Security: Protocols](#)

Video: [Internet Security Protocols - Bart Preneel](#)

### Suggestions for further reading

- [1] Kizza JM (2002) Computer network security and cyber ethics, McFarland Publishers, Jefferson
2. Cryptographic algorithms, when used in networks, are used within a cryptographic protocol. In the ENISA algorithms report of 2013, several protocols were discussed. In this document (which is the sister document of the 2014 report we extend the work in the 2013 report to cover more categories of protocols. Find more in the ENISA report “[Study on cryptographic protocols](#)”.

## Self-Assessment Exercises

### Exercise 5.1

Provide a list with the most imprint security protocols per layer.

### **Exercise 5.2**

SSL3.0 has been transformed into TLS 1.0. Study the TLS protocol specifications and show how all are met by SSL. There are some differences in the protocol specifications of the two. Describe these differences.

### **Activities**

S/MIME and PGP are sister protocols; they share a lot. Study the two protocols and discuss the qualities they share. Also look at the differences between them. Why is PGP more successful? Or is it?

### **Recommended time for the student to work**

20 hours

## AUTHENTICATION

6<sup>th</sup> Week

### Summary

This week we will discuss the concept of authentication and the various mechanisms for system authentication. One important concept is the Public Key or asymmetric cryptography and how it is applied to encrypt a message.

### Introductory Remarks

Authentication is the process of validating the identity of someone or something. It uses information provided to the authenticator to determine whether someone or something is in fact who or what it is declared to be. In private and public computing systems, for example, in computer networks, the process of authentication commonly involves someone, usually the user, using a password provided by the system administrator to logon. The user's possession of a password is meant to guarantee that the user is authentic. It means that at some previous time, the user requested, from the system administrator, and the administrator assigned and/or registered a self-selected password.

The user presents this password to the logon to prove that he or she knows something no one else could know. Generally, authentication requires the presentation of credentials or items of value to really prove the claim of who you are. The items of value or credential are based on several unique factors that show something you know, something you have, or something you are [1]:

- **Something you know:** This may be something you mentally possess. This could be a password, a secret word known by the user and the authenticator. Although this is inexpensive administratively, it is prone to people's memory lapses and other weaknesses including secure storage of the password files by the system administrators. The user may use the same password on all system logons or may change it periodically, which is recommended. Examples using this factor include passwords, passphrases, and personal identification numbers (PINs).
- **Something you have:** This may be any form of issued or acquired self-identification such as:
  - SecurID

- **CryptoCard**
- **ActivCard**
- **SafeWord**
- **Many other forms of cards and tags**

This form is slightly safer than something you know because it is hard to abuse individual physical identifications. For example, it is harder to lose a smart card than to remember the card number.

- **Something you are:** This is a naturally acquired physical characteristic such as voice, fingerprint, iris pattern, and other biometrics.

Although biometrics are very easy to use, this ease of use can be offset by the expenses of purchasing biometric readers. Examples of items used in this factor include fingerprints, retinal patterns, DNA patterns, and hand geometry. In addition to the top three factors, another factor, though indirect, also plays a part in authentication:

- **Somewhere you are:** This usually is based on either physical or logical location of the user. The use, for example, may be on a terminal that can be used to access certain resources.

Number	Factor	Examples	Vulnerabilities
1	What you know	Password, PIN	Can be forgotten, guessed, duplicated
2	What you have	Token, ID card, keys	Can be lost, stolen, duplicated
3	What you are	Iris, voiceprint, fingerprint	Nonrepudiable

Table 2 - Authentication factors and their vulnerabilities<sup>1</sup>.

In general, authentication takes one of the following three forms [2]:

- **Basic authentication involving a server.** The server maintains a user file of either passwords and usernames or some other useful piece of authenticating information. This information is always examined before authorization is granted. This is the most common way computer network systems authenticate users. It has several weaknesses though, including forgetting and misplacing authenticating information such as passwords.
- **Challenge-response,** in which the server or any other authenticating system generates a challenge to the host requesting for authentication and expects a response.

---

<sup>1</sup>Ratha, Nalini K., Jonathan H. Connell and Ruud M. Bolle. "Secure Fingerprint-based Authentication for Lotus Notes." <https://faculty.unlv.edu/thatcher/is485/readings/biometrics.pdf>

- **Centralized authentication**, in which a central server authenticates users on the network and in addition also authorizes and audits them. These three processes are done based on server action. If the authentication process is successful, the client seeking authentication is then authorized to use the requested system resources. However, if the authentication process fails, the authorization is denied. The process of auditing is done by the server to record all information from these activities and store it for future use.

In the same area, Public key algorithms are fundamental security ingredients in cryptosystems, applications and protocols. They underpin various Internet standards, such as Transport Layer Security (TLS) that we studied in Week3, such as S/MIME, PGP, and GPG. Some public key algorithms provide key distribution and secrecy (e.g., Diffie–Hellman key exchange), some provide digital signatures (e.g., Digital Signature Algorithm), and some provide both (e.g., RSA).

However, still our main concern is related to password protection as it is widely known that passwords are cracked. Passwords are in fact one of the weakest links to security. Therefore, system administrators and users should pay special attention and apply mechanisms for enhanced password protection.

## Aim/Objectives

The objective of this section is to understand the concept of authentication and the various mechanisms for system authentication. One important concept is the Public Key, or asymmetric cryptography and how it is applied to encrypt a message. The student will be taught how to use the best password managers, how passwords are cracked and how to mitigate the cracking through the use of better hashing and key stretching technology and also the choice of good passwords. In addition to this the student will learn how to best use methods of authentication including passwords, multifactor authentication, like soft tokens and hard tokens.

## Learning Outcomes

Upon successful completion of this course, students should be able to:

- Define the concept of Authentication
- Identify the various authentication mechanisms
- Identify the various authentication technologies
- State the main concept behind asymmetric cryptography
- Describe strong password policies and methods
- List the steps for a good authentication policy

## Key Words

Authentication	Passwords	Public Key cryptography
Password cracking	Public Key authentication	Authentication policy

## Annotated Bibliography

### Basic

Guide to Computer Network Security, 4th Edition, Joseph Migga Kizza, 2017, DOI 10.1007/978-3-319-55606-2, Available to all EUC students via the <https://www.openathens.net/> service that is available to all EUC students. Related link: <https://www.springer.com/gp/book/9783319556055>

This week is based on the above eBook and more specifically in Chapter 10 pages 207-225. This chapter provides an overview of the concept of authentication and how it is applied to secure networks and systems. After a short introduction the various authentication method are explained with emphasis to types of authentication and authentication methods. Public Key authentication is discussed and how the public key encryption system allows and how passwords are cracked along with mitigation measures to protect our passwords. The student will be given also the opportunity to review password attacks and how to mitigate the cracking through the use of better hashing and key stretching technology and also the choice of good passwords.

### Supplementary

Power point presentation slides available in the platform.

#### How Passwords are cracked

1. The rule-based attack is one of the most complicated of all the attack modes. The reason for this is very simple. The rule-based attack is like a **programming language** designed for password candidate generation. It has functions to modify, cut or extend words and has conditional operators to skip some, etc. That makes it the most flexible, accurate and efficient attack. You can find more on rule-based attack in this [site](#).
2. Leet, also known as eleet or leetspeak, is a system of modified spellings and verbiage used primarily on the Internet for many [citation needed] phonetic languages. It uses some ASCII characters to

replace Latinate characters in ways that play on the similarity of their glyphs via reflection or other resemblance. Additionally, it modifies certain words based on a system of suffixes and alternate meanings. You can learn more in this [article](#).

3. Lots are known about passwords. Most are short, simple, and easy to crack. But much less is known about the psychological reasons a person chooses a specific password. We've analyzed the password choices of 10 million people, from CEOs to scientists, to find out what they reveal about the things we consider easy to remember and hard to guess. You can find more in this [article](#).

#### Suggestions for further reading

1. **Network Security Essentials: Applications and Standards, Sixth Edition, William Stallings, 2017, ISBN-13: 978-0134527338, ISBN-10: 9780134527338**

Chapter 3 in this book provides a deeper insight in Public Key Cryptography and principles. You can read more in message authentication modes and cryptographic algorithms.

### Self-Assessment Exercises

#### Exercise 6.1

How we classify the various areas of credentials to authenticate ourselves in a system

#### Exercise 6.2

What are the three general forms of authentication?

### Recommended time for the student to work

15 hours

## MALICIOUS SOFTWARE

7<sup>th</sup> Week

### Summary

This week we will discuss the various types of malicious software or malware and the main differences between host-based and independent malware. We will see how malware is classified and how they can infect computers and devices.

### Introductory Remarks

Perhaps the most sophisticated types of threats to computer systems are presented by programs that exploit vulnerabilities in computing systems. Such threats are referred to as **malicious software**, or **malware**. In this context, we are concerned with threats to application programs as well as utility programs, such as editors and compilers, and kernel-level programs.

We will examine this week malicious software, with a special emphasis on viruses and worms. We will begin with a survey of various types of malware, with a more detailed look at the nature of viruses and worms. We then turn to distributed denial-of-service attacks. Throughout, the discussion presents both threats and countermeasures.

The terminology in this area presents problems because of a lack of universal agreement on all of the terms and because some of the categories overlap.

Malicious software is software that is intentionally included or inserted in a system for a harmful purpose. Malicious software can be divided into two categories: those that need a host program, and those that are independent.

Viruses, logic bombs, and backdoors are examples of those that need a host program. A **virus** is a piece of software that can “infect” other programs by modifying them; the modification includes a copy of the virus program, which can then go on to infect other programs.

A **logic bomb** is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files (such as a salary database trigger), should they ever be terminated from the company.

Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Some viruses attack their host systems on specific dates, such as Friday the 13th or April Fools' Day. Trojans that activate on certain dates are often called "time bombs".

A **backdoor** is a method, often secret, of bypassing normal authentication or encryption in a computer system, a product, or an embedded device (e.g. a home router), or its embodiment, e.g. as part of a cryptosystem, an algorithm, a chipset, or a "homunculus computer" —a tiny computer-within-a-computer (such as that as found in Intel's AMT technology) ([1], [2]). Backdoors are often used for securing remote access to a computer or obtaining access to plaintext in cryptographic systems.

Independent malware is a self-contained program that can be scheduled and run by the operating system. Worms and bot programs are examples. A **worm** is a program that can replicate itself and send copies from computer to computer across network connections. Upon arrival, the worm may be activated to replicate and propagate again. In addition to propagation, the worm usually performs some unwanted function.

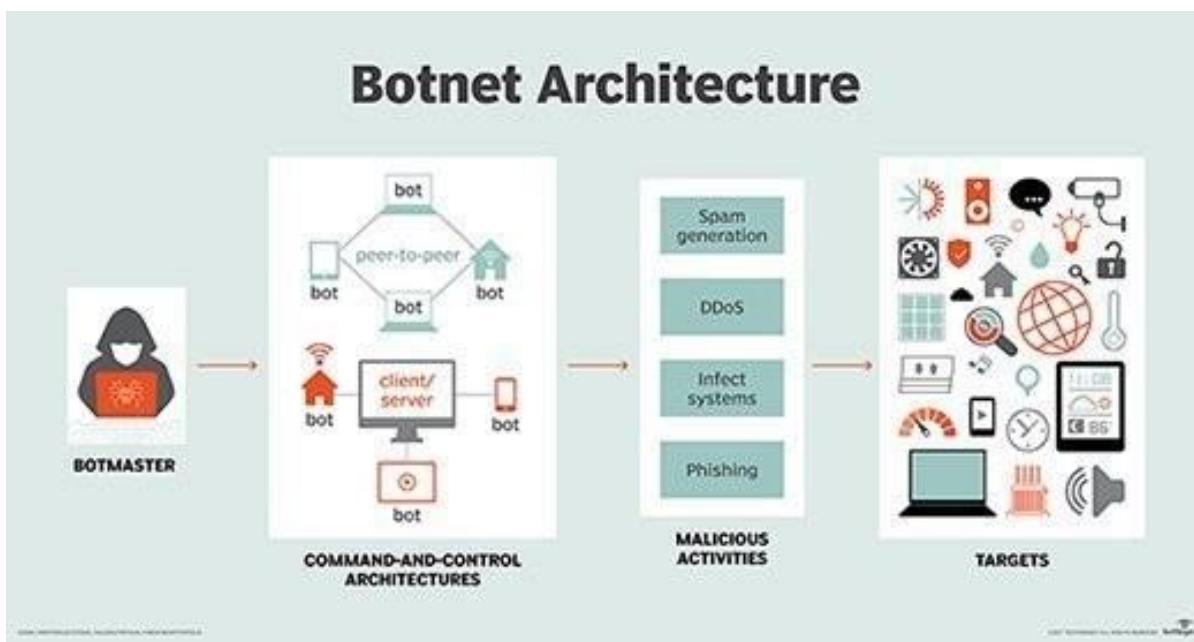


Figure 8 – Illustration of botnet architecture.

A **botnet** is a number of Internet-connected devices, each of which is running one or more bots. Botnets can be used to perform distributed denial-of-service attack (DDoS attack), steal data, send spam, and

allows the attacker to access the device and its connection. The owner can control the botnet using command and control (C&C) software. The word "botnet" is a combination of the words "robot" and "network". The term is usually used with a negative or malicious connotation.

The best way to address the above threats is to apply prevention mechanisms. In other words, do not allow a virus to get into the system in the first place, or block the ability of a virus to modify any files containing executable code or macros. This goal is, in general, almost impossible to achieve, although prevention can reduce the number of successful viral attacks. The next best approach is to be able to do the following:

- **Detection:** Once the infection has occurred, determine that it has occurred and locate the virus.
- **Identification:** Once detection has been achieved, identify the specific virus that has infected a program.
- **Removal:** Once the specific virus has been identified, remove all traces of the virus from the infected program and restore it to its original state. Remove the virus from all infected systems so that the virus cannot spread further.

Other important area of malicious software and the subsequent threats is widely known as Denial of Service (DoS). In computing a denial-of-service attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

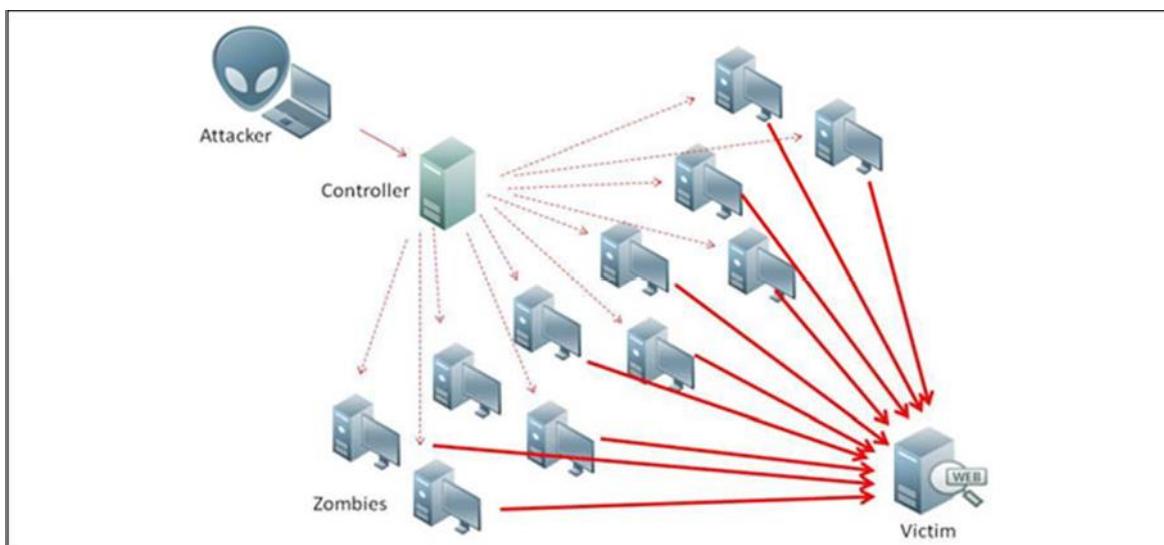


Figure 9 – DoS attack illustration.

Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. In a Distributed denial of service (DDoS) a large number of compromised hosts are amassed to send useless packets. In recent years, the attack methods and tools have become more sophisticated, effective, and more difficult to trace to the real attackers, while defense technologies have been unable to withstand large-scale attacks.

## Aim/Objectives

The objective of this section is to understand the various types of malicious software or malware and the main differences between host-based and independent malware. The student will be to understand and classify malware. Distinguishing and classifying different types of malware from each other is important to better understanding how they can infect computers and devices, the threat level they pose and how to protect against them. Another important objective in this week is for the student to understand what DoS is and how this attack is used to temporarily or indefinitely disrupting services of a host connected to the Internet. DoS and DDos attacks present a significant security threat to corporations, and the threat appears to be growing.

## Learning Outcomes

Upon successful completion of this course, students should be able to:

- Define what malicious software is.
- Define then various types of malicious software.
- Classify malicious software threats and its effects in networks and systems.
- Describe the possible Antivarious approaches.
- Explain the State of Worm Technology.
- Explain what DoS and DDOS are.

## Key Words

Malware	Distributed Denial of Service (DDoS)	botnet
logic bomb	Backdoor	worm

## Annotated Bibliography

## **Basic**

**Network Security Essentials: Applications and Standards, Sixth Edition, William Stallings, 2017, ISBN-13: 978-0134527338, ISBN-10: 9780134527338**

This week is based on the above book and more specifically in Chapter 10 – Malicious software. In this chapter an introduction is given of the various types of malicious software or malware. Backdoors, logic bombs Trojan horses, mobile code and Multiple-Threat Malware are described and explained. The nature of computer with their classification is described along with the counter measures to address these threats. The worm propagation model is explained with an overview of the most recent worm attacks. In addition, the worm Countermeasures are described. Distributed denial of service (DDoS) attacks are explained as they present a significant security threat to corporations and the threat appears to be growing.

## **Supplementary**

1. Power point presentation slides available in the platform.
2. Malware, also known as "malicious software," can be classified several ways in order to distinguish the unique types of malware from each other. Distinguishing and classifying different types of malware from each other is important to better understanding how they can infect computers and devices, the threat level they pose and how to protect against them. Malware, also known as "malicious software," can be classified several ways in order to distinguish the unique types of malware from each other. Distinguishing and classifying different types of malware from each other is important to better understanding how they can infect computers and devices, the threat level they pose and how to protect against them. Learn more about malware classification in Kaspersky Lab [report](#)
3. EU Member States' CSIRTs work together in the EU CSIRT Network. In the course of their incident handling duties and in their publications, CSIRTs use specialised terminology the meaning of which is not always self-explanatory. These pages seek to explain this terminology in plain, jargon-free language. As new concepts are added, they will form an independent and unbiased information security glossary. The glossary entries can be viewed [here](#)

## **Suggestions for further reading**

1. 2017 was the year in which incidents in the cyberthreat landscape have led to the definitive recognition of some omnipresent facts. We have gained unwavering evidence regarding monetization

methods, attacks to democracies, cyber-war, transformation of malicious infrastructures and the dynamics within threat agent groups.

But 2017 has also brought successful operations against cyber-criminals. Law enforcement, governments and vendors have managed to shut down illegal dark markets, de-anonymize the Darknet and arrest cyber-criminals. Moreover, state-sponsored campaigns have been revealed and details of technologies deployed by nation states have been leaked. Mostly remarkable though is the manifestation of the cyberthreat landscape within framework programmes that are about to be established in the financial sector: cyberthreats make up the basis for the development and implementation of red and blue teaming activities in financial sector, both within Member States and across Europe. Read more on [ENISA Threat Landscape Report 2017](#)

2. EURPOL has currently released the 2018 Internet Organised Crime Threat Assessment (IOCTA), which has been and continues to be one of the flagship strategic products for Europol. It provides a unique law enforcement focused assessment of the emerging threats and key developments in the field of cybercrime over the last year. Read more in this [report](#)

## Self-Assessment Exercises

### Exercise 7.1

What is Denial of Service (DoS) and Distributed denial of service (DDoS)?

The question arises as to whether it is possible to develop a program that can analyse a piece of software to determine if it is a virus. Consider that we have a program D that is supposed to be able to do that. That is, for any program P, if we run D(P), the result returned is TRUE (P is a virus) or FALSE (P is not a virus).

Now consider the following program:

```
Program CV :=
{ ...
main-program :=
    {if D(CV) then goto next:
        else infect-executable;
    }
next:
}
```

In the preceding program, infect-executable is a module that scans memory for executable programs and replicates itself in those programs. Determine if D can correctly decide whether CV is a virus.

## Exercise 7.2

Consider the following fragment in an authentication program:

```
username = read_username();
password = read_password();
if username is "133t h4ck0r"
    return ALLOW_LOGIN;
if username and password are valid
    return ALLOW_LOGIN
else return DENY_LOGIN
```

What type of malicious software is this?

**Recommended time for the student to work**

15 hours

# COMPUTER NETWORK VULNERABILITIES

8<sup>th</sup> Week

## Summary

This week we will work towards computer network vulnerabilities. We will also do a practical exercise with open tools for the discovery of network and system voluntarily.

## Introductory Remarks

System vulnerabilities are weaknesses in the software or hardware on a server or a client that can be exploited by a determined intruder to gain access to or shut down a network. Vulnerabilities exist not only in hardware and software that constitute a computer system but also in policies and procedures, especially security policies and procedures, that are used in a computer network system and in users and employees of the computer network systems. Since vulnerabilities can be found in so many areas in a network system, one can say that a security vulnerability is indeed anything in a computer network that has the potential to cause or be exploited for an advantage. The frequency of attacks in the last several years and the speed and spread of these attacks indicate serious security vulnerability problems in our network systems.

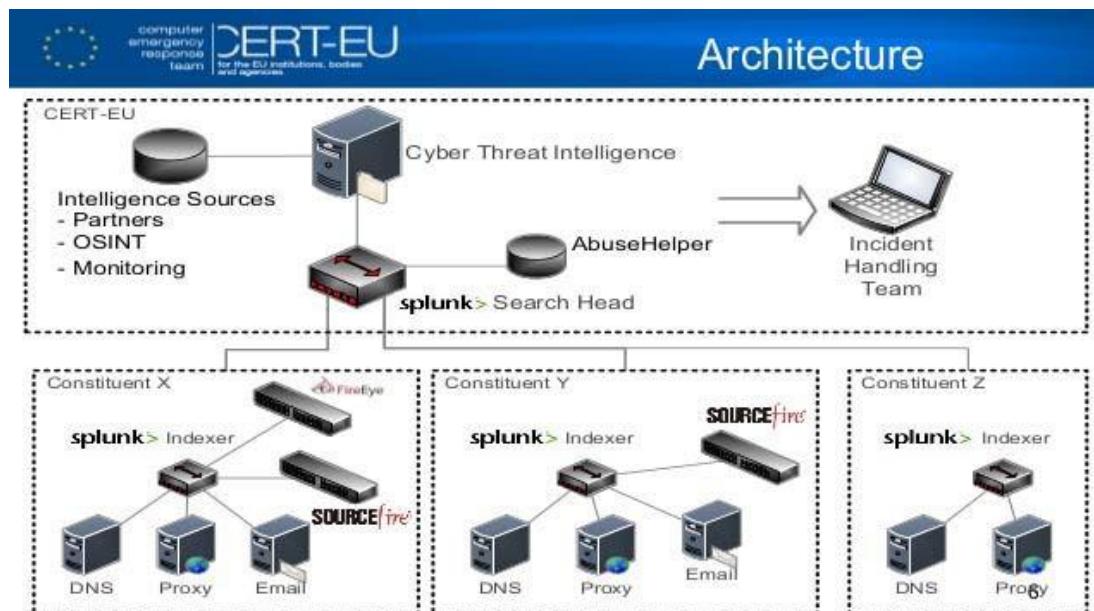


Figure 10 – CERT-EU Architecture.

There is no definitive list of all possible sources of these system vulnerabilities. Many scholars and indeed many security incident reporting agencies, such as Bugtraq, the mailing list for vulnerabilities; CERT-EU, the **EU Computer Emergency Response Team**; US-CERT, the USA Computer Emergency Response Team, NTBugtraq, the mailing list for Windows security and others, have called attention to not only one but multiple factors that contribute to these security problems and pose obstacles to the security solutions. Among the most frequently mentioned sources of security vulnerability problems in computer networks are design flaws, poor security management, incorrect implementation, Internet technology vulnerability, the nature of intruder activity, the difficulty of fixing vulnerable systems, the limits of effectiveness of reactive solutions, and social engineering [1].

Vulnerability assessment is a process that works on a system to identify, track, and manage the repair of vulnerabilities on the system. The assortment of items that are checked by this process in a system under review varies depending on the organization. It may include all desktops, servers, routers, and firewalls. Most vulnerability assessment services will provide system administrators with:

- Network mapping and system fingerprinting of all known vulnerabilities
- A complete vulnerability analysis and ranking of all exploitable weaknesses based on potential impact and likelihood of occurrence for all services on each host
- Prioritized list of misconfigurations

## VULNERABILITY ASSESSMENT

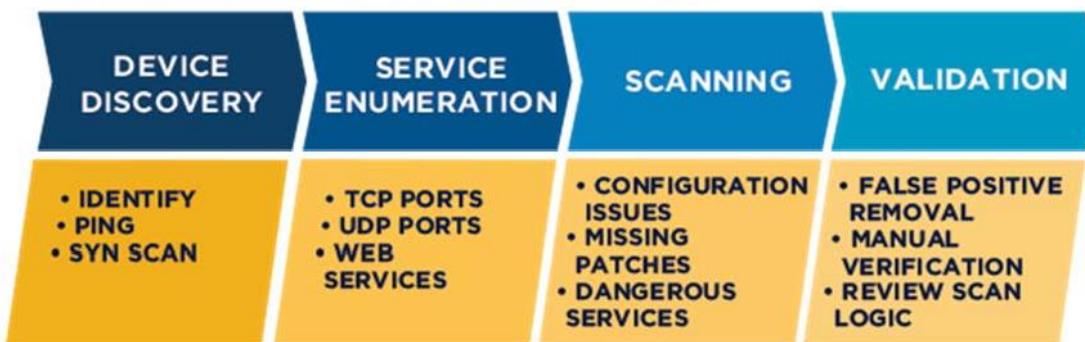


Figure 11 – Network vulnerability assessment process.

In addition, at the end of the process, a final report is always produced detailing the findings and the best way to go about overcoming such vulnerabilities. This report consists of prioritized recommendations for mitigating or eliminating weaknesses, and based on an organization's operational schedule, it also

contains recommendations of further reassessments of the system within given time intervals or on a regular basis.

## Aim/Objectives

The scope of this week is twofold. i) to introduce the student with the theoretical foundation for understanding computer and network vulnerabilities, and ii) to do a practical exercise with open tools for the discovery of network and system voluntarily. The student will be able after the study of this week to determine if there are any internal or external security vulnerabilities on his/her router or other network devices that attackers could exploit. The student will be familiarized with a fair large number of tools that he can use to scan a local network by conducting and internal and external vulnerability scanning. As we go deeper in our study in network security practical exercises are important for the student to grasp and better understand the theory behind network security.

## Learning Outcomes

Upon successful completion of this course, students should be able to:

- State and identify the sources of system vulnerabilities.
- Explain the importance of vulnerability assessment.
- Explain the advantages of vulnerability discovery.
- Practice with vulnerability scanners in his/her local area network.
- Illustrate host discovery, port and vulnerability scanning.

## Key Words

Vulnerability Assessment	router scanning	man-in-the-middle
Security management	Software updates	Demilitarized zones (DMZ)
Port scanning	TCP scan	UDP scan

## Annotated Bibliography

### Basic

Guide to Computer Network Security, 4th Edition, Joseph Migga Kizza, 2017, DOI 10.1007/978-3-319-55606-2, Available to all EUC students via the <https://www.openathens.net/> service that is available to all EUC students. Related link: <https://www.springer.com/gp/book/9783319556055>

This eightieth week is based on the above eBook and more specifically in Chapter 4 pages 87-103. This chapter provides a simplified approach and presents the main concepts in vulnerability assessment. In addition to this a number of free tools available online are offered to the students to conduct practical exercises.

### **Supplementary**

Power point presentation slides available in the platform

Video: [Testimonial CERT-EU](#)

Video: [Nmap Tutorial For Beginners](#)

Video: [Kali Linux 2017.2 - Review & Updates](#)

**From Hacking to Report Writing: An Introduction to Security and Penetration Testing, Robert Svensson, ISBN-13 (pbk): 978-1-4842-2282-9 ISBN-13 (electronic): 978-1-4842-2283-6, DOI 10.1007/978-1-4842-2283-6, Library of Congress Control Number: 2016957882.**

This book details how to do high-quality security and penetration testing and provides in detail, the step-by-step process used by security professionals to locate security weaknesses. This book will also teach the reader how to use the very same tools and techniques that hackers use to break into computer systems. We will concentrate, however, in this week only on Chapter 6 “Identifying Vulnerabilities” and more specifically on nmap port scanning.

### **Kali Linux - Brief description**

Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing. It is preinstalled with over 300 penetration-testing programs, including Armitage (a graphical cyber-attack management tool), nmap (a port scanner), Wireshark (a packet analyzer), John the Ripper (a password cracker), Aircrack-ng (a software suite for penetration-testing wireless LANs), Burp suite and OWASP ZAP (both web application security scanners). Kali Linux can run natively when installed on a computer's hard disk, can be booted from a live CD or live USB, or it can run within a virtual machine. It is a supported platform of the Metasploit Project's Metasploit Framework, a tool for developing and executing security exploits.

Note – Kali Linux includes a huge number of tools, including some of the other ones mentioned in this document, plus others that could be used for teaching purposes (the teaching staff should explore this Linux distribution and decide on which additional software to use, depending on expertise – for a full list, see <http://tools.kali.org/tools-listing>). The analysis of all of these tools is beyond the scope of this document. Kali Linux also includes some software that can be used for forensic analysis (the forensics software that is used by most police departments (FTK <http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk> and Encase <https://www.guidancesoftware.com/encase-forensic>) are very expensive products. The university should check whether any cheaper student or educational editions are available.

Website: <https://www.kali.org/>

Price: Free

Dependencies: Needs to be installed on a physical computer or a VM – it is a standalone OS.

### **Nmap - Brief description**

Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).

Website: <https://nmap.org/>

Price: Free

Dependencies: None – it can be installed on single machines.

### **Tools for scanning the home router**

1. This [site](#) provides a database for default router passwords

2. Find your IP of your home router in this [site](#)

### **External vulnerability scanning**

3. You can conduct an external vulnerability scanning in this [site](#)
4. Conduct a free on-line vulnerability scanning in this [site](#)

### **Suggestions for further reading**

[1] Pethia RD. Information technology—essential but vulnerable: how prepared are we for attacks? A related research paper on cyber attacks.

2. The Software Engineering Institute recently released a revamped CERT Coordination Center (CERT/CC) Vulnerabilities Database website at <https://www.kb.cert.org/vuls>. The Vulnerability Notes Database provides information about software vulnerabilities, including summaries, technical details, remediation information, and lists of affected vendors. Find more in [SEI Launches New CERT Vulnerabilities Website](#)

3. If you want to see a list of Common default IP Addresses for routers then check this [site](#)

### **Common default IP Addresses for routers**

4. You can check the list of List of Well-Known TCP Port Number [here](#)

## **Self-Assessment Exercises**

### **Exercise 8.1**

What are the main vulnerability assessment services that provided to system administrators?

### **Assignment - Vulnerability scanning (20 points)**

In most cases, your local network consists of you ADSL modem that is an all-in-one box with the modem, firewall, router, switch, firewall and a wireless Access Point (AP) similar to one presented in Figure 12.

In this assignment, you are requested to conduct an Internal and External vulnerability scanning in your home network. In an internal vulnerability scanning, you will have to discover all the hosts in your home network and discover any open ports of all the devices that are connected to your home router. To do so, you will need to use nmap and perform a number of different scans for TCP and UDP. You have to take screenshots as a proof of your work and explain your findings.

In an external vulnerability scanning, you can use a number of tools that are already provided to you in the Lab sessions. You need to find your ip address and choose some of the tools to run external scanning to your router. Again, you will need to take screenshots as a proof of your work and explain your findings.

Firewall settings: Open your network firewall and make sure that DMZ is not enabled. Explain the meaning of the DMZ and make sure that you have not running services inside the DMZ unless it is necessary. You will need to take screenshots as a proof of your work and explain your findings.

All the above results with explanations of the tools you have used will be submitted as a report.

In addition to this, you are requested to present your work in the classroom and get ready to provide explanations on your work, at the end of the course.

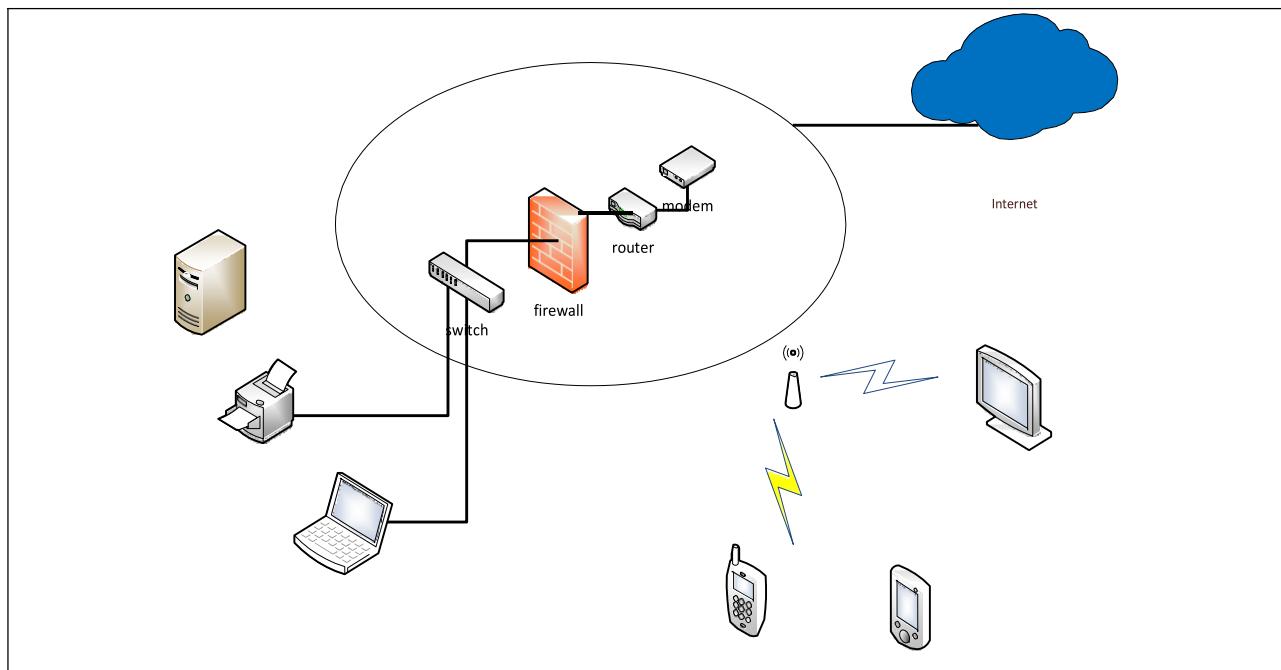


Figure 12 – Sample home network architecture.

### Recommended time for the student to work

40 hours

## SCRIPTING AND SECURITY

9<sup>th</sup> Week

### Summary

This week we will discuss how scripting has been used especially for an interactive Web in order to meet the growing demand of millions of Web services from users around the world. We will see, however, that scripting poses a major threat in computer networking.

### Introductory Remarks

The rapid growth of the Internet and its ability to offer services have made it the fastest-growing medium of communication today. Today's and tomorrow's business transactions involving financial data; product development and marketing; storage of sensitive company information; and the creation, dissemination, sharing, and storing of information are and will continue to be made online, most specifically on the Web. The automation and dynamic growth of an interactive Web has created a huge demand for a new type of Web programming to meet the growing demand of millions of Web services from users around the world. Some services and requests are tedious, and others are complex, yet the rate of growth of the number of requests, the amount of services requested in terms of bandwidth, and the quality of information requested warrant a technology to automate the process.

Script technology came in timely to the rescue. **A program script is a logical sequence of line commands which causes the computer to accomplish some task.** Many times, we refer to such code as macros or batch files because they can be executed without user interaction. A script language is a programming language through which you can write scripts. Scripts can be written in any programming language or a special language as long as they are surrogated by another program to interpret and execute them on the fly by a program unlike compiled programs that are run by the computer operating system.

Because scripts are usually small programs, written with a specific purpose in mind to perform tasks very quickly and easily, many times in constrained and embedded environments with abstracted performance and safety, unlike general purpose programs written in general-purpose programming languages, scripts are not in most cases full-featured programs, but tend to be “glue” programs that hold together other pieces of software. Therefore, scripting languages are not your general-purpose programming languages.

Their syntax, features, library, etc. are focused more around accomplishing small tasks quickly. The scripts can be either application scripts, if they are executed by an application program surrogate like Microsoft spreadsheet, or command line scripts if they are executed from a command line like the Windows or Unix/Linux command line.

Scripting is a powerful automation technology on the Internet that makes the Web highly interactive. Scripting technology is making the Web interactive and automated as Web servers accept inputs from users and respond to user inputs. While scripting is making the Internet and, in particular, the Web is alive and productive, it also introduces a huge security problem to an already security-burdened cyberspace.

Hostile scripts embedded in Web pages, as well as HTML formatted e-mail, attachments, and applets introduce a new security paradigm in cyberspace security. In particular, security problems are introduced in two areas: at the server and at the client.

Several security risks are introduced at both sides. A server-side script, whether compiled or interpreted, and its interpreter are included in a Web server as a module or executed as a separate CGI binary. It can access files, execute commands, and open network connections on the server. These capabilities make server-side scripts a security threat because they make anything run on the Web server unsecure by default. Among the many sever-side scripting languages are ERL, PHP, ColdFusion, ASP, MySQL, Java servlets, and MivaScript.

At the client-side all scripts like **JavaScript** and **VBScript** that execute in the browser can compromise the security of the user system. These scripts create hidden frames on Web sites so that as a user navigates a Web site, the scripts running in the browser can store information from the user for short-time use, just like a cookie. The hidden frame is an area of the Web page that is invisible to the user but remains in place for the script to use. Data stored in these hidden frames can be used by multiple Web pages during the user session or later. Also, when a user visits a Web site, the user may not be aware that there are scripts executing at the Web site. Hackers can use these loopholes to threaten the security of the user system.

One of the most essential useful areas in network performance when scripting plays a vital role is in the network client-server information exchange. This is done via a **Common Gateway Interface** or CGI. CGI is a standard to specify a data format that servers, browsers, and programs must use in order to exchange information. A program written in any language that uses this standard to exchange data between a Web server and a client's browser is a CGI script.

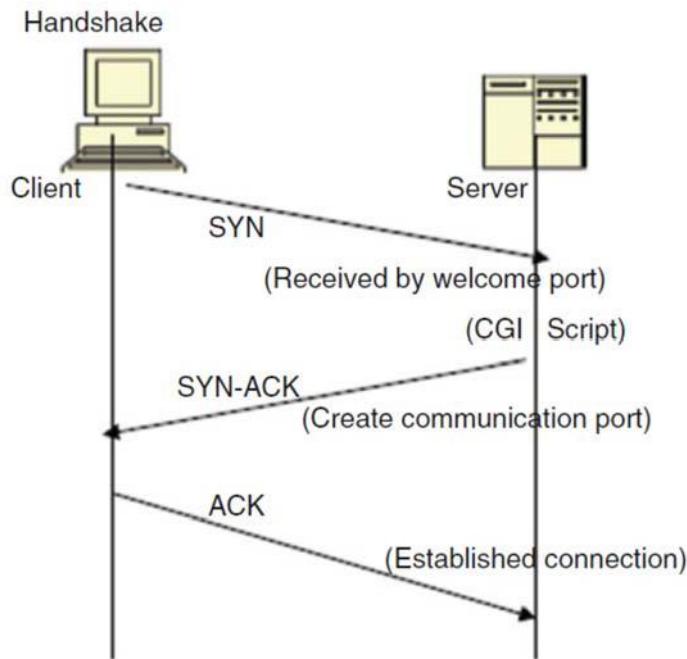


Figure 13 – The position of a CGI script in a three-way handshake.

However, hackers are constantly developing and testing a repertoire of their own scripts that will compromise other scripts wherever they are on the Web, in the computer network system or in applications. The most common of such hacker techniques today include Web cross-site scripting or XSS or CSS. Cross-site scripting allows attackers of Web sites to embed malicious scripts into dynamic unsuspecting Web and network scripts. Although this is a threat to most scripts, we will focus our script security discussion on the CGI scripts.

## Aim/Objectives

The scope of this week is for the student to underline how scripting has been used especially for an interactive Web in order to meet the growing demand of millions of Web services from users around the world. The student is not required to learn any scripting language although knowledge of scripting programming is a valuable and necessary asset for cybersecurity majors. However, scripting languages are taught in almost all computer science programs. One important aspect of scripting programming and especially for interactive web services is that they introduce a number of security threats as segments of code are executed in the client side. Therefore, the core of this week is for the student to fully understand how to best reduce the attack surface of the browser and harden it for maximum security and privacy. In

addition to this, the student will learn techniques showing how browsers are hacked and methods to mitigate all those attack vectors.

## Learning Outcomes

Upon successful completion of this course, students should be able to:

- Describe the type of scripting languages
- Describe scripting languages security threats
- Define web browsing vulnerabilities
- Apply protection measures for safer browsing
- Describe the differences between client-side and server-side scripting.
- Suggest ways to improve script security threats.
- Understand VBScript and explain why VBScript was not so popular.

## Key Words

Scripting languages	Server-side scripting	client-side scripting
Common Gateway Interface (CGI)	Web Script Security	Browser attack
JavaScript	VBScript	PHP

## Annotated Bibliography

### Basic

Guide to Computer Network Security, 4th Edition, Joseph Migga Kizza, 2017, DOI 10.1007/978-3-319-55606-2, Available to all EUC students via the <https://www.openathens.net/> service that is available to all EUC students. Related link: <https://www.springer.com/gp/book/9783319556055>

This week is based on the above eBook and more specifically in Chapter 6 pages 133-145. In this textbook an introduction is given for scripting languages and how scripting enabled the automation and dynamic growth of an interactive Web. Server-Side Scripting Languages are discussed and how web interactions such as maintaining a state, filling out forms; error checking or performing numeric calculation can be handled on the client's side. The most important part of this chapter is related not to scripting languages but to the security concerns and threats, they introduce.

## **Supplementary**

1. Power point presentation slides available in the platform
2. Which Web Programming Language is the Most Secure? Learn more on this [article](#).

## **Suggestions for further reading**

1. Network administrators have used scripting since long before Windows or even DOS came on the scene. UNIX administrators, for instance, have been using shell scripting and its powerful capabilities for decades. Scripting can significantly ease the burden of network administration. However, learning to create useful and effective scripts for networking tasks is not easy and requires a lot of patience and practice. Learn more about the role of scripting in network administration in this [article](#).

## **Self-Assessment Exercises**

### **Exercise 9.1**

What is a script program and its fundamental reference from compiled programs?

### **Exercise 9.2**

The most common CGI function is to fill in forms; the processing script actually takes the data input by the Web surfer and sends it as e-mail to the form administrator. Discuss the different ways such a process can fall victim to an attacker.

## **Recommended time for the student to work**

15 hours

## CLOUD COMPUTING TECHNOLOGY AND SECURITY

10<sup>th</sup> Week

### Summary

Cloud computing is an emerging technology. In this week, we will concentrate on this technology and investigate the main security risks associated with the cloud-computing infrastructure and services.

### Introductory Remarks

Cloud computing as a technology is difficult to define because it is evolving without a clear start point and no clear prediction of its future course. Even though this is the case, one can say that it is a continuous evolution of a computer network technology going beyond the client-server technology. It is a technology extending the realms of a computer network creating an environment that offers scalability, better utilization of hardware, on-demand applications and storage, and lower costs over the long run through the creation of virtual servers cloned from existing instances each offering near instantaneous increase in performance, allowing companies to react quickly and dynamically to emerging demands. The “cloud” or “cloud solution,” as the technology is commonly referred to, can either be hosted on-site by the company or off-site such as Microsoft, Amazon and Google cloud and any other cloud provider. The cloud technology seems to be in flux; hence, it may be one of the foundations of the next generation of computing. It may be in that in the next few years, a grid of a few cloud infrastructure may provide computing for millions of users. This is a broader view of cloud computing. Cloud computing technology consists of and rests on a number of sound, fundamental, and proven technologies including virtualization, service-oriented architectures, distributed computing, grid computing, broadband networks, Software as a Service, browser as a platform, free and open-source software, autonomic systems, Web application frameworks, and service-level agreements [1].

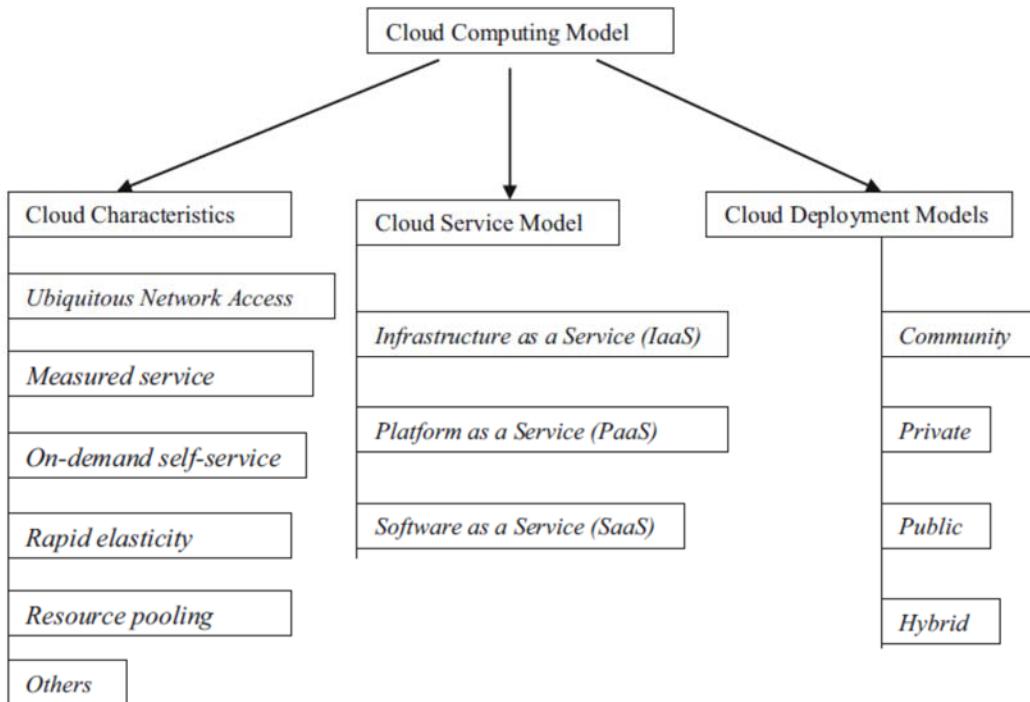


Figure 14 – Broad view of a cloud computing model.

First, let us start by trying to give a broad but specific view of the technology, what it is composed of, and how it works. We will start by a more specific definition given by the National Institute of Standards and Technology (NIST). According to NIST [1], cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources like networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction.

The cloud computing service models can be defined as follows:

**Infrastructure as a Service (IaaS):** The process of providing the customer with the ability and capability to manage and control, via a Web-based virtual server instance API, system resources such as starting, stopping, accessing, and configuring the virtual servers, operating systems, applications, storage, processing, and other fundamental computing resources is referred to as Infrastructure as a Service (IaaS).

**Platform as a Service (PaaS):** This is a set of software and product development tools hosted on the provider's infrastructure and accessible to the customer via a Web-based virtual server instance API.

**Software as a Service (SaaS):** Under this model, there is a different way of purchasing. Under SaaS, there is the elimination of the upfront license fee. All software applications are retained by the provider, and

the customer has access to all applications of choice from the provider via various client devices through either a thin client interface, such as a Web browser, a Web portal, or a virtual server instance API.

However, cloud services expose a number of concerns as the model as we know it today did not start overnight. The process has taken years moving through seven software models beginning with in-house software, licensed software normally referred to as the traditional model, open source, outsourcing, hybrid, Software as a Service, and finally the Internet model, the last two being part of the cloud computing model. When one carefully examines the cloud servicing model, one does not fail to notice the backward compatibilities or the carryovers of many of the attributes that characterized software through all the models. While this brings the benefits of each one of those software models, also many, if not all, of the software complexity and security issues in those models were carried over into the cloud computing model. Because of this, our first thought was to discuss the security issues in the cloud computing model through the prism of these models. It is tempting, but we are going to follow a different path while keeping the reader rooted into the different software models. Security is and continues to be a top issue in the cloud-computing model. The other three related issues are performance, compliance, and availability.

We want to start the discussion of cloud computing security by paraphrasing Greg Papadopoulos, CTO of Sun Microsystems, who said that cloud users normally “trust” cloud service providers with their data like they trust banks with their money. This means that they expect the three issues of security, availability, and performance to be of little concern to them as they are with their banks [3].

If we want to quickly summarize, the most important security concerns associated with cloud computing are as follows:

- Access control
- Security of Data and Applications in the Cloud
- Security of Data in Transition: Cloud Security Best Practices
- Data Encryption
- Web Access Point Security
- Compliance

## Aim/Objectives

The scope of this week is for the student to underline the main concept and the elements of cloud computing concept and its associated security risks. Cloud computing as concept and technology is very

board and dynamic. It is not, however, our scope to describe in detail cloud computing technologies but to provide an overview of these emerging technologies and the associated security risks. The student will be able to gain a greater knowledge on these topics by studying the current publications that are provided as supplementary study.

## Learning Outcomes

Upon successful completion of this course, students should be able to:

- Describe the main concept of cloud computing
- Define the cloud computing service models
- State the main security risks in cloud computing
- State the seven business models of software.
- Explain who are the main players in the cloud computing model

## Key Words

Cloud Security	Infrastructure as a Service	cloud computing service
availability	reliability	End-to-end security
Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)

## Annotated Bibliography

### Basic

Guide to Computer Network Security, 4th Edition, Joseph Migga Kizza, 2017, DOI 10.1007/978-3-319-55606-2, Available to all EUC students via the <https://www.openathens.net/> service that is available to all EUC students. Related link: <https://www.springer.com/gp/book/9783319556055>

This week is based on the above eBook and more specifically on Chapter 22 pages 477-500.

### Supplementary

1. Power point presentation slides available in the platform
2. European Union Agency for Network and Information Security (ENISA): [Cloud Security](#)
3. NIST: National Institute of Standards and Technology: [Cloud Security Automation Framework](#)

## Suggestions for further reading

- [1] Mell P, Grance T. The NIST definition of cloud computing, NIST special publication 800–145,  
<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

## Self-Assessment Exercises

### Exercise 10.1

How can you define the cloud-computing model?

### Exercise 10.2

What are the main security concerns associated with cloud computing?

## Activities

After you visit ENISA's portal try to identify the agency's related work in relation to the cloud computing security. Discuss the actions taken by the agency and list the most important publications in relation to cloud computing security.

## Recommended time for the student to work

20 hours

## INTERNET OF THINGS (IOT) SECURITY

11<sup>th</sup> Week

### Summary

This week we will discuss the emerging technology of Internet of Things (IoT). We will start first by taking a sharp look at the architecture and networking of IoT. We will then investigate the various security challenges and concerns of this technology and how major organizations such as ENISA address them by providing a number of implementation recommendations.

### Introductory Remarks

According to Wikipedia, the Internet of Things (IoT) is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these things to connect, collect and exchange data.

IoT involves extending Internet connectivity beyond standard devices, such as desktops, laptops, smartphones and tablets, to any range of traditionally dumb or non-internet-enabled physical devices and everyday objects. Embedded with technology, these devices can communicate and interact over the Internet, and they can be remotely monitored and controlled. With the arrival of driverless vehicles, a branch of IoT, i.e. the Internet of Vehicles starts to gain more attention.

The conceptual model and now what is forming in reality has the potential to impact our lives in many unprecedented ways both good and bad, as most technologies are.

The authors in [1] have defined the Internet of Things as a smart environment that is made up of an interconnection of sensing and actuating devices providing the ability to share information across platforms through a unified framework, developing a common operating picture for enabling innovative applications. This smart environment is achieved by seamless ubiquitous sensing, data analytics, and information representation with cloud computing as the unifying framework. It is this ecosystem described by P. Guillemin and P. Friess in their paper “Internet of things strategic research roadmap,” as part of the Cluster of European Research Projects [2]. Jacob Morgan [3] also sees it an environmental ecosystem that “allows for virtually endless opportunities and connections to take place, many of which

we can't even think of or fully understand the impact of today." Because it is going to affect our lives in every possible way, known and unknown in every sphere and dimension, it is in fact, as one scholar puts it, the new Industrial Revolution, again.

It's not hard to see how and why the IoT is such a hot topic today; it certainly opens the door to a lot of opportunities but also to many challenges. Security is a big issue that is oftentimes brought up. With billions of devices being connected together, what can people do to make sure that their information stays secure? Will someone be able to hack into your toaster and thereby get access to your entire network? The IoT also opens up companies all over the world to more security threats. Then we have the issue of privacy and data sharing. This is a hot-button topic even today, so one can only imagine how the conversation and concerns will escalate when we are talking about many billions of devices being connected.

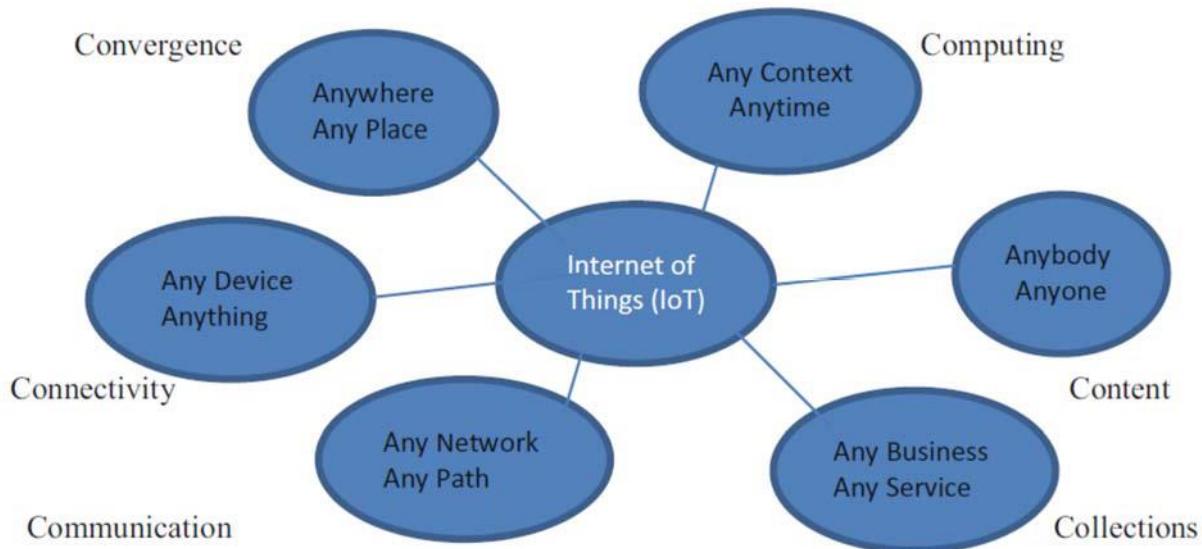


Figure 15 – Definition of Internet of Things (IoT) [1].

### Architecture and Networking of IoT

We have seen in the beginning of this week that IoT is defined as an interconnection of sensing, actuating, and communication digital devices providing the ability to share information across platforms through a unified framework, developing a common operating ecosystem (COE) for enabling innovative applications. For the IoT ecosystem to function and support intended applications and accommodate the

heterogeneity of devices and applications in the ecosystem, the IoT had to adopt the open standards of TCP/IP suite. However, the open standards of TCP/IP suite were initially developed for the wired global Internet several decades ago, as the networking solution. But, as we have outlined above in our discussion of IoT, there are fundamental differences between the traditional wired computer networks and the heterogeneous combination of wired and wireless device ecosystem. To get a good understanding of the IoT architectures and networking, we need to first understand the underlying network topology supported by the heterogeneous technologies, devices, and standards. The networking technology standard currently being used in the IoT falls into three categories (Figure 16):

1. point-to-point, for example, an end device to a gateway
- (2) star, with a gateway connected to several end devices by one hop links
- (3) a mesh, with one or more gateways connecting to several end devices one or more hop links away.

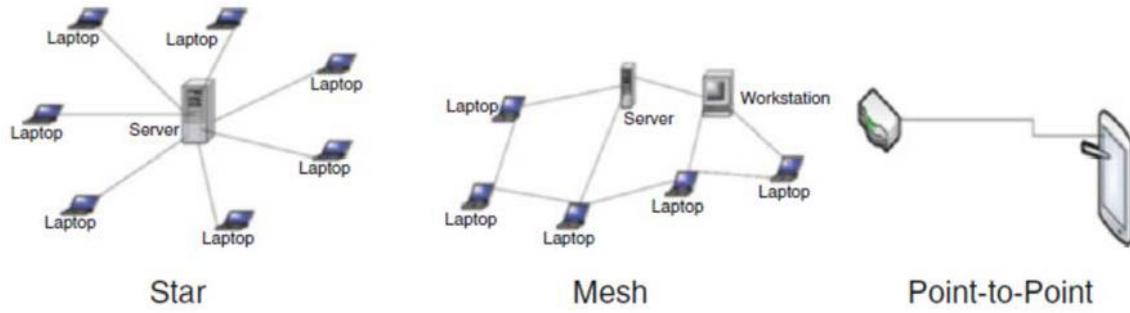


Figure 16 – Current IoT topologies

Based on these three topologies, we can cascade end devices and gateways to get a real model of the IoT communication network architecture as shown in Figure 17.

All IoT known technologies like Wi-Fi, Bluetooth, WiMax, ZigBee, Z-Wave, RFID, near-field communication (NFC), and others support this communication architecture.

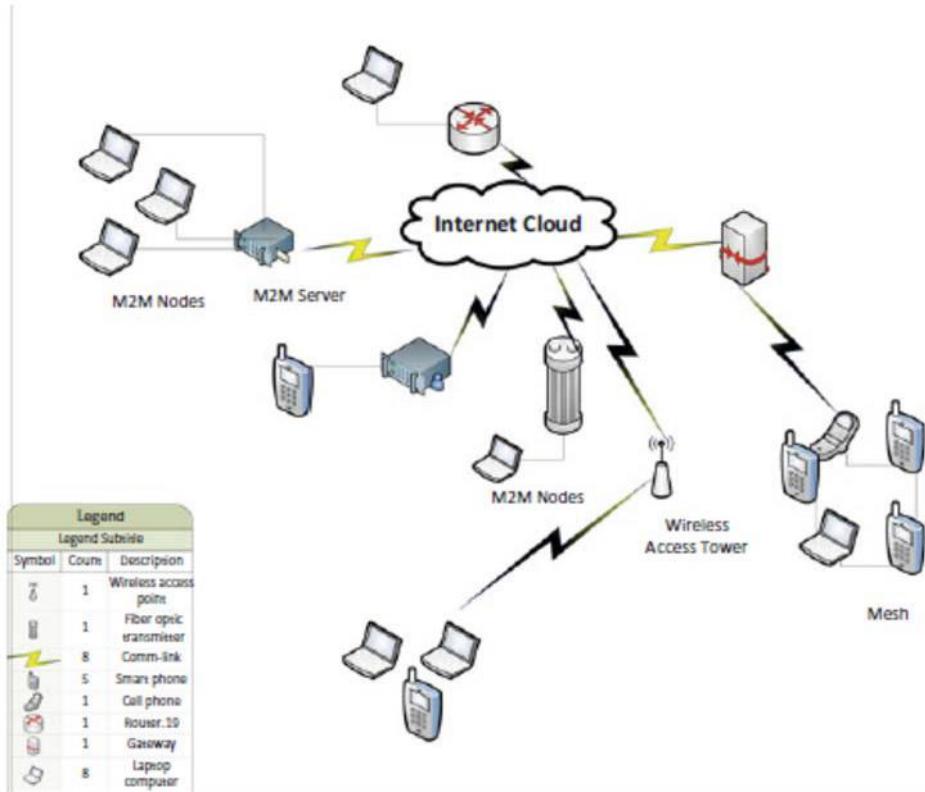


Figure 17 – IoT communication network architecture

### IoT Governance and Privacy

As we have pointed out throughout this chapter, an inherent characteristic of the IoT is its heterogeneity resulting from a plethora of things with different data communication capabilities like protocols and hardware, data rates, reliability, and others; computational, storage, and energy capabilities; diversity in the types and formats of data like audio, video, text, numeric, and streams; and IoT standards including device standards, standards to represent data, IEEE projects on IoT standards, ITU and ISO IoT standards, and others [12]. This diversity in devices, service, and protocols presents challenges unseen and unprecedented in the modern communication.

Let us see now, the issues related with the IoT governance. Globally, governance is mostly understood to refer to the rules, processes, and behavior that affect the way in which powers are exercised, particularly as regards openness, participation, accountability, effectiveness, and coherence [4]. These five principles of good governance have been already applied to the Internet for specific aspects, and there are already organizations like IETF, ICANN, RIRs, ISOC, IEEE, IGF, and W3C, which are each responsible and dealing with every specific area [4]. But currently this is not the case with the IoT. What this is pointing to is that

the governance of the current IoT possesses an array of problems for all those connected to the Internet, the most serious of which are security threats and attacks originating from and targeting both Internet-connected endpoints and data privacy risks posed by those same devices.

### **IoT Security Challenges**

Security is critical to IoT applications due to their close interaction with the physical world. In Internet communication, based on TCP/IP, IP has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers. For this purpose, IP defines packet structures that encapsulate the data to be delivered. It also defines addressing methods that are used to label the datagram with source and destination information. As a most widely used secure protocol in IP, TLS and its datagram variant DTLS are the main security protocols offering end-to-end secure communications between a server and client. TLS, with its two main constituent protocols, the handshake protocol, responsible for key exchange and authentication, and the record protocol, responsible for a secure channel for handling the delivery of data, makes the security of all IP-based communications a channel-based security. The secured-channel solutions, however, do not fit into the IoT environments for several reasons.

Based on the ENISA IoT high-level reference model and the interactions of its elements, we classify the security aspects of the IoT and Cloud convergence in the following three main categories:

- **Connectivity:** interactions and communications among endpoints, gateways and Cloud;
- **Analysis:** processing, filtering and aggregation of the data coming from the IoT devices in different levels of the IoT ecosystem;
- **Integration:** features that enable real-time bidirectional flow of data (e.g. Cloud APIs and remote command and control (C&C) of IoT devices through Cloud).

### **Aim/Objectives**

The scope of this week is for the student to underline the main concept and the elements of Internet of Things (IoT) concept and its associated security risks. IoT technology is very broad and dynamic. It is not, however, our scope to describe in detail the IoT technology but rather to provide an overview of these emerging technologies and the associated security risks. The student will be able to gain a greater knowledge on these topics by studying the current publications that are provided as supplementary study.

## Learning Outcomes

Upon successful completion of this course, students should be able to:

- Define the main concept of IoT.
- Describe the IoT architecture.
- State the main security risks in IoT networking.
- Define the main security challenges in IoT computing.
- Define the architecture and protocol stack of IoTs
- Study ENISA's baseline recommendations for IoT security.

## Key Words

Connectivity	Edge devices	IoT security
IoT architecture		End-to-end security

## Annotated Bibliography

### Basic

Guide to Computer Network Security, 4th Edition, Joseph Migga Kizza, 2017, DOI 10.1007/978-3-319-55606-2, Available to all EUC students via the <https://www.openathens.net/> service that is available to all EUC students. Related link: <https://www.springer.com/gp/book/9783319556055>

This week is based on the above eBook and more specifically on Chapter 24 pages 517-531.

### Supplementary

1. Power point presentation slides available in the platform
2. European Union Agency for Network and Information Security (ENISA):[Baseline Security Recommendations for IoT](#)
3. European Union Agency for Network and Information Security (ENISA):[Towards secure convergence of Cloud and IoT](#)

### Suggestions for further reading

[1] Gubbia J, et. al., Internet of Things (IoT): a vision, architectural elements, and future directions. Elsevier. <http://www.sciencedirect.com/science/article/pii/S0167739X13000241>

[2] Guillemin P, Friess P., Internet of things strategic research roadmap. The Cluster of European Research Projects, Tech. Rep., September 2009.

[http://www.internet-of-things-research.eu/pdf/IoT\\_Cluster\\_Strategic\\_Research\\_Agenda\\_2009.pdf](http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2009.pdf)

[3] Morgan J. A simple explanation of ‘the internet of things’

<http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#5939c9768284>

[4] IERC. Internet of things IoT governance, privacy and security issues. European research cluster on the internet of things January 2015.

## Self-Assessment Exercises

### Exercise 11.1

Globally, governance is mostly understood to refer to the rules, processes, and behavior that affect the way in which powers are exercised, particularly as regards openness, participation, accountability, effectiveness, and coherence. These five principles of good governance have been already applied to the Internet for specific aspects, and there are already organizations like IETF, ICANN, RIRs, ISOC, IEEE, IGF, and W3C, which are each responsible and dealing with every specific area. Explain why this is not the case with the IoT?

### Exercise 11.2

How ENISA classifies the main security aspects of the IoT and Cloud convergence?

## Recommended time for the student to work

15 hours

## INTRUSION DETECTION AND PREVENTION

12<sup>th</sup> Week

### Summary

This week we will discuss network and host-based intrusion detection and prevention mechanisms. The concept of intrusion detection, and its processes will be presented following with a description of the Intrusion Detection Systems (IDS). The two types of IDSs will be described namely the Network-based Intrusion Detection Systems (NIDSs) and Host-based Intrusion Detection Systems (NIDSs) so that the student will be able to identify the main differences between them.

### Introductory Remarks

The psychology and politics of ownership have historically dictated that individuals and groups tend to protect valuable resources. This grew out of the fact that once a resource has been judged to have value, no matter how much protection given to it, there is always a potential that the security provided for the resource will at some point fail. This notion has driven the concept of system security and defined the disciplines of computer and computer network security. Computer network security is made up of three principles: i) prevention, ii) detection, and iii) response. Although these three are fundamental ingredients of security, most resources have been devoted to detection and prevention because if we are able to detect all security threats and prevent them, then there is no need for response.

**Intrusion detection is a technique of detecting unauthorized access to a computer system or a computer network.** An intrusion into a system is an attempt by an outsider to the system to illegally gain access to the system. **Intrusion prevention, on the other hand, is the art of preventing an unauthorized access of a system's resources.** The two processes are related in a sense that while intrusion detection passively detects system intrusions, intrusion prevention actively filters network traffic to prevent intrusion attempts. For the rest of the week, let us focus on these two processes.

The notion of intrusion detection in computer networks comes from a 1980 James Anderson's paper, "Computer Security Threat Monitoring and Surveillance." In that paper [1], Anderson noted that computer audit trails contained vital information that could be valuable in tracking misuse and understanding user

behavior. The paper, therefore, introduced the concept of “detecting” misuse and specific user events and has prompted the development of intrusion detection systems.

An intrusion is a deliberate unauthorized attempt, successful or not, to break into, access, manipulate, or misuse some valuable property and where the misuse may result into or render the property unreliable or unusable. The person who intrudes is an intruder.

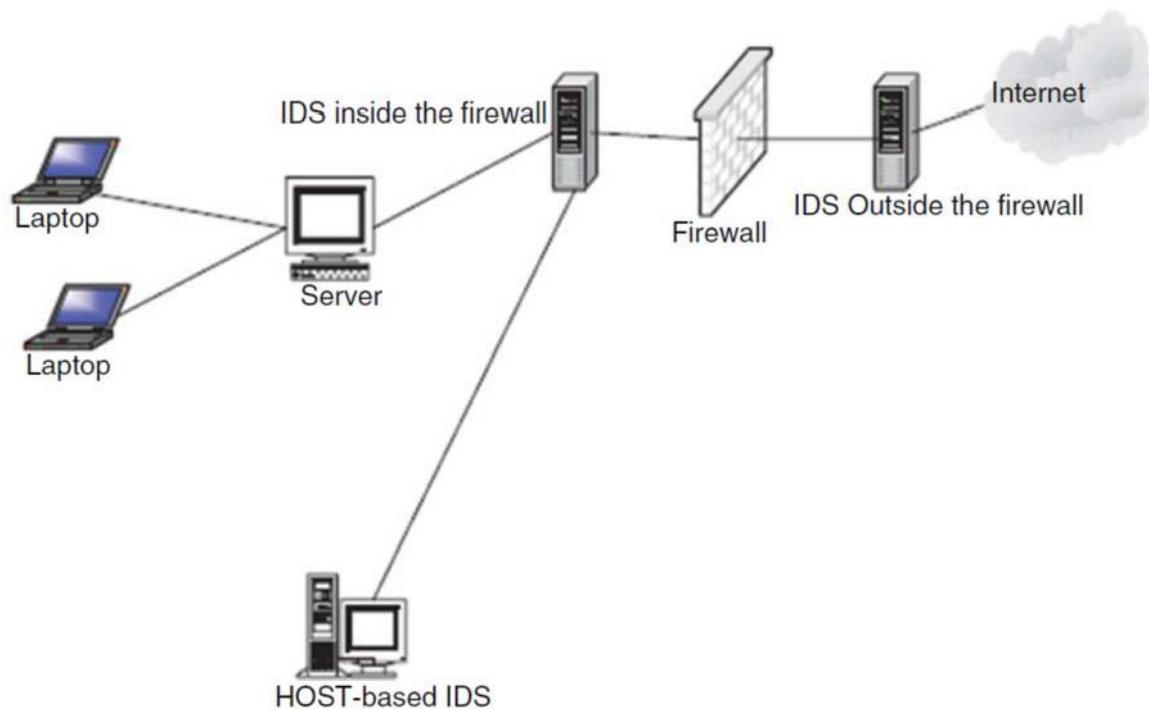


Figure 18 – The architecture of a network-based intrusion detection system.

Aurobindo Sundaram [2] divides intrusions into six types as follows:

- Attempted break-ins, which are detected by atypical behavior profiles or violations of security constraints. An intrusion detection system for this type is called anomaly-based IDS. Masquerade attacks, which are detected by atypical behavior profiles or violations of security constraints. These intrusions are also detected using anomaly-based IDS.
- Penetrations of the security control system, which are detected by monitoring for specific patterns of activity.
- Leakage, which is detected by atypical use of system resources.
- Denial of service, which is detected by atypical use of system resources.

- Malicious use, which is detected by atypical behavior profiles, violations of security constraints, or use of special privileges.

The intrusion process into a system includes a number of stages that start with the identification of the target, followed by reconnaissance that produces as much information about the target as possible. After enough information is collected about the target and weak points are mapped, the next job is to gain access into the system and finally the actual use of the resources of the system. The intrusion process consists of the following stages:

- **Reconnaissance**
- **Physical Intrusion**
- **Denial of Service**

In order to detect intrusion a number of tools are used, with the most common that is called an “Intrusion Detection System (IDS)”. The IDS is a system used to detect unauthorized intrusions into computer systems and networks. As technology has developed, a whole new industry based on intrusion detection has sprung up. Security firms are cropping up everywhere to offer individual and property security—to be a watchful eye so that the property owner can sleep or take a vacation in peace. These new systems have been made to configure changes, compare user actions against known attack scenarios, and be able to predict changes in activities that indicate and can lead to suspicious activities. There are six subdivisions of system intrusions. These six can now be put into three models of intrusion detection mechanisms: i) anomaly-based detection, ii), signature-based detection, and iii) hybrid detection.

Intrusion detection systems are also classified based on their monitoring scope. There are those that monitor only a small area and those that can monitor a wide area. Those that monitor a wide area are known as network-based intrusion detection, and those that have a limited scope are known as host-based detections.

The response to System Intrusion is relative to the type of attack. Some attacks do not require responses; others require a precautionary response. Yet others need a rapid and forceful response. For the most part, a good response must consist of preplanned defensive measures that include an incident response team and ways to collect IDS logs for future use and for evidence when needed.

Although IDS have been one of the cornerstones of network security, they have covered only one component of the total network security picture. They have been, and they are a passive component which only detects and reports without preventing. A promising new model of intrusion is developing and

picking up momentum. It is the intrusion prevention system (IPS), which according to Andrew Yee [10] is to prevent attacks. Like their counterparts, the IDS, IPS fall into two categories: network based, and host based.

The Network-Based Intrusion Prevention Systems (NIPSS) are passively detecting intrusions into the network without preventing them from entering the networks, many organizations in recent times have been bundling up IDS and firewalls to create a model that can detect and then prevent.

Host-Based Intrusion Prevention Systems (HIPSs) work by sandboxing, a process of restricting the definition of acceptable behavior rules used on HIPSs. HIPS prevention occurs at the agent residing at the host.

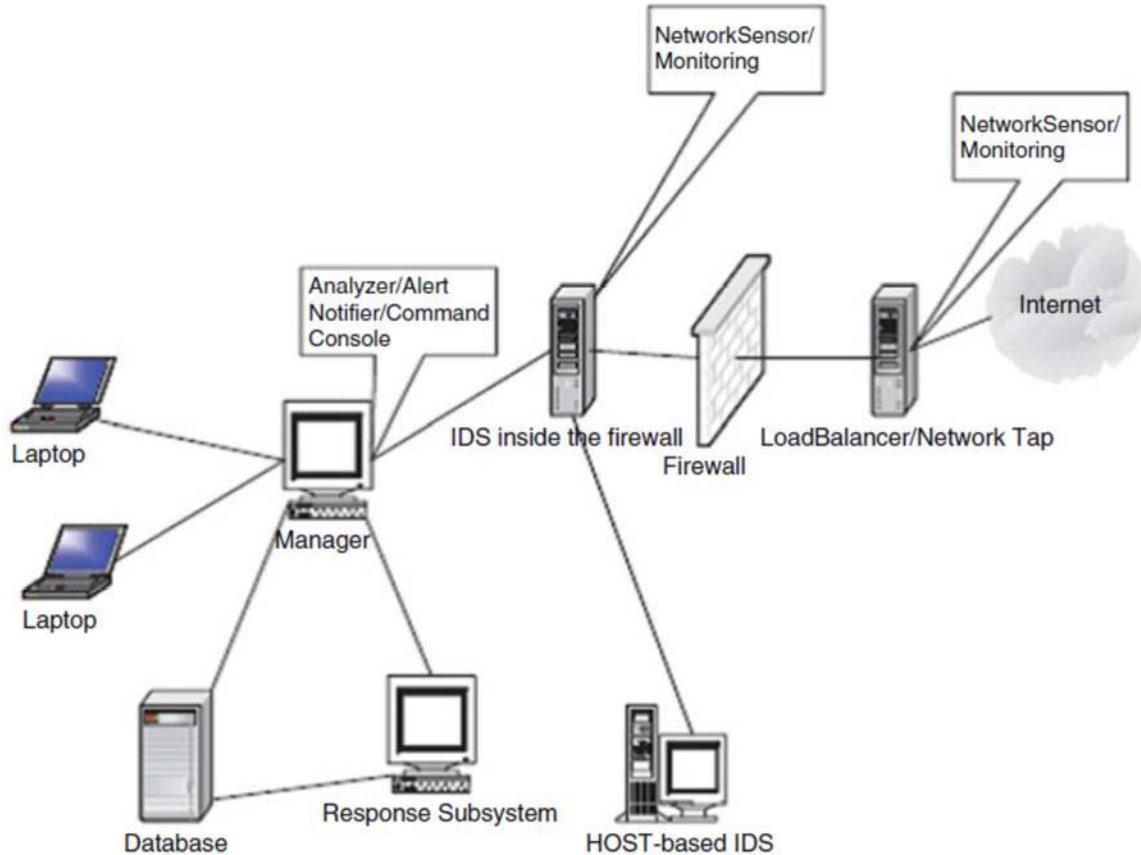


Figure 19 – The various places of placing the IDS sensors.

## Aim/Objectives

The scope of this week is for the student to express the network and host-based intrusion detection and prevention mechanisms. The concept of intrusion detection, and its processes will be presented following with a description of the Intrusion Detection Systems (IDS). The two types of IDSs will be described namely the Network-based Intrusion Detection Systems (NIDSs) and Host-based Intrusion Detection Systems (NIDSs) so that the student will be able to identify the main differences between them. After the study of the IDS we will discuss how we can address intrusion in our network with the use of Intrusion Prevention Systems (IPSs). The two main IPSs will be discussed focusing mainly into the Network-based Intrusion Prevention Systems (NIPPs). Along with the above theoretical foundation a number of experiments as self-study will provide the student with more tangible results by using free tools. The student will be able to monitor his network and understand how to find and detect hackers and malware and stop protocol leaks.

## Learning Outcomes

Upon successful completion of this course, students should be able to:

- State the concept of Intrusion detection in computer networks
- State the intrusion process into a system
- Classify the various types of Intrusion Detection Systems (IDS)
- State the concept of Intrusion Prevention Systems (IPS)
- Classify the various types of Intrusion Prevention Systems
- Practice with Intrusion Detection and Intrusion Prevention tools

## Key Words

Intrusion Detection Systems (IDS)	Intrusion Prevention (IPS)	Network-Based Intrusion Detection Systems (NIDSs)
Network-Based Intrusion Prevention Systems (NIPPs)	Host-Based Intrusion Prevention Systems (HIPSs)	Host-Based Intrusion Detection Systems (HIDS)
Parasitic Grids	Best Practices	WiMAX

## Annotated Bibliography

## **Basic**

Guide to Computer Network Security, 4th Edition, Joseph Migga Kizza, 2017, DOI 10.1007/978-3-319-55606-2, Available to all EUC students via the <https://www.openathens.net/> service that is available to all EUC students. Related link: <https://www.springer.com/gp/book/9783319556055>

This week is based on the above eBook and more specifically in Chapter 13 pages 275-300. This chapter provides an overview on the concept of intrusion detection and the classification of the various types of Intrusion Detection Systems (IDS). The challenges related to the implementation of IDS are explained with the main one related to the perception that IDS is not the cure of all computer network ills. The emphasis is also given to Intrusion Prevention Systems (IPS) that protect our network and prevent from attacks and malicious insiders. Another one objective this week is the course exercises that the student will conduct with a number of related free tools in order to get at first sight a better understanding of IDS and IPS, their use and limitations.

## **Supplementary**

1. Power point presentation slides available in the platform

**2. Wireshark - Brief description**

Wireshark is a free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on Linux, OS X, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows. There is also a terminal-based (non-GUI) version called TShark. Wireshark, and the other programs distributed with it such as TShark, are free software, released under the terms of the GNU General Public License.

Website: <https://www.wireshark.org/>

Price: Free (possibly needing to add additional network cards at around €50 each or the AirPcap USB dogle for wireless networks, if required, at around \$700 each).

**3. Snort - Brief description**

Snort's open source network-based intrusion detection system (NIDS) has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks. Snort performs protocol analysis, content searching and matching. These basic services have many purposes including application-aware

triggered quality of service, to de-prioritize bulk traffic when latency-sensitive applications are in use. The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, common gateway interface, buffer overflows, server message block probes, and stealth port scans. Snort can also perform IPS functions.

Website: <https://www.snort.org/>

Price: Free

Dependencies: None – it can be installed on single machines.

#### **Malware Defender - Brief description**

Malware Defender is a HIPS (Host Intrusion Prevention System) with firewall. It is effective to protect your computer system from all forms of malware (viruses, worms, trojans, adware, spyware, keyloggers, rootkits). Malware Defender is also an advanced rootkit detector. It provides many useful tools that can be used to detect and remove already installed malware. Added support for adding child application rules, driver rules, hook module rules, file rules and registry rules to member of application group, added an option to allow running user specified applications if no explicit 'deny' rule is found, added a new choice of rule object to the Alert dialog and other improvements.

Website: <https://www.snort.org/>

Price: Free Trial

Dependencies: None – it can be installed on single machines.

#### **Suricata - Brief description**

Suricata is a free and open source, mature, fast and robust network threat detection engine. The Suricata engine is capable of real time intrusion detection (IDS), inline intrusion prevention (IPS), network security monitoring (NSM) and offline pcap processing. Suricata inspects the network traffic using a powerful and extensive rules and signature language and has powerful Lua scripting support for detection of complex threats. With standard input and output formats like YAML and JSON integrations with tools like existing SIEMs, Splunk, Logstash/Elasticsearch, Kibana, and another database become effortless. Suricata's fast paced community driven development focuses on security, usability and efficiency. The Suricata project and code is owned and supported by the Open Information Security Foundation (OISF), a non-profit foundation committed to ensuring Suricata's development and sustained success as an open source project.

Website: <https://suricata-ids.org/>

Price: Free

Dependencies: None – it can be installed on single machines.

#### **Open Source Host-based Intrusion Detection System (HIDS) - Brief description**

OSSEC is a scalable, multi-platform, open source Host-based Intrusion Detection System (HIDS). It has a powerful correlation and analysis engine, integrating log analysis, file integrity checking, Windows registry monitoring, centralized policy enforcement, rootkit detection, real-time alerting and active response. It runs on most operating systems, including Linux, OpenBSD, FreeBSD, MacOS, Solaris and Windows.

Website: <http://www.ossec.net/index.html>

Price: Free

Dependencies: None – it can be installed on single machines.

#### **Suggestions for further reading**

[1] J. P. Anderson, “Computer Security Threat Monitoring and Surveillance,” James P. Anderson Co., Fort Washington, 1980.

[2] Sundaram A., An introduction to intrusion detection, ACM Digital Library. <http://dl.acm.org/citation.cfm?id=332161>

### **Self-Assessment Exercises**

#### **Exercise 9.1**

What is Intrusion detection? How it is related to intrusion prevention?

#### **Exercise 9.2**

Can you define the three stages of an intrusion process?

### **Group Assignment: Packet Inspection with Wireshark (20 points)**

Wireshark is a free and open source packet analyzer. In your home computer use Wireshark to capture packets that are destined to and sourced from your computer. We suggest you to capture the packets over the time of few seconds.

A quick tutorial on how to install and capture packets is provided in this [link](#).

After you run Wireshark and capture a number of packets examine the following:

1. Identify your internal IP address by running either *ipconfig* (Windows) or *ifconfig* (Linux).
2. Check all the TCP and UDP packets and identify the source and the destination address.
3. Identify the port number for each packet for both TCP and UDP.
4. Check to see known vulnerabilities associated with the specific port numbers by using an online Database (<https://www.speedguide.net/ports.php> ).
5. Identify either the source or destination of each TCP and UDP packet by using an online [IP Lookup Tool](#).

Take some screenshots to prove your findings, report the results and provide justification of your findings.

### **Recommended time for the student to work**

40 hours

## PROTECTING MEASURES - FIREWALLS

13<sup>th</sup> Week

### Summary

This week we will see how the network can be protected with the use of a special security component (firewalls). We will also what threats each firewall can mitigate and most important what threats they do not protect us from.

### Introductory Remarks

The rapid growth of the Internet has led to a corresponding growth of both users and activities in cyberspace. Unfortunately, not all these users and their activities are reputable; thus, the Internet has been increasingly, at least to many individuals and businesses, turning into a “bad Internet.” Bad people are plowing the Internet with evil activities that include, among other things, intrusion into company and individual systems looking for company data and individual information that erodes privacy and security. There has, therefore, been a need to protect company systems, and now individual Personal Computers (PCs), keeping them out of access from those “bad users” out on the “bad Internet.” As companies build private networks and decide to connect them onto the Internet, network security becomes one of the most important concerns network system administrators face. In fact, these network administrators are facing threats from two fronts: the external Internet and the internal users within the company network. Therefore, network system administrators must be able to find ways to restrict access to the company network or sections of the network from both the “bad Internet” outside and from unscrupulous inside users.

Such security mechanisms are based on a firewall. **A firewall is a hardware, a software, or a combination of both that monitors and filters traffic packets that attempt to either enter or leave the protected private network.** It is a tool that separates a protected network or part of a network, and now increasingly a user PC, from an unprotected network—the “bad network” like the Internet. In many cases the “bad network” may even be part of the company network. By definition, a “firewall,” is a tool that provides a filter of both incoming and outgoing packets.

Most firewalls perform two basic security functions:

- Packet filtering based on accept or deny policy that is itself based on rules of the security policy.
- Application proxy gateways that provide services to the inside users and at the same time protect each individual host from the “bad” outside users.

By denying a packet, the firewall actually drops the packet. In modern firewalls, the firewall logs are stored into log files, and the most urgent or dangerous ones are reported to the system administrator. This reporting is slowly becoming real time.

In its simplest form, a firewall can be implemented by any device or tool that connects a network or an individual PC to the Internet. For example, an Ethernet bridge or a modem that connects to the “bad network” can be set as a firewall. Most firewall products actually offer much more as they actively filter packets from and into the organization network according to certain established criteria based on the company security policy. Most organization firewalls are bastion host, although there are variations in the way this is set up. A bastion host is one computer on the organization network with bare essential services, designated and strongly fortified to withstand attacks. This computer is then placed in a location where it acts as a gateway or a choke point for all communication into or out of the organization network to the “bad network.” This means that every computer behind the bastion host must access the “bad network” or networks through this bastion host.

For most organizations, a firewall is a network perimeter security, a first line of defense of the organization’s network that is expected to police both network traffic inflow and outflow. This perimeter security defense varies with the perimeter of the network. For example, if the organization has an extranet, an extended network consisting of two or more LAN clusters, or the organization has a virtual private network (VPN), then the perimeter of the organization’s network is difficult to define.

As we pointed out earlier, the accept/deny policy used in firewalls is based on an organization’s security policy. The security policies most commonly used by organizations vary ranging from completely disallowing some traffic to allowing some of the traffic or all the traffic. These policies are consolidated into two commonly used **firewall security policies** [1]:

- Deny-everything-not-specifically-allowed which sets the firewall in such a way that it denies all traffic and services except a few that are added as the organization needs develop.
- Allow-everything-not-specifically-denied which lets in all the traffic and services except those on the “forbidden” list which is developed as the organization’s dislikes grow.

Based on these policies, the following design goals are derived:

- All traffic into and out of the protected network must pass through the firewall.
- Only authorized traffic, as defined by the organizational security policy, in and out of the protected network, will be allowed to pass.
- The firewall must be immune to penetration by use of a trusted system with secure operating system.

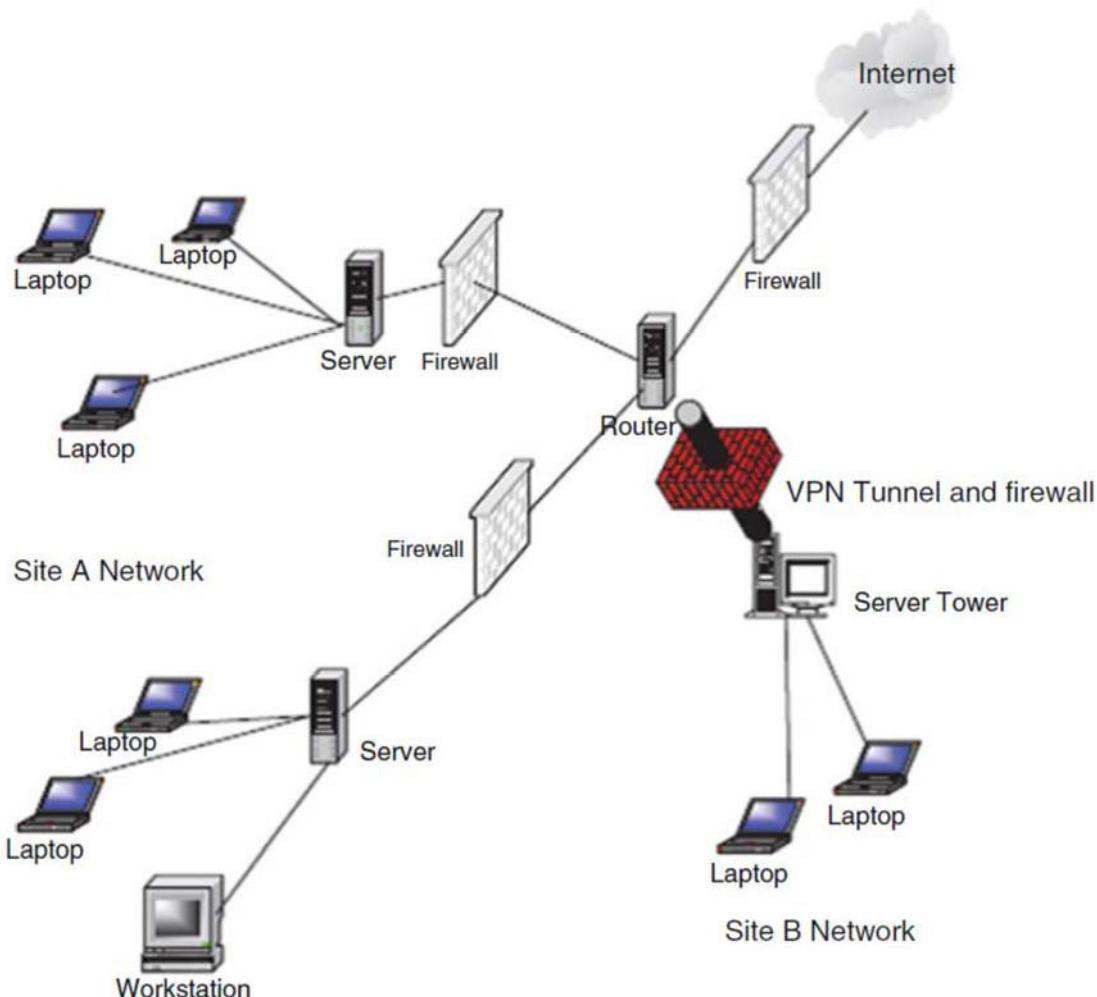


Figure 20 – Firewalls in a changing parameter security.

There are basically two types of firewalls. **The first type is the packet inspection or filtering router.** This type of firewall uses a set of rules to determine whether to forward or block individual packets. A packet inspection router could be a simple machine with multiple network interfaces or a sophisticated one with

multiple functionalities. **The second type is the application inspection or proxy server.** The proxy server is based on specific application daemons to provide authentication and to forward packets.

## Aim/Objectives

The scope of this week is twofold. i) to introduce the student the theoretical foundation for understanding how the network can be protected with the use of a special security component (firewalls), and ii) to practice with virtual, network and host-based firewalls. The student will be able after the study of this week to classify what threats each firewall can mitigate and most important what threats they do not protect us from. The students will have a solid understanding of the best available firewalls across the platforms including the usual Windows and Linux machines.

## Learning Outcomes

Upon successful completion of this course, students should be able to:

- State what is the firewall and its importance in network security.
- State the main policies for a firewall set up
- State the main types of firewalls
- Practice with available firewalls to better understand its set up
- Make use of network protecting measures

## Key Words

Firewall	accept/deny policy	Inflow and outflow traffic
The Demilitarized Zone (DMZ)	Packet inspection	authorized traffic

## Annotated Bibliography

### Basic

Guide to Computer Network Security, 4th Edition, Joseph Migga Kizza, 2017, DOI 10.1007/978-3-319-55606-2, Available to all EUC students via the <https://www.openathens.net/> service that is available to all EUC students. Related link: <https://www.springer.com/gp/book/9783319556055>

This week is based on the above eBook and more specifically in Chapter 12 pages 251-274. This chapter provides a detailed guidance on the various types of firewalls and explains in which way firewalls can

protect the network from attacks. It also describes the concept of the Demilitarized Zone (DMZ) and how DMA is providing some insulation and extra security to servers that provide the organization services for protocols such as HTTP/ SHTTP, FTP, DNS, and SMTP to the general public. In addition to this a number of free resources available online are offered to the students for further study and practical exercises.

### **Supplementary**

Power point presentation slides available in the platform.

Video: [What is a Firewall? : Cisco ASA Firewall Tutorial](#)

Video: [Configuring Windows Firewall](#)

### **Suggestions for further reading**

1. Windows Firewall Control is a powerful tool which extends the functionality of Windows Firewall and provides new extra features which makes Windows Firewall better. It runs in the system tray and allows the user to control the native firewall easily without having to waste time by navigating to the specific part of the firewall. This is the best tool to manage the native firewall from Windows 10, 8.1, 8, 7, Server 2016, Server 2012. Read more on this [site](#).
2. An *Iptables* tutorial can be find in this [site](#)
3. If you want to set up your own Personal firewall for your laptop using iptables & ipv6tables, then use the sources in [GitHub](#)

## **Self-Assessment Exercises**

### **Exercise 13.1**

What is a firewall and its main functions?

### **Exercise 13.2**

What are the common security policies posed by a firewall?

## **Recommended time for the student to work**

15 hours

## **STUDY WEEK AND FINAL EXAMS**

The final examination will consist of true/false, multiple-choice questions and a small number of questions

### **Recommended time for the student to work**

40 hours

**Date/Time of Final Exam: TBD**

## ANSWERS TO REVIEW QUESTIONS

### INTRODUCTION TO COMPUTER NETWORKING – 1<sup>st</sup> Week

#### Exercise 1.1

Application Layer: HTTP, FTP, SMTP, SNMP

Transport Layer: TCP, UDP

Network layer: IP, ICMP

Datalink layer: Ethernet, ARP, 802.11

#### Exercise 1.2

In wireless networking We can identify the following elements:

- **Wireless hosts.** As in the case of wired networks, hosts are the end-system devices that run applications. A wireless host might be a laptop, palmtop, smartphone, or desktop computer. The hosts themselves may or may not be mobile.
- **Wireless links.** A host connects to a base station (defined below) or to another wireless host through a wireless communication link. Different wireless link technologies have different transmission rates and can transmit over different distances.
- **Base station.** The base station is a key part of the wireless network infrastructure. Unlike the wireless host and wireless link, a base station has no obvious counterpart in a wired network. A base station is responsible for sending and receiving data (e.g., packets) to and from a wireless host that is associated with that base station.

### COMPUTER NETWORK SECURITY FUNDAMENTALS – 2<sup>nd</sup> Week

#### Exercise 2.1

This state of security can be guaranteed if the following four protection mechanisms are in place: deterrence, prevention, detection, and response [1, 2].

- **Deterrence** is usually the first line of defense against intruders who may try to gain access. It works by creating an atmosphere intended to frighten intruders. Sometimes this may involve warnings of severe consequences if security is breached.

- **Prevention** is the process of trying to stop intruders from gaining access to the resources of the system. Barriers include firewalls, demilitarized zones (DMZs), and the use of access items like keys, access cards, biometrics, and others to allow only authorized users to use and access a facility.
- **Detection** occurs when the intruder has succeeded or is in the process of gaining access to the system. Signals from the detection process include alerts to the existence of an intruder. Sometimes, these alerts can be real time or stored for further analysis by the security personnel.
- **Response** is an aftereffect mechanism that tries to respond to the failure of the first three mechanisms. It works by trying to stop and/or prevent future damage or access to a facility.

### **Exercise 2.2**

Information security, often referred to as InfoSec, refers to the processes and tools designed and deployed to protect sensitive business information from modification, disruption, destruction, and inspection.

## **SECURITY IN WIRELESS NETWORKS AND DEVICES – 3<sup>rd</sup> Week**

### **Exercise 3.1**

The evolving security architecture consists of the following five components:

- **Security associations:** A context to maintain the security state relevant to a connection between a base station (BS) and a subscriber station (SS).
- **Certificate profile**—X.509 to identify communication parties to each other.
- **PKM authorization**—authorization protocol to distribute an authorization token to an authorized SS.
- **Privacy and key management**—a protocol to rekey the security association (SA).
- **Encryption**—payload field encryption using Data Encryption Standard (DES) algorithm in the Cipher Block Chaining (CBC) mode of operation in 802.16d, DES-CBC, and Advanced Encryption Standard-Counter with Cipher Block Chaining-Message Authentication Code (AES-CCM) in 802.16e.

### **Exercise 3.2**

This is judgement question and the student is free to justify his answer.

## CYBER CRIMES AND HACKERS – 4<sup>th</sup> Week

### Exercise 4.1

A cybercrime is a crime like any other crime, except that in this case, the illegal act must involve a connected computing system as either an object of a crime, an instrument used to commit a crime, or a repository of evidence related to a crime.

## COMPUTER NETWORK SECURITY PROTOCOLS – 5<sup>th</sup> Week

### Exercise 5.1

**Application-level security:** (for TCP/IP) and application and presentation (for ISO)—RADIUS, TACACS, PGP, S/MIME, S-HTTP, HTTPS, SET, SSH, and Kerberos

- **Transport-level security:** (for TCP/IP) and session and transport (for ISO)—SSL and TLS
- **Network-level security:** for both TCP/IP and ISO—PPTP, L2TP, IPsec, and VPNs
- **Physical link-level security:** (for TCP/IP) and data link and physical (for ISO)— packet filters, NAT, CHAP, and PAP.

### Exercise 5.2

This is judgement question and the student is free to justify his answer.

## AUTHENTICATION – 6<sup>th</sup> Week

### Exercise 6.1

Generally, authentication requires the presentation of credentials or items of value to really prove the claim of who you are. The items of value or credential are based on several unique factors that show something you know, something you have, or something you are:

- **Something you know:** This may be something you mentally possess. This could be a password, a secret word known by the user and the authenticator. Although this is inexpensive administratively, it is prone to people's memory lapses and other weaknesses including secure storage of the password files by the system administrators. The user may use the same password

on all system logons or may change it periodically, which is recommended. Examples using this factor include passwords, passphrases, and personal identification numbers (PINs).

- **Something you have:** This may be any form of issued or acquired self-identification such as:
  - **SecurID**
  - **CryptoCard**
  - **ActivCard**
  - **SafeWord**
  - **Many other forms of cards and tags**

This form is slightly safer than something you know because it is hard to abuse individual physical identifications. For example, it is harder to lose a smart card than to remember the card number.

**Something you are:** This is a naturally acquired physical characteristic such as voice, fingerprint, iris pattern, and other biometrics.

### Exercise 6.2

In general, authentication takes one of the following three forms:

- **Basic authentication involving a server.** The server maintains a user file of either passwords and usernames or some other useful piece of authenticating information. This information is always examined before authorization is granted. This is the most common way computer network systems authenticate users. It has several weaknesses though, including forgetting and misplacing authenticating information such as passwords.
- **Challenge-response,** in which the server or any other authenticating system generates a challenge to the host requesting for authentication and expects a response.
- **Centralized authentication,** in which a central server authenticates users on the network and in addition also authorizes and audits them. These three processes are done based on server action. If the authentication process is successful, the client seeking authentication is then authorized to use the requested system resources. However, if the authentication process fails, the authorization is denied. The process of auditing is done by the server to record all information from these activities and store it for future use.

## MALICIOUS SOFTWARE – 7<sup>th</sup> Week

### Exercise 7.1

This is judgement question and the student is free to justify his answer.

### **Exercise 7.2**

This is judgement question and the student is free to justify his answer.

## **COMPUTER NETWORK VULNERABILITIES -8<sup>th</sup> Week**

### **Exercise 8.1**

Most vulnerability assessment services will provide system administrators with:

- Network mapping and system fingerprinting of all known vulnerabilities
- A complete vulnerability analysis and ranking of all exploitable weaknesses based on potential impact and likelihood of occurrence for all services on each host
- Prioritized list of misconfigurations

## **SCRIPTING AND SECURITY – 9<sup>th</sup> Week**

### **Exercise 9.1**

**A program script is a logical sequence of line commands which causes the computer to accomplish some task.** Many times, we refer to such code as macros or batch files because they can be executed without user interaction. A script language is a programming language through which you can write scripts. Scripts can be written in any programming language or a special language as long as they are surrogated by another program to interpret and execute them on the fly by a program unlike compiled programs that are run by the computer operating system.

### **Exercise 9.2**

This is judgement question and the student is free to justify his answer.

## CLOUD COMPUTING TECHNOLOGY AND SECURITY -10<sup>th</sup> Week

### Exercise 10.1

The cloud computing service models can be defined as follows:

**Infrastructure as a Service (IaaS):** The process of providing the customer with the ability and capability to manage and control, via a Web-based virtual server instance API, system resources such as starting, stopping, accessing, and configuring the virtual servers, operating systems, applications, storage, processing, and other fundamental computing resources is referred to as Infrastructure as a Service (IaaS).

**Platform as a Service (PaaS):** This is a set of software and product development tools hosted on the provider's infrastructure and accessible to the customer via a Web-based virtual server instance API.

**Software as a Service (SaaS):** Under this model, there is a different way of purchasing. Under SaaS, there is the elimination of the upfront license fee. All software applications are retained by the provider, and the customer has access to all applications of choice from the provider via various client devices through either a thin client interface, such as a Web browser, a Web portal, or a virtual server instance API.

### Exercise 10.2

The security concerns associated with cloud computing can be summarized as follows:

- Access control
- Security of Data and Applications in the Cloud
- Security of Data in Transition: Cloud Security Best Practices
- Data Encryption
- Web Access Point Security
- Compliance

## INTERNET OF THINGS (IOT) SECURITY – 11<sup>th</sup> Week

### Exercise 11.2

This is judgement question and the student is free to justify his answer.

### Exercise 11.2

Based on the ENISA IoT high-level reference model and the interactions of its elements, we classify the security aspects of the IoT and Cloud convergence in the following three main categories:

- **Connectivity**: interactions and communications among endpoints, gateways and Cloud;
- **Analysis**: processing, filtering and aggregation of the data coming from the IoT devices in different levels of the IoT ecosystem;
- **Integration**: features that enable real-time bidirectional flow of data (e.g. Cloud APIs and remote command and control (C&C) of IoT devices through Cloud).

## INTRUSION DETECTION AND PREVENTION – 12<sup>th</sup> Week

### Exercise 12.1

**Intrusion detection** is a technique of detecting unauthorized access to a computer system or a computer network. An intrusion into a system is an attempt by an outsider to the system to illegally gain access to the system. **Intrusion prevention**, on the other hand, is the art of preventing an unauthorized access of a system's resources. The two processes are related in a sense that while intrusion detection passively detects system intrusions, intrusion prevention actively filters network traffic to prevent intrusion attempts. For the rest of the week, let us focus on these two processes.

### Exercise 12.2

The intrusion process consists of the following stages:

- **Reconnaissance**
- **Physical Intrusion**
- **Denial of Service**

## PROTECTING MEASURES – FIREWALLS – 13<sup>th</sup> Week

### Exercise 13.1

**A firewall is a hardware, a software, or a combination of both that monitors and filters traffic packets that attempt to either enter or leave the protected private network.** It is a tool that separates a protected network or part of a network, and now increasingly a user PC, from an unprotected network—the “bad network” like the Internet. In many cases the “bad network” may even be part of the company network. By definition, a “firewall,” is a tool that provides a filter of both incoming and outgoing packets.

### **Exercise 13.2**

The security policies most commonly used by organizations vary ranging from completely disallowing some traffic to allowing some of the traffic or all the traffic. These policies are consolidated into two commonly used **firewall security policies**:

- Deny-everything-not-specifically-allowed which sets the firewall in such a way that it denies all traffic and services except a few that are added as the organization needs develop.
- Allow-everything-not-specifically-denied which lets in all the traffic and services except those on the “forbidden” list which is developed as the organization’s dislikes grow.



**FORM: 200.1.3**

## **STUDY GUIDE**

**Course: CYS604 - Cryptography**

## Course Information

<b>Institution</b>	European University Cyprus		
<b>Programme of Study</b>	Cybersecurity (MSc)		
<b>Course unit</b>	CYS604 Cryptography		
<b>Level</b>	<i>Undergraduate</i>	<i>Postgraduate</i>	
		<i>Master</i>	<i>PhD</i>
		√	
<b>Language of Instruction</b>	English		
<b>Teaching Methodology</b>	Distance Learning		
<b>Course Type</b>	<i>Compulsory</i>		<i>Optional</i>
		√	
<b>Number of Group Consultation Meetings/Web-Conferences/</b>	<i>Total</i>	<i>Face to Face</i>	<i>Web-Conferences</i>
Lectures	14	1	13
<b>Number of Activities/ Assignments</b>	4		
<b>Final Assessment</b>	<i>Assignments</i>	<i>Final Examinations</i>	
	50 %	50 %	
<b>Number of Credits (ECTS)</b>	10		

<b>Study Guide drafted by</b>	Dr Philippos Isaia
<b>Editing and final approval of</b>	
<b>Study Guide by</b>	Dr Yianna Danidou

## COURSE CONTENTS

	Page
Introductory Notes	4
First Group Consultation Meeting	6
1 Introduction ( <a href="#">1<sup>st</sup> Week</a> )	8
2 Cryptography Principles and Syntax ( <a href="#">2<sup>nd</sup> Week</a> )	14
3 Computational Security ( <a href="#">3<sup>rd</sup> Week</a> )	21
4 Pseudorandom Generators & Stream Ciphers ( <a href="#">4<sup>th</sup> Week</a> )	28
5 Block Ciphers ( <a href="#">5<sup>th</sup> Week</a> )	36
6 Data Encryption Standard - DES ( <a href="#">6<sup>th</sup> Week</a> )	44
7 Message Authentication Code - MAC ( <a href="#">7<sup>th</sup> Week</a> )	48
8 Hash Functions ( <a href="#">8<sup>th</sup> Week</a> )	59
9 Number Theory and Cryptography ( <a href="#">9<sup>th</sup> Week</a> )	67
10 Key Management & Public-Key Cryptography ( <a href="#">10<sup>th</sup> Week</a> )	82
11 Public-Key Cryptography ( <a href="#">11<sup>th</sup> Week</a> )	90
12 RSA Encryption ( <a href="#">12<sup>th</sup> Week</a> )	96
13 Digital Signatures ( <a href="#">13<sup>th</sup> Week</a> )	101
14 Revision and Final Examination	107
Indicative answers to Self-Assessment exercises	108

## INTRODUCTORY NOTES

The present Study Guide for **Cryptography** is a result of collective effort and cooperation of the members of Adjunct Faculty (AF) for this course. Every year this study guide is reviewed and updated based on the changes of the educational material posted on the platform.

The Cryptography course is a first semester **compulsory** course. The course scope is to introduce fundamental concepts of cryptography and its uses in cyber and information security. Beyond the basic uses for keeping information secret and the different methods available, additional forms such as hashes, digital signatures, non-repudiation and steganography are introduced.

Upon successful completion of this course, students should be able to:

1. Describe the underlying principles of cryptography, clear text, plain text, algorithms and keys.
2. Explain the different kinds of encryption methods (symmetric, asymmetric) and the differences between them.
3. Classify and describe a number of different encryption algorithms and the way that they work.
4. Describe the mathematical principles behind encryption and the mathematical properties of ciphertext.
5. Describe and evaluate different methods used to crack encryption.
6. Explain the different uses of encryption methods and the security objectives that they meet.

This Study Guide is a necessary and useful tool for the students, especially in the cases that the educational material is not written with open and distance learning methodology. It encourages and facilitates the study and understanding of the issues addressed by the Course.

In addition, through the self-assessment exercises, it stimulates and encourages work at home, providing incentives for further study and contributes to the development of critical thinking.

The Study Guide is structured in a weekly basis and includes summary and brief introductory remarks, purpose and expected outcomes, keywords - basic concepts, annotated references, recommended student study time, self-assessment exercises, critical thinking and case studies, with indicative answers/solutions, aiming at a more meaningful understanding of the content, terms and concepts that each unit deals with.

The recommended weekly working time, apart from studying, includes the follow-up of (tele) meetings and Group Consultation Meeting (GCM), the search for bibliography/references, completion of any coursework, weekly exercises, etc. Although it is sufficiently clear, it should be noted that the study guide does not substitute the educational material posted on the platform that the student needs to read carefully and understand in order to be able to meet the requirements of the program and successfully complete the course.

## 1st GROUP CONSULTATION MEETING

### Programme Presentation

Leading companies today are rethinking the role of information security in their organizations. They realize that in a digital world, cybersecurity is the key to safeguarding their most precious assets—intellectual property, customer information, financial data, and employee records, among others. But far more than a defensive measure, companies also know that cybersecurity can better position their organization with business partners, customers, investors, and other stakeholders.

The European cybersecurity market is about 25% (i.e. about €17bln) of the world market (estimated at €70bln in 2015), with an average yearly growth slightly larger than 6%, when the world market is growing at about 10%/year. Recent study compiled by Europe's cybersecurity industry leaders pointed out that Europe is in danger of falling behind in the international digital economy field.

The Master in Cybersecurity is a cutting-edge program, designed for those wishing to develop a career as a cyber-security professional, or to take a leading technical or managerial role in an organization critically dependent upon data and information communication technology. Students will develop an advanced knowledge of information security and an awareness of the context in which information security operates in terms of safety, environmental, social and economic aspects. They will gain a wide range of intellectual, practical and transferable skills, enabling them to develop a flexible professional career in IT.

Key elements of this postgraduate degree are: the *real life experience* given by the opportunity to apply their theoretical knowledge through specialized virtual and remote security laboratories in which they will be able to carry out activities such as reconnaissance, network scanning and exploitation exercises, and investigate the usage and behavior of security systems such as Intrusion Detection and Prevention Systems thus becoming confident in the practical application of the latest tools; the *high-level insight* that will enhance student's ability to research and design creative cyber security solutions to address business problems; *hands-on skills* through experimentation with security techniques, cryptographic algorithms, cyber forensics building an ethical hacking environment; and *flexibility* since students will also be able to choose either the completion of a Master thesis or to complete a Research methods course and two elective courses.

Students undertake modules to the value of 90 ECTS credits.

## **Recommended Study Time for Students**

Approximately 5 hours for the study of the Study Guide

## INTRODUCTION

1<sup>st</sup> Week

### Summary

In this week, the basic concepts and definitions of Cryptography will be introduced to the students. More specifically, the initial uses of cryptography as well as its evolution, together with several uses throughout the history will be covered.

### Introductory Remarks

#### Cryptology

The most general term is Cryptology coming from the Greek words “κρυπτός” (kruptos, “hidden”) and “λόγος” (logos, “word”), meaning hiding word or hiding a speech. Cryptology splits down into two branches, Cryptography and Cryptanalysis.

Cryptography is the science of secret writing with the goal of hiding the meaning of a message. Modern cryptography involves the study of mathematical techniques for securing digital information, systems, and distributed computations against adversarial attacks.

Cryptanalysis is the science of breaking cryptography systems (called cryptosystems). When it comes down to evaluation and evolution of systems, cryptanalysis is not a crime, due to the fact

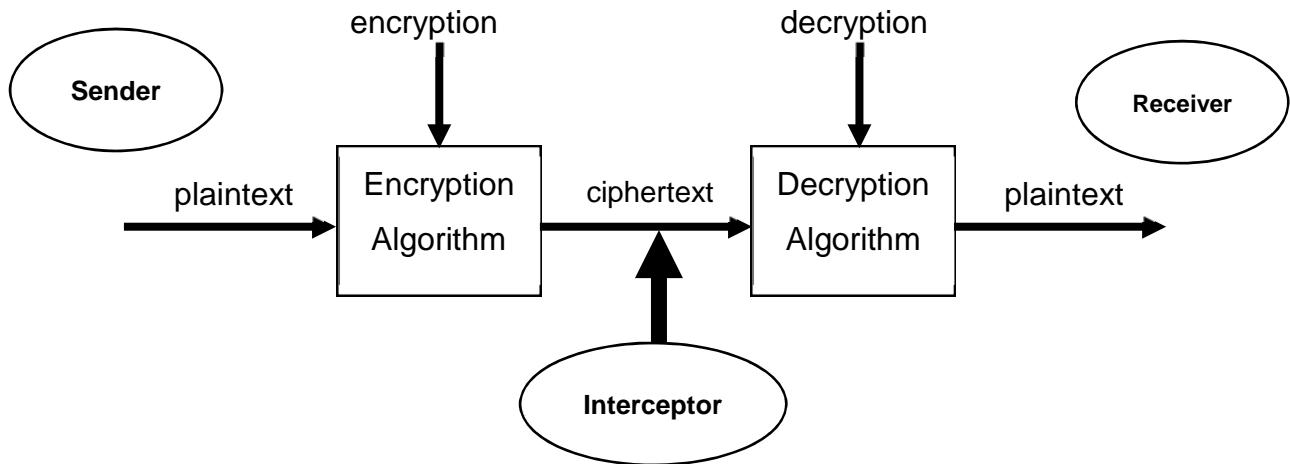


Figure 1 A Typical Cryptosystem

that it helps evolve a cryptosystem and find possible bugs that can cause security breaches or retrieval of sensitive information.

The need for cryptography starts when two parties want to exchange sensitive information that cannot be leaked or revealed to non-authorised parties. As shown in Figure 1, a sender has a message (called *plaintext*) that has to be transmitted to a receiver. The sender has to encrypt the plaintext using an encryption algorithm and an encryption key. The resultant message (called *ciphertext*) must be unreadable by any non-authorised party. That ciphertext is then transmitted to the receiver who uses a decryption algorithm and a decryption key to decrypt the ciphertext and read the original message. A cryptosystem (the mechanism or method of encrypting a message) is sometimes called a *cipher*.

## **Steganography**

One of the oldest form of cryptography used is steganography. Steganography is the practice of concealing information within ordinary information. This can take place both physical and digital methods. One of the earliest steganography applications mentioned by the ancient Greek Herodotus, in 440BC, says that Histiaeus shaved the head of his most trusted slave and tattooed a message on it. After his hair had grown, the message was hidden. The servant then travelled to the receiver of the message who shaved his head again to read it. Other forms of physical steganography include the use of invincible ink, Morse code knitted into pieces of cloth, photosensitive glass used during WWII as well as microdots embedded in the paper covered by adhesive, again used during WWII. In digital steganography, some of the methods used are concealing messages within images, sounds or random data, as well as the *chaffing and winnowing* method.

## **Concealing Messages within Images**

In digital images, each pixel is represented by 3 values. The red, green and blue values. Each of these values is represented by eight bits (one byte) ranging from 0 to 255 in decimal or 00000000 to 11111111 in binary. The leftmost bit is the most significant bit. If that bit is changed, it will have a large impact on the final value; therefore, the colour difference will be obvious to the naked eye. For example, if we change the leftmost bit from 1 to 0 (11111111 to 01111111) it will change the decimal value from 255 to 127.

On the other hand, the rightmost bit is the less significant bit. If that bit is changed, it will have less impact on the final value. For example, if we change the rightmost bit from 1 to 0 (11111111 to 11111110) it will change the decimal value from 255 to 254.

For example, changing the last two bits in a completely red pixel from 11111111 to 11111101 only changes the red value from 255 to 253, which to the naked eye creates a nearly imperceptible

change in colour but still allows us to encode data inside of the picture. As a result, the least significant bits in an image can be used to hide some information.

### **Chaffing and Winnowing**

Let's say a sender wants to send a message to a receiver. The sender enumerates the symbols and sends them out each in a separate packet. Takes each bit, adds a serial number and a **MAC** (Message Authentication Code). The sender then adds some chaff packets (i.e. fake packets with invalid MAC) (**chaffing**). Finally, the sender sends both valid and invalid packets together to the receiver. The receiver has to authenticate each packet and discard the ones with the invalid MAC (**winnowing**).

### **Symmetric Cryptography**

It is the use of the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. One party can send a message, or plaintext, to the other by using the shared key to encrypt the message and thus obtain a ciphertext that is transmitted to the receiver. The receiver uses the same key to decrypt the ciphertext and recover the original message. This of course faces some problems. For example is the systems needs a secure channel for distribution of the key between the sender and the receiver. In addition, it faces message integrity as well sender authentication problems as we will discuss later in this course.

### **Caesar Cipher**

The Caesar cipher is one of the earliest known and simplest ciphers. It is a type of substitution cipher in which each letter in the plaintext is 'shifted' a certain number of places down the alphabet. For example, with a shift of 1 "A" would be replaced by "B", "B" would become "C", and so on. The method is named after Julius Caesar, who apparently used it to communicate with his generals.

### **Affine Cipher**

The Affine cipher is a special case of the more general mono-alphabetic substitution cipher. The cipher is *less* secure than a substitution cipher as it is vulnerable to all of the attacks that work against substitution ciphers, in *addition* to other attacks. The cipher's primary weakness comes from the fact that if the cryptanalyst can discover (by means of frequency analysis, brute force, guessing or otherwise) the plaintext of two ciphertext characters, then the key can be obtained by solving a simultaneous equation.

## **One-Time Pad**

A one-time pad is a system in which a private key generated randomly is used only once to encrypt a message that is then decrypted by the receiver using a matching one-time pad and key. Messages encrypted with keys based on randomness have the advantage that there is theoretically no way to "break the code" by analysing a succession of messages. Each encryption is unique and bears no relation to the next encryption so that some pattern can be detected. With a one-time pad, however, the decrypting party must have access to the same key used to encrypt the message and this raises the problem of how to get the key to the decrypting party safely or how to keep both keys secure.

Theoretically for one-time pad to be "unbreakable", the pre-shared key (one-time pad) has to be truly random, must be kept secret, used only once and its length has to be equal or longer to the plaintext.

## **Aim/Objectives**

The purpose of the 1<sup>st</sup> Week is to introduce to the students the basic concepts and definitions of Cryptography. In addition, some old cryptographic methods are introduced and explained in order to explain the evolution of cryptography through the years.

## **Learning Outcomes**

After the successful completion of the 1<sup>st</sup> Week, students should be able to:

- Distinguish between the basic concepts and definitions such as cryptology, cryptography, cryptanalysis, plaintext, ciphertext
- Explain the basic principles behind a typical cryptosystem
- Show physical and digital uses of steganography with examples
- Explain concept of shift / substitution cipher and encrypt or decrypt messages using Caesar or Affine ciphers
- Show how One-Time Pad method works and encrypt or decrypt messages using it
- Explain the concept of Symmetric Cryptography

## Key Words

Cryptology	Cryptography	Cryptanalysis
Cryptosystem	Cipher	Ciphertext
Plaintext	Encryption	Decryption
Steganography	Substitution	Shift

## Annotated Bibliography

### Basic

- C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2010, Chapter 1 “*Introduction to Cryptography and Data Security*”

The first Chapter of this book introduces the most important terms of modern cryptology and indicates the differences of proprietary and openly known algorithms. It also introduces some historical ciphers as well as the evolution of ciphers through time.

### Suggestions for further reading

- D. Boneh and V. Shoup, A Graduate Course in Applied Cryptography, 2017, Part 1 “Secret Key Cryptography”

Essentially the first part of this book covers a lot of the material covered in this course. It covers the basic principles of Encryption, and goes through some historical ciphers as well as some basic cryptanalysis.

- Secrets Hidden in Images (Steganography) – Computerphile, [Youtube Video], Available at: <https://www.youtube.com/watch?v=TWEXCYQKyDc>

## Self-Assessment Exercises

### Exercise 1.1

Explain in your own words how “Chaffing and Winnowing” works.

### Exercise 1.2

Explain in your own words how one can hide messages inside digital images.

### **Exercise 1.3**

Explain how one time pad works, and what rules one has to follow to make sure it cannot be cracked.

### **Exercise 1.4**

Using one time pad, encrypt the message “introduction to cryptography” using the key “pesbusededenayallgmncofwis”. Make sure to remove the empty spaces in the message.

### **Exercise 1.5**

The ciphertext below was encrypted using a substitution cipher. Decrypt the ciphertext without knowledge of the key

wshpualea pz h alyt bzlk pu jyfwavnyhwof aoha ylmlyz av h tlzzhnl ilmvyl lujyfwapvu vy hmaly klijyfwapvu wshpu alea ylmlyz av alea jvuzpzapun luapylsf vm johyhjalyz aoha hyl bzlk pu zvtl dypaal obthu shunbhnl hz jvuayhzalk dpao zlxblujlz vm ipaz aoha kv uva ylwylzlua obthu ylhkhisl johyhjalyz jpwolyalea pa pz aol buylkhisl vbawba vm hu lujyfwapvu hsnvypaot aol alyt jpwoly pz zvtlaplz bzlk hz hu hsalyuhapcl alyt mvy jpwolyalea jpwolyalea pz uva buklyzahukhisl buaps pa ohz illu jvuclyalk puav wshpu alea bzpun h rlf jpwoly pz aol ihzpj tijohupzt vm lujyfwapun h tlzzhnl bzpun h rlf

- a) Compute the relative frequency of all letters (a to z) in the ciphertext. You can use a paper and a pencil or use an online tool such as the one provided at <http://www.cryptoprograms.com/tools/frequency>
- b) Try to decrypt the ciphertext with the help of letter relative frequency.

### **Exercise 1.6**

Give an example use of symmetric cryptography. Explain what problems symmetric cryptography can face.

### **Exercise 1.7**

Using a programming language that you are familiar with, create a simple command line software which takes plaintext and a key and performs one time pad encryption. Go a step further and develop decryption as well.

## **Recommended time for the student to work**

15 hours

## Summary

In this week, some important principles of Cryptography will be introduced such as the Kerckhoffs' Principle as well as the idea of perfect secrecy. A formal syntax will be given for cryptosystems as well as a more in-depth cryptanalysis of some shift ciphers will be covered.

## Introductory Remarks

### Kerckhoffs' Principle

It is clear from the encryption methodology and the correctness requirement that if an eavesdropping adversary knows the algorithm of encryption and decryption as well as the key shared by the two communicating parties, then that adversary will be able to decrypt any ciphertexts transmitted by those parties. Perhaps they should keep the decryption algorithm secret.

In 1883 Auguste Kerckhoffs argued the opposite in a paper he wrote elucidating several design principles for military ciphers. One of the most important of these, now known simply as Kerckhoffs' principle, was "*The cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.*"

There are several arguments in favour of this principle, such as:

- a) It is significantly easier for the parties to maintain secrecy of a short key than to keep secret the (more complicated) algorithm they are using.
- b) In case the honest parties' shared, secret information is ever exposed, it will be much easier for them to change a key than to replace an encryption scheme.
- c) For large-scale deployment it is significantly easier for users to all rely on the same encryption algorithm/software (with different keys) than for everyone to use their own custom algorithm.

## Syntax of Encryption

A private-key encryption scheme is defined by specifying a **message space M** (M defines the set of legal messages, i.e. those supported by the scheme) along with three algorithms:

- a) A procedure for generating keys (**Gen**)
- b) A procedure for encrypting (**Enc**)
- c) A procedure for decrypting (**Dec**)

The algorithms have the following functionality:

- a) The key-generation algorithm (**Gen**) is a probabilistic algorithm that outputs a key **k** chosen according to some distribution. The set of all possible keys output by **Gen** is called a **key space**, denoted by **K**.
- b) The encryption algorithm (**Enc**) takes as input a key **k** and a message **m** and outputs a ciphertext **c**. We denote by **Enc<sub>k</sub>(m)** the encryption of a plaintext **m** using the key **k**.
- c) The decryption algorithm (**Dec**) takes as input a key **k** and a ciphertext **c** and outputs a plaintext **m**. We denote **Dec<sub>k</sub>(c)** the decryption of a ciphertext **c** using a key **k**.

## Cryptanalysis of Shift Cipher

The **shift cipher** can be viewed as a variant of Caesar's cipher. Specifically, in the shift cipher the key **k** is a number between 0 and 25. Mapping this to the syntax of encryption described earlier, the message space consists of arbitrary length strings of English letters with punctuation, spaces (sometimes), and numerals removed, and with no distinction between upper and lower case. Algorithm **Gen** outputs a uniform key **k**  $\in \{0, \dots, 25\}$ . Algorithm **Enc** takes a key **k** and a plaintext and shifts each letter of the plaintext forward **k** positions (wrapping around at the end of the alphabet). Algorithm **Dec** takes a key **k** and a ciphertext and shifts every letter of the ciphertext backward **k** positions.

An attack that involves trying every possible key is called a **brute-force** or **exhaustive-search attack**. Clearly, for an encryption scheme to be secure it must not be vulnerable to such an attack. This observation is known as the **sufficient key-space principle**:

*“Any secure encryption scheme must have a key space that is sufficiently large to make an exhaustive-search attack infeasible”*

One can debate what amount of effort makes a task “infeasible,” and an exact determination of feasibility depends on both the resources of a potential attacker and the length of time the sender and receiver want to ensure secrecy of their communication.

Is it possible to recover the message without knowing **k**? Actually, it is trivial! The reason is that there are only 26 possible keys. So one can try to decrypt the ciphertext using every possible key

and thereby obtain a list of 26 candidate plaintexts. The correct plaintext will certainly be on this list; moreover, if the ciphertext is “long enough” then the correct plaintext will likely be the only candidate on the list that “makes sense.” (The latter is not necessarily true, but will be true most of the time. Even when it is not, the attack narrows down the set of potential plaintexts to at most 26 possibilities.) By scanning the list of candidates it is easy to recover the original plaintext.

### **Mono-Alphabetic Substitution Cipher**

In the shift cipher, the key defines a map from each letter of the (plaintext) alphabet to some letter of the (ciphertext) alphabet, where the map is a fixed shift determined by the key. In the mono-alphabetic substitution cipher, the key also defines a map on the alphabet, but the map is now allowed to be arbitrary subject only to the constraint that it be one-to-one so that decryption is possible. The key space thus consists of all bijections, or permutations, of the alphabet.

Assuming the English alphabet is being used, the key space is of size  $26! = 26 * 25 * 24 * \dots * 2 * 1$ , which is approximately  $2^{88}$ . This is a huge number, which means brute-force is infeasible (in sufficient time). This however, does not mean the cipher is secure! Statistical patterns in the English language allow as to use a letter-frequency attack

### **Poly-Alphabetic Substitution Cipher**

The statistical attack on the mono-alphabetic substitution cipher can be carried out because the key defines a fixed mapping that is applied letter-by-letter to the plaintext. Such an attack could be thwarted by using a poly-alphabetic substitution cipher where the key instead defines a mapping that is applied on blocks of plaintext characters. For example, a key might map the 2-character block ab to DZ while mapping ac to TY; note that the plaintext character a does not get mapped to a fixed ciphertext character. Poly-alphabetic substitution ciphers “smooth out” the frequency distribution of characters in the ciphertext and make it harder to perform statistical analysis. The **Vigenère cipher**, is a special case of the poly-alphabetic substitution cipher. Works by applying several independent instances of the substitution cipher in sequence. The key is now viewed as a string of letters; encryption is done by shifting each plaintext character by the amount indicated by the character of the key, wrapping around when necessary. (Note: if the key is shorter than the message then the key is repeated)

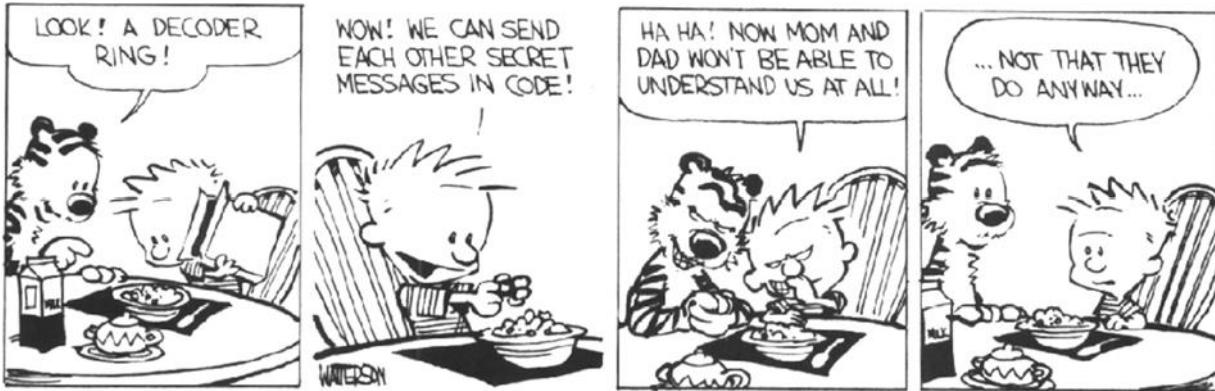


Figure 2 Using a Key Funny by ALERT (Active Learning Experiences in Resourceful Thinking)

### Perfect Secrecy

Since we have discussed a formal syntax of encryption, we are ready to define the notion of perfect secrecy. We can imagine an adversary who knows the probability distribution over  $M$ ; that is, the adversary knows the likelihood that different messages will be sent. This adversary also knows the encryption scheme being used; the only thing unknown to the adversary is the key shared by the parties. A message is chosen by one of the honest parties and encrypted, and the resulting ciphertext transmitted to the other party. The adversary can eavesdrop on the parties' communication, and thus observe this ciphertext. For a scheme to be perfectly secret, observing this ciphertext should have no effect on the adversary's knowledge regarding the actual message that was sent. This means that the ciphertext reveals nothing about the underlying plaintext, and the adversary learns absolutely nothing about the plaintext that was encrypted. Formally:

An encryption scheme (**Gen**, **Enc**, **Dec**) with message space  $\mathbf{M}$  is perfectly secret if for every probability distribution over  $\mathbf{M}$ , every message  $m \in M$ , and every ciphertext  $c \in C$  for which  $Pr[C = c] > 0$ :

$$Pr[M = m | C = c] = Pr[M = m]$$

Note:  $Pr[C = c] > 0$  is a technical requirement to prevent a zero-probability event

We now give an equivalent formulation of perfect secrecy. Informally, this formulation requires that the probability distribution of the ciphertext does not depend on the plaintext i.e. for any two messages  $m, m' \in M$  the distribution of the ciphertext when  $m$  is encrypted should be identical to the distribution of the ciphertext when  $m'$  is encrypted. Formally, for every  $m, m' \in M$ , and every  $c \in C$ ,

$$Pr[Enc_k(m) = c] = Pr[Enc_k(m') = c]$$

## Aim/Objectives

The purpose of the 2<sup>nd</sup> Week is to introduce Kerckhoffs' Principle and explain the importance of having a publicly available cryptosystem. In addition, a formal syntax for cryptography is introduced in order to define several concepts in a more formal form. Those include correctness requirements as well as perfect secrecy. Finally, cryptanalysis is performed on typical shift ciphers and then mono-alphabetic and poly-alphabetic substitution ciphers are introduced in order to indicate ways of preventing brute-force or letter frequency attacks.

## Learning Outcomes

After the successful completion of the 2<sup>nd</sup> Week, students should be able to:

- Evaluate Kerckhoffs' Principle and argue in its favour
- Construct a formal Encryption Syntax
- Formally indicate the Correctness Requirements as well as Perfect Secrecy
- Perform cryptanalysis on shift ciphers
- Explain how brute-force and letter frequency analysis works
- Specify the use of mono-alphabetic substitution ciphers
- Specify the use of poly-alphabetic substitution ciphers

## Key Words

Perfect Secrecy	Kerckhoffs' Principle	Correctness Requirement
Letter Frequency	Brute-Force	Vigenère cipher
Encryption Syntax	Bayes' Theorem	

## Annotated Bibliography

### Basic

- C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer, 2010, Chapters 1 “*Introduction to Cryptography and Data Security*” and 2 “*Stream Ciphers*”

The first Chapter of this book introduces the most important terms of modern cryptology and indicates the differences of proprietary and openly known algorithms. It also introduces some historical ciphers as well as the evolution of ciphers through time.

The second Chapter analyses the advantages and disadvantages of stream ciphers, as well as some random and pseudorandom number generators. Goes through the unbreakable One-Time Pad cipher as well as it performs some cryptanalysis on it as well as on some modern stream ciphers

### Suggestions for further reading

- D. Boneh and V. Shoup, A Graduate Course in Applied Cryptography, 2017, Part 1 “Secret Key Cryptography”

Essentially the first part of this book covers a lot of the material covered in this course. It covers the basic principles of Encryption, and goes through some historical ciphers as well as some basic cryptanalysis.

- Bayes' Theorem – The Simplest Case, Trefor Bazett, [Youtube Video], Available at: <https://www.youtube.com/watch?v=XQoLVI31ZfQ>
- Darma Nasution, Surya & Ginting, Guidio & Syahrizal, Muhammad & Rahim, Robbi. (2017). Data Security Using Vigenere Cipher and Goldbach Codes Algorithm. International Journal of Engineering Research & Technology. 6. 360-363.

## Self-Assessment Exercises

### Exercise 2.1

Give a proper syntax for encryption, explaining the algorithms used

### Exercise 2.2

What correctness requirement should an encryption scheme satisfy, and why is that important?

### Exercise 2.3

Explain Kerckhoff's Principle, and give arguments in favour of the principle.

### Exercise 2.4

Explain why a standard shift cipher can be easily brute-forced.

### Exercise 2.5

Consider a shift cipher, with the following distribution over M

$$\Pr[M = a] = 0.2, \Pr[M = b] = 0.2, \Pr[M = c] = 0.3, \Pr[M = d] = 0.3$$

- a) What is the probability that the ciphertext is B?
- b) What is the probability that the ciphertext is C?

### **Exercise 2.6**

Compare Vigenère cipher with one time pad.

### **Recommended time for the student to work**

15 hours

### Summary

In this week, we will discuss the idea of computational security, introducing two new concepts, the concepts of **concrete** and **asymptotic** approach.

### Introductory Remarks

#### Computational Security

Perfect secrecy is a worthwhile goal, but it is also unnecessarily strong. It requires that no information about the encrypted message is leaked, even if the attacker/eavesdropper has unlimited computational power. Practically, an encryption scheme is considered secure if it leaked only a tiny amount of information to eavesdroppers with bounded computational power. For example, an encryption scheme that leaks information with probability  $2^{-60}$  after investing 200 years of computational effort on the fastest available supercomputer is adequate for any real-world application. Security definitions that take into account computational limits on the attacker, and allow for a small probability of failure, are called computational, to distinguish them from notions (like perfect secrecy) that are information-theoretic in nature. Computational security is now the de facto way in which security is defined for all cryptographic purposes.

Computational security incorporates two relaxations relative to information theoretic notions of security:

1. Security is only guaranteed against efficient adversaries that run for some feasible amount of time. This means that given enough time (or sufficient computational resources) an attacker may be able to violate security. If we can make the resources required to break the scheme larger than those available to any realistic attacker, then for all practical purposes the scheme is unbreakable.
2. Adversaries can potentially succeed (i.e., security can potentially fail) with some very small probability. If we can make this probability sufficiently small, we do not need to worry about it.

To obtain a meaningful theory, we need to precisely define the above relaxations. There are two general approaches for doing so: the **concrete** approach and the **asymptotic** approach.

### Concrete Approach

The concrete approach to computational security quantifies the security of a cryptographic scheme by explicitly bounding the maximum success probability of any (randomized) adversary running for some specified amount of time or, more precisely, investing some specific amount of computational effort.

Concrete Definition:

*A scheme is  $(t, E)$ -secure if any adversary running for time at most  $t$  succeeds in breaking the scheme with probability at most  $E$ .*

For example, a scheme with the guarantee that no adversary running for at most 200 years using the fastest available supercomputer can succeed in breaking the scheme with probability better than  $2^{-60}$ . Alternatively, it may be more convenient to measure running time in terms of CPU cycles, and to construct a scheme such that no adversary using at most  $2^{80}$  cycles can break the scheme with probability better than  $2^{-60}$ . It is instructive to get a feel for the large values of  $t$  and the small values of  $\epsilon$  that are typical of modern cryptographic schemes.

Modern private-key encryption schemes are generally assumed to give almost optimal security in the following sense: when the key has length  $n$ , and so the key space has size  $2^n$ , an adversary running for time  $t$  (measured in, say, computer cycles) succeeds in breaking the scheme with probability at most  $\frac{ct}{2^n}$  for some fixed constant  $c$ .

Assuming  $c = 1$  for simplicity, a key of length  $n = 60$  provides adequate security against an adversary using a desktop computer. Indeed, on a 4 GHz processor (that executes  $4 \times 10^9$  cycles per second)  $2^{60}$  CPU cycles require  $\frac{2^{60}}{4 \times 10^9}$  seconds, or about 9 years. However, a fast

supercomputer can execute roughly  $2 \times 10^{16}$  floating point operations per second, and  $2^{60}$  such operations require only about 1 minute on such a machine. Taking  $n = 80$  would be a more prudent choice; even the computer just mentioned would take about 2 years to carry out  $2^{80}$  operations.

The above numbers are for illustrative purposes only; in practice  $c > 1$ , and several other factors, such as the time required for memory access and the possibility of parallel computation on a network of computers, significantly affect the performance of brute-force attacks.

Today, however, a recommended key length might be  $n = 128$  or even  $n = 256$ . The difference between  $2^{80}$  and  $2^{128}$  is a multiplicative factor of  $2^{48}$ . To get a feeling for how big this is, note that according to physicists' estimates the number of seconds since the Big Bang is approximately  $2^{58}$ .

If the probability that an attacker can successfully recover an encrypted message in one year is at most  $2^{-60}$ , then it is much more likely that the sender and receiver will both be hit by lightning in that same period of time. An event that occurs once every hundred years can be roughly estimated to occur with probability  $2^{-30}$  in any given second. Something that occurs with probability  $2^{-60}$  in any given second is  $2^{30}$  times less likely, and might be expected to occur roughly once every 100 billion years.

The concrete approach is important in practice, since concrete guarantees are what users of a cryptographic scheme are ultimately interested in. However, precise concrete guarantees are difficult to provide. One must be careful in interpreting concrete security claims. For example, a claim that no adversary running for 5 years can break a given scheme with probability better than  $E$  begs the questions:

1. What type of computing power (e.g., desktop PC, supercomputer, network of hundreds of computers) does this assume?
2. Does this take into account future advances in computing power (which, by Moore's Law, roughly doubles every 18 months)?
3. Does the estimate assume the use of "off-the-shelf" algorithms, or dedicated software implementations optimized for the attack?

Furthermore, such a guarantee says little about the success probability of an adversary running for 2 years (other than the fact that it can be at most  $E$ ) and says nothing about the success probability of an adversary running for 10 years. In other words the concrete approach is mostly used and mostly describes symmetric cryptography

### **Asymptotic Approach**

This approach, rooted in complexity theory, introduces an integer-valued security parameter (denoted by  $n$ ) that parameterizes both cryptographic schemes as well as all involved parties. When honest parties initialize a scheme (i.e., when they generate keys), they choose some value  $n$  for the security parameter. The security parameter is assumed to be known to any adversary

attacking the scheme, and we now view the running time of the adversary, as well as its success probability, as functions of the security parameter rather than as concrete numbers.

We equate “efficient adversaries” with randomized (i.e., probabilistic) algorithms running in time **polynomial in  $n$** . This means there is some polynomial  $p$  such that the adversary runs for time at most  $p(n)$  when the security parameter is  $n$ . We also require, for real-world efficiency, that honest parties run in polynomial time, although we stress that the adversary may be much more powerful (and run much longer than) the honest parties. We equate the notion of “small probabilities of success” with success probabilities smaller than any inverse polynomial in  $n$ . Such probabilities are called **negligible**,  $f(n) < \frac{1}{p(n)}$ .

*A scheme is secure if any Probabilistic Polynomial Time (PPT) adversary succeeds in breaking the scheme with at most negligible probability.*

Say we have a scheme that is asymptotically secure, then it may be the case that an adversary running for  $n^3$  minutes can succeed in “breaking the scheme” with probability  $2^{40} \cdot 2^{-n}$  (which is a negligible function of  $n$ ). When  $n := 40$  this means that an adversary running for  $40^3$  minutes (about 6 weeks) can break the scheme with probability 1, so such values of  $n$  are not very useful.

Even for  $n = 50$  an adversary running for  $50^3$  minutes (about 3 months) can break the scheme with probability roughly  $\frac{1}{1000}$ , which may not be acceptable. On the other hand, when  $n = 500$  an adversary running for 200 years breaks the scheme only with probability roughly  $2^{-500}$ .

As indicated by the example, we can view the security parameter as a mechanism that allows the honest parties to “tune” the security of a scheme to some desired level. Increasing the security parameter also increases the time required to run the scheme, as well as the length of the key, so the honest parties will want to set the security parameter as small as possible subject to defending against the class of attacks they are concerned about. Viewing the security parameter as the key length, this corresponds roughly to the fact that the time required for a brute-force attack grows exponentially in the length of the key. The ability to “increase security” by increasing the security parameter has important practical ramifications, since it enables honest parties to defend against increases in computing power.

## Efficient algorithms

We can define an algorithm to be efficient if it runs in polynomial time. An algorithm  $A$  runs in polynomial time if there exists a polynomial  $p$  such that, for every input  $x \in \{0, 1\}^*$ , the computation of  $A(x)$  terminates within at most  $p(|x|)$  steps ( $|x|$  denotes the length of the string  $x$ ). As mentioned earlier, we are only interested in adversaries whose running time is polynomial in the security parameter  $n$ . Since we measure the running time of an algorithm in terms of the length of its input, we sometimes provide algorithms with the security parameter written in unary (i.e., as  $1^n$ , or a string of  $n$  ones) as input. Parties (or, more precisely, the algorithms they run) may take other inputs besides the security parameter (e.g. a message to be encrypted) and we allow their running time to be polynomial in the (total) length of their inputs.

By default, we allow all algorithms to be probabilistic (or randomized). Any such algorithm may “toss a coin” at each step of its execution, this is a metaphorical way of saying that the algorithm can access an unbiased random bit at each step. Equivalently, we can view a randomized algorithm as one that, in addition to its input, is given a uniformly distributed random tape of sufficient length whose bits it can use, as needed, throughout its execution. We consider randomized algorithms by default for two reasons:

1. Randomness is essential to cryptography and so honest parties must be probabilistic; given this, it is natural to allow adversaries to be probabilistic as well.
2. Randomization is practical and gives attackers additional power. Since our goal is to model all realistic attacks, we prefer a more liberal definition of efficient computation.

## Negligible Success Probability

A negligible function is one that is asymptotically smaller than any inverse polynomial function. To define that formally, we can say that a function  $f$  from the natural numbers to the non-negative real numbers is negligible if for every positive polynomial  $p$  there is an  $N$  such that for all integers  $n > N$  it holds that  $f(n) < \frac{1}{p(n)}$ .

This can also be stated as follows, for every polynomial  $p$  and all sufficiently large values of  $n$  it holds that  $f(n) < \frac{1}{p(n)}$ .

An equivalent formulation of the above is to require that for all constants  $c$  there exists an  $N$  such that for all  $n > N$  it holds that  $f(n) < n^{-c}$ . We typically denote an arbitrary negligible function by  $\text{negl}$ .

## Aim/Objectives

The purpose of the 3<sup>rd</sup> Week is to introduce the notion of computational security. This is really important in order to understand that not all cryptography methods need to be perfectly secret. Students have to realise that each cryptography method comes at a cost (in the form of processing time/power needed), and this cost not only affects an adversary attacking the encrypted information but also the honest parties who are just trying to use the cryptography model.

## Learning Outcomes

After the successful completion of the 3<sup>rd</sup> Week, students should be able to:

- Evaluate computational security
- Explain concrete approach with examples
- Explain asymptotic approach with examples
- Formally indicate the differences between the two approaches as well as their uses
- Explain efficient algorithms and their importance in cryptography
- Specify the negligible success probability and its importance

## Key Words

Computational security	Concrete	Asymptotic
Negligible	Success	Probability
Polynomial Time	Efficient	Adversary

## Annotated Bibliography

### Basic

- C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2010, Chapter 1 “*Introduction to Cryptography and Data Security*”

The first Chapter of this book introduces the most important terms of modern cryptology and indicates the differences of proprietary and openly known algorithms. It also introduces some historical ciphers as well as the evolution of ciphers through time.

- **Suggestions for further reading**
- Cryptography – Perfect Secrecy by intrigano [Youtube Video], Available at [https://www.youtube.com/watch?v=DK7S\\_rZ0vUE](https://www.youtube.com/watch?v=DK7S_rZ0vUE)

This video explains the encryption syntax as well as the notion of perfect secrecy.

## **Self-Assessment Exercises**

### **Exercise 3.1**

Proof shift cipher perfect secrecy if the message length = 1

### **Exercise 3.2**

Proof one-time pad perfect secrecy

### **Exercise 3.3**

Using the concrete approach and assuming  $c=1$  and key length  $n=60$ , explain why such a key provides adequate security against an adversary using a desktop computer.

### **Exercise 3.4**

Explain the terms “Polynomial Time” and “Probabilistic Polynomial Time Algorithm”.

### **Exercise 3.5**

Briefly explain the Asymptotic Approach, giving at least one example.

### **Exercise 3.6**

In the asymptotic approach as well as in cryptography in general, we always consider randomized algorithms. Why is that?

## **Recommended time for the student to work**

15 hours

## Summary

In this week, pseudorandom generators will be covered showing how important they are in cryptography models. In addition, stream ciphers will be introduced.

## Introductory Remarks

### Pseudorandom Generators (PRG)

A pseudorandom generator  $G$  is an efficient, deterministic algorithm for transforming a short, uniform string called the seed into a longer, “uniform looking” (or “pseudorandom”) output string. Stated differently, a pseudorandom generator uses a small amount of true randomness in order to generate a large amount of pseudorandomness. This is useful whenever a large number of random (looking) bits are needed, since generating true random bits is difficult and slow. Indeed, pseudorandom generators have been studied since at least the 1940s when they were proposed for running statistical simulations. In that context, researchers proposed various statistical tests that a pseudorandom generator should pass in order to be considered “good.”

The seed  $s$  for a pseudorandom generator is analogous to the cryptographic key used by an encryption scheme, and the seed must be chosen uniformly and be kept secret from any adversary. Another important point, is that  $s$  must be long enough so that it is not feasible to enumerate all possible seeds. In an asymptotic sense this is taken care of by setting the length of the seed equal to the security parameter, so that exhaustive search over all possible seeds requires exponential time. In practice, the seed must be long enough so that it is impossible to try all possible seeds within some specified time bound.

Let  $I$  be a polynomial and let  $G$  be a deterministic polynomial-time algorithm such that for any  $n$  and any input  $s \in \{0, 1\}^n$ , the result  $G(s)$  is a string of length  $I(n)$ . We say that  $G$  is a pseudorandom generator if the following conditions hold:

1. For every  $n$  it holds that  $I(n) > n$
2. For any PPT algorithm  $D$ , there is a negligible function  $negl$  such that

$$IPr[G(G(s)) = 1] - Pr[D(r) = 1] \leq negl(n)$$

Where the first probability is taken over uniform choice of  $s \in \{0, 1\}^n$  and the randomness of  $D$  and the second probability is taken over uniform choice of  $r \in \{0, 1\}^{l(n)}$  and the randomness of  $D$ . We call  $l$  the expansion factor of  $G$ .

A (true) random generator requires a naturally occurring source of randomness. Designing a hardware device or software program to exploit this randomness and produce a bit sequence that is free of biases and correlations is a difficult task. Additionally, for most cryptographic applications, the generator must not be subject to observation or manipulation by an adversary. Hardware-based random generators exploit the randomness which occurs in some physical phenomena. Such physical processes may produce bits that are biased or correlated, in which case they should be subjected to de-skewing techniques discussed later on. Examples of such physical phenomena include:

1. elapsed time between emission of particles during radioactive decay
2. thermal noise from a semiconductor diode or resistor
3. the frequency instability of a free running oscillator
4. the amount a metal insulator semiconductor capacitor is charged during a fixed period of time
5. air turbulence within a sealed disk drive which causes random fluctuations in disk drive sector read latency times
6. sound from a microphone or video input from a camera

Designing a random generator in software is even more difficult than doing so in hardware. Processes upon which software random bit generators may be based include:

1. the system clock;
2. elapsed time between keystrokes or mouse movement;
3. content of input/output buffers;
4. user input
5. operating system values such as system load and network statistics

The behaviour of such processes can vary considerably depending on various factors, such as the computer platform. It may also be difficult to prevent an adversary from observing or

manipulating these processes. A natural source of random bits may be defective in that the output bits may be:

1. Biased - the probability of the source emitting a 1 is not equal to  $\frac{1}{2}$
2. Correlated - the probability of the source emitting a 1 depends on previous bits emitted

There are various techniques for generating truly random bit sequences from the output bits of such a defective generator; such techniques are called de-skewing techniques.

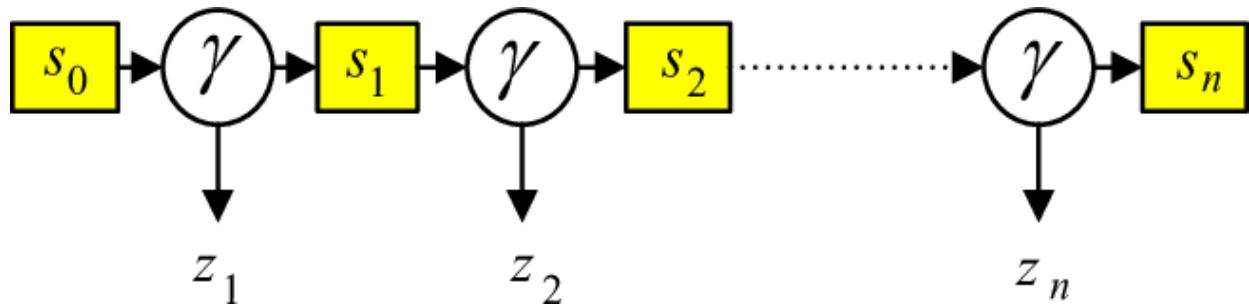


Figure 3 Structure of a Typical PRG by Behrooz Khadem

### Stream Ciphers

Stream ciphers are an important class of encryption algorithms. They encrypt **individual** characters (usually binary digits) of a plaintext message one at a time, using an encryption transformation which varies with time. By contrast, block ciphers (discussed later) tend to simultaneously encrypt **groups** of characters of a plaintext message using a fixed encryption transformation. Stream ciphers are generally faster than block ciphers in hardware, and have less complex hardware circuitry. They are also more appropriate, and in some cases mandatory, when buffering is limited or when characters must be individually processed as they are received. Because they have limited or no error propagation, stream ciphers may also be advantageous in situations where transmission errors are highly probable.

There are plenty of Stream Cipher types. In this course we will discuss the following:

1. **Synchronous** Stream Ciphers
2. **Self-synchronizing** Stream Ciphers

## Synchronous Stream Ciphers

A synchronous stream cipher is one in which the keystream is generated independently of the plaintext message and of the ciphertext.

The encryption process of a synchronous stream cipher can be described by the equations

$$u_i + 1 = f(u_{i-1}, k)$$

$$z_i = g(u_i, k)$$

$$c_i = h(z_i, m_i)$$

Where:

1.  $u_0$  is the initial state and may be determined from the key  $k$
2.  $f$  is the next-state function
3.  $g$  is the function which produces the keystream  $z_i$
4.  $h$  is the output function which combines the keystream and plaintext  $m_i$  to produce ciphertext  $c_i$

Properties of Synchronous Stream Ciphers:

1. **Synchronization Requirements** - In a synchronous stream cipher, both the sender and receiver must be synchronized, using the same key and operating at the same position (state) within that key, to allow for proper decryption.
2. **No Error Propagation** - A ciphertext digit that is modified (but not deleted) during transmission does not affect the decryption of other ciphertext digits.
3. **Active Attacks** - As a consequence of property (1), the insertion, deletion, or replay of ciphertext digits by an active adversary causes immediate loss of synchronization, and hence might possibly be detected by the decryptor. As a consequence of property (2), an active adversary might possibly be able to make changes to selected ciphertext digits, and know exactly what effect these changes have on the plaintext.

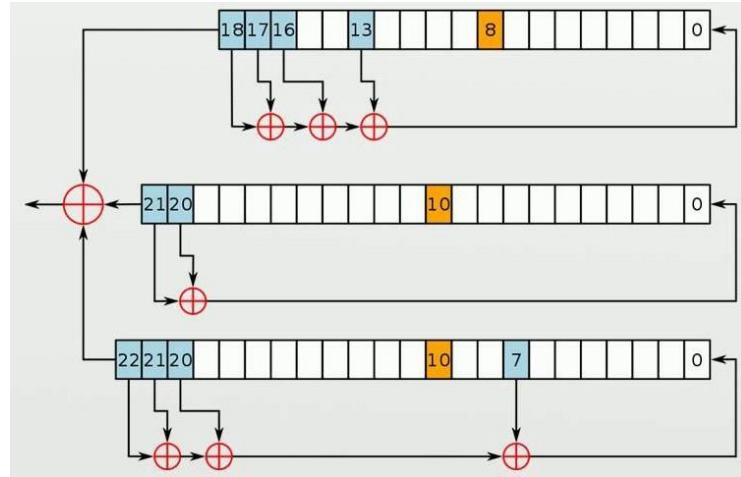


Figure 4 Stream Ciphers (Source: Wikipedia)

### **Self-Synchronizing Stream Ciphers**

A self-synchronizing or asynchronous stream cipher is one in which the keystream is generated as a function of the key and a fixed number of previous ciphertext digits. The encryption function can be described by the equations:

$$u_i = (c_{i-t}, c_{i-t+1}, \dots, c_{i-1})$$

$$z_i = g(u_i, k)$$

$$c_i = h(z_i, m_i)$$

Where:

1.  $u_0 = (c_{-t}, c_{-t+1}, \dots, c_{-1})$  is the (non-secret) initial state
2.  $k$  is the key
3.  $g$  is the function which produces the keystream  $z_i$
4.  $h$  is the output function which combines the keystream and plaintext  $m_i$  to produce ciphertext  $c_i$

Properties of self-synchronizing Stream Ciphers:

1. **Self-Synchronization** - is possible if ciphertext digits are deleted or inserted, because the decryption mapping depends only on a fixed number of preceding ciphertext characters.

2. **Limited Error Propagation** - Suppose that the state of a self-synchronization stream cipher depends on  $t$  previous ciphertext digits. If a single ciphertext digit is modified (or even deleted or inserted) during transmission, then decryption of up to  $t$  subsequent ciphertext digits may be incorrect, after which correct decryption resumes.
3. **Active Attacks** - Property (2) implies that any modification of ciphertext digits by an active adversary causes several other ciphertext digits to be decrypted incorrectly, thereby improving (compared to synchronous stream ciphers) the likelihood of being detected by the decryptor. As a consequence of property (1), it is more difficult (than for synchronous stream ciphers) to detect insertion, deletion, or replay of ciphertext digits by an active adversary.
4. **Diffusion of Plaintext Statistics** - Since each plaintext digit influences the entire following ciphertext, the statistical properties of the plaintext are dispersed through the ciphertext. Hence, self-synchronizing stream ciphers may be more resistant than synchronous stream ciphers against attacks based on plaintext redundancy.

## Aim/Objectives

The purpose of the 4<sup>th</sup> Week is to introduce the concept of randomness and pseudorandomness as well as stream ciphers. First the properties of randomness are explained as well as the difficulty faced in order to create random numbers. Then we explain several ways of getting random values either in software or physical phenomena, as well as we discuss ways that those values might be affected and not be random. Finally we discuss stream ciphers and explain the methodology and the properties synchronous and self-synchronizing stream ciphers have.

## Learning Outcomes

After the successful completion of the 4<sup>th</sup> Week, students should be able to:

- Explain the hardness of generating random values
- Explain ways to create random values using software or physical phenomena
- Explain how random values might be affected and not be random
- Explain how pseudorandom generators work and how they can be used
- Explain the importance of stream ciphers in cryptography
- Explain the differences as well as the properties of synchronous and self-synchronizing stream ciphers

## Key Words

Pseudorandom	Stream	Randomness
Polynomial	Error Propagation	Synchronization
Active Attacks	Statistics Diffusion	

## Annotated Bibliography

### Basic

- C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2010, Chapter 2 “Stream Ciphers”

The second Chapter of this book introduces random and pseudorandom number generators as well as stream ciphers. Goes through several stream ciphers and explains their advantages and disadvantages against other forms of ciphers.

### Suggestions for further reading

- Pseudorandom Generators,  
<https://www.coursera.org/lecture/cryptography/pseudorandom-generators-okKCx>

This video explains pseudorandom generators, how they work and their importance in cryptography.

- Khadem, Behrooz & Madadi, Ali & Bakhtiyari, Kaveh. (2018). Time/Memory/Data Trade-Off Attack on a Chaotic Pseudo-Random Generator: A Case Study of GMJK. Journal of Computational and Theoretical Nanoscience.

## Self-Assessment Exercises

### Exercise 4.1

Briefly explain pseudorandom generators. Give their difference/s from random generators.

### Exercise 4.2

Explain random generators, the difficulty of creating one, as well as hardware and software random generators and ways of ensuring that any patterns in bits can be eliminated.

**Exercise 4.3**

Briefly explain the two types of stream ciphers.

**Exercise 4.4**

List and explain the properties of synchronous and self-synchronizing stream ciphers.

**Recommended time for the student to work**

15 hours

## BLOCK CIPHERS

(5<sup>th</sup> Week)

### Summary

In this week, block ciphers will be covered and evaluated as well as the most common modes of operation of block ciphers will be shown and discussed.

### Introductory Remarks

A block cipher is a function which maps **n-bit plaintext blocks** to **n-bit ciphertext blocks**;  $n$  is called the **blocklength**. It may be viewed as a simple substitution cipher with large character size. The function is parameterized by a  $k$ -bit key  $K$ , taking values from a subset  $K$  (the key space) of the set of all  $k$ -bit vectors  $V_k$ . It is generally assumed that the key is chosen at random. Use of plaintext and ciphertext blocks of equal size avoids data expansion. To allow unique decryption, the encryption function must be one-to-one (i.e., invertible). For **n-bit** plaintext and ciphertext blocks and a fixed key, the encryption function is a bijection, defining a permutation on  $n$ -bit vectors. Each key potentially defines a different bijection. The number of keys is  $|K|$ , and the effective key size is  $\log_{10} |K|$ . This equals the key length if all  $k$ -bit vectors are valid keys ( $K = V_k$ ).

If keys are equiprobable and each defines a different bijection, the entropy of the key space is also  $\log_{10} |K|$ . Block ciphers can be either symmetric-key or public-key.

Symmetric-key block ciphers are the most prominent and important elements in many cryptographic systems. Individually, they provide confidentiality, as a fundamental building block, their versatility allows construction of pseudorandom number generators, stream ciphers, MACs, and hash functions. They may furthermore serve as a central component in message authentication techniques, data integrity mechanisms, entity authentication protocols, and (symmetric-key) digital signature schemes.

The **unicity distance** of a cipher is the minimum amount of ciphertext (i.e. the number of characters) required to allow a computationally unlimited adversary to recover the unique encryption key. It is a theoretical measure usually used to find if a cipher is perfectly secret or

computationally secure. However, that does **not** mean that a small unicity distance cipher is insecure in practice. Many criteria can be used to evaluate block ciphers, including:

1. **Estimated Security Level** – confidence in the security of a cipher grows if it has been subjected to (and withstood) expert cryptanalysis over a substantial time period. The amount of ciphertext required to mount practical attacks often vastly exceeds a cipher's unicity distance, which provides a theoretical estimate of the amount of ciphertext required to recover the unique encryption key
2. **Key Size** – the effective bit-length of the key, defines an upper bound on the security of a cipher. Typically, longer keys impose additional costs (i.e. generation, transmission, storage etc.)
3. **Throughput** – the data transfer in either hardware or software. It is related to the complexity of the cryptographic mapping and the degree to which the mapping is tailored to a particular implementation medium or platform
4. **Block Size** – it impacts both security and complexity as well as it affects the performance
5. **Complexity of Cryptographic Mapping** – algorithmic complexity affects the implementation costs both in terms of development and fixed sources as well as real-time performance for fixed sources (throughput). That is why sometimes hardware is preferred instead of software
6. **Data Expansion** – it is desirable and often mandatory that the encryption scheme does not increase the size of plaintext data
7. **Error Propagation** – decryption of ciphertext containing bit errors may result in various effects on the recovered plaintext, including propagation of errors to subsequent plaintext blocks

To evaluate block cipher security, it is customary to always assume that an adversary:

1. has access to all data transmitted over the ciphertext channel
2. knows all the details of the encryption function except the secret key (Kerckhoffs' principle)

Under standard assumptions, attacks are classified based on what information a cryptanalyst has access to in addition to intercepted ciphertext. The most prominent classes of attack for symmetric-key ciphers are (for a fixed key):

1. ciphertext-only – no additional information is available
2. known-plaintext – plaintext-ciphertext pairs are available.

3. chosen-plaintext – ciphertexts are available corresponding to plaintexts of the adversary's choice. A variation is an adaptive chosen-plaintext attack, where the choice of plaintexts may depend on previous plaintext-ciphertext pairs.

**Ciphertext-Only Attack (COA)** is an attack model where the attacker is assumed to have access only to a set of ciphertexts. In practice, the attacker might have some knowledge of the plaintext. For example, the attacker might know the language in which the plaintext is written or the expected statistical distribution of characters in the plaintext.

**Known-Plaintext Attack (KPA)** is an attack model where the attacker has access to both the plaintext, and the ciphertext. This can be used to reveal further secret information such as secret keys.

**Chosen-Plaintext Attack (CPA)** is an attack model which presumes that the attacker can obtain the ciphertexts for arbitrary plaintexts. The goal of the attack is to gain information that reduces the security of the encryption scheme. Modern ciphers aim to provide semantic security, also known as **ciphertext indistinguishability** under chosen-plaintext attack, and are therefore by design generally immune to chosen-plaintext attacks if correctly implemented. It is customary to use ciphers **resistant** to chosen-plaintext attack even when mounting such an attack is not feasible. A cipher secure against chosen-plaintext attack is secure against known-plaintext and ciphertext-only attacks.

A **Chosen-Ciphertext Attack (CCA)** operates under the following model, an adversary is allowed to plaintext-ciphertext pairs for some number of ciphertexts of his choice, and thereafter attempts to use this information to recover the key.

In a **Related-Key Attack**, an adversary is assumed to have access to the encryption of plaintexts under both an unknown key and unknown keys chosen to have or known to have certain relationships with the key.

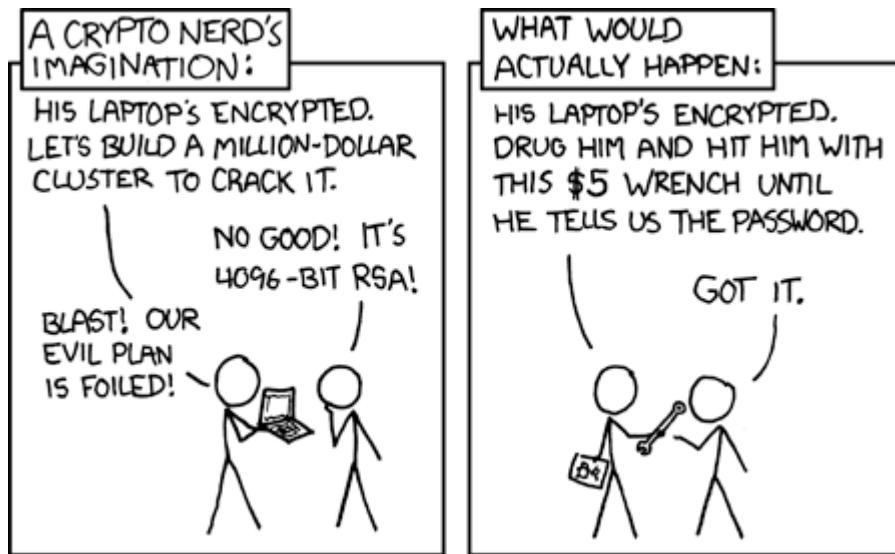


Figure 5 Funny Way of Cracking a Hard Encryption (Source **xkcd**, available at <https://xkcd.com/538/>)

With few exceptions (i.e. One-Time Pad), the best available measure of security for practical ciphers is the complexity of the best (up to date) known attack. That complexity breaks down into various aspects:

1. **Data Complexity** – expected number of input data units required (i.e. ciphertext)
2. **Storage Complexity** – expected number of storage units required
3. **Processing Complexity** – expected number of operations required to process input data and/or fill storage with data

### Block Ciphers Modes of Operation

The block ciphers have several modes of operation, with the most common ones being:

1. Electronic Codebook (ECB)
2. Cipher-Block Chaining (CBC)
3. Cipher Feedback (CFB)
4. Output Feedback (OFB)

### Electronic Codebook (ECB) Properties

1. **Identical plaintext** blocks (under the same key) result in identical ciphertext.
2. **Chaining dependencies** - blocks are enciphered independently of other blocks.  
Reordering ciphertext blocks results in correspondingly re-ordered plaintext blocks.

3. **Error propagation** - one or more bit errors in a single ciphertext block affect decipherment of that block only. For typical ciphers, decryption of such a block is then random (with about 50% of the recovered plaintext bits in error).

### Cipher Block-Chaining (CBC) Properties

1. **Identical plaintexts** - identical ciphertext blocks result when the same plaintext is enciphered under the same key and **IV** (n-bit initialization vector). Changing the IV, key, or first plaintext block results in different ciphertext.
2. **Chaining dependencies** - the chaining mechanism causes ciphertext  $c_j$  to depend on  $x_j$  and all preceding plaintext blocks. Consequently, rearranging the order of ciphertext blocks affects decryption. Proper decryption of a correct ciphertext block requires a correct preceding ciphertext block.
3. **Error propagation** - a single bit error in ciphertext block  $c_j$  affects decipherment of blocks  $c_j$  and  $c_{j+1}$ . Block  $m_j$  recovered from  $c_j$  is typically totally random (50% in error), while the recovered plaintext  $m_{j+1}$  has bit errors precisely where  $c_j$  did. Thus an adversary may cause predictable bit changes in  $m_{j+1}$  by altering corresponding bits of  $c_j$ .
4. **Error recovery** - the CBC mode is *self-synchronizing* in the sense that if an error (including loss of one or more entire blocks) occurs in block  $c_j$  but not  $c_{j+1}, c_{j+2}$  is correctly decrypted to  $m_{j+2}$

### Cipher Feedback (CFB) Properties

1. **Identical plaintexts** - as per CBC encryption, changing the **IV** results in the same plaintext input being enciphered to a different output. The IV need not be secret.
2. **Chaining dependencies** - similar to CBC encryption, the chaining mechanism causes ciphertext block  $c_j$  to depend on both  $m_j$  and preceding plaintext blocks; consequently, re-ordering ciphertext blocks affects decryption.
3. **Error propagation** - one or more bit errors in any single r-bit ciphertext block  $c_j$  affects the decipherment of that and the next  $\frac{r}{r}l$  ciphertext blocks. The recovered plaintext  $m_j$  will differ from original  $m_j$  precisely in the bit positions  $c_j$  was in error. Thus an adversary may cause predictable bit changes in  $m_j$  by altering corresponding bits of  $c_j$ .
4. **Error recovery** - the CFB mode is self-synchronizing similar to CBC, but requires  $\frac{r}{r}l$  ciphertext blocks to recover.

5. **Throughput** - for  $r < n$ , throughput is decreased by a factor of  $\frac{n}{r}$  in that each execution of Enc yields only  $r$  bits of ciphertext output.

### Output Feedback (OFB) Properties

1. **Identical plaintexts** - as per CBC and CFB modes, changing the **IV** results in the same plaintext being enciphered to a different output.
2. **Chaining dependencies** - the keystream is plaintext-independent.
3. **Error propagation** - one or more bit errors in any ciphertext character  $c_j$  affects the decipherment of only that character, in the precise bit position(s)  $c_j$  is in error, causing the corresponding recovered plaintext bit(s) to be complemented.
4. **Error recovery** - the OFB mode recovers from ciphertext bit errors, but cannot self-synchronize after loss of ciphertext bits, which destroys alignment of the decrypting keystream.
5. **Throughput** - for  $r < n$ , throughput is decreased as per the CFB mode. However, in all cases, since the keystream is independent of plaintext or ciphertext, it may be pre-computed.

### Aim/Objectives

The purpose of the 5<sup>th</sup> Week is to introduce the concept of block ciphers. The importance of block ciphers in cryptography, such as their use in pseudorandom number generators, MACs and hash functions. Four modes of operation of block ciphers are explained, namely Electronic Codebook, Cipher-Block Chaining, Cipher Feedback and Output Feedback. Their properties are listed and compared between them. Finally, several attacks are discussed and ways of preventing them.

### Learning Outcomes

After the successful completion of the 5<sup>th</sup> Week, students should be able to:

- Explain the importance of block ciphers in cryptography
- Explain the four most important modes of operation of block ciphers
- Explain the properties of each mode of operation and compare them to indicate possible scenarios that they might be used
- Explain attacks such as COA, KPA, CPA and CCA and indicate how they can be performed and how they can be stopped

## Key Words

Block	Blocklength	Known-Plaintext
Known-Ciphertext	Unicity Distance	Chaining Dependencies
Processing Complexity	Error Recovery	Throughput

## Annotated References / Bibliography

### Basic

- C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2010, Chapter 5 “More About Block Ciphers”

The fifth Chapter of this book introduces block ciphers and explains the most important modes of operation of block ciphers. In addition, it shows practical uses of block ciphers in several encryption schemes.

### Suggestions for further reading

- Introduction to Block Ciphers (CSS322, L4, Y14) – Steven Gordon, [Youtube Video], Available at: <https://www.youtube.com/watch?v=Lh4r8QkFiF0>
- T. Courtois, Nicolas & Oprisanu, Bristena & Schmeh, Klaus. (2018). Linear cryptanalysis and block cipher design in East Germany in the 1970s. *Cryptologia*

## Self-Assessment Exercises

### Exercise 5.1

Explain what Block Ciphers are and how they work.

### Exercise 5.2

What is Unicity Distance?

### Exercise 5.3

Evaluate block ciphers using a number of different criteria.

**Exercise 5.4**

Give block ciphers standard assumptions, and explain the most prominent classes of attack under those standard assumptions.

**Exercise 5.6**

List and explain the four most common modes of operation of block ciphers.

**Exercise 5.7**

Compare Block Ciphers with Stream Ciphers.

**Activity (5 points)**

Activity, that includes solving questions related to the syllabus covered up to Week 5, as well as applying the knowledge gathered up to this week in order to solve problems related to cryptography.

This activity counts 5% of the final course mark.

You will need approximately 5 hours to solve this Graded Activity

**Recommended time for the student to work**

20 hours

## DATA ENCRYPTION STANDARD - DES

6<sup>th</sup> Week

### Summary

In this week, Data Encryption Standard (DES) will be covered. In addition, the building blocks of DES, namely Product and Feistel ciphers will be introduced and discussed in detail.

### Introductory Remarks

DES is the most known symmetric-key block cipher developed by IBM and National Security Agency (NSA), based on the cipher **Lucifer**. It is recognized world-wide and 1977 it became the first commercial-grade block cipher with openly and fully specified implementation details.

Here are some interesting historical data:

1. In 1998 Electronic Frontier Foundation (EFF) demonstrated that DES could be attacked very practically, using a DES specific attack (they manage to break a DES key in 56 hours!). In 1999 EFF together with distributed.net manage to break a DES key in 22hours and 15 minutes.
2. In 1999 they decided to start using what is called as the Triple DES (3DES), which is the application of the DES algorithm three times.
3. In 2016 hashcat (an open source password cracking software) was able to brute force DES using a single NVIDIA GTX1080Ti GPU in 15 days. Using multiple GPUs or distributed computing can brute force DES in a much smaller time frame.
4. In 2017 DES was cracked in 25 seconds using a rainbow table attack. Note that extra time is needed to actually compute the rainbow tables which is not included in the 25 seconds

The design of DES is related to two general concepts: product ciphers and Feistel ciphers. Each involves iterating a common sequence or round of operations.

A **Product cipher** combines two or more transformations in a manner intending that the resulting cipher is more secure than the individual components.

Combines a sequence of simple transformations such as substitution (S-box), permutation (P-box), and modular arithmetic.

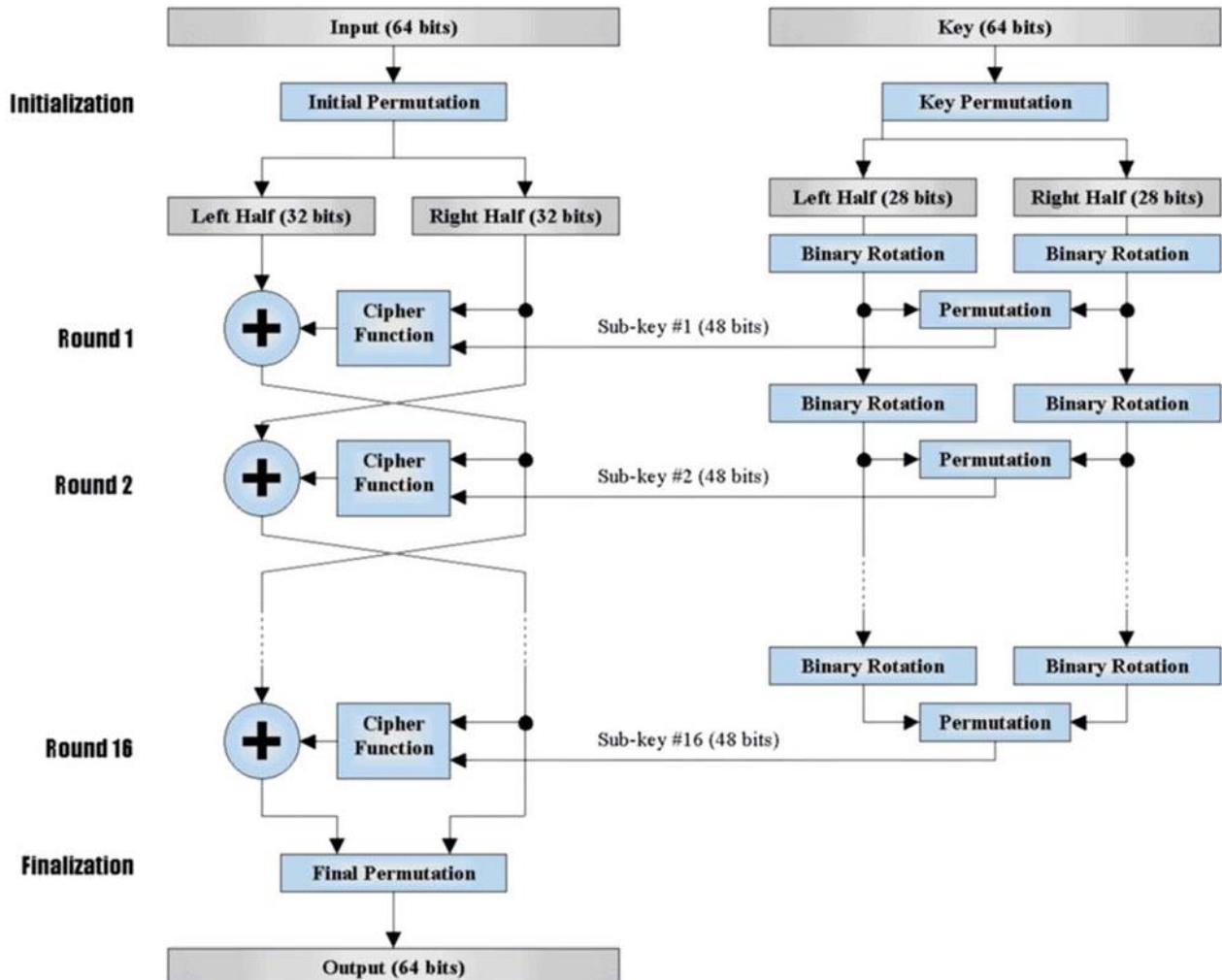


Figure 6 DES (Available at [www.cybrary.it](http://www.cybrary.it))

A **permutation box** (or **P-box**) is a method of bit-shuffling used to permute or transpose bits across S-boxes inputs, retaining diffusion while transposing.

A **substitution box** (or **S-box**) takes some number of input bits, **m**, and transforms them into some number of output bits, **n**, where **n** is not necessarily equal to **m**.

A **Feistel cipher** is an iterated cipher mapping a  $2t$ -bit plaintext  $(L_0, R_0)$ , for  $t$ -bit blocks  $L_0$  and  $R_0$ , to a ciphertext  $(R_r, L_r)$ , through an  $r$ -round process where  $r \geq 2: 1$ .

Let  $F$  be the round function and let  $K_0, K_1, \dots, K_n$  be the sub-keys for the rounds  $0, 1, \dots, n$  respectively.

Suppose that a message has 12 bits and is written as  $L_0R_0$ , where  $L_0$  consists of the first 6 bits and  $R_0$  consists of the last 6 bits.

The key  $K$  has 9 bits. The  $i^{\text{th}}$  round of the algorithm transforms an input  $L_{i-1}R_{i-1}$  to the output  $L_iR_i$  using an 8-bit key  $K_i$  derived from  $K$ .

The main part of the encryption process is a function  $f(R_{i-1}, K_i)$  that takes a 6-bit input  $R_{i-1}$  and an 8-bit input  $K_i$  and produces a 6-bit output which will be described later.

The output of the  $i^{\text{th}}$  round is defined as:

$$L_i = R_{i-1} \text{ and } R_i = L_{i-1} \text{ XOR } f(R_{i-1}, K_i)$$

The **decryption** is the reverse of encryption.

$$[L_n] [R_n \text{ XOR } f(L_n, K_n)] = \square = [R_{n-1}] [L_{n-1}]$$

## Aim/Objectives

The purpose of the 6<sup>th</sup> Week is to introduce the Data Encryption Standard (DES) and explain its importance in cryptography. In addition, we explain how DES evolved and how it was attacked which forced the community to find solutions such as the 3DES. Furthermore, we explain the building blocks of DES, product and Feistel ciphers.

## Learning Outcomes

After the successful completion of the 6<sup>th</sup> Week, students should be able to:

- Evaluate Data Encryption Standard (DES)
- Explain how DES was attacked
- Explain the use of 3DES
- Evaluate the two building blocks of DES, namely Product and Feistel ciphers

## Keywords

Permutation	Substitution	Feistel Cipher
Rounds	Lucifer	3DES
Product Cipher	Sequence	Blocks

## Annotated Bibliography

### Basic

- C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2010, Chapter 3 "The Data Encryption Standard (DES) and Alternatives"

The third Chapter of this book introduces DES, shows its design in order to explain some technical terms regarding modern cryptography. In addition, it goes through security analysis of DES and shows some DES alternatives such as 3DES.

### Suggestions for further reading

- Data Encryption Standard,  
[https://www.tutorialspoint.com/cryptography/data\\_encryption\\_standard.htm](https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm)  
This website explains in detail the DES, giving examples as well as useful figures to understand how DES works internally.
- D. Coppersmith, "The Data Encryption Standard (DES) and its strength against attacks," in IBM Journal of Research and Development, vol. 38, no. 3, pp. 243-250, May 1994.

## Self-Assessment Exercises

### Exercise 6.1

Briefly explain the two concepts DES is related to.

### Exercise 6.2

What is the difference between an S-box and a P-box

## Recommended time for the student to work

15 hours

### Summary

In this week, Message Authentication Codes (MACs) will be covered, as well as the methodology that one follows in order to use MACs. In addition, use cases of MACs will be discussed.

### Introductory Remarks

One of the most basic goals of cryptography is to enable parties to communicate over an open communication channel in a **secure** way. However, not all security concerns are related to secrecy. In many cases, it is of equal or greater importance to **guarantee message integrity** (or **message authentication**) in the sense that each party should be able to identify when a message it receives was sent by the party claiming to send it, and was not modified in transit.

Consider the case of a user communicating with their bank over the Internet. When the bank receives a request to transfer \$1,000 from the user's account to the account of some other user X, the bank has to consider the following:

1. Is the request authentic? That is, did the user in question really issue this request, or was the request issued by an adversary (perhaps X itself) who is impersonating the legitimate user?
2. Assuming a transfer request was issued by the legitimate user, are the details of the request as received exactly those intended by the legitimate user? Or was, e.g., the transfer amount modified?

A second scenario where the need for message integrity arises in practice is with regard to web cookies.

The HTTP protocol used for web traffic is stateless, and so when a client and server communicate in some session (e.g., when a user [client] shops at a merchant's [server's] website), any state generated as part of that session (e.g., the contents of the user's shopping cart) is often placed in a "cookie" that is stored by the client and sent from the client to the server as part of each message the client sends.

Assume that the cookie stored by some user includes the items in the user's shopping cart along with a price for each item, as might be done if the merchant offers different prices to different

users (reflecting, e.g., discounts and promotions, or user-specific pricing). It should be infeasible here for the user to modify the cookie that it stores so as to alter the prices of the items in its cart. The merchant thus needs a technique to ensure the integrity of the cookie that it stores at the user. Note that the contents of the cookie (namely, the items and their prices) are not secret and, in fact, must be known by the user. The problem here is thus purely one of integrity.

Just as the goals of secrecy and message integrity are different, so are the techniques and tools for achieving them.

Secrecy and integrity are often confused and unnecessarily intertwined, so let us be clear up front: **encryption** does not (in general) provide any integrity, and encryption should never be used with the intent of achieving message authentication unless it is specifically designed with that purpose in mind.

One might mistakenly think that encryption solves the problem of message authentication. (In fact, this is a common error.) This is due to the fuzzy, and incorrect, reasoning that since a ciphertext completely hides the contents of the message, an adversary cannot possibly modify an encrypted message in any meaningful way. Despite its intuitive appeal, this reasoning is completely false. We illustrate this point by showing that all the encryption schemes we have seen thus far do not provide message integrity.

### Encryption using stream ciphers

Consider the simple encryption scheme in which  $\text{Enc}_k(m)$  computes the ciphertext  $c \triangleq G(k) \oplus m$ , where  $G$  is a pseudorandom generator.

Ciphertexts in this case are very easy to manipulate: flipping any bit in the ciphertext  $c$  results in the same bit being flipped in the message that is recovered upon decryption. Thus, given a ciphertext  $c$  that encrypts a (possibly unknown) message  $m$ , it is possible to generate a modified ciphertext  $c'$  such that  $m' \triangleq \text{Dec}_k(c')$  is the same as  $m$  but with one (or more) of the bits flipped. This simple attack can have severe consequences

As an example, consider the case of a user encrypting some amount of money he wants to transfer from his bank account, where the amount is represented in binary. Flipping the least significant bit has the effect of changing this amount by only €1, but flipping the 11th least significant bit changes the amount by more than €1,000!

Interestingly, the adversary in this example does not necessarily learn whether it is increasing or decreasing the initial amount, i.e., whether it is flipping a 0 to a 1 or vice versa. But if the adversary has some partial knowledge about the amount—say, that it is less than €1,000 to begin with—

then the modifications it introduces can have a predictable effect. We stress that this attack does not contradict the secrecy of the encryption scheme.

In fact, the exact same attack applies to the one-time pad encryption scheme, showing that even perfect secrecy is not sufficient to ensure the most basic level of message integrity.

We have seen that, in general, encryption does not solve the problem of message integrity. Rather, an additional mechanism is needed that will enable the communicating parties to know whether or not a message was tampered with. The right tool for this task is a **Message Authentication Code (MAC)**.

The aim of a message authentication code is to prevent an adversary from modifying a message sent by one party to another, or from injecting a new message, without the receiver detecting that the message did not originate from the intended party.

As in the case of encryption, this is only possible if the communicating parties share some secret that the adversary does not know (otherwise nothing can prevent an adversary from impersonating the party sending the message).

Here, we will continue to consider the private key setting where the parties share the same secret key.

Before formally defining security of a message authentication code, we first define what a MAC is and how it is used.

Two users who wish to communicate in an authenticated manner begin by generating and sharing a secret key  $k$  in advance of their communication. When one party wants to send a message  $m$  to the other, she computes a **MAC tag**  $t$  based on the message and the shared key, and sends the message  $m$  and the **tag**  $t$  to the other party.

The tag is computed using a tag-generation algorithm denoted by  $Mac$ ; thus, rephrasing what we have already said, the sender of a message  $m$  computes  $t \leftarrow Mac_k(m)$  and transmits  $(m, t)$  to the receiver. Upon receiving  $(m, t)$ , the second party verifies whether  $t$  is a valid tag on the message  $m$  (with respect to the shared key) or not.

This is done by running a verification algorithm  $Vrfy$  that takes as input the shared key as well as a message  $m$  and a tag  $t$ , and indicates whether the given tag is valid.

Formally:

A message authentication code (MAC) consists of three probabilistic polynomial-time algorithms ( $Gen$ ,  $Mac$ ,  $Vrfy$ ) such that:

1. The key-generation algorithm  $Gen$  takes as input the security parameter  $1^n$  and outputs a key  $k$  with  $|k| \geq n$

2. The tag-generation algorithm  $Mac$  takes as input a key  $k$  and a message  $m$ , and outputs a tag  $t$ . Since the algorithm may be randomized, we write this as  $t \leftarrow Mac_k(m)$
3. The deterministic verification algorithm  $Vrfy$  takes as input a key  $k$ , a message  $m$  and a tag  $t$ . It outputs a bit  $b$ , with  $b = 1$  meaning valid and  $b = 0$  meaning invalid. We write this as

$$b \triangleq Vrfy_k(m, t)$$

Note: It is required that for every  $n$ , every key  $k$  output by  $Gen(1^n)$ , and every  $m$ , it holds that

$$Vrfy_k(m, Mac_k(m)) = 1$$

The intuitive idea behind the definition is that no efficient adversary should be able to generate a valid tag on any “new” message that was not previously sent (and authenticated) by one of the communicating parties.

As with any security definition, to formalize this notion we have to define both the adversary’s power as well as what should be considered a “break.” As usual, we consider only probabilistic polynomial-time adversaries and so the real question is how we model the adversary’s interaction with the communicating parties.

In the setting of message authentication, an adversary observing the communication between the honest parties may be able to see all the messages sent by these parties along with their corresponding MAC tags.

The adversary may also be able to influence the content of these messages, whether directly or indirectly (if, e.g., external actions of the adversary affect the messages sent by the parties).

For example, in a web cookie, where the user’s own actions influence the contents of the cookie being stored on his computer.

To formally model the above we allow the adversary to request MAC tags for any messages of its choice. Formally, we give the adversary access to a MAC  $Mac_k(\cdot)$ ; the adversary can repeatedly submit any message  $m$  of its choice to  $Mac_k(\cdot)$ , and is given in return a tag  $t \leftarrow Mac_k(m)$ . (For a fixed-length MAC, only messages of the correct length can be submitted.)

We will consider it a “break” of the scheme if the adversary is able to output any message  $m$  along with a tag  $t$  such that:

1.  $t$  is a valid tag on the message  $m$  (i.e.,  $Vrfy_k(m, t) = 1$ )
2. the adversary had not previously requested a **MAC tag** on the message  $m$

The first condition means that if the adversary were to send  $(m, t)$  to one of the honest parties, then this party would be mistakenly fooled into thinking that  $m$  originated from the legitimate party since  $Vrfy_k(m, t) = 1$ .

The second condition is required because it is always possible for the adversary to just copy a message and MAC tag that were previously sent by one of the legitimate parties (and, of course, these would be accepted as valid). Such a **replay attack** is not considered a “break” of the message authentication code. This does not mean that replay attacks are not a security concern; they are, and we will discuss them later on.

A MAC satisfying the level of security specified above is said to **be existentially unforgeable under an adaptive chosen-message attack**.

“**Existential unforgeability**” refers to the fact that the adversary must not be able to forge a valid tag on any message.

“**Adaptive chosen-message attack**” refers to the fact that the adversary is able to obtain MAC tags on arbitrary messages chosen adaptively during its attack.

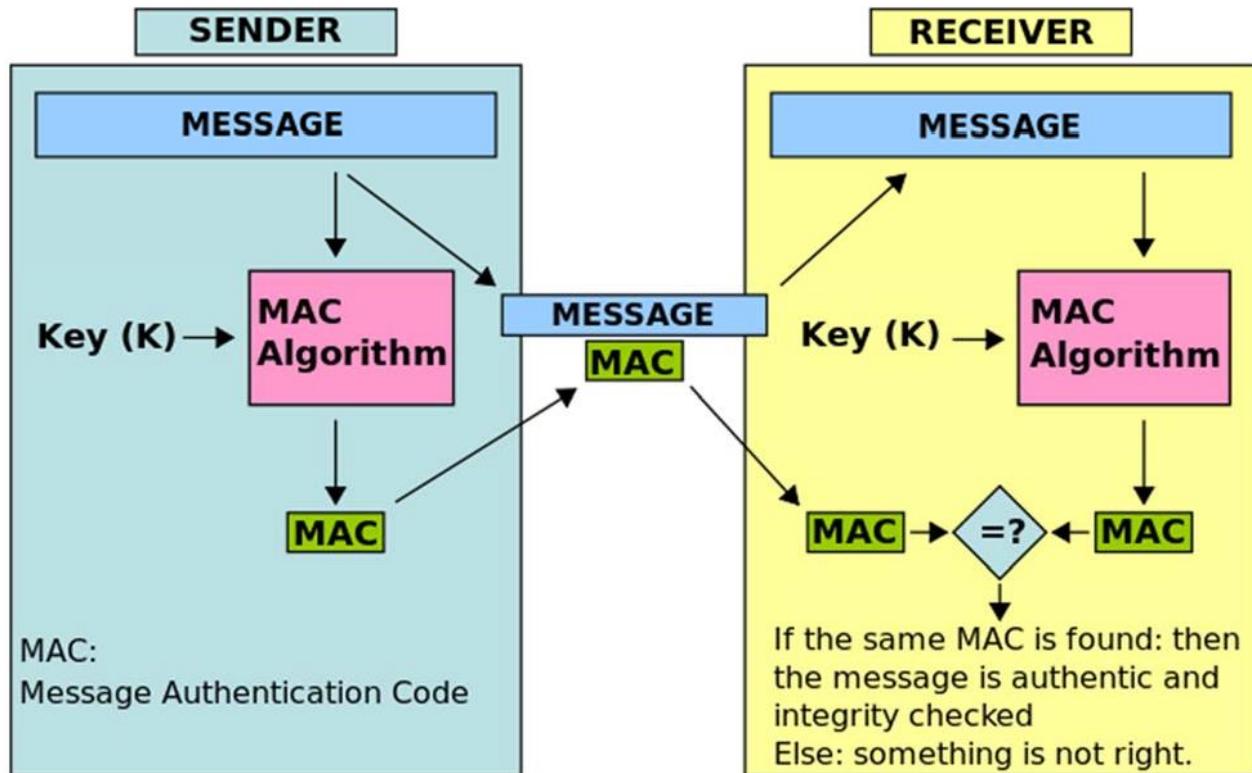


Figure 7 Message Authentication Code (Source Wikipedia)

Toward the formal definition, consider the following experiment for a message authentication code  $\mathcal{H} = (\text{Gen}, \text{Mac}, \text{Vrfy})$ , an adversary  $A$ , and value  $n$  for the security parameter:

1. A key  $k$  is generated by running  $\text{Gen}(1^n)$
2. The adversary  $A$  is given input  $1^n$  and access to  $\text{Mac}_k(\cdot)$ . The adversary eventually outputs  $(m, t)$ . Let  $Q$  denote the set of all queries that  $A$  asked  $\text{Mac}_k(\cdot)$
3.  $A$  succeeds if and only if:

- a)  $Vrfy_k(m, t) = 1$
- b)  $m \in Q$

A MAC is secure if no efficient adversary can succeed in the above experiment with non-negligible probability.

Therefore, we can conclude that:

A message authentication code  $\Pi = (Gen, Mac, Vrfy)$  is existentially unforgeable under an adaptive chosen-message attack, or just secure, if for all probabilistic polynomial-time adversaries A, there is a negligible function  $negl$  such that:

$$\Pr[MacForge_{A,\Pi}(n) = 1] : s: negl(n)$$

The above definition is rather strong in two respects:

1. The adversary is allowed to request MAC tags for any messages of its choice
2. The adversary is considered to have “broken” the scheme if it can output a valid tag on any previously unauthenticated message.

One might object that both these components of the definition are unrealistic and overly strong: in “real-world” usage of a MAC, the honest parties would only authenticate “meaningful” messages, and similarly it should only be considered a breach of security if the adversary can forge a valid tag on a “meaningful” message.

The crucial point is that what constitutes a meaningful message is entirely application dependent. While some applications of a MAC may only ever authenticate English-text messages, other applications may authenticate spreadsheet files, others database entries, and others raw data. Protocols may also be designed where anything will be authenticated—in fact, certain protocols for entity authentication do exactly this. By making the definition of security for MACs as strong as possible, we ensure that secure MACs are broadly applicable for a wide range of purposes, without having to worry about compatibility of the MAC with the semantics of the application.

We emphasize that message authentication codes on their own, offer no protection against replay attacks.

Replay attacks are when a previously sent message (and its MAC tag) are replayed to an honest party. Replay attacks are a serious concern.

Consider the scenario where a user (say, Alice) sends a request to her bank to transfer €1,000 from her account to some other user (say, Bob). In doing so, Alice can compute a MAC tag and append it to the request so the bank knows the request is authentic.

If the MAC is secure, Bob will be unable to intercept the request and change the amount to €10,000 because this would involve forging a valid tag on a previously unauthenticated message. However, nothing prevents Bob from intercepting Alice's message and replaying it ten times to the bank. If the bank accepts each of these messages, the net effect is that €10,000 will be transferred to Bob's account rather than the desired €1,000.

Two common techniques for preventing replay attacks are to use **sequence numbers** (also known as counters) or **time-stamps**.

The first approach, requires the communicating users to maintain (synchronized) state, and can be problematic when users communicate over a lossy channel where messages are occasionally dropped.

In the second approach, using time-stamps, the sender prepends the current time  $T$  (say, to the nearest millisecond) to the message before authenticating, and sends  $T$  along with the message and the resulting **tag**  $t$ . When the receiver obtains  $T, m, t$ , it verifies that  $t$  is a valid tag and that  $T$  is within some acceptable clock skew from the current time  $T'$  at the receiver. This method has certain drawbacks as well, including the need for the sender and receiver to maintain closely synchronized clocks, and the possibility that a replay attack can still take place if it is done quickly enough (specifically, within the acceptable time window).

Pseudorandom functions are a natural tool for constructing secure message authentication codes. Intuitively, if the MAC tag  $t$  is obtained by applying a pseudorandom function to the message  $m$ , then forging a tag on a previously unauthenticated message requires the adversary to correctly guess the value of the pseudorandom function at a "new" input point.

The probability of guessing the value of a random function on a new point is  $2^{-n}$  (if the output length of the function is  $n$ ). The probability of guessing such a value for a pseudorandom function can be only negligibly greater.

This idea can be expressed as follows:

Let  $F$  be a pseudorandom function. Define a fixed-length MAC for messages of length  $n$  as follows:

1. *Mac*: on input a key  $k \in \{0, 1\}^n$  and a message  $m \in \{0, 1\}^n$ , output the tag  $t \in F_k(m)$
2. *Vrfy*: on input a key  $k \in \{0, 1\}^n$ , a message  $m \in \{0, 1\}^n$ , and a tag  $t \in \{0, 1\}^n$ , output 1 if and only if  $t = F_k(m)$

CBC-MAC is a standardized message authentication code used widely in practice. A basic version of CBC-MAC, secure when authenticating messages of any fixed length, is given below:

Let  $F$  be a pseudorandom function, and fix a length function  $l > 0$ . The basic CBC-MAC construction is as follows:

1. *Mac*: on input a key  $k \in \{0, 1\}^n$  and a message  $m$  of length  $l(n) \cdot n$ , do the following:
  - a. Parse  $m$  as  $m = m_1, \dots, m_l$  where each  $m_i$  is of length  $n$
  - b. Set  $t_0 \leftarrow 0^n$ . Then, for  $i = 1$  to  $l$  set  $t_i \leftarrow F_k(t_{i-1} \oplus m_i)$
2. *Vrfy*: on input a key  $k \in \{0, 1\}^n$ , a message  $m$ , and a **tag**  $t$ , do: If  $m$  is not of length  $l(n) \cdot n$  then output 0. Otherwise, output 1 if and only if  $t = Mac_k(m)$

Over the last weeks, we studied how it is possible to obtain secrecy in the private-key setting using encryption. This week, we have shown how to ensure integrity using message authentication codes.

One might naturally want to achieve both goals simultaneously, and this is the problem we turn to now.

It is best practice to always ensure **secrecy** and **integrity** by default in the private-key setting. Indeed, in many applications where secrecy is required it turns out that integrity is essential also. Moreover, a lack of integrity can sometimes lead to a breach of secrecy.

At an abstract level, our goal is to realize an “ideally secure” communication channel that provides both secrecy and integrity.

Such a definition is extremely hard, instead, lets provide a simpler set of definitions that treat secrecy and integrity separately.

These definitions and our subsequent analysis suffice for understanding the key issues at hand. Let  $\mathcal{II} = (\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$  be a private-key encryption scheme. As mentioned already, we define security by separately defining secrecy and integrity. The notion of secrecy we consider is that we require to be secure against chosen-ciphertext attacks (**CCA-Secure**)

We are concerned about chosen-ciphertext attacks here because we are explicitly considering an active adversary who can modify the data sent from one honest party to the other. Our notion of integrity will be essentially that of existential unforgeability under an adaptive chosen-message attack. Since  $\mathcal{II}$  does not satisfy the syntax of a message authentication code, however, we introduce a definition specific to this case.

Consider the following experiment defined for a private-key encryption scheme  $\mathcal{II} = (\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ , adversary  $A$ , and value  $n$  for the security parameter

The unforgeable encryption experiment  $\mathit{EncForge}_{A,\mathcal{II}}(n)$ :

1. Run  $\mathit{Gen}(1^n)$  to obtain a key  $k$
2. The adversary  $A$  is given input  $1^n$  and access to an encryption  $\mathit{Enc}_k(\cdot)$

3. Let  $m \in Dec_k(c)$ , and let  $Q$  denote the set of all queries that  $A$  asked its encryption  $Enc_k(\cdot)$ .  
The output of the experiment is 1 if and only if  $m \in Q$

Using the experiment described we can conclude to two definitions:

1. A private-key encryption scheme  $\Pi$  is unforgeable if for all probabilistic polynomial-time adversaries  $A$ , there is a negligible function  $negl$  such that

$$Pr[EncForge_{A,\Pi}(n) = 1] : s: negl(n)$$

2. A private-key encryption scheme is an authenticated encryption scheme if it is CCA-secure and unforgeable.

## Aim/Objectives

The purpose of the 7<sup>th</sup> Week is to introduce the concept of Message Authentication Codes (MACs). The notions of message integrity and message authentication are explained with example scenarios. We take a look at the HTTP protocol and how one can edit information to affect shopping cards or even replay messages to transfer money. Then we explain how stream ciphers and pseudorandom generators can be used to help solve the problems.

## Learning Outcomes

After the successful completion of the 7<sup>th</sup> Week, students should be able to:

- Evaluate Message Authentication Codes
- Explain the term Message Integrity
- Give scenarios that Message Integrity is really important
- Explain the use of pseudorandom generators as well as stream ciphers in the context of MACs
- Explain the term Existential Unforgeability
- Evaluate attacks such as Adaptive Chosen-Message

## Key Words

MAC	Guarantee	Authentication
Integrity	Existential Unforgeability	Tag
Significant Attacks	PPT Algorithms	Replay Attack

## Annotated Bibliography

### Basic

- C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2010, Chapter 12 “Message Authentication Codes (MACs)”

The twelfth Chapter of this book introduces MACs, shows the basic principle behind MACs as well as the security properties that can be achieved using MACs. In addition, it explains the relationship between MACs, hash functions and block ciphers.

### Suggestions for further reading

- Message Authentication Code by WikiAudio [Youtube Video], Available at <https://www.youtube.com/watch?v=N6tKTI9ZcJ0>

This video explains how MACs work and how are used in real life

- Bernstein D.J. (2005) The Poly1305-AES Message-Authentication Code. In: Gilbert H., Handschuh H. (eds) Fast Software Encryption. FSE 2005. Lecture Notes in Computer Science, vol 3557. Springer, Berlin, Heidelberg

## Self-Assessment Exercises

### Exercise 7.1

Give an example in which message integrity is needed

### Exercise 7.2

Give an example in which an attack can affect a message encrypted using stream ciphers

### Exercise 7.3

Explain the aim of MAC and explain how it works

**Exercise 7.4**

Give a formal definition of MAC

**Recommended time for the student to work**

15 hours

### Summary

In this week, we will discuss the idea of hash functions. We will discuss the different types of hash functions such as the keyed and unkeyed ones, as well as how hash functions are used. In addition, we will discuss collision resistance as well as preimage resistance terms.

### Introductory Remarks

At the most basic level, a hash function provides a way to map a long input string to a shorter output string sometimes called a **digest**. The primary requirement is to avoid collisions, or two inputs that map to the same digest.

Collision-resistant hash functions have numerous uses. One example is HMAC, achieving domain extension for message authentication codes. Beyond that, hash functions have become ubiquitous in cryptography, and they are often used in scenarios that require properties much stronger than collision resistance.

It has become common to model cryptographic hash functions as being “completely unpredictable”. Hash functions are intriguing in that they can be viewed as lying between the worlds of private and public-key cryptography.

On the one hand, they are (in practice) constructed using symmetric-key techniques, and many of the canonical applications of hash functions are in the symmetric-key setting. From a theoretical point of view, however, the existence of collision-resistant hash functions appears to represent a qualitatively stronger assumption than the existence of pseudorandom functions.

Hash functions may be split into two classes:

1. **Unkeyed hash functions:** whose specification dictates a single input parameter (a message)
2. **Keyed hash functions:** whose specification dictates two distinct inputs, a message and a secret key

For actual use, a more goal-oriented classification of hash functions (beyond *keyed* vs. *unkeyed*) is necessary, based on further properties they provide and reflecting requirements of specific

applications. Of the numerous categories in such a *functional classification*, two types of hash functions will be discussed in this course:

1. **Modification Detection Codes** (MDCs), also known as *manipulation detection codes*, and less commonly as *message integrity codes* (MICs), the purpose of an MDC is to provide a representative image or *hash* of a message. The end goal is to facilitate, in conjunction with additional mechanisms, data integrity assurances as required by specific applications. MDCs are a subclass of *unkeyed* hash functions, and themselves may be further classified as:
  - i. *one-way hash functions* (**OWHFs**): for these, finding an input which hashes to a pre-specified hash-value is difficult
  - ii. *collision resistant hash functions* (**CRHFs**): for these, finding any two inputs having the same hash-value is difficult.
2. **Message Authentication Codes** (MACs), the purpose of a MAC is (informally) to facilitate, without the use of any additional mechanisms, assurances regarding both the source of a message and its integrity (See Lecture 7). MACs have two functionally distinct parameters, a message input and a secret key; they are a subclass of *keyed* hash functions.

## Hash Functions

Hash functions are simply functions that take inputs of some length and **compress** them into short, fixed-length outputs. The classic use of hash functions is in data structures, where they can be used to build hash tables that enable  $O(1)$  lookup time when storing a set of elements. Specifically, if the range of the hash function  $H$  is of size  $N$ , then element  $x$  is stored in row  $H(x)$  of a table of size  $N$ . To retrieve  $x$ , it suffices to compute  $H(x)$  and probe that row of the table for the elements stored there. A “good” hash function for this purpose is one that yields few collisions, where a collision is a pair of distinct items  $x$  and  $x'$  for which  $H(x) = H(x')$ ; in this case we also say that  $x$  and  $x'$  collide.

## Collision Resistance

**Collision-resistant** hash functions are similar in spirit. Again, the goal is to avoid collisions. However, there are fundamental differences. For one, the desire to minimize collisions in the setting of data structures becomes a requirement to avoid collisions in the setting of cryptography. Furthermore, in the context of data structures we can assume that the set of data elements is chosen independently of the hash function and without any intention to cause collisions. In the

context of cryptography, in contrast, we are faced with an adversary who may select elements with the explicit goal of causing collisions. This means that collision-resistant hash functions are much harder to design.

Informally, a function  $H$  is **collision resistant** if it is infeasible for any probabilistic polynomial-time algorithm to find a collision in  $H$ . We will only be interested in hash functions whose domain is larger than their range. In this case collisions must exist, but such collisions should be hard to find. Formally, we consider **keyed hash functions**. That is,  $H$  is a two-input function that takes as input a key  $\mathbf{s}$  and a string  $\mathbf{x}$ , and outputs a string  $H^s(x) \in H(s, x)$ . The requirement is that it must be hard to find a collision in  $H^s$  for a randomly generated key  $\mathbf{s}$ . There are at least two differences between keys in this context and keys as we have used them until now:

1. Not all strings necessarily correspond to valid keys (i.e.,  $H^s$  may not be defined for certain  $\mathbf{s}$ ), and therefore the key  $\mathbf{s}$  will typically be generated by an algorithm **Gen** rather than being chosen uniformly.
2. More importantly, this key  $\mathbf{s}$  is (generally) not kept secret, and collision resistance is required even when the adversary is given  $\mathbf{s}$ . In order to emphasize this, we superscript the key and write  $H^s$  rather than  $H_s$ .

## Formal Definitions

A hash function (with output length  $l$ ) is a pair of probabilistic polynomial-time algorithms  $(\text{Gen}, H)$  satisfying the following:

1. **Gen** is a probabilistic algorithm which takes as input a security parameter  $1^n$  and outputs a key  $\mathbf{s}$ . We assume that  $1^n$  is implicit in  $\mathbf{s}$
2.  $H$  takes as input a key  $\mathbf{s}$  and a string  $x \in \{0, 1\}^n$  and outputs a string  $H^s(x) \in \{0, 1\}^{l(n)}$  (where  $n$  is the value of the security parameter implicit in  $\mathbf{s}$ )

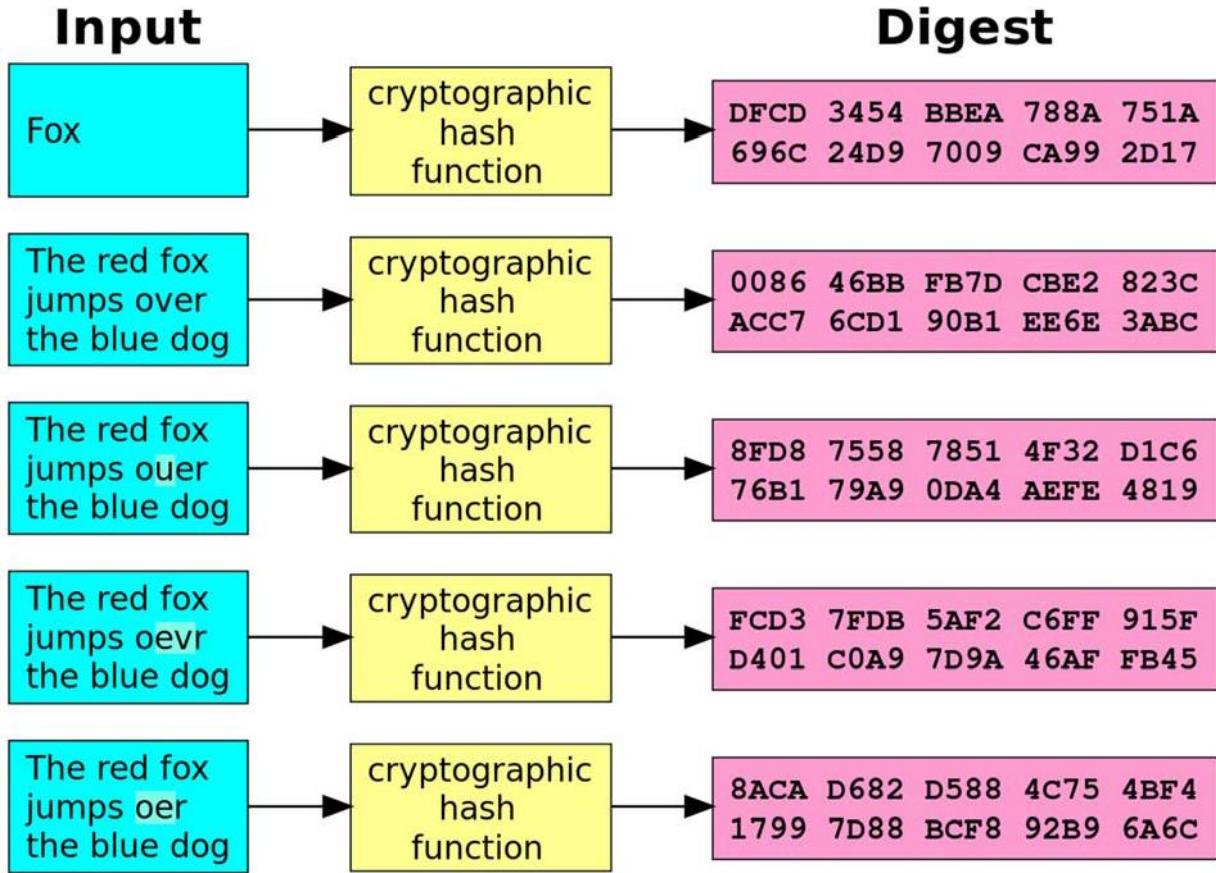


Figure 8 Hash Function (Source Wikipedia)

If  $H^s$  is defined only for inputs  $x \in \{0, 1\}^{l'(n)}$  and  $l'(n) > l(n)$ , then we say that  $(Gen, H)$  is a fixed-length hash function for inputs of length  $l'$ . In this case, we also call  $H$  a compression function. In the fixed-length case we require that  $l'$  be greater than  $l$ . This ensures that the function **compresses** its input. In the general case the function takes as input strings of arbitrary length. Thus, it also compresses (albeit only strings of length greater than  $l(n)$ ). Note that without compression, collision resistance is trivial (since one can just take the identity function  $H^s(x) = x$ ).

We now proceed to define security. As usual, we first define an experiment for a hash function  $\Pi = (Gen, H)$ , an adversary **A**, and a security parameter **n**. The collision-finding experiment  $Hash - coll_{A,\Pi}(n)$ :

1. A key  $s$  is generated by running  $Gen(1^n)$
2. The adversary **A** is given  $s$  and outputs  $\mathbf{x}, \mathbf{x}'$ . (If  $\Pi$  is a fixed-length hash function for inputs of length  $l'(n)$ , then we require  $x, x' \in \{0, 1\}^{l'(n)}$ )

3. The output of the experiment is defined to be **1** if and only if  $x = x'$  and  $H^s(x) = H^s(x')$ . In such a case we say that **A** has found a collision

A hash function  $\mathcal{H} = (\text{Gen}, H)$ , is collision resistant if for all probabilistic polynomial-time adversaries **A** there is a negligible function **negl** such that:

$$\Pr[\text{HashColl}_{A,\mathcal{H}}(n) = 1] : s: \text{negl}(n)$$

**Preimage resistance**: for essentially all pre-specified outputs, it is computationally infeasible to find any input which hashes to that output, i.e., to find any preimage  $x'$  such that  $h(x') = y$  when given any  $y$  for which a corresponding input is not known. (one-way)

**2nd-preimage resistance**: it is computationally infeasible to find any second input which has the same output as any specified input, i.e., given  $x$ , to find a 2nd-preimage  $x' \neq x$  such that  $h(x) = h(x')$ .

### Unkeyed hash functions

Cryptographic hash functions used in practice generally have a fixed output length (just as block ciphers have a fixed key length) and are usually unkeyed, meaning that the hash function is just a fixed function  $H: \{0, 1\}^{\mathbb{D}} \rightarrow \{0, 1\}^{\mathbb{I}}$ . This is problematic from a theoretical standpoint since for any such function there is always a constant-time algorithm that outputs a collision in **H**: the algorithm simply outputs a colliding pair  $(x, x')$  hardcoded into the algorithm itself. Using keyed hash functions solves this technical issue since it is impossible to hardcode a colliding pair for every possible key using a reasonable amount of space (and in an asymptotic setting, it would be impossible to hardcode a colliding pair for every value of the security parameter).

Notwithstanding the above, the (unkeyed) cryptographic hash functions used in the real world are collision resistant for all practical purposes since colliding pairs are unknown (and computationally difficult to find) even though they must exist. Proofs of security for some construction based on collision resistance of a hash function are meaningful even when an unkeyed hash function **H** is used, as long as the proof shows that any efficient adversary “breaking” the primitive can be used to efficiently find a collision in **H**. (All the proofs in this book satisfy this condition.) In this case, the interpretation of the proof of security is that if an adversary can break the scheme in practice, then it can be used to find a collision in practice, something that we believe is hard to do.

### Weaker Notions of Security

In some applications it suffices to rely on security requirements weaker than collision resistance. These include:

Second-preimage or target-collision resistance: Informally, a hash function is second preimage resistant if given  $s$  and a uniform  $x$  it is infeasible for a **PPT** adversary to find  $x' \neq x$  such that  $H^s(x') = H^s(x)$ .

Preimage resistance: Informally, a hash function is preimage resistant if given  $s$  and a uniform  $y$  it is infeasible for a **PPT** adversary to find a value  $x$  such that  $H^s(x) = y$ . (This essentially means that  $H^s$  is one-way.)

Any hash function that is collision resistant is also second preimage resistant. This holds since if, given a uniform  $x$ , an adversary can find  $x' \neq x$  for which  $H^s(x') = H^s(x)$ , then it can clearly find a colliding pair  $x$  and  $x'$ . Likewise, any hash function that is second preimage resistant is also preimage resistant. This is due to the fact that if it were possible, given  $y$ , to find an  $x$  such that  $H^s(x) = y$ , then one could also take a given input  $x'$ , compute  $y \in H^s(x')$ , and then obtain an  $x$  with  $H^s(x) = y$ . With high probability  $x' \neq x$  (relying on the fact that **H** compresses, and so multiple inputs map to the same output), in which case a second preimage has been found.

The objective of an adversary who wishes to “attack” an MDC is as follows:

1. to attack a OWHF: given a hash-value  $y$ , find a preimage  $x$  such that  $y = h(x)$ ; or given one such pair  $(x, h(x))$ , find a second preimage  $x'$  such that  $h(x') = h(x)$
2. to attack a CRHF: find any two inputs  $x, x'$  such that  $h(x') = h(x)$

The objective of an adversary who wishes to “attack” a MAC is as follows:

to attack a MAC: without prior knowledge of a key  $k$ , compute a new text-MAC pair  $(x, h_k(x))$  for some text  $x \neq x_i$ , given one or more pairs  $(x_i, h_k(x_i))$

## Aim/Objectives

The purpose of the 8<sup>th</sup> Week is introduce the concept of hash functions. We explain the basics of hash functions and how they work as well as some of their features such as collision-resistance, preimage-resistance as well as keyed and unkeyed hash functions. In addition we discuss modification detection codes as well as one-way hash functions and collision resistant hash functions

## Learning Outcomes

After the successful completion of the 8<sup>th</sup> Week, students should be able to:

- Evaluate the use of hash functions
- Explain keyed and unkeyed hash functions
- Evaluate Modification Detection Codes (MDCs) and explain One-Way hash functions and Collision-Resistant hash functions
- Explain collision-resistance, preimage-resistance and 2<sup>nd</sup> preimage-resistance

## Key Words

Digest	Compression	Unkeyed
Modification Detection	Collision Resistance	Preimage Resistance
OWHF	CRHF	Keyed

## Annotated Bibliography

### Basic

- C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2010, Chapter 11 “Hash Functions”

The eleventh Chapter of this book introduces Hash functions and explains why they play an important role in modern cryptography. In addition, it explains why they are required in digital signature schemes. It shows the most important properties of hash functions and performs a security analysis on them.

### Suggestions for further reading

- Hashing Algorithms and Security – Computerphile, [Youtube Video], Available at: <https://www.youtube.com/watch?v=b4b8ktEV4Bg>
- Coron JS., Dodis Y., Malinaud C., Puniya P. (2005) Merkle-Damgård Revisited: How to Construct a Hash Function. In: Shoup V. (eds) Advances in Cryptology – CRYPTO 2005. CRYPTO 2005. Lecture Notes in Computer Science, vol 3621. Springer, Berlin, Heidelberg

## **Self-Assessment Exercises**

### **Exercise 8.1**

Briefly explain what a hash function is

### **Exercise 8.2**

Give the two hash function classes

### **Exercise 8.3**

Give the categories in which hash functions are used

### **Exercise 8.4**

Explain what are collision-resistance, preimage resistance and 2nd-preimage resistance

## **Individual Assignment (20 points)**

The individual assignment includes solving questions related to the syllabus covered in this course. The questions can vary from practical ones, to essay style questions asking to use your current skills in order to describe existing cryptography protocols.

In addition, there will be one exercise asking to implement using any programming language, one of the protocols already taught in the course.

This assignment counts 20% of the final course mark.

You will need approximately 20 hours to solve this Individual Assignment.

## **Recommended time for the student to work**

35 hours

## Summary

In this week we are going to study the fundamental principles behind Public-Key Cryptography. We will discuss the number theory and the building blocks that are used in public key cryptography. In addition, we will see how public key cryptography was first proposed.

## Introductory Remarks

### Greatest Common Divisor

The **greatest common divisor** of two integers  $a, b$  written as  $\gcd(a, b)$ , is the largest integer  $c$  such that  $c/a$  and  $c/b$ . (Note:  $\gcd(a, b) = \gcd(|a|, |b|)$  and  $\gcd(b, 0) = \gcd(0, b) = b$ )

If  $p$  is prime, then  $\gcd(a, p)$  is either equal to 1 or  $p$ . If  $\gcd(a, b) = 1$  then  $a$  and  $b$  are **relatively prime**.

Formally, let  $a, b$  be positive integers. Then there exists integers  $X, Y$  such that  $Xa + Yb = \gcd(a, b)$ . Furthermore,  $\gcd(a, b)$  is the smallest positive integer that can be expressed in this way.

If  $c|ab$  and  $\gcd(a, c) = 1$  then  $c|b$ . Thus, if  $p$  is prime and  $p|ab$  then either  $p|a$  or  $p|b$ .

If  $a|N$ ,  $b|N$  and  $\gcd(a, b) = 1$  then  $ab|N$ .

### Modular Arithmetic

Let  $a, b, N \in \mathbb{Z}$  with  $N > 1$ . We use the notion  $a \bmod N$  to denote the remainder of  $a$  upon division by  $N$ . In detail, there exist unique  $q, r$  with  $a = qN + r$  and  $0 \leq r < N$ , and we define  $a \bmod N$  to be equal to this  $r$ . We say that  $a$  and  $b$  are **congruent modulo  $N$** , written  $a \equiv b \pmod{N}$ , if  $a \bmod N = b \bmod N$ . (i.e. the remainder when  $a$  is divided by  $N$  is the same as the remainder when  $b$  is divided by  $N$ )

Congruence modulo  $N$  is an equivalent relation. i.e. it is reflexive ( $a \equiv a \pmod{N}$  for all  $a$ ), symmetric ( $a \equiv b \pmod{N}$  implies  $b \equiv a \pmod{N}$ ) and transitive (if  $a \equiv b \pmod{N}$  and  $b \equiv c \pmod{N}$ , then  $a \equiv c \pmod{N}$ )

Congruence modulo  $N$  obeys the standard rules of arithmetic with respect to addition, subtraction and multiplication, for example if  $a = a^r \text{ mod } N$  and  $b = b^r \text{ mod } N$  then  $(a + b) = (a^r + b^r) \text{ mod } N$  and  $ab = a^r b^r \text{ mod } N$

Congruence modulo  $N$  does not (in general) respect division. That is, if  $a = a^r \text{ mod } N$  and  $b = b^r \text{ mod } N$  then it is not necessarily true that  $\frac{a}{b} = \frac{a^r}{b^r} \text{ mod } N$ .

In fact, the expression  $\frac{a}{b} \text{ mod } N$  is not always well-defined. As a specific example that often causes confusion,  $ab = cb \text{ mod } N$  does not necessarily imply that  $a = c \text{ mod } N$ .

In certain cases, however, we can define a meaningful notion of division. If for a given integer  $b$  there exists an integer  $c$  such that  $bc = 1 \text{ mod } N$ , we say that  $b$  is **invertible modulo  $N$**  and call  $c$  a (multiplicative) inverse of  $b$  **modulo  $N$** . Clearly, 0 is never invertible.

It is also not difficult to show that if  $c$  is a multiplicative inverse of  $b$  **modulo  $N$**  then so is  $c \text{ mod } N$ . Furthermore, if  $c'$  is another multiplicative inverse of  $b$  then  $c \text{ mod } N = c'^r \text{ mod } N$ . When  $b$  is invertible we can therefore simply let  $b^{-1}$  denote the unique multiplicative inverse of  $b$  that lies in the range  $\{1, \dots, N - 1\}$ .

When  $b$  is invertible modulo  $N$ , we define division by  $b$  **modulo  $N$**  as multiplication by  $b^{-1}$  (i.e., we define  $\frac{a}{b} \text{ mod } N \triangleq ab^{-1} \text{ mod } N$ ). We stress that division by  $b$  is only defined when  $b$  is invertible. If  $ab = cb \text{ mod } N$  and  $b$  is invertible, then we may divide each side of the equation by  $b$  (or multiply each side by  $b^{-1}$ ) to obtain

$$(ab) \cdot b^{-1} = (cb) \cdot b^{-1} \text{ mod } N \triangleq a = c \text{ mod } N$$

Formally, let  $b, N$  be integers, with  $b \geq 1$  and  $N > 1$ . Then  $b$  is invertible modulo  $N$  if and only if  $\gcd(b, N) = 1$

## Groups

Let  $C$  be a set. A binary operation  $\circ$  on  $C$  is simply a function  $\circ(\cdot, \cdot)$  that takes as input two elements of  $C$ . If  $g, h \in C$  then instead of using the difficult notation  $\circ(g, h)$  we write  $g \circ h$ .  
Definition: A group is a set  $C$  along with a binary operation  $\circ$  for which the following conditions hold:

- **Closure:** For all  $g, h \in C$ ,  $g \circ h \in C$
- **Existence of an identity:** There exists an identity  $e \in C$  such that for all  $g \in C$ ,  $g \circ e = g$  and  $e \circ g = g$ .
- **Existence of inverses:** For all  $g \in C$  there exists an element  $h \in C$  such that  $g \circ h = e$  and  $h \circ g = e$ . Such an  $h$  is called an inverse of  $g$ .
- **Associativity:** For all  $g_1, g_2, g_3 \in C$ ,  $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$

When  $C$  has a finite number of elements, we say  $C$  is finite and let  $|C|$  denote the order of the group (that is, the number of elements in  $C$ ). A group  $C$  with operation  $\circ$  is **abelian** if the following holds:

- **Commutativity:** For all  $g, h \in C$ ,  $g \circ h = h \circ g$

Associativity implies that we do not need to include parentheses when writing long expressions; that is, the notation  $g_1 \circ g_2 \dots g_n$  is unambiguous since it does not matter in what order we evaluate the operation  $\circ$ .

In general, we will not use the notation  $\circ$  to denote the group operation. Instead, we will use either **additive** notation or **multiplicative** notation depending on the group under discussion. This does not imply that the group operation corresponds to integer addition or multiplication; it is merely useful notation. When using additive notation, the group operation applied to two elements  $g, h$  is denoted  $g + h$ ; the identity is denoted by  $0$ ; the inverse of an element  $g$  is denoted by  $-g$ ; and we write  $h - g$  in place of  $h + (-g)$ . When using multiplicative notation, the group operation applied to  $g, h$  is denoted by  $g \cdot h$  or simply  $gh$ ; the identity is denoted by  $1$ ; the inverse of an element  $g$  is denoted by  $g^{-1}$ ; and we sometimes write  $\underset{g}{\overset{h}{\cdot}}$  in place of  $hg^{-1}$ .

Finally, we formalise something called “**cancellation law**” for groups. Let  $C$  be a group and  $a, b, c \in C$ . If  $ac = bc$ , then  $a = b$ . In particular, if  $ac = c$  then  $a$  is the identity in  $C$ . It is often useful to be able to describe the group operation applied  $m$  times to a fixed element  $g$ , where  $m$  is a positive integer. When using additive notation, we express this as  $m \circ g$  or  $mg$ ; that is

$$mg = m \circ g \underset{m \text{ times}}{\circ} g \underset{m \text{ times}}{\circ} g$$

When using multiplicative notation, we express application of the group operation  $m$  times to an element  $g$  by  $g^m$ . That is,

$$g^m \underset{m \text{ times}}{\circ} g \underset{m \text{ times}}{\circ} g$$

Observe that  $-g$  is the inverse of  $g$  and, as one would expect,  $(-m) \cdot g = -(mg)$ . When using multiplicative notation,  $g^0 = 1$  and  $g^{-m} = (g^{-1})^m$ . Again,  $g^{-1}$  is the inverse of  $g$ , and we have  $g^{-m} = (g^m)^{-1}$ . Let  $g \in C$  and  $b \geq 0$  be an integer. Then the exponentiation  $g^b$  can be computed using a polynomial number of underlying group operations in  $C$ . Thus, if the group operation can be computed in polynomial time then so can exponentiation.

We now know enough to prove the following remarkable result. Let  $C$  be a finite group with  $m = |C|$ , the order of the group. Then for any element  $g \in C$ ,  $g^m = 1$ . Using this we can actually work modulo the group order in the exponent. Let  $C$  be a finite group with  $m = |G| > 1$ . Then for any  $g \in C$  and any integer  $x$ , we have  $g^x = g^{[x \text{ mod } m]}$ .

Let  $C$  be a finite group with  $m = |C| > 1$ . Let  $e > 0$  be an integer, and define the function  $f_e: G \rightarrow G$  by  $f_e(g) = g^e$ . If  $\gcd(e, m) = 1$ , then  $f_e$  is a permutation. Moreover, if  $d = e^{-1} \bmod m$  then  $f_d$  is the inverse of  $f_e$ .

### Group $'1_N^{\mathbb{Z}}$

As discussed, the set  $Z_N = \{0, \dots, N - 1\}$  is a group under addition modulo  $N$ . Can we define a group with respect to multiplication modulo  $N$ ?

In doing so, we will have to eliminate those elements in  $Z_N$  that are not invertible; e.g., we will have to eliminate  $0$  since it has no multiplicative inverse. Nonzero elements may also fail to be invertible. Which elements  $b \in \{1, \dots, N - 1\}$  are invertible modulo  $N$ ?

We already know that these are exactly those elements  $b$  for which  $\gcd(b, N) = 1$ .

We have also seen that whenever  $b$  is invertible, it has an inverse lying in the range  $\{1, \dots, N - 1\}$ .

This leads us to define, for any  $N > 1$ , the set

$$'1_N^{\mathbb{Z}} = \{b \in \{1, \dots, N - 1\} / \gcd(b, N) = 1\}$$

i.e.  $'1_N^{\mathbb{Z}}$  consists of integers in the set  $\{1, \dots, N - 1\}$  that are relatively prime to  $N$ . The group operation is multiplication modulo  $N$ , i.e.  $ab \in [ab \bmod N]$ .

We claim that  $'1_N^{\mathbb{Z}}$  is an abelian group with respect to this operation. Since  $1$  is always in  $'1_N^{\mathbb{Z}}$ , the

set clearly contains an identity element. The discussion above shows that each element in  $'1_N^{\mathbb{Z}}$  has a multiplicative inverse in the same set. Commutativity and associativity follow from the fact that these properties hold over the integers. To show that closure holds, let  $a, b \in '1_N^{\mathbb{Z}}$ . Then  $[ab \bmod N]$  has inverse  $[b^{-1}a^{-1} \bmod N]$ , which means that  $\gcd([ab \bmod N], N) = 1$  and so  $ab \in '1_N^{\mathbb{Z}}$ .

Summary:

Let  $N > 1$  be an integer. Then  $'1_N^{\mathbb{Z}}$  is an abelian group under multiplication modulo  $N$ . Define  $\phi(N) = |'1_N^{\mathbb{Z}}|$ , the order of the group  $'1_N^{\mathbb{Z}}$ . ( $\phi$  is called the Euler phi function.) What is the value of  $\phi(N)$ ?

First consider the case when  $N = p$  is prime. Then all elements in  $\{1, \dots, p - 1\}$  are relatively prime to  $p$ , and so  $\phi(p) = |'1_p^{\mathbb{Z}}| = p - 1$ . Next consider the case that  $N = pq$ , where  $p, q$  are distinct primes. If an integer  $a \in \{1, \dots, N - 1\}$  is not relatively prime to  $N$ , then either  $p/a$  or  $q/a$  ( $a$  cannot be divisible by both  $p$  and  $q$  since this would imply  $pq/a$  but  $a < N = pq$ ). The elements in  $\{1, \dots, N - 1\}$  divisible by  $p$  are exactly the  $(q - 1)$  elements  $p, 2p, 3p, \dots, (q - 1)p$ , and the elements divisible by  $q$  are exactly the  $(p - 1)$  elements

$q, 2q, \dots, (p - 1)q$ . The number of elements remaining (i.e., those that are neither divisible by  $p$  nor  $q$ ) is therefore given by

$$(N - 1) - (q - 1) - (p - 1) = pq - p - q + 1 = (p - 1)(q - 1)$$

We have thus proved that  $\phi(N) = (p - 1)(q - 1)$  when  $N$  is the product of two distinct primes  $p$  and  $q$ . Let  $N = \prod_i p_i^{e_i}$ , where the  $\{p_i\}$  are distinct primes and  $e_i \geq 1$ . Then  $\phi(N) = \prod_i p_i^{e_i-1} (p_i - 1)$

## Isomorphisms

Two groups are isomorphic if they have the same underlying structure. From a mathematical point of view, an isomorphism of a group  $C$  provides an alternate, but equivalent, way of thinking about  $C$ . From a computational perspective, an isomorphism provides a different way to represent elements in  $C$ , which can often have a significant impact on algorithmic efficiency.

Let  $C, IH$  be groups with respect to the operations  $\circ_C, \circ_{IH}$  respectively. A function  $f: C \rightarrow IH$  is an isomorphism from  $C$  to  $IH$  if:

1.  $f$  is a bijection
2. For all  $g_1, g_2 \in C$  we have  $f(g_1 \circ_C g_2) = f(g_1) \circ_{IH} f(g_2)$

If there exists an isomorphism from  $C$  to  $IH$  then we say that these groups are isomorphic and we write  $C \cong IH$ .

In essence, an isomorphism from  $C$  to  $IH$  is just a renaming of elements of  $C$  as elements of  $IH$ . (Note that if  $C$  is finite and  $C \cong IH$ , then  $IH$  must be finite and of the same size as  $C$ ) Also, if there exists an isomorphism  $f$  from  $C$  to  $IH$  then  $f^{-1}$  is an isomorphism from  $IH$  to  $C$ . It is possible, however, that  $f$  is efficiently computable while  $f^{-1}$  is not (or vice versa). The aim of this section is to use the language of isomorphisms to better understand the group structure of  $\mathbb{Z}_N^*$  and  $\mathbb{Z}_N^\times$  when  $N = pq$  is a product of two distinct primes. We first need to introduce the notion of a direct product of groups. Given groups  $C, IH$  with group operations  $\circ_C, \circ_{IH}$ , respectively, we define a new group  $C \times IH$  (the direct product of  $C$  and  $IH$ ) as follows:

The elements of  $C \times IH$  are ordered pairs  $(g, h)$  with  $g \in C$  and  $h \in IH$ , thus, if  $C$  has  $n$  elements and  $IH$  has  $n'$  elements,  $C \times IH$  has  $n \cdot n'$  elements. The group operation  $\circ$  on  $C \times IH$  is applied component-wise; that is:

$$(g, h) \circ (g', h') = (g \circ_C g', h \circ_{IH} h')$$

## Chinese Remainder Theorem

Let  $N = pq$  where  $p, q > 1$  are relatively prime. Then

$$\cdot 1_N \otimes \cdot 1_p x \cdot 1_q \textbf{and} \frac{\cdot 1_N^T \otimes \cdot 1_q^T x \cdot 1_p^T}{p-q}$$

Moreover, let  $f$  be the function mapping elements  $x \in \{0, \dots, N-1\}$  to pairs  $(x_p, x_q)$  with  $x_p \in \{0, \dots, p-1\}$  and  $x_q \in \{0, \dots, q-1\}$  defined by

$$f(x) = ([x \bmod p], [x \bmod q])$$

Then  $f$  is an isomorphism from  $\mathbb{Z}_N$  to  $\mathbb{Z}_p \times \mathbb{Z}_q$ , and the restriction of  $f$  to  $\mathbb{Z}_N^{\times}$  is an isomorphism from  $\mathbb{Z}_N^{\times}$  to  $\mathbb{Z}_p^{\times} \times \mathbb{Z}_q^{\times}$ .

If two groups are isomorphic, then they both serve as representations of the same underlying “algebraic structure.” Nevertheless, the choice of which representation to use can affect the **computational efficiency** of group operations. We discuss this abstractly, and then in the specific context of  $\mathbb{Z}_N$  and  $\mathbb{Z}_N^{\times}$ .

## Proof of Chinese Remainder Theorem

$$\text{Let } \mathbf{N}_1 = n_2 n_3 \quad \mathbf{N}_2 = n_1 n_3 \quad \mathbf{N}_3 = n_1 n_2$$

Since  $\mathbf{N}_i$  and  $n_i$  are relatively prime, this implies that there exist  $x_1, x_2, x_3$

$$\mathbf{N}_1 x_1 \equiv 1 \pmod{n_1} \quad \mathbf{N}_2 x_2 \equiv 1 \pmod{n_2} \quad \mathbf{N}_3 x_3 \equiv 1 \pmod{n_3}$$

$$\text{So, } a_1 \mathbf{N}_1 x_1 \equiv a_1 \pmod{n_1}, a_2 \mathbf{N}_2 x_2 \equiv a_2 \pmod{n_2}, a_3 \mathbf{N}_3 x_3 \equiv a_3 \pmod{n_3}$$

$$\boxed{\text{Let } x = a_1 \mathbf{N}_1 x_1 + a_2 \mathbf{N}_2 x_2 + a_3 \mathbf{N}_3 x_3}$$

$$\text{Since } n_1 | \mathbf{N}_2 \text{ and } n_1 | \mathbf{N}_3, \quad x \equiv a_1 \mathbf{N}_1 x_1 \pmod{n_1}$$

$$\text{Since } \mathbf{N}_1 x_1 \equiv 1 \pmod{n_1}, \quad \boxed{x \equiv a_1 \pmod{n_1}}$$

Similarly,

$$\boxed{x \equiv a_2 \pmod{n_2}}$$

$$\boxed{x \equiv a_3 \pmod{n_3}}$$

Figure 9 Chinese Remainder Theorem Proof

Let  $C, IH$  be groups with operations  $\cdot_C, \cdot_{IH}$  respectively, and say  $f$  is an isomorphism from  $C$  to  $IH$  where both  $f$  and  $f^{-1}$  can be computed efficiently.

Then for  $g_1, g_2 \in C$  we can compute  $g = g_1 \cdot_C g_2$  in two ways: either by directly computing the group operation in  $C$ , or via the following steps:

1. Compute  $h_1 = f(g_1)$  and  $h_2 = f(g_2)$
2. Compute  $h = h_1 \oplus_{IH} h_2$  using the group operation in  $IH$
3. Compute  $g = f^{-1}(h)$

This extends in the natural way when we want to compute multiple group operations in  $C$  (e.g., to compute  $g^x$  for some integer  $x$ ). Which method is better depends on the relative efficiency of computing the group operation in each group, as well as the efficiency of computing  $f$  and  $f^{-1}$ . We now turn to the specific case of computations modulo  $N$ , when  $N = pq$  is a product of distinct primes. The Chinese remainder theorem shows that addition, multiplication, or exponentiation (which is just repeated multiplication) modulo  $N$  can be “transformed” to analogous operations modulo  $p$  and  $q$ .

One thing we have not yet discussed is how to convert back and forth between the representation of an element modulo  $N$  and its representation modulo  $p$  and  $q$ . The conversion can be carried out efficiently provided the factorization of  $N$  is known. Assuming  $p$  and  $q$  are known, it is easy to map an element  $x$  modulo  $N$  to its corresponding representation modulo  $p$  and  $q$ :

the element  $x$  corresponds to  $([x \bmod p], [x \bmod q])$ , and both the modular reductions can be carried out efficiently. For the other direction, we make use of the following observation:

an element with representation  $(x_p, x_q)$  can be written as

$$(x_p, x_q) = x_p \cdot (1, 0) + x_q \cdot (0, 1)$$

So, if we can find elements  $1_p, 1_q \in \{0, \dots, N - 1\}$  such that  $1_p \leftrightarrow (1, 0)$  and  $1_q \leftrightarrow (0, 1)$ , then (appealing to the Chinese remainder theorem) we know that

$$(x_p, x_q) \leftrightarrow [(x_p \cdot 1_p + x_q \cdot 1_q) \bmod N]$$

Since  $p, q$  are distinct primes,  $\gcd(p, q) = 1$ . We can use the extended Euclidean algorithm to find integers  $X, Y$  such that

$$X_p + Y_q = 1$$

(Note that  $Y_q = 0 \text{ mod } q$  and  $Y_q = 1 - X_p = 1 \text{ mod } p$ . This means that  $[Y_q \text{ mod } N] \leftrightarrow (1, 0)$ ; i.e.,  $[Y_q \text{ mod } N] = 1_p$ . Similarly,  $[X_p \text{ mod } N] = 1_q$ )

**Input:** Integers  $a, b$  with  $a \geq b > 0$

**Output:**  $(d, X, Y)$  with  $d = \gcd(a, b)$  and  $Xa + Yb = d$

```

if  $b$  divides  $a$ 
    return  $(b, 0, 1)$ 
else
    Compute integers  $g, r$  with  $a = qb + r$  and  $0 < r < b$ 
     $(d, X, Y) \leftarrow eGCD(b, r)$  //note that  $Xb + Yr = d$ 
    return  $(d, Y, X - Yq)$ 
```

In summary, we can convert an element represented as  $(x_p, x_q)$  to its representation modulo  $N$  in the following way (assuming  $p$  and  $q$  are known):

1. Compute  $X, Y$  such that  $X_p + Y_q = 1$
2. Set  $1_p := [Y_q \text{ mod } N]$  and  $1_q := [X_p \text{ mod } N]$
3. Compute  $x := [(x_p \cdot 1_p + x_q \cdot 1_q) \text{ mod } N]$

If many such conversions will be performed, then  $1_p, 1_q$  can be computed once-and-for-all in a pre-processing phase.

## Factoring

We will start discussing about number-theoretic problems that are conjectured to be “hard.” We begin with a discussion of one of the oldest problems: **integer factorization** or just **factoring**.

Given a composite integer  $N$ , the factoring problem is to find integers  $p, q > 1$  such that  $pq = N$ . Factoring is a classic example of a hard problem, both because it is so simple to describe and since it has been recognized as a hard computational problem for a long time (even before its use in cryptography).

The problem can be solved in exponential time  $O(\sqrt{N} \cdot \text{polylog}(N))$  using **trial division**: that is, by exhaustively checking whether  $p$  divides  $N$  for  $p = 2, \dots, \lfloor \sqrt{N} \rfloor$ .

This method requires  $\sqrt{N}$  divisions, each one taking  $\text{polylog}(N) = \lceil N \rceil^c$  time for some constant  $c$ .

This always succeeds because although the **largest** prime factor of  $N$  may be as large as  $\frac{N}{2}$ , the **smallest** prime factor of  $N$  can be at most  $\sqrt{N}$ .

Although algorithms with better running time are known, no polynomial-time algorithm for factoring has been demonstrated despite many years of effort.

Consider the following experiment for a given algorithm  $A$  and parameter  $n$ :

The weak factoring experiment  $w - \text{Factor}_A(n)$ :

1. Choose two uniform  $n$ -bit integers  $x_1, x_2$
2. Compute  $N := x_1 \bullet x_2$
3.  $A$  is given  $N$ , and outputs  $x_1^r, x_2^r > 1$
4. The output of the experiment is defined to be 1 if  $x_1^r \bullet x_2^r = N$ , and 0 otherwise.

We have just said that the factoring problem is believed to be hard. Does this mean that

$$\Pr[w - \text{Factor}_A(n) = 1] : s: \text{negl}(n)$$

is negligible for every PPT algorithm  $A$ ?

Not at all. For starters, the number  $N$  in the above experiment is even with probability  $\frac{3}{4}$  (this occurs when either  $x_1$  or  $x_2$  is even); it is, of course, easy for  $A$  to factor  $N$  in this case. While we can make  $A$ 's job more difficult by requiring  $A$  to output integers  $x_1^r, x_2^r$  of length  $n$ , it

remains the case that  $x_1$  or  $x_2$  (and hence  $N$ ) might have small prime factors that can still be easily found.

For cryptographic applications, we will need to prevent this.

As this discussion indicates, the “hardest” numbers to factor are those having only large prime factors. This suggests redefining the above experiment so that  $x_1, x_2$  are random  $n$ -bit primes rather than random  $n$ -bit integers, and in fact such an experiment will be used when we formally define the factoring assumption.

For this experiment to be useful in a cryptographic setting, however, it is necessary to be able to generate random  $n$ -bit primes efficiently.

### Generating Random Primes

A natural approach to generating a random  $n$ -bit prime is to repeatedly choose random  $n$ -bit integers until we find one that is prime; we repeat this at most  $t$  times or until we are successful. Note that the algorithm forces the output to be an integer of length exactly  $n$  (rather than length at most  $n$ ) by fixing the high-order bit of  $p$  to “1.” Our convention throughout this course is that

an “integer of length  $n$ ” means an integer whose binary representation with most significant bit equal to 1 is exactly  $n$  bits long.

Given a way to determine whether or not a given integer  $p$  is prime, the above algorithm outputs a uniform  $n$ -bit prime conditioned on the event that it does not output fail.

The probability that the algorithm outputs fail depends on  $t$ , and for our purposes we will want to set  $t$  so as to obtain a failure probability that is negligible in  $n$ . To show that the algorithm leads to an efficient (i.e., polynomial-time in  $n$ ) algorithm for generating primes, we need a better understanding of two issues:

1. the probability that a uniform  $n$ -bit integer is prime
2. how to efficiently test whether a given integer  $p$  is prime.

### **The distribution of primes**

The prime number theorem, an important result in mathematics, gives fairly precise bounds on the fraction of integers of a given length that are prime. For our purposes, we need only a weak, one-sided version of that result that we do not prove here:

For any  $n > 1$ , the fraction of  $n$ -bit integers that are prime is at least  $\frac{1}{3}n$

Returning to the approach for generating primes described above, this implies that if we set  $t = 3n^2$  then the probability that a prime is not chosen in all  $t$  iterations of the algorithm is at most

$$(1 - \frac{1}{3n})^t = ((1 - \frac{1}{3n})^{3n})^n : s: (e^{-1})^n = e^{-n}$$

which is negligible in  $n$ . Thus, using  $\text{poly}(n)$  iterations we obtain an algorithm for which the probability of outputting fail is negligible in  $n$ .

### **Testing primality**

The problem of efficiently determining whether a given number is prime has a long history. In the 1970s the first efficient algorithms for testing primality were developed.

These algorithms were probabilistic and had the following guarantee: if the input  $p$  were a prime number, the algorithm would always output “prime.” On the other hand, if  $p$  were composite, then the algorithm would almost always output “composite,” but might output the wrong answer (“prime”) with probability negligible in the length of  $p$ .

Put differently, if the algorithm outputs “composite” then  $p$  is definitely composite, but if the output is “prime” then it is very likely that  $p$  is prime but it is also possible that a mistake has occurred (and  $p$  is really composite).

When using a randomized primality test of this sort in the algorithm, the output of the algorithm is a uniform prime of the desired length so long as the algorithm does not output fail and the randomized primality test did not err during the execution of the algorithm.

This means that an additional source of error (besides the possibility of outputting fail) is introduced, and the algorithm may now output a composite number by mistake.

Since we can ensure that this happens with only negligible probability, this remote possibility is of no practical concern and we can safely ignore it.

A deterministic polynomial-time algorithm for testing primality was demonstrated in a breakthrough result in 2002. That algorithm, although running in polynomial time, is slower than the probabilistic tests mentioned above. For this reason, probabilistic primality tests are still used exclusively in practice for generating large prime numbers.

### Miller-Rabin Test

If  $p$  is prime, then the Miller–Rabin test always outputs “prime.” If  $p$  is composite, the algorithm outputs “composite” except with probability at most  $2^{-t}$ .

Given the preceding discussion, we can now describe a polynomial-time prime-generation algorithm that, on input  $n$ , outputs an  $n$ -bit prime except with probability negligible in  $n$ ; moreover, conditioned on the output  $p$  being prime,  $p$  is a uniformly distributed  $n$ -bit prime.

### Generating Primes of a Particular Form

It is sometimes desirable to generate a random  $n$ -bit prime  $p$  of a particular form, for example, satisfying  $p = 3 \bmod 4$  or such that  $p = 2q + 1$  where  $q$  is also prime ( $p$  of the latter type are called **strong primes**).

In this case, appropriate modifications of the prime-generation algorithm can be used.

For example, in order to obtain a prime of the form  $p = 2q + 1$ , modify the algorithm to generate a random prime  $q$ , compute  $p := 2q + 1$ , and then output  $p$  if it too is prime.

While these modified algorithms work well in practice, rigorous proofs that they run in polynomial time and fail with only negligible probability are more complex (and, in some cases, rely on unproven number-theoretic conjectures regarding the density of primes of a particular form)

### The Factoring Assumption

Let  $\text{GenModulus}$  be a polynomial-time algorithm that, on input  $1^n$ , outputs  $(N, p, q)$  where  $N = pq$ , and  $p$  and  $q$  are  $n$ -bit primes except with probability negligible in  $n$ .

Note: The natural way to do this is to generate two uniform  $n$ -bit primes, and then multiply them to obtain  $N$ .

Then consider the following experiment for a given algorithm  $A$  and parameter  $n$ :

The factoring experiment  $\text{Factor}_{A,\text{GenModulus}}(n)$ :

1. Run  $\text{GenModulus}(1^n)$  to obtain  $(N, p, q)$
2.  $A$  is given  $N$ , and outputs  $p'q' > 1$
3. The output of the experiment is defined to be 1 if  $p' \cdot q' = N$ , and 0 otherwise.

Note that if the output of the experiment is 1 then  $\{p', q'\} = \{p, q\}$ , unless  $p$  or  $q$  are composite (which happens with only negligible probability).

We now formally define the factoring assumption:

Factoring is hard relative to  $\text{GenModulus}$  if for all probabilistic polynomial-time algorithms  $A$  there exists a negligible function  $\text{negl}$  such that

$$\Pr[\text{Factor}_{A,\text{GenModulus}}(n) = 1] : s: \text{negl}(n)$$

The factoring assumption is the assumption that there exists a  $\text{GenModulus}$  relative to which factoring is hard.

### The RSA Assumption

The factoring problem has been studied for hundreds of years without an efficient algorithm being found. Although the factoring assumption does give a one-way function, it unfortunately does not directly yield practical cryptosystems.

This has motivated a search for other problems whose difficulty is related to the hardness of factoring. The best known of these is a problem introduced in 1978 by Rivest, Shamir, and Adleman and now called the RSA problem in their honour.

Given a modulus  $N$  and an integer  $e > 2$  relatively prime to  $\phi(N)$ , the exponentiation to the  $e^{\text{th}}$  power modulo  $N$  is a permutation.

We can therefore define  $[y^e \bmod N]$  (for any  $y \in \mathbb{Z}_N^\times$ ) as the unique element of  $\mathbb{Z}_N^\times$  which yields  $y$  when raised to the  $e^{\text{th}}$  power modulo  $N$ ;

That is,  $x = y^e \bmod N$  if and only if  $x^e = y \bmod N$ . The RSA problem, informally, is to compute  $[y^e \bmod N]$  for a modulus  $N$  of unknown factorization.

Formally, let  $\text{GenRSA}$  be a probabilistic polynomial-time algorithm that, on input  $1^n$ , outputs a modulus  $N$  that is the product of two  $n$ -bit primes, as well as integers  $e, d > 0$  with  $\gcd(e, \phi(N)) = 1$  and  $ed = 1 \bmod \phi(N)$ .

Such a  $d$  exists since  $e$  is invertible modulo  $\phi(N)$ . The algorithm may fail with probability negligible in  $n$ . Consider the following experiment for a given algorithm  $A$  and parameter  $n$ :

The RSA experiment  $\text{RSA} - \text{inv}_{A,\text{GenRSA}}(n)$ :

1. Run  $\text{GenRSA}(1^n)$  to obtain  $(N, e, d)$
2. Choose a uniform  $y \in \mathbb{Z}_N^\times$
3.  $A$  is given  $N, e, y$ , and outputs  $x \in \mathbb{Z}_N^\times$
4. The output of the experiment is defined to be 1 if  $x^e = y \pmod{N}$ , and 0 otherwise.

The RSA problem is hard relative to  $\text{GenRSA}$  if for all probabilistic polynomial-time algorithms  $A$  there exists a negligible function  $\text{negl}$  such that

$$\Pr[\text{RSA} - \text{inv}_{A, \text{GenRSA}}(n) = 1] : s: \text{negl}(n)$$

The RSA assumption is that there exists a  $\text{GenRSA}$  algorithm relative to which the RSA problem is hard. A suitable  $\text{GenRSA}$  algorithm can be constructed from any algorithm  $\text{GenModulus}$  that generates a composite modulus along with its factorization.

## Aim/Objectives

The purpose of the 9<sup>th</sup> Week is to introduce all the mathematical concepts needed in order to be able to understand the concepts used in public-key cryptography. More specifically, the topics covered include greatest common divisor, prime numbers, modulo as well as groups. In addition, isomorphisms is described as well as the Chinese remainder theorem. Finally we conclude with factoring, prime number concepts such as creating, distributing and testing their primality as well as the factoring and RSA assumptions.

## Learning Outcomes

After the successful completion of the 9<sup>th</sup> Week, students should be able to:

- Explain the term Greatest Common Divisor
- Evaluate modular arithmetic by explaining the terms congruent modulo and invertible modulo
- Explain groups, the conditions they follow as well as their importance in cryptography
- Explain the term isomorphism
- Evaluate the Chinese remainder theorem
- Explain factoring and factoring assumptions
- Explain the problems of primes, such as generation, distribution and testing
- Explain the RSA assumption

## Key Words

Greatest Common Divisor	Relative Prime	Congruent Modulo
Invertible Modulo	Groups	Cancellation Law
Isomorphisms	Chinese Remainder Theorem	Factoring
Primes Distribution	Primality	Assumptions

## Annotated Bibliography

### Basic

- C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2010, Chapter 8 “Public-Key Cryptosystems Based on the Discrete Logarithm Problem”

The eighth Chapter of this book introduces the basics of algebra, groups, subgroups and cyclic groups. It shows the discrete logarithm problem in general as well as in the prime fields. It then shows the important role it has in cryptography.

### Suggestions for further reading

- The Chinese Remainder Theorem Made Easy by Randell Heyman [Youtube Video], Available at <https://youtu.be/ru7mWZJIRQg>

This is a perfect example and the easiest practical explanation of the Chinese Remainder Theorem.

## Self-Assessment Exercises

### Exercise 9.1

Describe greatest common divisor

### Exercise 9.2

Explain congruent modulo and invertible modulo

**Exercise 9.3**

Give the conditions that hold when a group is a set  $C$  with binary operation  $\circ$

**Exercise 9.4**

Explain cancellation law

**Exercise 9.5**

Explain isomorphisms

**Exercise 9.6**

Explain Chinese remainder theorem

**Recommended time for the student to work**

15 hours

## Summary

Up to now we have seen several encryption schemes, that all use a private key that has to be shared by both honest parties. In this week we will introduce the notion of public key cryptography, and its advantages compared to private key cryptography.

## Introductory Remarks

The biggest problem for all this schemes is how the honest parties will manage to share the secret private key in the first place.

It is clear that such a key cannot be sent over public communication channels since we use encryption in the first place due to the fact that we do not trust public communication. It will be meaningless to send the key of our encryption through such a communication medium.

The honest parties might have access to a secure channel or they might be co-located for a short period of time at which they exchange keys. Using a secure channel may not be the best solution. Imagine what will happen in a large multinational company. Each pair of remote employees will have to use a secure channel or even visit the other employee in order to exchange keys. A better solution would be to use a trusted courier service as a secure channel.

Assuming these employees, denoted by  $N$ , find a way to share keys with each other. This will form another significant drawback. Each employee will have to manage and store  $N - 1$  secret keys. Not only that, but if it also needs a key for each server, database, etc. then the number of stored keys increases. In addition, all these keys must be stored securely. Imagine what will happen if one of those employee computer is infected by a virus or any other form of malicious software.

Even if we solve the problems mentioned above, we will still face problems with open systems. For example, consider using encryption to send credit-card information to an Internet merchant from whom you have not previously purchased anything. In such case, private-key cryptography alone is not a solution.

To summarize, there are at least three distinct problems related to the use of private-key cryptography.

- a. Key distribution
- b. Storing and managing large numbers of secret keys
- c. Inapplicability to open systems

### **Key-Distribution Centers (KDC)**

To solve some of the problems mentioned above, is to use a key-distribution center (KDC) to establish shared keys. Reconsider the large multinational company example. Each employee may trust one entity that can act as a KDC. The KDC will then help all the employees share pairwise keys. When a new employee joins, the KDC can share a key with that employee (in person, in a secure location) as part of that employee's first day of work.

The KDC will also distribute shared keys between that employee and all existing employees. That is, when the  $i$ th employee joins, the KDC could generate  $i - 1$  keys  $k_1, \dots, k_{i-1}$ , give these keys to the new employee, and then send key  $k_j$  to the  $j$ th existing employee by encrypting it using the key that employee already shares with the KDC.

A much better approach, is to use KDC online to generate keys "on demand" whenever two employees wish to communicate securely. Let's say that KDC generates and shares key  $k_A$  with Alice, and  $k_B$  with Bob. When Alice wants to communicate with Bob, she can send a message to the KDC asking to communicate with Bob. KDC will generate a new random key, the **session key**, and send this key  $k_S$  to Alice encrypted using  $k_A$ , and to Bob encrypted using  $k_B$ . Once they both have the session key, they can use it to communicate and when they finish they just dispose the key.

Advantages of KDC:

- a. Each employee needs to store only one long-term secret key
- b. When an employee joins the organization, all that must be done is to set up a key between this employee and the KDC

Disadvantages of KDC:

- a. A successful attack on the KDC will result in a complete break of the system:

The KDC is a single point of failure (can be solved with distribution or backup KDCs but also increases the points of attack)

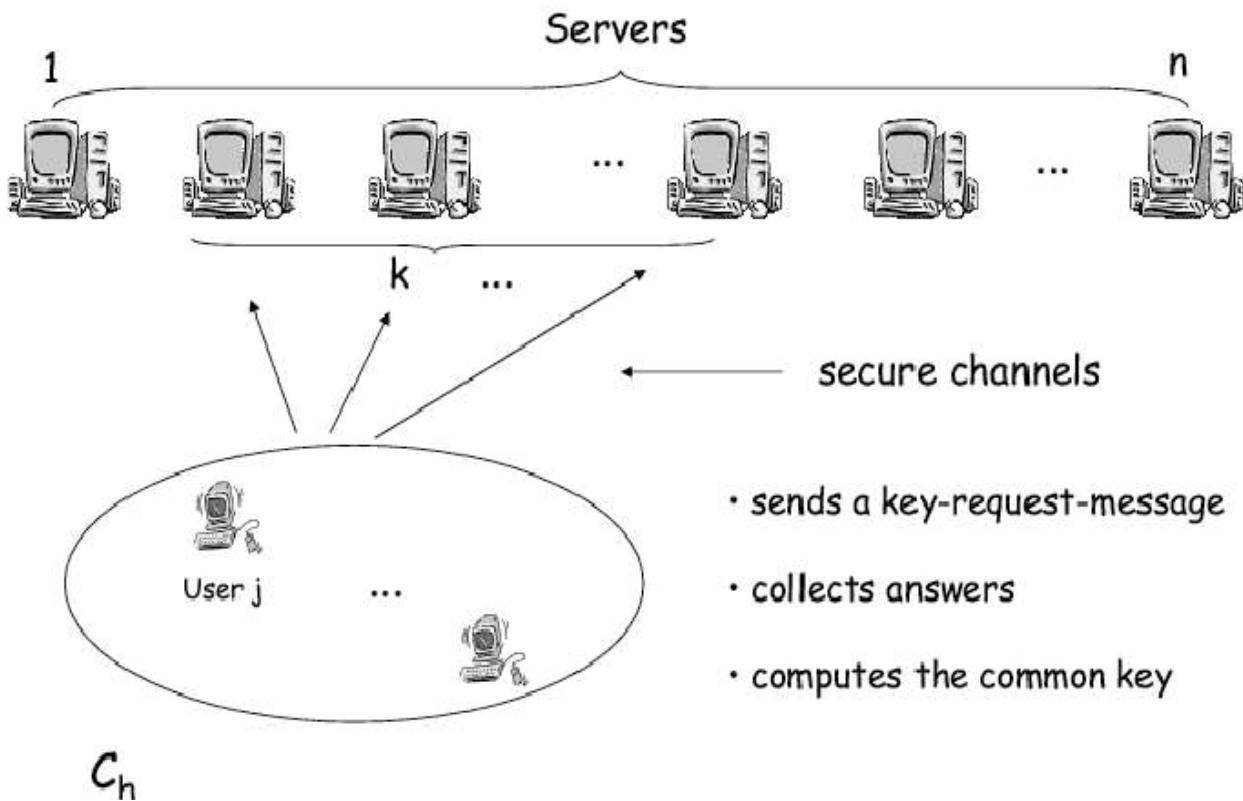


Figure 10 Distributed Key Distribution Centers (Source [www.semanticscholar.org](http://www.semanticscholar.org))

KDCs are commonly used in practice, but they still have the problem that at some point, a secure channel has to be used to share keys.

Thus, they cannot solve the problem of key distribution in open systems. Here is where asymmetry comes into cryptography; in particular, there are some actions that are easy to perform but very hard to be reversed. For example, it is easy to multiply two large primes but difficult to recover those primes from their product.

In 1976, Whitfield Diffie and Martin Hellman realized that such an approach could be used to create protocols for secure key exchange. These protocols can allow two parties to share a secret key with the uses of a public communication channel, by performing operations that they can reverse but an adversary cannot.

### The Diffie–Hellman key-exchange protocol

Consider an example with Alice and Bob who run a probabilistic protocol to generate a shared secret key. Alice and Bob begin by holding the security parameter  $1^n$ . Alice runs the protocol (denoted by  $G$ ) to obtain  $(C, q, g)$ . She uses  $(C, q, g)$  and a uniform  $x \in \mathbb{Z}_q$  to compute  $h_A = g^x$ .

She then sends  $(C, q, g, h_A)$  to Bob. Bob receives them and uses a uniform  $y \in \mathbb{Z}_q$  to compute

$h_B \oplus g^y$ . He then uses  $h_A$  to output  $k_B \oplus h^y$  sends  $h_B$  to Alice. Alice receives  $h_B$  and she computes  $k_A \oplus h_B^x$ .

Let's try that with actual numbers. Alice and Bob agree to use a modulus  $p = 49$  and base  $g = 11$  (has to be a primitive root). Alice chooses a secret integer  $x = 16$ , then sends Bob  $h_A = g^x \bmod p$

$$h_A = 11^{16} \bmod 23 = 18$$

Bob chooses a secret integer  $y = 24$ , then sends Alice  $h_B = g^y \bmod p$

$$h_B = 11^{24} \bmod 23 = 6$$

Alice computes  $k_A = h_B^x \bmod p$

$$k_A = 6^{16} \bmod 23 = 2$$

Bob computes  $k_B = h_A^y \bmod p$

$$k_B = 18^{24} \bmod 23 = 2$$

Alice and Bob now share the same secret key, “2”.

In order for this protocol to be secure there are some assumptions. At first, a minimal requirement for security is that the discrete-logarithm problem must be hard relative to  $G$ . If not, then an adversary given the transcript can compute the secret value of one of the parties (i.e.,  $x$ ) and then easily compute the shared key using that value. So, hardness of the discrete-logarithm problem is necessary for the protocol to be secure. But this is not enough for the protocol to be secure, as it is possible that there are other ways of computing the key  $k_A = k_B$  without explicitly computing  $x$  or  $y$ . The computational assumption which would only guarantee that the key  $g^{xy}$  is hard to compute in its entirety from the transcript, does not suffice either. What is required is that the shared key  $g^{xy}$  should be indistinguishable from uniform for any adversary given  $g, g^x, g^y$ .

So far we have considered only an eavesdropping adversary. Even though they are the most common attacks, active attacks play a very important role in cryptography. In active attacks, the adversary sends messages of its own to one or both of the parties. The objective is to impersonate one of the two parties and gain access to the keys. In addition, there are the man-in-the-middle attacks where both honest parties are executing the protocol and the adversary is intercepting and modifying messages being sent from one party to the other. The Diffie–Hellman protocol is completely insecure against man-in-the-middle attacks. In fact, a man-in-the-middle adversary can act in such a way that Alice and Bob terminate the protocol with different keys that

are both known to the adversary, yet neither Alice nor Bob can detect that any attack was carried out.

The Diffie–Hellman protocol in its basic form is typically not used in practice due to its insecurity against man-in-the-middle attacks, as discussed above. This does not detract in any way from its importance. The Diffie–Hellman protocol served as the first demonstration that asymmetric techniques could be used to alleviate the problems of key distribution in cryptography. Furthermore, the Diffie–Hellman protocol is at the core of standardized key-exchange protocols that are resilient to man-in-the-middle attacks and are in wide use today.

Except from key exchange, Diffie and Hellman introduced in their ground-breaking work the notion of public-key (or asymmetric) cryptography. In the public-key cryptography, a party who wishes to communicate securely generates a pair of keys: a public key that is widely disseminated, and a private key that it keeps secret. Due to the fact that this scheme has two keys, it is called asymmetric cryptography. Having generated these keys, a party can use them to ensure secrecy for messages it receives using a public-key encryption scheme, or integrity for messages it sends using a digital signature scheme.

In a public-key encryption scheme, the public key generated by some party serves as an encryption key; anyone who knows that public key can use it to encrypt messages and generate corresponding ciphertexts. The private key serves as a decryption key and is used by the party who knows it to recover the original message from any ciphertext generated using the matching public key. Furthermore, the secrecy of encrypted messages is preserved even against an adversary who knows the encryption. In other words, the (public) encryption key is of no use for an attacker trying to decrypt ciphertexts encrypted using that key. To enable secret communication, then, a receiver can simply send her public key to a potential sender, or publicize her public key on her webpage or in some central database. A public-key encryption scheme thus enables private communication without relying on a private channel for key distribution.

A digital signature scheme is a public-key analogue of MAC. Here, the private key serves as an “authentication key” that enables the party who knows this key to generate “authentication tags” for messages it sends.

The public key acts as a verification key, allowing anyone who knows it to verify signatures issued by the sender. As with MACs, a digital signature scheme can be used to prevent undetected tampering of a message. The fact that verification can be done by anyone who knows the public key of the sender, however, turns out to have far-reaching ramifications. Specifically, it makes it possible to take a document that was signed by Alice and present it to a third party as proof that Alice indeed signed the document.

This property is called non-repudiation and has extensive applications in electronic commerce. For example, it is possible to digitally sign contracts, send signed electronic purchase orders or promises of payments, and so on. Digital signatures are also used for the secure distribution of public keys as part of a public-key infrastructure.

In their paper, Diffie and Hellman set forth the notion of public-key cryptography but did not give any candidate constructions. A year later, Ron Rivest, Adi Shamir, and Len Adleman proposed the RSA problem and presented the first public-key encryption and digital signature schemes based on the hardness of this problem.

We close by summarizing how public-key cryptography addresses the limitations of the private-key cryptography.

- Public-key encryption allows key distribution to be done over public channels.
- Public-key cryptography reduces the need for users to store many secret keys.
- Finally, public-key cryptography is (more) suitable for open environments where parties who have never previously interacted want the ability to communicate securely.

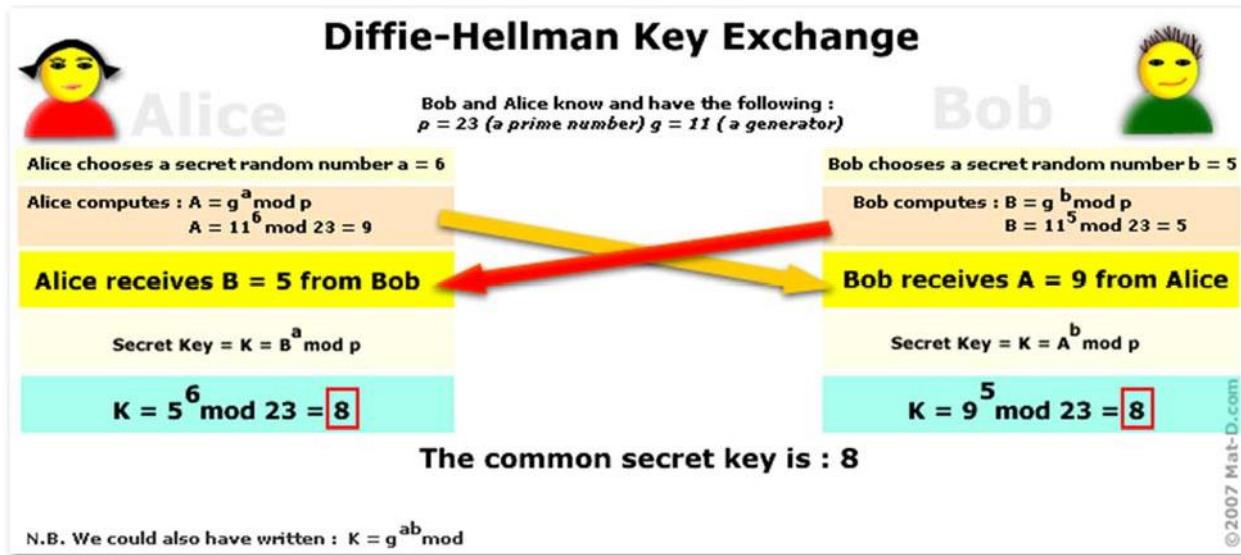


Figure 11 Diffie-Hellman Key Exchange Protocol (Source [www.internetokracy.appspot.com](http://www.internetokracy.appspot.com))

## Aim/Objectives

The purpose of the 10<sup>th</sup> Week is to show the basic problems faced with key management as well as the breakthrough public-key cryptography brings into the world of cryptography. We explain specific key management problems such as distribution, storing and its problems with open systems, and we give some existing solutions such as the Key-Distribution Centers (KDCs). We

then show the Diffie-Hellman key-exchange protocol and we discuss the innovation that protocol brought to cryptography and how it introduced the world to the public-key cryptography.

## Learning Outcomes

After the successful completion of the 10<sup>th</sup> Week, students should be able to:

- Evaluate key management in symmetric cryptography
- Explain the problems of key distribution, key storage and key management
- Explain why symmetric key cryptography is definitely not suitable for open systems
- Evaluate Key-Distribution Centers (KDCs)
- Explain the Diffie-Hellman key-exchange protocol

## Key Words

Public	Open Systems	Distribution Center
Session	Indistinguishable	Man-in-the-middle
Primitive Root	Single Point of Failure	Impersonation

## Annotated Bibliography

### Basic

- C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2010, Chapter 13 “Key Establishment”

The thirteenth Chapter of this book explains how the keys are established both in symmetric and in public-key cryptography, and it explains techniques of key distribution.

- W. Diffie and M. Hellman, "New directions in cryptography," in *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, November 1976.

### Suggestions for further reading

- Key Distribution Problem in Cryptography by Nirmal Jeyaraj [Youtube Video], Available at <https://www.youtube.com/watch?v=Jzxsxd0Un-w>

This video explains the key distribution problem faced in symmetric key cryptography

## **Self-Assessment Exercises**

### **Exercise 10.1**

Explain the problems faced with private-key cryptography

### **Exercise 10.2**

Explain what Key-Distribution centers are, giving their advantages and disadvantages

### **Exercise 10.3**

Explain the Diffie-Hellman key-exchange protocol

### **Exercise 10.4**

Show how public-key cryptography addresses private-key cryptography limitations

### **Exercise 10.5**

Using your preferred programming language, develop a simple implementation of the Diffie-Hellman key-exchange protocol.

## **Activity (5 points)**

Graded activity, which includes solving questions related to the syllabus covered up to Week 10, as well as applying the knowledge gathered up to this week in order to solve problems related to cryptography.

This activity counts 5% of the final course mark.

You will need approximately 5 hours to solve this Graded Activity

## **Recommended time for the student to work**

20 hours

## Summary

Public-key cryptography enables private communication without having to agree on any secret information in advance. In this week will go into further details about public key cryptography.

## Introductory Remarks

The differences between private-key and public-key cryptography are enormous. Private-key requires secret storage of all the keys, whereas public-key requires secrecy for only the private key. In private-key cryptography, the communicating parties must share the secret key without allowing any third party to learn it. In public-key, the key can be sent from one party to the other over a public channel without compromising security. Private-key cryptography uses the same key for both encryption and decryption whereas public-key cryptography use different keys for each operation. Furthermore, in public-key, a single key scheme enables multiple senders to communicate privately with a single receiver, in contrast to the private-key cryptography where a secret key shared between

two parties enables private communication only between those two parties.

The most important disadvantage of public-key cryptography is the need of computational power. Public-key encryption is roughly 2 to 3 orders of magnitude slower than private-key encryption. That means resource-constrained devices are severely affected.

## Public-Key Distribution

Up to now we assumed that any adversary is passive, for example the adversary only eavesdrops on communication between the sender and receiver without interfering with the communication. But if the adversary tampers all the communication between the honest parties, and these honest parties share no keys in advance, then privacy simply cannot be achieved. Let's discuss an example of such an attack. Let's say Alice sends her public key  $pk$  to Bob but the adversary replaces it with a key  $pk'$  of his own (for which it knows the matching private key  $sk'$ ), then even though Bob encrypts his message using  $pk'$  the adversary will easily be able to recover the message (using  $sk'$ ).

Similarly, if an adversary is able to change the value of Alice's public key that is stored in some public directory, or if the adversary can tamper with the public key as it is transmitted from the public directory to Bob.

If Alice and Bob do not share any information in advance, and are not willing to rely on some mutually trusted third party, there is nothing Alice or Bob can do to prevent active attacks of this sort, or even to tell that such an attack is taking place.

For the purposes of this course we will assume that the sender is able to receive a legitimate copy of the receiver's public key.

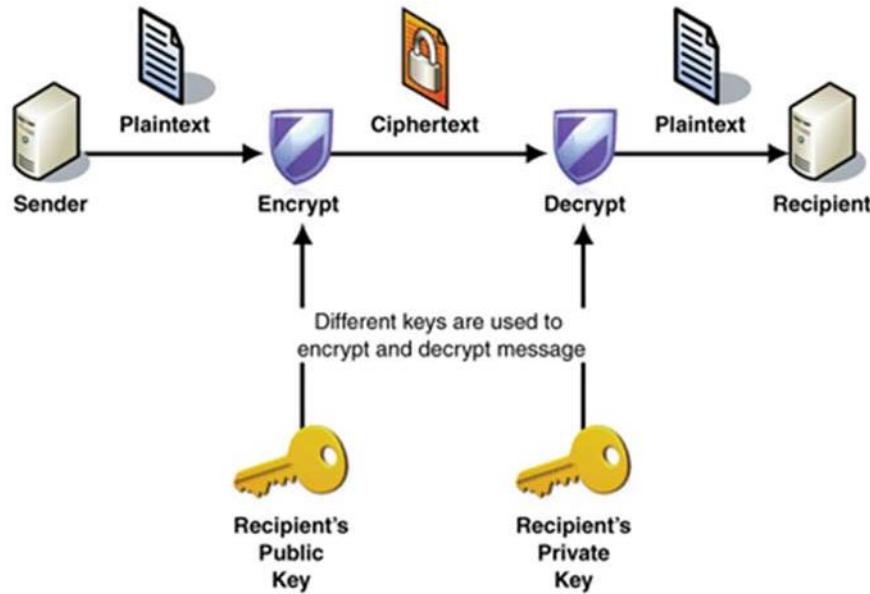


Figure 12 Public-Key Cryptography (Source [www.profwoodward.org](http://www.profwoodward.org))

### Public-Key Cryptography Syntax

A public-key encryption scheme is a triple of probabilistic polynomial-time algorithms ( $Gen$ ,  $Enc$ ,  $Dec$ ) such that:

- The key-generation algorithm  $Gen$  takes as input the security parameter  $1^n$  and outputs a pair of keys  $(pk, sk)$ . That is the public key  $pk$  and the private key  $sk$ . We assume for convenience that  $pk$  and  $sk$  each has length at least  $n$ , and that  $n$  can be determined from  $pk, sk$ .
- The encryption algorithm  $Enc$  takes as input a public key  $pk$  and a message  $m$  from some message space (that may depend on  $pk$ ). It outputs a ciphertext  $c$ , and we write this as  $c \leftarrow Enc_{pk}(m)$ . (Note that  $Enc$  needs to be probabilistic to achieve meaningful security.)

- c. The deterministic decryption algorithm  $Dec$  takes as input a private key  $sk$  and a ciphertext  $c$ , and outputs a message  $m$  or a special symbol  $\perp$  denoting failure. We write this as  $m \triangleq Dec_{sk}(c)$ .

It is required that, except possibly with negligible probability over  $(pk, sk)$  output by  $Gen(1^n)$ , we have  $Dec_{sk}(Enc_{pk}(m)) = m$  for any (legal) message  $m$ .

The important difference from the private-key cryptography is that the key generation algorithm  $Gen$  now outputs two keys instead of one. The public key  $pk$  is used for encryption, while the private key  $sk$  is used for decryption.  $pk$  is assumed to be widely distributed so that anyone can encrypt messages for the party who generated this key, but  $sk$  must be kept private by the receiver in order for security to possibly hold.

We allow for a negligible probability of decryption error and, indeed, some of the schemes have a negligible error probability.

For practical usage of public-key encryption, we will want the message space to be  $\{0, 1\}^n$  or  $\{0, 1\}^\perp$  (and, in particular, to be independent of the public key). Although we will sometimes describe encryption schemes using some message space  $M$  that does not contain all bit-strings of some fixed length (and that may also depend on the public key), we will in such cases also specify how to encode bit-strings as elements of  $M$ . This encoding must be both efficiently computable and efficiently reversible, so the receiver can recover the bit-string that was encrypted.

### **Chosen-Plaintext Attacks**

Given a public-key encryption scheme  $n = (Gen, Enc, Dec)$  and an adversary  $A$ , consider the following experiment:

The eavesdropping indistinguishability experiment  $PubK_{A,I}^{eav}(n)$ :

- a.  $Gen(1^n)$  is run to obtain keys  $(pk, sk)$
- b. Adversary  $A$  is given  $pk$ , and outputs a pair of equal-length messages  $m_0, m_1$  in the message space
- c. A uniform bit  $b \in \{0, 1\}$  is chosen, and then a ciphertext  $c \leftarrow Enc_{pk}(m_b)$  is computed and given to  $A$ . We call  $c$  the challenge ciphertext
- d.  $A$  outputs a bit  $b'$ . The output of the experiment is  $1$  if  $b' = b$ , and  $0$  otherwise. If  $b' = b$  we say that  $A$  succeeds.

A public-key encryption scheme  $n = (Gen, Enc, Dec)$  has indistinguishable encryptions in the presence of an eavesdropper if for all probabilistic polynomial-time adversaries  $A$  there is a negligible function  $negl$  such that

$$Pr[PubK_{A, ll}^{eav}(n) = 1] : s: \frac{1}{2} + negl(n)$$

### **Chosen-Ciphertext Attacks**

Chosen-ciphertext attacks, in which an adversary is able to obtain the decryption of arbitrary ciphertexts of its choice, are a concern in the public-key cryptography just as they are in the private-key cryptography. In fact, they are arguably more of a concern in the public-key cryptography since there a receiver expects to receive ciphertexts from multiple senders who are possibly unknown in advance, whereas a receiver in the private-key cryptography intends to communicate only with a single, known sender using any particular secret key.

Assume an eavesdropper  $A$  observes a ciphertext  $c$  sent by a sender  $S$  to a receiver  $R$ . Broadly speaking, in the public-key cryptography there are two classes of chosen-ciphertext attacks:

- a.  $A$  might send a modified ciphertext  $c'$  to  $R$  on behalf of  $S$ . In this case, although it is unlikely that  $A$  would be able to obtain the entire decryption  $m'$  of  $c'$ , it might be possible for  $A$  to infer some information about  $m'$  based on the subsequent behavior of  $R$ . Based on this information,  $A$  might be able to learn something about the original message  $m$ .
- b.  $A$  might send a modified ciphertext  $c'$  to  $R$  in its own name. In this case,  $A$  might obtain the entire decryption  $m'$  of  $c'$  if  $R$  responds directly to  $A$ . Even if  $A$  learns nothing about  $m'$ , this modified message may have a known relation to the original message  $m$  that can be exploited by  $A$ .

The CCA indistinguishability experiment  $PubK_{A, ll}^{cca}(n)$ :

- a.  $Gen(1^n)$  is run to obtain keys  $(pk, sk)$
- b. The adversary  $A$  is given  $pk$  and access to a decryption oracle  $Dec_{sk}(\bullet)$ . It outputs a pair of messages  $m_0, m_1$  of the same length
- c. A uniform bit  $b \in \{0, 1\}$  is chosen, and then a ciphertext  $c \leftarrow Enc_{pk}(m_b)$  is computed and given to  $A$
- d.  $A$  continues to interact with the decryption oracle, but may not request a decryption of  $c$  itself. Finally,  $A$  outputs a bit  $b'$
- e. The output of the experiment is defined to be 1 if  $b' = b$ , and 0 otherwise

A public-key encryption scheme  $n = (Gen, Enc, Dec)$  has indistinguishable encryptions under a chosen-ciphertext attack (or is CCA-secure) if for all probabilistic polynomial-time adversaries  $A$  there exists a negligible function  $negl$  such that

$$Pr[PubK_{A,II}^{cca}(n) = 1] : s: \frac{1}{2} + negl(n)$$

## Aim/Objectives

The purpose of the 11<sup>th</sup> Week is to introduce public-key cryptography. We explain how public-key cryptography enables private communication without the parties having to share a secret key at the beginning. We explain how keys work in public-key cryptography and how they are distributed. Finally we explain some attacks that might take place in such a scheme and what they can achieve.

## Learning Outcomes

After the successful completion of the 11<sup>th</sup> Week, students should be able to:

- Evaluate public-key cryptography
- Explain how key distribution is performed in public-key cryptography
- Explain how a chosen-plaintext attack can take place in such a scheme
- Explain how a chosen-ciphertext attack can take place in such a scheme

## Key Words

Computational Power	Distribution	Eavesdropping
Tampering	Key Pair	Indistinguishable

## Annotated Bibliography

### Basic

- C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2010, Chapter 6 “introduction to Public-Key Cryptography”

The sixth Chapter of this book introduces the concept of public-key cryptography. It explains why it is important and it also gives its advantages and disadvantages compared to private-key cryptography.

### **Suggestions for further reading**

- Public Key Cryptography – Computerphile, [Youtube Video], Available at: [https://www.youtube.com/watch?v=GSIDS\\_lvRv4](https://www.youtube.com/watch?v=GSIDS_lvRv4)
- Al-Riyami S.S., Paterson K.G. (2003) Certificateless Public Key Cryptography. In: Laih CS. (eds) Advances in Cryptology - ASIACRYPT 2003. ASIACRYPT 2003. Lecture Notes in Computer Science, vol 2894. Springer, Berlin, Heidelberg

## **Self-Assessment Exercises**

### **Exercise 11.1**

Briefly explain how public-key is distributed in public-key cryptography

### **Exercise 11.2**

Give a proper public-key cryptography definition and syntax

### **Exercise 11.3**

Explain chosen-plaintext and chosen-ciphertext attacks in public-key cryptography

### **Exercise 11.4**

Compare Public Key to Private Key cryptography, giving appropriate examples

## **Recommended time for the student to work**

15 hours

### Summary

In this week we introduce the RSA Encryption which are encryption schemes based on the RSA assumption which we defined in week 9.

### Introductory Remarks

Even though RSA based encryption is in widespread use today, there is a gradual shift away from using RSA, and toward using CDH/DDH-based cryptosystems, due to the longer key lengths required for RSA based schemes.

#### Plain RSA

Let's describe a simple encryption scheme based on the RSA problem. Even though such a scheme is insecure, it is a good way to start an RSA based encryption.

Let  $\text{GenRSA}$  be a *PPT* algorithm that, on input  $1^n$ , outputs a modulus  $N$  that is the product of two n-bit primes, along with integers  $e, d$  satisfying  $ed = 1 \bmod \phi(N)$ . Let  $N, e, d$  satisfy the equation, and let  $c = m^e \bmod N$ . RSA encryption relies on the fact that someone who knows  $d$  can recover  $m$  from  $c$  by computing  $c^d \bmod N$ . This works because

$$c^d = (m^e)^d = m^{ed} = m \bmod N$$

On the other hand, without knowledge of  $d$  (even if  $N$  and  $e$  are known) the RSA assumption implies that it is difficult to recover  $m$  from  $c$ , at least if  $m$  is chosen uniformly from  $\mathbb{Z}_N^\times$ .

Therefore we can summarise this plain RSA encryption as follows

Let  $\text{GenRSA}$  be as in the text.

- a. *Gen*: on input  $1^n$  run  $\text{GenRSA}(1^n)$  to obtain  $N, e$ , and  $d$ . The public key is  $\langle N, e \rangle$  and the private key is  $\langle N, d \rangle$ .
- b. *Enc*: on input a public key  $pk = \langle N, e \rangle$  and a message  $m \in \mathbb{Z}_N^\times$  compute the ciphertext  $c \in \mathbb{Z}_N^\times$   $= [m^e \bmod N]$ .
- c. *Dec*: on input a private key  $sk = \langle N, d \rangle$  and a ciphertext  $c \in \mathbb{Z}_N^\times$  compute the message  $m \in \mathbb{Z}_N^\times$   $= [c^d \bmod N]$ .

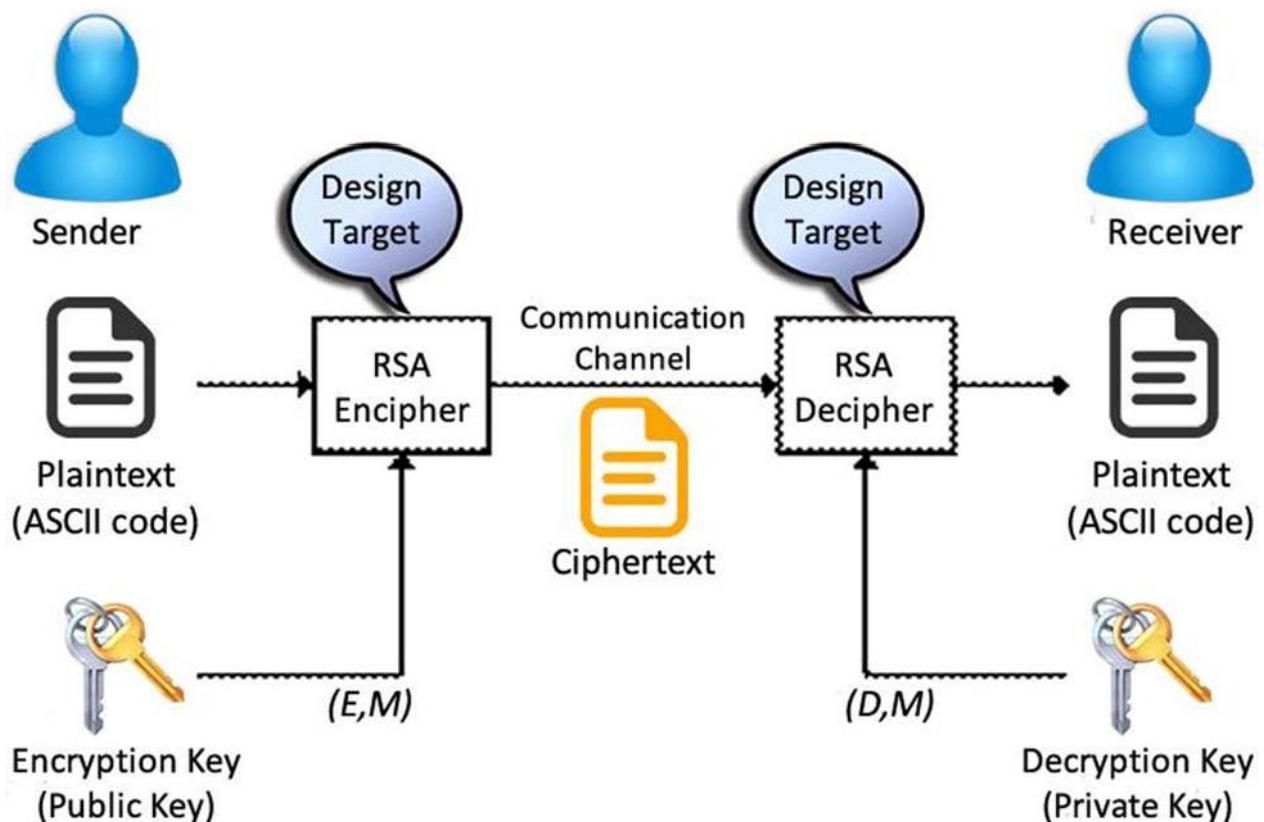


Figure 13 RSA Encryption Scheme (Source [www.researchgate.net](http://www.researchgate.net))

The factoring assumption implies that it is computationally infeasible for an attacker who is given the public key to derive the corresponding private key. This is necessary, but not sufficient, for a public-key encryption scheme to be secure. The RSA assumption implies that if the message  $m$  is chosen uniformly from  $\{1\}_N^{\mathbb{Z}}$  then an eavesdropper given  $N$ ,  $e$ , and  $c$  cannot recover  $m$ . But these are weak guarantees, and fall far short of the level of security we want. In particular, they leave open the possibility that an attacker can recover the message when it is not chosen uniformly from  $\{1\}_N^{\mathbb{Z}}$ . In addition, it does not rule out the possibility that an attacker can learn partial information about the message, even when it is uniform. Moreover, plain RSA encryption is deterministic and so must be insecure.

We have already noted that plain RSA encryption is not CPA-secure. Nevertheless, there may be a temptation to use plain RSA for encrypting “random messages” and/or in situations where leaking a few bits of information about the message is acceptable. We warn against this in general, and provide here just a few examples of what can go wrong.

#### Quadratic Improvement in Recovering M

Since plain RSA encryption is deterministic, we know that if  $m < B$  then an attacker can determine  $m$  from the ciphertext  $c = [m^e \text{ mod } N]$  in time  $O(B)$  using a brute-force attack. One might hope, however, that plain RSA encryption can be used if  $B$  is large, i.e., if the message is chosen from a reasonably large set of values. One possible scenario where this might occur is in the context of hybrid encryption, where the “message” is a random  $n$ -bit key and so  $B = 2^n$ . Unfortunately, there is a clever attack that recovers  $m$ , with high probability, in time roughly  $O(\sqrt{B})$ . This can make a significant difference in practice: a  $2^{80}$ -time attack (say) is infeasible, but an attack running in time  $2^{40}$  is relatively easy to carry out.

### Encrypting short messages using small $e$

The previous attack shows how to recover a message  $m$  known to be smaller than some bound  $B$  in time roughly  $O(\sqrt{B})$ . Here we show how to do the same thing in time  $\text{poly}(\|N\|)$  if  $B : s: N^{1/e}$ . The attack relies on the observation that when  $m < N^{1/e}$ , raising  $m$  to the  $e$ th power modulo  $N$  involves no modular reduction. This means that given the ciphertext  $c = [m^e \text{ mod } N]$ , an attacker can determine  $m$  by computing  $m \equiv c^{1/e}$  over the integers. This can be done easily in time  $\text{poly}(\|c\|) = \text{poly}(\|N\|)$  since finding  $e$ th roots is easy over the integers and hard only when working mod  $N$ . For small  $e$  this represents a serious weakness of plain RSA encryption. For example, if we take  $e = 3$  and assume  $\|N\| \geq 1024$  bits, then the attack works even when  $m$  is a uniform 300-bit integer; this once again rules out security of plain RSA even when used as part of a hybrid encryption scheme.

### Encrypting a partially known message

This attack can be viewed as a generalization of the previous one. It assumes a sender who encrypts a message, part of which is known. Here we rely on a powerful result of Coppersmith which says:

Let  $p(x)$  be a polynomial of degree  $e$ . Then in time  $\text{poly}(\|N\|, e)$  one can find all  $m$  such that  $p(m) = 0 \text{ mod } N$  and  $|m| : s: N^{1/e}$ .

Due to the dependence of the running time on  $e$ , the attack is only practical for small  $e$ . In what follows we assume  $e = 3$  for concreteness. Assume a sender encrypts a message  $m = m_1 // m_2$  to a receiver with public key  $(N, 3)$ , where the first portion  $m_1$  of the message is known but the second portion  $m_2$  is not. For concreteness, say  $m_2$  is  $k$  bits long, so  $m = B \cdot m_1 + m_2$  where we let  $B = 2^k$ . Given the resulting ciphertext  $c = [(m_1 // m_2)^3 \text{ mod } N]$ , an eavesdropper can

define  $p(x) \triangleq (2^k \cdot m_1 + x)^3 - c$ , a cubic polynomial. This polynomial has  $m_1$  as a root (modulo  $N$ )<sup>2</sup>, and  $|m_2| < B$ . A similar attack works when  $m_2$  is known but  $m_1$  is not.

## Aim/Objectives

The purpose of the 12<sup>th</sup> Week is to show how RSA Encryption works using the RSA assumption. We show how this can be applied in cryptography but at the same time we show how insecure it is. Finally, we describe several attacks that can be performed on such a plain RSA scheme.

## Learning Outcomes

After the successful completion of the 12<sup>th</sup> Week, students should be able to:

- Evaluate RSA Encryption
- Explain how RSA assumption can be used in favour of RSA encryption
- Explain quadratic improvement in recovering message  $m$
- Explain the problem of encrypting using small  $e$
- Explain an attack that can be performed if the RSA scheme encrypts a partially known message

## Key Words

RSA	Problem	Assumption
PPT	Uniformly	CPA-Secure
Quadratic	Small $e$	Known Message

## Annotated Bibliography

### Basic

- C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2010, Chapter 7 “The RSA Cryptosystem”

The seventh Chapter of this book explains how RSA works. It gives the practical aspects of RSA, such as the fast encryption and decryption as well as its computation parameters. Finally, it shows its security estimations and implementation aspects.

### Suggestions for further reading

- Public Key Cryptography: RSA Encryption Algorithm [Youtube Video], Available at: [https://www.youtube.com/watch?v=wXB-V\\_Keiu8](https://www.youtube.com/watch?v=wXB-V_Keiu8)
- Encryption and HUGE numbers - Numberphile [Youtube Video], Available at: <https://www.youtube.com/watch?v=M7kEpw1tn50>
- Xin Zhou and Xiaofei Tang, "Research and implementation of RSA algorithm for encryption and decryption," Proceedings of 2011 6th International Forum on Strategic Technology, Harbin, Heilongjiang, 2011, pp. 1118-1121.

## Self-Assessment Exercises

### Exercise 12.1

Explain plain RSA giving a formal definition

### Exercise 12.2

Give some examples in which RSA can go wrong

## Group Assignment (20 points)

The group assignment includes solving questions related to the syllabus covered in this course. The questions can vary from practical ones, to essay style questions asking to use your current skills as a group in order to describe existing cryptography methods, or even program them into fully working solutions.

In addition, there will be one exercise asking to implement using any programming language, one of the protocols already taught in the course.

This assignment counts 20% of the final course mark.

You will need approximately 20 hours to solve this Group Assignment.

## Recommended time for the student to work

35 hours

## Summary

Signature schemes allow a signer  $S$  who has established a public key  $pk$  to “sign” a message using the associated private key  $sk$  in such a way that anyone who knows  $pk$ , and knows that this public key was established by  $S$ , can verify that the message originated from  $S$  and was not modified in transit. In this week we will discuss what digital signatures are and how they are used.

## Introductory Remarks

As a prototypical application, consider a software company that wants to disseminate software updates in an authenticated manner; that is, when the company releases an update it should be possible for any of its clients to verify that the update is authentic, and a malicious third party should never be able to fool a client into accepting an update that was not actually released by the company. To do this, the company can generate a public key  $pk$  along with a private key  $sk$ , and then distribute  $pk$  in some reliable manner to its clients while keeping  $sk$  secret. When releasing a software update  $m$ , the company computes a digital signature  $u$  on  $m$  using its private key  $sk$ , and sends  $(m, u)$  to every client. Each client can verify the authenticity of  $m$  by checking that  $u$  is a correct signature on  $m$  with respect to the public key  $pk$ .

A malicious party might try to issue a fraudulent update by sending  $(m', u')$  to a client, where  $m'$  represents an update that was never released by the company. This  $m'$  might be a modified version of some previous update, or it might be completely new and unrelated to any prior updates. If the signature scheme is “secure”, however, then when the client attempts to verify  $u'$  it will find that this is an invalid signature on  $m'$  with respect to  $pk$ , and will therefore reject the signature. The client will reject even if  $m'$  is modified only slightly from a genuine update  $m$ . This is not just a theoretical application of digital signatures, but one that is used extensively today for distributing software updates.

## Digital Signatures Compared to Message Authentication Codes (MACs)

Both MACs and digital signature schemes are used to ensure the integrity of transmitted messages. Using digital signatures rather than MACs simplifies key distribution and management, especially when a sender needs to communicate with multiple receivers. By using a digital signature scheme the sender avoids having to establish a distinct secret key with each potential receiver, and avoids having to compute a separate MAC tag with respect to each such key. Instead, the sender need only compute a single signature that can be verified by all recipients. A qualitative advantage that digital signatures have as compared to MACs is that signatures are publicly verifiable. This means that if a receiver verifies that a signature on a given message is legitimate, then all other parties who receive this signed message will also verify it as legitimate. This feature is not achieved by MACs if the signer shares a separate key with each receiver. Public verifiability implies that signatures are transferable: a signature  $u$  on a message  $m$  by a signer  $S$  can be shown to a third party, who can then verify herself that  $u$  is a legitimate signature on  $m$  with respect to  $S$ 's public

key. By making a copy of the signature, this third party can then show the signature to another party and convince them that  $S$  authenticated  $m$ , and so on. Public verifiability and transferability are essential for the application of digital signatures to certificates and public-key infrastructures. Digital signature schemes also provide the very important property of non-repudiation. This means that once  $S$  signs a message he cannot later deny having done so. This aspect of digital signatures is crucial for legal applications where a recipient may need to prove to a third party that a signer did indeed “certify” a particular message: assuming  $S$ 's public key is known to the judge, or is otherwise publicly available, a valid signature on a message serves as convincing evidence that  $S$  indeed signed this message. MACs simply cannot provide non-repudiation. Let's say users  $S$  and  $R$  share a key  $k_{SR}$ , and  $S$  sends a message  $m$  to  $R$  along with a (valid) MAC tag  $t$  computed using this key. Since the judge does not know  $k_{SR}$ , there is no way for the judge to determine whether  $t$  is valid or not. If  $R$  were to reveal the key  $k_{SR}$  to the judge, there would be no way for the judge to know whether this is the “actual” key that  $S$  and  $R$  shared, or whether it is some “fake” key manufactured by  $R$ . Finally, even if we assume the judge can somehow obtain the actual key  $k_{SR}$  shared by the parties, there is no way for the judge to distinguish whether  $S$  generated  $t$  or whether  $R$  did.

As in the case of private-key vs. public-key encryption, MACs have the advantage of being shorter and roughly 2–3 orders of magnitude more efficient to generate/verify than digital signatures.

Thus, in situations where public verifiability, transferability, and/or non-repudiation are not needed, and the sender communicates primarily with a single recipient MACs should be used.

Digital signatures are the public-key counterpart of MACs, and their syntax and security guarantees are analogous. The algorithm that the sender applies to a message is here denoted *Sign* (rather than *Mac*), and the output of this algorithm is now called a *signature* (rather than a *tag*). The algorithm that the receiver applies to a message and a signature in order to verify validity is still denoted *Vrfy*.

A (digital) signature scheme consists of three probabilistic polynomial-time *PPT* algorithms (*Gen*, *Sign*, *Vrfy*) such that:

- a. The key-generation algorithm *Gen* takes as input a security parameter  $1^n$  and outputs a pair of keys  $(pk, sk)$ . These are called the public key and the private key, respectively. We assume that  $pk$  and  $sk$  each has length at least  $n$ , and that  $n$  can be determined from  $pk$  or  $sk$ .
- b. The signing algorithm *Sign* takes as input a private key  $sk$  and a message  $m$  from some message space (that may depend on  $pk$ ). It outputs a signature  $u$ , and we write this as  $u \leftarrow \text{Sign}_{sk}(m)$ .
- c. The deterministic verification algorithm *Vrfy* takes as input a public key  $pk$ , a message  $m$ , and a signature  $u$ . It outputs a bit  $b$ , with  $b = 1$  meaning valid and  $b = 0$  meaning invalid. We write this as  $b \leftarrow \text{Vrfy}_{pk}(m, u)$ .

It is required that except with negligible probability over  $(pk, sk)$  output by  $\text{Gen}(1^n)$ , it holds that  $\text{Vrfy}_{pk}(m, \text{Sign}_{sk}(m)) = 1$  for every (legal) message  $m$ . If there is a function  $l$  such that for every  $(pk, sk)$  output by  $\text{Gen}(1^n)$  the message space is  $\{0, 1\}^{l(n)}$ , then we say that  $(\text{Gen}, \text{Sign}, \text{Vrfy})$  is a signature scheme for messages of length  $l(n)$ .

A signature scheme is used in the following way. One party  $S$ , who acts as the sender, runs  $\text{Gen}(1^n)$  to obtain keys  $(pk, sk)$ . The public key  $pk$  is then publicized as belonging to  $S$ . For example,  $S$  can put the public key on its webpage or place it in some public directory. As in the case of public-key encryption, we assume that any other party is able to obtain a legitimate copy of  $S$ 's public key. When  $S$  wants to authenticate a message  $m$ , it computes the signature  $u \leftarrow \text{Sign}_{sk}(m)$  and sends  $(m, u)$ . Upon receipt of  $(m, u)$ , a receiver who knows  $pk$  can verify the authenticity of  $m$  by checking whether  $\text{Vrfy}_{pk}(m, u) = 1$ . This establishes both that  $S$  sent  $m$ ,

and also that  $m$  was not modified in transit. As in the case of MACs, however, it does not say anything about when  $m$  was sent, and replay attacks are still possible.

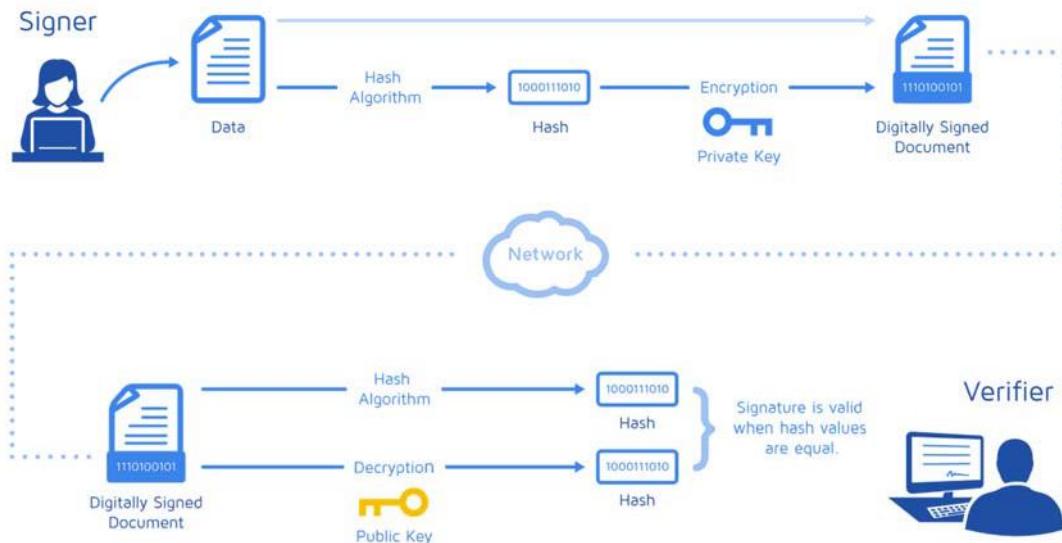


Figure 14 Digital Signature (Source [www.medium.com](http://www.medium.com))

## Aim/Objectives

The purpose of the 13<sup>th</sup> Week is to introduce the concept of digital signatures. We first examine the basic principles of digital signatures and then compare them to MACs. We explain why for some applications are better than MACs but we also discuss the computational cost, and how we can use MACs if computation cost is important. We then define digital signatures and giving an example use of it.

## Learning Outcomes

After the successful completion of the 13<sup>th</sup> Week, students should be able to:

- Evaluate digital signatures
- Explain the differences between digital signatures and MACs
- Explain when it is better to use a digital signature and when MACs are preferred
- Explain how digital signatures work giving example usages

## Key Words

Digital Signature	Public Key	Private Key
Malicious Party	Secure	Distribution
Verifiability	Transferability	Infrastructures

## Annotated Bibliography

### Basic

- C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2010, Chapter 10 “Digital Signatures”

The tenth Chapter of this book explains the principles of digital signatures. It describes security services and the objectives that can be achieved by a security system. It then explains the RSA digital signature scheme.

### Suggestions for further reading

- Digital Signatures - Udacity [Youtube Video], Available at: <https://www.youtube.com/watch?v=704dudhA7UI>
- Blundo, Carlo and Paolo D'Arco. "Analysis and Design of Distributed Key Distribution Centers." Journal of Cryptology 18 (2005): 391-414.

## Self-Assessment Exercises

### Exercise 13.1

Explain what digital signatures are and how are used

### Exercise 13.2

Give the differences between digital signatures and MACs

### Exercise 13.3

Give a formal definition of digital signatures

### Exercise 13.4

Compare MACs and Digital Signatures

## **Recommended time for the student to work**

15 hours

## **REVISION AND FINAL EXAMINATION**

The final examination will consist of a series of questions covering the material covered in this course.

Those questions will be in the form of multiple choice, essay style questions (mainly for methods and protocol explanations) as well as more practical questions for solving mathematical equations applied to cryptography.

The Final Examinations counts 50% of the final course mark.

### **Recommended time for the student to work**

40 hours

**Date/Time of Final Exam: TBD**

## INDICATIVE ANSWERS TO SELF-ASSESSMENT EXERCISES

### Introduction (1<sup>st</sup> Week)

#### Exercise 1.1

The sender (Alice) wants to send a message to the receiver (Bob). Alice enumerates (gives them an ascending serial number) the characters (usually bits) in her message and splits them out each in a separate packet. Alice predefines a method with Bob so he can authenticate packets and adds a Message Authentication Code (MAC) to each packet. Alice interleaves the packets with corresponding bogus packets (called "chaff") with corresponding serial numbers, arbitrary characters, and a random number in place of the MAC. She then sends the packets to Bob.

Bob uses the MAC to find the authentic messages and drops the "chaff" messages. This process is called "winnowing". An eavesdropper located between Alice and Bob would have to tell which packets are bogus and which are real (i.e. to winnow, or "separate the wheat from the chaff"). That is infeasible if the MAC used is secure.

#### Exercise 1.2

Pixels are the smallest individual element of an image. The intensity of each pixel is variable. In colour imaging systems, a colour is typically represented by three or four component intensities such as red, green, and blue, (RGB Model) or cyan, magenta, yellow, and black (CMYK Model). The RGB colour model is an additive colour model in which red, green and blue light are added together in various ways to reproduce a broad array of colours. The name of the model comes from the initials of the three additive primary colours, red, green, and blue. The main purpose of the RGB colour model is for the sensing, representation and display of images in electronic systems, such as televisions and computers, though it has also been used in conventional photography.

So, each pixel from the image is composed of 3 values (red, green, blue) which are 8-bit values (the range is 0–255). When working with binary codes, we have more significant bits and less significant bits.

The leftmost bit is the most significant bit. If we change the leftmost bit it will have a large impact on the final value. For example, if we change the leftmost bit from 1 to 0 (11111111 to 01111111) it will change the decimal value from 255 to 127.

On the other hand, the rightmost bit is the less significant bit. If we change the rightmost bit it will have less impact on the final value. For example, if we change the rightmost bit from 1 to 0 (11111111 to 11111110) it will change the decimal value from 255 to 254. Note that the rightmost bit will change only 1 in a range of 256 (it represents less than 1%). Therefore we can use rightmost bit (or bits, we can use the rightmost 2 bits) to hide information.

### Exercise 1.3

Plaintext is paired with the random secret pre-shared key (one-time pad), then each character of the plaintext is encrypted by combining it with the corresponding one-time pad character using addition. To decrypt it you need the pre-shared secret key to reverse the process.

Suppose Alice wishes to send the message "HELLO" to Bob. The one time pad key that Alice will use in this case is "XMCKL". Alice will have to find the numerical values (alphabet location) of each of the letters in her message, then do the exact same process for the key letters and add the two numerical values of corresponding message and key letters together. Then Alice will have to perform modulus 26 (if she uses English. This value is the amount of characters present in the alphabet used) and use the resulting number as a number indicating a position to find the letter in the alphabet.

	H	E	L	L	O	Message
	7 (H)	4 (E)	11 (L)	11 (L)	14 (O)	Message with alphabet location
+	23 (X)	12 (M)	2 (C)	10 (K)	11 (L)	Key
=	30	16	13	21	25	Message + Key
mod 26	4 (E)	16 (Q)	13 (N)	21 (V)	25 (Z)	(Message + Key) mod 26
	E	Q	N	V	Z	Ciphertext

### Exercise 1.4

	I	N	T	R	O	D	U	C	T	I	O	N	T	O
	I(8)	N(13)	T(19)	R(17)	O(14)	D(3)	U(20)	C(2)	T(19)	I(8)	O(14)	N(13)	T(19)	O(14)
+	P(15)	E(4)	S(18)	B(1)	U(20)	S(18)	E(4)	D(3)	E(4)	D(3)	E(4)	N(13)	A(0)	Y(24)
=	23	17	37	18	34	21	24	5	23	11	18	26	19	38
mod 26	23	17	11	18	8	21	24	5	23	11	18	0	19	12
	X	R	L	S	I	V	Y	F	X	L	S	A	T	M

	C	R	Y	P	T	O	G	R	A	P	H	Y
	C(2)	R(17)	Y(24)	P(15)	T(19)	O(14)	G(6)	R(17)	A(0)	P(15)	H(7)	Y(24)
+	A(0)	L(11)	L(11)	G(6)	M(12)	N(13)	C(2)	O(14)	F(5)	W(22)	I(8)	S(18)
=	2	28	35	21	31	27	8	31	5	37	15	42
mod 26	2	2	9	21	5	1	8	5	5	11	15	16

	C	C	J	V	F	B	I	F	F	L	P	Q
--	---	---	---	---	---	---	---	---	---	---	---	---

### Exercise 1.5

- a) Using the crypto tool provided at <http://www.cryptoprograms.com/tools/frequency>

Ciphertext		English Language	
Letter	Frequency (%)	Letter	Frequency (%)
L	13.8	E	12.7
A	12	T	9.1
H	8.4	A	8.2
Y	7.7	O	7.5
U	7.5	I	6.9
P	7.3	N	6.7
Z	6.9	S	6.3
V	4.9	H	6.1
J	4.1	R	5.9
O	4.1	D	4.3
W	3.3	L	4.0
B	2.9	C	2.8
T	2.6	U	2.8
K	2.2	M	2.4
S	2.2	W	2.4
N	2	F	2.2
F	1.8	G	2
M	1.8	Y	1.9
E	1.4	P	1.9
I	1.4	B	1.5
C	0.4	V	0.9
D	0.4	K	0.7
R	0.4	J	0.2
X	0.2	X	0.2
G	0	Q	0.1
Q	0	Z	0.1

- b) Using the results from part (a), there are several ways we can follow in order to decrypt the cipher.

The first way is to replace each letter using with the corresponding letter in the English language using the relative frequency. This can be a very good method, but you might face some problems in the least frequent letters and you might have to switch repeatedly to find the correct sequence.

For this particular example, there is a better way to solve it. We already know that this is a substitution cipher, therefore there has to be a key (or shift, the number of places you move through the alphabet). Therefore, to find the key we can try as follows

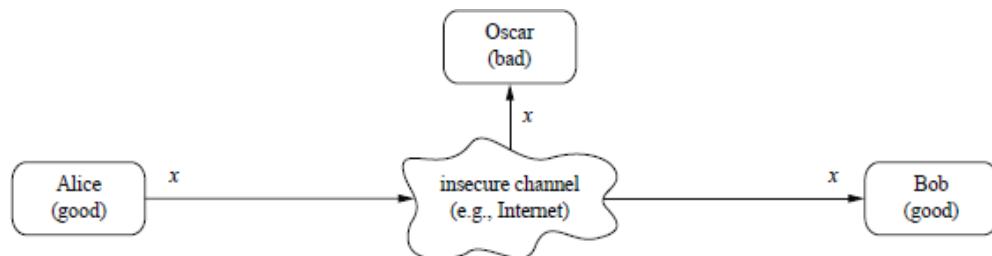
- 1) Take the most frequent letter in the English language and find the most frequent in the ciphertext. In this case its E and L. What is the difference in alphabet positions (shift) between the two letters? The answer is 7.

- 2) Take the second most frequent. In this case is T and A. The difference between the two in alphabet positions starting from T and going to A in ascending order is 7 again.
- 3) Take the third most frequent. A and H. The difference is again 7.
- 4) Therefore, this is a really good indication that the key has to be 7

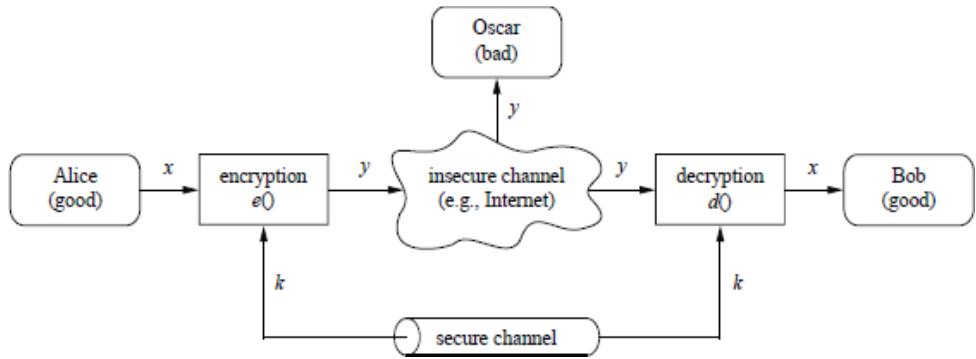
If we use key=7 and try to decode the message we get the following result

plaintext is a term used in cryptography that refers to a message before encryption or after decryption plain text refers to text consisting entirely of characters that are used in some written human language as contrasted with sequences of bits that do not represent human readable characters ciphertext it is the unreadable output of an encryption algorithm the term cipher is sometimes used as an alternative term for ciphertext. Ciphertext is not understandable until it has been converted into plain text using a key cipher is the basic mechanism of encrypting a message using a key

### Exercise 1.6



There are two users, Alice and Bob, who want to communicate over an insecure channel. The actual problem starts with the bad guy, Oscar, who has access to the channel, for instance, by hacking into an Internet router or by listening to the radio signals of a Wi-Fi communication. This type of unauthorized listening is called **eavesdropping**.



Symmetric cryptography offers a powerful solution: Alice encrypts her message  $x$  using a symmetric algorithm, yielding the ciphertext  $y$ . Bob receives the ciphertext and decrypts the message. Decryption is, thus, the inverse process of encryption. If we have a strong encryption algorithm, the ciphertext will look like random bits to Oscar and will contain no information whatsoever that is useful to him.

### Problems

The system needs a secure channel for distribution of the key between Alice and Bob. If Oscar gets hold of the key, he can easily decrypt the message since the algorithm is publicly known. Hence it is crucial to note that the problem of transmitting a message securely is reduced to the problems of transmitting a key secretly and of storing the key in a secure fashion.

In this scenario we only consider the problem of **confidentiality**, that is, of hiding the contents of the message from an eavesdropper. We will see later that there are many other things we can do with cryptography, such as preventing Oscar from making unnoticed changes to the message (message **integrity**) or assuring that a message really comes from Alice (sender **authentication**).

### Exercise 1.7

Solution using the Python programming language

```

def charToNum(char):
    alphabet = "abcdefghijklmnopqrstuvwxyz"
    num = 1
    for letter in alphabet:
        if letter == char:
            break
        else:
            num+=1
    return num

def numToChar(num):
    alphabet = "abcdefghijklmnopqrstuvwxyz"

```

```

        return alphabet[num+1]

def encodeChar(pText, key):
    cNum = (charToNum(pText) + charToNum(key)) % 26
    cText = numToChar(cNum)
    return cText

def decodeChar(cText, key):
    pNum = charToNum(cText) - charToNum(key)
    pText= numToChar(pNum)
    return pText

def encode(pText, key):
    cText= ""
    for i in range(0, len(pText)):
        cText += encodeChar(pText[i], key[i])

    return cText

def decode(cText, key):
    pText=""
    for i in range(0, len(cText)):
        pText += decodeChar(cText[i], key[i])
    return pText

def main():
    cont=True
    choice=""
    print("OTP Program. Key must be less than or equal to plaintext in length. Plaintext must not contain numbers.")
    print("\nChoices:\n1: Encode\n2: Decode\n3: Quit")
    while cont == True:
        choice = input(">>> ")
        if choice == "1":
            print("Your ciphertext is " + encode(input("Please enter your plaintext: "), input("Please enter your key: ")))

        elif choice == "2":
            print("Your plaintext is " + decode(input("Please enter your ciphertext: "), input("Please enter your key: ")))

        elif choice == "3":
            cont = False

        else:
            print("Please choose 1, 2, or 3")

main()

```

## Cryptography Principles and Syntax (2<sup>nd</sup> Week)

### Exercise 2.1

A private-key encryption scheme is defined by specifying a **message space  $M$**  ( $M$  defines the set of legal messages, i.e. those supported by the scheme) along with three algorithms.

- A procedure for generating keys (**Gen**)
- A procedure for encrypting (**Enc**)
- A procedure for decrypting (**Dec**)

The algorithms have the following functionality:

- The **key-generation algorithm (Gen)** is a probabilistic algorithm that outputs a key **k** chosen according to some distribution. The set of all possible keys output by **Gen** is called a **key space**, denoted by **K**.
- The **encryption algorithm (Enc)** takes as input a key **k** and a message **m** and outputs a ciphertext **c**. We denote by **Enc<sub>k</sub>(m)** the encryption of a plaintext **m** using the key **k**.
- The decryption algorithm (**Dec**) takes as input a key **k** and a ciphertext **c** and outputs a plaintext **m**. We denote **Dec<sub>k</sub>(c)** the decryption of a ciphertext **c** using a key **k**.

### Exercise 2.2

An encryption scheme must satisfy the following correctness requirement:

For every key **k** output by **Gen** and every message  $m \in M$ , it holds that

$$Dec_k(Enc_k(m)) = m$$

This is important because it guarantees that encryption and decryption of a message does not alter the original message, therefore the original message can be retrieved without alterations.

### Exercise 2.3

It is clear from the encryption methodology and the correctness requirement that if an eavesdropping adversary knows the algorithm of encryption and decryption as well as the key shared by the two communicating parties, then that adversary will be able to decrypt any ciphertexts transmitted by those parties. Perhaps they should keep the decryption algorithm secret.

In 1883 Auguste Kerckhoffs argued the opposite in a paper he wrote elucidating several design principles for military ciphers. One of the most important of these, now known simply as Kerckhoffs' principle, was "*The cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.*"

There are several arguments in favour of this principle, such as:

- a) It is significantly easier for the parties to maintain secrecy of a short key than to keep secret the (more complicated) algorithm they are using.
- b) In case the honest parties' shared, secret information is ever exposed, it will be much easier for them to change a key than to replace an encryption scheme.
- c) For large-scale deployment it is significantly easier for users to all rely on the same encryption algorithm/software (with different keys) than for everyone to use their own custom algorithm.

### Exercise 2.4

The **shift cipher** can be viewed as a variant of Caesar's cipher. Specifically, in the shift cipher the key  $k$  is a number between 0 and 25. Mapping this to the syntax of encryption described earlier, the message space consists of arbitrary length strings of English letters with punctuation, spaces (sometimes), and numerals removed, and with no distinction between upper and lower case. Algorithm **Gen** outputs a uniform key  $k \in \{0, \dots, 25\}$ . Algorithm **Enc** takes a key  $k$  and a plaintext and shifts each letter of the plaintext forward  $k$  positions (wrapping around at the end of the alphabet). Algorithm **Dec** takes a key  $k$  and a ciphertext and shifts every letter of the ciphertext backward  $k$  positions.

Is it possible to recover the message without knowing  $k$ ? Actually, it is trivial! The reason is that there are only 26 possible keys. So one can try to decrypt the ciphertext using every possible key and thereby obtain a list of 26 candidate plaintexts. The correct plaintext will certainly be on this list; moreover, if the ciphertext is “long enough” then the correct plaintext will likely be the only candidate on the list that “makes sense.” (The latter is not necessarily true, but will be true most of the time. Even when it is not, the attack narrows down the set of potential plaintexts to at most 26 possibilities.) By scanning the list of candidates it is easy to recover the original plaintext.

### Exercise 2.5

- a) There are only four ways this can occur:

- $M = a$  and  $K = 1$

- $M = b$  and  $K = 0$
- $M = c$  and  $K = 25$
- $M = d$  and  $K = 24$

By independence of **M** and **K**, we have

$$\begin{aligned} Pr[M = a \cap K = 1] &= Pr[M = a] \times Pr[K = 1] = 0.2 \times \frac{1}{26} \\ Pr[M = b \cap K = 0] &= Pr[M = b] \times Pr[K = 0] = 0.2 \times \frac{1}{26} \\ Pr[M = c \cap K = 25] &= Pr[M = c] \times Pr[K = 25] = 0.3 \times \frac{1}{26} \\ Pr[M = d \cap K = 24] &= Pr[M = d] \times Pr[K = 24] = 0.3 \times \frac{1}{26} \end{aligned}$$

Therefore

$$\begin{aligned} Pr[C = B] &= Pr[M = a \cap K = 1] + Pr[M = b \cap K = 0] + Pr[M = c \cap K = 25] \\ &\quad + Pr[M = d \cap K = 24] \\ &= 0.2 \times \frac{1}{26} + 0.2 \times \frac{1}{26} + 0.3 \times \frac{1}{26} + 0.3 \times \frac{1}{26} = \frac{1}{26} \end{aligned}$$

b) There are only four ways this can occur:

- $M = a$  and  $K = 2$
- $M = b$  and  $K = 1$
- $M = c$  and  $K = 0$
- $M = d$  and  $K = 25$

By independence of **M** and **K**, we have

$$\begin{aligned} Pr[M = a \cap K = 2] &= Pr[M = a] \times Pr[K = 2] = 0.2 \times \frac{1}{26} \\ Pr[M = b \cap K = 1] &= Pr[M = b] \times Pr[K = 1] = 0.2 \times \frac{1}{26} \\ Pr[M = c \cap K = 0] &= Pr[M = c] \times Pr[K = 0] = 0.3 \times \frac{1}{26} \\ Pr[M = d \cap K = 25] &= Pr[M = d] \times Pr[K = 25] = 0.3 \times \frac{1}{26} \end{aligned}$$

Therefore

$$\begin{aligned} Pr[C = B] &= Pr[M = a \cap K = 2] + Pr[M = b \cap K = 1] + Pr[M = c \cap K = 0] \\ &\quad + Pr[M = d \cap K = 25] \\ &= 0.2 \times \frac{1}{26} + 0.2 \times \frac{1}{26} \end{aligned}$$
26

$$\begin{array}{r} + 0.3x^1 \\ 26 \quad \underline{-} \\ = \end{array} \quad \begin{array}{r} - \\ - \\ - \end{array}$$
$$\begin{array}{r} 2 \\ 6 \end{array}$$

### **Exercise 2.6**

Vigenère cipher works by replacing each letter by another letter a specified number of positions further in the alphabet. For example J is 5 positions further than E. D is 5 positions after Y. (Y,Z,A,B,C,D)

The key is a sequence of shift amounts. If the sequence is of length 10, the 1st, 11th, 21st ...letters of the plaintext are processed using the first member of the key. The second member of the key processes plaintext letters 2, 12, 22, ...and so forth.

In one time pad a long key-sequence makes this approach more difficult, since we have fewer rows. The extreme case is that in which the key-sequence is as long as the plaintext itself. This leads to a theoretically unbreakable cipher. For any possible plaintext, there is a key for which the given ciphertext comes from that plaintext.

This type of cipher has reportedly been used by spies, who were furnished with notebooks containing page after page of randomly generated key-sequence. Notice that it is essential that each key-sequence be used only once (hence the name of the system). Otherwise the approach for Vigenère systems described above could be tried, since we would have at least two rows to work with.

One-time pads seem practical in situations where one agent is communicating with a central command. They become less attractive if several agents may need to communicate with each other.

## **Computational Security (3<sup>rd</sup> Week)**

### **Exercise 3.1**

Perfect Secrecy

$$Pr[M = m | C = c] = Pr[M = m]$$

In the shift cipher

$$Pr[C = c] = \sum_{k \in \mathbb{Z}_{26}} Pr[K = k] \cdot Pr[M = Dec_k(c)]$$

We know that

$$Pr[K = k] = \frac{1}{26}$$

and

$$Pr[M = Dec_k(C)] = Pr[M = c - k]$$

Therefore,

$$\begin{aligned} Pr[C = c] &= \sum_{k \in Z_{26}} \frac{1}{26} \cdot Pr[M = c - k] \\ &= \frac{1}{26} \sum_{k \in Z_{26}} Pr[M = c - k] \end{aligned}$$

We know that

$c - k$  gives the message  $m$ , therefore  $Pr[M = c - k]$  can become  $Pr[M = m]$

Therefore we can say that

$$\sum_{k \in Z_{26}} Pr[M = c - k] = \sum_{k \in Z_{26}} Pr[M = m] = 1$$

Substituting this in the equation gives,

$$Pr[C = c] = \frac{1}{26} \cdot 1$$

Therefore

$$Pr[C = c] = \frac{1}{26}$$

We also have that

$$Pr[C = c | M = m] = Pr[K = (c - m) \bmod 26] = \frac{1}{26}$$

Using Bayes' theorem we have

$$\begin{aligned} Pr[M = m] \cdot Pr[C = c | M = m] &= Pr[M = m] \cdot \frac{1}{26} \\ Pr[M = m | C = c] &= \frac{Pr[C = c]}{Pr[C = c]} = \frac{\frac{1}{26}}{\frac{1}{26}} = Pr[M = m] \end{aligned}$$

### Exercise 3.2

There are several ways to solve it. Since in lecture 6 we are going to see that one-time pad uses XOR, let solve this question using the actual way one-time pad works.

First of all, let's correctly define One-Time Pad encryption scheme

Fix an integer  $l > 0$ . The message space  $M$ , key space  $K$ , and ciphertext space  $C$  are all equal to  $\{0,1\}^l$  (the set of all binary strings of length  $l$ ).

- Gen: the key-generation algorithm chooses a key from  $K = \{0,1\}^l$  according to the uniform distribution (i.e., each of the  $2^l$  strings in the space is chosen as the key with probability exactly  $2^{-l}$ ).
- Enc: given a key  $K \in \{0,1\}^l$  and a message  $m \in \{0,1\}^l$ , the encryption algorithm outputs the ciphertext  $c \in K \oplus m$ .
- Dec: given a key  $K \in \{0,1\}^l$  and a ciphertext  $c \in \{0,1\}^l$ , the decryption algorithm outputs the message  $m \in K \oplus c$ .

Using the definition above, we can proof one-time pad perfect secrecy.

We first compute  $Pr[C = c|M = m']$  for arbitrary  $c \in C$  and  $m' \in M$ . For the one-time pad,

$$\begin{aligned} Pr[C = c|M = m'] &= Pr[Enc_K(m') = c] = Pr[m' \oplus K = c] \\ &= Pr[K = m' \oplus c] \\ &= 2^{-l} \end{aligned}$$

Where the final equality holds because the key  $K$  is a uniform  $l$ -bit string. Fix any distribution over  $M$ . For any  $c \in C$ , we have

$$\begin{aligned} Pr[C = c] &= \sum_{m' \in M} Pr[C = c|M = m'] \cdot Pr[M = m'] \\ &= 2^{-l} \cdot \sum_{m' \in M} Pr[M = m'] \\ &= 2^{-l} \end{aligned}$$

Where the sum is over  $m' \in M$  with  $Pr[M = m'] \neq 0$ . Bayes' Theorem gives:

$$Pr[M = m | C = c] = \frac{Pr[C = c|M = m] \cdot Pr[M = m]}{Pr[C = c]} = \frac{2^{-l} \cdot Pr[M = m]}{2^{-l}} = Pr[M = m]$$

### Exercise 3.3

$2^{60}$  CPU cycles are required. If we have a desktop computer with a 4 GHz processor (that executes  $4 \times 10^9$  cycles per second)  $2^{60}$  CPU cycles require  $\frac{2^{60}}{4 \times 10^9}$  seconds, or about 9 years.

### Exercise 3.4

**Polynomial time** is the time required for a computer to solve a problem, where this time is a simple polynomial function of the size of the input. An algorithm is said to be solvable in polynomial time if the number of steps required to complete the algorithm for a given input is  $O(n^k)$  for some nonnegative integer  $k$ , where  $n$  is the complexity of the input.

Polynomial-time algorithms are said to be "fast." Most familiar mathematical operations such as addition, subtraction, multiplication, and division, as well as computing square roots, powers, and logarithms, can be performed in polynomial time.

A **probabilistic polynomial time algorithm** is an algorithm that runs in polynomial time and may use (true) randomness to produce (possibly) non-deterministic results.

The "probabilistic" in the name comes from the fact that one can only predict certain outcomes with a certain probability. For example an algorithm that takes no input and simulates a coin-flip, would be such a probabilistic algorithm, as it's not sure (before evaluation) what the outcome will be, either head or tail?

### Exercise 3.5

This approach, rooted in complexity theory, introduces an integer-valued security parameter (denoted by  $n$ ) that parameterizes both cryptographic schemes as well as all involved parties.

When honest parties initialize a scheme (i.e., when they generate keys), they choose some value  $n$  for the security parameter.

The security parameter is assumed to be known to any adversary attacking the scheme, and we now view the running time of the adversary, as well as its success probability, as functions of the security parameter rather than as concrete numbers.

We equate "efficient adversaries" with randomized (i.e., probabilistic) algorithms running in time **polynomial in  $n$** . This means there is some polynomial  $p$  such that the adversary runs for time at most  $p(n)$  when the security parameter is  $n$ .

We also require, for real-world efficiency, that honest parties run in polynomial time, although we stress that the adversary may be much more powerful (and run much longer than) the honest parties.

We equate the notion of "small probabilities of success" with success probabilities smaller than any inverse polynomial in  $n$ . Such probabilities are called negligible.

**A scheme is secure if any Probabilistic Polynomial Time (PPT) adversary succeeds in breaking the scheme with at most negligible probability.**

Say we have a scheme that is asymptotically secure. Then it may be the case that an adversary running for  $n^3$  minutes can succeed in “breaking the scheme” with probability  $2^{40} \cdot 2^{-n}$  (which is a negligible function of  $n$ ).

When  $n \leq 40$  this means that an adversary running for  $40^3$  minutes (about 6 weeks) can break the scheme with probability 1, so such values of  $n$  are not very useful.

Even for  $n = 50$  an adversary running for  $50^3$  minutes (about 3 months) can break the scheme with probability roughly  $1/1000$ , which may not be acceptable.

On the other hand, when  $n = 500$  an adversary running for 200 years breaks the scheme only with probability roughly  $2^{-500}$ .

### Exercise 3.6

We consider randomized algorithms by default for two reasons.

- A. Randomness is essential to cryptography and so honest parties must be probabilistic; given this, it is natural to allow adversaries to be probabilistic as well.
- B. Randomization is practical and gives attackers additional power. Since our goal is to model all realistic attacks, we prefer a more liberal definition of efficient computation.

## Pseudorandom Generators & Stream Ciphers (4<sup>th</sup> Week)

### Exercise 4.1

A pseudorandom generator  $G$  is an efficient, deterministic algorithm for transforming a short, uniform string called the seed into a longer, “uniform looking” (or “pseudorandom”) output string. Stated differently, a pseudorandom generator uses a small amount of true randomness in order to generate a large amount of pseudorandomness. This is useful whenever a large number of random (looking) bits are needed, since generating true random bits is difficult and slow. Indeed, pseudorandom generators have been studied since at least the 1940s when they were proposed for running statistical simulations. In that context, researchers proposed various statistical tests that a pseudorandom generator should pass in order to be considered “good.”

The seed  $s$  for a pseudorandom generator is analogous to the cryptographic key used by an encryption scheme, and the seed must be chosen uniformly and be kept secret from any

adversary. Another important point, is that  $s$  must be long enough so that it is not feasible to enumerate all possible seeds. In an asymptotic sense this is taken care of by setting the length of the seed equal to the security parameter, so that exhaustive search over all possible seeds requires exponential time. In practice, the seed must be long enough so that it is impossible to try all possible seeds within some specified time bound.

### **Exercise 4.2**

A (true) random generator requires a naturally occurring source of randomness. Designing a hardware device or software program to exploit this randomness and produce a bit sequence that is free of biases and correlations is a difficult task. Additionally, for most cryptographic applications, the generator must not be subject to observation or manipulation by an adversary. Hardware-based random generators exploit the randomness which occurs in some physical phenomena. Such physical processes may produce bits that are biased or correlated, in which case they should be subjected to de-skewing techniques discussed later on. Examples of such physical phenomena include:

1. elapsed time between emission of particles during radioactive decay
2. thermal noise from a semiconductor diode or resistor
3. the frequency instability of a free running oscillator
4. the amount a metal insulator semiconductor capacitor is charged during a fixed period of time
5. air turbulence within a sealed disk drive which causes random fluctuations in disk drive sector read latency times
6. sound from a microphone or video input from a camera

Designing a random generator in software is even more difficult than doing so in hardware. Processes upon which software random bit generators may be based include:

1. the system clock;
2. elapsed time between keystrokes or mouse movement;
3. content of input/output buffers;
4. user input
5. operating system values such as system load and network statistics

The behaviour of such processes can vary considerably depending on various factors, such as the computer platform. It may also be difficult to prevent an adversary from observing or manipulating these processes. A natural source of random bits may be defective in that the output bits may be:

1. Biased - the probability of the source emitting a 1 is not equal to  $\frac{1}{2}$
2. Correlated - the probability of the source emitting a 1 depends on previous bits emitted

There are various techniques for generating truly random bit sequences from the output bits of such a defective generator; such techniques are called de-skewing techniques.

### **Exercise 4.3**

Briefly explain the two types of stream ciphers.

Stream ciphers are an important class of encryption algorithms. They encrypt **individual** characters (usually binary digits) of a plaintext message one at a time, using an encryption transformation which varies with time. By contrast, block ciphers (discussed later) tend to simultaneously encrypt **groups** of characters of a plaintext message using a fixed encryption transformation. Stream ciphers are generally faster than block ciphers in hardware, and have less complex hardware circuitry. They are also more appropriate, and in some cases mandatory, when buffering is limited or when characters must be individually processed as they are received. Because they have limited or no error propagation, stream ciphers may also be advantageous in situations where transmission errors are highly probable.

There are plenty of Stream Cipher types. In this course we will discuss the following:

1. **Synchronous** Stream Ciphers
2. **Self-synchronizing** Stream Ciphers

#### **Synchronous Stream Ciphers**

A synchronous stream cipher is one in which the keystream is generated independently of the plaintext message and of the ciphertext.

#### **Self-Synchronizing Stream Ciphers**

A self-synchronizing or asynchronous stream cipher is one in which the keystream is generated as a function of the key and a fixed number of previous ciphertext digits.

#### Exercise 4.4

Properties of Synchronous Stream Ciphers:

1. **Synchronization Requirements** - In a synchronous stream cipher, both the sender and receiver must be synchronized, using the same key and operating at the same position (state) within that key, to allow for proper decryption.
2. **No Error Propagation** - A ciphertext digit that is modified (but not deleted) during transmission does not affect the decryption of other ciphertext digits.
3. **Active Attacks** - As a consequence of property (1), the insertion, deletion, or replay of ciphertext digits by an active adversary causes immediate loss of synchronization, and hence might possibly be detected by the decryptor. As a consequence of property (2), an active adversary might possibly be able to make changes to selected ciphertext digits, and know exactly what effect these changes have on the plaintext.

Properties of self-synchronizing Stream Ciphers:

1. **Self-Synchronization** - is possible if ciphertext digits are deleted or inserted, because the decryption mapping depends only on a fixed number of preceding ciphertext characters.
2. **Limited Error Propagation** - Suppose that the state of a self-synchronization stream cipher depends on  $t$  previous ciphertext digits. If a single ciphertext digit is modified (or even deleted or inserted) during transmission, then decryption of up to  $t$  subsequent ciphertext digits may be incorrect, after which correct decryption resumes.
3. **Active Attacks** - Property (2) implies that any modification of ciphertext digits by an active adversary causes several other ciphertext digits to be decrypted incorrectly, thereby improving (compared to synchronous stream ciphers) the likelihood of being detected by the decryptor. As a consequence of property (1), it is more difficult (than for synchronous stream ciphers) to detect insertion, deletion, or replay of ciphertext digits by an active adversary.
4. **Diffusion of Plaintext Statistics** - Since each plaintext digit influences the entire following ciphertext, the statistical properties of the plaintext are dispersed through the ciphertext. Hence, self-synchronizing stream ciphers may be more resistant than synchronous stream ciphers against attacks based on plaintext redundancy.

## Block Ciphers (5<sup>th</sup> Week)

### Exercise 5.1

A block cipher is a function which maps **n-bit plaintext blocks** to **n-bit ciphertext blocks**;  $n$  is called the **blocklength**. It may be viewed as a simple substitution cipher with large character size. The function is parameterized by a  $k$ -bit key  $K$ , taking values from a subset  $K$  (the key space) of the set of all  $k$ -bit vectors  $V_k$ . It is generally assumed that the key is chosen at random. Use of plaintext and ciphertext blocks of equal size avoids data expansion. To allow unique decryption, the encryption function must be one-to-one (i.e., invertible). For **n-bit** plaintext and ciphertext blocks and a fixed key, the encryption function is a bijection, defining a permutation on  $n$ -bit vectors. Each key potentially defines a different bijection. The number of keys is  $|K|$ , and the effective key size is  $\log_{10} |K|$ . This equals the key length if all  $k$ -bit vectors are valid keys ( $K = V_k$ ).

If keys are equiprobable and each defines a different bijection, the entropy of the key space is also  $\log_{10} |K|$ . Block ciphers can be either symmetric-key or public-key.

### Exercise 5.2

The unicity distance of a cipher is the minimum amount of ciphertext (i.e. the number of characters) required to allow a computationally unlimited adversary to recover the unique encryption key. It is a theoretical measure usually used to find if a cipher is perfectly secret or computationally secure. However, that does not mean that a small unicity distance cipher is insecure in practice.

### Exercise 5.3

Many criteria can be used to evaluate block ciphers, including:

1. **Estimated Security Level** – confidence in the security of a cipher grows if it has been subjected to (and withstood) expert cryptanalysis over a substantial time period. The amount of ciphertext required to mount practical attacks often vastly exceeds a cipher's unicity distance, which provides a theoretical estimate of the amount of ciphertext required to recover the unique encryption key
2. **Key Size** – the effective bit-length of the key, defines an upper bound on the security of a cipher. Typically, longer keys impose additional costs (i.e. generation, transmission, storage etc.)

3. **Throughput** – the data transfer in either hardware or software. It is related to the complexity of the cryptographic mapping and the degree to which the mapping is tailored to a particular implementation medium or platform
4. **Block Size** – it impacts both security and complexity as well as it affects the performance
5. **Complexity of Cryptographic Mapping** – algorithmic complexity affects the implementation costs both in terms of development and fixed sources as well as real-time performance for fixed sources (throughput). That is why sometimes hardware is preferred instead of software
6. **Data Expansion** – it is desirable and often mandatory that the encryption scheme does not increase the size of plaintext data
7. **Error Propagation** – decryption of ciphertext containing bit errors may result in various effects on the recovered plaintext, including propagation of errors to subsequent plaintext blocks

#### **Exercise 5.4**

To evaluate block cipher security, it is customary to always assume that an adversary:

1. has access to all data transmitted over the ciphertext channel
2. knows all the details of the encryption function except the secret key (Kerckhoffs' principle)

Under standard assumptions, attacks are classified based on what information a cryptanalyst has access to in addition to intercepted ciphertext. The most prominent classes of attack for symmetric-key ciphers are (for a fixed key):

1. ciphertext-only – no additional information is available
2. known-plaintext – plaintext-ciphertext pairs are available.
3. chosen-plaintext – ciphertexts are available corresponding to plaintexts of the adversary's choice. A variation is an adaptive chosen-plaintext attack, where the choice of plaintexts may depend on previous plaintext-ciphertext pairs.

**Ciphertext-Only Attack (COA)** is an attack model where the attacker is assumed to have access only to a set of ciphertexts. In practise, the attacker might have some knowledge of the plaintext. For example, the attacker might know the language in which the plaintext is written or the expected statistical distribution of characters in the plaintext.

**Known-Plaintext Attack (KPA)** is an attack model where the attacker has access to both the plaintext, and the ciphertext. This can be used to reveal further secret information such as secret keys.

**Chosen-Plaintext Attack (CPA)** is an attack model which presumes that the attacker can obtain the ciphertexts for arbitrary plaintexts. The goal of the attack is to gain information that reduces the security of the encryption scheme. Modern ciphers aim to provide semantic security, also known as **ciphertext indistinguishability** under chosen-plaintext attack, and are therefore by design generally immune to chosen-plaintext attacks if correctly implemented. It is customary to use ciphers **resistant** to chosen-plaintext attack even when mounting such an attack is not feasible. A cipher secure against chosen-plaintext attack is secure against known-plaintext and ciphertext-only attacks.

A **Chosen-Ciphertext Attack (CCA)** operates under the following model, an adversary is allowed to plaintext-ciphertext pairs for some number of ciphertexts of his choice, and thereafter attempts to use this information to recover the key.

In a **Related-Key Attack**, an adversary is assumed to have access to the encryption of plaintexts under both an unknown key and unknown keys chosen to have or known to have certain relationships with the key.

### Exercise 5.5

The block ciphers have several modes of operation, with the most common ones being:

1. Electronic Codebook (ECB)
2. Cipher-Block Chaining (CBC)
3. Cipher Feedback (CFB)
4. Output Feedback (OFB)

### Electronic Codebook (ECB) Properties

1. **Identical plaintext** blocks (under the same key) result in identical ciphertext.
2. **Chaining dependencies** - blocks are enciphered independently of other blocks.  
Reordering ciphertext blocks results in correspondingly re-ordered plaintext blocks.
3. **Error propagation** - one or more bit errors in a single ciphertext block affect decipherment of that block only. For typical ciphers, decryption of such a block is then random (with about 50% of the recovered plaintext bits in error).

## Cipher Block-Chaining (CBC) Properties

1. **Identical plaintexts** - identical ciphertext blocks result when the same plaintext is enciphered under the same key and **IV** (n-bit initialization vector). Changing the IV, key, or first plaintext block results in different ciphertext.
2. **Chaining dependencies** - the chaining mechanism causes ciphertext  $c_j$  to depend on  $x_j$  and all preceding plaintext blocks. Consequently, rearranging the order of ciphertext blocks affects decryption. Proper decryption of a correct ciphertext block requires a correct preceding ciphertext block.
3. **Error propagation** - a single bit error in ciphertext block  $c_j$  affects decipherment of blocks  $c_j$  and  $c_{j+1}$ . Block  $m_j$  recovered from  $c_j$  is typically totally random (50% in error), while the recovered plaintext  $m_{j+1}$  has bit errors precisely where  $c_j$  did. Thus an adversary may cause predictable bit changes in  $m_{j+1}$  by altering corresponding bits of  $c_j$ .
4. **Error recovery** - the CBC mode is *self-synchronizing* in the sense that if an error (including loss of one or more entire blocks) occurs in block  $c_j$  but not  $c_{j+1}, c_{j+2}$  is correctly decrypted to  $m_{j+2}$

## Cipher Feedback (CFB) Properties

1. **Identical plaintexts** - as per CBC encryption, changing the **IV** results in the same plaintext input being enciphered to a different output. The IV need not be secret.
2. **Chaining dependencies** - similar to CBC encryption, the chaining mechanism causes ciphertext block  $c_j$  to depend on both  $m_j$  and preceding plaintext blocks; consequently, re-ordering ciphertext blocks affects decryption.
3. **Error propagation** - one or more bit errors in any single r-bit ciphertext block  $c_j$  affects the decipherment of that and the next  $\frac{r}{r}l$  ciphertext blocks. The recovered plaintext  $m_j$  will differ from original  $m_j$  precisely in the bit positions  $c_j$  was in error. Thus an adversary may cause predictable bit changes in  $m_j$  by altering corresponding bits of  $c_j$ .
4. **Error recovery** - the CFB mode is self-synchronizing similar to CBC, but requires  $\frac{r}{r}l$  ciphertext blocks to recover.
5. **Throughput** - for  $r < n$ , throughput is decreased by a factor of  $\frac{n}{r}$  in that each execution of Enc yields only  $r$  bits of ciphertext output.

## Output Feedback (OFB) Properties

1. **Identical plaintexts** - as per CBC and CFB modes, changing the **IV** results in the same plaintext being enciphered to a different output.
2. **Chaining dependencies** - the keystream is plaintext-independent.
3. **Error propagation** - one or more bit errors in any ciphertext character  $c_j$  affects the decipherment of only that character, in the precise bit position(s)  $c_j$  is in error, causing the corresponding recovered plaintext bit(s) to be complemented.
4. **Error recovery** - the OFB mode recovers from ciphertext bit errors, but cannot self-synchronize after loss of ciphertext bits, which destroys alignment of the decrypting keystream.

**Throughput** - for  $r < n$ , throughput is decreased as per the CFB mode. However, in all cases, since the keystream is independent of plaintext or ciphertext, it may be pre-computed.

### Exercise 5.7

Most symmetric algorithms use either a block cipher or a stream cipher. They are both symmetric, so they both use the same key to encrypt or decrypt data. However, they divide data in different ways.

A block cipher encrypts data in specific-sized blocks, such as 64-bit blocks or 128-bit blocks. The block cipher divides large files or messages into these blocks and then encrypts each individual block separately. Stream ciphers encrypt data as a stream of bits or bytes rather than dividing it into blocks.

In general, stream ciphers are more efficient than block ciphers when the size of the data is unknown or sent in a continuous stream, such as when streaming audio and video over a network. Block ciphers are more efficient when the size of the data is known, such as when encrypting a file or a specific-sized database field.

An important principle when using a stream cipher is that encryption keys should never be reused. If a key is reused, it is easier to crack the encryption.

## Data Encryption Standard - DES (6<sup>th</sup> Week)

### Exercise 6.1

The design of DES is related to two general concepts: product ciphers and Feistel ciphers. Each involves iterating a common sequence or round of operations.

A **Product cipher** combines two or more transformations in a manner intending that the resulting cipher is more secure than the individual components.

Combines a sequence of simple transformations such as substitution (S-box), permutation (P-box), and modular arithmetic.

A **permutation box** (or **P-box**) is a method of bit-shuffling used to permute or transpose bits across S-boxes inputs, retaining diffusion while transposing.

A **substitution box** (or **S-box**) takes some number of input bits, **m**, and transforms them into some number of output bits, **n**, where **n** is not necessarily equal to **m**.

A **Feistel cipher** is an iterated cipher mapping a  $2t$ -bit plaintext  $(L_0, R_0)$ , for  $t$ -bit blocks  $L_0$  and  $R_0$ , to a ciphertext  $(R_r, L_r)$ , through an  $r$ -round process where  $r \geq 1$ .

Let  $F$  be the round function and let  $K_0, K_1, \dots, K_n$  be the sub-keys for the rounds  $0, 1, \dots, n$  respectively.

### Exercise 6.2

A **permutation box** (or **P-box**) is a method of bit-shuffling used to permute or transpose bits across S-boxes inputs, retaining diffusion while transposing.

A **substitution box** (or **S-box**) takes some number of input bits, **m**, and transforms them into some number of output bits, **n**, where **n** is not necessarily equal to **m**.

## Message Authentication Code - MAC (7<sup>th</sup> Week)

### Exercise 7.1

In many cases, it is of equal or greater importance to **guarantee message integrity** (or **message authentication**) in the sense that each party should be able to identify when a message it receives was sent by the party claiming to send it, and was not modified in transit.

Consider the case of a user communicating with their bank over the Internet. When the bank receives a request to transfer \$1,000 from the user's account to the account of some other user X, the bank has to consider the following:

1. Is the request authentic? That is, did the user in question really issue this request, or was the request issued by an adversary (perhaps X itself) who is impersonating the legitimate user?
2. Assuming a transfer request was issued by the legitimate user, are the details of the request as received exactly those intended by the legitimate user? Or was, e.g., the transfer amount modified?

### Exercise 7.2

As an example, consider the case of a user encrypting some amount of money he wants to transfer from his bank account, where the amount is represented in binary. Flipping the least significant bit has the effect of changing this amount by only €1, but flipping the 11th least significant bit changes the amount by more than €1,000!

Interestingly, the adversary in this example does not necessarily learn whether it is increasing or decreasing the initial amount, i.e., whether it is flipping a 0 to a 1 or vice versa. But if the adversary has some partial knowledge about the amount—say, that it is less than €1,000 to begin with—then the modifications it introduces can have a predictable effect. We stress that this attack does not contradict the secrecy of the encryption scheme.

### Exercise 7.3

The aim of a message authentication code is to prevent an adversary from modifying a message sent by one party to another, or from injecting a new message, without the receiver detecting that the message did not originate from the intended party.

As in the case of encryption, this is only possible if the communicating parties share some secret that the adversary does not know (otherwise nothing can prevent an adversary from impersonating the party sending the message).

### Exercise 7.4

A message authentication code (MAC) consists of three probabilistic polynomial-time algorithms ( $\text{Gen}$ ,  $\text{Mac}$ ,  $\text{Vrfy}$ ) such that:

1. The key-generation algorithm  $\text{Gen}$  takes as input the security parameter  $1^n$  and outputs a key  $k$  with  $|k| \geq n$
2. The tag-generation algorithm  $\text{Mac}$  takes as input a key  $k$  and a message  $m$ , and outputs a tag  $t$ . Since the algorithm may be randomized, we write this as  $t \leftarrow \text{Mac}_k(m)$

3. The deterministic verification algorithm  $Vrfy$  takes as input a key  $k$ , a message  $m$  and a tag  $t$ . It outputs a bit  $b$ , with  $b = 1$  meaning valid and  $b = 0$  meaning invalid. We write this as

$$b \triangleq Vrfy_k(m, t)$$

Note: It is required that for every  $n$ , every key  $k$  output by  $Gen(1^n)$ , and every  $m$ , it holds that  $Vrfy_k(m, Mac_k(m)) = 1$

## Hash Functions (8<sup>th</sup> Week)

### Exercise 8.1

At the most basic level, a hash function provides a way to map a long input string to a shorter output string sometimes called a **digest**. The primary requirement is to avoid collisions, or two inputs that map to the same digest. Collision-resistant hash functions have numerous uses. One example is HMAC, achieving domain extension for message authentication codes. Beyond that, hash functions have become ubiquitous in cryptography, and they are often used in scenarios that require properties much stronger than collision resistance.

It has become common to model cryptographic hash functions as being “completely unpredictable”. Hash functions are intriguing in that they can be viewed as lying between the worlds of private and public-key cryptography.

### Exercise 8.2

Hash functions may be split into two classes:

1. **Unkeyed hash functions**: whose specification dictates a single input parameter (a message)
2. **Keyed hash functions**: whose specification dictates two distinct inputs, a message and a secret key

### Exercise 8.3

Of the numerous categories in such a *functional classification*, two types of hash functions will be discussed in this course:

1. **Modification Detection Codes** (MDCs), also known as **manipulation detection codes**, and less commonly as **message integrity codes** (MICs), the purpose of an MDC is to

provide a representative image or *hash* of a message. The end goal is to facilitate, in conjunction with additional mechanisms, data integrity assurances as required by specific applications. MDCs are a subclass of *unkeyed* hash functions, and themselves may be further classified as:

- i. *one-way hash functions (OWHFs)*: for these, finding an input which hashes to a pre-specified hash-value is difficult
  - ii. *collision resistant hash functions (CRHFs)*: for these, finding any two inputs having the same hash-value is difficult.
2. **Message Authentication Codes** (MACs), the purpose of a MAC is (informally) to facilitate, without the use of any additional mechanisms, assurances regarding both the source of a message and its integrity (See Lecture 7). MACs have two functionally distinct parameters, a message input and a secret key; they are a subclass of *keyed* hash functions.

#### Exercise 8.4

**Collision-resistant** hash functions are similar in spirit. Again, the goal is to avoid collisions. However, there are fundamental differences. For one, the desire to minimize collisions in the setting of data structures becomes a requirement to avoid collisions in the setting of cryptography. Furthermore, in the context of data structures we can assume that the set of data elements is chosen independently of the hash function and without any intention to cause collisions. In the context of cryptography, in contrast, we are faced with an adversary who may select elements with the explicit goal of causing collisions. This means that collision-resistant hash functions are much harder to design.

Informally, a function  $H$  is **collision resistant** if it is infeasible for any probabilistic polynomial-time algorithm to find a collision in  $H$ . We will only be interested in hash functions whose domain is larger than their range. In this case collisions must exist, but such collisions should be hard to find. Formally, we consider **keyed hash functions**. That is,  $H$  is a two-input function that takes as input a key  $s$  and a string  $x$ , and outputs a string  $H^s(x) \triangleq H(s, x)$ . The requirement is that it must be hard to find a collision in  $H^s$  for a randomly generated key  $s$ . There are at least two differences between keys in this context and keys as we have used them until now:

1. Not all strings necessarily correspond to valid keys (i.e.,  $H^s$  may not be defined for certain  $s$ ), and therefore the key  $s$  will typically be generated by an algorithm **Gen** rather than being chosen uniformly.

2. More importantly, this key  $\mathbf{s}$  is (generally) not kept secret, and collision resistance is required even when the adversary is given  $\mathbf{s}$ . In order to emphasize this, we superscript the key and write  $H^s$  rather than  $H_s$ .

**Preimage resistance**: for essentially all pre-specified outputs, it is computationally infeasible to find any input which hashes to that output, i.e., to find any preimage  $x'$  such that  $h(x') = y$  when given any  $y$  for which a corresponding input is not known. (one-way)

**2nd-preimage resistance**: it is computationally infeasible to find any second input which has the same output as any specified input, i.e., given  $x$ , to find a 2nd-preimage  $x' \neq x$  such that  $h(x) = h(x')$ .

## Number Theory and Cryptography (9<sup>th</sup> Week)

### Exercise 9.1

The **greatest common divisor** of two integers  $a, b$  written as  $gcd(a, b)$ , is the largest integer  $c$  such that  $c/a$  and  $c/b$ . (Note:  $gcd(a, b) = gcd(|a|, |b|)$  and  $gcd(b, 0) = gcd(0, b) = b$ )

If  $p$  is prime, then  $gcd(a, p)$  is either equal to 1 or  $p$ . If  $gcd(a, b) = 1$  then  $a$  and  $b$  are **relatively prime**.

Formally, let  $a, b$  be positive integers. Then there exists integers  $X, Y$  such that  $Xa + Yb = gcd(a, b)$ . Furthermore,  $gcd(a, b)$  is the smallest positive integer that can be expressed in this way.

If  $c|ab$  and  $gcd(a, c) = 1$  then  $c|b$ . Thus, if  $p$  is prime and  $p|ab$  then either  $p|a$  or  $p|b$ .

If  $a|N$ ,  $b|N$  and  $gcd(a, b) = 1$  then  $ab|N$ .

### Exercise 9.2

Let  $a, b, N \in \mathbb{Z}$  with  $N > 1$ . We use the notion  $a \bmod N$  to denote the remainder of  $a$  upon division by  $N$ . In detail, there exist unique  $q, r$  with  $a = qN + r$  and  $0 \leq r < N$ , and we define  $a \bmod N$  to be equal to this  $r$ . We say that  $a$  and  $b$  are **congruent modulo  $N$** , written  $a \equiv b \pmod{N}$ , if  $a \bmod N = b \bmod N$ . (i.e. the remainder when  $a$  is divided by  $N$  is the same as the remainder when  $b$  is divided by  $N$ )

Congruence modulo  $N$  is an equivalent relation. i.e. it is reflexive ( $a = a \text{ mod } N$  for all  $a$ ), symmetric ( $a = b \text{ mod } N$  implies  $b = a \text{ mod } N$ ) and transitive (if  $a = b \text{ mod } N$  and  $b = c \text{ mod } N$ , then  $a = c \text{ mod } N$ )

Congruence modulo  $N$  obeys the standard rules of arithmetic with respect to addition, subtraction and multiplication, for example if  $a = a^r \text{ mod } N$  and  $b = b^r \text{ mod } N$  then  $(a + b) = (a^r + b^r) \text{ mod } N$  and  $ab = a^r b^r \text{ mod } N$

Congruence modulo  $N$  does not (in general) respect division. That is, if  $a = a^r \text{ mod } N$  and  $b = b^r \text{ mod } N$  then it is not necessarily true that  $\frac{a}{b} = \frac{a^r}{b^r} \text{ mod } N$ .

In fact, the expression  $\frac{a}{b} \text{ mod } N$  is not always well-defined. As a specific example that often causes confusion,  $ab = cb \text{ mod } N$  does not necessarily imply that  $a = c \text{ mod } N$ .

In certain cases, however, we can define a meaningful notion of division. If for a given integer  $b$  there exists an integer  $c$  such that  $bc = 1 \text{ mod } N$ , we say that  $b$  is **invertible modulo  $N$**  and call  $c$  a (multiplicative) inverse of  $b$  **modulo  $N$** . Clearly, 0 is never invertible.

### Exercise 9.3

A group is a set  $C$  along with a binary operation  $\circ$  for which the following conditions hold:

- **Closure:** For all  $g, h \in C$ ,  $g \circ h \in C$
- **Existence of an identity:** There exists an identity  $e \in C$  such that for all  $g \in C$ ,  $e \circ gg = g \circ e = g$
- **Existence of inverses:** For all  $g \in C$  there exists an element  $h \in C$  such that  $g \circ h = eh \circ g$ . Such an  $h$  is called an inverse of  $g$
- **Associativity:** For all  $g_1, g_2, g_3 \in C$ ,  $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$

When  $C$  has a finite number of elements, we say  $C$  is finite and let  $|C|$  denote the order of the group (that is, the number of elements in  $C$ ). A group  $C$  with operation  $\circ$  is **abelian** if the following holds:

- **Commutativity:** For all  $g, h \in C$ ,  $g \circ h = h \circ g$

### Exercise 9.4

We formalise something called “**cancellation law**” for groups. Let  $C$  be a group and  $a, b, c \in C$ . If  $ac = bc$ , then  $a = b$ . In particular, if  $ac = c$  then  $a$  is the identity in  $C$ . It is often useful to be able to describe the group operation applied  $m$  times to a fixed element  $g$ , where  $m$  is a positive integer. When using additive notation, we express this as  $m \cdot g$  or  $mg$ ; that is

$$mg = m \cdot g \stackrel{m \text{ times}}{\underbrace{+ \dots + g}}$$

### Exercise 9.5

Two groups are isomorphic if they have the same underlying structure. From a mathematical point of view, an isomorphism of a group  $C$  provides an alternate, but equivalent, way of thinking about  $C$ . From a computational perspective, an isomorphism provides a different way to represent elements in  $C$ , which can often have a significant impact on algorithmic efficiency.

Let  $C, IH$  be groups with respect to the operations  $\circ_C, \circ_{IH}$  respectively. A function  $f: C \rightarrow IH$  is an isomorphism from  $C$  to  $IH$  if:

1.  $f$  is a bijection
2. For all  $g_1, g_2 \in C$  we have  $f(g_1 \circ_C g_2) = f(g_1) \circ_{IH} f(g_2)$

If there exists an isomorphism from  $C$  to  $IH$  then we say that these groups are isomorphic and we write  $C \cong IH$ .

In essence, an isomorphism from  $C$  to  $IH$  is just a renaming of elements of  $C$  as elements of  $IH$ . (Note that if  $C$  is finite and  $C \cong IH$ , then  $IH$  must be finite and of the same size as  $C$ )

### Exercise 9.6

The Chinese remainder theorem shows that addition, multiplication, or exponentiation (which is just repeated multiplication) modulo  $N$  can be “transformed” to analogous operations modulo  $p$  and  $q$ .

One thing we have not yet discussed is how to convert back and forth between the representation of an element modulo  $N$  and its representation modulo  $p$  and  $q$ . The conversion can be carried out efficiently provided the factorization of  $N$  is known. Assuming  $p$  and  $q$  are known, it is easy to map an element  $x$  modulo  $N$  to its corresponding representation modulo  $p$  and  $q$ :

the element  $x$  corresponds to  $([x \bmod p], [x \bmod q])$ , and both the modular reductions can be carried out efficiently. For the other direction, we make use of the following observation:

an element with representation  $(x_p, x_q)$  can be written as

$$(x_p, x_q) = x_p \cdot (1, 0) + x_q \cdot (0, 1)$$

So, if we can find elements  $1_p, 1_q \in \{0, \dots, N - 1\}$  such that  $1_p \leftrightarrow (1, 0)$  and  $1_q \leftrightarrow (0, 1)$ , then (appealing to the Chinese remainder theorem) we know that

$$(x_p, x_q) \leftrightarrow [(x_p \cdot 1_p + x_q \cdot 1_q) \bmod N]$$

Since  $p, q$  are distinct primes,  $\gcd(p, q) = 1$ . We can use the extended Euclidean algorithm to find integers  $X, Y$  such that

$$X_p + Y_q = 1$$

## Key Management & Public-Key Cryptography (10<sup>th</sup> Week)

### Exercise 10.1

The biggest problem for all these schemes is how the honest parties will manage to share the secret private key in the first place. It is clear that such a key cannot be sent over public communication channels since we use encryption in the first place due to the fact that we do not trust public communication. It will be meaningless to send the key of our encryption through such a communication medium.

The honest parties might have access to a secure channel or they might be co-located for a short period of time at which they exchange keys. Using a secure channel may not be the best solution. Imagine what will happen in a large multinational company. Each pair of remote employees will have to use a secure channel or even visit the other employee in order to exchange keys. A better solution would be to use a trusted courier service as a secure channel.

Assuming these employees, denoted by  $N$ , find a way to share keys with each other. This will form another significant drawback. Each employee will have to manage and store  $N - 1$  secret keys. Not only that, but if it also needs a key for each server, database, etc. then the number of stored keys increases. In addition, all these keys must be stored securely. Imagine what will happen if one of those employee computers is infected by a virus or any other form of malicious software.

Even if we solve the problems mentioned above, we will still face problems with open systems. For example, consider using encryption to send credit-card information to an Internet merchant from whom you have not previously purchased anything. In such case, private-key cryptography alone is not a solution.

To summarize, there are at least three distinct problems related to the use of private-key cryptography.

- a. Key distribution
- b. Storing and managing large numbers of secret keys
- c. Inapplicability to open systems

### **Exercise 10.2**

To solve some of the problems mentioned above, is to use a key-distribution center (KDC) to establish shared keys. Reconsider the large multinational company example. Each employee may trust one entity that can act as a KDC. The KDC will then help all the employees share pairwise keys. When a new employee joins, the KDC can share a key with that employee (in person, in a secure location) as part of that employee's first day of work.

The KDC will also distribute shared keys between that employee and all existing employees. That is, when the  $i$ th employee joins, the KDC could generate  $i - 1$  keys  $k_1, \dots, k_{i-1}$ , give these keys to the new employee, and then send key  $k_i$  to the  $j$ th existing employee by encrypting it using the key that employee already shares with the KDC.

A much better approach, is to use KDC online to generate keys "on demand" whenever two employees wish to communicate securely. Let's say that KDC generates and shares key  $k_A$  with Alice, and  $k_B$  with Bob. When Alice wants to communicate with Bob, she can send a message to the KDC asking to communicate with Bob. KDC will generate a new random key, the **session key**, and send this key  $k_S$  to Alice encrypted using  $k_A$ , and to Bob encrypted using  $k_B$ . Once they both have the session key, they can use it to communicate and when they finish they just dispose the key.

Advantages of KDC:

- a. Each employee needs to store only one long-term secret key
- b. When an employee joins the organization, all that must be done is to set up a key between this employee and the KDC

Disadvantages of KDC:

- a. A successful attack on the KDC will result in a complete break of the system:
- b. The KDC is a single point of failure (can be solved with distribution or backup KDCs but also increases the points of attack)

KDCs are commonly used in practice, but they still have the problem that at some point, a secure channel has to be used to share keys.

### **Exercise 10.3**

Consider an example with Alice and Bob who run a probabilistic protocol to generate a shared secret key. Alice and Bob begin by holding the security parameter  $1^n$ . Alice runs the protocol

(denoted by  $G$ ) to obtain  $(C, q, g)$ . She uses  $(C, q, g)$  and a uniform  $x \in \mathbb{Z}_q^*$  to compute  $h_A = g^x$ . She then sends  $(C, q, g, h_A)$  to Bob. Bob receives them and uses a uniform  $y \in \mathbb{Z}_q^*$  to compute  $h_B = g^y$ . He then uses  $h_A$  to output  $k_B = h_A^y$  and sends  $h_B$  to Alice. Alice receives  $h_B$  and she computes  $k_A = h_B^x$ .

Let's try that with actual numbers. Alice and Bob agree to use a modulus  $p = 49$  and base  $g = 11$  (has to be a primitive root). Alice chooses a secret integer  $x = 16$ , then sends Bob  $h_A = g^x \bmod p$

$$h_A = 11^{16} \bmod 49 = 18$$

Bob chooses a secret integer  $y = 24$ , then sends Alice  $h_B = g^y \bmod p$

$$h_B = 11^{24} \bmod 49 = 6$$

Alice computes  $k_A = h_B^x \bmod p$

$$k_A = 6^{16} \bmod 49 = 2$$

Bob computes  $k_B = h_A^y \bmod p$

$$k_B = 18^{24} \bmod 49 = 2$$

Alice and Bob now share the same secret key, "2".

#### Exercise 10.4

- a. Public-key encryption allows key distribution to be done over public channels.
- b. Public-key cryptography reduces the need for users to store many secret keys.
- c. Finally, public-key cryptography is (more) suitable for open environments where parties who have never previously interacted want the ability to communicate securely.

#### Exercise 10.5

Exercise solution using Python programming language

```
sharedPrime = 23      # p
sharedBase = 5       # g

aliceSecret = 6      # a
bobSecret = 15        # b

print( "Publicly Shared Variables:")
print( "Publicly Shared Prime: " , sharedPrime )
```

```

print( "Publicly Shared Base: " , sharedBase )

# Alice Sends Bob A = g^a mod p
A = (sharedBase**aliceSecret) % sharedPrime
print( "Alice Sends Over Public Channel: " , A )

# Bob Sends Alice B = g^b mod p
B = (sharedBase ** bobSecret) % sharedPrime
print("Bob Sends Over Public Channel: ", B )

print( "Privately Calculated Shared Secret:" )
# Alice Computes Shared Secret: s = B^a mod p
aliceSharedSecret = (B ** aliceSecret) % sharedPrime
print( "Alice Shared Secret: ", aliceSharedSecret )

# Bob Computes Shared Secret: s = A^b mod p
bobSharedSecret = (A**bobSecret) % sharedPrime
print( "    Bob Shared Secret: ", bobSharedSecret )

```

## Public-Key Cryptography (11<sup>th</sup> Week)

### Exercise 11.1

Up to now we assumed that any adversary is passive, for example the adversary only eavesdrops on communication between the sender and receiver without interfering with the communication. But if the adversary tampers all the communication between the honest parties, and these honest parties share no keys in advance, then privacy simply cannot be achieved. Let's discuss an example of such an attack. Let's say Alice sends her public key  $pk$  to Bob but the adversary replaces it with a key  $pk'$  of his own (for which it knows the matching private key  $sk'$ ), then even though Bob encrypts his message using  $pk'$  the adversary will easily be able to recover the message (using  $sk'$ ).

Similarly, if an adversary is able to change the value of Alice's public key that is stored in some public directory, or if the adversary can tamper with the public key as it is transmitted from the public directory to Bob.

If Alice and Bob do not share any information in advance, and are not willing to rely on some mutually trusted third party, there is nothing Alice or Bob can do to prevent active attacks of this sort, or even to tell that such an attack is taking place.

For the purposes of this course we will assume that the sender is able to receive a legitimate copy of the receiver's public key.

### Exercise 11.2

A public-key encryption scheme is a triple of probabilistic polynomial-time algorithms ( $Gen$ ,  $Enc$ ,  $Dec$ ) such that:

- a. The key-generation algorithm  $Gen$  takes as input the security parameter  $1^n$  and outputs a pair of keys  $(pk, sk)$ . That is the public key  $pk$  and the private key  $sk$ . We assume for convenience that  $pk$  and  $sk$  each has length at least  $n$ , and that  $n$  can be determined from  $pk, sk$ .
- b. The encryption algorithm  $Enc$  takes as input a public key  $pk$  and a message  $m$  from some message space (that may depend on  $pk$ ). It outputs a ciphertext  $c$ , and we write this as  $c \leftarrow Enc_{pk}(m)$ . (Note that  $Enc$  needs to be probabilistic to achieve meaningful security.)
- c. The deterministic decryption algorithm  $Dec$  takes as input a private key  $sk$  and a ciphertext  $c$ , and outputs a message  $m$  or a special symbol  $\perp$  denoting failure. We write this as  $m \perp = Dec_{sk}(c)$ .

It is required that, except possibly with negligible probability over  $(pk, sk)$  output by  $Gen(1^n)$ , we have  $Dec_{sk}(Enc_{pk}(m)) = m$  for any (legal) message  $m$ .

### Exercise 11.3

#### Chosen-Plaintext Attacks

Given a public-key encryption scheme  $n = (Gen, Enc, Dec)$  and an adversary  $A$ , consider the following experiment:

The eavesdropping indistinguishability experiment  $PubK_{A,I}^{eav}(n)$ :

- a.  $Gen(1^n)$  is run to obtain keys  $(pk, sk)$
- b. Adversary  $A$  is given  $pk$ , and outputs a pair of equal-length messages  $m_0, m_1$  in the message space
- c. A uniform bit  $b \in \{0, 1\}$  is chosen, and then a ciphertext  $c \leftarrow Enc_{pk}(m_b)$  is computed and given to  $A$ . We call  $c$  the challenge ciphertext
- d.  $A$  outputs a bit  $b'$ . The output of the experiment is  $1$  if  $b' = b$ , and  $0$  otherwise. If  $b' = b$  we say that  $A$  succeeds.

A public-key encryption scheme  $n = (Gen, Enc, Dec)$  has indistinguishable encryptions in the presence of an eavesdropper if for all probabilistic polynomial-time adversaries  $A$  there is a negligible function  $negl$  such that

$$\Pr[PubK_{A,II}^{eav}(n) = 1] \geq \frac{1}{2} + negl(n)$$

### **Chosen-Ciphertext Attacks**

Chosen-ciphertext attacks, in which an adversary is able to obtain the decryption of arbitrary ciphertexts of its choice, are a concern in the public-key cryptography just as they are in the private-key cryptography. In fact, they are arguably more of a concern in the public-key cryptography since there a receiver expects to receive ciphertexts from multiple senders who are possibly unknown in advance, whereas a receiver in the private-key cryptography intends to communicate only with a single, known sender using any particular secret key.

Assume an eavesdropper  $A$  observes a ciphertext  $c$  sent by a sender  $S$  to a receiver  $R$ . Broadly speaking, in the public-key cryptography there are two classes of chosen-ciphertext attacks:

- a.  $A$  might send a modified ciphertext  $c'$  to  $R$  on behalf of  $S$ . In this case, although it is unlikely that  $A$  would be able to obtain the entire decryption  $m'$  of  $c'$ , it might be possible for  $A$  to infer some information about  $m'$  based on the subsequent behavior of  $R$ . Based on this information,  $A$  might be able to learn something about the original message  $m$ .
- b.  $A$  might send a modified ciphertext  $c'$  to  $R$  in its own name. In this case,  $A$  might obtain the entire decryption  $m'$  of  $c'$  if  $R$  responds directly to  $A$ . Even if  $A$  learns nothing about  $m'$ , this modified message may have a known relation to the original message  $m$  that can be exploited by  $A$ .

### **Exercise 11.4**

The following points should be included in the correct answer

#### **Private/Secret key:**

- Private key is faster compared to public key
- Private key is symmetrical. Actually there is only one key. The other is a copy of it.
- Private key is truly private .Should be available with only the two communicating parties.
- The two parties must have met before at least once to share the key.

#### **Public key:**

- Relatively slow to encrypt/decrypt

- Asymmetrical

- Public key can be made public. Private key is truly secret.
- The two parties need not have met. The two may be strangers, half way around the globe.

## RSA Encryption (12<sup>th</sup> Week)

### Exercise 12.1

Let's describe a simple encryption scheme based on the RSA problem. Even though such a scheme is insecure, it is a good way to start an RSA based encryption.

Let  $\text{GenRSA}$  be a *PPT* algorithm that, on input  $1^n$ , outputs a modulus  $N$  that is the product of two n-bit primes, along with integers  $e, d$  satisfying  $ed = 1 \bmod \phi(N)$ . Let  $N, e, d$  satisfy the equation, and let  $c = m^e \bmod N$ . RSA encryption relies on the fact that someone who knows  $d$  can recover  $m$  from  $c$  by computing  $c^d \bmod N$ . This works because

$$c^d = (m^e)^d = m^{ed} = m \bmod N$$

On the other hand, without knowledge of  $d$  (even if  $N$  and  $e$  are known) the RSA assumption implies that it is difficult to recover  $m$  from  $c$ , at least if  $m$  is chosen uniformly from  $\mathbb{Z}_N^*$ .

Therefore we can summarise this plain RSA encryption as follows

Let  $\text{GenRSA}$  be as in the text.

- Gen*: on input  $1^n$  run  $\text{GenRSA}(1^n)$  to obtain  $N, e$ , and  $d$ . The public key is  $\langle N, e \rangle$  and the private key is  $\langle N, d \rangle$ .
- Enc*: on input a public key  $pk = \langle N, e \rangle$  and a message  $m \in \mathbb{Z}_N^*$  compute the ciphertext  $c \in [m^e \bmod N]$ .
- Dec*: on input a private key  $sk = \langle N, d \rangle$  and a ciphertext  $c \in \mathbb{Z}_N^*$  compute the message  $m \in [c^d \bmod N]$ .

### Exercise 12.2

#### Quadratic Improvement in Recovering M

Since plain RSA encryption is deterministic, we know that if  $m < B$  then an attacker can determine  $m$  from the ciphertext  $c = [m^e \bmod N]$  in time  $O(B)$  using a brute-force attack. One might hope, however, that plain RSA encryption can be used if  $B$  is large, i.e., if the message is chosen from a reasonably large set of values. One possible scenario where this might occur is in the context of hybrid encryption, where the “message” is a random n-bit key and so  $B = 2^n$ . Unfortunately,

there is a clever attack that recovers  $m$ , with high probability, in time roughly  $O(\sqrt{B})$ . This can make a significant difference in practice: a  $2^{80}$ -time attack (say) is infeasible, but an attack running in time  $2^{40}$  is relatively easy to carry out.

### Encrypting short messages using small $e$

The previous attack shows how to recover a message  $m$  known to be smaller than some bound  $B$  in time roughly  $O(\sqrt{B})$ . Here we show how to do the same thing in time  $\text{poly}(\|N\|)$  if  $B \leq N^{1/e}$ . The attack relies on the observation that when  $m < N^{1/e}$ , raising  $m$  to the  $e$ th power modulo  $N$  involves no modular reduction. This means that given the ciphertext  $c = [m^e \bmod N]$ , an attacker can determine  $m$  by computing  $m \equiv c^{1/e}$  over the integers. This can be done easily in time  $\text{poly}(\|c\|) = \text{poly}(\|N\|)$  since finding  $e$ th roots is easy over the integers and hard only when working mod  $N$ . For small  $e$  this represents a serious weakness of plain RSA encryption. For example, if we take  $e = 3$  and assume  $\|N\| \geq 1024$  bits, then the attack works even when  $m$  is a uniform 300-bit integer; this once again rules out security of plain RSA even when used as part of a hybrid encryption scheme.

### Encrypting a partially known message

This attack can be viewed as a generalization of the previous one. It assumes a sender who encrypts a message, part of which is known. Here we rely on a powerful result of Coppersmith which says:

Let  $p(x)$  be a polynomial of degree  $e$ . Then in time  $\text{poly}(\|N\|, e)$  one can find all  $m$  such that  $p(m) = 0 \bmod N$  and  $|m| \leq N^{1/e}$ .

Due to the dependence of the running time on  $e$ , the attack is only practical for small  $e$ . In what follows we assume  $e = 3$  for concreteness. Assume a sender encrypts a message  $m = m_1 // m_2$  to a receiver with public key  $(N, 3)$ , where the first portion  $m_1$  of the message is known but the second portion  $m_2$  is not. For concreteness, say  $m_2$  is  $k$  bits long, so  $m = B \cdot m_1 + m_2$  where we let  $B = 2^k$ . Given the resulting ciphertext  $c = [(m_1 // m_2)^3 \bmod N]$ , an eavesdropper can define  $p(x) = (2^k \cdot m_1 + x)^3 - c$ , a cubic polynomial. This polynomial has  $m_2$  as a root (modulo  $N$ ), and  $|m_2| < B$ . A similar attack works when  $m_2$  is known but  $m_1$  is not.

## Digital Signatures (13<sup>th</sup> Week)

### **Exercise 13.1**

Signature schemes allow a signer  $S$  who has established a public key  $pk$  to “sign” a message using the associated private key  $sk$  in such a way that anyone who knows  $pk$ , and knows that this public key was established by  $S$ , can verify that the message originated from  $S$  and was not modified in transit. As a prototypical application, consider a software company that wants to disseminate software updates in an authenticated manner; that is, when the company releases an update it should be possible for any of its clients to verify that the update is authentic, and a malicious third party should never be able to fool a client into accepting an update that was not actually released by the company. To do this, the company can generate a public key  $pk$  along with a private key  $sk$ , and then distribute  $pk$  in some reliable manner to its clients while keeping  $sk$  secret. When releasing a software update  $m$ , the company computes a digital signature  $u$  on  $m$  using its private key  $sk$ , and sends  $(m, u)$  to every client. Each client can verify the authenticity of  $m$  by checking that  $u$  is a correct signature on  $m$  with respect to the public key  $pk$ .

A malicious party might try to issue a fraudulent update by sending  $(m', u')$  to a client, where  $m'$  represents an update that was never released by the company. This  $m'$  might be a modified version of some previous update, or it might be completely new and unrelated to any prior updates. If the signature scheme is “secure”, however, then when the client attempts to verify  $u'$  it will find that this is an invalid signature on  $m'$  with respect to  $pk$ , and will therefore reject the signature. The client will reject even if  $m'$  is modified only slightly from a genuine update  $m$ . This is not just a theoretical application of digital signatures, but one that is used extensively today for distributing software updates.

### **Exercise 13.2**

Both MACs and digital signature schemes are used to ensure the integrity of transmitted messages. Using digital signatures rather than MACs simplifies key distribution and management, especially when a sender needs to communicate with multiple receivers. By using a digital signature scheme the sender avoids having to establish a distinct secret key with each potential receiver, and avoids having to compute a separate MAC tag with respect to each such key. Instead, the sender need only compute a single signature that can be verified by all recipients. A qualitative advantage that digital signatures have as compared to MACs is that signatures are publicly verifiable. This means that if a receiver verifies that a signature on a given message is legitimate, then all other parties who receive this signed message will also verify it as legitimate.

This feature is not achieved by MACs if the signer shares a separate key with each receiver. Public verifiability implies that signatures are transferable: a signature  $u$  on a message  $m$  by a signer  $S$  can be shown to a third party, who can then verify herself that  $u$  is a legitimate signature on  $m$  with respect to  $S$ 's public

key. By making a copy of the signature, this third party can then show the signature to another party and convince them that  $S$  authenticated  $m$ , and so on. Public verifiability and transferability are essential for the application of digital signatures to certificates and public-key infrastructures. Digital signature schemes also provide the very important property of non-repudiation. This means that once  $S$  signs a message he cannot later deny having done so. This aspect of digital signatures is crucial for legal applications where a recipient may need to prove to a third party that a signer did indeed “certify” a particular message: assuming  $S$ 's public key is known to the judge, or is otherwise publicly available, a valid signature on a message serves as convincing evidence that  $S$  indeed signed this message. MACs simply cannot provide non-repudiation. Let's say users  $S$  and  $R$  share a key  $k_{SR}$ , and  $S$  sends a message  $m$  to  $R$  along with a (valid) MAC tag  $t$  computed using this key. Since the judge does not know  $k_{SR}$ , there is no way for the judge to determine whether  $t$  is valid or not. If  $R$  were to reveal the key  $k_{SR}$  to the judge, there would be no way for the judge to know whether this is the “actual” key that  $S$  and  $R$  shared, or whether it is some “fake” key manufactured by  $R$ . Finally, even if we assume the judge can somehow obtain the actual key  $k_{SR}$  shared by the parties, there is no way for the judge to distinguish whether  $S$  generated  $t$  or whether  $R$  did.

As in the case of private-key vs. public-key encryption, MACs have the advantage of being shorter and roughly 2–3 orders of magnitude more efficient to generate/verify than digital signatures. Thus, in situations where public verifiability, transferability, and/or non-repudiation are not needed, and the sender communicates primarily with a single recipient MACs should be used.

### Exercise 13.3

Digital signatures are the public-key counterpart of MACs, and their syntax and security guarantees are analogous. The algorithm that the sender applies to a message is here denoted *Sign* (rather than *Mac*), and the output of this algorithm is now called a *signature* (rather than a *tag*). The algorithm that the receiver applies to a message and a signature in order to verify validity is still denoted *Vrfy*.

A (digital) signature scheme consists of three probabilistic polynomial-time *PPT* algorithms (*Gen*, *Sign*, *Vrfy*) such that:

- a. The key-generation algorithm  $Gen$  takes as input a security parameter  $1^n$  and outputs a pair of keys  $(pk, sk)$ . These are called the public key and the private key, respectively. We assume that  $pk$  and  $sk$  each has length at least  $n$ , and that  $n$  can be determined from  $pk$  or  $sk$ .
- b. The signing algorithm  $Sign$  takes as input a private key  $sk$  and a message  $m$  from some message space (that may depend on  $pk$ ). It outputs a signature  $u$ , and we write this as  $u \leftarrow Sign_{sk}(m)$ .
- c. The deterministic verification algorithm  $Vrfy$  takes as input a public key  $pk$ , a message  $m$ , and a signature  $u$ . It outputs a bit  $b$ , with  $b = 1$  meaning valid and  $b = 0$  meaning invalid. We write this as  $b \leftarrow Vrfy_{pk}(m, u)$ .

It is required that except with negligible probability over  $(pk, sk)$  output by  $Gen(1^n)$ , it holds that  $Vrfy_{pk}(m, Sign_{sk}(m)) = 1$  for every (legal) message  $m$ . If there is a function  $l$  such that for every  $(pk, sk)$  output by  $Gen(1^n)$  the message space is  $\{0, 1\}^{l(n)}$ , then we say that  $(Gen, Sign, Vrfy)$  is a signature scheme for messages of length  $l(n)$ .

#### Exercise 13.4

In both MAC and Digital Signature schemes, you have two algorithms:

- **Generation:** given the message  $m$  and a key  $K_1$ , compute the MAC value or signature  $s$ .
- **Verification:** given the message  $m$ , a key  $K_2$  and the MAC value or signature  $s$ , verify that they correspond to each other (the MAC value or signature is valid for the message  $m$ , using verification key  $K_2$ )

With a MAC, keys  $K_1$  and  $K_2$  are identical (or can be trivially recomputed from each other). With a signature, the verification key  $K_2$  is mathematically linked with  $K_1$  but not identical, and it is unfeasible to re-compute  $K_1$  from  $K_2$  or to generate valid signatures when you only know  $K_2$ .

Thus, signatures dissociate the generation and verification powers. With a MAC, any entity who can verify a MAC value necessarily has the power to generate MAC values of its own. With signatures, you can make the verification key public, while keeping the generation key private. Signatures are when you want to produce a proof verifiable by third party without having to entrust these third parties with anything.

Application: a CA (like Verisign, Thawte, etc.) issues a certificate to a SSL server. Everybody, and in particular your Web browser, can verify that the certificate issued to the SSL server has indeed been signed by Verisign/Thawte. But this does not give you the power to issue (sign) certificates yourself, which would appear as if they were issued by Verisign/Thawte.



**FORM: 200.1.3**

## **STUDY GUIDE**

**Course: CYS605 - Cybersecurity Policy, Governance,  
Law and Compliance**

## Course Information

<b>Institution</b>	European University Cyprus						
<b>Programme of Study</b>	Cybersecurity (MSc)						
<b>Course unit</b>	CYS605	Cybersecurity Policy, Governance, Law and Compliance					
<b>Level</b>	<i>Undergraduate</i>		<i>Postgraduate</i>				
			<i>Master</i>	<i>PhD</i>			
			√				
<b>Language of Instruction</b>	English						
<b>Teaching Methodology</b>	Distance Learning						
<b>Course Type</b>	<b>Compulsory</b>			<b>Optional</b>			
	√						
<b>Number of Group Consultation Meetings/ Web-Conferences/ Lectures</b>	<b>Total</b>		<b>Face to Face</b>	<b>Web-Conferences</b>			
	14		1	13			
<b>Number of Activities/ Assignments</b>	4						
<b>Final Assessment</b>	<b>Assignments</b>			<b>Final Examinations</b>			
	50 %			50 %			
<b>Number of Credits (ECTS)</b>	10						
<b>Study Guide drafted by</b>	Dr Yianna Danidou						
<b>Editing and final approval of Study Guide by</b>	Dr Yianna Danidou						

## COURSE CONTENTS

		Page
	<b>Error! Reference source not found.</b>	5
1	Week 1 -  CYBERSECURITY, NETWORK AND INFORMATION SECURITY  <b>1st Week</b>	9
2	Week 2 - INTRODUCTION TO INFORMATION SECURITY  <b>2nd Week</b>	19
3	Week 3 - INFORMATION SECURITY POLICY  <b>3rd Week</b>	25
4	Week 4 - INFORMATION SECURITY GOVERNANCE  <b>4th Week</b>	35
5	Week 5 - RISK MANAGEMENT: IDENTIFYING AND ASSESSING RISK  <b>5th Week</b>	56
6	Week 6 - COMPLIANCE: AUDITING, MONITORING, AND	88

	LOGGING	<b>6th Week</b>	
7	Week 7 - PLANNING FOR CONTINGENCIES	<b>7th Week</b>	96
8	Week 8 - INFORMATION SECURITY MAINTENANCE	<b>8th Week</b>	110
9	Week 9 - LEGAL AND REGULATORY REQUIREMENTS	<b>9th Week</b>	127
10	Week 10 - CYBER LAW	<b>10th Week</b>	144
11	Week 11 - GENERAL DATA PROTECTION REGULATION (GDPR)	<b>11th Week</b>	154



	<b>12th &amp; 13th Week</b>	
13	Week 13 - INVITED LECTURE	161
	<b>12th &amp; 13th Week</b>	
14	Revision Week and Final Examination	162
	Indicative answers to Self-Assessment exercises	163

## 1st GROUP CONSULTATION MEETING

### Programme Presentation

Leading companies today are rethinking the role of information security in their organizations. They realize that in a digital world, cybersecurity is the key to safeguarding their most precious assets—intellectual property, customer information, financial data, and employee records, among others. But far more than a defensive measure, companies also know that cybersecurity can better position their organization with business partners, customers, investors, and other stakeholders.

The European cybersecurity market is about 25% (i.e. about €17bln) of the world market (estimated at €70bln in 2015), with an average yearly growth slightly larger than 6%, when the world market is growing at about 10%/year. Recent study compiled by Europe's cybersecurity industry leaders pointed out that Europe is in danger of falling behind in the international digital economy field.

The Master in Cybersecurity is a cutting-edge program, designed for those wishing to develop a career as a cyber-security professional, or to take a leading technical or managerial role in an organization critically dependent upon data and information communication technology. Students will develop an advanced knowledge of information security and an awareness of the context in which information security operates in terms of safety, environmental, social and economic aspects. They will gain a wide range of intellectual, practical and transferable skills, enabling them to develop a flexible professional career in IT.

Key elements of this postgraduate degree are: the *real life experience* given by the opportunity to apply their theoretical knowledge through specialized virtual and remote security laboratories in which they will be able to carry out activities such as reconnaissance, network scanning and exploitation exercises, and investigate the usage and behavior of security systems such as Intrusion Detection and Prevention Systems thus becoming confident in the practical application of the latest tools; the *high-level insight* that will enhance student's ability to research and design creative cyber security solutions to address business problems; *hands-on skills* through experimentation with security techniques, cryptographic algorithms, cyber forensics building an ethical hacking environment; and *flexibility* since students will also be able to choose either the completion of a Master thesis or to complete a Research methods course and two elective courses.

Students undertake modules to the value of 90 ECTS credits.

## COURSE PRESENTATION THROUGH THE STUDY GUIDE

The CYS605 course is a compulsory course to be taught during the second semester of the Master's degree. Its main **aim** is to allow prospective graduates to develop security policies that will be supported by executive management and adopted by all employees, by developing knowledge and skills in risk-based information security management, geared toward preventive management and assurance of security of information and information systems in technology-enabled environments. This course examines the steps required in policy development including password protection, acceptable use of organization information technology assets, risk acceptance, identification of internal and external threats, countermeasures, intellectual property, proprietary information and privacy issues, compliance reporting, and escalation procedures. Related topics such as access controls, security standards, and policy implementation are covered. In the Cybersecurity Policy, Governance, Law and Compliance course we will examine the detailed steps that are required in developing cyber security policies, risk assessments, identification of internal and external threats, legal and privacy issues, reports, policy documents and other closely related documents. In support of these documents we will also explore the technology involved in creating firewall access controls, well developed social engineering security controls, and stake holder policy implementation and enforcement. Security Policy development and technology implementation will be covered in depth. Students are required to attend bi- weekly virtual classes to submit discussion posts, reading assignment case studies, media content review and exams.

On successful completion, the student will be able to:

- Demonstrate an understanding in writing cyber security policy documents and how to mitigate security risks appropriately.
- Understand the cybersecurity threat landscape
- Identify and document the various types of cyber attacks that threaten governmental and private industry information technology enterprises
- Assess options for mitigating risks after a cyber attack has occurred.
- Write cyber security policy documents that demonstrate an understanding of how to mitigate security risks appropriately
- Develop an appreciation for the importance of policy implementation and enforcement

This study guide has been prepared collectively by the academic staff teaching in the program of study this course belongs to and by the Distance Education Unit Director. The guide has been

approved by the relevant Department Chair and the Distance Education Unit Director. The study guide is based on the syllabus and learning material (provided through the online learning platform) of the course CYS605. The guide consists of a basic tool of the learning process for this course and it has been designed to use it along with the course learning material. The aim of this guide is to direct students on how to use the learning material of this course in order to understand and comprehend it. The guide aims to provide the necessary support needed for distance learning. The guide is continuously updated to keep in accord with the course learning material and to meet the aim of the course. Although the study guide provides extensive information related to the course, it does not substitute in any way the learning material provided on the learning platform. It is imperative that the studying of the learning material and executing the rest of the activities of the course (e.g. attending online lectures, completing coursework) are very important for the successful completion of the course.

This guide consists of a number of units, divided in 13 weeks, each one comprised of the summary and introductory remarks, aim, learning outcomes, keywords, required learning material, recommended further learning material, self-assessment activities and expected time for self-study. At the end of this study guide, students can find suggested solutions and proposed answers to all the self-assessment activities of this guide. It is very important that students carry out the suggested self-assessment activities because it will assist them to understand in a practical way the theoretical material they study for this course. In addition, the self-assessment activities help to motivate and encourage students to carry out their self-study and to develop their analytical and critical thinking skills. The self-assessment activities together with the model answers to the self-assessment activities serve as a kind of a self-assessment for students. The expected time for self-study of each unit includes the expected time spent on studying the learning material and carrying out the self-assessment activities of each unit. The expected time for self-study does not include the expected time for attending online lectures, coursework preparation, final examination preparation, and final examination itself.

## **Recommended time for the student to work**

Approximately 5 hours for comprehending the study guide.

# CYBERSECURITY, NETWORK AND INFORMATION SECURITY

1<sup>st</sup> Week

## Summary

Cybersecurity is defined as the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.

"some people have argued that the threat to Cybersecurity has been somewhat inflated"

## Introductory Remarks

There is a wide range of currently accepted cybersecurity definitions: The Committee on National Security Systems (CNSS-4009) defines cybersecurity as the ability to protect or defend an enterprise's use of cyberspace from an attack, conducted via cyberspace, for the purpose of: disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or, destroying the integrity of the data or stealing controlled information. The National Institute of Standards and Technology (NIST) defines cybersecurity as "*the process of protecting information by preventing, detecting, and responding to attacks.*"

Similar to financial and reputational risk, cybersecurity risk affects a company's bottom line. It can drive up costs and impact revenue. It can harm an organization's ability to innovate and to gain and maintain customers. The International Organization for Standardization defines cybersecurity or cyberspace security as the preservation of confidentiality, integrity and availability of information in the Cyberspace. In turn, "the Cyberspace" is defined as "*the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.*" At its core, cybersecurity seeks to protect your enterprise from those who wish to do harm to your business, steal your information or your money, or use your systems to target peers in the market.

Guaranteeing Cybersecurity requires coordinated efforts throughout an information system.

Elements of Cybersecurity include:

- Application security

- Information security
- Network security
- Disaster recovery / business continuity planning
- Operational security
- End-user education

One of the most problematic elements of Cybersecurity is the quickly and constantly evolving nature of security risks. The traditional approach has been to focus most resources on the most crucial system components and protect against the biggest known threats, which necessitated leaving some less important system components undefended and some less dangerous risks not protected against. Such an approach is insufficient in the current environment.



Adam Vincent, CTO-public sector at Layer 7 Technologies (a security services provider to federal agencies including Defense Department organizations), describes the problem:

"The threat is advancing quicker than we can keep up with it. The threat changes faster than our idea of the risk. It's no longer possible to write a large white paper about the risk to a particular system. You would be rewriting the white paper constantly..."

To deal with the current environment, advisory organizations are promoting a more proactive and adaptive approach. The National Institute of Standards and Technology (NIST), for example, recently issued updated guidelines in its risk assessment framework that recommended a shift toward continuous monitoring and real-time assessments.

A new study from Wombat Security and Aberdeen Group, a recognized leader in security

awareness and training, shows that boosting Cybersecurity awareness and education among employees can reduce enterprise security risks and cost. According to a pair of organizations behind a newly released study, Cybersecurity awareness and education is important, not just for IT professionals but for all employees of every organization, from management to the general rank-and-file of an organization's workforce.

However, it can be difficult for security officers to effectively communicate this importance to senior management. It is suggested that security awareness and changing employee behaviour can reduce the risk of a breach by up to 70%. While companies tend to spend a lot on security technologies, it was found that these controls are not 100% effective and may not account for one of the biggest threats to security: the errant behaviour of end users. Investing in awareness and training to teach employees how to effectively deal with common threats from social media or phishing can quantifiably reduce security-related risk by 45% to 70%, according to the companies, when accounting for both the likelihood and business impacts of security infections due to employee behaviour.

Information Governance (IG) is a sort of super discipline that has emerged as a result of new and tightened legislation governing businesses, external threats such as hacking and data breaches, and the recognition that multiple overlapping disciplines were needed to address today's information management challenges in an increasingly regulated and litigated business environment. IG is a subset of corporate governance, and includes key concepts from records management, content management, IT and data governance, information security, data privacy, risk management, litigation readiness, regulatory compliance, long-term digital preservation, and even business intelligence. This also means that it includes related technology and discipline subcategories, such as document management, enterprise search, knowledge management, and business continuity/ disaster recovery.

Practicing good IG is the essential foundation for building legally defensible disposition practices to discard unneeded information and to secure confidential information, which may include trade secrets, strategic plans, price lists, blueprints, or personally identifiable information (PII) subject to privacy laws; it provides the basis for consistent, reliable methods for managing data, e-documents, and records.

Having trusted and reliable records, reports, data, and databases enables managers to make key decisions with confidence. And accessing that information and business intelligence in a timely fashion can yield a long-term sustainable competitive advantage, creating more agile enterprises.

To do this, organizations must standardize and systematize their handling of information. They must analyze and optimize how information is accessed, controlled, managed, shared, stored, preserved, and audited. They must have complete, current, and relevant policies, processes, and technologies to manage and control information, including who is able to access what information, and when, to meet external legal and regulatory demands and internal governance policy requirements. In short, IG is about information control and compliance.

IG is a subset of corporate governance, which has been around as long as corporations have existed. IG is a rather new multidisciplinary field that is still being defined, but has gained traction increasingly over the past decade. The focus on IG comes not only from compliance, legal, and records management functionaries but also from executives who understand they are accountable for the governance of information and that theft or erosion of information assets has real costs and consequences.

Information security governance is the responsibility of the board of directors and senior executives. It must be an integral and transparent part of enterprise governance and be aligned with the IT governance framework. Whilst senior executives have the responsibility to consider and respond to the concerns and sensitivities raised by information security, boards of directors will increasingly be expected to make information security an intrinsic part of governance, integrated with processes they already have in place to govern other critical organisational resources.

To exercise effective enterprise and information security governance, boards and senior executives must have a clear understanding of what to expect from their enterprise's information security programme. They need to know how to direct the implementation of an information security programme, how to evaluate their own status with regard to an existing security programme and how to decide the strategy and objectives of an effective security programme.

Whilst there are many aspects to information security governance, there are several matters that can assist in focusing on the question, 'What is information security governance?'.

These are the:

- Desired outcomes of information security governance
- Knowledge and protection of information assets
- Benefits of information security governance
- Process integration

Information security governance consists of the leadership, organisational structures and processes that safeguard information. Critical to the success of these structures and processes is effective communication amongst all parties based on constructive relationships, a common language and shared commitment to addressing the issues. The six basic outcomes of information security governance should include:

1. Strategic alignment of information security with business strategy to support organisational objectives
2. Risk management by executing appropriate measures to manage and mitigate risks and reduce potential impacts on information resources to an acceptable level
3. Business process assurance/ convergence by integrating all relevant assurance processes to maximize the effectiveness and efficiency of security activities
4. Resource management by utilising information security knowledge and infrastructure efficiently and effectively
5. Performance measurement by measuring, monitoring and reporting information security governance metrics to ensure that organisational objectives are achieved
6. Value delivery by optimising information security investments in support of organisational objectives.

The National Association of Corporate Directors (NACD), the leading membership organisation for boards and directors in the US, recognises the importance of information security. It recommends four essential practices for boards of directors, as well as several specific practices for each point.

The four practices, which are based on the practicalities of how boards operate, are:

- Place information security on the board's agenda.
- Identify information security leaders, hold them accountable and ensure support for them.
- Ensure the effectiveness of the corporation's information security policy through review and approval.
- Assign information security to a key committee and ensure adequate support for that committee.

A key goal of information security is to reduce adverse impacts on the organisation to an acceptable level of risk. Information security protects information assets against the risk of loss, operational discontinuity, misuse, unauthorised disclosure, inaccessibility and damage. It also protects against the ever-increasing potential for civil or legal liability that organisations face as a

result of information inaccuracy and loss, or the absence of due care in its protection.

Information security covers all information processes, physical and electronic, regardless whether they involve people and technology or relationships with trading partners, customers and third parties. Information security addresses information protection, confidentiality, availability and integrity throughout the life cycle of the information and its use within the organisation.

Given the dramatic rise of information crimes, including phishing and other cyberattacks, few today would contend that improved security is not a requirement. With new worms/malware and the increase in reported losses of confidential customer information and intellectual property theft, senior management is left with little choice but to address these issues. Information security requires a balance between sound management and applied technology. With the widespread use of networks, individuals and organisations are concerned with other risks pertaining to privacy of personal information and the organisation's need to protect the confidentiality of information, whilst encouraging electronic business.

The systems and processes that handle information have become pervasive throughout enterprises. Organisations may survive the loss of other assets, including facilities, equipment and people, but few can continue with the loss of their critical information (i.e., accounting and financial reporting information and operations and process knowledge and information) or customer data. The risks, benefits and opportunities these resources present have made information security governance a critical facet of overall governance. Information security should be an integral part of enterprise governance, aligned with IT governance and integrated into strategy, concept, design, implementation and operation. Protecting critical information must constitute one of the major risks to be considered in management strategies and should also be recognised as a crucial contributor to success.

Thus, information security governance requires senior management commitment, a security-aware culture, promotion of good security practices and compliance with policy. It is easier to buy a solution than to change a culture, but even the most secure system will not achieve a significant degree of security if used by ill-informed, untrained, careless or indifferent personnel. Information security is a top-down process requiring a comprehensive security strategy that is explicitly linked to the organisation's business processes and strategy. Security must address entire organisational processes, both physical and technical, from end to end. To ensure that all relevant elements of security are addressed in an organisational security strategy, several security standards have been developed to provide guidance and ensure comprehensiveness.

Information security governance is a subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, manages risks appropriately, uses organisational resources responsibly, and monitors the success or failure of the enterprise security programme. Information security deals with all aspects of information (spoken, written, printed, electronic or any other medium) and information handling (created, viewed, transported, stored or destroyed). This is contrasted with IT security that is concerned with security of information within the boundaries of the network infrastructure technology domain. Typically, confidential information disclosed in an elevator conversation or sent via regular mail would be outside the scope of IT security. However, from an information security perspective, the nature and type of compromise is not as important as the fact that security has been breached; that is the crucial concern. To achieve effective information security governance, management must establish and maintain a framework to guide the development and maintenance of a comprehensive information security programme.

The information security governance framework generally consists of:

- An information security risk management methodology
- A comprehensive security strategy explicitly linked with business and IT objectives
- An effective security organisational structure
- A security strategy that talks about the value of information protected—and delivered
- Security policies that address each aspect of strategy, control and regulation
- A complete set of security standards for each policy to ensure that procedures and guidelines comply with policy
- Institutionalised monitoring processes to ensure compliance and provide feedback on effectiveness and mitigation of risk
- A process to ensure continued evaluation and update of security policies, standards, procedures and risks

This framework in turn provides the basis for the development of a cost effective information security programme that supports the organisation's goals and provides an acceptable level of predictability for operations by limiting the impacts of adverse events. The overall objective of the programme is to provide assurance that information assets are given a level of protection commensurate with their value or the risk their compromise poses to the organisation.

To promote alignment, the business strategy provides one of the inputs into risk management and information security strategy development. Other inputs are the business processes, risk

assessments, business input analyses and the information resources critical for their success. Regulatory requirements must also be considered in developing the security strategy. Security requirements are the output of the risk management activity and are input to the planning activity together with the current state of the enterprise relative to these security requirements. Other inputs to the planning stage are the available resources and applicable constraints for achieving the desired state of security.

Whilst emerging definitions of the scope of information security are adding concepts such as information usefulness and possession—the latter to cope with theft, deception and fraud—the networked economy adds the critical need for *trust* and accountability in electronic transactions. In this context, the security objective is met when:

- Information is available and usable when required, and the systems that provide it can appropriately resist or recover from attacks (availability)
- Information is observed by or disclosed to only those who have a need to know (confidentiality)
- Information is protected against unauthorised modification (integrity)
- Business transactions as well as information exchanges between enterprise locations or with external trading partners can be trusted (authenticity and non-repudiation)

The relative priority and significance of availability, confidentiality, integrity, authenticity and non-repudiation vary according to the data within the information system and the business context in which they are used. For example, integrity is especially important relative to management information due to the impact that information has on critical strategy related decisions and financial reporting. Confidentiality may be the most critical today as it relates to personal, financial or medical information, or the protection of trade secrets and other forms of intellectual property (IP).

## Aim/Objectives

This chapter aims to introduce students to cybersecurity and its relation to network and information security. Further it aims to explain the concepts of policy, information governance (IG), law and compliance.

## Learning Outcomes

In this chapter, students should be able to:

- Define the concept of cybersecurity

- Recount the history of computer security, and explain how it evolved into information security
- Explore cybersecurity's relationship with network and information security
- Explain the concepts of policy, information governance, compliance
- Describe the laws and regulations designed to force improvement in organisational governance, security, controls and transparency

## Key Words

Information security	Network security	Cybersecurity
Governance	Data	Information
Knowledge	Policy	Information assets

## Annotated Bibliography

### Required Materials

To achieve the educational needs of this unit the following material is used:

#### Primary Material

Chapter 1 of Information Security Governance: A Practical Development and Implementation Approach by Krag Brotby

Chapter 1 of Your Cybersecurity Program A High-Level Overview Book Editor(s): Chris Moschovitis

Vacca, J.R., 2013. Cyber security and IT infrastructure protection. Syngress.

Bayuk, J.L., Healey, J., Rohmeyer, P., Sachs, M.H., Schmidt, J. and Weiss, J., 2012. Cyber security policy guidebook. John Wiley & Sons.

#### Supportive material

[https://www.pwc.com/gx/en/information-security-survey/pdf/pwcsurvey2010\\_cio\\_reprint.pdf](https://www.pwc.com/gx/en/information-security-survey/pdf/pwcsurvey2010_cio_reprint.pdf)

[http://www.qualified-audit-partners.be/user\\_files/ITforBoards/GVIT\\_ITGI\\_IT\\_Governance\\_Global\\_Status\\_Report\\_-](http://www.qualified-audit-partners.be/user_files/ITforBoards/GVIT_ITGI_IT_Governance_Global_Status_Report_-)

## **Self-Assessment Exercises**

### **Exercise 1.1**

Why is information security a management problem? What can management do that technology cannot?

### **Exercise 1.2**

Why is data the most important asset an organization possesses? What other assets in the organization require protection?

## **Recommended time for the student to work**

15 hours

# INTRODUCTION TO INFORMATION SECURITY

2<sup>nd</sup> Week

## Summary

This chapter establishes the foundation for understanding the broader field of information security. This is accomplished by defining key terms such as concepts of cybersecurity, information security terms and concepts like Access, Asset, Attack, Control, safeguard, or countermeasure, Exploit, Exposure, Loss, Protection profile or security posture Risk, Subjects and objects of attack, Threat, Threat agent, Threat event, Threat source, Vulnerability. Explaining essential concepts and reviewing the origins of the field and its impact on the understanding of information security.

## Introductory Remarks

Information security in today's enterprise is a "critical business capability that needs to be aligned with corporate expectations and culture that provides the leadership and insight to identify risks and implement effective controls."<sup>1</sup> However, before analysing the details of information security, it is necessary to review the origins of this field and its impact on our understanding of information security today.

The need for computer security, or the need to secure the physical location of hardware from outside threats, began almost immediately after the first mainframes were developed. Groups developing code-breaking computations during World War II created the first modern computers. Badges, keys, and facial recognition of authorized personnel controlled access to sensitive military locations. In contrast, information security during these early years was rudimentary and mainly composed of simple document classification schemes. The primary threats to security, were physical theft of equipment, espionage against the products of the systems, and sabotage.

During the 1960s, the Department of Defense's Advanced Research Procurement Agency

---

<sup>1</sup> Martin Fisher, IT Security Manager at Northside Hospital in Atlanta

(ARPA) began examining the feasibility of a redundant networked communications system designed to support the military's need to exchange information. Larry Roberts, who is known as the founder of the Internet, developed the project from its inception. During the next decade, ARPANET grew in popularity and use, and so did its potential for misuse. In December of 1973, Robert M. Metcalfe indicated that there were fundamental problems with ARPANET security. Individual remote users' sites did not have sufficient controls and safeguards to protect data against unauthorized remote users and there was lack of safety procedures for dial-up connections to the ARPANET. User identification and authorization to the system were non-existent.

The movement toward security went beyond protecting physical locations and began with the Rand Report R-609. This was sponsored by the U.S. Department of Defense, which attempted to define multiple controls and mechanisms necessary for the protection of a multilevel computer system. The scope of computer security grew from physical security to include: Securing the data; Limiting random and unauthorized access to that data; Involvement of personnel from multiple levels of the organization.

At the close of the 20th century, as networks of computers became more common, so did the need to connect the networks to each other. This gave rise to the Internet, the first manifestation of a global network of networks. There has been a price for the phenomenal growth of the Internet, however. When security was considered at all, early Internet deployment treated it as a low priority. As the requirement for networked computers became the dominant style of computing, the ability to physically secure the physical computer was lost, and the stored information became more exposed to security threats. In the late 1990s and into 2000s, many large corporations began publicly integrating security into their organizations. Further the antivirus products became popular and information security began to emerge as an independent discipline.

Today, the Internet has brought millions of unsecured computer networks into communication with each other. Explain that our ability to secure each computer's stored information is now influenced by the security on each computer to which it is connected.

In general, security means to be protected from adversaries, from those who would do harm, intentionally or otherwise. The Committee on National Security Systems (CNSS) defines information security as the protection of information and its critical elements. A successful organization should have the following multiple layers of security in place for the protection of its operations: Information security management; Data security; Network security.

The C.I.A. triad, which has been considered the industry standard for computer security since the development of the mainframe. It was solely based on three characteristics that described the utility of information: confidentiality, integrity, and availability. The C.I.A. triangle has expanded into a list of critical characteristics of information.

The value of information comes from the characteristics it possesses:

**Availability** enables users who need to access information to do so without interference or obstruction and to retrieve that information in the required format.

**Accuracy** occurs when information is free from mistakes or errors and has the value that the end user expects. If information contains a value different from the user's expectations due to the intentional or unintentional modification of its content, it is no longer accurate.

**Authenticity** is the quality or state of being genuine or original, rather than a reproduction or fabrication. Information is authentic when it is the information that was originally created, placed, stored, or transferred.

**Confidentiality** is the quality or state of preventing disclosure or exposure to unauthorized individuals or systems.

**Integrity** is the quality or state of being whole, complete, and uncorrupted. The integrity of information is threatened when the information is exposed to corruption, damage, destruction, or other disruption of its authentic state.

**Utility** is the quality or state of having value for some purpose or end. Information has value when it serves a particular purpose. This means that if information is available, but not in a format meaningful to the end user, it is not useful.

**Possession** is the quality or state of having ownership or control of some object or item. Information is said to be in one's possession if one obtains it, independent of format or other characteristics. While a breach of confidentiality always results in a breach of possession, a breach of possession does not always result in a breach of confidentiality.



To fully understand the importance of information security, it is necessary to briefly review the elements of an information system. An information system (IS) is the entire set of software, hardware, data, people, procedures, and networks necessary to use information as a resource in the organization.

Software is the operating systems, applications, and assorted utilities of an information system. Hardware as the physical assets that run the applications that manipulate the data of an information system. As hardware has become more portable, the threat posed by hardware loss has become a more prominent problem. The lifeblood of an organization is the information needed to strategically execute on business opportunities and the data processed by information systems are critical to today's business strategy. People are often the weakest link in an information system, since they give the orders, design the systems, develop the systems, and ultimately use and game the systems that run today's business world. Procedures are the written instructions for accomplishing a task, which may include the use of technology or information systems, but not necessarily. These are the rules that we are supposed to follow and the foundation for the technical controls that security systems must be designed to implement. The modern information processing system is extremely complex and relies on many hundreds of connections, both internal and external. Networks are the highway over which information systems pass data and users complete their tasks. Proper control over all traffic in every network in an organization is vital to properly managing the information flow and security of that organization.

When considering information security, it is important to realize that it is impossible to obtain perfect security. Security is not an absolute; it is a process and not a goal. Security should be

considered a balance between protection and availability. To achieve balance, the level of security must allow reasonable access, yet protect against threats.

Security can begin as a grassroots effort when systems administrators attempt to improve the security of their systems. This is referred to as the bottom-up approach. The key advantage of the bottom-up approach, which is the technical expertise of the individual administrators. Unfortunately, this approach seldom works, as it lacks a number of critical features, such as participant support and organizational staying power. An alternative approach, which has a higher probability of success, is called the top-down approach. The project is initiated by upper management who issue policy, procedures, and processes, dictate the goals and expected outcomes of the project, and determine who is accountable for each of the required actions. The top-down approach has strong upper-management support, a dedicated champion, dedicated funding, clear planning, and the opportunity to influence organizational culture.

Information security must be managed in a manner similar to any other major system implemented in the organization. The traditional approach for implementing an information security system in an organization has given rise to a number of variations, including RAD, JAD, Agile, and a new approach, DevOps.

It takes a wide range of professionals to support a diverse information security program. To develop and execute specific security policies and procedures, additional administrative support and technical expertise is required.

The Chief Information Officer is the senior technology officer, although other titles such as vice president of information, VP of information technology, and VP of systems may also be used. The CIO is primarily responsible for advising the chief executive officer, president, or company owner on the strategic planning that affects the management of information in the organization. The Chief Information Security Officer is the individual primarily responsible for the assessment, management, and implementation of securing the information in the organization. The CISO may also be referred to as the manager for security, the security administrator, or a similar title.

The roles of those who own and safeguard the data.

Data Owners: Those responsible for the security and use of a particular set of information. Data owners usually determine the level of data classification associated with the data, as well as changes to that classification required by organizational change.

Data Custodians: Those responsible for the storage, maintenance, and protection of the

information. The duties of a data custodian often include overseeing data storage and backups, implementing the specific procedures and policies laid out in the security policies and plans, and reporting to the data owner.

Data Users: End users who work with the information to perform their daily jobs supporting the mission of the organization. Everyone in the organization is responsible for the security of data, so data users are included here as individuals with an information security role.

Each organization develops and maintains its own unique culture and values. A community of interest is a group of individuals who are united by similar interests or values within an organization and who share a common goal of helping the organization to meet its objectives. These professionals are focused on protecting the organization's information systems and stored information from attacks.

There can be many different communities of interest in an organization. The three that are most often encountered, and which have roles and responsibilities in information security, are listed here. In theory, each role must complement the other but this is often not the case.

With the level of complexity in today's information systems, the implementation of information security has often been described as a combination of art and science. The concept of the "security artisan" and explain that it is based on the way individuals have perceived systems technologists since computers became commonplace. There are no hard and fast rules regulating the installation of various security mechanisms, nor are there many universally accepted complete solutions. While there are many manuals to support individual systems, once these systems are interconnected, there is no magic user's manual for the security of the entire system. This is especially true with the complex levels of interaction between users, policy, and technology controls. We are dealing with technology developed by computer scientists and engineers—technology designed to operate at rigorous levels of performance. Even with the complexity of the technology, most scientists would agree that specific scientific conditions cause virtually all actions that occur in computer systems. Almost every fault, security hole, and systems malfunction is a result of the interaction of specific hardware and software. If developers had sufficient time, they could resolve and eliminate these faults.

## Aim/Objectives

This chapter aims to introduce students to information security and stress its importance to businesses and organisations. The CIA triad is analysed along with the roles of each person

interacting with information in an organisation.

## Learning Outcomes

In this chapter, students should be able to:

- Define information security
- Recount the history of computer security, and explain how it evolved into information security
- Define key terms and critical concepts of information security
- Explain the role of security in the systems development life cycle
- Describe the information security roles of professionals within an organization

## Key Words

Accuracy	Authenticity	Availability
C.I.A. triad	CIO	CISO
Communications security	Computer security	Confidentiality
Data custodians	Data owners	Data users
Information security	Integrity	Network security
Personally identifiable information (PII)	Physical security	Security
SDLC		

## Annotated Bibliography

### Required Materials

To achieve the educational needs of this unit the following material is used:

#### Primary Material

Bayuk, J.L., Healey, J., Rohmeyer, P., Sachs, M.H., Schmidt, J. and Weiss, J., 2012. Cyber security policy guidebook. John Wiley & Sons.

Kritzinger, E. and Smith, E., 2008. Information security management: An information security

retrieval and awareness model for industry. *Computers & Security*, 27(5-6), pp.224-231.

### **Supportive material**

1. National Training Standard for Information Security Professionals at <http://www.sait.fsu.edu/resources/NSTISSI-4011.pdf> for more detailed information about minimum training requirements for INFOSEC professionals.
2. Internet Society – Histories of the Internet

<http://www.isoc.org/internet/history/brief.shtml>

3. CNSS National Information Assurance Glossary

[https://www.ncsc.gov/nittf/docs/CNSSI-4009\\_National\\_Information\\_Assurance.pdf](https://www.ncsc.gov/nittf/docs/CNSSI-4009_National_Information_Assurance.pdf)

4. Microsoft Security Development Lifecycle

<http://www.microsoft.com/security/sdl/>

5. The Role of a Chief Security Officer

<http://www.govtech.com/security/The-Role-of-Chief-Security-Officer-is-More-Vital-than-Ever.html>

## **Self-Assessment Exercises**

### **Exercise 2.1**

Assume that a security model is needed for the protection of information in your class. Using the CNSS model, examine each of the cells and write a brief statement on how you would address the three components of each cell.

### **Recommended time for the student to work**

15 hours

# INFORMATION SECURITY POLICY

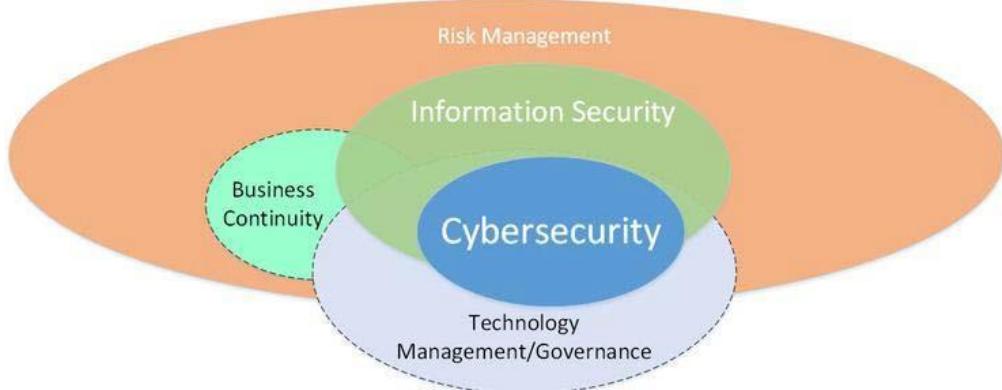
3<sup>rd</sup> Week

## Summary

Information security policies act as an outline for acceptable behavior and use of information. Policy functions as a low cost form of control for prevention of incidents involving information. Some of the basic rules that should be followed when creating a policy:

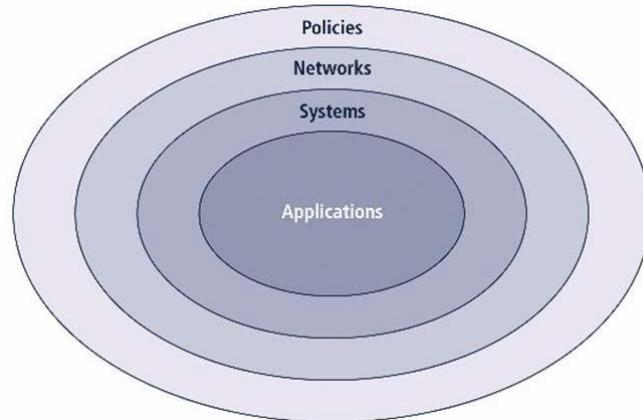
1. Policy should never conflict with law
2. Policy must be able to stand up in court if challenged
3. Policy must be properly supported and administered

Guidelines recommended by Bergeron and Berube on the creation of IT policy are followed: All policies must contribute to the success of the organization; Management must ensure the adequate sharing of responsibility for proper use of information systems; End users of information systems should be involved in the steps of policy formulation.



The four different layers of the bull's-eye model for prioritizing complex changes:

- a. Policies
- b. Networks
- c. Systems
- d. Applications



## Introductory Remarks

Policy is used in protecting an organization and its employees, by establishing acceptable use and allowed behaviors.

Policy can be described as a defined plan or course of action, intended to influence and determine decisions, actions, and other matters. Note that policy represents the formal statement of the organization's managerial philosophy. Policies are a set of rules that determine what behavior is acceptable and unacceptable within an organization. Policies must define what penalties exist for unacceptable behavior, as well as an appeals process.

A quality information security program begins and ends with policy.

Properly developed and implemented policies enable the information security program to function almost seamlessly within the workplace.

Although information security policies are the least expensive means of control to execute, they are often the most difficult to implement.

Some basic rules must be followed when shaping a policy:

- Policy should never conflict with law
- Policy must be able to stand up in court, if challenged
- Policy must be properly supported and administered

"All policies must contribute to the success of the organization."

Management must ensure the adequate sharing of responsibility for proper use of information systems.

End users of information systems should be involved in the steps of policy formulation.”

### The Bulls-eye Model

Bulls-eye model layers:

Policies—the outer layer in the bull’s-eye diagram

Networks—where threats from public networks meet the organization’s networking infrastructure

Systems—includes computers used as servers, desktop computers, and systems used for process control and manufacturing systems

Applications—includes all applications systems

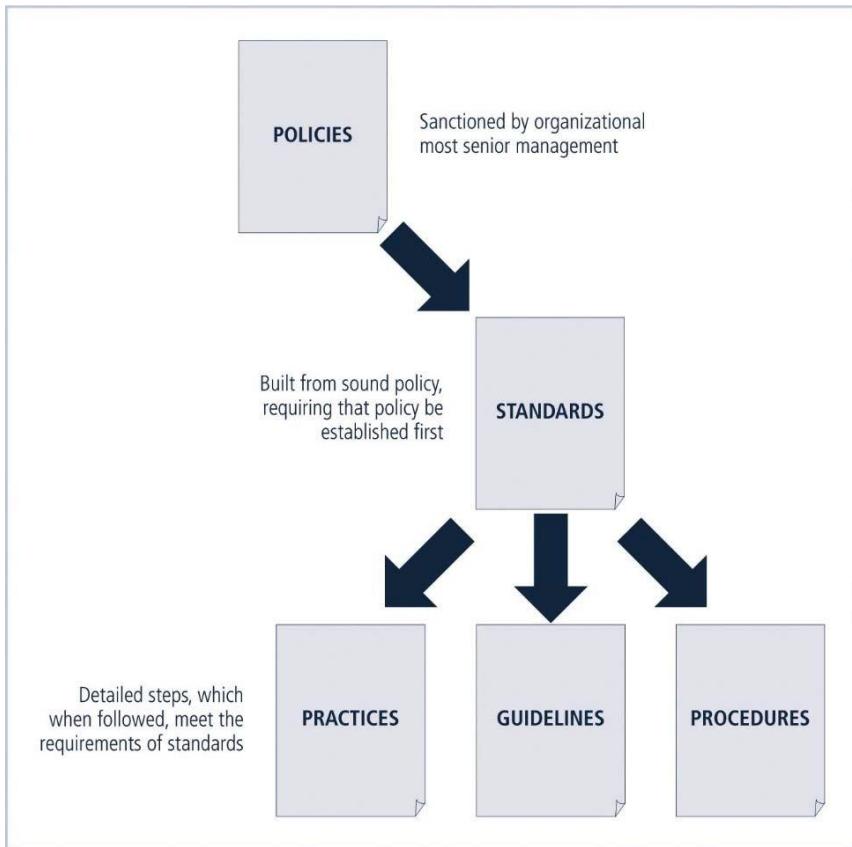
“...policies are important reference documents for internal audits and for the resolution of legal disputes about management’s due diligence [and] policy documents can act as a clear statement of management’s intent...”

### *Policy, Standards, and Practices*

Policy is “a plan or course of action, as of a government, political party, or business, intended to influence and determine decisions, actions, and other matters”.

A standard is a more detailed statement of what must be done to comply with policy.

Practices, procedures and guidelines explain how employees will comply with policy.



**FIGURE 4-2** Policies, Standards, and Practices

For policies to be effective they must be:

- properly disseminated
- read
- understood
- agreed-to

Policies require constant modification and maintenance.

In order to produce a complete information security policy, management must define three types of information security policy:

- Enterprise information security program policy
- Issue-specific information security policies
- Systems-specific information security policies

A standard can be described as a detailed statement of what must be done in order to comply with a policy. Practices, procedures, and guidelines determine how employees are to comply with

policy. The three types of policies that must be defined, according to NIST, often created in this order:

- Enterprise information security policy (EISP)
- Issue-specific security policies (ISSP)
- System-specific security policies (SysSP)

An enterprise information security policy (EISP) as a policy that sets the strategic direction, scope, and tone for all of an organization's security efforts. An EISP must support an organization's vision and mission statements, and that it must also be defensible if legal challenges arise. EISP plays an important role in stating the importance of information security, while it should not contradict the organizational mission statement.

The elements that should exist within an EISP document are:

- a. An overview of the corporate philosophy on security
- b. Information on the structure of the InfoSec organization and individuals who fulfill the InfoSec role
- c. Fully articulated responsibilities for security that are shared by all members of the organization
- d. Fully articulated responsibilities for security that are unique to each role within the organization

An issue-specific security policy (ISSP) is a policy that provides detailed, targeted guidance to instruct all members of the organization in the use of a resource. An ISSP should begin by introducing the organization's fundamental resource-use philosophy, and note that the ISSP typically includes more detail than higher level policy documents. An effective ISSP document accomplishes explaining how technology should be used, how technology is controlled, and should finally indemnifies the organization against liability for misuse.

The three characteristics that every ISSP should have are:

- a. To address specific technology-based resources
- b. To require frequent updates
- c. To contain an issue statement

The ISSP should begin with a clear statement of purpose that outlines the scope and applicability of the policy.

The authorized uses section of the policy is outlining who can use technology covered under the

policy, and for what purposes. The prohibited uses section is detailing what types of activities are not allowed. The systems management section is pertaining to users' relationships to systems management, and can cover proper use of e-mail and electronic documents, as well as storage of documents. The violations of policy section is outlining what actions will be taken as a result of violating a policy. The policy review and modification is involving the timetable and procedures for periodic review. The limitations of liability section is outlining the organization's liability and providing a set of disclaimers.

The three most common approaches for creating and managing ISSPs are as follows:

- a. Create a number of independent ISSP documents, each specifically tailored for a single issue
- b. Create a single comprehensive ISSP document that covers everything
- c. Create a modular ISSP document that unifies policy creation and administration while maintaining each specific issue's requirements

The recommended approach is the modular policy, due to the fact that a standard template can be used, while allowing for customization on specific issues.

The system-specific security policy (SysSP) IS being similar to a set of standards or procedures that must be followed when dealing with specific systems. There are two separate groups that can make up a SysSP: managerial guidance and technical specifications.

#### *Managerial Guidance SysSPs*

A managerial guidance SysSP document is created by management to guide implementation of new hardware and to address employee behavior. Any technology that can potentially affect the confidentiality, integrity, or availability of information must be evaluated using a SysSP.

#### *Technical Specification SysSPs*

A system administrator might need to create a different policy in order to implement a managerial policy, such as with passwords. There are two different methods for implementing technical controls:

- a. Access control lists are a list that allows or denies access based on authentication or types of network traffic.
- b. Configuration rules are instructional codes that guide the execution of a system as information is passing through it, and provide some examples, such as a firewall rule set.

Some of the privileges that can be assigned to a user within an ACL, such as:

- Read
- Write
- Execute
- Delete

Access control lists have been implemented on Linux-based and Microsoft Windows operating systems. A combination SysSP, takes the managerial SysSP document and combines it with the technical specifications SysSP.

#### *Guidelines for Effective Policy Development and Implementation*

The characteristics of a successful policy are as follows:

1. Developed using industry-accepted practices
2. Distributed using all appropriate methods
3. Read by all employees
4. Understood by all employees
5. Formally agreed to by act or affirmation
6. Uniformly applied and enforced

#### *Developing Information Security Policy*

The benefits of viewing the development process of an InfoSec policy in three parts, consisting of design and writing, policy approval, and the management process for distributing the policy throughout an organization. Issues can arise as a result of illiteracy or due to poor understanding of the native language in which a policy is written. Also challenges are faced by multinational organizations that must translate a policy into several languages.

It is important to ensure that employees will understand a policy, and jargon or technical terms should be kept to a minimum in order to ensure comprehension. Microsoft Word can be used to gather readability statistics for use in determining policy readability.

Policy compliance means that an employee must agree to a policy. Issues may arise if an employee refuses to agree to a policy, and some cases, this may be grounds for termination.

We can ensure policy enforcement, either by using punishment based or reward based systems.

The systems development life cycle (SDLC) can be used to develop a policy. Some of the different items that should be attained during the investigation phase of policy development are:

- a. Support from senior management

- b. Support and active involvement of IT management
- c. Clear articulation of goals
- d. Participation of the correct individuals
- e. A detailed outline of the scope of the policy development

The tasks that should occur at the analysis phase are:

- a. A new or recent risk assessment or IT audit
- b. The gathering of key reference materials

Some valuable resources for designing a policy can be found in:

- The Web
- Government sites
- Professional literature
- Peer networks
- Professional consultants

End-user license agreements (EULAs) have been used to outline fair use of software, and the typical steps available for a user to confirm acceptance of a EULA.

The implementation phase as the phase in which a policy development team writes the actual policies.

The maintenance phase is the phase in which policy is monitored, maintained, and modified as needed.

There are also automated policy management tools, such as the VigilEnt Policy Center (VPC) tool.

The VPC allows policy developers to create policy, manage the approval process with multiple individuals or groups, and distribute approved policy throughout their organizations.

NIST's Special Publication 800-18, Rev. 1, is a very enlightening document which describes a business process-centered approach to policy management. It is important to review existing policies on a schedule, as well as ensuring any policy revisions are properly dated.

Explain the role of a champion and a manager in the creation of policy, and note that the combination of these two roles is known as the policy administrator. It is important to use a proper review schedule, which is used to keep policies current. Note that a policy review should occur at least on a yearly basis. Allowing individuals to make recommendations for revisions to policy can

help a policy administrator improve a policy. Placing a proper timestamp on a policy, and properly dating revisions is also very important.

The use of policy is intended to improve employee productivity, and inform employees of acceptable / unacceptable behavior. An additional benefit of proper policy usage is the avoidance of litigation in the event of employee termination.

## Aim/Objectives

Week 3 introduces students to the concept of information security policies. Students will learn about the three different types of information security policies: enterprise information security policy, issue-specific security policy, and system-specific security policy. Elements of effective policy implementations are discussed as well.

## Learning Outcomes

In this chapter, students should be able to:

- Define information security policy and understand its central role in a successful information security program
- Describe the three major types of information security policy and discuss the major components of each
- Explain what is needed to implement effective policy
- Discuss the process of developing, implementing, and maintaining various types of information security policies

## Key Words

Enterprise information security policy (EISP)	Issue-specific security policies (ISSP)	System-specific security policies (SysSP)
Policy reading	Policy comprehension	Policy compliance
Policy enforcement		

## Annotated Bibliography

### Required Materials

To achieve the educational needs of this unit the following material is used:

#### Primary Material

Chapter 4 of Michael E. Whitman, Herbert J. Mattord, *Management of Information Security, Fifth Edition*. Cengage Learning, 2017, ISBN-13: 978-1-305-50125-6.

Bayuk, J.L., Healey, J., Rohmeyer, P., Sachs, M.H., Schmidt, J. and Weiss, J., 2012. Cyber security policy guidebook. John Wiley & Sons.

#### Supportive material

- SANS page containing security policy templates:  
<http://www.sans.org/security-resources/policies/>
- NIST Special Publication 800-18 Rev. 1 document, visit:  
<http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf>
- What is an Access Control List?:  
<http://searchsoftwarequality.techtarget.com/definition/access-control-list>
- The Systems Development Life Cycle  
[http://csrc.nist.gov/publications/nistbul/april2009\\_system-development-life-cycle.pdf](http://csrc.nist.gov/publications/nistbul/april2009_system-development-life-cycle.pdf)

## Self-Assessment Exercises

### Exercise 3.1

List and describe the three approaches to policy development presented in this chapter. In your opinion, which is best suited for use by a smaller organization and why? If the target organization were very much larger, which approach would be more suitable and why?

## Recommended time for the student to work

15 hours

# INFORMATION SECURITY GOVERNANCE

4<sup>th</sup> Week

## Summary

Role of cybersecurity and information security in the organization, levels of responsibility, the different personnel roles: information owner, information custodian, administrator, solution provider, change control, human resources, user. Certification and accreditation.

## Introductory Remarks

### *The Role of Planning*

Proper planning for information security is important, and we have seen the role of a chief information security officer (CISO) or chief security officer (CSO). Different groups that can be internal or external to an organization can also be involved in information security planning. A stakeholder is a person or organization that has a stake in a specific part of plan or operation. Stockholders are entities that hold stock in a particular organization.

It is important to understand an organization's planning process in order to ensure successful planning. Organizational planning should involve organizational leadership in the creation of general objectives in order to guide an organization's path, with the goal of creating detailed plans.

Important elements to be considered prior to planning, are specifically stating ethical, entrepreneurial, and philosophical perspectives.

A mission statement is used to indicate the primary business of an organization and its intended area of operations. Organizations may require the creation of a mission statement for each of its major departments, including the information security department.

Vision statement is a statement containing the aspirations of an organization and what it intends to achieve. A vision statement does not necessarily have to be realistic, but should serve to guide an organization's future.

The values statement, sets the standard by which an organization can evaluate itself and its current practices. Examples of values statements such as Microsoft's values statement can be found on its website.

Strategic planning is guiding an organization to the creation of specific goals, and re-iterate that a good strategic plan utilizes a top-down approach. A multilayered approach is used to accomplish the creation of a general strategy and contribute to overall strategic planning.

A strategic plan is created and we can observe how different levels of management would function in the top-down approach. For the organization's top management is important to fully understand the strategic goals of the organization, in order to create a strategic plan.

*The next step in strategic planning is to create tasks with objectives.* The strategic plan is used to create tactical plans, and that tactical plans are used to create operational plans. Tactical plans consist of specific, incremental objectives. As part of a tactical plan, we should include other plans such as project plans, resource acquisition planning documents, project budgets, project reviews, and monthly / annual reports. Tactical plans are sometimes called process project planning or intermediate planning, when they are created for a specific project. An operational plan is used to outline day-to-day tasks, and we will see what objectives may be included in an operational plan, such as the selection, configuration, and deployment of hardware, or the design and implementation of a SETA program.

A strategic plan should include some of the basic components of a typical strategic plan:

- a. Executive Summary
- b. Mission, Vision and Values Statement
- c. Organizational Profile and History
- d. Strategic Issues and Challenges
- e. Corporate Goals and Objectives
- f. Major Business Units Goals and Objectives
- g. Appendices - can assist in the identification of new directions or the elimination of unprofitable directions.

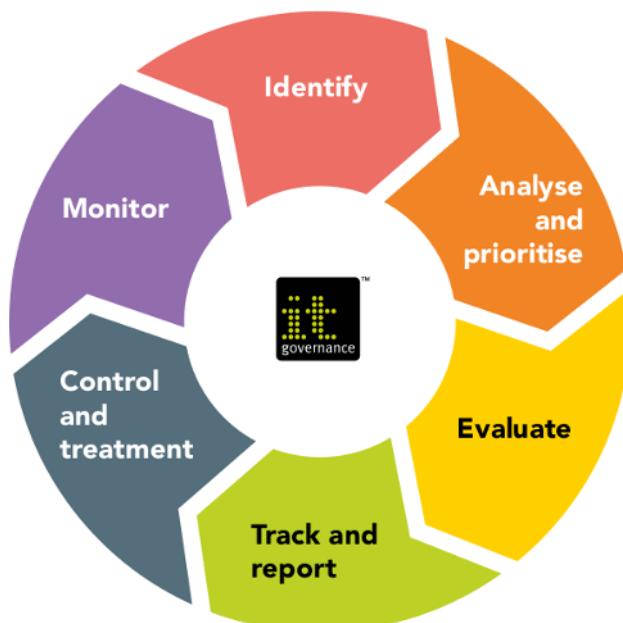
Governance, risk management and compliance (GRC) is the umbrella term covering an organization's approach across these three areas: Governance, risk management, and compliance. It is an approach to executive-level strategic planning.

Information Governance (IG) is a sort of super discipline that has emerged as a result of new and tightened legislation governing businesses, external threats such as hacking and data breaches, and the recognition that multiple overlapping disciplines were needed to address today's information management challenges in an increasingly regulated and litigated business environment. IG is a subset of corporate governance, and includes key concepts from records

management, content management, IT and data governance, information security, data privacy, risk management, litigation readiness, regulatory compliance, long-term digital preservation, and even business intelligence. This also means that it includes related technology and discipline subcategories, such as document management, enterprise search, knowledge management, and business continuity/ disaster recovery.

We define cyber risk assessment as the identification, analysis and evaluation of cyber risks. It studies and analyses the entire IT infrastructure and identifies possible vulnerabilities at the juncture of people, processes and technology, as well as vulnerabilities within the different systems. After the assessment has been made, the next logical step is risk management. Thus, a cyber risk management programme prioritises the identified risks in terms of likelihood of occurrence, then makes coordinated efforts to minimise, monitor and control the impact of those risks. "Cybersecurity Risk Management" means technologies, practices, and policies that address threats or vulnerabilities in networks, computers, programs and data, flowing from or enabled by connection to digital infrastructure, information systems, or industrial control systems, including but not limited to, information security, supply chain assurance, information assurance, and hardware and software assurance.

IT Governance defines cyber risk as any event that can lead to data breaches, financial loss, reputational damage, and disruption of operations caused by a failure of technology systems and procedures.



Risk management is an essential requirement of several of the most important information security standards and frameworks.

Information security is a managerial responsibility, and proper management involvement in ensuring information security.

### **Desired Outcomes**

The elements that are critical to information security governance, are effective communication, constructive relationships, common language, and shared commitment. The five basic outcomes of information security governance, and the National Association of Corporate Directors (NACD) recommendations on essential practices for boards of director are also important.

### **Benefits of Information Security Governance**

Some of the benefits of information security governance, are the increased share value or increased predictability and reduced uncertainty. Different aspects of an information security governance program that designers should consider, are the risk management methodology and effective security organizational structure.

### ***CERT Governing for Enterprise Security Implementation***

According to GES, the Enterprise Security Program (ESP) governance activities should be driven by a Board Risk Committee (BRC) in addition to the organization's executive management.

The three supporting documents included in the GES are:

- a. Article 1: Characteristics of Effective Security Governance
- b. Article 2: Defining an Effective Enterprise Security Program
- c. Article 3: Enterprise Security Governance Activities

### ***ISO/IEC 27014:2013 Governance of Information Security***

ISO 27014:2013 standard, specifies the following six high-level "action-oriented" information security governance principles:

- a. Establish organization-wide information security
- b. Adopt a risk-based approach
- c. Set the direction of investment decisions
- d. Ensure conformance with internal and external requirements
- e. Foster a security-positive environment
- f. Review performance in relation to business outcomes

The five governance processes promoted by the ISO 27014:2013 standard:

- a. Evaluate
- b. Direct
- c. Monitor
- d. Communicate
- e. Assure

The overall goals of governance as assessed in ISO/IEC 27014:2013 are:

- a. Alignment of objectives and strategies between the information security program and the overall organization
- b. Increased value added to the organization, its executive management, and stakeholders
- c. Effective assignment of risk to the appropriate responsible party

### *Security Convergence*

Security-related governance within organizations has merged over time, and accountability for information security has broadened across different management roles. Enterprise risk management (ERM) can be used to better align security functions with an organization's mission, including IT security and physical security elements.

### *Planning for Information Security Implementation*

The CIO and CISO play important roles in translating overall strategic planning into tactical and operational information security plans information security.

The CISO plays a more active role in the development of the planning details than does the CIO.

The job description for the Information Security Department Manager from Information Security Roles and Responsibilities Made Easy is:

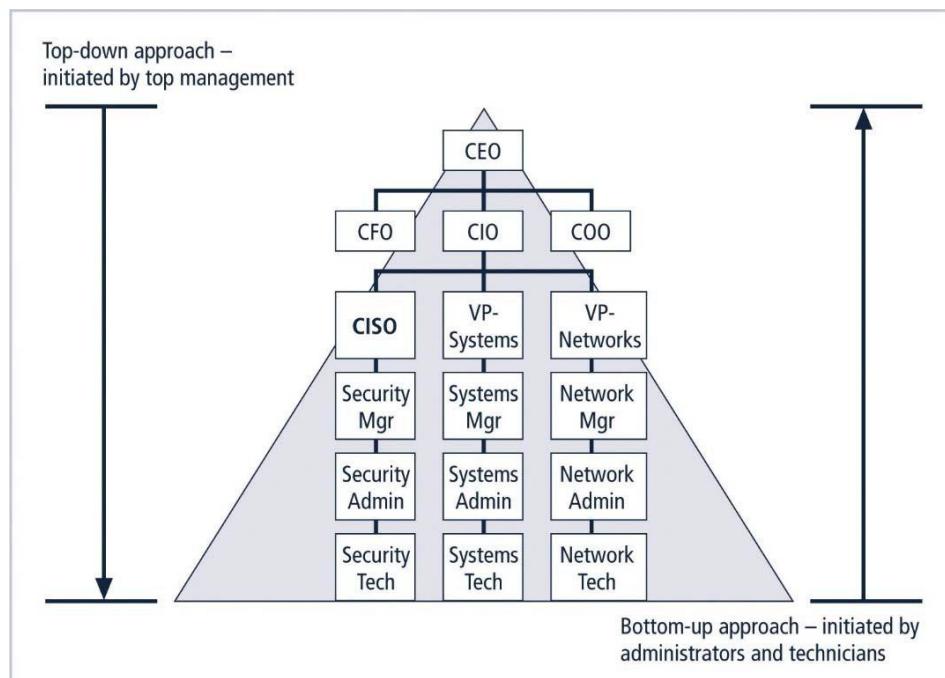
- Creates a strategic information security plan with a vision for the future of information security at Company X (utilizing evolving information security technology, this vision meets a variety of objectives such as management's fiduciary and legal responsibilities, customer expectations for secure modern business practices, and the competitive requirements of the marketplace)
- Understands the fundamental business activities performed by Company X, and based on this understanding, suggests appropriate information security solutions that uniquely protect these activities

- Develops action plans, schedules, budgets, status reports and other top management communications intended to improve the status of information security at Company X

Once the organization's overall strategic plan has been translated into IT and information security departmental objectives by the CIO, and then further translated into tactical and operational plans by the CISO, the implementation of information security can begin.

Implementation of information security can be accomplished in two ways: bottom-up or top-down. Define the bottom-up approach as involving system administrators who work to secure information systems without coordinated planning from upper management.

Compare the top-down approach to the bottom-up approach. Note the benefits that are available when supported by upper-management.



The top-down approach, in contrast, has strong upper management support, a dedicated champion, usually assured funding, a clear planning and implementation process, and the ability to influence organizational culture. High-level managers provide resources, give direction, issue policies, procedures and processes, dictate the goals and expected outcomes of the project, and determine who is accountable for each of the required actions. The most successful top-down approach also involves a formal development strategy referred to as the systems development life cycle. For any top-down approach to succeed, however, high-level management must buy

into the effort and provide all departments with their full support.

Such an initiative must have a champion—ideally, an executive with sufficient influence to move the project forward, ensure that it is properly managed, and push for acceptance throughout the organization. Involvement and support of the end users is also critical to the success of this type of effort.

A joint application design (JAD) team is a group of individuals who are affected by a project that are assigned to a team to assist in development. Recommended key steps for a JAD, are the identification of project objectives and limitations, or identification of critical success factors.

### *Introduction to the Security Systems Development Life Cycle*

The general systems development life cycle (SDLC) is a methodology for the design and implementation of an information system in an organization widely used in IT organizations.

A methodology is a formal approach to solving a problem based on a structured sequence of procedures. Using a methodology ensures a rigorous process, and increases the likelihood of achieving the desired final objective.

The impetus to begin a SDLC-based project may be event-driven, that is, started in response to some event in the business community, inside the organization, or within the ranks of employees, customers or other stakeholders. Or it could be plan-driven, that is, the result of a carefully developed planning strategy.

At the end of each phase, a structured review or reality check takes place, during which the team and its management-level reviewers determine if the project should be continued, discontinued, outsourced, or postponed until additional expertise or organizational knowledge is acquired.

#### **Investigation**

It identifies the problem that the system being developed is to solve.

Beginning with an examination of the event or plan that initiates the process, the objectives, constraints, and scope of the project are specified.

A preliminary cost/benefit analysis is developed to evaluate the perceived benefits and the appropriate costs for those benefits.

#### **Analysis**

The analysis phase begins with the information learned during the investigation phase. This phase assesses the organization's readiness, its current systems status, and its capability to implement

and then support the proposed systems.

Analysts determine what the new system is expected to do, and how it will interact with existing systems.

### **Logical Design**

In the logical design phase, the information obtained during the analysis phase is used to create a proposed system-based solution for the business problem.

Based on the business need, the team selects systems and/or applications capable of providing the needed services.

Finally, based on all of the above, the team selects specific types of technical controls that might prove useful when implemented as a physical solution.

The logical design is the implementation independent blueprint for the desired solution.

### **Physical Design**

During the physical design phase, the team selects specific technologies that support the alternatives identified and evaluated in the logical design.

The selected components are evaluated further as a make-or-buy decision, then a final design is chosen that integrates the various required components and technologies.

### **Implementation**

In the implementation phase, the organization's software engineers develop any software that is not to be purchased, and take steps to create integration modules.

These customized elements are tested and documented.

Users are trained and supporting documentation is created.

Once all components have been tested individually, they are installed and tested.

### **Maintenance**

This phase consists of the tasks necessary to support and modify the system for the remainder of its useful life cycle.

Periodically, the system is tested for compliance, and the feasibility of continuance versus discontinuance is evaluated.

Upgrades, updates, and patches are managed.

When the current system can no longer support the changed mission of the organization, it is terminated and a new systems development project is undertaken.

### **The Security Systems Development Life Cycle (SecSDLC)**

The security systems development life cycle (SecSDLC), may differ in several specific activities, but the overall methodology is the same.

The SecSDLC process involves the identification of specific threats and the risks that they represent, and the subsequent design and implementation of specific controls to counter those threats and assist in the management of the risk.

#### **Investigation in the SecSDLC**

The investigation phase of the SecSDLC begins with a directive from upper management specifying the process, outcomes, and goals of the project, as well as its budget and other constraints.

Frequently, this phase begins with the affirmation or creation of security policies on which the security program of the organization is or will be founded.

Teams of managers, employees, and contractors are assembled to analyze problems, define their scope, specify goals and objectives, and identify any additional constraints not covered in the enterprise security policy.

Finally, an organizational feasibility analysis determines whether the organization has the resources and commitment to conduct a successful security analysis and design.

#### **Analysis in the SecSDLC**

The development team created during the investigation phase conducts a preliminary analysis of existing security policies or programs, along with documented current threats and associated controls.

This phase also includes an analysis of relevant legal issues that could affect the design of the security solution.

The risk management task also begins in this stage.

#### **Risk Management**

Risk management is the process of identifying, assessing, and evaluating the levels of risk facing the organization, specifically the threats to the organization's security and to the information

stored and processed by the organization.

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

To better understand the analysis phase of the SecSDLC, you should know something about the kinds of threats facing organizations in the modern, connected world of information technology (or IT).

In this context, a threat is an object, person, or other entity that represents a constant danger to an asset.

Table 2-1 – Threats to Information Security:

Categories of threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Deviations in quality of service from service providers	Power and WAN service issues
9. Forces of nature	Fire, flood, earthquake, lightning
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies

An attack is a deliberate act that exploits a vulnerability.

It is accomplished by a threat agent that damages or steals an organization's information or physical asset.

An exploit is a technique or mechanism used to compromise a system.

A vulnerability is an identified weakness of a controlled system in which necessary controls are not present or are no longer effective.

An attack is the use of an exploit to achieve the compromise of a controlled system.

Common attacks include:

- Malicious code.
- Hoaxes
- Back doors.
- Password crack.
- Brute force.
- Dictionary.
- Denial-of-service (DoS) and distributed denial-of-service (DDoS).
- Spoofing.
- Man-in-the-middle
- Spam.
- Mail bombing.
- Sniffer.
- Social engineering.
- Buffer overflow
- Timing.

The last step in knowing the enemy is to find some method of prioritizing the risk posed by each category of threat and its related methods of attack.

This can be done by adopting threat levels from an existing study of threats, or by creating your own categorization of threats for your environment based on scenario analyses.

To manage risk, you must identify and assess the value of your information assets.

This iterative process must include a classification and categorization of all of the elements of an organization's systems: people, procedures, data and information, software, hardware and networking elements.

The next challenge in the analysis phase is to review each information asset for each threat it faces and create a list of the vulnerabilities.

As the analysis phase continues, the next task is to assess the relative risk for each of the information assets.

We accomplish this by a process called risk assessment or risk analysis.

Risk assessment assigns a comparative risk rating or score to each specific information asset.

Risk management is the part of the analysis phase that identifies vulnerabilities in an organization's information systems and takes carefully reasoned steps to assure the confidentiality, integrity, and availability of all the components in the organization's information system.



### Design in the SecSDLC

The design phase actually consists of two distinct phases, the logical design and the physical design.

In the logical design phase, team members create and develop the blueprint for security, and examine and implement key policies that influence later decisions.

In the physical design phase, team members evaluate the technology needed to support the security blueprint, generate alternative solutions, and agree upon a final design.

Between the of logical and physical design phases, a security manager may seek to use established security models to guide the design process.

Security models provide frameworks for ensuring that all areas of security are addressed; organizations can adapt or adopt a framework to meet their own information security needs.

One of the design elements of the information security program is the information security policy of the organization.

Management must define three types of security policy:

1. General or security program policy,

2. Issue-specific security policies and
3. Systems-specific security policies.

Another integral part of the information security program to be designed is the security education and training (SETA) program.

The SETA program consists of three elements: security education, security training, and security awareness.

The purpose of SETA is to enhance security by

1. Improving awareness of the need to protect system resources;
2. developing skills and knowledge so computer users can perform their jobs more securely and
3. building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems.”

As the design phase continues, attention turns to the design of the controls and safeguards used to protect information from attacks by threats.

There are three categories of controls:

- Managerial controls address the design and implementation of the security planning process and security program management. Management controls also addresses risk management and security controls reviews.
- Operational Controls cover management functions and lower level planning, such as disaster recovery and incident response planning. Operational controls also address personnel security, physical security and the protection of production inputs and outputs.
- Technical Controls address those tactical and technical issues related to designing and implementing security in the organization. Here the technologies necessary to protect information are examined and selected.

Another element of the design phase is the creation of essential preparedness documents.

- Contingency planning (CP) is the entire planning conducted by the organization to prepare for, react to and recover from events that threaten the security of information and information assets in the organization, and the subsequent restoration to normal business operations.
- Incident response planning (IRP) is the planning process associated with the identification, classification, response, and recovery from an incident.
- Disaster recovery planning (DRP) is the planning process associated with the preparation for and recovery from a disaster, whether natural or man-made.

- Business continuity planning (BCP) is the planning process associated with ensuring that critical business functions continue if a catastrophic incident or disaster occurs.

As the design phase progresses, attention now focuses on physical security, which addresses the design, implementation, and maintenance of countermeasures that protect the physical resources of an organization.

Physical resources include people, hardware, and the supporting system elements and resources associated with the management of information in all its states, transmission, storage, and processing.

### **Implementation in the SecSDLC**

The security solutions are acquired, tested, implemented, and tested again.

Personnel issues are evaluated and specific training and education programs conducted.

Perhaps the most important element of the implementation phase is the management of the project plan.

The major steps in executing the project plan are

- 1) planning the project,
- 2) supervising the tasks and action steps within the project plan, and
- 3) wrapping up the project plan.

Information security is a field with a vast array of technical and non-technical requirements.

The project team should consist of a number of individuals who are experienced in one or multiple requirements of both the technical and non-technical areas.

- The champion
- The team leader
- Security policy developers
- Risk assessment specialists
- Security professionals
- Systems administrators
- End users.

Just as each potential employee and potential employer look for the best fit, each organization should examine the options possible for staffing of the information security function.

- First, the entire organization must decide how to position and name the security function within

the organization.

- Second, the information security community of interest must plan for the proper staffing (or adjustments to the staffing plan) for the information security function.
- Third, the IT community of interest must understand the impact of information security across every role in the IT function and adjust job descriptions and documented practices accordingly.
- Finally, the general management community of interest must work with the information security professionals to integrate solid information security concepts into the personnel management practices of the organization.

It takes a wide range of professionals to support a diverse information security program

- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)
- Security Managers
- Security Technicians
- Data Owners
- Data Custodians
- Data Users

Many organizations seek professional certification so that they can more easily identify the proficiency of job applicants:

- CISSP
- SSCP
- GIAC
- SCP
- ICSA
- Security +
- CISM

### **Maintenance and Change in the SecSDLC**

Once the information security program is implemented, it must be operated, properly managed, and kept up to date by means of established procedures.

If the program is not adjusting adequately to the changes in the internal or external environment, it may be necessary to begin the cycle again.

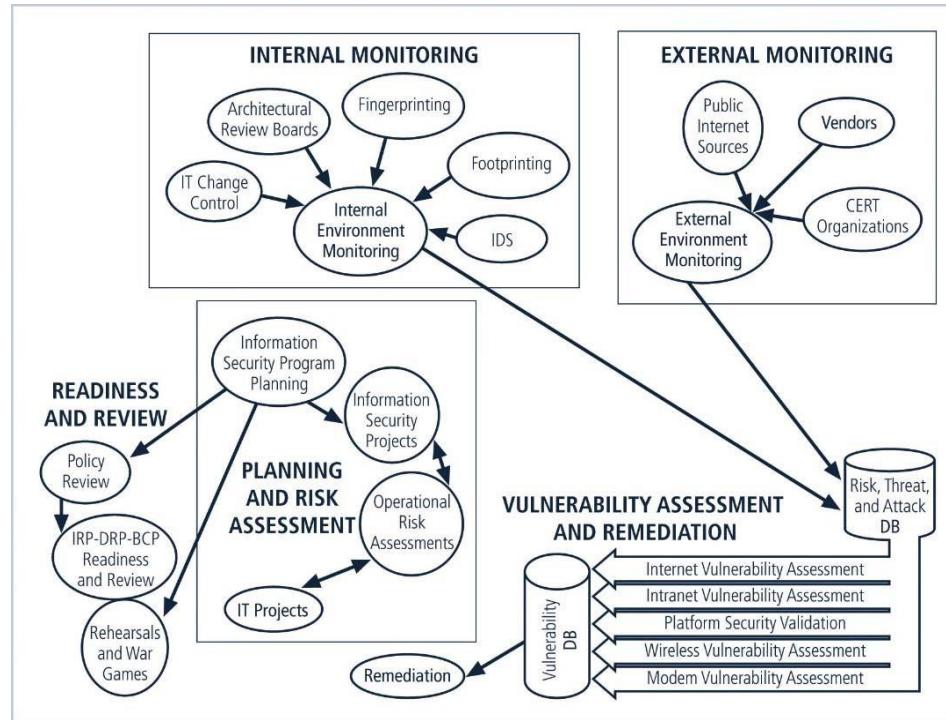
While a systems management models is designed to manage and operate systems, a

maintenance model is intended to complement a systems management model and focus organizational effort on system maintenance.

- External monitoring.
- Internal monitoring. .
- Planning and risk assessment.
- Vulnerability assessment and remediation
- Readiness and review.
- Vulnerability assessment

One of the maintenance issues that must be planned in the SecSDLC is the systems management model that will be used. The ISO management model is a five-area approach that provides structure to the administration and management of networks and systems. These five areas are:

- Fault management
- Configuration and name management
- Accounting management
- Performance management
- Security management



Fault Management. Involves identifying and addressing faults in the applied information security

profile and then addressing them. Also, the monitoring and resolution of user complaints.

**Configuration and Change Management.** The administration of various components involved in the security program as well as changes in the strategy, operation, or components of the information security program.

**Accounting and Auditing Management** involves chargeback accounting, and systems monitoring. Chargeback accounting happens when organizations internally charge their departments for system use. While chargebacks are seldom used today, certain kinds of resource usage are commonly tracked—such as those on a computing system (like a server or a desktop computer) or human effort-hours—to recover IT costs from non-IT units of the organization. Accounting management involves monitoring the use of a particular component of a system. In networking, this monitoring may simply determine which users are using which resources. However, in security, it may be easy to track which resources are being used but difficult to determine who is using them, at which point, accounting management begins to overlap with performance management, which is addressed in the next section. With accounting management you begin to determine optimal points of systems use as indicators for upgrade and improvement. Auditing is the process of reviewing the use of a system, not to determine its performance, but to determine if misuse or malfeasance has occurred.

**Performance Management.** Because many information security technical controls are implemented on common IT processors, they are affected by the same factors as most computer-based technologies. It is therefore important to monitor the performance of security systems and their underlying IT infrastructure to determine if they are effectively and efficiently doing the job they were implemented to do. Some information security control systems, such as Internet usage monitors that look for inappropriate use of Internet resources, operate as pass-by devices.

**Security Program Management.** Once an information security program is functional it must be operated and managed. The ISO five-area framework provides some structure for a management model; however, it focuses on ensuring that various areas are addressed, rather than guiding the actual conduct of management. In order to assist in the actual management of information security programs, a formal management standard can provide some insight into the processes and procedures needed. This could be based on the BS7799/ISO17799 model or the NIST models described earlier.

## **Comparing the SDLC and the SecSDLC**

Table 2-2:

	Steps common to the SDLC and the SecSDLC	Steps unique to the SecSDLC
Phase 1: Investigation	<ul style="list-style-type: none"> <li>■ Outline project scope/goals</li> <li>■ Estimate costs</li> <li>■ Evaluate existing resources</li> <li>■ Analyze feasibility</li> </ul>	<ul style="list-style-type: none"> <li>■ Define project process and goals and document them in the program security policy</li> </ul>
Phase 2: Analysis	<ul style="list-style-type: none"> <li>■ Assess current system against plan developed in Phase 1</li> <li>■ Develop preliminary system requirements</li> <li>■ Study integration of new system with existing system</li> <li>■ Document findings and update feasibility analysis</li> </ul>	<ul style="list-style-type: none"> <li>■ Analyze existing security policies and programs</li> <li>■ Analyze current threats and controls</li> <li>■ Examine legal issues</li> <li>■ Perform risk analysis</li> </ul>
Phase 3: Logical Design	<ul style="list-style-type: none"> <li>■ Assess current business needs against plan developed in Phase 2</li> <li>■ Select applications, data support, and structures</li> <li>■ Generate multiple solutions for selection of best</li> <li>■ Document findings and update feasibility analysis</li> </ul>	<ul style="list-style-type: none"> <li>■ Develop security blueprint</li> <li>■ Plan incident response actions</li> <li>■ Plan business response to disaster</li> <li>■ Determine feasibility of continuing and/or outsourcing the project</li> </ul>
Phase 4: Physical Design	<ul style="list-style-type: none"> <li>■ Select technologies to support solutions developed in Phase 3</li> <li>■ Select the best solution</li> <li>■ Decide whether to make or buy components</li> <li>■ Document findings and update feasibility analysis</li> </ul>	<ul style="list-style-type: none"> <li>■ Select technologies needed to support security blueprint</li> <li>■ Develop definition of successful solution</li> <li>■ Design physical security measures to support technological solutions</li> <li>■ Review and approve project</li> </ul>
Phase 5: Implementation	<ul style="list-style-type: none"> <li>■ Develop or buy software</li> <li>■ Order components</li> <li>■ Document system</li> <li>■ Train users</li> <li>■ Update feasibility analysis</li> <li>■ Present system to users</li> <li>■ Test system and review performance</li> </ul>	<ul style="list-style-type: none"> <li>■ Buy or develop security solutions</li> <li>■ At end of phase, present tested package to management for approval</li> </ul>
Phase 6: Maintenance	<ul style="list-style-type: none"> <li>■ Support and modify system for its useful life</li> <li>■ Test periodically for compliance with business needs</li> <li>■ Upgrade and patch as necessary</li> </ul>	<ul style="list-style-type: none"> <li>■ Constantly monitor, test, modify, update, and repair to respond to changing threats</li> </ul>

## Aim/Objectives

In week 4, students are introduced to the different roles within an organization that are involved in the planning process, and how the planning process is applied to information security. The reader will come to recognize the importance of planning and learn the principal components of

organizational planning as well as gaining an understanding of the principal components of information security system implementation planning as it functions within the organizational planning scheme. The different aspects of creating a plan are covered, as well as tactical planning and operational planning. Information security governance and its benefits are discussed. Finally, students will learn about the security systems development life cycle.

## Learning Outcomes

In this chapter, students should be able to:

- Identify the roles in organizations that are active in planning
- Explain strategic organizational planning for information security (InfoSec)
- Recognize the importance of planning and describe the principal components of organizational planning.
- Know and understand the principal components of information security system implementation planning as it functions within the organizational planning scheme.
- Discuss the importance, benefits, and desired outcomes of information security governance and how such a program would be implemented
- Explain the principal components of InfoSec system implementation planning in the organizational planning scheme

## Key Words

Systems development life cycle (SDLC)	Security systems development life cycle (SecSDLC)	Chief Information Officer (CIO)
Chief Information Security Officer (CISO)	Security Convergence	ISO/IEC 27014
Information Governance (IG)		

## Annotated Bibliography

### Required Materials

To achieve the educational needs of this unit the following material is used:

#### Primary Material

Chapter 3 of Michael E. Whitman, Herbert J. Mattord, *Management of Information Security, Fifth Edition*. Cengage Learning, 2017, ISBN-13: 978-1-305-50125-6.

Bayuk, J.L., Healey, J., Rohmeyer, P., Sachs, M.H., Schmidt, J. and Weiss, J., 2012. Cyber security policy guidebook. John Wiley & Sons.

ISACA 2006. Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition

#### Supportive material

Von Solms, B. and Von Solms, R., 2004. The 10 deadly sins of information security management. Computers & Security, 23(5), pp.371-376.

Flores, W.R., Antonsen, E. and Ekstedt, M., 2014. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Computers & Security, 43, pp.90-110.

Coertze, J. and von Solms, R., 2012, November. A model for information security governance in developing countries. In International Conference on e-Infrastructure and e-Services for Developing Countries (pp. 279-288). Springer, Berlin, Heidelberg.

For more examples of mission statements, see the following page:

1. [http://www.missionstatements.com/fortune\\_500\\_mission\\_statements.html](http://www.missionstatements.com/fortune_500_mission_statements.html)
2. Information Security Governance Guide:<http://searchsecurity.techtarget.com/tutorial/Information-Security-Governance-Guide>
3. The IDEAL Model: <http://www.sei.cmu.edu/library/assets/idealmodel.pdf>
4. The Systems Development Life Cycle.  
[http://csrc.nist.gov/publications/nistbul/april2009\\_system-development-life-cycle.pdf](http://csrc.nist.gov/publications/nistbul/april2009_system-development-life-cycle.pdf)

## **Self-Assessment Exercises**

### **Exercise 4.1**

Information security management and governance are not simply implemented tasks within organizations. An information security governance program is a program that must be thoroughly planned, include senior-level management involvement and guidance, be implemented throughout the organization, and be updated and maintained. The International Organization for Standards (ISO) and the International Electrotechnical Commission (IEC) has created information security governance standards. Review the information security governance information provided by ISACA, located [here](#).

Write a 3-6 page paper in which you:

1. Define the information security governance and management tasks that senior management needs to address.
2. Describe the outcomes and the items that will be delivered to the organization through the information security program.
3. Develop a list of at least five (5) best practices for implementing and managing an information security governance program within an organization.
4. Develop a checklist of items that needs to be addressed by senior management, including priorities and needed resources.
5. Use at least three (3) quality resources in this assignment. Note: Wikipedia and similar Websites do not qualify as quality resources.

Your assignment must follow these formatting requirements:

- Be typed, double spaced, using Times New Roman font (size 12), with one-inch margins on all sides; references must follow APA or school-specific format. Check with your professor for any additional instructions.
- Include a cover page containing the title of the assignment, the student's name, the professor's name, the course title, and the date. The cover page and the reference page are not included in the required page length.

## **Recommended time for the student to work**

15 hours

## RISK MANAGEMENT: IDENTIFYING AND ASSESSING RISK

5<sup>th</sup> Week

### Summary

An aspiring information security professional will have a key role to play in risk management. The IT community must serve the information technology needs of the broader organization and, at the same time, leverage the special skills and insights of the information security community. The information security team must lead the way with skill, professionalism, and flexibility as it works with the other communities of interest to appropriately balance the usefulness and security of the information system. In the past, an organization could establish a competitive business model, method, or technique to provide a product or service that was superior and create a competitive advantage. In order to keep up with the competition, organizations must design and create a safe environment in which business processes and procedures can function. This environment must maintain the confidentiality, privacy, and integrity of organizational data.

### Introductory Remarks

Risk management is the process of identifying vulnerabilities in an organization's information systems and taking carefully reasoned steps to ensure the confidentiality, integrity, and availability of all the components in the organization's information system. Information security departments are created primarily to manage IT risk.

Managing risk is one of the key responsibilities of every manager within the organization.

In any well-developed risk management program, two formal processes are at work:

- risk identification and assessment
- risk control

Risk management requires three major undertakings: risk identification, risk assessment, and risk control. Risk identification, which is the process of examining and documenting the security posture of an organization's information technology and the risks it faces. Risk control, which is the application of controls that reduce the risks to an organization's information systems.

We must first know ourselves by identifying, examining, and understanding the information and

systems currently in place. In order to protect our assets, defined here as the systems that use, store, and transmit information, we have to understand everything about the information. The policies, education and training programs, and technologies that protect information must be carefully maintained and administered to ensure they remain effective.

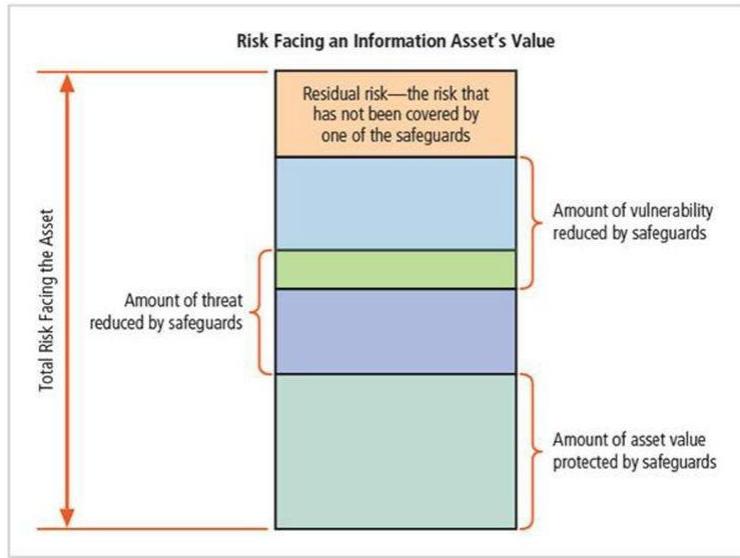
For information security, knowing the enemy means identifying, examining, and understanding the threats that most directly affect our organization and the security of our organization's information assets. We can use our understanding of these aspects to create a list of threats prioritized by importance to the organization.

Each community of interest must manage the risks the organization encounters. Information security understands the threats and attacks that introduce risk into the organization, so, they often take a leadership role. Management and users play a part in the early detection and response process; ensure that sufficient resources are allocated. The information technology community assists in building secure systems and operating them safely. General management, IT management, and information security management are collectively accountable for identifying and classifying all levels of risk. The three communities of interest that are also responsible for the following:

- Evaluating current and proposed risk controls
- Determining which control options are cost effective for the organization
- Acquiring or installing the needed controls
- Ensuring that the controls remain effective

Risk appetite is the amount of risk an organization is willing to accept as they evaluate the trade-offs between perfect security and unlimited accessibility. Residual risk is defined as the amount of risk that remains to an information asset even after the organization has applied its desired level of controls.

## Figure 5-3 Residual risk



### Risk Identification

A risk management strategy calls on information security professionals to identify, classify, and prioritize their organizations' information assets.

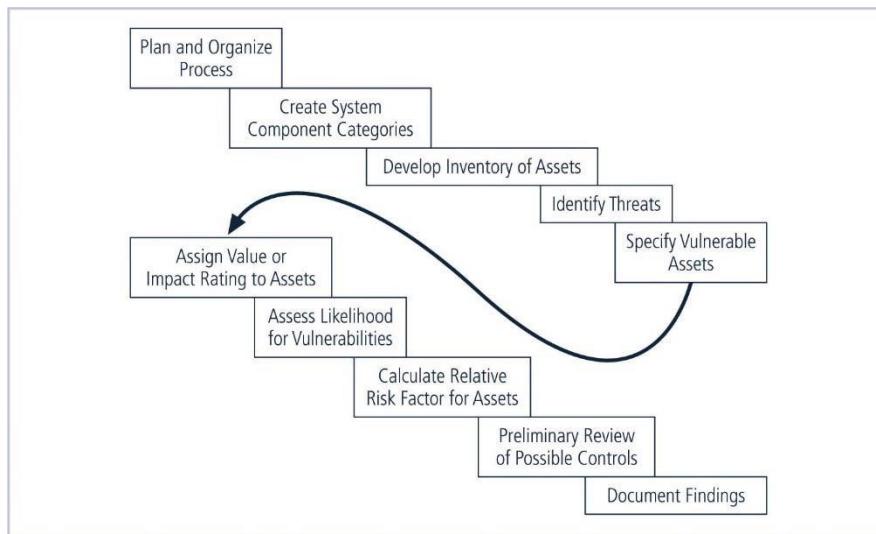
Risk identification begins with the process of self-examination.

At this stage, managers identify the organization's information assets, classify them into useful groups, and prioritize them by their overall importance.

### Creating an Inventory of Information Assets

The risk identification process begins with the identification of information assets, including people, procedures, data and information, software, hardware, and networking elements.

This step should be done without pre-judging the value of each asset; values will be assigned later in the process.



**FIGURE 7-1** Risk Identification Process

**TABLE 7-1** Organizational Assets Used in Systems

IT system components	Risk management components
People	People inside an organization Trusted employees Other staff
	People outside an organization People at organizations we trust Strangers
Procedures	Procedures IT and business standard procedures IT and business sensitive procedures
Data	Data/Information Transmission Processing Storage
Software	Software Applications Operating systems Security components
Hardware	Hardware Systems and peripherals Security devices
Networking	Networking components Intranet components Internet or Extranet components

### Identifying Hardware, Software, and Network Assets

Whether automated or manual, the inventory process requires a certain amount of planning.

Most importantly, you must determine which attributes of each of these information assets should be tracked.

That determination will depend on the needs of the organization and its risk management efforts, as well as the preferences and needs of the information security and information technology

communities.

When deciding which attributes to track for each information asset, consider the following list of potential attributes:

- Name
- IP address
- MAC address
- Asset type
- Serial number
- Manufacturer name
- Manufacturer's model or part number
- Software version, update revision, or FCO number
- Physical location
- Logical location
- Controlling entity

#### Identifying People, Procedures, and Data Assets

Responsibility for identifying, describing, and evaluating these information assets should be assigned to managers who possess the necessary knowledge, experience, and judgment.

As these assets are identified, they should be recorded via a reliable data-handling process like the one used for hardware and software.

- People
- Position name/number/ID
- Supervisor name/number/ID
- Security clearance level
- Special skills
- Procedures
- Description
- Intended purpose
- Software/hardware/networking elements to which it is tied
- Location where it is stored for reference
- Location where it is stored for update purposes
- Data
- Classification

- Owner/creator/manager
- Size of data structure
- Data structure used
- Online or offline
- Location
- Backup procedures

### Classifying and Categorizing Assets

Once the initial inventory is assembled, you must determine whether its asset categories are meaningful to the organization's risk management program.

The inventory should also reflect the sensitivity and security priority assigned to each information asset.

A classification scheme should be developed that categorizes these information assets based on their sensitivity and security needs, i.e. confidential, internal, and public.

Each of these classification categories designates the level of protection needed for a particular information asset.

Some asset types, such as personnel, may require an alternative classification scheme that would identify the information security processes used by the asset type.

Classification categories must be comprehensive and mutually exclusive.

### Assessing Values for Information Assets

As each information asset is identified, categorized, and classified, a relative value must also be assigned to it.

Relative values are comparative judgments made to ensure that the most valuable information assets are given the highest priority when managing risk.

- Which information asset is the most critical to the success of the organization?
- Which information asset generates the most revenue?
- Which information asset generates the highest profitability?
- Which information asset is the most expensive to replace?
- Which information asset is the most expensive to protect?
- Which information asset's loss or compromise would be the most embarrassing or cause the greatest liability?

System Name: <u>SLS E-Commerce</u>	Date Evaluated: <u>February 2003</u>	Evaluated By: <u>D. Jones</u>
<b>Information assets</b>	<b>Data classification</b>	<b>Impact to profitability</b>
<b>Information Transmitted:</b>		
EDI Document Set 1 — Logistics BOL to outsourcer (outbound)	Confidential	High
EDI Document Set 2 — Supplier orders (outbound)	Confidential	High
EDI Document Set 2 — Supplier fulfillment advice (inbound)	Confidential	Medium
Customer order via SSL (inbound)	Confidential	Critical
Customer service Request via e-mail (inbound)	Private	Medium
<b>DMZ Assets:</b>		
Edge Router	Public	Critical
Web server #1—home page and core site	Public	Critical
Web server #2—Application server	Private	Critical
Notes: BOL: Bill of Lading DMZ: Demilitarized Zone EDI: Electronic Data Interchange SSL: Secure Sockets Layer		

**FIGURE 7-2** Sample Asset Classification Worksheet

### Listing Assets in Order of Importance

The final step in the risk identification process is to list the assets in order of importance.

This goal can be achieved by using a weighted factor analysis worksheet.

### Data Classification Model

Corporate and military organizations use a variety of classification schemes.

Data owners must classify the information assets for which they are responsible.

Data owners must review these classifications periodically to ensure that the data are still classified correctly and the access controls are in place.

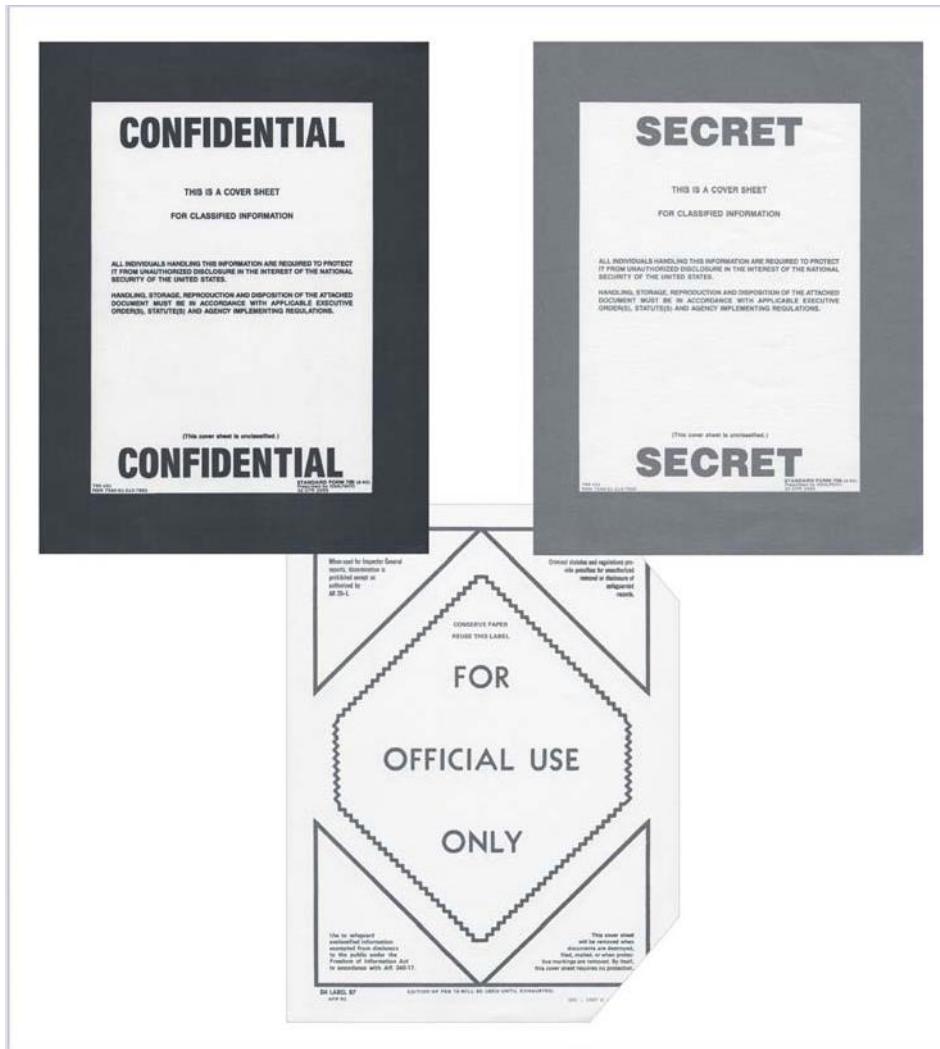
### For Example:

- Public
- For official use only
- Sensitive
- Classified

As you might expect, the U.S. military classification scheme relies on a more complex categorization system than the schemes of most corporations.

For most information, the U.S. military uses a five-level classification scheme as defined in Executive Order 12958:

- Unclassified Data:
- Sensitive But Unclassified (SBU) Data:
- Confidential Data:
- Secret Data:
- Top Secret Data:



**FIGURE 7-3** Military Data Classification Cover Sheets

### Security Clearances

The other part of the data classification scheme is the personnel security clearance structure, in which each user of an information asset is assigned an authorization level that indicates the level

of information classification he or she can access.

Most organizations have developed a set of roles and corresponding security clearances, so that individuals are assigned authorization levels that correlate with the classifications of the information assets.

Beyond a simple reliance on the security clearance of the individual is the need-to-know principle.

Regardless of one's security clearance, an individual is not allowed to view data simply because it falls within that individual's level of clearance.

That is, after an individual is granted a security clearance but before he or she is allowed access to a specific set of data, that person must also meet the need-to-know requirement.

#### Management of the Classified Information Asset

Managing an information asset includes considering the storage, distribution, portability, and destruction of that information asset. An information asset that has a classification designation other than unclassified or public must be clearly marked as such.

Classified documents must be available only to authorized individuals - locking cabinets, safes, etc.

To maintain the confidentiality of classified documents, managers can implement a clean desk policy.

When copies of classified information are no longer valuable or too many copies exist, care should be taken to destroy them properly to discourage dumpster diving.

#### Military Data Classification Cover Sheets

#### Threat Identification

Any organization typically faces a wide variety of threats.

If you assume that every threat can and will attack every information asset, then the project scope becomes too complex.

To make the process less unwieldy, each step in the threat identification and vulnerability identification processes is managed separately and then coordinated at the end.

#### Identify and Prioritize Threats and Threat Agents

Each of these threats presents a unique challenge to information security and must be handled with specific controls that directly address the particular threat and the threat agent's attack

strategy.

Before threats can be assessed in the risk identification process, however, each threat must be further examined to determine its potential to affect the targeted information asset.

In general, this process is referred to as a threat assessment.

**TABLE 7-3** Threats to Information Security

Threat	Example
Act of human error or failure	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
Deliberate acts of information extortion	Blackmail for information disclosure
Deliberate acts of sabotage or vandalism	Destruction of systems or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros, denial-of-service
Forces of nature	Fire, flood, earthquake, lightning
Quality of service deviations from service providers	Power and WAN quality of service issues
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

Source: ©2003 ACM, Inc., Included here by permission.

### Vulnerability Assessment

Once you have identified the information assets of the organization and documented some threat assessment criteria, you can begin to review every information asset for each threat.

This review leads to the creation of a list of vulnerabilities that remain potential risks to the organization.

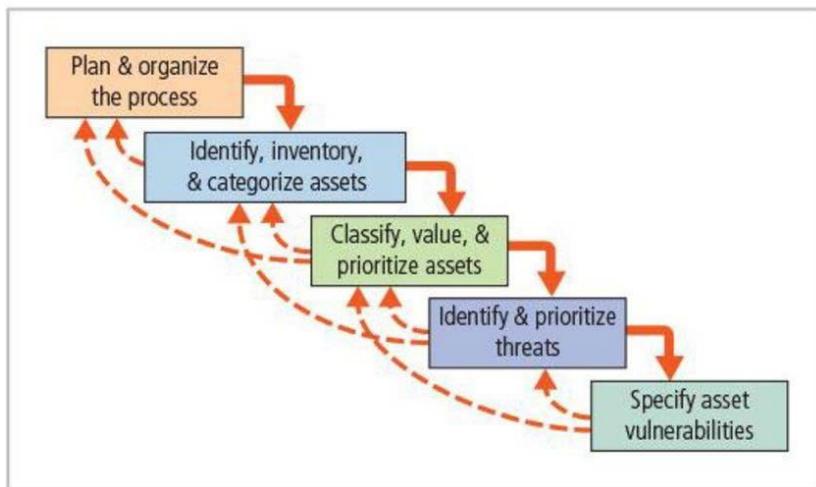
Vulnerabilities are specific avenues that threat agents can exploit to attack an information asset.

At the end of the risk identification process, a list of assets and their vulnerabilities has been developed.

This list serves as the starting point for the next step in the risk management process—risk assessment.

The goal at this point is to create a method to evaluate the relative risk of each listed vulnerability.

**Figure 5-4 Components of risk identification**



### 1. Planning and Organizing the Process

A risk management process requires applying the organization's project management principles to the risk management process. The process will need a proper project plan with periodic deliverables, including a task list and appropriate assignments.

### 2. Identifying, Inventorying, and Categorizing Assets

The iterative process, which begins with the identification of assets, including all of the following elements of an organization's system: people, procedures, data, software, hardware, and networking components.

The identification of people, procedures, and data assets.

- Identifying human resources, documentation, and data information is more difficult than identifying hardware and software assets.
- As the people, procedures, and data assets are identified, they should be recorded using a reliable data-handling process.

When deciding which information assets to track, consider the following asset attributes:

- People: Position name/number/ID (try to avoid names and stick to identifying positions, roles, or functions); supervisor; security clearance level; special skills
- Procedures: Description; intended purpose; relationship to software, hardware, and networking elements; storage location for reference; storage location for update
- Data: Classification; owner, creator, and manager; size of data structure; data structure used (sequential or relational); online or offline; location; backup procedures employed

### *Risk Management*

“If you know the enemy and know yourself, you need not fear the result of a hundred battles.

“If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

“If you know neither the enemy nor yourself, you will succumb in every battle.”

Sun Tzu

#### Knowing Ourselves

This means identifying, examining and understanding the information and how it is processed, stored, and transmitted.

Armed with this knowledge, they can then initiate an in-depth risk management program.

Risk management is a process, which means the safeguards and controls that are devised and implemented are not install-and-forget devices.

#### Knowing the Enemy

This means identifying, examining, and understanding the threats facing the organization’s information assets.

Managers must be prepared to fully identify those threats that pose risks to the organization and the security of its information assets.

Risk management is the process of assessing the risks to an organization’s information and determining how those risks can be controlled or mitigated.

#### Accountability for Risk Management

All communities of interest must work together to:

- Evaluating the risk controls
- Determining which control options are cost-effective

- Acquiring or installing the appropriate controls
- Overseeing processes to ensure that the controls remain effective
- Identifying risks, which includes:
  - Inventory information assets
  - Classifying/organizing assets
  - Assigning information asset value
  - Identifying threats to the cataloged assets
  - Pinpointing vulnerable assets by tying specific threats to specific assets
- Assessing risks, which includes:
  - Determining likelihood of attacks on vulnerable systems by specific threats
  - Assessing relative risk facing information assets, so risk management and control activities can prioritize
  - Calculating the risks to which assets are exposed in their current setting
  - Reviewing controls for identified vulnerabilities and says to control the risks that the assets face
  - Documenting the findings of risk identification and assessment

Summarizing the findings, which involves stating the conclusions of the analysis stage of risk assessment in preparation for moving into the stage of controlling risk by exploring methods to mitigate risk

### *Risk Assessment*

Risk is the likelihood of the occurrence of a vulnerability

Multiplied by

The value of the information asset

Minus

The percentage of risk mitigated by current controls

Plus

The uncertainty of current knowledge of the vulnerability



**FIGURE 7-4** Risk Identification Estimate Factors

### Likelihood

Likelihood is the overall rating—a numerical value on a defined scale (.1 – 1.0)—of the probability that a specific vulnerability will be exploited.

Using the information documented during the risk identification process, you can assign weighted scores based on the value of each information asset, i.e. 1-100, low-med-high, etc.

### Assessing Potential Loss

To be effective, the values must be assigned by asking:

- Which threats present a danger to this organization's assets in the given environment?
- Which threats represent the most danger to the organization's information?
- How much would it cost to recover from a successful attack?
- Which threats would require the greatest expenditure to prevent?
- Which of the aforementioned questions is the most important to the protection of information from threats within this organization?

### Percentage of Risk Mitigated by Current Controls

If a vulnerability is fully managed by an existing control, it can be set aside.

If it is partially controlled, estimate what percentage of the vulnerability has been controlled.

### *Uncertainty*

It is not possible to know everything about every vulnerability.

The degree to which a current control can reduce risk is also subject to estimation error. A factor that accounts for uncertainty must always be added to the equations; it consists of an estimate

made by the manager using good judgment and experience.

#### *Risk Determination*

For the purpose of relative risk assessment, risk equals likelihood of vulnerability occurrence times value (or impact) minus percentage risk already controlled plus an element of uncertainty.

Asset A has a value of 50 and has one vulnerability, which has a likelihood of 1.0 with no current controls. Your assumptions/data are 90% accurate.

Asset B has a value of 100 and has two vulnerabilities: Vul #2 has a likelihood of 0.5 with a current control that addresses 50% of its risk; vul # 3 has a likelihood of 0.1 with no current controls. Your assumptions and data are 80% accurate.

The resulting ranked list of risk ratings for the three vulnerabilities is as follows:

- Asset A: Vulnerability 1 rated as  $55 = (50 \times 1.0) - 0\% + 10\%$ .
- Asset B: Vulnerability 2 rated as  $35 = (100 \times 0.5) - 50\% + 20\%$ .
- Asset B: Vulnerability 3 rated as  $12 = (100 \times 0.1) - 0 \% + 20\%$ .

#### *Identify Possible Controls*

For each threat and its associated vulnerabilities that have residual risk, create a preliminary list of control ideas.

Three general categories of controls exist: policies, programs, and technical controls.

#### Access Controls

Access controls specifically address admission of a user into a trusted area of the organization.

These areas can include information systems, physically restricted areas such as computer rooms, and even the organization in its entirety.

Access controls usually consist of a combination of policies, programs, and technologies.

#### *Types of Access Controls*

Mandatory Access Controls (MACs) are required and are structured and coordinated with a data classification scheme.

When MACs are implemented, users and data owners have limited control over their access to information resources.

MACs use a data classification scheme that rates each collection of information.

## Types of Access Controls

In lattice-based access controls, users are assigned a matrix of authorizations for particular areas of access.

The matrix contains subjects and objects, and the boundaries associated with each subject/object pair are clearly demarcated.

With this type of control, the column of attributes associated with a particular object is called an access control list (ACL).

The row of attributes associated with a particular subject is a capabilities table.

Nondiscretionary controls are determined by a central authority in the organization and can be based on roles—called role-based controls—or on a specified set of tasks—called task-based controls.

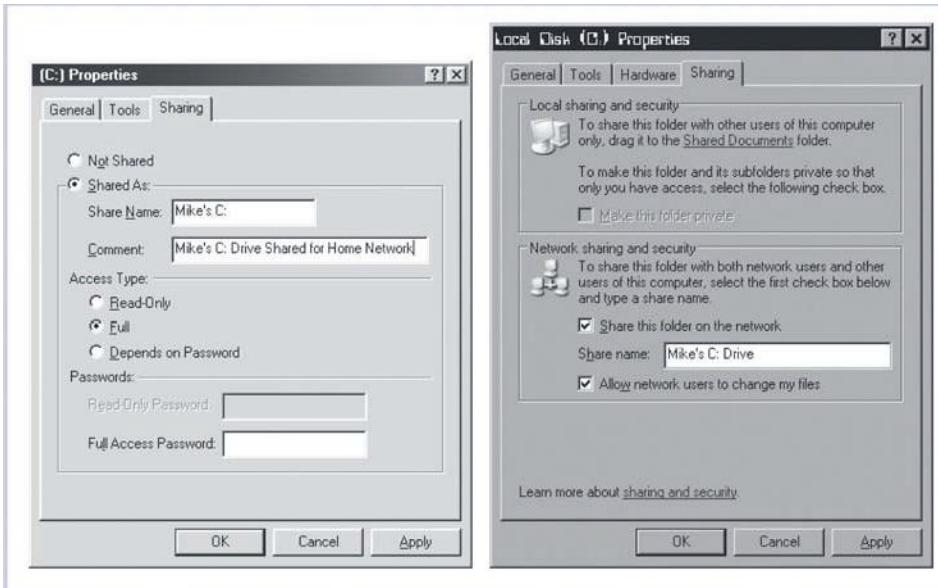
Task-based controls can, in turn, be based on lists maintained on subjects or objects.

Role-based controls are tied to the role that a particular user performs in an organization, whereas task-based controls are tied to a particular assignment or responsibility.

Discretionary Access Controls (DACs) are implemented at the discretion or option of the data user.

The ability to share resources in a peer-to-peer configuration allows users to control and possibly provide access to information or resources at their disposal.

The users can allow general, unrestricted access, or they can allow specific individuals or sets of individuals to access these resources.



**FIGURE 7-5** Discretionary Access Control

### *Documenting the Results of Risk Assessment*

The goal of the risk management process so far has been to identify information assets and their vulnerabilities and to rank them according to the need for protection.

In preparing this list, a wealth of factual information about the assets and the threats they face is collected.

Also, information about the controls that are already in place is collected.

The final summarized document is the ranked vulnerability risk worksheet.

**TABLE 7-6** Risk Identification and Assessment Deliverables

Deliverable	Purpose
Information asset classification worksheet	Assembles information about information assets and their impact on or value to the organization
Weighted criteria analysis worksheet	Assigns a ranked value or impact weight to each information asset
Ranked vulnerability risk worksheet	Assigns a risk-rating ranked value to each uncontrolled asset–vulnerability pair

### Ranked Vulnerability Risk Worksheet

#### *Documenting the Results of Risk Assessment*

- What should the documentation package look like?
- What are the deliverables from this stage of the risk management project?

The risk identification process should designate what function the reports serve, who is responsible for preparing them, and who reviews them.

A. Describe security clearances.

- The other side of the data classification scheme is the personnel security clearance structure. For each user of data in the organization, a single level of authorization must be assigned that indicates the level of classification he or she is authorized to view.
- Before an individual is allowed access to a specific set of data, he or she must meet the need-to-know standard. This extra level of protection ensures that the confidentiality of information is properly maintained.

B. Discuss the management of classified data.

- Management of classified data includes its storage, distribution, transportation, and destruction.
- Information that is not unclassified or public must be clearly marked as such. Use Figure 5-5 in your explanation.
- When classified data is stored, it must be available only to authorized individuals.
- When an individual carries classified information, it should be transported via inconspicuous means, such as in a locked briefcase or portfolio.
- The clean desk policy requires employees to secure all information in appropriate storage containers at the end of each day.
- When copies of classified information are no longer valuable or excessive copies exist, proper care should be taken to destroy them by means of shredding, burning, or transferring to an authorized document destruction service.
- It is important to enforce policies to ensure that no classified information is disposed of in trash or recycling areas since some individuals would not hesitate to engage in dumpster diving to retrieve information that could embarrass an organization or compromise information security.

**3. Information Asset Valuation**

Each asset of the organization is assigned to a category. These questions assist in developing the weighting criteria to be used for asset valuation. These questions include:

- Which information asset is the most critical to the success of the organization?
- Which information asset generates the most revenue?
- Which of these assets plays the biggest role in generating revenue or delivering services?

- Which information asset would be the most expensive to replace?
- Which information asset would be the most expensive to protect?
- Which information asset would most expose the company to liability or embarrassment if revealed?

The following are necessary to calculate, estimate or derive values for information assets:

- Value retained from the cost of creating the information asset
- Value retained from past maintenance of the information asset
- Value implied by the cost of replacing the information
- Value from providing the information
- Value incurred from the cost of protecting the information
- Value to owners
- Value of intellectual property
- Value to adversaries

Additional company-specific criteria may add value to the asset evaluation process and should be identified, documented, and added to the process. To finalize this step, the organization should assign a weight to each asset based on their given answers.

Information asset prioritization.

- Once the process of inventorying and assessing value is complete, you can prioritize each asset using weighted factor analysis. Use Table 5-2 in your explanation.
- In this process, each information asset is assigned a score for each critical factor. In addition, each critical factor is also assigned a weight (ranging from 1 to 100) to show that criteria's assigned importance for the organization.

### *Specifying Asset Vulnerabilities*

After identification of the organization's information assets and documentation of criteria for beginning to assess the threats it faces, review each information asset for each threat it faces and create a list of vulnerabilities.

### *Determining the Loss Frequency*

Likelihood is the probability that a specific vulnerability will be attacked.

- In risk assessment, you assign a numeric value to the likelihood of an attack on your

organization.

- The National Institute of Standards and Technology recommends in Special Publication 800-30 assigning a number between 0.1 for low and 1.0 for high.
- Zero is not used because vulnerabilities with a zero likelihood have been removed from the asset/vulnerability list.

Whatever rating system is utilized for assigning likelihood, use professionalism, experience, and judgment—and use the rating model you select consistently.

The second half of the loss frequency calculation is determining the probability of an attack's success.

- A key component of this assessment is that the attack successfully compromises vulnerabilities in the organization's information asset
- Another part of the assessment is determining the organization's current level of protection.

The person or team that performs the risk assessment calculations must work closely with the IT and information security groups. Combining the likelihood and attack success probability results in an assessment of the loss frequency, also known as loss event frequency.

### *Evaluating Loss Magnitude*

Loss magnitude as the combination of an asset's value and the percentage of it that might lost in an attack. Mention that loss magnitude is also known as asset exposure.

### *Calculating Risk*

For the purpose of relative risk determination, risk *equals* loss frequency *times* loss magnitude *plus* an element of uncertainty.

### *Assessing IRP*

For each threat and its associated vulnerabilities that have residual risk, we need to create a ranking of their relative risk levels. When the organization's risk appetite is less than the asset's residual risk, it must move to the next stage of risk control and look for additional strategies to further reduce the risk. The goal of this process has been to identify the organization's information assets that have specific vulnerabilities and list them, ranked according to those that most need protection. While preparing this list, we have collected and preserved a wealth of factual information about the assets, the threats they face, and the vulnerabilities they expose, as well as some information about the controls that are already in place.

The final summarized document, is the ranked vulnerability risk worksheet and contains the following data:

- Asset: Each vulnerable asset
- Asset relative value: Shows the results for this asset from the weighted factor analysis worksheet
- Vulnerability: Each uncontrolled vulnerability
- Loss frequency: The likelihood of the realization of the vulnerability by a threat agent, as noted in the vulnerability analysis step
- Loss magnitude: The figure calculated from the asset impact multiplied by loss frequency

The ranked vulnerability risk worksheet, is the working document for the next step in the risk management process: assessing and controlling risk.

### *Risk Control*

Risk control involves three basic steps: selection of control strategies, justification of these strategies to upper management , and the implementation, monitoring, and ongoing assessment of the adopted controls.

#### *Selecting Control Strategies*

Five control strategies:

- Defense
- Transference
- Mitigation
- Acceptance
- Termination

#### *Defense*

The defense strategy is the preferred approach by preventing exploitation of the vulnerability.

The three common methods of defense are the application of policy, education and training, and the application of technology.

A defense strategy is a security control that deflects attacks and minimizes the probability that an attack will succeed.

### *Transference*

The transfer control strategy attempts to shift the risk to other assets, other processes, or other organizations. This principle should be considered whenever an organization begins to expand its operations.

If an organization does not already have quality security management and administration experience, it should hire individuals or firms that provide such expertise. It is up to the owner of the information asset, IT management, and the information security team to ensure that the disaster recovery requirements of the outsourcing contract are sufficient and have been met before they are needed for recovery efforts.

### *Mitigation*

Mitigation is the control approach that attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation.

Mitigation begins with early detection of an attack in progress and relies on the ability of the organization to respond quickly, efficiently, and effectively.

There are three types of plans in this approach: the incident response plan (IRP), the disaster recovery plan (DRP), and the business continuity plan (BCP).

### *Acceptance*

The acceptance of risk is the choice to do nothing to protect a vulnerability and to accept the outcome of its exploitation. This may or may not be a conscious business decision.

The only acceptance strategy that is recognized as valid occurs when the organization has:

- Determined the level of risk
- Assessed the probability of attack
- Estimated the potential damage that could occur from these attacks
- Performed a thorough cost-benefit analysis
- Evaluated controls using each appropriate type of feasibility
- Decided that the particular function, service, information, or asset did not justify the cost of protection

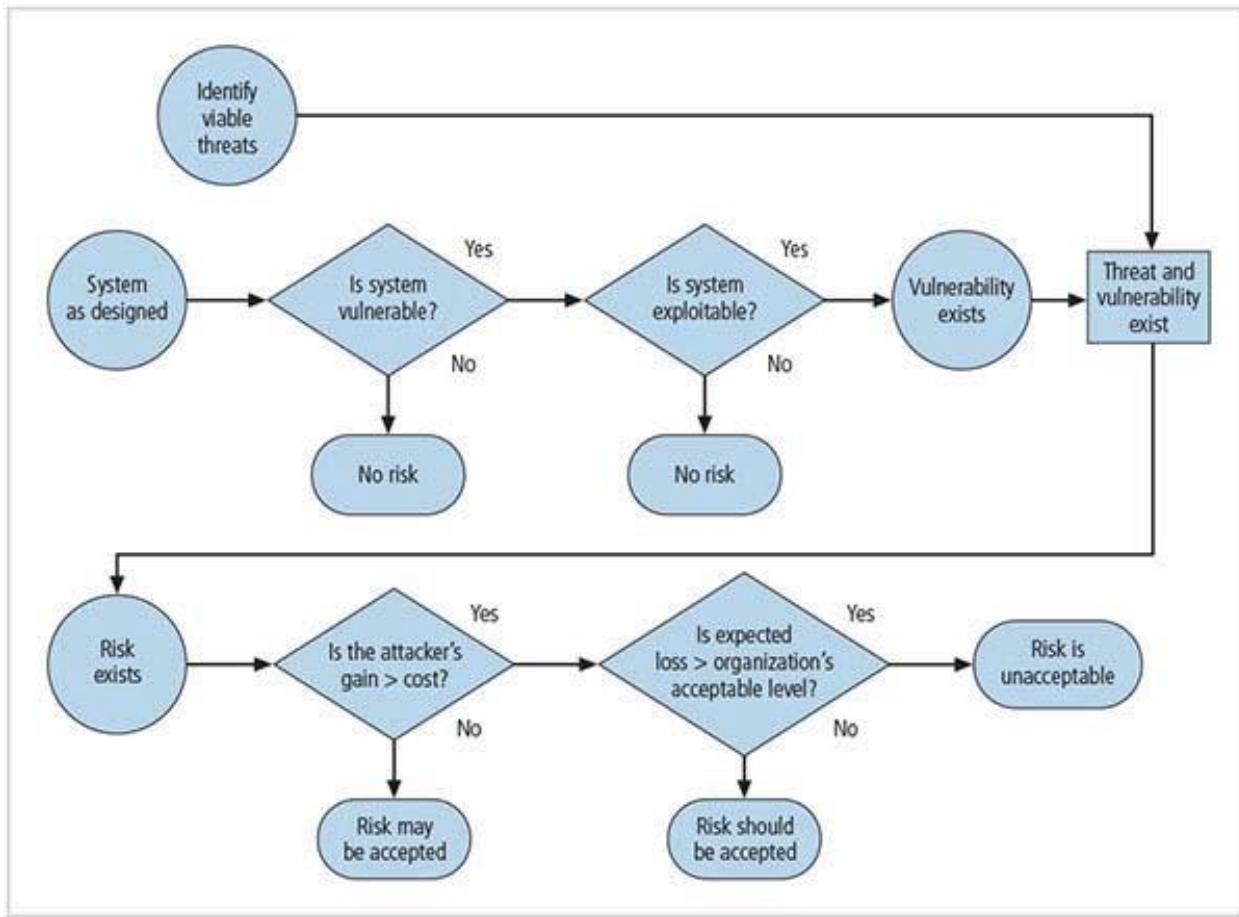
If every vulnerability identified in the organization is handled by means of acceptance, it may reflect an inability to conduct proactive security activities and an apathetic approach to security in general.

## *Termination*

The final risk control strategy directs the organization to avoid business activities that introduce uncontrollable risks.

## *Selecting a Risk Control Strategy*

Risk handling decision points



The level of threat and value of the asset should play a major role in the selection of a risk control strategy. The following rules of thumb that can be applied in selecting the preferred strategy:

- When a vulnerability exists, implement security controls to reduce the likelihood of the vulnerability being exercised.
- When a vulnerability can be exploited, apply layered protections, architectural designs, and administrative controls to minimize risk or prevent occurrence.
- When the attacker's cost is less than his potential gain, apply protections to increase the attacker's cost.

- When potential loss is substantial, apply design principles, architectural designs, and technical and nontechnical protections to limit the extent of the attack.

Before deciding on the strategy for a specific vulnerability, all the economic and noneconomic consequences of the vulnerability facing the information asset must be explored. Cost avoidance is the process of avoiding the financial impact of an incident by implementing a control. An organization begins by evaluating the worth of the information assets to be protected and the loss in value if those information assets are compromised by the specific vulnerability. Moreover, an organization should not spend more to protect an asset than the asset is worth. The formal decision-making process, which is used to consider the economic feasibility of implementing information security controls and safeguards is called a *cost benefit analysis* or an *economic feasibility study*.

It is difficult to determine the value of information, it is also difficult to determine the costs of safeguards. Some of the items that impact the cost of a control or safeguard include:

- Cost of development or acquisition
- Training fees
- Cost of implementation
- Service costs
- Cost of maintenance

The amount of benefit usually determined by valuing the information asset or assets exposed by the vulnerability and then determining how much of that value is at risk and how much risk there is for the asset.

The valuation of assets involves the estimation of real and perceived costs associated with the design, development, installation, maintenance, protection, recovery, and defense against market loss, and litigation for every set of information-bearing systems or information assets. Some information assets acquire value over time that is beyond the intrinsic value of the asset itself. This value gained over time is referred to as acquired value.

Once an organization has estimated the worth of various assets, it can begin to examine the potential loss that could occur from the exploitation of a vulnerability or a threat occurrence. This process results in the estimate of potential loss per risk.

The questions that must be asked are here:

- What damage could occur, and what financial impact would it have?

- What would it cost to recover from the attack, in addition to the financial impact of damage?
- What is the single loss expectancy for each risk (SLE)?

A single loss expectancy (SLE) is the calculation of the value associated with the most likely loss from an attack. It is a calculation based on the value of the asset and the exposure factor (EF), which is the expected percentage of loss that would occur from a particular attack, as follows:

$$\text{SLE} = \text{exposure factor (EF)} \times \text{asset value}$$

where EF equals the percentage loss that would occur from a given vulnerability being exploited.

The annualized rate of occurrence (ARO), which is simply how often you expect a specific type of attack to occur. To standardize calculations, you convert the rate to a yearly (annualized) value. This is expressed as the probability of a threat occurrence.

The expected value of a loss can be stated in the following equation:

$$\text{ALE} = \text{SLE} \times \text{ARO}$$

The cost benefit analysis (CBA) formula, In its simplest definition, determines whether or not a particular control is worth its cost. The CBA is calculated using the ALE from earlier assessments.

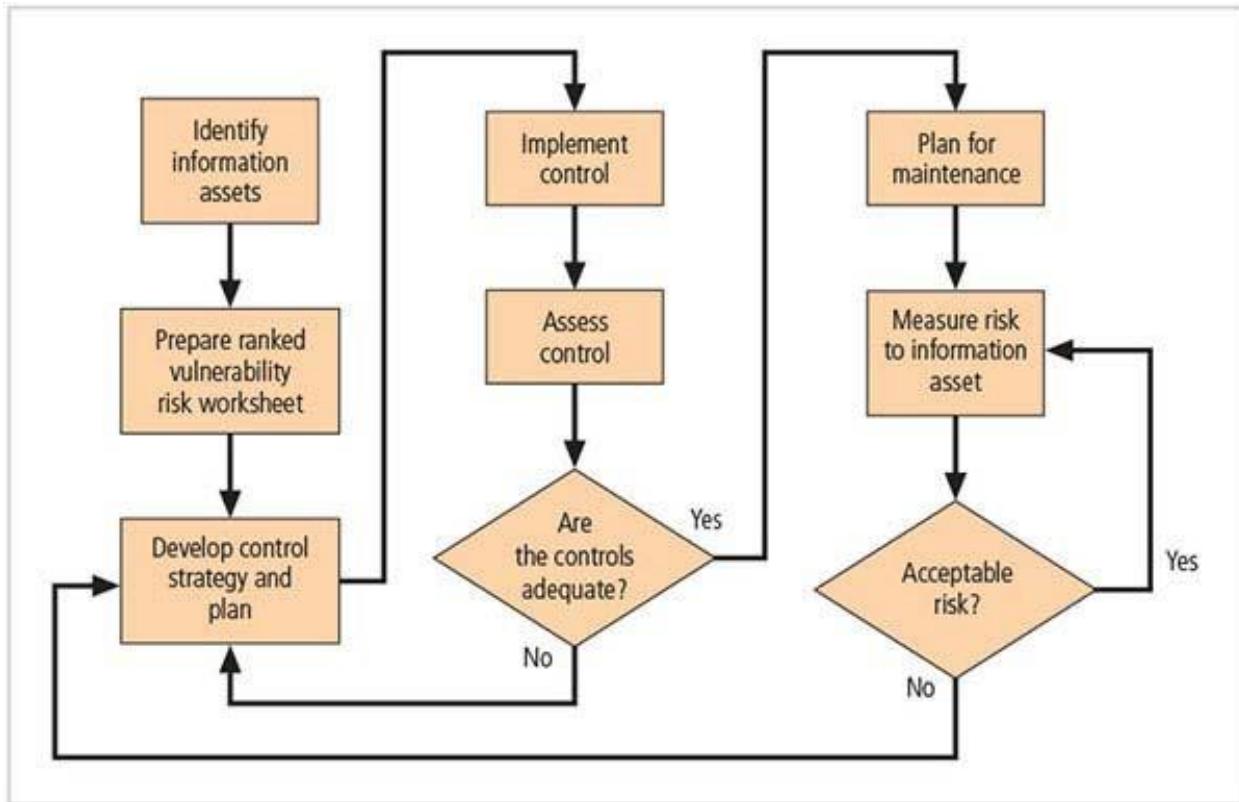
$$\text{CBA} = \text{ALE(prior)} - \text{ALE(post)} - \text{ACS}$$

ALE(prior) is the annualized loss expectancy of the risk before the implementation of the control. ALE(post) is the ALE examined after the control has been in place for a period of time. ACS is the annual cost of the safeguard.

Once controls are implemented, it is crucial to continue to examine their benefits to determine when they must be upgraded, supplemented, or replaced.

### *Implementation, Monitoring, and Assessment of Risk Controls*

The selection and implementation of a control strategy is not the end of a process. The strategy and its accompanying controls must be monitored and reevaluated on an ongoing basis to determine their effectiveness and to calculate more accurately the estimated residual risk. Use The risk control cycle is shown here:



### *Benchmarking and Best Practices*

benchmarking, is the process of seeking out and studying the practices used in other organizations that produce the results you desire in your organization. When benchmarking, an organization typically uses one of two measures to compare practices: metrics-based measures or process-based measures.

Metrics-based measures, are comparisons based on numerical standards, such as:

- Number of successful attacks
- Staff hours spent on systems protection
- Dollars spent on protection
- Number of security personnel
- Estimated value in dollars of the information lost in successful attacks
- Loss in productivity hours associated with successful attacks

An organization uses this information to rank competitive businesses with a similar size or market to determine how it measures up to competitors. The difference between an organization's measures and those of others is often referred to as a **performance gap**.

Process-based measures are generally less focused on numbers and more strategic than metrics-based measures. For each of the areas the organization is interested in benchmarking, process-based measures enable the organization to examine the activities an individual company performs in pursuit of its goal, rather than the specifics of how goals are attained. The primary focus is the method the organization uses to accomplish a particular process, rather than the outcome.

Security efforts that seek to provide a superior level of performance in the protection of information are referred to as **best business practices** or simply best practices or recommended practices.

Best security practices (BSPs), are those security efforts that are among the best in the industry, balancing the need to access with the need to provide adequate protection. Best practices seek to provide as much security as possible for information and systems while maintaining a solid degree of fiscal responsibility.

When considering to adopt best practices in your organization, consider the following:

- Does your organization resemble the identified target organization with the best practice under consideration?
- Can your organization expend resources similar to those identified with the best practice?
- Is your organization in a similar threat environment as that proposed in the best practice?

The seven key areas that Microsoft focuses on for home users and for small businesses.

Problems with the application of benchmarking and best practices:

- The biggest problem with benchmarking in information security is that organizations don't talk to each other.
- Another problem with benchmarking is that no two organizations are identical.
- A third problem is that best practices are a moving target. What worked well two years ago may be completely worthless against today's threats.
- One last issue to consider is that simply knowing what was going on a few years ago, as in benchmarking, doesn't necessarily tell us what to do next.

A baseline is performance value or metric used to compare changes in the object being measured. Baselineing is the analysis of measures against established standards. In information security, baselining is the comparison of security activities and events against the organization's future performance. When baselining, it is useful to have a guide to the overall process.

Other qualitative approaches can be used to determine an organization's readiness for any proposed set of controls are operational, technical, and political feasibility analyses.

Organizational feasibility examines how well the proposed information security alternatives will contribute to the efficiency, effectiveness, and overall operation of an organization. Above and beyond the impact on the bottom line, the organization must determine how the proposed alternatives contribute to the business objectives of the organization.

Operational feasibility analysis examines user acceptance and support, management acceptance and support, and the overall requirements of the organizations' stakeholders. Operational feasibility is sometimes known as behavioral feasibility, because it measures the behavior of users. One of the fundamental principles of systems development is obtaining user buy-in on a project. A common method for obtaining user acceptance and support is through user involvement. User involvement can be obtained via three simple steps: communicate, educate, and involve.

Organizations should communicate with system users throughout the development of the security program, letting them know that changes are coming. These three basic undertakings—communication, education, and involvement—can reduce resistance to change and build resilience for change. Resilience is the quality that allows workers not only to tolerate constant change, but also to accept it as a necessary part of their jobs.

In addition to the economic costs and benefits of proposed controls, the project team must also consider the technical feasibilities of their design, implementation, and management. Technical feasibility analysis examines whether or not the organization has or can acquire the technology necessary to implement and support the proposed control. Technical feasibility also examines whether the organization has the technological expertise to manage the new technology.

For some organizations, the most significant feasibility evaluated may be political. Within organizations, political feasibility defines what can and cannot occur based on the consensus and relationships between the communities of interest. The limits placed on an organization's actions or behaviors by the information security controls must fit within the realm of the possible before they can be effectively implemented, and that realm includes the availability of staff resources.

#### *Recommended Risk Control Practices*

Planned expenditures to implement a control strategy must be justified, and budget authorities must be convinced to spend the necessary amount to protect a particular asset from an identified

threat. Another factor to consider is that each control or safeguard affects more than one asset-threat pair. Information security professionals manage a dynamic matrix covering a broad range of threats, information assets, controls, and identified vulnerabilities. If a new safeguard is implemented, there is a risk decrease associated with all subsequent control evaluations. The action of implementing a control may change the values assigned or calculated in a prior estimate. There is an ongoing search for ways to design security architectures that go beyond the direct application of specific controls in which each is justified for a specific information asset vulnerability, to safeguards that can be applied to several vulnerabilities at once.

### *Documenting Results*

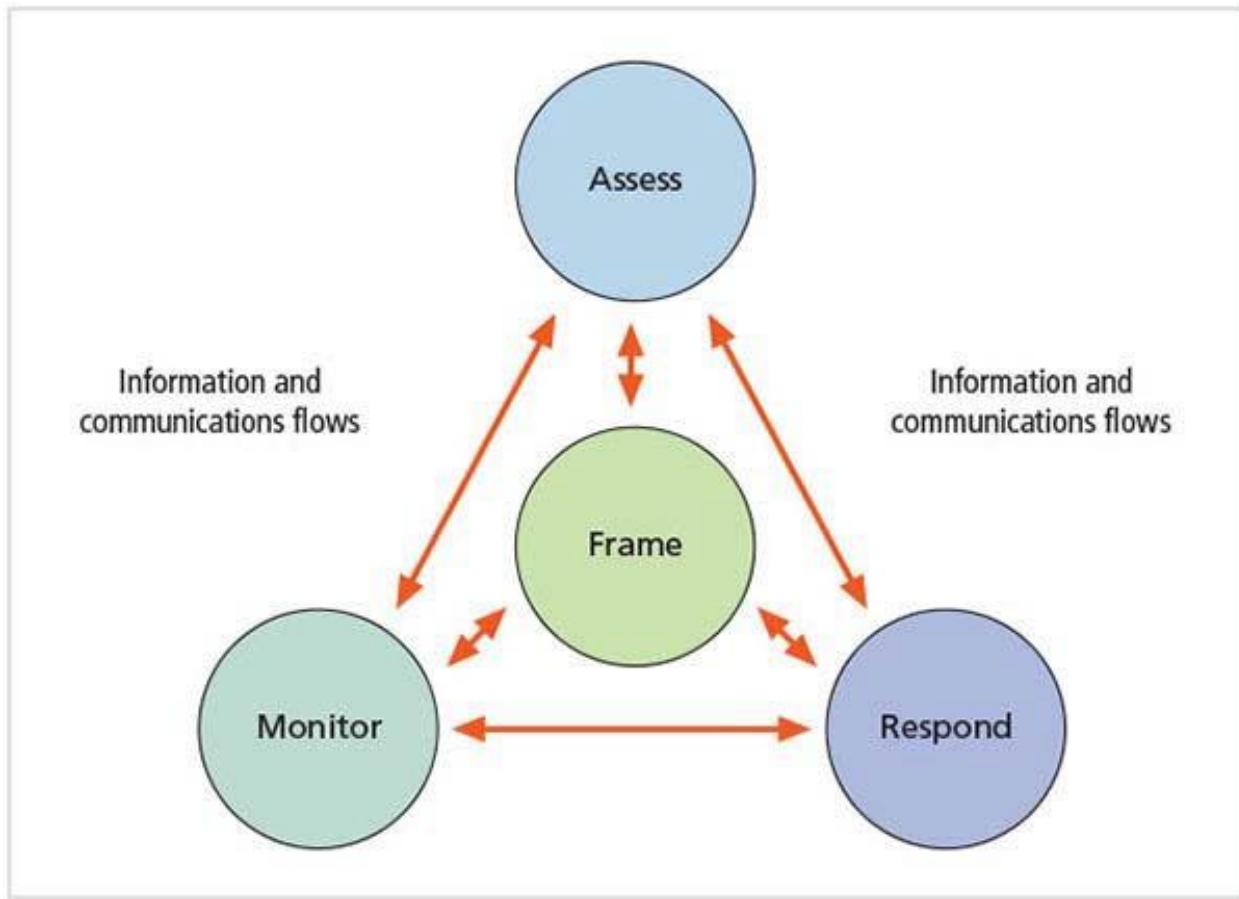
The results of risk assessment activities can be delivered. There are a number of ways: a report on a systematic approach to risk control, a project-based risk assessment, or a topic-specific risk assessment. When the organization is pursuing an overall risk management program, it requires a systematic report that enumerates the opportunities for controlling risk. This report documents a series of proposed controls, each of which has been justified by one or more feasibility or rationalization approaches. Another option is to document the outcome of the control strategy for each information asset-threat pair in an action plan. This action plan includes concrete tasks, each with accountability assigned to an organizational unit or to an individual.

Sometimes a risk assessment is prepared for a specific IT project at the request of the project manager, either because it is required by organizational policy or because it is good project management practice. The project risk assessment should identify the sources of risk in the finished IT system, with suggestions for remedial controls, as well as those risks that might impede the completion of the project.

When management requires details about a specific risk to the organization, risk assessment may be documented in a topic-specific report. These are usually demand reports that are prepared at the direction of senior management and are focused on a narrow area of information systems operational risk.

### *The NIST Risk Management Framework*

The NIST SP 800-37 Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach document established a common approach to using a Risk Management Framework (RMF) for information security practice.



## Aim/Objectives

Chapter 5 introduces students to the topic of risk management, and the use of different risk management techniques. Students will learn about risk identification using different strategies, including the use of different models, worksheets, and checklists. Finally, the topic of risk likelihood is covered, followed by the deliverables and results of the risk identification process.

Before the design of new security solutions can begin, the security analysts must first understand the current state of the organization and its relationship to security. Does the organization have any formal security mechanisms in place? How effective are they? What policies and procedures have been published to the security managers and end users? This chapter examines the processes necessary to undertake formal risk management activities in the organization. Risk management is the process of identifying, assessing, and reducing risk to an acceptable level and implementing effective control measures to maintain that level of risk. This is done with a number of processes from risk analysis through various types of feasibility analyses, including quantitative and qualitative assessment measures and evaluation of security controls.

## Learning Outcomes

In this chapter, your students will learn to:

- Define risk management, risk identification, and risk control
- Describe how risk is identified and assessed
- Assess risk based on probability of occurrence and likely expected impact
- Explain the fundamental aspects of documenting risk via the process of risk assessment
- Describe various options for a risk mitigation strategy
- Define risk appetite and explain how it relates to residual risk
- Discuss conceptual frameworks for evaluating risk controls and formulate a cost-benefit analysis

## Key Words

Access controls	Vulnerability risk	Risk control
Implementation, monitoring and assessment of risk controls	Benchmarking	NIST risk management framework
Risk management		

## Annotated Bibliography

### Required Materials

To achieve the educational needs of this unit the following material is used:

#### Primary Material

Chapter 6 of Michael E. Whitman / Michael J., *Principles of Information Security, Sixth Edition*. Cengage Learning, 2018, ISBN-13 9781337102063.

Wheeler, E., 2011. Security risk management: Building an information security risk management program from the Ground Up. Elsevier.

Donaldson, S.E., Siegel, S.G., Williams, C.K. and Aslam, A., 2018. Enterprise Cybersecurity Study Guide: How to Build a Successful Cyberdefense Program Against Advanced Threats.

Bayuk, J.L., Healey, J., Rohmeyer, P., Sachs, M.H., Schmidt, J. and Weiss, J., 2012. Cyber security policy guidebook. John Wiley & Sons.

### **Supportive material**

- <http://technet.microsoft.com/en-us/library/cc535173.aspx>
- Cultivating a Risk Intelligent Culture.  
[https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu\\_en\\_wp\\_riskintelligentculture\\_01082012.pdf](https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu_en_wp_riskintelligentculture_01082012.pdf)
- Creating a Culture of Risk Avoidance.  
<https://www.bloomberg.com/news/articles/2009-03-06/creating-a-culture-of-risk-avoidancebusinessweek-business-news-stock-market-and-financial-advice>
- Effective IT Risk Management <http://www.continuitycentral.com/feature0755.html>
- An Introduction to Cost Benefit Analysis <http://www.sjsu.edu/faculty/watkins/cba.htm>

### **Activity (5 points)**

Graded activity carrying 5% of the final grade. Using a Microsoft Windows system, open Internet Explorer. Click Internet Options on the Tools menu. Examine the contents of the Security and Privacy tabs. How can these tabs be configured to provide: (a) content filtering and (b) protection from unwanted items like cookies?

### **Recommended time for the student to work**

20 hours

## COMPLIANCE: AUDITING, MONITORING, AND LOGGING

6<sup>th</sup> Week

### Summary

Compliance: Reasons for specific cybersecurity legislation beyond cybercrime, compliance requirements, self-assessment, auditing principles, audit process.

### Introductory Remarks

We focus on two meanings: first, audit is a procedure for recording and reviewing the variety of events that occur on a network or systems. Second, audit is a periodic self-review of a network environment required to safely operate any complex organization.

Monitoring a system involves keeping a close watch on the operations (internal) and usage (external) of that system – that is, tracking specific events that occur on the system and recording them in the logs.

The basic operation of a system logging facility is to collect information from the operating system or application whenever specific actions occur.

#### *What to Audit?*

An event is any action that may be of interest to you on a device. A security event is an occurrence that you think might affect the system's security.

Process Events: Introduce the terms process, services, and daemon.

**Logon Events:** Point out that tracking user-related activities helps to identify what actions are taking place, who is initiating those actions, and ultimately provide an overview of the user session.

Once an attacker has gained access to a system through a normal user account, the next step in the attack is to elevate those privileges to those of an administrator. This is called **privilege escalation**.

**Resource Access Events:** Auditing is not without costs, and the decision about what events to collect is one of tradeoffs. Recording every possible detail for auditing carries a heavy cost. Note

that by enabling a maximum degree of audit detail, you will capture all legitimate events not just those that are exceptions.

**Network Connection Events:** Note that administrators can track connections that are allowed and established, connections that are denied and fail, or other network activity that does not fall into the firewall's ruleset.

Data leakage is a top concern for most security professionals since it denotes the exfiltration or unauthorised release of data. Data leakage prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.

**System Restart and Shutdown Events:** Keeping systems available for use is an IT team's number one priority. Therefore, it is important that auditing systems keep track of when systems are booted, restarted, and shut down.

**Audit System or Log Events:** Remind students that log records are a valuable source of information, particularly when they are centralized for consolidation and analysis. In most cases, the auditing system reports when various activities have occurred to the logs – when the logs have reached their capacities, when they have been truncated, and so forth.

### *Log Management Policy*

Auditing events for a single data source (e.g., a server) is extremely important to understand the health of that particular resource. However, looking at all the data sources within an IT environment in aggregate provides a more comprehensive picture of the overall health of the IT environment.

In order to create effective log management practices within your organization, you must address: storage, retention, baseline, encryption, and disposal.

### *Standard OS Logs*

Note that it is important to look at some common systems to get a sense of the nature of the type of data that can be logged and some of the kinds of information that can be recorded.

**Windows-Based Logging:** On most current versions of Microsoft Windows-based systems, logging is managed by the Event Viewer, which is accessible from the system control panel. With the introduction of Windows 7, Microsoft divided logs into two categories: (1) Windows Logs and (2) Applications and Services Logs.

Linux-Based Logging.

### *Log Management Technology*

Most system logs are very difficult to collect, store, read, and understand. In cases where an administrator is looking for a specific event, the chore can be overwhelming. Luckily, a number of software manufacturers make tools that make log file analysis much easier.

Log Management.

**Security Information and Event Management (SIEM):** Although log management is focused primarily on the collection, centralization, and storage of network event information, the next level of intelligence is provided by security information and event management (SIEM) technology.

**Security Operations Center (SOC):** one of the needs that quickly becomes apparent with the deployment of log management and SIEM technologies is a talented pool of people to manage these technologies, watch these events as they occur, and then investigate and resolve them as needed.

### *Configuration and Change Management (CCM)*

Change and Configuration management (CMM) controls the effects of revisions to configurations on information systems and networks, a crucial aspect in performing ongoing audits of the network systems and their associated configurations. The configuration management process helps avoid confusion, problems, and unnecessary spending. The additional resources required to correct a problem that could have been prevented through sound configuration management practices is likely to far exceed the amount of resources required to develop and implement an effective enterprise process.

Change management seeks to prevent changes that could detrimentally affect the security of a system. In its entirety, the CCM process reduces the risk that any changes made to a system (insertions, installations, deletions, uninstallations, or modifications) result in a compromise to system or data confidentiality, integrity, or availability.

The change management process identifies the steps required to ensure that all changes are properly requested, evaluated, and authorized. Also, the process provides a detailed, step-by-step procedure for identifying, processing, tracking, and documenting changes.

Following you can see the change management process:

- **Step 1: Identify Change:** Note that change may consist of updating the database fields or records, or it may consist of upgrading the operating system using the latest security patches.
- **Step 2: Evaluate Change Request:** After a change request has been made, an analysis of the affects that the change management will have on the system or related systems is conducted using the guidelines on Page 418.
- **Step 3: Implementation Decision:** Discuss possible actions that could be taken after the change has been reviewed and evaluated.
- **Step 4: Implement Approved Change Request:** If implementation is authorized, the change is moved from the test environment and into production.
- **Step 5: Continuous Monitoring:** Note that the change process calls for continuous monitoring to ensure that the system is operating as intended and that implemented changes do not adversely affect either the performance or the security posture of the system.

### *IT Auditing*

One of the most prevalent standards for IT auditing was issued by the Information Systems Audit and Control Association (ISACA). This document, called “IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals” provides a comprehensive set of standards and guidelines for the IT audit professional.

The following topics should be discussed:

- **Phase 1: Initiation and Planning:** In the initiation portion Phase 1, the auditing group is contacted by an organizational entity that requested an audit of a particular system, department, or organization. Introduce the term **engagement letter**.
- **Phase 2: Fieldwork:** The second phase of the audit process involves the on-site visit. From the target organization’s perspective, this is the audit. A group of auditors arrives on the site and is given access to systems, documentation, organizational policies, procedures and standards, and pretty much anything else they need to conduct the evaluation.
- **Phase 3: Analysis and Review:** The third phase involves taking the findings from the on-site visit and conducting detailed analyses of those findings. The reports developed by the various auditors are compiled and compared, and the overall findings are examined.
- **Phase 4: Final Reporting:** After the analysis and review are complete, the auditing team makes a formal report to the target organization and/or requesting entity. This report summarizes the findings of the audit team.
- **Phase 5: Follow-Up:** At a predetermined interval after the final report has been delivered -

hopefully, after the target organization has had a chance to resolve any issues - there is typically a follow-up audit.

#### *Systems Certification, Accreditation, and Authorization*

**Accreditation** is the authorization of an IT system to process, store or transmit information. Accreditation is issued by a management official and serves as a means of ensuring that systems are of adequate quality.

**Certification** is the comprehensive evaluation of the technical and nontechnical security controls of an IT system to support the accreditation process that establishes the extent to which a design and implementation meets a set of specified security requirements.

Accreditation and certification are not permanent. Just as standards of due diligence and due care require an ongoing maintenance effort, most accreditation and certification processes require reaccreditation or recertification every few years (typically every three to five years).

#### *Auditing for Government and Classified Information Systems*

Information processed by the federal government is grouped into three categories: national security information (NSI), non-NSI, and intelligence community (IC). Note that National security information is processed on national security systems (NSSs).

#### *Auditing and the ISO 27000 Series*

Most commercial systems audit against a recognized standard. Currently, the most widely recognized one is called “Information Technology – Code of Practice for Information Security Management.”

The stated purpose of ISO/IEC 27002 is to provide recommendations for information security management for use by those who are responsible for initiating, implementing, or maintaining security in their organization.

#### *Auditing and COBIT*

Control Objectives for Information and Related Technology (COBIT) provides advice about the implementation of sound controls and control objectives for information security. Note that this document can be used not only as a planning tool for information security but also as an auditing framework controls model.

Although COBIT was designed to be an IT governance structure, it provides a framework to support information security requirements and assessment needs.

The following topics should be discussed:

- **Acquire and Implement:** The acquisition and implementation domain focuses on the specification of requirements, the acquisition of needed components, and the integration of these components into the organization's systems.
- **Delivery and Support:** The delivery and support domain focuses on the functionality of the system for the end user. It also focuses on the systems applications - including the input, processing, and output components.
- **Monitor and Evaluate:** The monitor and evaluate domain focuses on the alignment between IT systems usage and organizational strategy. This assessment identifies the regulatory requirements for which controls are needed.

## Aim/Objectives

In this chapter, we examine those aspects of auditing that are of benefit to network security, along with the standards that are used to audit network security operations. Keep in mind that auditing is also the term used for reviews of financial (accounting) systems and information systems. In fact, there are domains of knowledge for financial auditing and information systems auditing that will have characteristics that overlap those being discussed here.

## Learning Outcomes

In this chapter, students will learn to:

- List the various events that should be monitored in network environments
- Describe the various network logs available for monitoring
- Discuss the various log management, SIEM, and monitoring technologies
- Explain the role that configuration and change management play in auditing the network environment
- Discuss formal audit programs and how they relate to network environments
- Describe Certification and Accreditation (C&A) programs implemented by the U.S. federal government and other international agencies

## Key Words

Certification	Accreditation	IT Audit
Log management	Change and Configuration management (CMM)	

## Annotated Bibliography

### Required Materials

To achieve the educational needs of this unit the following material is used:

#### Primary Material

Chapter 10 of *Guide to Network Security, 2013, 1st Edition*, Michael E. Whitman, Herbert J. Mattord, David Mackey, Andrew Green, M.S.I.S., ISBN: 9780840024220

#### Supportive material

Bulgurcu, B., Cavusoglu, H. and Benbasat, I., 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 34(3), pp.523-548.

von Solms, S.B., 2005. Information Security Governance—compliance management vs operational management. *Computers & Security*, 24(6), pp.443-447.

Vance, A., Siponen, M. and Pahnila, S., 2012. Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, 49(3-4), pp.190-198.

- Windows Logs: <http://windows.microsoft.com/en-us/windows7/What-information-appears-in-event-logs-Event-Viewer>
- Information Systems Audit: <http://www.csoonline.com/article/492804/information-systems-audit-the-basics>
- Log Files: <http://computer.howstuffworks.com/workplace-surveillance4.htm>
- Daemons: <http://magazine.redhat.com/2007/03/09/understanding-your-red-hat-enterprise-linux-daemons/>
- Change Management: <http://www.methodframeworks.com/article/change-management-process-accomplishing-change-and-making-it-stick/index.html>

## **Self-Assessment Exercises**

### **Exercise 6.1**

What do you think are the advantages and disadvantages of storing log files on a central server?  
Give a short explanation.

### **Recommended time for the student to work**

15 hours

## PLANNING FOR CONTINGENCIES

7<sup>th</sup> Week

### Summary

With a rise in cyber-crime and unpredictable natural disasters, it is very important for companies to ensure that their Information Technology (IT) equipment, services and data are protected at all costs. Companies cannot predict when natural disasters or security breaches will occur. However, it is possible for companies to develop a plan to follow, in the event of a security breach, to help mitigate the impact. This plan is called a cyber security contingency plan. A cyber security contingency plan is a written risk management document that provides instructions, recommendations, and considerations for a company on how to recover their IT services and data in the event of a security breach, disaster or system disruption.

### Introductory Remarks

A cyber security contingency plan's primary objective is to protect data and assets after a security breach or disaster has occurred. This type of plan will include steps on protective measures, on ways to prevent future attacks, breaches or loss. It will also include approaches on how to collect and preserve evidence and how to develop a root cause analysis. Planning for unexpected events typically involves general business management and information technology and InfoSec management.

Having a plan in place that addresses how to identify, contain and resolve an unexpected event, is very important and the NIST recommendations on contingency planning should be taken into consideration.

#### *Fundamentals of Contingency Planning*

A contingency plan is a plan devised for an outcome other than in the usual (expected) plan. It is often used for risk management for an exceptional risk that, though unlikely, would have catastrophic consequences. Contingency plans are often devised by governments or businesses.

The four major components of contingency planning:

1. Business impact analysis (BIA)

2. Incident response plan (IR plan)
3. Disaster recovery plan (DR plan)
4. Business continuity plan (BC plan)

Each element of contingency planning functions, and an organization uses plans depending on the scale of an event, which is determined by a response team.

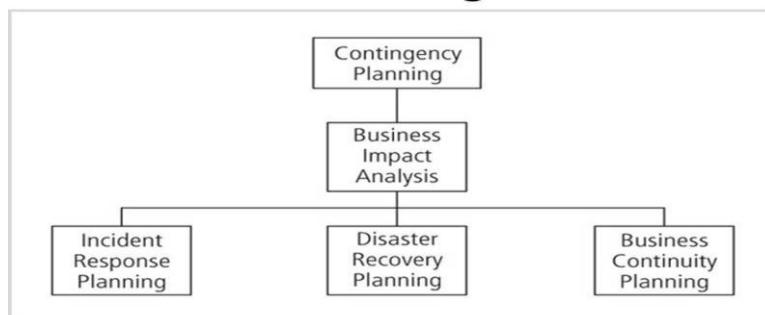
All four components of contingency planning can be included in a single plan, or can be developed separately. The role of a contingency planning management team (CPMT) in developing a contingency planning document. The students will be aware of the steps recommended by NIST for the creation of the CP document. CP policy is defined by executive management for use by the CPMT in the creation of an effective CP document.

Different teams and roles involved in CP and contingency operations:

1. CPMT, which gathers information for the development of contingency plans, and should include the following personnel:
  - a) Champion
  - b) Project Manager
  - c) Team members
2. Incident response team, which executes the incident response plan
3. Disaster recovery team, which executes the disaster response plan
4. Business continuity team, which executes the business continuity plan

The recommendations made by NIST's Computer Security Resource Center (CSRC) for the coordination of an organizations contingency plans, business interruption plans, and continuity plans, with the backup, contingency, and recovery plans of support systems.

## Components of Contingency Planning



### *Business Impact Analysis*

The Business Impact Analysis (BIA) works by assuming all risk management controls have been bypassed, essentially assuming that the worst has happened, and then estimating the impact.

Some of the considerations that should be taken into account when performing a BIA:

- a) Scope
- b) Plan
- c) Balance
- d) Know the objective
- e) Follow-up

The NIST SP 800-34, Rev. 1 document on how a CPMT should conduct a BIA in three stages:

- a) Determine mission/business process and recovery criticality
- b) Identify resource requirements
- c) Identify recovery priorities for system resources

The first major BIA task is the analysis and prioritization of business processes within an organization, based on its mission. A business process is a task performed by an organization or organizational sub-unit in support of an organization's overall mission. Potential issues arising in the prioritization of one department or business process over another, and note that decisions regarding which business processes are the most critical are the responsibility of senior management. A weighted analysis table can be used to assess the overall importance of specific business functions. The BIA questionnaire, can be used to assess impacts of different business functions on an organization. The recommendations made by NIST regarding the use of categories, such as low impact, moderate impact, and high impact, to organize security objectives.

The following key recovery measures:

- a) Recovery Time Objective (RTO) is the maximum amount of time a system resource can be unavailable before there is unacceptable impact on other system resources.
- b) Recovery Point Objective (RPO) is the point in time, prior to disruption or outage, to which mission/business process data can be recovered after an outage.
- c) Maximum Tolerable Downtime (MTD), which represents the maximum amount of time that a system can be down.
- d) Work Recovery Time (WRT) is an extension of RTO that measures the amount of effort

(time) required to get a business function operation after a technology element is recovered.

Longer interruptions result in larger impacts to an organization, and note that solutions that reduce the RTO are typically more expensive. The importance of identifying, classifying, and prioritizing information assets, in order to simplify the assessment of priorities and relative values on mission/business processes. How an organization uses a priority list to determine necessary resources required to recover processes and assets. The last stage of BIA involves the prioritizing of resources associated with mission/business processes, and the use of weighted tables.

A simple valuation and classification scale, using values such as Primary/Secondary/Tertiary, or Critical/Very Important/Important/Routine.

#### *Contingency Planning Policies*

There is a need to have a proper policy environment for assisting with the BIA process and the creation of planning components, such as the IR, DR, and BC.

#### *Incident Response*

Incident response plan (IR plan) is a plan designed to deal with the effects of an unexpected event, and incident response planning (IRP) involves the preparation for an unexpected event.

Incident response (IR) can be explained as the procedures that commence when an incident occurs. Born out of crisis, the modern Computer Security Incident Response Team, or CSIRT (pronounced ‘see-sert’) is responsible for coordinating the response to an organization’s computer security incidents.

#### *Incident Response Policy*

The key components of a typical IR policy that are recommended by NIST, are the statement of management commitment and purpose / objectives of the policy.

#### *Incident Response Planning*

The characteristics of an event that make up an information security incident:

- a. It is directed against information assets
- b. It has a realistic chance of success
- c. It threatens confidentiality / integrity / availability of information resources and assets

Incident response is a reactive measure, rather than a preventive one. An organization’s IR plan is created by a CISO or IT manager, and the IR plan should outline the roles and responsibilities

of IR team members, as well as critical contacts that should be notified when an incident occurs.

The three sets of incident-handling procedures: before, during and after the incident. The execution of an IR plan is typically the duty of the CSIRT, which is a team of professionals who diagnose and respond to an incident.

The three basic phases of incident response actions:

- a. Detection
- b. Reaction
- c. Recovery

Additional options that can be used by an organization to protect information and assist in the recovery process:

- a. Traditional data backups
- b. Electronic vaulting
- c. Remote journaling
- d. Database shadowing

### *Detecting Incidents*

Incident classification as the process of examining an incident, or incident candidate, to determine if it qualifies as a genuine incident. This determination is made by the IR team. Some of the indicators of an actual incident:

- a. Presence of unfamiliar files
- b. Presence or execution of unknown programs or processes
- c. Unusual consumption of computing resources
- d. Unusual system crashes

List some probable indicators of an actual incident:

- a. Activities at unexpected times
- b. Presence of new accounts
- c. Reported attacks
- d. Notification from IDPS

The following list consists of definite indicators of an incident:

- a. Use of dormant accounts
- b. Changes to logs

- c. Presence of hacker tools
- d. Notifications by partner or peer
- e. Notification by hacker

When the following actual incidents are confirmed, the corresponding IR must be immediately activated:

- a. Loss of availability
- b. Loss of integrity
- c. Loss of confidentiality
- d. Violation of policy
- e. Violation of law or regulation

### *Reacting to Incidents*

The move from the detection phase to the reaction phase, once an actual incident has occurred. The reaction phase should be described as involving recovery processes, notification of key personnel, assignment of tasks, and documentation of the incident.

An alert roster is a document that lists contact information for personnel that must be notified of an actual incident. This list can be sequential or hierarchical.

An alert message is a scripted description of the incident containing enough information for each member of an alert list to implement relevant portions of the IR plan.

Notification procedures should occur after personnel on the alert roster have been notified, such as informing general management, legal, communications, and human resources departments.

An incident should be documented as it is occurring, and the documentation should include the who, what, when, where, why, and how of each action taken.

Incident containment is consisting of two tasks: stopping the incident and recovering control of affected systems. Examples of potential containment strategies, is the application of access lists, disabling compromised user accounts, or stopping all computers and devices.

### *Recovering from Incidents*

The step of incident recovery, occurs after an incident has been contained and system control has been regained.

Incident damage assessment, documents the extent of damage to an organization, and evidence should be preserved in this step.

An after-action review (AAR) is a detailed examination of events that have occurred, starting with first detection and ending with the final recovery.

### *Disaster Recovery*

Disaster recovery planning (DRP) is involving the preparation for and recovery from a disaster, regardless of cause. When a disaster is detected, the disaster recovery plan (DR plan) is activated.

The role of the DR response teams (DRRTs), is to actually implement the DR plan in the event of a disaster. List some of the most common DRRTs.

### *The Disaster Recovery Process*

Two criteria for determining a disaster:

1. An organization is unable to contain or control the impact of an incident
2. Level of damage from an incident is so severe that it prevents quick recovery

Eight-steps adapted from the seven-step program from NIST regarding the DRP process:

1. Organize the DR team
2. Develop the DR planning policy statement
3. Review the BIA
4. Identify preventive controls
5. Create DR strategies
6. Develop the DR plan document
7. Ensure DR plan testing, training, and exercises
8. Ensure DR plan maintenance

### *Disaster Recovery Policy*

The DR policy, is developed soon after the formation of a DR team, and list the key elements in a DR policy:

- a. Purpose
- b. Scope
- c. Roles and responsibilities
- d. Resource requirements
- e. Training requirements
- f. Exercise and testing schedules

- g. Plan maintenance schedule
- h. Special considerations

### *Disaster Classification*

A disaster might be classified, such as whether an event is a natural disaster or man-made disaster. Note that disasters can be classified as rapid-onset disasters, which occur without warning, or slow-onset disasters, which occur over time.

### *Planning to Recover*

Human resource considerations in a disaster recovery scenario are important, and the use of cross-training to ensure quick restoration of an organization is imperative.

Some of the key elements that a CPMT should build into a DR plan:

- a. Clear delegation of roles and responsibilities
- b. Execution of the alert roster and notification of key personnel
- c. Clear establishment of priorities
- d. Procedures for documentation of the disaster
- e. Action steps to mitigate the impact of the disaster on the operations of the organization
- f. Alternative implementations for the various systems components, should primary version be unavailable

### *Responding to the Disaster*

The necessity for flexibility in a DR plan, in order to handle disaster events that may overwhelm DR plans is important.

### *Simple Disaster Recovery Plan*

Discuss the nine steps within a simple DR plan, and note that a larger organization will most likely require a more complex DR plan. Outline the following steps:

- a. Name of company
- b. Date of completion or update of the plan and the date of the most recent test
- c. Staff to be called in the event of a disaster
- d. Emergency services to be called (if needed) in event of a disaster
- e. Locations of in-house emergency equipment and supplies
- f. Sources of off-site equipment and supplies
- g. Salvage priority list

- h. Agency disaster recovery procedures
- i. Follow-up assessment

### *Business Continuity*

Business continuity planning (BCP) ensures that critical business functions can continue if a disaster occurs. A BC plan is usually managed by the organization's CEO and is activated and executed at the same time as a DR plan when the disaster is major or long term and requires more complex restoration of information and IT resources.

The first step in contingency efforts is the development of policy, followed by planning.

### *Business Continuity Policy*

BCP begins with the development of a BC policy, and list the key sections of a BP policy:

- a. Purpose
- b. Scope
- c. Roles and responsibilities
- d. Resource requirements
- e. Training requirements
- f. Exercise and testing schedules
- g. Plan maintenance schedule
- h. Special considerations

One of the most important pieces of a BC plan involves the identification of critical business functions.

The importance of testing the health of an offsite facility regularly, as well as looking for better alternative offsite locations.

### *Continuity Strategies*

Different strategies for CP and BC planning exist, and note the three different types of usage strategies:

- a. Hot site, which duplicates resources and requires only the latest backup and personnel to function.
- b. Warm site, similar to a hot site, but lacks some of the same services and typically doesn't have all necessary software applications available
- c. Cold site, provides bare minimum services, without computer hardware. A cold site is

essentially an empty room with heating / cooling, and electrical service.

The three different strategies for shared use of a facility when needed for contingency options:

- a. Timeshare, typically operated in conjunction with a business partner or organization, with an advantage in cost and a disadvantage in total amount of hardware required.
- b. Service bureau, which provides services for a fee, typically under contract agreement.
- c. Mutual agreement, which is typically a contract between two organizations in which the organizations agree to assist each other in the event of a disaster.

#### *Timing and Sequence of CP Elements*

The concurrent nature of the BC plan and the DR plan when damage is major or long term. Despite the close relationship of the IR, DR, and BC within CP, each has a distinct place, separate role, and unique planning requirement.

#### *Crisis Management*

Crisis management (CM) is the action steps that affect people inside and outside of an organization that are taken during and after a disaster. Some organizations plan for crisis management is a completely separate process.

The roles performed by a crisis management team:

- a. Supporting personnel and their loved ones during the crisis
- b. Keeping the public informed about an event and the actions being taken
- c. Communicating with major customers, suppliers, partners, regulatory agencies, industry organizations, the media, and other interested parties

The importance of the crisis management team (CMT) establishing a base of operations or command center near the site of the crisis as soon as possible. Note the three primary responsibilities of a CMT:

- a. Verifying personnel status
- b. Activating the alert roster
- c. Coordinating with emergency services

#### *Business Resumption*

The DR and BC plans can be combined into a single document, known as the business resumption plan (BR plan). Note that this plan should be separate from the IR plan. The BC plan template is provided by the Federal Agency Security Practices section of the NIST's CSRC.

### *Testing Contingency Plans*

The importance of testing a contingency plan to discover areas for improvement. Four strategies that can be used to test contingency plans:

- a. Desk check
- b. Structured walk-through (or talk-through / chalk talk)
- c. Simulation
- d. Full interruption testing

There is a need to perform continuous process improvement (CPI). Note that CPI can occur from rehearsing plans and from reviewing previous disasters to determine what can be improved.

### *Managing Investigations in the Organization*

Digital forensics are based on traditional forensics, which is the application of methodical investigatory techniques to present evidence of crimes in a court or court-like setting.

Digital forensics includes the preservation, identification, extraction, documentation and interpretation of computer media for evidentiary and/or root cause analysis. Evidentiary material (EM) or items of potential evidentiary value, should be noted as any information that may be useful to an organization's legal-based or policy-based case against a suspect. e-discovery is the identification and preservation of EM related to a specific legal action, and note that digital forensics tools and methods may be used to carry out e-discovery. The two different purposes for which digital forensics can be used:

- a. To investigate allegations of digital malfeasance
- b. To perform root cause analysis

Digital malfeasance is a crime against or using digital media, computer technology, or related components. Some investigations can be handled by organizational personnel, while others may require involvement of law enforcement.

### *Digital Forensics Team*

Most organizations cannot sustain a permanent digital forensics team, but use outsourcing to assign the analysis to a regional expert. InfoSec personnel should be familiar with forensic processes, so that EM is not damaged or destroyed.

## *Digital Forensics Methodology*

All investigations utilizing digital forensics follow the same basic methodology:

- a. Identify relevant items of evidentiary value (EM)
- b. Acquire (seize) the evidence without alteration or damage
- c. Take steps to assure that the evidence is at every stage verifiably authentic and is unchanged from the time it was seized
- d. Analyze the data without risking modification or unauthorized access
- e. Report the findings to the proper authority

An organization may want to seek legal advice or consult with local or state law enforcement when seeking to perform digital forensics. Digital forensics team identifies potential EM and its probable location, and the importance of documenting this information in a search warrant or authorization document.

Chain of evidence or chain of custody procedures, involve detailed documentation of the collection, storage, transfer, and ownership of collected evidence from crime scene through its presentation in court. Evidence is authenticated by establishing that an analyzed copy or image is a true and accurate replica of the source EM.

## *Law Enforcement Involvement*

There is responsibility to notify proper authorities, such as the FBI, when an incident violates civil or criminal law. There are advantages and disadvantages of involving law enforcement. One advantage is that law enforcement typically has more resources for dealing with an incident. A disadvantage is that an organization may lose control of the chain of events following an incident.

## *Disaster Recovery is not the same as Cybersecurity Recovery*

It's a common misconception that disaster recovery and cybersecurity recovery are one in the same. Although they are similar and have some overlap, disaster recovery's primary objective is to provide business continuity after disruption from man-made or natural causes. Security recovery, on the other hand, protects data assets after a data breach.

"The nature of the threats within security recovery plans are more dynamic than within disaster recovery... for example, recent ransomware attacks, such as WannaCry, are incredibly destructive and require security recovery plans to examine how to effectively respond to new threats and risks," says Mark Testoni, president and CEO of SAP National Security Services. Most security experts recommend different plans with complementary policies and procedures.

## Here's How to Develop a Cybersecurity Recovery Plan

	<b>Disaster recovery plan</b>	<b>Security recovery plan</b>
<b>Primary objective</b>	Provide business continuity after disruption from man-made or natural causes	Protect data assets after a data breach
<b>Response requirements</b>	Open communication with stakeholders, focus on rapid data recovery	A stealthy approach that includes evidence collection and preservation, and root cause analysis
<b>Tactical differences</b>	Rapid, accurate data recovery	Protective controls focused on preventing future loss
<b>Plan management</b>	Dedicated team that focuses on best practices and lessons learned from disaster recovery experiences	Dedicated team that keeps up to date on new cyber security threats and modifies the plan accordingly

CSO

Figure: Differences in disaster recovery plan versus security recovery plan (Source: CSOonline.com)

At the end of the day, both plans are part of a larger security objective to ensure the confidentiality, integrity, and availability of your company's systems and data assets. Disaster recovery directly ties into availability objectives for information security. However, most organizations don't have a true understanding of which elements impact availability.

For instance, most DRPs start with a secondary location for running data replication between their primary site and secondary DR site. Consider that a cyberattack may corrupt data, in which case the DR implementation will not protect the information, as the corrupted data would be replicated to both locations. To avoid this, you should use layered defense tools, and build relevant controls for your risk management process.

## Annotated Bibliography

### Required Materials

To achieve the educational needs of this unit the following material is used:

#### Primary Material

Chapter 10 of Michael E. Whitman, Herbert J. Mattord, *Management of Information Security, Fifth Edition*. Cengage Learning, 2017, ISBN-13: 978-1-305-50125-6.

Brotby, K., 2009. Information security governance: A practical development and implementation approach (Vol. 53). John Wiley & Sons.

### **Supportive material**

Smith, D., 1990. Beyond contingency planning: Towards a model of crisis management. *Industrial Crisis Quarterly*, 4(4), pp.263-275.

Lentzos, F. and Rose, N., 2009. Governing insecurity: contingency planning, protection, resilience. *Economy and Society*, 38(2), pp.230-254.

NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems

## **Self-Assessment Exercises**

### **Exercise 7.1**

List your thoughts when considering contingency planning for ransomware and DoS attacks. Find some real cyberattacks that did not involve contingency planning and describe how many data were lost and how the company recovered from disaster.

## **Recommended time for the student to work**

Estimated 15 hours

# INFORMATION SECURITY MAINTENANCE

8<sup>th</sup> Week

## Summary

Upon successfully implementing and testing a new and improved security profile, an organization might begin feeling more confident about the level of protection it is providing for its information assets. However, this should not be the case. By the time the organization has completed implementing the changes mandated by an upgraded security program, a good deal of time has passed. In that time, everything that is dynamic in the organization's environment will have changed.

## Introductory Remarks

Some of the factors that are likely to change and affect an organization's information security environment:

- The acquisition of new assets and the divestiture of old assets
- The emergence of vulnerabilities associated with new or existing assets
- Shifting business priorities
- The formation of new partnerships
- The dissolution of old partnerships
- The departure of personnel who are trained, educated, and aware of policies, procedures, and technologies
- The hiring of personnel.

If an organization deals successfully with change and has created procedures and systems that can be adjusted to the environment, the security program will probably continue to work well.

### *Security Management Maintenance Models*

To manage and operate the ongoing security program; the information security community must adopt a management maintenance model. In general, management models are frameworks that structure the tasks of managing a particular set of activities or business functions.

*NIST SP 800-100 Information Security Handbook: A Guide for Managers*

The NIST SP 800-100, is a guide to information security governance which provides managerial guidance for the establishment and implementation of an information security program. The handbook addresses the ongoing tasks expected of an information security manager once the program is working and day-to-day operations are established. There are thirteen areas of information security management presented in the SP 800-100. The following describe monitoring actions for the 13 information security areas:

An effective information security governance program requires constant review. Table 12-1 provides a broad overview of key ongoing activities that can assist in monitoring and improving an agency's information governance activities. Agencies should monitor the status of their programs to ensure that:

- Ongoing information security activities are providing appropriate support to the agency mission.
- Policies and procedures are current and aligned with evolving technologies, if appropriate.
- Controls are accomplishing their intended purpose.

Awareness and training is the backbone of an information security program, ensuring that all users are both aware and trained on a minimum level of information security. Capital planning and investment control, implements a formal enterprise capital planning and investment control process for the investment life cycle resulting in a seven-step process for prioritizing security investments.

The NIST SP 800-47 approach includes a four phase (plan, establish, maintain, and disconnect) plan for all interconnected systems.

The value of performance measurement: with this type program, organizations develop information security metrics that measure the effectiveness of their security program and provide data to be analyzed and used by program managers and system owners to isolate problems, justify investment requests, and target funds to the areas in need of improvement. It is important to monitor the performance of security systems and their underlying IT infrastructure to determine if they are working effectively. The 60% rule can be used by security personnel when exploring the issues of system and network performance.

Security planning, found in strategic, tactical and operational plans must be developed in alignment with and support organizational and IT plans, goals, and objectives. Information

technology contingency planning consists of a process for recovery and documentation of procedures for conducting recovery. Contingency plan must always be in a ready state for use immediately upon notification.

Risk management is a cycle that is fundamental to the information security program and its continuous improvement. The principal goal is to protect the organization and its ability to perform its mission. Certification, accreditation, and security assessments as a monitoring program that implements the following, as a minimum:

- Configuration management and configuration control processes for the information system.
- Security impact analyses on changes to the information system.
- Assessment of selected security controls in the information system and reporting of the system's security status to appropriate agency officials.

Security services and products acquisition, suggest that when acquiring information security products, organizations are encouraged to conduct a cost benefit analysis—one that also includes the costs associated with risk mitigation. This cost benefit analysis should include a life cycle cost estimate for the status quo and one for each identified alternative while highlighting the benefits associated with each alternative. A well-defined incident response capability helps the organization detect incidents rapidly, minimize loss and destruction, identify weaknesses, and restore IT operations rapidly. The configuration and change management process is one that involves the continuous monitoring and management of changes to information systems or networks. The CM process identifies the steps required to ensure that all changes are properly requested, evaluated, and authorized. The CM process also provides a detailed, step-by-step procedure for identifying, processing, tracking, and documenting changes.

The five steps of the CM process:

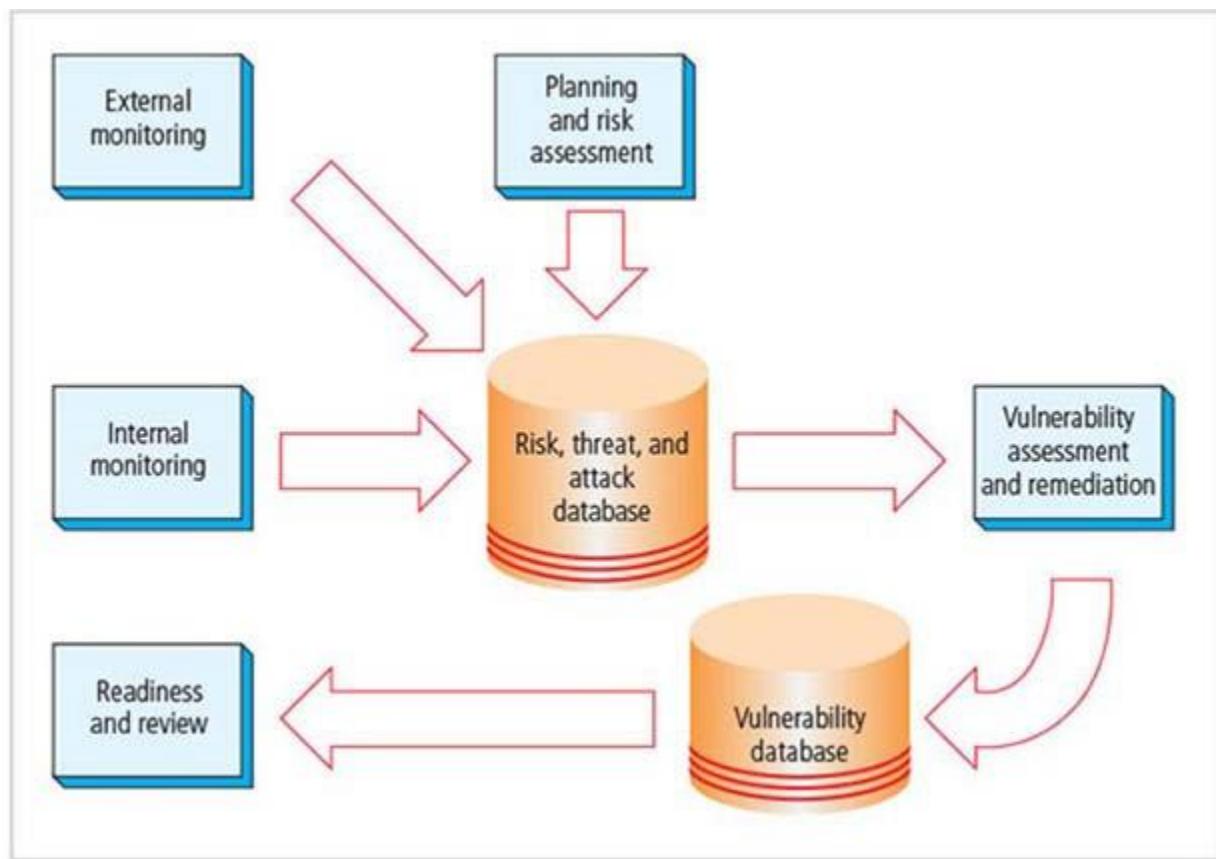
- Step 1: Identify change
- Step 2: Evaluate change request
- Step 3: Implementation decision
- Step 4: Implement Approved Change Request
- Step 5: Continuous monitoring

### *The Security Maintenance Model*

A maintenance model is intended to complement the chosen management model and focus

organizational effort on maintaining systems. The following figure, illustrates a full maintenance program and serves as a framework for the discussion of maintenance that follows. The model is based on five subject areas or domains:

- External monitoring
- Internal monitoring
- Planning and risk assessment
- Vulnerability assessment and remediation
- Readiness and review



### Monitoring the External Environment

The objective of the external monitoring domain in the maintenance model is to provide the early awareness of new and emerging threats, threat agents, vulnerabilities, and attacks that are needed to mount an effective and timely defense. External monitoring entails collecting intelligence from data sources, and then giving that intelligence context and meaning for use by decision makers within the organization. The purpose of and types of data sources.

Acquiring data about threats, threat agents, vulnerabilities, and attacks is not difficult. There are many sources of raw intelligence and few costs associated with gathering it. What is challenging and can be expensive is turning this flood of good and timely data into information that decision makers can use.

External intelligence can come from these classes of sources:

- Vendors
- CERT organizations
- Public network sources
- Membership sites

Regardless of how the organization collects external monitoring data, the CISO evaluates the actions and personnel needed to act on the information. The responsibility for establishing a viable external monitoring program includes the following tasks:

- Staff the function with people who understand the technical aspects of information security, have a comprehensive understanding of the IT infrastructure, and have a thorough grounding in the organization's business operations.
- Provide documented and repeatable procedures.
- Train the primary and backup staff assigned to perform the monitoring tasks.
- Equip assigned staff with proper access and tools to perform the monitoring function.
- Cultivate expertise among the monitoring analysts so that they can cull meaningful summaries and actionable alerts from the vast flow of raw intelligence.
- Develop suitable communications methods for moving processed intelligence to designated internal decision makers in all three communities of interest.
- Integrate the incident response plan with the results of the external monitoring process for appropriate, timely responses.

Monitoring, escalation, and incident response processes.

- The basic function of the external monitoring process is to monitor activity, report results, and escalate warnings. The optimum approach for escalation is based on a thorough integration of the monitoring process into the IRP.
- The monitoring process has three primary deliverables:

- Specific warning bulletins issued when developing threats and specific attacks pose a measurable risk to the organization
- Periodic summaries of external information
- Detailed intelligence on the highest risk warnings

Data collection and management.

- Over time, the external monitoring processes should capture knowledge about the external environment in a format that can be referenced both across the organization as threats emerge and for historical use.
- In the final analysis, external monitoring collects raw intelligence, filters it for relevance to the organizations, assigns it a relative risk impact, and communicates these findings to the decision makers in time to make a difference.

#### *Monitoring the Internal Environment*

It is just as important to monitor the internal computing environment, as it is to monitor the external environment. The primary goal of the internal monitoring domain is to maintain an informed awareness of the state of all of the organization's networks, information systems, and information security defenses. Internal monitoring is accomplished by:

- Building and maintaining an inventory of network devices and channels, IT infrastructure and applications, and information security infrastructure elements.
- Leading the IT governance process within the organization to integrate the inevitable changes found in all network, IT, and information security programs.
- Monitoring of IT activity in real time using IDPS to detect and initiate responses to specific actions or trends of events that introduce risk to the organization's assets.

Monitoring the internal state of the organization's networks and systems.

- Network characterization and inventory process.
- Each organization should have a carefully planned and fully populated inventory for all network devices, communication channels, and computing devices.
- The process of collecting this information is called characterization, as it is the systematic collection of the characteristics of the network and computer devices that are present in the environment. Once the characteristics have been identified, they must be carefully organized and stored using a manual or automated mechanism that allows timely retrieval and rapid integration of disparate facts.

IDPSs work should work as follows:

- To be effective, IDPS must be integrated into the maintenance process. An endless flow of alert messages makes little difference to the effectiveness of the information security program.
- The most important value of the raw intelligence provided by the IDPS is that it can be used to prevent risk in the future.
- Whether the organization outsources IDPS monitoring, staffs IDPS monitoring 24/7, staffs IDPS monitoring during business hours, or merely ignores the real-time alerts from IDPS, the log files from the IDPS engines can be mined for information that can be added to the internal monitoring knowledge base.
- Another element of IDPS monitoring is traffic analysis. Analyzing attack signatures for unsuccessful system attacks can identify weaknesses in various security efforts.

To detect differences:

- One approach that has achieved good results is to perform various combinations of manual and automated difference analysis to identify changes to the internal environment. Table 12-8 shows how several kinds of difference analyses can be used.
- Difference analysis is a procedure that compares the current state of a network segment (the systems and services it offers) against a known previous state of that same network segment (the baseline of systems and services).

### *Planning and Risk Assessment*

The primary objective of the planning and risk assessment domain is to keep a lookout over the entire information security program. This is done by identifying and planning ongoing information security activities that further reduce risk.

The risk assessment group also identifies and documents risks introduced by both IT projects and information security projects. The group also identifies and documents risks that may be latent in the present environment.

The primary objectives of this domain as follows:

- Establish a formal information security program review process that complements and supports both IT planning and strategic planning.
- Institute formal project identification, selection, planning, and management processes for follow-up activities that augment the current security program.
- Coordinate with IT project teams to introduce risk assessment and review for all IT projects,

so that risks introduced from the launching of IT projects are identified, documented, and factored into projects decisions.

- Integrate a mindset of risk assessment across the organization to encourage the performance of risk assessment activities when any technology system is implemented or modified.

The main issues surrounding information security program planning and review.

- An organization should periodically review its ongoing information security program and any planning for enhancements and extensions.
- The strategic planning process should examine the future IT needs of the organization and the impact those needs will have on information security.
- A recommended approach is to take advantage of the fact that most larger organizations have annual capital budget planning cycles.
- Projects that organizations might fund to maintain, extend, or enhance the information security program will arise in almost every planning cycle. Larger information security projects should be broken into smaller, incremental projects. Doing this is important for several reasons:
  - Smaller projects tend to have more manageable impacts on the networks and users.
  - Larger projects tend to complicate the change control process in the implementation phase.
  - Shorter planning, development, and implementation schedules reduce any uncertainty for IT planners and financial sponsors.
  - Most large projects can easily be broken into smaller projects, providing more opportunities to change direction and gain flexibility as events occur and circumstances change.

The process of conducting security risk assessments (RA).

- A key component in the engine that drives change in the information security program is a relatively straightforward process called risk assessment.
- The RA is a method of identifying and documenting the risk that a project, process, or action introduces to the organization and may also offer suggestions for controls that can reduce that risk.
- The information security group often finds itself in the business of coordinating the preparation of many different types of RA documents, including:
  - Network connectivity RA
  - Business partner RA
  - Application RA
  - Vulnerability RA

- Privacy RA
- Acquisition or divesture RA
- Other RAs

### *Vulnerability Assessment and Remediation*

The primary goal of the vulnerability assessment and remediation domain is to identify specific, documented vulnerabilities and remediate them in a timely fashion. This is accomplished by:

- Using vulnerability assessment procedures that are documented to safely collect intelligence about networks, platforms, dial-in modems, and wireless network systems.
- Documenting background information and providing tested remediation procedures for the reported vulnerabilities.
- Tracking vulnerabilities from the time they are identified until they are remediated; or the risk of loss has been accepted by an authorized member of management.
- Communicating vulnerability information, including an estimate of the risk and detailed remediation plans to the owners of vulnerable systems.
- Reporting on the status of vulnerabilities that have been identified.
- Ensuring that the proper level of management is involved in deciding to accept the risk of loss associated with unprepared vulnerabilities.

Even though the exact procedures can vary, the following five vulnerability assessment processes can serve many organizations as they attempt to balance the intrusiveness of vulnerability assessment with the need for a stable and productive production environment.

- Internet VA
- Intranet VA
- Platform security validation
- Wireless VA
- Modem VA

Pen test is a level of sophistication beyond vulnerability testing. A penetration test, or pen test, is usually performed periodically as part of a full security audit.

Vulnerability testing is usually performed inside the organization's security perimeter with complete knowledge of the networks' configuration and operations, pen testing can be conducted in one of two ways—black box pen testing and white box pen testing.

In black box pen testing, or blind testing, the “attacker” has no prior knowledge of the systems or

network configurations and thus must investigate the organization's information infrastructure from scratch. In white box testing, also known as full-disclosure testing, the organization provides information about the systems to be examined, allowing for a faster, more focused test.

A common methodology for pen testing is found in the Open Source Security Testing Methodology Manual (OSSTMM), a manual on security testing and analysis created by Pete Herzog and provided by ISECOM, the nonprofit Institute for Security and Open Methodologies.

A number of penetration testing certifications are available for people who are interested in this aspect of security testing.

The Internet vulnerability assessment process is designed to find and document the vulnerabilities that may be present in the public-facing network of the organization.

Skilled attackers from this direction can take advantage of any loophole or flaw; this assessment is usually performed against all public-facing addresses, using every possible penetration testing approach.

- The steps in the process are:
  - Planning, scheduling, and notification of the penetration testing: Large organizations often take an entire month to perform the data collection phase, using nights and weekends and avoiding change control blackout windows.
  - Target selection: Working from the network characterization elements that are stored in the risk, threat, and attack database, the penetration targets are selected.
  - Test selection: Using the external monitoring intelligence generated previously, the test engine is configured for the tests to be performed.
  - Scanning: The penetration test engine is unleashed at the scheduled time using the planned target list and test selection. The results of the entire test run are logged in text log files for analysis.
  - Analysis: A knowledgeable and experienced vulnerability analyst screens the test results for the vulnerabilities logged during scanning.
  - Record keeping: The organization records the details of the documented vulnerability in the vulnerability database, identifying the logical and physical characteristics and assigning a response risk level to the vulnerability to differentiate the truly urgent from the merely critical.

The intranet vulnerability assessment process is designed to find and document selected

vulnerabilities that are likely to be present on the internal network of the organization. Attackers from this direction are often internal members of the organization, affiliates of business partners, or automated attack vectors (such as viruses and worms).

This assessment is usually performed against selected critical internal devices with a known, high value by using selective penetration testing. The steps in the process are almost identical to the steps in the Internet vulnerability assessment, except as noted below.

- Planning, scheduling, and notification of the penetration testing: There will be substantially more systems to assess. Intranet administrators often prefer that penetration testing is performed during working hours.
- Target selection: At first, the penetration test scanning and analysis should focus on testing only the highest value, most critical systems. As the configuration of these systems is improved, and fewer candidate vulnerabilities are found in the scanning step, the target list can be expanded.
- Test selection: The selection of the tests to be performed usually evolves over time to correspond with the evolution of the threat environment. Most organizations focus their intranet scanning efforts on a few very critical vulnerabilities at first, and then expand the test pool to include more scripts.
- Scanning: Just as it is in Internet scanning, the process should be monitored so that if an invasive penetration test causes disruption, it can be reported for repair.
- Analysis: Follows the same three steps as Internet analysis: classify, validate, and document.
- Record keeping: Identical to the one followed in an Internet vulnerability analysis.

The platform security validation (PSV) process is designed to find and document the vulnerabilities that may be present because of misconfigured systems in use within the organization.

These misconfigured systems fail to comply with company policy or standards as adopted by the IT governance groups and communicated in the information security and awareness program.

Fortunately, automated measurement systems are available to help with the intensive process of validating the compliance of platform configuration with policy.

The approach and terminology based on the NetIQ product:

- Product selection
- Policy configuration

- Deployment
- Measurement
- Exclusion handling
- Reporting
- Remediation

The wireless vulnerability assessment process is designed to find and document the vulnerabilities that may be present in the wireless local area networks of the organization.

Because attackers from this direction are likely to take advantage of any loophole or flaw, this assessment is usually performed against all publicly accessible areas, using every possible wireless penetration testing approach.

The steps in the process are as follows:

- Planning, scheduling, and notification of wireless penetration testing
- Target selection
- Test selection
- Scanning
- Analysis

The vulnerability database, like the risk, threat, and attack database, both store and tracks information. It should provide details about the vulnerability being reported as well as linkage to the information assets that are characterized in the risk, threat, and attack database.

While this can be done through manual data storage, the low cost and ease of use associated with relational databases make them a more realistic choice.

The data stored in the vulnerability database should include:

- A unique vulnerability ID number for reporting and tracking remediation actions
- Linkage to the risk, threat, and attack database based on the physical information asset underlying the vulnerability
- Vulnerability details usually based on the test script used for the scanning step of the process
- Dates and times of notification and remediation activities

- Current status of the vulnerability instance
- Comments
- Other fields as needed to manage the reporting and tracking processes in the remediation phase

The vulnerability database is an essential part of effective remediation as it helps organizations avoid losing track of specific vulnerability instances as they are reported and remediated.

The process of remediating vulnerabilities.

- The objective of remediation is to repair the flaw that is causing a vulnerability instance or remove the risk associated with the vulnerability. Alternatively, informed decision makers with the proper authority can accept the risk.
- When approaching the remediation process, it is important to recognize that building relationships with those who control the information assets is the key to success. Success depends on the organization adopting a team approach to remediation in place of push and pull between departments.

The acceptance or transference of risk involves the following issues.

- In some instances, risk must simply be acknowledged as part of the organization's business process.
- The information security professional must assure the general management community that the decision to accept the risk was made by properly informed decision makers. These decision makers must have the proper level of authority to accept the risk.

Threat removal involves the following issues.

- In some circumstances, threats can be removed without repairing the vulnerability. The vulnerability can no longer be exploited, and the risk has been removed.
- Other vulnerabilities may be mitigated by inexpensive controls.

Vulnerability repair involves the following issues.

- The optimum solution in most cases is to repair the vulnerability. Applying patch software or implementing a workaround to the vulnerability often accomplishes this.
- The most common repair is the application of a software patch to make the system function in the expected fashion and to remove the vulnerability.

### *Readiness and Review*

The primary goal of the readiness and review domain is to keep the information security program functioning as designed and to keep it continuously improving over time. This is accomplished by:

- Policy review: Sound policy needs to be reviewed and refreshed from time to time to provide a current foundation for the information security program.
- Program review: Major planning components should be reviewed on a periodic basis to ensure they are current, accurate, and appropriate.
- Rehearsals: When possible, major plan elements should be rehearsed.

### *Digital Forensics*

When the asset attacked is in the purview of the CISO he is expected to understand how policies and laws require the matter to be managed. The investigation of what happened and how is called digital forensics.

Digital forensics is based on the field of traditional forensics. Forensics is the coherent application of methodical investigatory techniques to present evidence of crimes in a court or court-like setting.

Digital forensics involves the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis. Like traditional forensics, it follows clear, well-defined methodologies, but still tends to be as much art as science.

Evidentiary material (EM), also known as an item of potential evidentiary value, is any information that could potentially support the organization's legal or policy-based case against a suspect.

Digital forensics can be used for two key purposes.

- To investigate allegations of digital malfeasance: Such an investigation requires digital forensics to gather, analyze, and report the findings.
- To perform root cause analysis: If the organization suspects an attack was successful, digital forensics can be used to examine the path and methodology used to gain unauthorized access, as well as to determine how pervasive and successful the attack was.

The organization must choose one of two approaches when employing digital forensics.

- Protect and forget: This approach, also known as patch and proceed, focuses on the defense of the data and the systems that house, use, and transmit it.
- Apprehend and prosecute: This approach, also known as pursue and prosecute, focuses on

the identification and apprehension of responsible individuals, with additional attention to the collection and preservation of potential EM that might support administrative or criminal prosecution.

## Aim/Objectives

The last and most important discussion addresses information security maintenance and change. Week 8 presents the ongoing technical and administrative evaluation of the security program. This chapter explores ongoing risk analysis, risk evaluation, and measurement, all of which are part of risk management. From Internet penetration testing to wireless network risk assessment, this chapter explores the special considerations that must be taken to analyze the variety of vulnerabilities in an organization.

## Learning Outcomes

In this chapter, your students will learn to:

- Discuss the need for ongoing maintenance of the information security program.
- List the recommended security management models.
- Define a model for a full maintenance program.
- Identify the key factors involved in monitoring the external and internal environment.
- Describe how planning, risk assessment, vulnerability assessment, and remediation tie into information security maintenance.
- Explain how to build readiness and review procedures into information security maintenance.
- Discuss digital forensics, and describe how to manage it.
- Describe the process of acquiring, analyzing, and maintaining potential evidentiary material.

## Key Words

Digital forensics	Risk assessment	Planing
Vulnerability assessment	Remediation	Maintenance

## Annotated Bibliography

### Required Materials

To achieve the educational needs of this unit the following material is used:

#### Primary Material

Chapter 12 Michael E. Whitman / Michael J., *Principles of Information Security, Sixth Edition*. Cengage Learning, 2018, ISBN-13 9781337102063.

#### Supportive material

Lipson, H.F. and Fisher, D.A., 1999, September. Survivability—a new technical and business perspective on security. In Proceedings of the 1999 workshop on New security paradigms (pp. 33-39). ACM.

Ellison, R.J., Fisher, D.A., Linger, R.C., Lipson, H.F., Longstaff, T.A. and Mead, N.R., 1999. Survivability: Protecting your critical systems. IEEE Internet Computing, 3(6), pp.55-63.

## Self-Assessment Exercises

### Exercise 8.1

What is the difference between vulnerability assessment and penetration testing?

## Individual Assignment (20 points)

Individual Assignment carrying 20% of the total grade. Search the Web for two or more sites that discuss the ongoing responsibilities of the security manager. What other components of security management can be adapted for use in the security management model?

## **Recommended time for the student to work**

35 hours

## LEGAL AND REGULATORY REQUIREMENTS

9<sup>th</sup> Week

### Summary

Relevant laws and legal/regulatory frameworks on the national, European and international level. Different types of law related to cyberattacks – computer as the means, computer as a victim. Problems of jurisdiction, borderless nature of cybercrime, relevance and importance of data protection and privacy, investigations.

### Introductory Remarks

#### *Security Governance and Regulation.*

As a future information security professional, you must understand the scope of an organization's legal and ethical responsibilities. To minimize liabilities and reduce risks from electronic and physical threats, and to reduce all losses from legal action, the information security practitioner must understand the current legal environment, stay current with new laws and regulations, and watch for new issues as they emerge.

#### *Law and Ethics in Information Security*

Laws are rules that mandate or prohibit certain behavior in society. They are drawn from ethics, which define socially acceptable behaviors. Ethics, are based on cultural mores and express the fixed moral attitudes or customs of a particular group. Some ethics are recognized as universal among cultures.

Even if there is no breach of criminal law, there can still be liability. Liability, is the legal obligation of an entity that extends beyond criminal or contract law; it includes the legal obligation to make restitution, or to compensate for wrongs committed by an organization or its employees. An organization increases its liability if it refuses to take measures known as due care. Due care has been taken when an organization makes sure that every employee knows what is acceptable or unacceptable behavior, and knows the consequences of illegal or unethical actions. Due diligence requires that an organization make a valid effort to protect others and continually maintain this level of effort.

Under the U.S. legal system, any court can impose its authority over an individual or organization if it can establish jurisdiction—that is, the court's right to hear a case if the wrong was committed in its territory or involving its citizenry. Trying a case in the injured party's home area is usually favorable to the injured party.

### *Policy Versus Law*

Within an organization, information security professionals help maintain security via the establishment and enforcement of policies. Policies function as laws and must be crafted with the same care to ensure that they are complete, appropriate, and fairly applied to everyone in the workplace. The difference between a policy and a law, which is that ignorance of a policy is an acceptable defense.

For a policy to be enforceable, it must meet the following five criteria and demonstrate that it has done so:

- Dissemination (distribution)
- Review (reading)
- Comprehension (understanding)
- Compliance (agreement)
- Uniform enforcement

Only when all of these conditions are met can an organization penalize employees who violate the policy, without fear of legal retribution.

### *Types of Law*

Civil law, which represents a wide variety of laws that govern a nation or state and deal with the relationships and conflicts between organizational entities and people.

Criminal law addresses violations harmful to society and is actively enforced by the state.

Private law regulates the relationship between the individual and the organization, and encompasses family law, commercial law, and labor law.

Public law regulates the structure and administration of government agencies and their relationships with citizens, employees, and other governments, providing careful checks and balances. Examples of public law include criminal, administrative, and constitutional law.

### *General Computer Crime Laws*

The **Computer Fraud and Abuse Act of 1986 (CFA Act)** is the cornerstone of many computer-related federal laws and enforcement efforts. The **National Information Infrastructure Protection Act of 1996**, was amended the CFA Act in October 1996. It modified several sections of the CFA and increased the penalties for selected crimes. The severity of the penalty depends on the value of the information obtained and whether the offense is judged to have been committed:

- For purposes of commercial advantage
- For private financial gain
- In furtherance of a criminal act

The **USA PATRIOT Act of 2001**, modified a wide range of existing laws to provide law enforcement agencies with broader latitude of actions in order to combat terrorism-related activities.

In 2006, this act was amended with the **USA PATRIOT Improvement and Reauthorization Act**, which made permanent 14 of the 16 expanded powers of the Department of Homeland Security and the FBI in investigating terrorist activity. The act also reset the date of expiration written into the law for certain wiretaps under the Foreign Intelligence Surveillance Act of 1978 (FISA) and revised many of the criminal penalties and procedures associated with criminal and terrorist activities.

The **PATRIOT Sunset Extension Act of 2011** provided extension of certain provisions of the USA PATRIOT Act, specifically those related to wiretaps, searching of business records, and the surveillance of suspected terrorists.

In May 2015, the U.S. Senate failed to extend the USA PATRIOT Act, resulting in its expiration on June 1, 2015. However, President Obama signed the USA FREEDOM Act into law in June 2015, as a replacement. The **Computer Security Act of 1987** was one of the first attempts to protect federal computer systems by establishing minimum acceptable security practices. The **Federal Information Security Management Act (FISMA)**, which mandates all federal agencies to establish information security programs to protect information assets.

### *Privacy*

The issue of privacy has become one of the hottest topics in information security at the beginning of the 21st century. The ability to collect information, combine facts from separate sources, and

merge it all with other information has resulted in databases of information that were previously impossible to set up. In response to pressure for privacy protection, the number of statutes addressing an individual's right to privacy has grown.

The **Privacy of Customer Information Section** of the common carrier regulation specifies that any proprietary information shall be used explicitly for providing services, and not for any marketing purposes. It also stipulates that carriers cannot disclose this information except when necessary to provide their services. The only other exception is when a customer requests the disclosure of information, and then the disclosure is restricted to that customer's information only.

The **Federal Privacy Act of 1974** regulates government agencies and holds them accountable if they release private information about individuals or businesses without permission.

The **Electronic Communications Privacy Act of 1986** regulates the interception of wire, electronic, and oral communications. The ECPA works in conjunction with the **Fourth Amendment of the U.S. Constitution**, which protects citizens from unlawful search and seizure.

The **Health Insurance Portability & Accountability Act Of 1996 (HIPAA)**, also known as the **Kennedy-Kassebaum Act**, protects the confidentiality and security of health-care data by establishing and enforcing standards and by standardizing electronic data interchange. This act impacts all health-care organizations. The act requires organizations that retain health-care information to use information security mechanisms to protect this information, as well as policies and procedures to maintain this security. The act also requires a comprehensive assessment of the organization's information security systems, policies, and procedures. The standards provide patients the right to know who has access to their information and who has accessed it. The standards also restrict the use of health information to the minimum necessary for the health-care services required.

HIPAA has five fundamental principles:

- Consumer control of medical information
- Boundaries on the use of medical information
- Accountability to maintain the privacy of specified types of information
- Balance of public responsibility for the use of medical information for the greater good measured against impact to the individual
- Security of health information

HIPAA was updated in 2013 with a Department of Health and Human Services Regulatory Action

intended to strengthen the act's privacy and security protections.

The **Financial Services Modernization Act**, or **Gramm-Leach-Bliley Act of 1999**, requires all financial institutions to disclose their privacy policies on the sharing of nonpublic personal information. It also requires due notice to customers so that they can request that their information not be shared with third parties.

### *Identify Theft*

Identity theft. - The Federal Trade Commission defines identity theft as "occurring when someone uses your personally identifying information (PII), like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes".

In May of 2006, President Bush signed an Executive Order creating the Identity Theft Task Force. The goals of this group are to create a strategic plan to improve efforts of the government and private organizations and individuals in combating identity theft. The group seeks better coordination among groups, more effective prosecution of criminals engaged in these activities, and methods to increase restitution made to victims. While numerous states have passed identity theft laws, at the federal level the primary legislation is the **Fraud And Related Activity In Connection With Identification Documents, Authentication Features, And Information** (Title 18, U.S.C. § 1028), which criminalizes creation, reproduction, transfer, possession, or use of unauthorized or false identification documents or document-making equipment. Penalties for such offenses range from one to 25 years in prison and fines as determined by the courts.

The Federal Trade Commission recommends the following four steps people can take when they suspect a theft of identity has occurred:

- Place an initial fraud alert
- Order your credit reports
- Create an identity theft report
- Monitor your progress

### *Export and Espionage Laws*

An attempt to protect American ingenuity, intellectual property, and competitive advantage, Congress passed the **Economic Espionage Act (EEA)** in 1996. This law attempts to prevent trade secrets from being illegally shared.

The **Security and Freedom through Encryption Act of 1999 (SAFE)**, which provides guidance on the use of encryption and provides measures of protection from government intervention.

### *U.S. Copyright Law*

Intellectual property is recognized as a protected asset in the United States. U.S. copyright laws extend this privilege to the published word, including electronic formats.

Fair use of copyrighted materials includes their use to support news reporting, teaching, scholarship, and a number of other related activities, as long as the use is for educational or library purposes, not for profit, and is not excessive.

As long as proper acknowledgment is provided to the original author of such works, including a proper citation, and the work is not represented as one's own, it is entirely permissible to include portions of someone else's work as reference.

### *Financial Reporting*

The **Sarbanes-Oxley Act of 2002**, is a critical piece of legislation that affects the executive management of publicly traded corporations and public accounting firms, seeks to improve the reliability and accuracy of financial reporting, as well as increase the accountability of corporate governance, in publicly traded companies.

Executives working in firms covered by this law will seek assurance on the reliability and quality of information systems from senior information technology managers who, in turn, will likely ask information security managers to verify the confidentiality and integrity of those same information systems.

### *Freedom of Information Act of 1966 (FOIA)*

The **Freedom of Information Act**, allows any person to request access to federal agency records or information not determined to be a matter of national security. U.S. government agencies are required to disclose any requested information upon receipt of a written request.

Some information is protected from disclosure, however, and the act does not apply to state or local government agencies or to private businesses or individuals, although many states have their own version of the FOIA.

### *Payment Card Industry Data Security Standards (PCI DSS)*

The Payment Card Industry (PCI) Security Standards Council offers a standard of performance to which participating organizations must comply. Point out that it is not a law, but is a standard designed to enhance the security of customers' account data.

The six areas that PCI DSS addresses:

Area 1: Build and maintain a secure network and systems

Area 2: Protect cardholder data

Area 3: Maintain a vulnerability management program

Area 4: Implement strong access control measures

Area 5: Regularly monitor and test networks

Area 6: Maintain an information security policy

#### *[State and Local Regulations](#)*

In addition to the national and international restrictions placed on organizational use of computer technology, each state or locality may have a number of its own applicable laws and regulations.

The information security professional must understand state laws and regulations and ensure that the organization's security policies and procedures comply with those laws and regulations.

#### *[International Laws and Legal Bodies](#)*

It is important for IT professionals and information security practitioners to realize that when their organizations do business on the Internet, they do business globally. As a result, these professionals must be sensitive to the laws and ethical values of many different cultures, societies, and countries. While there are currently few international laws relating to privacy and information security, the few that do exist are important but are limited in their enforceability.

#### *[U.K. Computer Security Laws](#)*

United Kingdom laws on computer security are:

- a. Computer Misuse Act 1990
- b. Privacy and Electronic Communications (EC Directive) Regulations 2003
- c. Police and Justice Act 2006
- d. Personal Internet Safety 2007

#### Australian Computer Security Laws

Australian laws:

- a. Privacy Act 1988
- b. Telecommunications Act 1997
- c. Corporations Act 2001
- d. Spam Act 2003

e. Cybercrime Legislation Amendment Bill 2011

*Council of Europe Convention on Cybercrime*

The Council of Europe adopted the **Convention on Cybercrime** in 2001.

- It provides for the creation of an international task force to oversee a range of security functions associated with Internet activities for standardized technology laws across international borders.
- It also attempts to improve the effectiveness of international investigations into breaches of technology law.

While 34 countries attended the signing in November 2001, 41 nations, including the U.S. and U.K., have ratified the Convention as of January 2014. While the U.S. is technically not a “member state of the council of Europe” but does participate in the convention. The Convention on Cybercrime lacks any realistic provisions for enforcement. The overall goal of the convention is to simplify the acquisition of information for law enforcement agencies in certain types of international crimes and it also simplifies the extradition process.

*World Trade Organization and the Agreement on Trade-Related Aspects of Intellectual Property Rights*

The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), created by the World Trade Organization (WTO), introduced intellectual property rules into the multilateral trade system.

The WTO TRIPS agreement, covers five issues:

1. How basic principles of the trading system and other international intellectual property agreements should be applied
2. How to give adequate protection to intellectual property rights
3. How countries should enforce those rights adequately in their own territories
4. How to settle disputes on intellectual property between members of the WTO
5. Special transitional arrangements during the period when the new system is being introduced

*Digital Millennium Copyright Act*

The **Digital Millennium Copyright Act (DMCA)** is the American contribution to an international effort to reduce the impact of copyright, trademark, and privacy infringement, especially through the removal of technological copyright protection measures.

In 1995 the European Union had adopted **Directive 95/46/EC**, which added protection for individuals with regard to the processing of personal data and the use and movement of such data. The United Kingdom has also already implemented a version of this law called the **Database Right**, in order to comply with Directive 95/46/EC.

The DMCA provisions are:

- Prohibits the circumvention of protections and countermeasures implemented by copyright owners to control access to protected content.
- Prohibits the manufacture of devices to circumvent protections and countermeasures to control access to protected content.
- Bans trafficking in devices manufactured to circumvent protections and countermeasures to control access to protected content
- Prohibits the altering of information attached or imbedded into copyrighted material.
- Excludes Internet service providers from certain forms of contributory copyright infringement.

In June 2016, the US and the European Union signed an agreement that superseded the prior agreement known as “Safe Harbor”. Discuss the new agreement.

### *Ethics and Information Security*

Many professional groups have explicit rules governing ethical behavior in the workplace. Note that the information technology field and the information security field do not have a binding code of ethics. Instead, professional associations (such as the Association for Computing Machinery and the Information Systems Security Association) and accreditation agencies (such as ISC2) work to establish the profession's ethical codes of conduct.

### *Ethical Differences Across Cultures*

Cultural differences can make it difficult to determine what is and is not ethical, especially when it comes to the use of computers. Difficulties arise when one nationality's ethical behavior violates the ethics of another national group. Approximately 90 percent of all software is created in the United States.

A study published in 1999, examined computer use ethics of nine nations: Singapore, Hong Kong, the United States, England, Australia, Sweden, Wales, and the Netherlands.

- This study selected a number of computer-use vignettes and presented them to students in universities in these nine nations.
- The responses indicated a degree of ethical sensitivity or knowledge about the performance

of the individuals in the short case studies.

- The scenarios were grouped into three categories of ethical computer use: software license infringement, illicit use, and misuse of corporate resources.

Software license infringement:

- Overall, most of the nations studied had similar attitudes toward software piracy.
- Statistically speaking, only the United States and the Netherlands had attitudes that differed substantially from those of all other countries examined.
- The United States was significantly less tolerant of piracy, while the Netherlands was significantly more permissive.
- Peer pressure, the lack of legal disincentives, the lack of punitive measures, or any one of a number of other reasons could also explain why these alleged piracy centers were not oblivious to intellectual property laws.

Illicit use.

- The study respondents unilaterally condemned viruses, hacking, and other forms of system abuse.
- There were, however, different degrees of tolerance for such activities among the groups.

Misuse of corporate resources.

- In general, individuals displayed a rather lenient view of personal use of company equipment.
- Only Singapore and Hong Kong view personal use of company equipment as unethical.
- Overall, the researchers found that there is a general agreement among nationalities as to what is acceptable or unacceptable computer use.
- There is, however, a range of views as to whether some actions are moderately or highly unacceptable.

### *Ethics and Education*

Employees must be trained and kept aware of a number of topics related to information security, not the least of which is the expected behaviors of an ethical employee.

This is especially important in information security, as many employees may not have the formal technical training to understand that their behavior is unethical or even illegal.

### *Deterring Unethical and Illegal Behavior*

It is the responsibility of information security personnel to do everything in their power to deter

illegal, immoral, or unethical behavior and to use policy, education and training, and technology to protect information and systems.

The three general causes of unethical and illegal behavior: ignorance, accident, and intent. Deterrence is the best method for preventing an illegal or unethical activity. Laws, policies, and technical controls are all examples of deterrents.

It is generally agreed that laws and policies and their associated penalties only deter if three conditions are present:

- Fear of penalty
- Probability of being apprehended
- Probability of penalty being applied

#### *Codes of Ethics and Professional Organizations*

Many professional organizations have established codes of conduct or codes of ethics that members are expected to follow. Codes of ethics can have a positive effect on an individual's judgment regarding computer use. Table 3-3 discusses some of the Information Security Professional Organizations available.

Professional Organization	Web Resource Location	Description	Focus
Association of Computing Machinery	www.acm.org	Code of 24 imperatives of personal and ethical responsibilities for security professionals	Ethics of security professionals
Information Systems Audit and Control Association	www.isaca.org	Focus on auditing, information security, business process analysis, and IS planning through the OSA and OSM certifications	Tasks and knowledge required of the information systems audit professional

information Systems Security Association	<a href="http://www.issa.org">www.issa.org</a>	Professional association of information systems security professionals; provides education forum, publications, and peer networking for members	Professional security information sharing
International Information Systems Security Certification Consortium (ISQ2)	<a href="http://www.isc2.org">www.isc2.org</a>	International consortium dedicated to improving the quality of security professionals through SSCP and CISSP certifications	Requires certificants to follow its published code of ethics
SANS Institute's Global Information Assurance Certification	<a href="http://www.giac.org">www.giac.org</a>	GIAC certifications focus on four security areas: security administration, security management IT audits, and software security, these areas have standard, gold, and expert levels	Requires certificants to follow its published code of ethic

Security professionals must act ethically and according to the policies and procedures of their employers, their professional organizations, and the laws of society.

#### *Major Information Security Professional Organizations*

The Association of Computing Machinery (ACM).

- The **ACM** ([www.acm.org](http://www.acm.org)) is a respected professional society, originally established in 1947, as “the world's first educational and scientific computing society.”
- The ACM's code of ethics requires members to perform their duties in a manner befitting an ethical computing professional. The code contains specific references to protecting the confidentiality of information, causing no harm, protecting the privacy of others, and respecting the intellectual property and copyrights of others.

The International Information Systems Security Certification Consortium, Inc. (ISC)<sup>2</sup>.

- The **(ISC)<sup>2</sup>** ([www.isc2.org](http://www.isc2.org)) is a nonprofit organization that focuses on the development and implementation of information security certifications and credentials.
- The code of ethics put forth by (ISC)<sup>2</sup> is primarily designed for information security

professionals who have earned a certification from (ISC)<sup>2</sup>.

- This code focuses on four mandatory canons:
- Protect society, the commonwealth, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principals.
- Advance and protect the profession.

The System Administration, Networking, and Security Institute (SANS).

- **SANS** ([www.sans.org](http://www.sans.org)) is a professional organization with a large membership dedicated to the protection of information and systems.
- SANS offers a set of certifications called the Global Information Assurance Certification or GIAC.

The Information Systems Audit and Control Association (ISACA).

- **ISACA** ([www.isaca.org](http://www.isaca.org)) is a professional association with a focus on auditing, control, and security.
- Although it does not focus exclusively on information security, the Certified Information Systems Auditor (CISA) certification does contain many information security components.
- The ISACA also has a code of ethics for its professionals. It requires many of the same high standards for ethical performance as the other organizations and certifications.

The Information Systems Security Association (ISSA).

- **ISSA** ([www.issa.org](http://www.issa.org)) is a nonprofit society of information security professionals.
- As a professional association, its primary mission is to bring together qualified practitioners of information security for information exchange and educational development.
- ISSA also promotes a code of ethics whose focus is “promoting management practices that will ensure the confidentiality, integrity, and availability of organizational information resources.”

### *Key U.S. Federal Agencies*

The key U.S. federal agencies charged with the protection of American information resources and the investigation of threats to, or attacks on, these resources.

#### *Department of Homeland Security*

The Department of Homeland Security (DHS), was created in 2003 through the Homeland

Security Act of 2002, which was passed in response to the events of September 11, 2001.

- DHS is made up of five directorates, or divisions, through which it carries out its mission of protecting the people, as well as the physical and informational assets, of the United States.
- The Directorate of Information & Infrastructure works to create and enhance capabilities used to discover and respond to attacks on national information systems and critical infrastructure.
- The Science and Technology Directorate is responsible for research and development activities in support of homeland defense.
- This effort is guided by a continuing examination of the vulnerabilities throughout the national infrastructure.
- It sponsors the emerging best practices developed to counter threats and weaknesses in the system.

The U.S. Computer Emergency Readiness Team (US-CERT) is a division of DHS's National Cybersecurity and Communications Integration Center (NCCIC). Note that DHS provides mechanisms to report: phishing, malware, software vulnerabilities, and other types of security incidents.

#### *U.S. Secret Service*

The U.S. Secret Service, was relocated from the Department of the Treasury to the DHS in 2002.

- The Secret Service has been charged with the responsibility of safeguarding the nation's financial infrastructure and payments systems the integrity of the economy.
- Discuss the strategic objectives that address cybersecurity-related activity.

#### *Federal Bureau of Investigation (FBI)*

The FBI is the primary U.S. law enforcement agency and it investigates both traditional crimes and cybercrimes.

The key priorities of the FBI, when investigating cybercrime:

- Computer and network intrusions
- Identity theft
- Fraud

The National InfraGard Program began as a cooperative effort between the FBI's Cleveland field office and local technology professionals, which was established in January of 2001.

- Every FBI field office has established an InfraGard chapter and collaborates with

public and private organizations and the academic community to share information about attacks, vulnerabilities, and threats.

- The National InfraGard Program serves its members in four basic ways:
  - Maintains an intrusion alert network using encrypted e-mail
  - Maintains a secure Web site for communication about suspicious activity or intrusions
  - Sponsors local chapter activities
  - Operates a help desk for questions

### *National Security Agency (NSA)*

The National Security Agency (NSA):

- The NSA is responsible for signal intelligence and information system security.
- The NSA's Information Assurance Directorate (IAD) provides information security "solutions including the technologies, specifications and criteria, products, product configurations, tools, standards, operational doctrine, and support activities needed to implement the project, detect and report, and respond elements of cyber defense."
- Explain that the IAD is responsible for the protection of systems that store, process, and transmit classified information.
- The NSA has a program to certify curriculum in information security.
- The Information Assurance Courseware Evaluation process examines information security courses in an institution and, if accepted, provides a three-year accreditation.
- Graduates of these programs receive certificates that indicate this accreditation.

### **Additional Resources**

1. Electronic Frontier Foundation  
<http://www.eff.org/>
2. Summary of the HIPAA Security Rule  
<https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>
3. National Security Agency (NSA)  
<https://www.nsa.gov/>
4. Elcomsoft Verdict: Not Guilty  
<http://news.cnet.com/2100-1023-978176.html>
5. Legal in US: Jailbreaking your iPhone, ripping a DVD for educational purposes  
<http://www.crunchgear.com/2010/07/26/now-legal-in-the-u-s-jailbreaking-your-iphone->

## Aim/Objectives

As a fundamental part of the SecSDLC investigation process, a careful examination of current legislation, regulation, and common ethical expectations of both national and international entities provides key insights into the regulatory constraints that govern business. This chapter examines several key laws that shape the field of information security, and it presents a detailed examination of computer ethics necessary to better educate those implementing security. Although ignorance of the law is no excuse, it's considered better than negligence (knowing and doing nothing). This chapter also presents several legal and ethical issues that are commonly found in today's organizations, as well as formal and professional organizations that promote ethics and legal responsibility.

## Learning Outcomes

In this chapter, students will learn to:

- Describe the functions of and relationships among laws, regulations, and professional organizations in information security.
- Explain the differences between laws and ethics
- Identify major national laws that affect the practice of information security
- Discuss the role of privacy as it applies to law and ethics in information security

## Key Words

Security Governance	Regulation	Computer Crime
Privacy	Identity theft	Export
Espionage	Financial reporting	Ethics

## Annotated Bibliography

### Required Materials

To achieve the educational needs of this unit the following material is used:

## **Primary Material**

Chapter 3 of Michael E. Whitman / Michael J., *Principles of Information Security, Sixth Edition*. Cengage Learning, 2018, ISBN-13 9781337102063.

## **Supportive material**

Sittig, D.F., Gonzalez, D. and Singh, H., 2014. Contingency planning for electronic health record-based care continuity: a survey of recommended practices. International journal of medical informatics, 83(11), pp.797-804.

Schoppmann, M.J. and Sanders, D.L., 2004. HIPAA compliance: The law, reality, and recommendations. Journal of the American College of Radiology, 1(10), pp.728-733.

## **Self-Assessment Exercises**

### **Exercise 9.1**

Using the resources in your library, find out what laws your country has passed to prosecute computer crime.

### **Recommended time for the student to work**

15 hours

### Summary

#### *The World Wide What? Defining Cyberspace*

Part of why cyberspace is so difficult to define lies not only in its expansive, global nature, but also in the fact that the cyberspace of today is almost unrecognizable compared to its humble beginnings. The US Department of Defense can be considered the godfather of cyberspace, dating back to its funding of early computing and original networks like ARPANET (more on this soon). Yet even the Pentagon has struggled to keep pace as its baby has grown up.

### Introductory Remarks

Over the years, it has issued at least twelve different definitions of what it thinks of as cyberspace. These range from the “notional environment in which digitized information is communicated over computer networks,” which was rejected because it implied cyberspace was only for communication and largely imaginary, to a “domain characterized by the use of electronics and the electromagnetic spectrum,” which was also rejected as it encompassed everything from computers and missiles to the light from the sun.

In its latest attempt in 2008, the Pentagon assembled a team of experts who took over a year to agree on yet another definition of cyberspace. This time they termed it “the global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.” It is certainly a more detailed definition but so dense that one almost wishes we could go back to just the “tubes.”

At its essence, cyberspace is the realm of computer networks (and the users behind them) in which information is stored, shared, and communicated online. But rather than trying to find the exact perfectly worded definition of cyberspace, it is more useful to unpack what these definitions are trying to get at. What are the essential features that not only compose cyberspace, but also make it unique? Cyberspace is first and foremost an information environment. It is made up of digitized data that is created, stored, and, most importantly, shared. This means that it is not

merely a physical place and thus defies measurement in any kind of physical dimension. But cyberspace isn't purely virtual. It comprises the computers that store data plus the systems and infrastructure that allow it to flow. This includes the Internet of networked computers, closed intranets, cellular technologies, fiber-optic cables, and space-based communications.

While we often use "Internet" as shorthand for the digital world, cyberspace has also come to encompass the people behind those computers and how their connectivity has altered their society. One of the key features, then, of cyberspace is that its systems and technologies are man-made. As such, cyberspace is defined as much by the cognitive realm as by the physical or digital. Perceptions matter, and they inform cyberspace's internal structures in everything from how the names within cyberspace are assigned to who owns which parts of the infrastructure that powers and uses it.

This leads to an important point often misunderstood. Cyberspace may be global, but it is not "stateless" or a "global commons," both terms frequently used in government and media. Just as we humans have artificially divided our globe into territories that we call "nations" and, in turn, our human species into various groups like "nationalities," the same can be done with cyberspace. It relies on physical infrastructure and human users who are tied to geography, and thus is also subject to our human notions like sovereignty, nationality, and property. Or, to put it another way, cyberspace's divisions are as real as the meaningful, but also imaginary.

But cyberspace, like life, is constantly evolving. The hybrid combination of technology and the humans that use it is always changing, inexorably altering everything from cyberspace's size and scale to the technical and political rules that seek to guide it. As one expert put it, "The geography of cyberspace is much more mutable than other environments. Mountains and oceans are hard to move, but portions of cyberspace can be turned on and off with the click of a switch." The essential features remain the same, but the topography is in constant flux. The cyberspace of today is both the same as but also utterly different from the cyberspace of 1982.

### *What Are the Threats?*

The defining aspects of threats are the actor and the consequence.

The acknowledgment of an actor forces us to think strategically about threats. The adversary can pick and choose which vulnerability to exploit for any given goal. This implies that we must not only address a range of vulnerabilities with respect to any given threat, but also understand that the threat may evolve in response to our defensive actions.

There are many kinds of bad actors, but it is too easy to get lulled into using media clichés like “hackers” to lump them all together. An actor’s objective is a good place to start when parcelling them out. In the variety of attacks cited by the senators above, the Citigroup attackers wanted account details about bank customers with an ultimate goal of financial theft. In the attack on RSA, the attackers wanted key business secrets in order to spy on other companies. For Stuxnet (a case we’ll explore further in Part II), the attackers wanted to disrupt industrial control processes involved in uranium enrichment, so as to sabotage the Iranian nuclear program.

Finally, it is useful to acknowledge when the danger comes from one of your own. As cases like Bradley Manning and WikiLeaks or Edward Snowden and the NSA scandal illustrate, the “insider threat” is particularly tough because the actor can search for vulnerabilities from within systems designed only to be used by trusted actors. Insiders can have much better perspectives on what is valuable and how best to leverage that value, whether they are trying to steal secrets or sabotage an operation.

It is also important to consider whether the threat actor wants to attack you, or just wants to attack. Some attacks target specific actors for particular reasons, while other adversaries go after a certain objective regardless of who may control it. Untargeted malicious code could, for example, infect a machine via e-mail, search for stored credit card details of anyone, and relay those details back to its master without any human involvement. The key difference in these automated attacks is one of cost, both from the attacker’s and the defender’s perspective. For the attacker, automation hugely reduces cost, as they don’t have to invest in all the tasks needed, from selecting the victim to identifying the asset to coordinating the attack. Their attack costs roughly the same no matter how many victims they get. A targeted attack, on the other hand, can quickly scale up in costs as the number of victims rises. These same dynamics shape the expected returns. To be willing to invest in targeted attacks, an attacker must have a higher expected return value with each victim. By contrast, automated attacks can have much lower profit margins. The good news is that there are only three things you can do to a computer: steal its data, misuse credentials, and hijack resources. Unfortunately, our dependence on information systems means that a skilled actor could wreak a lot of damage by doing any one of those.

Stolen data can reveal the strategic plans of a country or undermine the competitiveness of an entire industry. Stolen credentials can give the ability to change or destroy code and data, changing payrolls or opening up dams, as well as the ability to cover tracks. Hijacking resources can prevent a company from reaching customers or deny an army the ability to communicate.

In the end, there are many things that can happen, but they have to be caused by someone. Threats should be assessed by understanding potential bad actors, what they are trying to do, and why.

Different vulnerabilities allow an attacker to achieve different goals. In some cases, it might be the ability to read confidential data. Or the goal could be the ultimate prize—compromise of the entire system. When the attacker has such “root access,” the ability to execute any command, the victim is completely vulnerable, or what hackers call “pwned” (An apocryphal story is that a hacker meant to type that a target was now “owned.” But he typed too fast, mistakenly hit the p key right next to the o , and a cool term was born.)

Often the easiest way to gain control of the system is simply to ask. A time-honored tradition for breaking into systems from hacking’s early days is to call up a low-level employee, claim to be from technical support, and ask for the person’s password. This falls into the category of what is known as “social engineering,” manipulating people into revealing confidential information and thereby helping the attacker. The manipulation can take many forms, often with the attacker trying to set up a scenario designed to encourage cooperation through psychological mechanisms. Fear is a powerful motivator. When a user’s computer displays a message threatening to expose activities on a pornographic website, fear of exposure can motivate payment. More often, however, users just follow social cues. In our daily lives, we regularly encounter problems that need fixing, like a program that won’t close until you just “click here,” or people who need our help. A particularly common form of social engineering is the “phishing” attack. Phishing e-mails look like official e-mails from the victim’s bank, employer, or some other trusted entity. They claim to require some action by the victim, perhaps to correct an account error or see a message on Facebook, and fool victims into visiting a web page where they are asked to enter their credentials. If the victim enters his or her account details, the attacker can now do anything with that information, from transfer money to read confidential e-mails. The phony credentials web page may have a URL that looks similar to the authentic one. If you don’t look closely, maybe [www.paypai.com](http://www.paypai.com) looks like [www.paypal.com](http://www.paypal.com). In sophisticated phishing attacks, the fake page may also actually log the user into the real website to minimize the chance of detection.

Malicious software, or “malware,” is a pre packaged exploitation of a vulnerability. There is often a “payload” of instructions detailing what the system should do after it has been compromised. Some types of malware contain instructions for reproduction, in order to spread the attack. “Worms” spread themselves automatically over the network. In some cases, this can be sufficient to cause drastic harm: many of the worms that attacked Microsoft Windows in the late 1990s and

early 2000s had no direct malicious effect but still overwhelmed corporate networks because they tried to send out an exponentially large number of copies. One worm even sought to patch vulnerable computers, a “good worm,” but still managed to cripple networks. Other vulnerabilities have been exploited to allow the attacker to capture valuable personal data or, in an anarchistic turn, just destroy data on the victim’s computer.

DDoS attacks target the subsystems that handle connections to the Internet, such as web servers. Their vulnerabilities are based on the principle that responding to an incoming query consumes computational and bandwidth resources. If someone were to call your phone incessantly, you would first lose the ability to concentrate and then lose the ability to use your phone for any other purpose. Similarly, in the cyber world, if the attacker can overwhelm the connection link, the system is effectively removed from the Internet.

### *Governing cybercrime in the European Union*

EU approaches towards cybercrime have developed in parallel to its information society strategies such as the eEurope (European Commission 1999) initiative for enhancing the use and enjoying the benefits of digital technologies in a socially inclusive way. As the EU’s aspirations to become an information society have progressed, so too have its efforts to protect those emerging benefits from criminal activity. In this context the eEurope initiative was followed by an eEurope Action Plan agreed in June 2000 at the Feira European Council, which emphasised the salience of addressing issues of network security and combating cybercrime. More specifically, the proposed approaches at this stage were both of a policy and a technical nature. For enhancing Internet security, whilst acknowledging that industry was primarily responsible for this (European Commission 1999, p.11), it also argued for the evolution of a public-private relationship for nascent industry, whereby the public sector was seen as playing a catalysing, stimulating role for private initiatives. There was a clear steer towards a hands-off metagovernance approach to reinforce private sector driven action. There was also an emphasis in the Action Plan on developing better co-operation and co-ordination related to the discussion of the Budapest Convention in different international fora.

The final report on eEurope (2003) noted some progress on the issue of Internet security, but also that use of the Directives launched remained limited. However, eEurope did provide the basis for a more comprehensive approach to network and information security by the EU. In June 2001, two parallel documents were published by the European Commission that outlined the contours of this comprehensive approach that also aimed to address crime in cyberspace. The first of

these, a communication (European Commission 2001a) entitled 'Creating a Safer Information Society by Improving the Security of Infrastructures and Combating Computer-Related Crime', proposed a series of substantial and procedural legal provisions, as well as non-legal measures to address the criminal activities domestically and transnationally, whilst also stressing the need to preserve the balance between security and respect for the fundamental rights of individuals (2001a, p.2).

In terms of substantive law, for instance, there was an emphasis on agreeing on common definitions of cybercrime, as well as common incriminations and sanctions and introducing EU enforcement mechanisms that build on the Budapest Convention to enable it to take effective action on issues such as child pornography, racism and xenophobia online. Procedurally, the central focus was on criminal law and the steer was on the improved cooperation of law and other enforcement agencies (through mutual recognition but also enhanced mechanisms), in line with EU law, to facilitate more effective responses and requests from other countries in relation to cybercrime offences. The final report on eEurope (2003) noted some progress on the issue of Internet security, but also that use of the Directives launched remained limited. However, eEurope did provide the basis for a more comprehensive approach to network and information security by the EU.

With the globalization of commerce and the growth and expected growth of e-commerce, the flexibility and the ability of the law to deal with contracts concluded in cyber-space are severely tested. There is a widely held belief that the law is slow moving and unable to properly cope with the demands of modern technology. In fact, despite the ancient history of the law of contract, it is surprisingly resilient and flexible and therefore able to deal with new phenomena without any major changes. As the electronic transaction takes place virtually there is not a necessary physical proof of the transaction is absent. The proof that does exist is electronic, and is capable of easy manipulation and therefore not very *trustworthy*. This fact further undermines consumer confidence in the medium. The law of contract has developed over time on the assumption that the contracting parties are in the presence of one another. Communications from a distance are the exception rather than the rule and special rules have been developed for these situations. A contract becomes final and binding once there is consensus or agreement between the parties. Consensus is reached once both parties have the same rights and obligations in mind and have agreed to them. This is the so-called subjective or will theory of consensus.

In web-trading the offer may either be contained on the website if that is the intention of the e-business, or a website may simply contain an "invitation" to do business. Any order sent to the

website, will constitute a purchase offer which may be accepted or rejected by the website. Thus only the “confirmation” of the offer will usually constitute an acceptance by the webtrader of the offer made by the client. However, if the website offering is itself viewed as a valid offer, the mere placement of the order by the client will constitute an acceptance.

Thus, moving transactions to an electronic environment has two important consequences. Firstly, in many cases it is difficult to know when one can rely on the integrity and authenticity of an electronic message. This, of course, makes difficult those decisions that involve entering into contracts, especially for significant transactions. Secondly, this lack of reliability can make proving a case in court difficult at best. For example, if the defendant denies making the signature that is appended to an electronic document, it may be virtually impossible for the plaintiff to prove the authenticity of that electronic signature in the absence of additional evidence.

If e-commerce is to reach its full potential, however, parties must be able to *trust* electronic communications for a wide range of transactions, particularly ones where the size of the transaction is substantial or the nature of the transaction is of higher risk. In such cases, a party relying on an electronic communication will need to know whether the message is authentic, whether the integrity of its contents is intact, and whether the relying party can establish both of those facts in court if a dispute arises.

One of the growing problems in relation to cybercrime given developments in the IT environment and the increased use of the Internet more generally across different dimensions is the exploitation of the online world for the purposes of abusing children. Whilst the EU has had legislation in place since 2004 to address the issue of sexual abuse and exploitation of children and child pornography, this legislation was reconsidered precisely because of such new developments and the opportunities that this brought to criminals. The 2004 framework decision was deemed inadequate in several ways, not least because it only introduced minimal approximation of legislation in member states, which made it difficult for national authorities and agencies to coordinate and cooperate in investigations. In addition, given that it had been operational since 2004, new forms of sexual abuse and exploitation facilitated by the Internet (for example, grooming and pornography) were not criminalised. The revised proposal submitted by the Commission in 2010 (and agreed in June 2011) sought to move beyond minimal legislation to a more hands-on meta-governance in terms of scope and substance – in criminalisation of child sexual abuse and exploitation (substantive criminal law), cross-jurisdictional investigations, proceedings, and cases, and the prevention of offences, such as, for example, national mechanisms to block access to websites with child pornography.

Whilst the E-Privacy Directive (2009) prohibited the practice of infecting computers and turning them into botnets, technological developments and the increased use of sophisticated attack methods by criminals highlighted the need for further action in order to combat this growing threat. The Directive on attacks against information systems (2010) built on a review of the implementation of its predecessor, and identified, among other things, the lack of harmonisation in the legal framework of the EU as a major obstacle to effective security as resilience in cybercrime. Indeed it represented a step-change within the governance of combating cybercrime and in particular the use of botnets.

The EU approach to cybercrime is fragmented, in the sense that there is no overarching framework but rather a series of legal and regulatory instruments that overlap, as demonstrated in the above analysis. Indeed, whilst a more comprehensive approach to cybercrime was considered an option by the EU, as was updating the Budapest Convention in the impact assessment for the Directive on attacks against information systems (2010), these were not deemed viable. Instead the EU moved to define a strategy – articulated first in a proposal for Internet security (2011) and then in a more elaborate form in the EUCSS (2013), with five clear priorities, one of which is ‘drastically reducing cybercrime’. Within this priority there is a focus on the legal dimension – national, regional and global – as well as the operational layer and coordination between and within all levels relating to cybercrime.

## Aim/Objectives

This week introduces students to cyberspace, cyberlaw and the various threats as well as other important terms like privacy, child exploitation, trust and trustworthiness seen from an EU regulatory perspective.

## Learning Outcomes

In this chapter, students will learn to:

- Describe laws governing cyberspace and analyze the role of Internet Governance in framing policies for Internet security
- Discuss different types of cybercrimes and analyze legal frameworks of different countries to deal with these cybercrimes
- Explain the importance of jurisdictional boundaries and identify the measures to overcome cross jurisdictional cyber crimes

- Illustrate the importance of ethics in legal profession and determine the appropriate ethical and legal behavior according to legal frameworks
- Identify intellectual property right issues in the cyberspace and design strategies to protect your intellectual property
- Create security policy to comply with laws governing privacy and develop the policies to ensure secure communication

## Key Words

Cyber law	Ethics	Security policy
Privacy	Legal responsibility	

## Annotated Bibliography

### Required Materials

To achieve the educational needs of this unit the following material is used:

#### Primary Material

European Commission (1999), Communication of 8 December 1999 on a Commission Initiative for the Special European Council of Lisbon, 23 and 24 March 2000 – eEurope – An Information Society for All, COM (1999) 687 Final (not published in the Official Journal).

European Commission (2001a), 'Creating a Safer Information Society by Improving the Security of Infrastructures and Combating Computer-Related Crime', COM (2000) 890, 26 January 2001.

European Parliament and the Council (2002), Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications).

European Parliament and the Council (1995), Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic

communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA

Christou, G. (2016). Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy. Springer.

### **Supportive material**

Privacy, Data Protection and Cybersecurity in Europe edited by Wolf J. Schünemann, Max-Otto Baumann

Chapter 7 of The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities By Domenic Antonucci Copyright © 2017 by John Wiley & Sons, Inc.

Danidou, Yianna, and Burkhard Schafer. "In law we trust? Trusted Computing and legal responsibility for Internet security." IFIP International Information Security Conference. Springer, Berlin, Heidelberg, 2009.

### **Activity (5 points)**

Graded activity carrying 5% of the final grade. Write an essay discussing a cyber law issue of your choice. Write 4-5 pages following extensive research of the field.

### **Recommended time for the student to work**

20 hours

# GENERAL DATA PROTECTION REGULATION (GDPR)

11<sup>th</sup> Week

## Summary

The EU's General Data Protection Regulation (GDPR) was approved in 2017, and the enforcement date of May 25, 2018 has now passed. Organisations found to be in non-compliant will face heavy fines.

## Introductory Remarks

### What is the GDPR?

The GDPR was designed to harmonize data privacy laws across Europe, bolstering privacy protection for EU citizens and empowering them to better control how their data is used. The regulation introduces the 'Rights of the Data Subjects', which essentially states that data belongs to the individual, not the organisation. For individuals, this means that they can access their personal data that's being stored, and can request changes or even removal. They also have the right to compensation if their rights are violated. For organisations, information must be held only as long as it's required, and in many cases they'll need to appoint a Data Protection Officer to ensure that personal data is not compromised.

Organisations are now facing challenges interpreting what the new regulations mean to them and understanding what they need to do to ensure compliancy. Just deploying technology is not a good answer here, as organisations need to understand the data they are storing to ensure they have a legitimate reason for holding this data. It's important to keep in mind six core principles when storing personal data. Data must be:

- Processed lawfully, fairly, and transparently
- Collected for specified, explicit, and legitimate purposes
- Relevant and limited to what is necessary
- Accurate and up to date
- Retained for only as long as necessary

- Processed in an appropriate manner to maintain security

## The Path to GDPR Compliance

Because of the greater control individuals have over their personal data, it is the organisation's duty to ensure that nothing happens to that data. There are two big questions you should ask yourself when assessing how compliant your organisation is with the GDPR:

### 1. Is the data protected?

If the personal data your organisation stores ends up compromised, the organisation will be held accountable. You must make sure your data is protected from:

- **Device failures** – This includes any physical storage component, such as disk drives, storage controllers, and data centres.
- **Logical/soft failures** – This refers to human errors such as accidental deletion/overwrite, as well as viruses and file data corruption. This currently accounts for up to 80% of data losses.
- **Security breaches** – Data must be secure from forceful entry/hacks.

Data availability must be guaranteed not only for the security and privacy of personal data, but also in the event that individuals want to make changes to their data.

### 2. Can I find the data?

The second question you should ask is around data location awareness. If someone requests their personal data, would you be able to quickly locate and procure it? Not only does the data you're storing need to be housed in GDPR-compliant systems and data centres, but the data itself needs to be searchable and well-organised. If you are not able to produce the requested data in a timely fashion, you may face fines under the new regulations.

#### *Assessment of current data privacy practices*

Compliance with data privacy regulations is not easy; in many cases, each customer must consent to each use of their personal data. They also have the right to know how companies are using their data, the right to object to that use, and can request to be forgotten from businesses. Businesses should examine their existing data privacy practices against the GDPR requirements to identify the actions they need to change or implement to meet the GDPR requirements. They may then want to identify the key compliance issues they need to focus on to implement their future projects involving the management of personal data in line with their commercial objectives

and market trends. This assessment should be cautiously carried out as it will determine what they need to do to comply with their GDPR obligations. This may include assessing the current technologies used to deliver the services to their clients, so they also help meet the GDPR requirements.

#### *Creation of a data privacy governance structure*

The creation of a data privacy governance structure is helpful to implement and drive a GDPR data privacy compliance programme. It needs to involve senior management at the outset of its inception to ensure it is incorporated into the board management's agenda and is fully supported throughout its lifecycle. It should set out the tasks, responsibilities and reporting lines of the individuals involved and should remain in place on a permanent basis to ensure continuous compliance with the GDPR. Businesses that already have a data protection officer (DPO) in place may be tasked to create a governance structure and be accountable for the overall data privacy programme. Those who do not have a DPO yet should carefully consider designating one internally or externally, whether they are required to do so.

#### *Personal data inventory*

Data controllers and processors have the responsibility to maintain records of their processing activities including the personal data flows. This is a major shift from the current European data protection regime where some Member States require prior approval of certain personal data processing activities such as the transfer of personal data. This also means that businesses will need to have a clear understanding of their data processing activities and security systems to be able to record them all. A data mapping exercise may prove useful to achieve this. This involves creating specific instrument that capture the obligations and constantly monitor and report on data processing activities. That inventory must be up-to-date and as accurate as possible as it may be subject to audit by SAs.

#### *Creating information notices*

One fundamental factor is privacy notices – how businesses explain at the point of data collection what users can expect will happen to their data. The GDPR requires data controllers to inform the data subjects about the processing activities carried out including detailing the type of data collected, the purpose for which it is collected, how it is being used and protected, the name of the organisation processing the personal data and the data subject's rights including the right of access, to object, and to erasure (the right to be forgotten). This transparency obligation means that businesses will have to comply with their notice obligations and amend their internal policies

accordingly.

#### *Consent mechanisms*

Consent is in principle a mechanism of building trust between the user and an organisation. Consent is a component of information management. It is a formal tool allowing to process (collect, store, use, etc.) user data. For users, requirement of consent offers choice. The conditions for consent are tougher to meet under the GDPR and businesses will have to review their current data processing activities which rely on consent, as well as their privacy policies. In addition, businesses will have to document the collection of consent. The GDPR sets a high standard for consent. But businesses often won't need consent. If consent is difficult, look for a different lawful basis. Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build customer trust and engagement, and enhance business reputation.

#### *Implementation of technical and organisational measures*

Data controllers and processors must implement suitable technical and organisational measures to ensure that personal data processed is securely and adequately protected. Businesses should implement security techniques such as privacy by design in their data processing activities. Additionally, they should also work alongside their cyber security teams and other business functions to ensure that the appropriate security measures are applied and comply with their clients' requirements where appropriate. Designing and organising a security protocol to fit the nature of the personal data and the harm that may result from a security breach must be clear about who in the organisation is responsible for ensuring information security; making sure there is appropriate physical and technical security, backed up by robust policies and procedures and reliable, and well-trained staff. Moreover, there should be clear documentation of these techniques as well as regular testing and updating.

#### *Data Protection Impact Assessments (DPIAs)*

DPIAs help organisations identify, assess and mitigate or minimise privacy risks with data processing activities. They're particularly relevant when a new data processing process, system or technology is being introduced. DPIAs also support the accountability principle, as they help organisations comply with the requirements of the GDPR and demonstrate that appropriate measures have been taken to ensure compliance. The GDPR mandates a DPIA be conducted where data processing "is likely to result in a high risk to the rights and freedoms of natural persons". They are crucial in showing the SAs that a business has done everything it can to

ensure data is processed in accordance with the law.

#### *Reporting personal data breaches*

The GDPR specifically outlines that reporting personal data breaches forms part of the accountability principle. Businesses will need to create formal procedures to ensure that personal data breaches are addressed appropriately and in a timely manner to mitigate the risks to the individuals affected by the breach such as misuse, loss of data, damage, rights and freedoms of the individuals. If the breach is likely to result in an elevated risk of adversely affecting individuals' rights and freedoms, businesses must inform those individuals without undue delay and ensure their clients of a robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether businesses need to notify the relevant supervisory authority and the affected individuals. Additionally, businesses must also keep a record of any personal data breaches, regardless of whether they are required to notify. Such procedures will need to be verified to ensure they work correctly.

Full GDPR compliance will not be an easy task, but you can start prepping your organisation for the enforcement date by making sure your data is protected, available, and searchable.

## **Aim/Objectives**

The General Data Protection Regulation (GDPR) is a regulation by which the European Parliament, the Council of the European Union, and the European Commission aim to strengthen and unify data protection for all individuals within the European Union (EU). GDPR came into effect on 25th May 2018 and has a significant effect on businesses' approach to data privacy compliance. Therefore, it is important for businesses to prepare for GDPR to make sure they are compliant and can manage risk accordingly.

## **Learning Outcomes**

In this chapter, students will learn to:

- be aware of their compliance responsibilities under GDPR;
- Mitigate the risk of compliance breaches;
- Encourage a better workplace culture; and
- Remove legal liability from the organization in the event of wrongdoing;

## Key Words

Accountability and governance	data processing principles	Lawful processing
Privacy rights of individuals	Valid consent	Data protection by design and by default
Transparency and privacy notices	Data breach reporting	

## Annotated Bibliography

### Required Materials

To achieve the educational needs of this unit the following material is used:

#### Primary Material

Deloitte Malta Risk Advisory, 2018, Understanding the General Data Protection Regulation (GDPR) A short walk through of the key aspects.

Organisations must meet the demands of the complex regulatory landscape, but be flexible enough that the regulatory programme keeps pace with a rapidly changing environment—all with an industry-focus. This white paper helps you to understand if your approach to regulatory risk, is designed to preserve value and power performance?

#### Supportive material

Nuvias 2018, Guide to Cyber Security Compliance with GDPR

Ernst and Young 2018, General Data Protection Regulation (GDPR): The paradigm shift in privacy August, 2018

## Self-Assessment Exercises

### Exercise 11.1

A case study will be handed to students and they will have to discuss on whether the organisations described is GDPR compliant. The essay will be 2-3 pages long.

## **Recommended time for the student to work**

15 hours

## INVITED LECTURE

12<sup>th</sup> & 13<sup>th</sup> Week

### Summary

Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on reasons behind and expected benefits of compliance requirements and on recent/future developments.

### Introductory Remarks

Possible invited organisations:

- Office of the Commissioner for Personal Data Protection
- Security risk assessment practitioners
- Compliance practitioners

### Annotated Bibliography

### Required Materials

To achieve the educational needs of this unit, all the relevant material will be at student's disposal in Blackboard for further studying.

### Group Assignment (20 points)

Group assignment carrying 20% of the total grade.

Students (in pairs) will work on cybersecurity policies for a case study given by the instructor.

### Recommended time for the student to work

Week 12: 35 hours and Week 13: 15 hours

## **REVISION WEEK AND FINAL EXAMINATION**

The final exam will contain multiple choice questions, open ended questions, closed ended questions and case studies.

### **Recommended time for the student to work**

40 hours

**Date/Time of Final Exam: TBD**

## INDICATIVE ANSWERS TO SELF-ASSESSMENT EXERCISES

### INTRODUCTION TO INFORMATION SECURITY – WEEK 2

#### Exercise 2.1

General management, IT management, and information security management are each responsible for implementing information security that protects the organization's ability to function.

Decision makers must set policy and operate their organizations in a manner that complies with complex, shifting political legislation concerning the use of technology. Management is responsible for informed policy choices, the enforcement of decisions that affect applications, and the IT infrastructures that support them. Management can also implement an effective information security program to protect the integrity and value of the organization's data.

#### Exercise 2.2

Without data, an organization will lose its record of transactions and its ability to deliver value to customers. Any business, educational institution, or government agency that functions within the modern social context of connected and responsive service relies on information systems to support these services. Protecting data is critical to these efforts.

Other assets that require protection include the ability of the organization to function, the safe operation of applications, and technology assets.

### INFORMATION SECURITY POLICY – WEEK 3

#### Exercise 3.1

Confidentiality – Policy – Storage: An example of protecting the confidentiality of class information in storage by means of policy would be issuing rules to keep access restricted to unauthorized viewers. One such rule could be to lock file cabinets that contain the information.

Confidentiality – Policy – Processing: An example of protecting the confidentiality of class information in processing by means of policy would be issuing rules to keep access restricted to

authorized viewers while information is being processed. For instance, only registered students in the class should be allowed to attend and listen to lectures.

Confidentiality – Policy – Transmission: An example of protecting the confidentiality of class information in transmission by means of policy would be issuing rules to keep access restricted to authorized viewers while information is being transmitted. For instance, a policy may require that all transmission of confidential data over public networks must be encrypted.

Confidentiality – Education – Storage: An example of protecting the confidentiality of class information in storage by means of education would be to train students and faculty about which people have authorized access to the information in storage.

Confidentiality – Education – Processing: An example of protecting the confidentiality of class information being processed by means of education would be to train students and faculty to verify whether people are authorized to get the information before class starts by using a student ID or schedule.

Confidentiality – Education – Transmission: An example of protecting the confidentiality of class information being transmitted by means of education would be to train students and faculty to close classroom doors during a lecture so that others outside could not hear it.

Confidentiality – Technology – Storage: An example of protecting the confidentiality of class information being stored by means of technology would be using locks on file cabinets that contain the information while not in use.

Confidentiality – Technology – Processing: An example of protecting the confidentiality of class information being processed by means of technology would be forcing the use of electronic IDs during classes.

Confidentiality – Technology – Transmission: An example of protecting the confidentiality of class information being transmitted by means of technology would be having a password on a class Web site.

Integrity – Policy – Storage: An example of protecting the integrity of class information being stored by means of policy would be a simple rule that only certified people may alter the information.

Integrity – Policy – Processing: An example of protecting the integrity of class information being processed by means of policy would be a rule that forces students to study in quiet areas without the help of people who are not in the class.

Integrity – Policy – Transmission: An example of protecting the integrity of class information being transmitted by means of policy would be a rule that the teacher is not allowed to drink alcohol before class.

Integrity – Education – Storage: An example of protecting the integrity of class information being stored by means of education would be teaching people who store the information the names and roles of others who are authorized to change it.

Integrity – Education – Processing: An example of protecting the integrity of class information being processed by means of education would be informing students not to risk receiving incorrect information by studying with people who are not in the class.

Integrity – Education – Transmission: An example of protecting the integrity of class information being transmitted by means of education would be providing instructors with effective ways to teach.

Integrity – Technology – Storage: An example of protecting the integrity of class information being stored by means of technology would be electronically storing all data on a device that requires authorization to modify.

Integrity – Technology – Processing: An example of protecting the integrity of class information being processed by means of technology would be creating PowerPoint presentations to verify what the teacher says.

Integrity – Technology – Transmission: An example of protecting the integrity of class information being transmitted by means of technology would be printing the PowerPoint presentations and giving a copy to each student.

Availability – Policy – Storage: An example of protecting the availability of class information being stored by means of policy would be a policy that only authorized students are allowed access to certain stored information.

Availability – Policy – Processing: An example of protecting the availability of class information being processed by means of policy would be a rule that only authorized people are allowed to enter the classroom.

Availability – Policy – Transmission: An example of protecting the availability of class information being transmitted by means of policy would be a rule that only students are allowed into the classroom.

Availability – Education – Storage: An example of protecting the availability of class information

being stored by means of education would be teaching correct storage processes so information doesn't get lost.

Availability – Education – Processing: An example of protecting the availability of class information being processed by means of education would be instructing those who teach the information to speak up so everyone in the classroom can hear.

Availability – Education – Transmission: An example of protecting the availability of class information being transmitted by means of education would be teaching students to remain quiet in the classroom so everyone can hear.

Availability – Technology – Storage: An example of protecting the availability of class information being stored by means of technology would be making the information available on the Internet via a password-protected Web site.

Availability – Technology – Processing: An example of protecting the availability of class information being processed by means of technology would be a teacher making PowerPoint files available to students via the Internet.

Availability – Technology – Transmission: An example of protecting the availability of class information being transmitted by means of technology would be a teacher using a microphone so lectures are loud enough for all students to hear.

## INFORMATION SECURITY GOVERNANCE – WEEK 4

### **Exercise 4.1**

Three approaches to policy are the enterprise information security policy, issue-specific security policy, and the system-specific policy. The EISP is broad-based, encompassing and defining large areas of responsibility and implementation. The ISSP is tailored toward the organization's intent for how a certain technology-based system is to be used. The system-specific policy is written more as a standard and procedure to be used in the configuration of a system. A large organization would need a policy written along the lines of an EISP in order to cover all of the various systems and information security needs. For instance, a government contractor might have a very detailed policy to protect confidential information when it is required by the customer, the federal government. A smaller company, say a restaurant, might only need a system to help track its daily sales, inventory, and labor records. All of these records may be confidential, but could easily be handled by a policy like the SysSP.

## COMPLIANCE: AUDITING, MONITORING, AND LODGING – WEEK 6

### Exercise 6.1

A. You have two options for configuring Internet Explorer to control the kinds of content users can view in the browser. You can use content rating systems or you can specify Web sites. Content rating systems are administered by independent organizations, but Internet Explorer uses the ratings from the Internet Content Rating Association by default.

To enable the Content Advisor feature, open Internet Explorer, and click Internet Options on the Tools menu. Click the Content tab. Under Content Advisor, click Enable to open the Content Advisor dialog box.

(Source: <http://support.microsoft.com/kb/310401>)

B. You can configure your privacy settings in Internet Explorer by clicking Internet Options on the Tools menu, and then clicking the Privacy tab.

Note that an administrator can customize your privacy settings and remove the Privacy tab from the interface in the Internet Options dialog box. If the Privacy tab is not available, contact your administrator or see “Additional Information for Advanced Users and IT Professionals” at <http://support.microsoft.com/kb/283185>.

The Privacy settings slider has six settings: Block All Cookies, High, Medium High, Medium (default level), Low, and Accept All Cookies.

## PLANNING FOR CONTINGENCIES – WEEK 7

### Exercise 7.1

Your logs are a treasure trove of information. If properly set up, they record every network event on your servers, devices and applications -- for example, Access and permission changes to Files, Folders, and Objects containing financial, customer or compliance data, object access attempts, login failures, etc. This information is critical when launching an immediate incident response when you face a network outage or a security threat. Keeping your log data in two formats—as database records and as compressed flat files—offers a distinct storage/auditing advantage. Event log data in flat files compresses extremely well, often down to 5% of the original size. Therefore, in terms of storage cost, it costs very little to keep archived log data for many years

should an auditor ever need it. However, flat files are a very poor medium for analysis and reporting, so keeping an active working set of data (often 60 to 90 days) in a database allows ad hoc reporting as well as scheduled reporting to be available for recent events.

Centralized Log Management (CLM) is a type of logging solution system that consolidates all of your log data and pushes it to one central, accessible, and easy-to-use interface. Centralized logging is designed to make your life easier. Not only does CLM provide multiple features that allow you to easily collect log information, but it also helps you consolidate, analyze, and view that information quickly and clearly. Centralized logging provides two important benefits. First, it places all of your log records in a single location, greatly simplifying log analysis and correlation tasks. Second, it provides you with a secure storage area for your log data. In the event that a machine on your network becomes compromised, the intruder will not be able to tamper with the logs stored in the central log repository -- unless that machine is also compromised.

CLM gives you tons of capabilities including:

- Storing log data from multiple sources in a central location
- Enforcing retention policies on your logs so they are available for a specific time period
- Easily searching inside the logs for important information
- Generating alerts based on metrics you define on the logs
- Sharing your dashboard and log information with others simply and quickly
- Low costs and increased storage and backup for historical data
- Setting up security alerts and granting login access to particular users without granting server root access
- are indispensable to troubleshooting
- reduce the risk of losing data: A centralized logging system removes the individual server from the equation. If the server you're trying to troubleshoot is down, local log files won't be accessible, rendering you blind. Centralized logging (with proper system backups) ensures you always have a place to view the logs and diagnose the issue.
- improve network security: When a system is compromised you can no longer trust its logs. Centralized logs give you the forensic ability to determine what happened right before the compromise, including any user activity. This data is instrumental in preventing a recurrence. If a system is under attack via brute force, you'll quickly be able to see this in the logs. Even if the attack is spread across multiple systems and there's a more subtle correlation, you can still see the attack in the logs and respond to it. By comparison, detecting a multi-system

attack by looking at local logs would be extremely difficult.

Taking advantage of centrally storing and analyzing your logs with a CLM program will make your organization more dynamic, profitable, and secure.

## INFORMATION SECURITY MAINTENANCE – WEEK 8

### Exercise 8.1

Consider the increasingly widespread encryption blackmail attacks, or “ransomware” being leveled against public and private organizations. Hackers penetrate internal networks, usually via worm virus, and encrypt all the data it encounters on servers and workstations using a key that only they hold. When the encryption has been successful, the hackers contact the organization and demand a bribe to decrypt the data.

Ransomware attacks increased by 300 percent from 2015 to 2016 and there’s no sign the trend will change anytime soon. Although many victims never come forward with the details, Department of Justice reports suggest that payouts average between \$200 and \$10,000. However, one Los Angeles hospital paid out \$17,000 to unlock vital data, and the University of Calgary paid out around \$20,000 to deal with a ransomware attack.

But if the data has been backed up to a secure container, free from the encryption virus, then there is nothing to hold hostage—the company can simply clean its systems of the virus, restore the known good copy of the data, and continue on about its business. The backup, in this instance, is a security feature, not simply a disaster recovery safeguard.

Two German hospitals hit in early 2016 with ransomware attacks shrugged them off with moderate annoyance and only lost access to data for a few hours after restoring it from recent backup files.

In a similar vein, denial of service (DoS) attacks can be used for purposes of extortion, or simply to shut down business communications for other malicious purposes. But an organization with solid business continuity plans will have alternative methods for getting servers and services back online, allowing it to sidestep DoS attacks.

According to a 2014 study published by the Ponemon Institute, a privacy and security research group, organizations that integrate the cybersecurity function with business continuity planning are five percent less likely to suffer a data breach and spend about \$10 less per stolen record in

recovery costs.

## LEGAL AND REGULATORY REQUIREMENTS – WEEK 9

### Exercise 9.1

The primary goal of the vulnerability assessment is to identify specific, documented vulnerabilities, using the inventory of environment characteristics stored in the risk, threat, and attack database. These vulnerabilities are stored, tracked, and reported in the vulnerability database until they are remediated. Penetration testing, a level beyond vulnerability testing, is a set of security tests and evaluations that simulate attacks by a malicious hacker. A penetration test, or pen test, is usually performed periodically as part of a full security audit. In most security tests, such as vulnerability assessments, great care is taken not to disrupt normal business operations, but in pen testing the analyst tries to get as far as possible by simulating the actions of an attacker.

### Exercise 9.2

The following sites discuss the ISO management model:

- Solstice Enterprise Manager Application Development Guide  
([www.dkrz.de/~k202046/em/products/sem/Manuals/dev\\_guide/network.doc.html#470](http://www.dkrz.de/~k202046/em/products/sem/Manuals/dev_guide/network.doc.html#470))
- HP Open View Performance Insight Courses: Student Pre-course Study Guide  
([www.hp.com/education/briefs/u1614s\\_prestudy.pdf](http://www.hp.com/education/briefs/u1614s_prestudy.pdf))

The ISO network management model addresses management and operation through five topics:

- Fault management
- Configuration and name management
- Accounting management
- Performance management
- Security management

A major component of network management that can be adapted to the security management model is a firewall that serves a dual role to keep external intrusions away from an organization's internal data. Fault management is a network component that can be adapted to the security model by detecting, logging, and automatically fixing network problems to keep it running effectively. Because faults can cause downtime or unacceptable network degradation, fault management is perhaps the most widely implemented element of ISO network management. The security management model identifies sensitive network resources, including systems, files, and other entities, and determines mappings between sensitive network resources and user sets. The

model also monitors access points to sensitive network resources and logs inappropriate access to sensitive network resources.



**FORM: 200.1.3**

## **STUDY GUIDE**

**Course: CYS606 – Cybersecurity Architecture and Operations**

## Course Information

<b>Institution</b>	European University Cyprus		
<b>Programme of Study</b>	Cybersecurity (MSc)		
<b>Course unit</b>	CYS606	Cybersecurity Architecture and Operations	
<b>Level</b>	<i>Undergraduate</i>	<i>Postgraduate</i>	
		<i>Master</i>	<i>PhD</i>
		√	
<b>Language of Instruction</b>	English		
<b>Teaching Methodology</b>	Distance Learning		
<b>Course Type</b>	<i>Compulsory</i>		<i>Optional</i>
	√		
<b>Number of Group Consultation Meetings/ Web-Conferences/ Lectures</b>	<b>Total</b>	<b>Face to Face</b>	<b>Web-Conferences</b>
	14	1	13
<b>Number of Activities/ Assignments</b>	4		
<b>Final Assessment</b>	<i>Assignments</i>		<i>Final Examinations</i>
	50 %		50 %
<b>Number of Credits (ECTS)</b>	10		

<b>Study Guide drafted by</b>	Dr Nikolaos Tsalis
<b>Editing and final approval of Study Guide by</b>	Dr Yianna Danidou

## COURSE CONTENTS

		Page
	Introductory Notes	4
	First Group Consultation Meeting	5
1	Week 1 – Introduction to information security framework for improving cyber security	7
2	Week 2 – Introduction to the Identify phase	11
3	Week 3 – Identify phase main modules	14
4	Week 4 – Identify phase additional modules	16
5	Week 5 – Introduction to the Protect phase	18
6	Week 6 – Protect phase main modules	20
7	Week 7 – Protect phase additional modules	22
8	Week 8 – Introduction to the Detect phase	24
9	Week 9 – Detect phase modules	26
10	Week 10 – Introduction to the Respond phase	28
11	Week 11 – Respond phase main modules	30
12	Week 12 – Introduction to the Recover phase	32
13	Week 13 – Recover phase main modules	34
14	Revision and Final Examination	36

## **INTRODUCTORY NOTES**

This course introduces the fundamental security principles of confidentiality, integrity, availability, as well as related security services such as accountability, non-repudiation, authentication, etc. The whole operational environment is described, with reference to ongoing security processes such as user provisioning, vulnerability management, penetration testing, exercising, change management, incident response, risk assessment and others. The five phases of cybersecurity are discussed here – Identify, Protect, Detect, Respond, Recover.

Analytic structure of the course per units of study follows.

## 1st GROUP CONSULTATION MEETING

### Programme Presentation

Leading companies today are rethinking the role of information security in their organizations. They realize that in a digital world, cybersecurity is the key to safeguarding their most precious assets—intellectual property, customer information, financial data, and employee records, among others. But far more than a defensive measure, companies also know that cybersecurity can better position their organization with business partners, customers, investors, and other stakeholders.

The European cybersecurity market is about 25% (i.e. about €17bln) of the world market (estimated at €70bln in 2015), with an average yearly growth slightly larger than 6%, when the world market is growing at about 10%/year. Recent study compiled by Europe's cybersecurity industry leaders pointed out that Europe is in danger of falling behind in the international digital economy field.

The Master in Cybersecurity is a cutting-edge program, designed for those wishing to develop a career as a cyber-security professional, or to take a leading technical or managerial role in an organization critically dependent upon data and information communication technology. Students will develop an advanced knowledge of information security and an awareness of the context in which information security operates in terms of safety, environmental, social and economic aspects. They will gain a wide range of intellectual, practical and transferable skills, enabling them to develop a flexible professional career in IT.

Key elements of this postgraduate degree are: the *real life experience* given by the opportunity to apply their theoretical knowledge through specialized virtual and remote security laboratories in which they will be able to carry out activities such as reconnaissance, network scanning and exploitation exercises, and investigate the usage and behavior of security systems such as Intrusion Detection and Prevention Systems thus becoming confident in the practical application of the latest tools; the *high-level insight* that will enhance student's ability to research and design creative cyber security solutions to address business problems; *hands-on skills* through experimentation with security techniques, cryptographic algorithms, cyber forensics building an ethical hacking environment; and *flexibility* since students will also be able to choose either the completion of a Master thesis or to complete a Research methods course and two elective courses.

Students undertake modules to the value of 90 ECTS credits.

## COURSE PRESENTATION THROUGH THE STUDY GUIDE

The Cybersecurity Architecture and Operations is a compulsory course in the Cybersecurity master program.

The Study Guide, a tool that is necessary and useful for students, especially in those cases where the training material is not written with the methodology of open and distance learning, encourages and facilitates the study and understanding of the issues addressed by the thematic module. In addition, through self-assessment exercises, it stimulates and encourages work at home, provides incentives for further study, and contributes to the development of your critical thinking. The Study Guide is structured on a weekly basis and includes a summary and some very brief introductory remarks, purpose and expected outcome, key words - basic concepts, annotated literature, recommended student's time, self-assessment exercises, critical thinking and case studies, with indicative answers in the end, aiming at a more meaningful understanding of the content, terms and concepts that each unit deals with. The recommended weekly working time includes, apart from the study, the follow-up of teleconferences and OSS, bibliography search, two weekly exercises, etc. Although it is self-evident, it should be noted that the study guide does not substitute to the minimum the educational material on the platform that the student needs to read carefully and assimilate in order to be able to meet the requirements of the program and to successfully complete the thematic module them.

## **Recommended time for the student to work**

Approximately 5 hours for the study guide

# INTRODUCTION TO INFORMATION SECURITY FRAMEWORK FOR IMPROVING CYBERSECURITY

1<sup>st</sup> Week

## Summary

The Framework Core provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes. The Core is not a checklist of actions to perform. It presents key cybersecurity outcomes identified by stakeholders as helpful in managing cybersecurity risk. The Core comprises four elements: Functions, Categories, Subcategories, and Informative References.

In addition, the content of this week will include recent cyber security events, their related impact and which controls failed to adequately protect against the related threats.

## Introductory Remarks

The Framework provides a common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. It can be used to manage cybersecurity risk across entire organizations or it can be focused on the delivery of critical services within an organization. Different types of entities – including sector coordinating structures, associations, and organizations – can use the Framework for different purposes, including the creation of common Profiles.

The Framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business/mission drivers and cybersecurity activities. These components are explained below.

- The Framework Core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level

to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization’s management of cybersecurity risk. The Framework Core then identifies underlying key Categories and Subcategories – which are discrete outcomes – for each Function and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.

- Framework Implementation Tiers (“Tiers”) provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization’s cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization’s practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.
- A Framework Profile (“Profile”) represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a “Current” Profile (the “as is” state) with a “Target” Profile (the “to be” state). To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business/mission drivers and a risk assessment, determine which are most important; it can add Categories and Subcategories as needed to address the organization’s risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

## Aim/Objectives

The aim of this material of the course is to:

- Introduce students to the framework of the information security services.
- Acquaint students with the most important textbooks, articles and scientific texts pertaining to the methodology of research.
- Establish the scientific framework of the course.

## Learning Outcomes

After successfully completing this material of the course, the students should be able to:

- identify the main phases of the information security framework
- understand what each phase includes and how it affects the effective completion of the testing methodology
- focus on the important aspects of a penetration testing activity

## Key Words

Penetration testing

Information Security

Controls

Countermeasures and  
security mechanisms

Testing

## Annotated Bibliography

### Basic

- Farwell, J.P., Roddy, V.N., Chalker, Y. and Elkins, G.C., 2017. The Architecture of Cybersecurity: How General Counsel, Executives, and Boards of Directors Can Protect Their Information Assets. University of Louisiana at Lafayette.
- Santos, O., 2018. Developing Cybersecurity Programs and Policies. Pearson.
- “Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”, by Thomas A. Johnson (Editor)

### Suggestions for further reading:

- “The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)”, by Anne Kohnke and Dan Shoemaker
- ISO 27002:2013 - Information technology – Security techniques – Code of practice for information security management
- IEEE Journals and Magazines

## **Self-Assessment Exercises**

### **Exercise 1.1**

Briefly outline the contents of the security framework

### **Exercise 1.2**

Collaborate on the correlation between the elements.

### **Exercise 1.3**

Outline each module in a comprehensive manner to outline its objective.

### **Exercise 1.4**

Practical exercise: A related topic (e.g. case scenario of an organization that requires to enhance its information security posture) will be chosen on the 1st week and students will have to comment and discuss how each phase could be adequately utilized and implemented, so as to achieve the required objective. This exercise will be repeated on each week (according to its phase), so as to build up gradually the case scenario.

## **Recommended time for the student to work**

15 hours

## INTRODUCTION TO THE IDENTIFY PHASE

2<sup>nd</sup> Week

### Summary

Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

### Introductory Remarks

The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

### Aim/Objectives

The aim of this material of the course is to:

- Introduce the students to the first steps towards the identify phase
- Prepare the roadmap to a successful infrastructure protection

### Learning Outcomes

After successfully completing this material of the course, the students should be able to:

- outline which are the main steps of the identify phase
- effectively prepare for the conduct of a testing activity
- identify the includes assets and their properties

## Key Words

Penetration testing	Information Security	Controls
Countermeasures and security mechanisms	Testing	

## Annotated Bibliography

### Basic

- Farwell, J.P., Roddy, V.N., Chalker, Y. and Elkins, G.C., 2017. The Architecture of Cybersecurity: How General Counsel, Executives, and Boards of Directors Can Protect Their Information Assets. University of Louisiana at Lafayette.
- Santos, O., 2018. Developing Cybersecurity Programs and Policies. Pearson.
- “Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”, by Thomas A. Johnson (Editor)

### Suggestions for further reading:

- “The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)”, by Anne Kohnke and Dan Shoemaker
- ISO 27002:2013 - Information technology – Security techniques – Code of practice for information security management
- IEEE Journals and Magazines

## Self-Assessment Exercises

### Exercise 2.1

Briefly outline the contents of this phase

### Exercise 2.2

Write the advantages and disadvantages of executing this phase of the framework

## **Recommended time for the student to work**

15 hours

## IDENTIFY PHASE MAIN MODULES

3<sup>rd</sup> Week

### Summary

Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

### Introductory Remarks

The main modules of this phase include:

- Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
- Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
- Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

### Aim/Objectives

The aim of this material of the course is to:

- Introduce the students to the first steps towards the identify phase
- Prepare the roadmap to a successful infrastructure protection

### Learning Outcomes

After successfully completing this material of the course, the students should be able to:

- outline which are the main steps of the identify phase
- effectively prepare for the conduct of a testing activity
- identify the includes assets and their properties

## Key Words

Penetration testing	Information Security	Controls
Countermeasures and security mechanisms	Testing	

## Annotated Bibliography

### Basic

- Farwell, J.P., Roddy, V.N., Chalker, Y. and Elkins, G.C., 2017. The Architecture of Cybersecurity: How General Counsel, Executives, and Boards of Directors Can Protect Their Information Assets. University of Louisiana at Lafayette.
- Santos, O., 2018. Developing Cybersecurity Programs and Policies. Pearson.
- “Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”, by Thomas A. Johnson (Editor)

### Suggestions for further reading:

- “The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)”, by Anne Kohnke and Dan Shoemaker
- ISO 27002:2013 - Information technology – Security techniques – Code of practice for information security management
- IEEE Journals and Magazines

## Self-Assessment Exercises

### Exercise 3.1

Briefly outline the contents of this phase

### Exercise 3.2

Outline how to implement the included modules

## Recommended time for the student to work

15 hours

## IDENTIFY PHASE ADDITIONAL MODULES

4<sup>th</sup> Week

### Summary

Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

### Introductory Remarks

The additional modules of this phase include:

- Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
- Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
- Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.

### Aim/Objectives

The aim of this material of the course is to:

- Introduce the students to the first steps towards the identify phase
- Prepare the roadmap to a successful infrastructure protection

### Learning Outcomes

After successfully completing this material of the course, the students should be able to:

- outline which are the main steps of the identify phase
- effectively prepare for the conduct of a testing activity
- identify the includes assets and their properties

## Key Words

Penetration testing	Information Security	Controls
Countermeasures and security mechanisms	Testing	

## Annotated Bibliography

### Basic

- Farwell, J.P., Roddy, V.N., Chalker, Y. and Elkins, G.C., 2017. The Architecture of Cybersecurity: How General Counsel, Executives, and Boards of Directors Can Protect Their Information Assets. University of Louisiana at Lafayette.
- Santos, O., 2018. Developing Cybersecurity Programs and Policies. Pearson.
- “Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”, by Thomas A. Johnson (Editor)

### Suggestions for further reading:

- “The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)”, by Anne Kohnke and Dan Shoemaker
- ISO 27002:2013 - Information technology – Security techniques – Code of practice for information security management
- IEEE Journals and Magazines

## Self-Assessment Exercises

### Exercise 4.1

Briefly outline the contents of this phase

### Exercise 4.2

Outline how to implement the included modules

## Recommended time for the student to work

15 hours

## INTRODUCTION TO PROTECT PHASE

5<sup>th</sup> Week

### Summary

Develop and implement appropriate safeguards to ensure delivery of critical services.

### Introductory Remarks

The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

### Aim/Objectives

The aim of this material of the course is to:

- Introduce the students to the first steps towards the protect phase
- Prepare the roadmap to a successful infrastructure protection

### Learning Outcomes

After successfully completing this material of the course, the students should be able to:

- outline which are the main steps of the protect phase
- effectively prepare for the conduct of a testing activity
- identify the required protections mechanisms
- measure the effectiveness of the selected countermeasures

### Key Words

Penetration testing	Information Security	Controls
Countermeasures and security mechanisms	Testing	

## Annotated Bibliography

### Basic

- Farwell, J.P., Roddy, V.N., Chalker, Y. and Elkins, G.C., 2017. The Architecture of Cybersecurity: How General Counsel, Executives, and Boards of Directors Can Protect Their Information Assets. University of Louisiana at Lafayette.
- Santos, O., 2018. Developing Cybersecurity Programs and Policies. Pearson.
- “Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”, by Thomas A. Johnson (Editor)

### Suggestions for further reading:

- “The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)”, by Anne Kohnke and Dan Shoemaker
- ISO 27002:2013 - Information technology – Security techniques – Code of practice for information security management
- IEEE Journals and Magazines

## Self-Assessment Exercises

### Exercise 5.1

Briefly outline the contents of this phase

### Exercise 5.2

Write the advantages and disadvantages of executing this phase of the framework

## Activity (5 points)

The activity subject will be announced at a later stage.

## Recommended time for the student to work

20 hours

## PROTECT PHASE MAIN MODULES

6<sup>th</sup> Week

### Summary

Develop and implement appropriate safeguards to ensure delivery of critical services.

### Introductory Remarks

The main modules of this phase include:

- Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
- Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.
- Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

### Aim/Objectives

The aim of this material of the course is to:

- Introduce the students to the first steps towards the protect phase
- Prepare the roadmap to a successful infrastructure protection

### Learning Outcomes

After successfully completing this material of the course, the students should be able to:

- outline which are the main steps of the protect phase
- effectively prepare for the conduct of a testing activity
- identify the required protections mechanisms
- measure the effectiveness of the selected countermeasures

## Key Words

Penetration testing	Information Security	Controls
Countermeasures and security mechanisms	Testing	

## Annotated Bibliography

### Basic

- Farwell, J.P., Roddy, V.N., Chalker, Y. and Elkins, G.C., 2017. The Architecture of Cybersecurity: How General Counsel, Executives, and Boards of Directors Can Protect Their Information Assets. University of Louisiana at Lafayette.
- Santos, O., 2018. Developing Cybersecurity Programs and Policies. Pearson.
- “Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”, by Thomas A. Johnson (Editor)

### Suggestions for further reading:

- “The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)”, by Anne Kohnke and Dan Shoemaker
- ISO 27002:2013 - Information technology – Security techniques – Code of practice for information security management
- IEEE Journals and Magazines

## Self-Assessment Exercises

### Exercise 6.1

Briefly outline the contents of this phase

### Exercise 6.2

Outline how to implement the included modules

## Recommended time for the student to work

15 hours

## PROTECT PHASE ADDITIONAL MODULES

7<sup>th</sup> Week

### Summary

Develop and implement appropriate safeguards to ensure delivery of critical services.

### Introductory Remarks

The additional modules of this phase include:

- Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
- Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
- Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

### Aim/Objectives

The aim of this material of the course is to:

- Introduce the students to the first steps towards the protect phase
- Prepare the roadmap to a successful infrastructure protection

### Learning Outcomes

After successfully completing this material of the course, the students should be able to:

- outline which are the main steps of the protect phase
- effectively prepare for the conduct of a testing activity
- identify the required protections mechanisms
- measure the effectiveness of the selected countermeasures

## Key Words

Penetration testing	Information Security	Controls
Countermeasures and security mechanisms	Testing	

## Annotated Bibliography

### Basic

- Farwell, J.P., Roddy, V.N., Chalker, Y. and Elkins, G.C., 2017. The Architecture of Cybersecurity: How General Counsel, Executives, and Boards of Directors Can Protect Their Information Assets. University of Louisiana at Lafayette.
- Santos, O., 2018. Developing Cybersecurity Programs and Policies. Pearson.
- “Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”, by Thomas A. Johnson (Editor)

### Suggestions for further reading:

- “The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)”, by Anne Kohnke and Dan Shoemaker
- ISO 27002:2013 - Information technology – Security techniques – Code of practice for information security management
- IEEE Journals and Magazines

## Self-Assessment Exercises

### Exercise 7.1

Briefly outline the contents of this phase

### Exercise 7.2

Outline how to implement the included modules

## Recommended time for the student to work

15 hours

# INTRODUCTION TO THE DETECT PHASE

8<sup>th</sup> Week

## Summary

Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

## Introductory Remarks

The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

## Aim/Objectives

The aim of this material of the course is to:

- Introduce the students to the first steps towards the detect phase
- Prepare the roadmap to a successful infrastructure protection

## Learning Outcomes

After successfully completing this material of the course, the students should be able to:

- outline which are the main steps of the detect phase
- effectively prepare for the conduct of a testing activity
- develop detection mechanisms for the current threats
- apply such mechanisms and review their performance

## Key Words

Penetration testing	Information Security	Controls
Countermeasures and security mechanisms	Testing	

## Annotated Bibliography

### Basic

- Farwell, J.P., Roddy, V.N., Chalker, Y. and Elkins, G.C., 2017. The Architecture of Cybersecurity: How General Counsel, Executives, and Boards of Directors Can Protect Their Information Assets. University of Louisiana at Lafayette.
- Santos, O., 2018. Developing Cybersecurity Programs and Policies. Pearson.
- “Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”, by Thomas A. Johnson (Editor)

### Suggestions for further reading:

- “The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)”, by Anne Kohnke and Dan Shoemaker
- ISO 27002:2013 - Information technology – Security techniques – Code of practice for information security management
- IEEE Journals and Magazines

## Self-Assessment Exercises

### Exercise 8.1

Briefly outline the contents of this phase

### Exercise 8.2

Write the advantages and disadvantages of executing this phase of the framework

## Individual Assignment (20 points)

The module includes a theoretical assignment, where the student needs to review the related literature and provide a state-of-the-art project based on a specific topic.

## Recommended time for the student to work

35 hours

## DETECT PHASE MODULES

9<sup>th</sup> Week

### Summary

Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

### Introductory Remarks

The main modules of this phase include:

- Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.
- Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
- Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.

### Aim/Objectives

The aim of this material of the course is to:

- Introduce the students to the first steps towards the detect phase
- Prepare the roadmap to a successful infrastructure protection

### Learning Outcomes

After successfully completing this material of the course, the students should be able to:

- outline which are the main steps of the detect phase
- effectively prepare for the conduct of a testing activity
- develop detection mechanisms for the current threats
- apply such mechanisms and review their performance

## Key Words

Penetration testing	Information Security	Controls
Countermeasures and security mechanisms	Testing	

## Annotated Bibliography

### Basic

- Farwell, J.P., Roddy, V.N., Chalker, Y. and Elkins, G.C., 2017. The Architecture of Cybersecurity: How General Counsel, Executives, and Boards of Directors Can Protect Their Information Assets. University of Louisiana at Lafayette.
- Santos, O., 2018. Developing Cybersecurity Programs and Policies. Pearson.
- “Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”, by Thomas A. Johnson (Editor)

### Suggestions for further reading:

- “The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)”, by Anne Kohnke and Dan Shoemaker
- ISO 27002:2013 - Information technology – Security techniques – Code of practice for information security management
- IEEE Journals and Magazines

## Self-Assessment Exercises

### Exercise 9.1

Briefly outline the contents of this phase

### Exercise 9.2

Outline how to implement the included modules

## Recommended time for the student to work

15 hours

## INTRODUCTION TO THE RESPOND PHASE

10<sup>th</sup> Week

### Summary

Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

### Introductory Remarks

The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

### Aim/Objectives

The aim of this material of the course is to:

- Introduce the students to the first steps towards the respond phase
- Prepare the roadmap to a successful infrastructure protection

### Learning Outcomes

After successfully completing this material of the course, the students should be able to:

- outline which are the main steps of the respond phase
- effectively prepare for the conduct of a testing activity
- respond to a security event
- identify the tasks to be executed during the response phase

### Key Words

Penetration testing  Countermeasures and security mechanisms	Information Security  Testing	Controls
---	-------------------------------------	----------

## Annotated Bibliography

### Basic

- Farwell, J.P., Roddy, V.N., Chalker, Y. and Elkins, G.C., 2017. The Architecture of Cybersecurity: How General Counsel, Executives, and Boards of Directors Can Protect Their Information Assets. University of Louisiana at Lafayette.
- Santos, O., 2018. Developing Cybersecurity Programs and Policies. Pearson.
- “Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”, by Thomas A. Johnson (Editor)

### Suggestions for further reading:

- “The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)”, by Anne Kohnke and Dan Shoemaker
- ISO 27002:2013 - Information technology – Security techniques – Code of practice for information security management
- IEEE Journals and Magazines

## Self-Assessment Exercises

### Exercise 10.1

Briefly outline the contents of this phase.

### Exercise 10.2

Write the advantages and disadvantages of executing this phase of the framework.

## Activity (5 points)

The activity subject will be announced at a later stage.

## Recommended time for the student to work

20 hours

## RESPOND PHASE MAIN MODULES

11<sup>th</sup> Week

### Summary

Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

### Introductory Remarks

The main modules of this phase include:

- Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.
- Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).
- Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.
- Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.
- Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

### Aim/Objectives

The aim of this material of the course is to:

- Introduce the students to the first steps towards the respond phase
- Prepare the roadmap to a successful infrastructure protection

### Learning Outcomes

After successfully completing this material of the course, the students should be able to:

- outline which are the main steps of the respond phase
- effectively prepare for the conduct of a testing activity
- respond to a security event

- identify the tasks to be executed during the response phase

## Key Words

Penetration testing	Information Security	Controls
Countermeasures and security mechanisms	Testing	

## Annotated Bibliography

### Basic

- Farwell, J.P., Roddy, V.N., Chalker, Y. and Elkins, G.C., 2017. The Architecture of Cybersecurity: How General Counsel, Executives, and Boards of Directors Can Protect Their Information Assets. University of Louisiana at Lafayette.
- Santos, O., 2018. Developing Cybersecurity Programs and Policies. Pearson.
- “Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”, by Thomas A. Johnson (Editor)

### Suggestions for further reading:

- “The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)”, by Anne Kohnke and Dan Shoemaker
- ISO 27002:2013 - Information technology – Security techniques – Code of practice for information security management
- IEEE Journals and Magazines

## Self-Assessment Exercises

### Exercise 11.1

Briefly outline the contents of this phase

### Exercise 11.2

Outline how to implement the included modules

## Recommended time for the student to work

15 hours

## INTRODUCTION TO THE RECOVER PHASE

12<sup>th</sup> Week

### Summary

Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

### Introductory Remarks

The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

### Aim/Objectives

The aim of this material of the course is to:

- Introduce the students to the first steps towards the recover phase
- Prepare the roadmap to a successful infrastructure protection

### Learning Outcomes

After successfully completing this material of the course, the students should be able to:

- outline which are the main steps of the recover phase
- effectively prepare for the conduct of a testing activity
- recover from the occurrence of a security event
- apply recovery mechanisms

### Key Words

Penetration testing	Information Security	Controls
Countermeasures and security mechanisms	Testing	

## Annotated Bibliography

### Basic

- Farwell, J.P., Roddy, V.N., Chalker, Y. and Elkins, G.C., 2017. The Architecture of Cybersecurity: How General Counsel, Executives, and Boards of Directors Can Protect Their Information Assets. University of Louisiana at Lafayette.
- Santos, O., 2018. Developing Cybersecurity Programs and Policies. Pearson.
- “Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”, by Thomas A. Johnson (Editor)

### Suggestions for further reading:

- “The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)”, by Anne Kohnke and Dan Shoemaker
- ISO 27002:2013 - Information technology – Security techniques – Code of practice for information security management
- IEEE Journals and Magazines

## Self-Assessment Exercises

### Exercise 12.1

Briefly outline the contents of this phase

### Exercise 12.2

Write the advantages and disadvantages of executing this phase of the framework

## Group Assignment (20 points)

The subject of the group assignment will be announced at a later stage.

## Recommended time for the student to work

35 hours

## RECOVER PHASE MAIN MODULES

13<sup>th</sup> Week

### Summary

Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

### Introductory Remarks

The main modules of this phase include:

- Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.
- Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.
- Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

### Aim/Objectives

The aim of this material of the course is to:

- Introduce the students to the first steps towards the recover phase
- Prepare the roadmap to a successful infrastructure protection

### Learning Outcomes

After successfully completing this material of the course, the students should be able to:

- outline which are the main steps of the recover phase
- effectively prepare for the conduct of a testing activity
- recover from the occurrence of a security event
- apply recovery mechanisms

## Key Words

Penetration testing	Information Security	Controls
Countermeasures and security mechanisms	Testing	

## Annotated Bibliography

### Basic

- Farwell, J.P., Roddy, V.N., Chalker, Y. and Elkins, G.C., 2017. The Architecture of Cybersecurity: How General Counsel, Executives, and Boards of Directors Can Protect Their Information Assets. University of Louisiana at Lafayette.
- Santos, O., 2018. Developing Cybersecurity Programs and Policies. Pearson.
- “Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”, by Thomas A. Johnson (Editor)

### Suggestions for further reading:

- “The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)”, by Anne Kohnke and Dan Shoemaker
- ISO 27002:2013 - Information technology – Security techniques – Code of practice for information security management
- IEEE Journals and Magazines

## Self-Assessment Exercises

### Exercise 13.1

Briefly outline the contents of this phase

### Exercise 13.2

Outline how to implement the included modules

## Recommended time for the student to work

15 hours

## **REVISION AND FINAL EXAMINATION**

The final examination will consist of true/false, multiple-choice questions and a small number of questions.

### **Recommended time for the student to work**

40 hours

**Date/Time of Final Exam: TBD**



**FORM: 200.1.3**

## **STUDY GUIDE**

**Course: CYS607 – Ethical Hacking and Penetration Testing**

## Course Information

<b>Institution</b>	European University Cyprus		
<b>Programme of Study</b>	Cybersecurity (MSc)		
<b>Course unit</b>	CYS607	Ethical Hacking and Penetration Testing	
<b>Level</b>	<b>Undergraduate</b>	<b>Postgraduate</b>	
		<b>Master</b>	<b>PhD</b>
		√	
<b>Language of Instruction</b>	English		
<b>Teaching Methodology</b>	Distance Learning		
<b>Course Type</b>	<b>Compulsory</b>		<b>Optional</b>
	√		
<b>Number of Group Consultation Meetings/ Web-Conferences/ Lectures</b>	<b>Total</b>	<b>Face to Face</b>	<b>Web-Conferences</b>
	14	1	13
<b>Number of Activities/ Assignments</b>	4		
<b>Final Assessment</b>	<b>Assignments</b>		<b>Final Examinations</b>
	50 %		50 %
<b>Number of Credits (ECTS)</b>	10		

<b>Study Guide drafted by</b>	Dr Nikolaos Tsalis
<b>Editing and final approval of Study Guide by</b>	Dr Yianna Danidou

## COURSE CONTENTS

		Page
	Introductory Notes	4
	First Group Consultation Meeting	5
1	Week 1 – Introduction to penetration testing and ethical hacking	7
2	Week 2 – Pre-engagement tasks	14
3	Week 3 – Setting up the Lab	17
4	Week 4 – Get familiarized with Kali tools	22
5	Week 5 – Additional Kali tools	28
6	Week 6 – Intelligence Gathering phase	32
7	Week 7 – Threat modeling phase	35
8	Week 8 – Vulnerability assessment phase	37
9	Week 9 – Automated Tools for Penetration Testing and Reporting	40
10	Week 10 – Vulnerability exploitation phase	44
11	Week 11 – Post-exploitation tasks	46
12	Week 12 – Reporting	48
13	Week 13 – Lab Practice	50
14	Revision and Final Examination	52

## INTRODUCTORY NOTES

The objective of this course is to provide a detailed introduction into the world of ethical hacking and to understand its usefulness to organizations in practical terms. Hacking concepts, tools and techniques, and countermeasures are covered, along with how penetration testing fits into a comprehensive cybersecurity regime. Beyond the confines of ethical hacking, this course covers aggressive hacking techniques that are essential knowledge for professionals who need to be able to defend against such advanced attacks.

Analytic structure of the course per units of study follows.

## 1st GROUP CONSULTATION MEETING

### Programme Presentation

Leading companies today are rethinking the role of information security in their organizations. They realize that in a digital world, cybersecurity is the key to safeguarding their most precious assets—intellectual property, customer information, financial data, and employee records, among others. But far more than a defensive measure, companies also know that cybersecurity can better position their organization with business partners, customers, investors, and other stakeholders.

The European cybersecurity market is about 25% (i.e. about €17bln) of the world market (estimated at €70bln in 2015), with an average yearly growth slightly larger than 6%, when the world market is growing at about 10%/year. Recent study compiled by Europe's cybersecurity industry leaders pointed out that Europe is in danger of falling behind in the international digital economy field.

The Master in Cybersecurity is a cutting-edge program, designed for those wishing to develop a career as a cyber-security professional, or to take a leading technical or managerial role in an organization critically dependent upon data and information communication technology. Students will develop an advanced knowledge of information security and an awareness of the context in which information security operates in terms of safety, environmental, social and economic aspects. They will gain a wide range of intellectual, practical and transferable skills, enabling them to develop a flexible professional career in IT.

Key elements of this postgraduate degree are: the *real life experience* given by the opportunity to apply their theoretical knowledge through specialized virtual and remote security laboratories in which they will be able to carry out activities such as reconnaissance, network scanning and exploitation exercises, and investigate the usage and behavior of security systems such as Intrusion Detection and Prevention Systems thus becoming confident in the practical application of the latest tools; the *high-level insight* that will enhance student's ability to research and design creative cyber security solutions to address business problems; *hands-on skills* through experimentation with security techniques, cryptographic algorithms, cyber forensics building an ethical hacking environment; and *flexibility* since students will also be able to choose either the completion of a Master thesis or to complete a Research methods course and two elective courses.

Students undertake modules to the value of 90 ECTS credits.

## COURSE PRESENTATION THROUGH THE STUDY GUIDE

The Ethical Hacking and Penetration Testing is a compulsory course in the Cybersecurity master program.

The Study Guide, a tool that is necessary and useful for students, especially in those cases where the training material is not written with the methodology of open and distance learning, encourages and facilitates the study and understanding of the issues addressed by the thematic module. In addition, through self-assessment exercises, it stimulates and encourages work at home, provides incentives for further study, and contributes to the development of your critical thinking. The Study Guide is structured on a weekly basis and includes a summary and some very brief introductory remarks, purpose and expected outcome, key words - basic concepts, annotated literature, recommended student's time, self-assessment exercises, critical thinking and case studies, with indicative answers in the end, aiming at a more meaningful understanding of the content, terms and concepts that each unit deals with. The recommended weekly working time includes, apart from the study, the follow-up of teleconferences and OSS, bibliography search, two weekly exercises, etc. Although it is self-evident, it should be noted that the study guide does not substitute to the minimum the educational material on the platform that the student needs to read carefully and assimilate in order to be able to meet the requirements of the program and to successfully complete the thematic module them.

### **Recommended time for the student to work**

Approximately 5 hours for the study guide

# INTRODUCTION TO PENETRATION TESTING AND ETHICAL HACKING

1<sup>st</sup> Week

## Summary

A phased information security assessment methodology offers a number of advantages. The structure is easy to follow and provides natural breaking points for staff transition. Its methodology should contain at minimum the following phases:

- **Planning.** Critical to a successful security assessment, the planning phase is used to gather information needed for assessment execution—such as the assets to be assessed, the threats of interest against the assets, and the security controls to be used to mitigate those threats—and to develop the assessment approach. A security assessment should be treated as any other project, with a project management plan to address goals and objectives, scope, requirements, team roles and responsibilities, limitations, success factors, assumptions, resources, timeline, and deliverables. Section 6 of this guide covers planning.
- **Execution.** Primary goals for the execution phase are to identify vulnerabilities and validate them when appropriate. This phase should address activities associated with the intended assessment method and technique. Although specific activities for this phase differ by assessment type, upon completion of this phase assessors will have identified system, network, and organizational process vulnerabilities.
- **Post-Execution.** The post-execution phase focuses on analyzing identified vulnerabilities to determine root causes, establish mitigation recommendations, and develop a final report. Section 8 of this guide addresses reporting and mitigation.

## Introductory Remarks

An information security assessment is the process of determining how effectively an entity being assessed (e.g., host, system, network, procedure, person—known as the assessment object) meets specific security objectives. Three types of assessment methods can be used to accomplish this—testing, examination, and interviewing. Testing is the process of exercising one or more assessment objects under specified conditions to compare actual and expected behaviors. Examination is the process of checking, inspecting, reviewing, observing, studying, or

analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence. Interviewing is the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or identify the location of evidence. Assessment results are used to support the determination of security control effectiveness over time.

Hacking has been a part of computing for almost five decades and it is a very broad discipline, which covers a wide range of topics. The first known event of hacking had taken place in 1960 at MIT and at the same time, the term "Hacker" was originated.

Hacking is the act of finding the possible entry points that exist in a computer system or a computer network and finally entering into them. Hacking is usually done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer.

Hacking is usually legal as long as it is being done to find weaknesses in a computer or network system for testing purpose. This sort of hacking is what we call Ethical Hacking.

A computer expert who does the act of hacking is called a "Hacker". Hackers are those who seek knowledge, to understand how systems operate, how they are designed, and then attempt to play with these systems.

We will present in this first week a broad overview of Ethical Hacking and Penetration Testing.

In addition, the content of this week will include recent cyber security events, their related impact and which controls failed to adequately protect against the related threats.

## **Types of Hacking**

We can segregate hacking into different categories, based on what is being hacked. Here is a set of examples:

- Website Hacking: Hacking a website means taking unauthorized control over a web server and its associated software such as databases and other interfaces.
- Network Hacking: Hacking a network means gathering information about a network by using tools like Telnet, NS lookup, Ping, Tracert, Netstat, etc. with the intent to harm the network system and hamper its operation.
- Email Hacking: It includes getting unauthorized access on an Email account and using it without taking the consent of its owner.

- Ethical Hacking: Ethical hacking involves finding weaknesses in a computer or network system for testing purpose and finally getting them fixed.
- Password Hacking: This is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.
- Computer Hacking: This is the process of stealing computer ID and password by applying hacking methods and getting unauthorized access to a computer system.

Hackers can be classified into different categories such as white hat, black hat, and grey hat, based on their intent of hacking a system. These different terms come from old Spaghetti Westerns, where the bad guy wears a black cowboy hat and the good guy wears a white hat.

### **White Hat Hackers**

White Hat hackers are also known as Ethical Hackers. They never intent to harm a system, rather they try to find out weaknesses in a computer or a network system as a part of penetration testing and vulnerability assessments. Ethical hacking is not illegal and it is one of the demanding jobs available in the IT industry. There are numerous companies that hire ethical hackers for penetration testing and vulnerability assessments.

### **Black Hat Hackers**

Black Hat hackers, also known as crackers, are those who hack in order to gain unauthorized access to a system and harm its operations or steal sensitive information. Black Hat hacking is always illegal because of its bad intent which includes stealing corporate data, violating privacy, damaging the system, blocking network communication, etc.

### **Grey Hat Hackers**

Grey hat hackers are a blend of both black hat and white hat hackers. They act without malicious intent but for their fun, they exploit a security weakness in a computer system or network without the owner's permission or knowledge. Their intent is to bring the weakness to the attention of the owners and getting appreciation or a little bounty from the owners.

### **Miscellaneous Hackers**

Apart from the above well-known classes of hackers, we have the following categories of hackers based on what they hack and how they do it:

#### **Red Hat Hackers**

Red hat hackers are again a blend of both black hat and white hat hackers. They are usually on the level of hacking government agencies, top-secret information hubs, and generally anything that falls under the category of sensitive information.

### **Blue Hat Hackers**

A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch. They look for loopholes that can be exploited and try to close these gaps. Microsoft also uses the term BlueHat to represent a series of security briefing events.

### **Elite Hackers**

This is a social status among hackers, which is used to describe the most skilled. Newly discovered exploits will circulate among these hackers.

### **Script Kiddie**

A script kiddie is a non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept, hence the term Kiddie.

### **Neophyte**

A neophyte, "n00b", or "newbie" or "Green Hat Hacker" is someone who is new to hacking or phreaking and has almost no knowledge or experience of the workings of technology and hacking.

### **Hacktivist**

A hacktivist is a hacker who utilizes technology to announce a social, ideological, religious, or political message. In general, most hacktivism involves website defacement or denial-of-service attacks.

### **Methodology**

Like all good projects, ethical hacking too has a set of distinct phases. It helps hackers to make a structured ethical hacking attack.

Different security training manuals explain the process of ethical hacking in different ways, but for me as a Certified Ethical Hacker, the entire process can be categorized into the following six phases.



## Aim/Objectives

The aim of this material of the course is to:

- Introduce students to the framework of a penetration testing activity.
- Acquaint students with the most important textbooks, articles and scientific texts pertaining to the methodology of research.
- Establish the scientific framework of the course.
- Elaborate on the modern penetration testing techniques
- Obtain a deep understanding of how networks and web applications operate

## Learning Outcomes

After successfully completing this material of the course, the students should be able:

- To identify the main phases of a penetration testing framework
- To understand what each phase includes and how it affects the effective completion of the testing methodology
- To focus on the important aspects of a penetration testing activity

## Key Words

Penetration testing	Information Security	Hacking
Cacking	Exploiting	

## Annotated Bibliography

### Basic

- Kim, P., 2018. The Hacker Playbook 3: Practical Guide to Penetration Testing.
- Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G. and Williams, T., 2018. Gray hat hacking: the ethical hacker's handbook. McGraw-Hill Education.

### Suggestions for further reading:

- "Hacking: The Art of Exploitation, 2nd Edition", by Jon Erickson
- "Social Engineering: The Art of Human Hacking", by Christopher Hadnagy and Paul Wilson
- IEEE Journals and Magazines

## Self-Assessment Exercises

### Exercise 1.1

Briefly outline the contents of a penetration testing engagement

### Exercise 1.2

Collaborate on the correlation between the elements.

### Exercise 1.3

List some of the types of hackers.

**Exercise 1.4**

Define the elements of Hacking Methodology.

**Recommended time for the student to work**

15 hours

## PRE-ENGAGEMENT TASKS

2<sup>nd</sup> Week

### Summary

Defining scope is arguably one of the most important components of a penetration test, yet it is also one of the most overlooked. While many volumes have been written about the different tools and techniques which can be utilized to gain access to a network, very little has been written on the topic which precedes the penetration: preparation. Neglecting to properly complete pre-engagement activities has the potential to open the penetration tester (or his firm) to a number of headaches including scope creep, unsatisfied customers, and even legal troubles. The scope of a project specifically defines what is to be tested. How each aspect of the test will be conducted will be covered in the Rules of Engagement section.

One key component of scoping an engagement is outlining how the testers should spend their time. As an example, a customer requests that one hundred IP addresses be tested for the price of \$100,000. This means that the customer is offering \$1,000 per IP address tested. However, this cost structure only remains effective at that volume. A common trap some testers fall into is maintaining linear costs throughout the testing process. If the customer had only asked for one business-critical application to be tested at the same pricing structure (\$1,000), while the tester will still be only attacking a single IP, the volume of work has increased dramatically. It is important to vary costs based on work done. Otherwise a firm can easily find themselves undercharging for their services, which motivates them to do a less than complete job.

Despite having a solid pricing structure, the process is not all black and white. It is not uncommon for a client to be completely unaware of exactly what it is they need tested. It is also possible the client will not know how to communicate effectively what they're expecting from the test. It is important in the Pre-Engagement phase that the tester is able to serve as a guide through what may be uncharted territory for a customer. The tester must understand the difference between a test which focuses on a single application with severe intensity and a test where the client provides a wide range of IP addresses to test and the goal is to simply find a way in.

In addition, regarding the recent cyber security events that were discussed last week, it will be discussed how could an organization further protect against the utilized threat and which additional controls were required but not implemented.

## Introductory Remarks

The aim of this section is to present and explain the tools and techniques available which aid in a successful pre-engagement step of a penetration test. The information within this section is the result of the many years of combined experience of some of the most successful penetration testers in the world. If you are a customer looking for penetration testing, we strongly recommend going to the General Questions section of this document. It covers the major questions that should be answered before a test begins. Remember, a penetration test should not be confrontational. It should not be an activity to see if the tester can "hack" you. It should be about identifying the business risk associated with an attack.

## Aim/Objectives

The aim of this material of the course is to:

- Introduce the students to the first steps towards a penetration testing
- Prepare the roadmap to a successful testing
- Focus on key-risk areas
- Identify vital network and web components
- Prioritize tasks

## Learning Outcomes

After successfully completing this material of the course, the students should be able:

- To outline which are the main steps of the pre-engagement phase
- To effectively prepare for the conduct of a penetration testing activity
- To plan according to the identified threat landscape

## Key Words

Penetration testing	Information Security	Hacking
---------------------	----------------------	---------

Cacking

Exploiting

## Annotated Bibliography

### Basic

- Kim, P., 2018. The Hacker Playbook 3: Practical Guide to Penetration Testing.
- Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G. and Williams, T., 2018. Gray hat hacking: the ethical hacker's handbook. McGraw-Hill Education.

### Suggestions for further reading:

- "Hacking: The Art of Exploitation, 2nd Edition", by Jon Erickson
- "Social Engineering: The Art of Human Hacking", by Christopher Hadnagy and Paul Wilson
- IEEE Journals and Magazines

## Self-Assessment Exercises

### Exercise 2.1

Outline the core elements of this phase.

### Exercise 2.2

Elaborate on which tasks need to be performed to prepare yourself for a penetration testing engagement.

## Recommended time for the student to work

15 hours

## SETTING UP THE LAB

3<sup>rd</sup> Week

### Summary

Discuss setting up a home pentesting lab.

### Introductory Remarks

#### Why Set Up a Home Pentesting Lab?

The obvious reason for setting up a home pentesting lab is to provide a convenient way for the students to test new pentesting skills and software. But beyond convenience, there are several reasons why setting up your own isolated lab is a good idea.

A home pentesting lab is a good way to hone skills while staying out of legal trouble. Hacking into other people's computers and networks is illegal without prior consent, but it's perfectly legal to set up your own lab that mimics someone else's environment and then pentest your copy.

Penetration testing in an isolated lab is also good from a security standpoint. Some penetration-testing tools and techniques have the potential to damage or destroy the target computer or network. If malware is used in testing, there is the potential for infection and spread if testing in an Internet-connected testbed. A standalone, isolated testbed guarantees that the effects of the testing are limited to the lab hardware and software.

Finally, setting up a home pentesting lab can be useful for research and development of new pentesting tools and techniques. An isolated lab provides a controlled environment for testing and the ability to configure the target to the exact specifications needed for the test.

#### Installing Software on the VM

Installing software on a virtual machine works the same way as installing it on a normal computer. Software can either be downloaded from the Internet from within the VM or downloaded to the host computer and transferred to the VM from there. Virtualbox and VMware even have the functionality to allow the VM to use the host machine's CD/DVD drive and USB ports to allow programs to be installed from removable media.

## **What Do I Need for My Lab?**

For the beginning pentester, a pentesting lab only needs to include a vulnerable target computer and a pentesting computer. However, as skill levels and the need for realism increase, the number and complexity of the targets will need to grow, and more components will be added to the target network. In this section, we'll talk about setting up basic targets, how to grow the complexity of the target network, and what a good pentesting machine looks like.

### **The Target**

The design of the target environment in a pentesting lab should depend on the skill level of the pentester and the goal of the pentesting exercise. A beginning pentester should start with a simple environment and add complexity as needed. A pentester preparing for an engagement or testing a new tool or technique should design the lab network to mimic the target as closely as possible. By starting with a vulnerable target and adding complexity as needed, a pentester can design an environment with exactly the right level of complexity to suit their needs.

### **Getting Started with Vulnerable Targets**

If you're just starting as a pentester, you may not know what makes a target vulnerable or not or how to configure a target to be vulnerable to a given type of attack. Luckily, several individuals and organizations have done most of the work for you and provide downloadable vulnerable target machines.

Setting up a computer to be vulnerable can be a lot of work. Several websites offer free downloads of preconfigured vulnerable targets. The following examples are "whole packages," including a virtual machine image preconfigured to be vulnerable. A quick web search will reveal other packages that require installation on an existing VM or computer.

As its name suggests, DVWA (Damn Vulnerable Web Application) is a web application designed to have built-in vulnerabilities. It is written in PHP and MySQL and is designed to be vulnerable to cross-site scripting, SQL injection and other web-based attack vectors.

Metasploitable is a virtual machine created by Rapid7, the developers of the pentesting tool Metasploit. Metasploitable is designed to be vulnerable to the attacks included in the Metasploit framework.

The Web Security Dojo by Maven Security is another web security pentesting target. Built on Xubuntu, it also includes the tools necessary to exploit it, combining the roles of target and pentesting machine.

Google Gruyere is a vulnerable web application hosted online. Using it requires Internet access for the pentesting machine; this separates it from the others listed here, which should be run in a sandboxed environment.

## **Target Network Upgrades**

The simplest pentesting network is a target machine and a pentesting machine (which may both be the same computer). However, as a pentester's skills and needs increase, a larger, more complex network will be needed.

The simplest way to increase the complexity of a pentesting network is to increase the number of targets in the network. By setting up a variety of machines with different operating systems and services, a pentester can gain familiarity with how different computers look from an attacker's perspective.

Another simple way of increasing difficulty is upgrades to services installed on target machines. Vulnerable machines like Metasploitable are intentionally running versions of software known to be vulnerable to certain types of attacks. Incremental upgrades to installed software and researching the vulnerability reports associated with the given version of the software provides an in-depth understanding of the software's internals and a walk through increasingly difficult types of attacks.

Finally, the complexity of a pentesting target environment can be increased by expanding the threat surface of the network. This can be accomplished by expanding the types of service running, including email, web, FTP, database and file servers. Network-level modifications like adding routers and services like DHCP and DNS change the landscape of the target network. Including firewalls and other security measures like PKI, IDS/IPS and SIEM increases the difficulty of the pentesting exercise. Finally, the type of networking can be expanded by adding WiFi, Bluetooth and Near Field Communications (NFC) functionality.

## **The Pentesting Machine**

Now that we've covered how to design a good target environment, it's time to consider the pentesting machine. In general, it's best to have both a Windows and a Linux box for pentesting as different tools and functionality are available on each. There are two methods for setting up a pentesting machine: downloading a preconfigured machine or building your own.

For a novice pentester, downloading a preconfigured pentesting machine is probably the better choice. The Kali distribution of Linux (formerly called Backtrack) is freely available and comes with many of the common Linux-based pentesting tools built-in.

## Aim/Objectives

The aim of this material of the course is to:

- Introduce the students to the first steps towards a penetration testing
- Prepare the roadmap to a successful testing
- Focus on key-risk areas
- Identify vital network and web components
- Prioritize tasks

## Learning Outcomes

After successfully completing this material of the course, the students should be able:

- To outline which are the main steps of the preparation phase
- To effectively prepare for the conduct of a penetration testing activity
- To plan according to the identified threat landscape

## Key Words

Penetration testing	Information Security	Hacking
Cacking	Exploiting	

## Annotated Bibliography

### Basic

- Kim, P., 2018. The Hacker Playbook 3: Practical Guide to Penetration Testing.
- Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G. and Williams, T., 2018. Gray hat hacking: the ethical hacker's handbook. McGraw-Hill Education.

### Suggestions for further reading:

- “Hacking: The Art of Exploitation, 2nd Edition”, by Jon Erickson
- “Social Engineering: The Art of Human Hacking”, by Christopher Hadnagy and Paul Wilson
- IEEE Journals and Magazines

## **Self-Assessment Exercises**

### **Exercise 3.1**

Download and install Virtualization Software.

### **Exercise 3.2**

Download and install Virtual Machines

### **Exercise 3.3**

Install and configure Kali Machine as Attacker and Metasploitable Machine as Vulnerable target machine.

### **Exercise 3.4**

List the command to find interface IP address on Kali and Metasploitable

## **Recommended time for the student to work**

15 hours

## GET FAMILIARIZED WITH KALI TOOLS

4<sup>th</sup> Week

### Summary

Familiarize with Kali Linux penetration testing platform tools.

### Introductory Remarks

Kali Linux is the world's most powerful and popular penetration testing platform, used by security professionals in a wide range of specializations, including penetration testing, forensics, reverse engineering, and vulnerability assessment. It is the culmination of years of refinement and the result of a continuous evolution of the platform, from WHoppiX to WHAX, to BackTrack, and now to a complete penetration testing framework leveraging many features of Debian GNU/Linux and the vibrant open source community worldwide.

Kali Linux has not been built to be a simple collection of tools, but rather a flexible framework that professional penetration testers, security enthusiasts, students, and amateurs can customize to fit their specific needs.

While Kali's focus can be quickly summarized as "penetration testing and security auditing", there are many different tasks involved behind those activities. Kali Linux is built as a framework, because it includes many tools covering very different use cases (though they may certainly be used in combination during a penetration test).

For example, Kali Linux can be used on various types of computers: obviously on the laptops of penetration testers, but also on servers of system administrators wishing to monitor their network, on the workstations of forensic analysts, and more unexpectedly, on stealthy embedded devices, typically with ARM CPUs, that can be dropped in the range of a wireless network or plugged in the computer of target users. Many ARM devices are also perfect attack machines due to their small form factors and low power requirements. Kali Linux can also be deployed in the cloud to quickly build a farm of password-cracking machines and on mobile phones and tablets to allow for truly portable penetration testing.

But that is not all; penetration testers also need servers: to use collaboration software within a team of pen-testers, to set up a web server for use in phishing campaigns, to run vulnerability scanning tools, and other related activities.

## **Basic Tools of Kali – Part 1**

### **Netcat**

Netcat, usually abbreviated to nc, is a network utility with which you can use TCP/IP protocols to read and write data across network connections. You can use it to create any kind of connection as well as to explore and debug networks using tunneling mode, port-scanning, etc.

### **Nmap (Network Mapper)**

Nmap is an abbreviation of ‘Network Mapper’, and it’s very well known free open source hackers tool. Nmap is mainly used for network discovery and security auditing. Literally, thousands of system admins all around the world will use nmap for network inventory, check for open ports, manage service upgrade schedules, and monitor host or service uptime. Nmap, as a tool uses raw IP packets in creative ways to determine what hosts are available on the network, what services (application name and version) those hosts are providing information about, what operating systems (fingerprinting) and what type and version of packet filters/ firewalls are being used by the target. There are dozens of benefits of using nmap, one of which is that fact that the admin user is able to determine whether the network (and associated nodes) need patching. It’s also worth mentioning that there’s a GUI version of Nmap called ‘Zenmap’. We’d advise you to learn using Nmap (i.e. the ‘command line’) then rotate into Zenmap when you are feeling all confident.

### **Metasploit Penetration Testing Software**

#### **Vulnerability Exploitation Tool**

The Metasploit Project is a hugely popular pentesting or hacking framework. Metasploit, along with nmap (see above) and Wireshark (see below) and probably the ‘best known’ three hacker software tools out there. If you are new to Metasploit think of it as a ‘collection of hacking tools and frameworks’ that can be used to execute various tasks. Also – we should also add that if you have never heard of Metasploit and are interested in getting into the Cybersecurity Industry, especially as a Penetration Tester, then this is a ‘must-learn’ tool. Most practical IT Security courses such as OSCP and CEH include a Metasploit component. Widely used by cybersecurity professionals and penetration testers this is an awesome piece of software that you really ought to learn. Metasploit is

essentially a computer security project (framework) that provides the user with vital information regarding known security vulnerabilities and helps to formulate penetration testing and IDS testing plans, strategies and methodologies for exploitation. There's a ton of incredibly useful Metasploit information out there and we hope that the books that we've chosen go someway to help you on your journey, not least if you are a beginner just starting out and looking for beginners tutorials in how to use Metasploit.

### **John The Ripper**

#### Password Cracking Tool

Often you'll see it abbreviated as 'JTR' this is an awesome bit of hacking software that is designed to crack even very complicated passwords. John the Ripper, mostly just referred to as simply, 'John' is a popular password cracking pentesting tool that is most commonly used to perform dictionary attacks. John the Ripper takes text string samples (from a text file, referred to as a 'wordlist', containing popular and complex words found in a dictionary or real passwords cracked before), encrypting it in the same way as the password being cracked (including both the encryption algorithm and key), and comparing the output to the encrypted string. This tool can also be used to perform a variety of alterations to dictionary attacks. If you are somewhat confused between John the Ripper and THC Hydra then think of John the Ripper as an 'offline' password cracker whilst THC Hydra is an "online" cracker. Simple.

### **OWASP Zed**

#### Web Vulnerability Scanner

The Zed Attack Proxy (ZAP) is now one of the most popular OWASP projects. The fact that you've reached this page means that you are likely already a relatively seasoned cybersecurity professional so it's highly likely that you are very familiar with OWASP, not least the OWASP Top Ten Threats listing which is considered as being the 'guide-book' of web application security. This hacking and pentesting tool is a very efficient as well as being an 'easy to use' program that finds vulnerabilities in web applications. ZAP is a popular tool because it does have a lot of support and the OWASP community is really an excellent resource for those that work within Cyber Security. ZAP provides automated scanners as well as various tools that allow you the cyber pro to discover security vulnerabilities manually. Understanding and being able to master this tool would also be advantageous to your career as a penetration tester. If you are a developer, then you have it's obviously highly recommended that you learn how to become very proficient with this 'hacker tool!'

## **Wireshark**

### Packet Sniffing Software

Wireshark is a very popular pentesting tool and for over a year it was not included on our list, however, by popular demand we added it in late June 2016. Wireshark essentially captures data packets in a network in real time and then displays the data in human-readable format (verbose). The tool (platform) has been highly developed and it includes filters, color-coding and other features that lets the user dig deep into network traffic and inspect individual packets. If you'd like to become a penetration tester or work as a Cyber Security practitioner, then learning how to use Wireshark is a must. There are a ton of resources out there to learn Wireshark, and, of particular interest, there's also a Wireshark Certification which you can achieve and place on your LinkedIn profile.

## **Aircrack-ng**

### Password Cracking Tool

The Aircrack suite of Wifi (Wireless) hacking tools are legendary because they are very effective when used in the right hands. For those new to this wireless-specific hacking program, Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking hacking tool that can recover keys when sufficient data packets have been captured (in monitor mode). For those tasked with penetrating and auditing wireless networks Aircrack-ng will become your best friend. It's useful to know that Aircrack-ng implements standard FMS attacks along with some optimizations like KoreKattacks, as well as the PTW attacks to make their attacks more potent. If you are a mediocre hacker then you'll be able to crack WEP in a few minutes and you ought to be pretty proficient at being able to crack WPA/ WPA2. For those interested in Wireless Hacking we'd also highly recommend taking a look at the very awesome Reaver, another very popular hacking tool that alas we couldn't add to our list.

## **Aim/Objectives**

The aim of this material of the course is to:

- Learn how to use Kali tools against Target machines or Networks
- Download, install and update Kali Software and 3rd party software on Kali Machine
- Learn how to scan, find Vulnerabilities and Exploit target machines.

## Learning Outcomes

After successfully completing this material of the course, the students should be able:

- To outline which are the main steps of the preparation phase
- To effectively prepare for the conduct of a penetration testing activity
- To plan according to the identified threat landscape

## Key Words

Penetration testing	Information Security	Hacking
Cacking	Exploiting	

## Annotated Bibliography

### Basic

- Kim, P., 2018. The Hacker Playbook 3: Practical Guide to Penetration Testing.
- Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G. and Williams, T., 2018. Gray hat hacking: the ethical hacker's handbook. McGraw-Hill Education.

### Suggestions for further reading:

- "Hacking: The Art of Exploitation, 2nd Edition", by Jon Erickson
- "Social Engineering: The Art of Human Hacking", by Christopher Hadnagy and Paul Wilson
- IEEE Journals and Magazines

## Self-Assessment Exercises

### Exercise 4.1

Lab exercise 1.

### Exercise 4.2

Lab exercise 2.

## Recommended time for the student to work

15 hours

## ADDITIONAL KALI TOOLS

5<sup>th</sup> Week

### Summary

Tools of Kali Linux penetration testing platform.

### Introductory Remarks

Kali Linux is the world's most powerful and popular penetration testing platform, used by security professionals in a wide range of specializations, including penetration testing, forensics, reverse engineering, and vulnerability assessment. It is the culmination of years of refinement and the result of a continuous evolution of the platform, from WHoppiX to WHAX, to BackTrack, and now to a complete penetration testing framework leveraging many features of Debian GNU/Linux and the vibrant open source community worldwide.

Kali Linux has not been built to be a simple collection of tools, but rather a flexible framework that professional penetration testers, security enthusiasts, students, and amateurs can customize to fit their specific needs.

While Kali's focus can be quickly summarized as "penetration testing and security auditing", there are many different tasks involved behind those activities. Kali Linux is built as a framework, because it includes many tools covering very different use cases (though they may certainly be used in combination during a penetration test).

For example, Kali Linux can be used on various types of computers: obviously on the laptops of penetration testers, but also on servers of system administrators wishing to monitor their network, in the workstations of forensic analysts, and more unexpectedly, on stealthy embedded devices, typically with ARM CPUs, that can be dropped in the range of a wireless network or plugged in the computer of target users. Many ARM devices are also perfect attack machines due to their small form factors and low power requirements. Kali Linux can also be deployed in the cloud to quickly build a farm of password-cracking machines and on mobile phones and tablets to allow for truly portable penetration testing.

But that is not all; penetration testers also need servers: to use collaboration software within a team of pen-testers, to set up a web server for use in phishing campaigns, to run vulnerability scanning tools, and other related activities.

## **Basic Tools of Kali – Part 2**

### **Armitage**

Vulnerability Exploitation Tool

open source software and fantastic GUI front-end for the Metasploit Framework developed by Raphael Mudge with the goal of helping security professionals better understand hacking and to help them realize the power of Metasploit. Armitage organizes Metasploit's capabilities around the hacking process. There are features for discovery, access, post-exploitation, and maneuver. It's a scriptable red team collaboration tool for Metasploit that visualizes targets, recommends exploits, and exposes the advanced post-exploitation features in the framework.

### **Maltego**

Digital Forensics

Maltego is different in that it works within a digital forensics sphere. Maltego is a platform that was designed to deliver an overall cyber threat picture to the enterprise or local environment in which an organization operates. One of the awesome things about Maltego which likely makes it so popular (and included in the Kali Linux Top Ten) is its unique perspective in offering both network and resource based entities is the aggregation of information sourced throughout the web – whether it's the current configuration of a vulnerable router within a network or the current whereabouts of your staff members on their international visits, Maltego can locate, aggregate and visualize this data! For those interested in learning how to use Maltego we'd also recommend learning about OSINT cybersecurity data procurement.

### **Cain and Abel Hacking Tool**

Password Cracker/ Password Hacking

Cain and Abel (often simply abbreviated to Cain) is a hugely popular hacking tool and one that is very often mentioned online in a variety of 'hacking tutorials'. At its' heart, Cain and Abel is a password recovery tool for Microsoft Windows but it can be used off-label in a variety of uses, for example, white and black hat hackers use Cain to recover (i.e. 'crack') many types of passwords using methods such as network packet sniffing and by using the tool to crack password hashes.

Cain, for example, when used to crack password hashes would use methods such as dictionary attacks, brute force, rainbow table attacks and cryptanalysis attacks.

### **Nikto Website Vulnerability Scanner**

#### Website Vulnerability Scanner Hacking Tool

Nikto is another classic 'Hacking Tool' that a lot of pentesters like to use. Worth mentioning that Nikto is sponsored by Netsparker (which is yet another Hacking Tool that we have also listed in our directory). Nikto is an Open Source (GPL) web server scanner which is able to scan and detect web servers for vulnerabilities. The system searches against a database of over 6800 potentially dangerous files/ programs when scanning software stacks. Nikto, like other scanners out there, also scans for outdated (unpatched) versions of over 1300 servers, and version specific problems on over 275 servers. Interestingly, Nikto can also check server configuration items such as the presence of multiple index files, HTTP server options, and the platform will also try to identify installed web servers and web applications. Nikto will get picked up by any semi-decent IDS tool so its' really useful when conducting a white-hat/ white-box pentest. Certainly a great tool to learn your skills on when attacking an open box for training.

### **Aim/Objectives**

The aim of this material of the course is to:

- Learn how to use Kali tools against Target machines or Networks
- Download, install and update Kali Software and 3rd party software on Kali Machine
- Learn how to scan, find Vulnerabilities and Exploit target machines.

### **Learning Outcomes**

After successfully completing this material of the course, the students should be able:

- Learn how to use Kali tools against Target machines or Networks
- Download, install and update Kali Software and 3rd party software on Kali Machine
- Learn how to scan, find Vulnerabilities and Exploit target machines.

## Key Words

Penetration testing	Information Security	Hacking
Cacking	Exploiting	

## Annotated Bibliography

### Basic

- Kim, P., 2018. The Hacker Playbook 3: Practical Guide to Penetration Testing.
- Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G. and Williams, T., 2018. Gray hat hacking: the ethical hacker's handbook. McGraw-Hill Education.

### Suggestions for further reading:

- "Hacking: The Art of Exploitation, 2nd Edition", by Jon Erickson
- "Social Engineering: The Art of Human Hacking", by Christopher Hadnagy and Paul Wilson
- IEEE Journals and Magazines

## Self-Assessment Exercises

### Exercise 5.1

Lab exercise 3.

## Activity (5 points)

The subject of the activity will be announced at a later stage.

## Recommended time for the student to work

20 hours

# INTELLIGENCE GATHERING PHASE

6<sup>th</sup> Week

## Summary

This section defines the Intelligence Gathering activities of a penetration test. The purpose of this document is to provide a standard designed specifically for the pentester performing reconnaissance against a target (typically corporate, military, or related). The document details the thought process and goals of pentesting reconnaissance, and when used properly, helps the reader to produce a highly strategic plan for attacking a target.

## Introductory Remarks

The Intelligence Gathering levels are currently split into three categories, and a typical example is given for each one. These should guide the adding of techniques in the document below. For example, an intensive activity such as creating a facebook profile and analyzing the target's social network is appropriate in more advanced cases, and should be labeled with the appropriate level. See the mindmap below for examples.

- Level 1 Information Gathering: (think: Compliance Driven) Mainly a click-button information gathering process. This level of information can be obtained almost entirely by automated tools. Bare minimum to say you did IG for a PT. Acme Corporation is required to be compliant with PCI / FISMA / HIPAA. A Level 1 information gathering effort should be appropriate to meet the compliance requirement.
- Level 2 Information Gathering: (think: Best Practice) This level can be created using automated tools from level 1 and some manual analysis. A good understanding of the business, including information such as physical location, business relationships, org chart, etc. Widgets Inc is required to be in compliance with PCI, but is interested in their long term security strategy, and is acquiring several smaller widget manufacturers. A Level 2 information gathering effort should be appropriate to meet their needs.
- Level 3 Information Gathering: (think: State Sponsored) More advanced pentest, Redteam, full-scope. All the info from level 1 and level 2 along with a lot of manual analysis.

Think cultivating relationships on SocNet, heavy analysis, deep understanding of business relationships, most likely a large number of hours to accomplish the gathering and correlation. An Army Red Team is tasked to analyze and attack a segment of the Army's network in a foreign country to find weaknesses that could be exploited by a foreign national. A level 3 information gathering effort would be appropriate in this case.

## Aim/Objectives

The aim of this material of the course is to:

- Introduce the students to the information gathering phase
- Prepare the roadmap to a successful testing
- Collect all related information to the target
- Search for relevant information sources
- Identify the related and most important information

## Learning Outcomes

After successfully completing this material of the course, the students should be able to:

- outline which are the main steps of the information gathering phase
- effectively prepare for the conduct of a penetration testing activity
- prioritize the collected information
- map the retrieved information with the target system

## Key Words

Penetration testing	Information Security	Hacking
Cacking	Exploiting	

## Annotated Bibliography

### Basic

- Kim, P., 2018. The Hacker Playbook 3: Practical Guide to Penetration Testing.

- Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G. and Williams, T., 2018. Gray hat hacking: the ethical hacker's handbook. McGraw-Hill Education.

### Suggestions for further reading:

- "Hacking: The Art of Exploitation, 2nd Edition", by Jon Erickson
- "Social Engineering: The Art of Human Hacking", by Christopher Hadnagy and Paul Wilson
- IEEE Journals and Magazines

## Self-Assessment Exercises

### Exercise 6.1

Identify the importance of the information gathering phase.

### Exercise 6.2

Elaborate on which tools are used in phase and what type of information is gathered

## Recommended time for the student to work

15 hours

## THREAT MODELING PHASE

7<sup>th</sup> Week

### Summary

- Gather relevant documentation
- Identify and categorize primary and secondary assets
- Identify and categorize threats and threat communities
- Map threat communities against primary and secondary assets

### Introductory Remarks

This section defines a threat modeling approach as required for a correct execution of a penetration testing. The standard does not use a specific model, but instead requires that the model used be consistent in terms of its representation of threats, their capabilities, their qualifications as per the organization being tested, and the ability to repeatedly be applied to future tests with the same results. The section focuses on two key elements of traditional threat modeling - assets and attacker (threat community/agent). Each one is respectively broken down into business assets and business processes and the threat communities and their capabilities. As a minimum, all four elements should be clearly identified and documented in every penetration test.

### Aim/Objectives

The aim of this material of the course is to:

- Introduce the students to the threat modeling phase
- Prepare the roadmap to a successful testing

### Learning Outcomes

After successfully completing this material of the course, the students should be able to:

- outline which are the main steps of the threat modeling phase
- effectively prepare for the conduct of a penetration testing activity
- understand the key risk areas

- identify the threats that the target currently faces

## Key Words

Penetration testing	Information Security	Hacking
Cacking	Exploiting	

## Annotated Bibliography

### Basic

- Kim, P., 2018. The Hacker Playbook 3: Practical Guide to Penetration Testing.
- Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G. and Williams, T., 2018. Gray hat hacking: the ethical hacker's handbook. McGraw-Hill Education.

### Suggestions for further reading:

- “Hacking: The Art of Exploitation, 2nd Edition”, by Jon Erickson
- “Social Engineering: The Art of Human Hacking”, by Christopher Hadnagy and Paul Wilson
- IEEE Journals and Magazines

## Self-Assessment Exercises

### Exercise 7.1

Identify the importance of the threat modeling phase.

### Exercise 7.2

Elaborate on which tools are used in phase and what type of information is gathered.

## Recommended time for the student to work

15 hours

## VULNERABILITY ASSESSMENT PHASE

8<sup>th</sup> Week

### Summary

Vulnerability testing is the process of discovering flaws in systems and applications which can be leveraged by an attacker. These flaws can range anywhere from host and service misconfiguration, or insecure application design. Although the process used to look for flaws varies and is highly dependent on the particular component being tested, some key principals apply to the process.

### Introductory Remarks

- Active testing involves direct interaction with the component being tested for security vulnerabilities. This could be low level components such as the TCP stack on a network device, or it could be components higher up on the stack such as the web-based interface used to administer such a device. There are two distinct ways to interact with the target component: automated, and manual.
- Metadata analysis involves looking at data that describes a file, as opposed to the file data itself. A Microsoft Office document for example, might list the document author, company, when the document was last saved, when the document was created, and so on. Many documents even allow for the entry of custom metadata. This could potentially contain internal addresses and paths to servers, internal IP addresses, and other information a penetration tester could use to gain additional access or information.
- Once a vulnerability has been reported in a target system, it is necessary to determine the accuracy of the identification of the issue, and to research the potential exploitability of the vulnerability within the scope of the penetration test. In many cases, the vulnerability will be a reported software vulnerability in a commercial or open source software package, and in other cases the vulnerability can be a flaw in a business process, or a common administrative error like misconfiguration or default password usage.

## Aim/Objectives

The aim of this material of the course is to:

- Introduce the students to the vulnerability assessment phase
- Prepare the roadmap to a successful testing
- Understand how vulnerability assessment operates
- Identify key risk components

## Learning Outcomes

After successfully completing this material of the course, the students should be able to:

- outline which are the main steps of the vulnerability assessment phase
- effectively prepare for the conduct of a penetration testing activity
- prioritize the identified vulnerabilities
- assess the vulnerable network and web components

## Key Words

Penetration testing	Information Security	Hacking
Cacking	Exploiting	

## Annotated Bibliography

### Basic

- Kim, P., 2018. The Hacker Playbook 3: Practical Guide to Penetration Testing.
- Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G. and Williams, T., 2018. Gray hat hacking: the ethical hacker's handbook. McGraw-Hill Education.

### Suggestions for further reading:

- "Hacking: The Art of Exploitation, 2nd Edition", by Jon Erickson
- "Social Engineering: The Art of Human Hacking", by Christopher Hadnagy and Paul Wilson
- IEEE Journals and Magazines

## **Self-Assessment Exercises**

### **Exercise 8.1**

Identify the importance of the vulnerability assessment phase.

### **Exercise 8.2**

Elaborate on which tools are used in phase and what type of information is gathered.

## **Individual Assignment (20 points)**

The subject of the individual assignment will be announced at a later stage.

## **Recommended time for the student to work**

35 hours

# AUTOMATED TOOLS FOR PENETRATION TESTING AND REPORTING

9<sup>th</sup> Week

## Summary

The automated penetration test plays an important role in the security professional's toolkit. As part of a comprehensive security program, these tools can quickly evaluate the security of systems, networks and applications against a wide variety of threats. But security pros should view them as a supplement, rather than a replacement, for traditional manual testing techniques.

## Introductory Remarks

### What is automated penetration testing?

During a penetration test, security professionals conduct deliberate attacks on systems and applications to determine whether it is possible to gain unauthorized access. The goal of these tests is to assume the "hacker mindset" and probe for security vulnerabilities using the same tools and techniques employed by real attackers. Penetration testing is widely considered the best test of a system's security, as it most closely approximates real-world attacks. Conducting these tests properly requires time-consuming work by highly skilled individuals. Ideally, the engineers performing the tests have a level of skill equal to or exceeding the skill level of the likely attacker.

The highly manual nature and great expense associated with penetration tests leads many organizations to automate parts of the process. The test is still guided by a skilled professional, but many steps are automated to remove the rote components of the test. For example, the testers might employ vulnerability scanners to test a large number of systems for the presence of vulnerabilities. Similarly, automated exploit tools might be used to carry out a multi-step attack.

### Why use automated testing?

The use of these tools provides organizations with several key benefits. First, the use of frequent scanning increases the speed of detection when new vulnerabilities arise. Second, tools can broadly test a large number of systems for a huge number of known vulnerabilities, compared to a tedious manual testing process. Finally, automated tools relieve highly skilled individuals of monotonous work, allowing them to focus their energy on coordinating the test and applying their expertise where it is most valuable.

Automated testing tools can also be a key component of IT compliance programs. For example, the Payment Card Industry Data Security Standard (PCI DSS) requires regular vulnerability assessments of card-processing systems. Automation is the only realistic way of meeting this requirement. It is important to note, however, that automation is not a silver bullet for PCI compliance. The standard recognizes this: "Penetration testing is generally a highly manual process. While some automated tools may be used, the tester uses their knowledge of systems to penetrate into an environment."

## **Automated Penetration Testing Tools**

### **Nessus**

#### Penetration Testing Software

Nessus is one of the most popular and capable vulnerability scanners, particularly for UNIX systems. It was initially free and open source, but they closed the source code in 2005 and removed the free "Registered Feed" version in 2008. It now costs \$2,190 per year, which still beats many of its competitors. A free "Nessus Home" version is also available, though it is limited and only licensed for home network use.

Nessus is constantly updated, with more than 70,000 plugins. Key features include remote and local (authenticated) security checks, a client/server architecture with a web-based interface, and an embedded scripting language for writing your own plugins or understanding the existing ones.

### **OpenVAS**

#### Penetration Testing Software

OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. The framework is part of Greenbone Networks' commercial vulnerability management solution from which developments are contributed to the Open Source community since 2009.

The actual security scanner is accompanied with a regularly updated feed of Network Vulnerability Tests (NVTs), over 50,000 in total.

All OpenVAS products are Free Software. Most components are licensed under the GNU General Public License (GNU GPL).

## **Dradis**

Dradis is an open source framework to enable effective information sharing, specially during security assessments. Dradis is a self-contained web application that provides a centralized repository of information to keep track of what has been done so far, and what is still ahead.

Features include:

- Easy report generation.
- Support for attachments.
- Integration with existing systems and tools through server plugins.
- Platform independent.

## **Aim/Objectives**

The aim of this material of the course is to:

- Introduce the students to the vulnerability assessment phase
- Prepare the roadmap to a successful testing
- Understand how vulnerability assessment operates
- Identify key risk components

## **Learning Outcomes**

After successfully completing this material of the course, the students should be able to:

- Learn how to use Automated Vulnerability Scanning Software against Target machines or Networks
- Learn how to create the report for Vulnerability findings
- Learn how to mitigate/fix the Vulnerabilities

## **Key Words**

Penetration testing	Information Security	Hacking
Cacking	Exploiting	

## Annotated Bibliography

### Basic

- Kim, P., 2018. The Hacker Playbook 3: Practical Guide to Penetration Testing.
- Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G. and Williams, T., 2018. Gray hat hacking: the ethical hacker's handbook. McGraw-Hill Education.

### Suggestions for further reading:

- "Hacking: The Art of Exploitation, 2nd Edition", by Jon Erickson
- "Social Engineering: The Art of Human Hacking", by Christopher Hadnagy and Paul Wilson
- IEEE Journals and Magazines

## Self-Assessment Exercises

### Exercise 9.1

Lab exercise 4

### Recommended time for the student to work

15 hours

## VULNERABILITY EXPLOITATION PHASE

10<sup>th</sup> Week

### Summary

- Identify the weakness
- Find specific characteristics of the vulnerability
- Find the related tool/approach
- Exploit the vulnerability

### Introductory Remarks

The exploitation phase of a penetration test focuses solely on establishing access to a system or resource by bypassing security restrictions. If the prior phase, vulnerability analysis was performed properly, this phase should be well planned and a precision strike. The main focus is to identify the main entry point into the organization and to identify high value target assets. If the vulnerability analysis phase was properly completed, a high value target list should have been compiled. Ultimately the attack vector should take into consideration the success probability and highest impact on the organization.

### Aim/Objectives

The aim of this material of the course is to:

- Introduce the students to the vulnerability exploitation phase
- Prepare the roadmap to a successful testing

### Learning Outcomes

After successfully completing this material of the course, the students should be able to:

- To outline which are the main steps of the vulnerability exploitation phase
- To effectively prepare for the conduct of a penetration testing activity

## Key Words

Penetration testing	Information Security	Hacking
Cacking	Exploiting	

## Annotated Bibliography

### Basic

- Kim, P., 2018. The Hacker Playbook 3: Practical Guide to Penetration Testing.
- Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G. and Williams, T., 2018. Gray hat hacking: the ethical hacker's handbook. McGraw-Hill Education.

### Suggestions for further reading:

- "Hacking: The Art of Exploitation, 2nd Edition", by Jon Erickson
- "Social Engineering: The Art of Human Hacking", by Christopher Hadnagy and Paul Wilson
- IEEE Journals and Magazines

## Self-Assessment Exercises

### Exercise 10.1

Identify the importance of the vulnerability exploitation phase.

### Exercise 10.21

Elaborate on which tools are used in phase and what type of information is gathered.

## Activity (5 points)

The subject of the activity will be announced at a later stage.

## Recommended time for the student to work

20 hours

## POST-EXPLOITATION TASKS

11<sup>th</sup> Week

### Summary

- Protect the client
- Analyze the infrastructure
- Cover tracks

### Introductory Remarks

The purpose of the Post-Exploitation phase is to determine the value of the machine compromised and to maintain control of the machine for later use. The value of the machine is determined by the sensitivity of the data stored on it and the machines usefulness in further compromising the network. The methods described in this phase are meant to help the tester identify and document sensitive data, identify configuration settings, communication channels, and relationships with other network devices that can be used to gain further access to the network, and setup one or more methods of accessing the machine at a later time. In cases where these methods differ from the agreed upon Rules of Engagement, the Rules of Engagement must be followed.

### Aim/Objectives

The aim of this material of the course is to:

- Introduce the students to the post-exploitation phase
- Prepare the roadmap to a successful testing
- Understand the tasks to be performed after the exploitation

### Learning Outcomes

After successfully completing this material of the course, the students should be able to:

- outline which are the main steps of the post-exploitation phase
- effectively prepare for the conduct of a penetration testing activity
- protect identification after exploitation

## Key Words

Penetration testing	Information Security	Hacking
Cacking	Exploiting	

## Annotated Bibliography

### Basic

- Kim, P., 2018. The Hacker Playbook 3: Practical Guide to Penetration Testing.
- Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G. and Williams, T., 2018. Gray hat hacking: the ethical hacker's handbook. McGraw-Hill Education.

### Suggestions for further reading:

- "Hacking: The Art of Exploitation, 2nd Edition", by Jon Erickson
- "Social Engineering: The Art of Human Hacking", by Christopher Hadnagy and Paul Wilson
- IEEE Journals and Magazines

## Self-Assessment Exercises

### Exercise 11.1

Identify the importance of the this current phase.

### Exercise 11.2

Elaborate on which tools are used in phase and what type of information is gathered.

## Recommended time for the student to work

15 hours

# REPORTING

12<sup>th</sup> Week

## Summary

- Executive summary
- Technical Report

## Introductory Remarks

This document is intended to define the base criteria for penetration testing reporting. While it is highly encouraged to use your own customized and branded format, the following should provide a high-level understanding of the items required within a report as well as a structure for the report to provide value to the reader.

## Aim/Objectives

The aim of this material of the course is to:

- Introduce the students to the reporting phase
- Prepare the roadmap to a successful testing
- Understand the importance of reporting
- Develop the report's key components

## Learning Outcomes

After successfully completing this material of the course, the students should be able to:

- outline which are the main steps of the reporting phase
- effectively prepare for the conduct of a penetration testing activity
- prepare a thorough report
- summarize key findings
- suggest related solutions

## Key Words

Penetration testing	Information Security	Hacking
Cacking	Exploiting	

## Annotated Bibliography

### Basic

- Kim, P., 2018. The Hacker Playbook 3: Practical Guide to Penetration Testing.
- Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G. and Williams, T., 2018. Gray hat hacking: the ethical hacker's handbook. McGraw-Hill Education.

### Suggestions for further reading:

- "Hacking: The Art of Exploitation, 2nd Edition", by Jon Erickson
- "Social Engineering: The Art of Human Hacking", by Christopher Hadnagy and Paul Wilson
- IEEE Journals and Magazines

## Self-Assessment Exercises

### Exercise 12.1

Identify the importance of the reporting phase.

### Exercise 12.2

Elaborate on which tools are used in phase and what type of information is gathered.

## Group Assignment (20 points)

The group assignment subject will be announced at a later stage.

## Recommended time for the student to work

35 hours

# LAB PRACTICE

13<sup>th</sup> Week

## Summary

Lab Practice.

## Introductory Remarks

This is a lab-only practice week, where the students will be reviewed based on what they have learned from all the above chapters.

## Aim/Objectives

The aim of this material of the course is to:

- Prepare the students for the penetration testing engagement
- Prepare the roadmap to a successful testing
- Understand the importance of testing
- Develop the report's key components

## Learning Outcomes

After successfully completing this material of the course, the students should be able to:

- outline which are the main steps of the penetration testing
- effectively prepare for the conduct of a penetration testing activity
- prepare a thorough report
- summarize key findings
- suggest related solutions

## Key Words

Penetration testing	Information Security	Hacking
Cacking	Exploiting	

## Annotated Bibliography

### Basic

- Kim, P., 2018. The Hacker Playbook 3: Practical Guide to Penetration Testing.
- Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G. and Williams, T., 2018. Gray hat hacking: the ethical hacker's handbook. McGraw-Hill Education.

### Suggestions for further reading:

- "Hacking: The Art of Exploitation, 2nd Edition", by Jon Erickson
- "Social Engineering: The Art of Human Hacking", by Christopher Hadnagy and Paul Wilson
- IEEE Journals and Magazines

## Recommended time for the student to work

15 hours

## **REVISION AND FINAL EXAMINATION**

The final examination will consist of true/false, multiple-choice questions and a small number of questions.

### **Recommended time for the student to work**

40 hours

**Date/Time of Final Exam: TBD**



**FORM: 200.1.3**

## **STUDY GUIDE**

**Course: CYS621 – Research Methods in Cybersecurity**

## Course Information

<b>Institution</b>	European University Cyprus		
<b>Programme of Study</b>	Cybersecurity (MSc)		
<b>Course unit</b>	CYS621	Research Methods in Cybersecurity	
<b>Level</b>	<i>Undergraduate</i>	<i>Postgraduate</i>	
		<i>Master</i>	<i>PhD</i>
		√	
<b>Language of Instruction</b>	English		
<b>Teaching Methodology</b>	Distance Learning		
<b>Course Type</b>	<i>Compulsory</i>		<i>Optional</i>
			√
<b>Number of Group Consultation Meetings/ Web-Conferences/ Lectures</b>	<b>Total</b>	<b>Face to Face</b>	<b>Web-Conferences</b>
	14	1	13
<b>Number of Activities/ Assignments</b>	4		
<b>Final Assessment</b>	<i>Assignments</i>		<i>Final Examinations</i>
	50 %		50 %
<b>Number of Credits (ECTS)</b>	10		

<b>Study Guide drafted by</b>	Dr. George Christou
<b>Editing and final approval of Study Guide by</b>	Dr Yianna Danidou

## COURSE CONTENTS

		Page
	Introductory Notes	4
	First Group Consultation Meeting	6
1	Week 1 – What is Research	8
2	Week 2 – The Language of Statistics	11
3	Week 3 – Organizing and Presenting Data	14
4	Week 4 – The Research Article	17
5	Week 5 – The Research Article continued	21
6	Week 6 – Qualitative Methods	24
7	Week 7 – Quantitative Methods	28
8	Week 8 – Descriptive Statistics	31
9	Week 9 – Probability and Distributions	35
10	Week 10 – Hypothesis Testing	38
11	Week 11 – Regression and Correlation	41
12	Week 12 – Review	44
13	Week 13 – Presentation	45
14	Revision and Final Examination	46
	Indicative answers to Self-Assessment Exercises	47

## INTRODUCTORY NOTES

### 1.1 Instructor and Communication

The instructor for this course is Dr. George Christou. You can contact Dr. Christou through email – [g.christou@euc.ac.cy](mailto:g.christou@euc.ac.cy), during his office hours face-to-face at his office located at Room 114, or through the phone at +357-22713104. You can also use blackboard to arrange for an online meeting whenever the need arises.

*Students are encouraged to communicate with the instructor throughout the duration of this course. The students should not only communicate with the instructor, but should also use blackboard's course forum to communicate with each other, exchange ideas, and collaborate in solving and clarifying their questions. Collaboration is what drives scientific enquiry, and even though each student will create a unique thesis, several questions about the research and the writing are common to everyone. As such, the students should feel free to post and answer questions on the course forum, and utilize the instructor to the fullest extent. The contact details and ways of contacting the instructor are described in the first part of this guide.*

### 1.2 Short course description and objectives:

*The CYS621 course is one of the core course of the program. Students must have a firm grasp and understanding of the areas that encompass the field of Research Methods, most particularly in a field such as Cybersecurity. Because there will be times that experiments will need to be run on machines to simulate specific vulnerabilities and problems, the security professional needs to be aware of how to properly set up experiments that will provide evidence towards the specific problems he or she faces. Thus, the course will introduce students to the current trends in research methods, starting with understanding what research is, and ending with statistical methods that allow for the performance of experiments to find interactions between different variables during execution of those experiments.*

*Students are required to attend weekly virtual classes to submit discussion posts, to solve problem sets, to hand-in assignments and to write exams.*

*On successful completion, the student will have the knowledge and skills to:*

- *Explain the scientific method*
- *Discuss the various types of research*
- *Assess data through descriptive statistics*

- Create correct scientific experiments
- Propose critical analyses of data based on statistical tests
- Explain correlation and regression evidence as part of the analysis of an experimental result

*In particular, course assignments will emphasize researcher and practitioner reflexivity, allowing students to explore their own understanding of the subject matter.*

*This study guide has been prepared collectively by Dr. Georgios Christou. The guide has been approved by the relevant Department Chair and the Distance Education Unit Director. The study guide is based on the syllabus and learning material (provided through the online learning platform) of the course CYS6XX. The guide consists of a basic tool of the learning process for this course and it has been designed to use it along with the course learning material. The aim of this guide is to direct students on how to use the learning material of this course in order to understand and comprehend it. The guide aims to provide the necessary support needed for distance learning. The guide is continuously updated to keep in accord with the course learning material and to meet the aim of the course. Although the study guide provides extensive information related to the course, it does not substitute in any way the learning material provided on the learning platform. It is imperative that the studying of the learning material and executing the rest of the activities of the course (e.g. attending online lectures, completing coursework) are very important for the successful completion of the course.*

*This guide consists of a number of units, divided in 13 weeks, each one comprised of the summary and introductory remarks, aim, learning outcomes, keywords, required learning material, recommended further learning material, self-assessment activities and expected time for self-study. At the end of this study guide, students can find suggested solutions and proposed answers to all the self-assessment activities of this guide. It is very important that students carry out the suggested self-assessment activities because it will assist them to understand in a practical way the theoretical material they study for this course. In addition, the self-assessment activities help to motivate and encourage students to carry out their self-study and to develop their analytical and critical thinking skills. The self-assessment activities together with the model answers to the self-assessment activities serve as a kind of a self-assessment for students. The expected time for self-study of each unit includes the expected time spent on studying the learning material and carrying out the self-assessment activities of each unit. The expected time for self-study does not include the expected time for attending online lectures, coursework preparation, final examination preparation, and final examination itself.*

## 1st GROUP CONSULTATION MEETING

### Programme Presentation

Leading companies today are rethinking the role of information security in their organizations. They realize that in a digital world, cybersecurity is the key to safeguarding their most precious assets—intellectual property, customer information, financial data, and employee records, among others. But far more than a defensive measure, companies also know that cybersecurity can better position their organization with business partners, customers, investors, and other stakeholders.

The European cybersecurity market is about 25% (i.e. about €17bln) of the world market (estimated at €70bln in 2015), with an average yearly growth slightly larger than 6%, when the world market is growing at about 10%/year. Recent study compiled by Europe's cybersecurity industry leaders pointed out that Europe is in danger of falling behind in the international digital economy field.

The Master in Cybersecurity is a cutting-edge program, designed for those wishing to develop a career as a cyber-security professional, or to take a leading technical or managerial role in an organization critically dependent upon data and information communication technology. Students will develop an advanced knowledge of information security and an awareness of the context in which information security operates in terms of safety, environmental, social and economic aspects. They will gain a wide range of intellectual, practical and transferable skills, enabling them to develop a flexible professional career in IT.

Key elements of this postgraduate degree are: the *real life experience* given by the opportunity to apply their theoretical knowledge through specialized virtual and remote security laboratories in which they will be able to carry out activities such as reconnaissance, network scanning and exploitation exercises, and investigate the usage and behavior of security systems such as Intrusion Detection and Prevention Systems thus becoming confident in the practical application of the latest tools; the *high-level insight* that will enhance student's ability to research and design creative cyber security solutions to address business problems; *hands-on skills* through experimentation with security techniques, cryptographic algorithms, cyber forensics building an ethical hacking environment; and *flexibility* since students will also be able to choose either the completion of a Master thesis or to complete a Research methods course and two elective courses.

Students undertake modules to the value of 90 ECTS credits.

## **Recommended time for the student to work**

*During the first week, the student is recommended to take as much time as required to study this guide, and to attend the online training to become familiarized with the Blackboard platform and the Library's online functions.*

*The approximate time required is about five (5) hours of study.*

## WHAT IS RESEARCH

1<sup>st</sup> Week

### Summary

After the completion of the three-hour meeting, the students should be able to critically assess and compare the two major types of research, quantitative and qualitative, discuss how academic discourse works, and be able to suggest what type of research they should use given the specific topics provided by the Thesis Topic Catalogue provided by the departmental members.

### Introductory Remarks

During the second meeting of the semester, the students will discuss and become exposed to the major paradigms of **research**. Research is the investigation or experimentation aimed at the discovery and interpretation of facts, revision of accepted theories or laws in the light of new facts, or practical application of such new or revised theories or laws. The students will compare these paradigms, and critically discuss how research takes place in the context of **academic discourse**, or academic dialogue, the inclusion of all lingual material for a specific topic. They will also assess the **ethical**, **legal**, and **social** implications of the performance of a research project, given its particular objectives and scientific questions. The students will further delve into a discussion on the differences between **qualitative research** and **quantitative research**. Qualitative research is a scientific method that is based on gathering non-numerical data, such as notes, bodies of text, etc. whereas quantitative research is a scientific method that requires the gathering and analysis of numerical data.

### Aim/Objectives

The aim of this meeting will be for the students to be able to critically discuss the various types of research that they can use

### Learning Outcomes

After the completion of the three hour meeting, the student should begin to grasp the method of how to select and justify a research topic. The student will be able to discuss the ethical, legal

and social implications of research, and be able to critically assess these implications for his or her selected project.

## Key Words

Academic Discourse	Research	Research Paradigm
Qualitative Research	Quantitative Research	Research Proposal
Ethics in Research	Legal Issues in Research	Social Issues in Research

## Annotated Bibliography

### Basic Material

Edgar, T. W. and Manz, D. O. (2017). Research Methods for Cyber Security. Cambridge, MA: Syngress.

### Supplementary Material

Notes and slides handed out by the instructor of the course

## Self-Assessment Exercises

### Exercise 1.1

What is the most appropriate research design for each of the following studies? Why do you think so?

- a) A new social program is being developed to help troubled youth.
- b) A grant is awarded for the purpose of studying the differences in attitudes towards eldercare in the US versus Japan.
- c) A physician has a patient with a particularly unusual case of plantar warts, which seem to be completely resistant to all known forms of treatment. He wants to study the course of the disease in this particular case. As far as he knows, this is the only such case in existence.
- d) A physical education specialist wants to know if training on elliptical machines is more effective than training on treadmills.

- e) A physician who works with overweight and obese clients wants to determine if body weight is related to blood pressure.

### **Recommended time for the student to work**

15 hours

# THE LANGUAGE OF STATISTICS

2<sup>nd</sup> Week

## Summary

During this week, the basic concepts of statistics and research design will be introduced.

## Introductory Remarks

This meeting introduces some of the basic concepts of statistics and research design. The differences among **descriptive**, **inferential**, **correlational**, and **predictive** statistics are discussed in some detail. We also discuss variables and the various ways of their classification.

Further, we will examine various research designs and discuss validity in design. **Internal Validity** refers to how well an experiment is done, especially whether it avoids confounding (more than one possible independent variable [cause] acting at the same time). The less chance for confounding in a study, the higher its internal validity is. On the other hand, **External Validity** is the measure of how generalizable the results of a study are in the general population.

The discussion focuses on the types of statistical analyses as follows. First descriptive statistics are explained, in that they are the statistical properties of any group for features that can be measured. Then Inferential statistics are presented, again as the concept that allows researchers to make decisions about differences between groups. Correlational statistics are then presented, as they tell us how interactions between the statistical properties of groups develop. Finally, we discuss predictive statistics, as techniques that allow us to decide about a property of a group, knowing one of its other properties.

Another idea behind this meeting is to make students comfortable with the concept of statistics, particularly if this is the first statistics course the students are exposed to.

## Aim/Objectives

The aim of this meeting is to provide the students the method and scope of statistics in research, and to remove any anxiety they may have about taking a statistics course.

## Learning Outcomes

The students will be able to recognize different types of statistical methods, and when these methods should be applied. Further, the students will be exposed to the types of statistical tools that can be used to answer a scientific question. Finally, the students will discuss the concept of validity and how it pertains in scientific experiments.

## Key Words

Descriptive	Inferential	Correlational
Predictive	Statistics	Internal Validity
External Validity		

## Annotated Bibliography

### Basic Material

Edgar, T. W. and Manz, D. O. (2017). Research Methods for Cyber Security. Cambridge, MA: Syngress.

### Supplementary Material

Notes and slides handed out by the instructor of the course

## Self-Assessment Exercises

### Exercise 2.1

In the following scenario, list any factors that might threaten internal and external validity, and suggest possible ways of compensating for shortcomings. Also, if any safeguards are already in place to preserve validity, list them and explain why they are useful.

A study of the emotional effects of abortion on women is being funded and conducted by an organization that actively opposes abortion. Random samples are selected from women who have an abortion performed at a private abortion clinic. Upon coming to the clinic for pre-abortion counseling, each woman's attitude and feelings about having an abortion are assessed by an anonymous questionnaire. The researchers intend to study each woman over a period of five

years using periodic anonymous questionnaires. However, after three years, only 60% of the original study group remain in the study.

### **Recommended time for the student to work**

15 hours

# ORGANIZING AND PRESENTING DATA

3<sup>rd</sup> Week

## Summary

The purpose of this meeting is to examine the various methods of charting and plotting data and employing them in preparing presentations.

## Introductory Remarks

One of the easiest ways to understand data is to see them in a graph or a chart. Looking at data graphically allows us to get a feel for how the data behaves, and to decide on our further analysis. The goal of this meeting is to examine the various methods of charting and plotting data, so that they can be presented to others in an understandable manner.

The students will be exposed to various types of graphs and plots. Starting with simple **pie charts** that present parts of a whole as distinct pieces, we will move into **column charts**, which provide a block in a chart for each piece of data that goes together. We will then move to **line charts** that use a point for each data, and connect the data with a line running through them. We will then examine **boxplots**, which provide more than just the data items, and that also display other statistical information on them.

Using more than one axis, we will move to **scatterplots** that show how two variables interact, and then add more dimensions to the mix, to examine **radar charts**. These charts combine more than two variables and show an overview of a larger amount of dimensions.

## Key Words

Pie charts	Column charts	Line charts
Boxplots	Scatterplots	Radar Charts

## Annotated Bibliography

### Basic Material

Edgar, T. W. and Manz, D. O. (2017). Research Methods for Cyber Security. Cambridge, MA: Syngress.

### Supplementary Material

Notes and slides handed out by the instructor of the course

## Self-Assessment Exercises

### Exercise 3.1

For the following, present the data in the appropriate figure. Explain your choice. Label all axes.

- a. Survey respondents were asked to respond to the statement: "More money should be spent on health care for the elderly." Responses were on a scale of 1 (strongly disagree) to 7 (strongly agree).

Response	f
7	49
6	30
5	23
4	20
3	13
2	9
1	6

- b. Respondents are asked to indicate the type of dwelling in which they live.

Response	f
Single house	87
Duplex	6
Townhouse	9
Apartment	18
Mobile home	6

- c. A small company has each of its employees participate in a 5 km run, and their times are recorded.

Time (min)	cf
32–34	50
29–31	47
26–28	40
23–25	30

20–22	16
17–19	8
14–16	2

### **Recommended time for the student to work**

15 hours

## THE RESEARCH ARTICLE

4<sup>th</sup> Week

### Summary

During this meeting, students will gain an understanding on how to perform a well-defined, systematic literature review; as well as commence drafting their project towards writing their own Literature Review, which will be their semester project.

### Introductory Remarks

In academia, dialogue occurs through the writing up of the researchers' experimental results and their analysis and through their publication in academic journals. For the articles to be published, they have to pass through a process known as **peer-review**, where other experts in the field, read the articles and provide feedback to the authors. Once an article is considered good enough, then it becomes published in the academic journal or conference that the author chose.

While this course will give you the necessary tools to create, perform and analyze your experiments, one of the sections of a research article is the literature review. The literature review is also a chapter or more in a thesis, and it can also be a stand-alone article, that summarizes the advances in a field. During this meeting you will discuss the literature review, and begin your project towards writing your own, which is your project for the semester.

The **Literature Review** is one of the primary ways that one becomes deeply involved with the specific material of his/her scientific question. Thus, understanding how to perform a well-defined, systematic literature review provides the student with a tool that can be not only allows him/her to find **relevant** information, but also allows the student to drop information that may seem interesting but is tangential or irrelevant to the topic of the scientific question.

A literature review is a summary of the publications written on a specific topic. These publications, also called articles, are published through **Academic Publishers**. These are companies that print or post online scientific work that has gone through a **peer-review process**. Peer-review is the process of having multiple experts in the field of the publication read and decide whether it is worthy of publication or if it needs more work to become part of the scientific dialogue on its topic.

When the literature review follows a specific methodology, also called a **Review Protocol**, that tries to encompass the whole of a topic, it becomes a **Systematic Review**. The systematic review is no longer a summary of a topic, but it is focused on a specific question, and reviews all the literature around that specific question, coming to a conclusion about whether a definitive answer exists or not.

In both cases, the most common way of finding scientific articles is through the use of a **Search Engine**, an online machine that only focuses on scientific articles, rather than the whole of the World Wide Web.

## Aim/Objectives

The aim of the meeting is to provide the students of a clear plan of action on how to write a systematic literature review, based on the presentation of existing systematic reviews in the literature.

## Learning Outcomes

The literature review is the required project for this course. During this week and the next, the students will learn how to assemble material according to specific methods. They will then synthesize a coherent piece of work that describes the existing knowledge in the field and that critically examines this knowledge. Through the critical examination, the students will then extract scientific questions that are born through their reviews as conclusions.

A literature review consists of assembling together the relevant existing knowledge about a topic into a coherent story which concludes with the scientific question that will be answered in the final thesis of the student. More specifically, a literature review is used to summarize existing knowledge about a treatment or technology, to identify gaps in the existing knowledge, thus identifying scientific questions that need an answer, and to provide the backdrop upon which an existing research activity takes place.

A systematic review is a thorough and fair review of the existing literature, and not a vague selection of pieces of literature whose only purpose is to guide the reader to believe that the scientific question that is posed is important. As such, the methodology for performing a systematic review is another important piece in the understanding of the research question. It provides strong evidence towards the scientific question, evidence that when treated fairly will withstand the test of peer-review.

Thus, a systematic review requires a plan of action. This plan of action is usually called the Review Protocol, and it is through the careful design of this protocol that the readers will be convinced that the review is a fair treatment of the existing knowledge that is considered within.

During the three hour meeting the students will analyse existing systematic reviews taken from the recent literature, so that they will have tangible examples of the creation of a Review Protocol, and a clear understanding of how a systematic review binds together the research that it cites into a coherent whole that leads to the required result.

As most of the time not one but two or more researchers work towards the completion of a research project, the goal of the literature review is not just to learn how to write one. You will have to work in pairs, so that you can gain experience in writing a significant piece of work within a small team. The literature review is due on Week 12 of the course, and is worth 20% of your total grade.

## Key Words

Literature Review	Systematic Review	Search Engine
Academic Publishers	Peer-Reviewed Publications	Review Protocol

## Annotated Bibliography

### Basic Material

Edgar, T. W. and Manz, D. O. (2017). Research Methods for Cyber Security. Cambridge, MA: Syngress.

### Supplementary Material

Notes and slides handed out by the instructor of the course

### Suggestions for further reading

Murray, R. (2011). How to Write a Thesis (Vol. 3rd ed). Maidenhead: McGraw-Hill Education.

Goshert, J. C. (2011) Entering the Academic Conversation: Strategies for Research Writing. Boston: Longman.

Various Systematic Review articles gathered from the recent literature.

## **Self-Assessment Exercises**

### **Exercise 4.1**

Study the provided systematic reviews and critically assess the Review Protocol, the synthesis of information, and the analysis provided in each. Create a small presentation that will discuss one of the provided reviews to be presented during the next class meeting

### **Exercise 4.2**

Begin gathering literature for preparing your own literature review article.

## **Recommended time for the student to work**

15 hours

## THE RESEARCH ARTICLE - CONTINUED

5<sup>th</sup> Week

### Summary

During this meeting, students will gain an understanding on how to perform a well-defined, systematic literature review; as well as commence drafting their project towards writing their own Literature Review, which will be their semester project.

### Introductory Remarks

During this week the students will present their own assessment of the provided systematic reviews as per the previous week's assignment.

### Aim/Objectives

The goal of this meeting is to allow the students to discuss an existing systematic review, thus through its deconstruction to understand the style, the structure and the flow of the argumentation in such reviews.

### Learning Outcomes

The literature review is the required project for this course. During this week and the next, the students will learn how to assemble material according to specific methods. They will then synthesize a coherent piece of work that describes the existing knowledge in the field and that critically examines this knowledge. Through the critical examination, the students will then extract scientific questions that are born through their reviews as conclusions.

A literature review consists of assembling together the relevant existing knowledge about a topic into a coherent story which concludes with the scientific question that will be answered in the final thesis of the student. More specifically, a literature review is used to summarize existing knowledge about a treatment or technology, to identify gaps in the existing knowledge, thus identifying scientific questions that need an answer, and to provide the backdrop upon which an existing research activity takes place.

A systematic review is a thorough and fair review of the existing literature, and not a vague selection of pieces of literature whose only purpose is to guide the reader to believe that the scientific question that is posed is important. As such, the methodology for performing a systematic review is another important piece in the understanding of the research question. It provides strong evidence towards the scientific question, evidence that when treated fairly will withstand the test of peer-review.

Thus, a systematic review requires a plan of action. This plan of action is usually called the Review Protocol, and it is through the careful design of this protocol that the readers will be convinced that the review is a fair treatment of the existing knowledge that is considered within.

During the three-hour meeting the students will analyse existing systematic reviews taken from the recent literature, so that they will have tangible examples of the creation of a Review Protocol, and a clear understanding of how a systematic review binds together the research that it cites into a coherent whole that leads to the required result.

As most of the time not one but two or more researchers work towards the completion of a research project, the goal of the literature review is not just to learn how to write one. You will have to work in pairs, so that you can gain experience in writing a significant piece of work within a small team. The literature review is due on Week 12 of the course, and is worth 20% of your total grade.

## Key Words

Literature Review	Systematic Review	Search Engine
Academic Publishers	Peer-Reviewed Publications	Review Protocol

## Annotated Bibliography

### Basic Material

Edgar, T. W. and Manz, D. O. (2017). Research Methods for Cyber Security. Cambridge, MA: Syngress.

### Supplementary Material

Notes and slides handed out by the instructor of the course

### Suggestions for further reading

Murray, R. (2011). How to Write a Thesis (Vol. 3rd ed). Maidenhead: McGraw-Hill Education.

Goshert, J. C. (2011) Entering the Academic Conversation: Strategies for Research Writing. Boston: Longman.

Various Systematic Review articles gathered from the recent literature.

### **Activity (5 points)**

You must by now have accumulated a number of scientific articles that pertain to your scientific question. You will have one week to provide the first draft of your systematic review for peer-review and presentation to the group.

### **Recommended time for the student to work**

20 hours

## QUALITATIVE METHODS

6<sup>th</sup> Week

### Summary

Students will come in contact with the various methods of data gathering, such as questionnaires, focus groups and interviews for qualitative assessment.

### Introductory Remarks

Once the student has began their literature review, he/she is ready to move on to learning about the design of the methodology and experiments that need to be performed to gather data to answer the scientific question. The next four weeks are dedicated towards this objective.

Over the course of these four weeks the students will be exposed to two major paradigms of research: Qualitative and Quantitative. **Qualitative Research** is mostly research that aims to explore a topic rather than to provide a specific answer to a specific question. It is usually performed to provide insights into a problem or to help towards creating questions that can then be answered through **Quantitative Research**. Quantitative Research on the other hand, is used when the problem has become structured, and we can assign measures and metrics towards its solution. It is used to quantify statistical variables that can be used to measure specific aspects of the problem to be studied.

Qualitative Research uses various data collection methods, such as **Interviews** and **Focus Groups**. Interviews are one-on-one question and answer sessions, and vary in that if the interviewer does not deviate at all from the questions that must be asked, then we call this the **Fully Structured Interview**. If the interviewer is allowed to deviate from the question structure to explore things that the interviewee mentions and seem interesting, then we have a **Semi-Structured Interview**. Finally, if the interviewer is allowed to completely forget the question structure and ask about anything, then the interview becomes an **Open Interview**. One may create a **focus group** as well, a group of people that are brought together in a room, to provide opinion on a specific product or service.

The discussions in both cases are recorded, and then the researcher **Codifies**, or creates a group of patterns that have been talked about throughout the interview. This allows the researcher to

see the patterns of structures that lead to specific items that can maybe be studied through quantitative research.

## Aim/Objectives

The aim of this week is to introduce students to various methods of data gathering, such as questionnaires, focus groups and interviews for qualitative assessment.

## Learning Outcomes

The students will be exposed to the various methods of data gathering. The students will examine the methodology of building a validated questionnaire and the ways of using existing questionnaires from the literature to gather data.

The students will also be introduced to how a focus group is used to extract data, and how to codify the verbal answers of the group into data that can be analysed using statistical methods.

Finally, the students will examine three types of interviews, fully structured, semi-structured, and open interviews, in order to understand their differences, and how each type of interview may lead to the introduction of scientific questions, or provide data towards the answer of a specific scientific question.

Thus, the focus of the three hour meeting falls on the understanding and examination of qualitative techniques.

## Key Words

Qualitative Research	Focus Group	Interview
Codification	Questionnaire	Fully-structured interview
Semi-structured Interview	Open Interview	

## Annotated Bibliography

### Basic Material

Edgar, T. W. and Manz, D. O. (2017). Research Methods for Cyber Security. Cambridge, MA: Syngress.

## **Supplementary Material**

Notes and slides handed out by the instructor of the course

### **Self-Assessment Exercises**

#### **Exercise 6.1**

- 1) The author viewed himself as a pioneer in the field of qualitative research because
  - A) earlier books focused solely on qualitative methods.
  - B) earlier books focused solely on quantitative methods.
  - C) later books focused on a combination of qualitative and quantitative methods.
  - D) later books imitated his writing style.
- 2) The goal of Berg's book is to
  - A) provide basic training for new researchers.
  - B) create a research "cookbook" for qualitative methods.
  - C) deliver advanced concepts in quantitative research.
  - D) teach readers how to take charge of a research project.
- 3) What type of concept does quantitative research measure?
  - A) Definition
  - B) Characteristic
  - C) Number
  - D) Essence
- 4) What type of concept does qualitative research measure?
  - A) Description
  - B) Measure
  - C) Extent
  - D) Distribution
- 5) The technique of using multiple lines of sight, or an array of symbols and theoretical content to create a better research result, or picture of reality, is called
  - A) triangulation.
  - B) ethnography.
  - C) sociometry.
  - D) quantitative.
- 6) Dr. Kleisch is building a map. She observes the mountainous area from three known points of view. The area where all three lines of sight intersect is called the
  - A) multiple operationalism.
  - B) convergent validation.
  - C) line of action.
  - D) triangle of error.

- 7) Triangulation can be used to describe the use of multiple methods of data collection to measure a single subject. What is it called when multiple data-collection methods, multiple theories, multiple researchers, multiple methodologies, or a combination of these four categories are involved in research activities?
- A) Multiple operationalism
  - B) Convergent validations
  - C) Lines of action
  - D) Triangles of error
- 8) Blumer suggested that through interactions, people derive
- A) knowledge.
  - B) goals.
  - C) meaning.
  - D) opportunities.
- 9) The Chicago school of symbolic interaction proposes that people account for meaning in two ways. Meaning can be intrinsically attached to an object or event. Secondly, people can impose meaning on the object, event, or phenomenon. What is this second way of deriving meaning called?
- A) Empathy
  - B) Psychical accretion
  - C) Definitions of a situation
  - D) Twenty-statement test
- 10) What is a key difference between the Iowa School of Symbolic Interactionism and the Chicago School of Symbolic Interaction?
- A) Iowa uses a twenty-statement test, while Chicago uses participant observation.
  - B) Iowa uses interviews, while Chicago uses a twenty-statement test.
  - C) Iowa uses historic documents, while Chicago uses interviews.
  - D) Iowa uses participant observation, while Chicago uses historic documents.

### Recommended time for the student to work

15 hours

## QUANTITATIVE METHODS

7<sup>th</sup> Week

### Summary

Students will become familiar with the concept of statistical analysis; whereas they will be provided with the required knowledge to design their own experiments and carry out their own statistical analysis, using appropriate statistics techniques and methods

### Introductory Remarks

Quantitative methods differ from qualitative ones. Whereas in qualitative research one is looking at data that cannot be put into numbers, such as bodies of text and answers to questions, quantitative methods seek to find relationships between numerical data. As such, questionnaires that ask questions that can be answered through the ascription of a number to a particular concept, are treated as a quantitative method.

Quantitative methods require some understanding of probabilities and statistics. Over the course of the next few meetings, our aim will be to become familiar with this type of analysis. Students will be provided with the required knowledge to design their own experiments and to carry out their own statistical analysis using appropriate statistics techniques and methods.

The students will begin by looking at various types of **Experimental Designs**, in other words, how to setup two or more groups of participants so that they can compare different types of effects on each group. The students will see types of **Factorial Designs**, an experimental design that compares many different groups that each may have more than one effect placed upon them by the experiment.

The experimental designs should be valid. **Validity** is the manner in which the different effects on each group of participants interacts with other effects. On the other hand, **Reliability** expresses the random error that can occur when choosing a set of participants, or any other error that can happen during the process of an experiment. To reduce random error, we do not assign participants to each experimental group specifically. Rather, we use a random process to place them in groups, called **Random Assignment**.

Finally, students need to understand the necessary ingredients for **Causation**, which is the expressed reliance of one experimental effect on another. In statistics, it is generally difficult to show causation, so instead we show **Correlation**. Correlation is a measure that shows that if one experimental effect varies, then another experimental effect varies together with the first one.

## Aim/Objectives

The aim of this meeting is for students to dissect the concept of an experiment, and toy with the idea of NxN experimental design.

## Learning Outcomes

Having completed this three hour meeting, the student will be able to differentiate experimental and nonexperimental designs. The student will also be able to critically assess a scientific question that requires quantitative evaluation, and provide a preliminary experimental design which should uphold structure, content, construct, and internal validity. The student should also be able to describe the factors needed to assess causation between variables, and perform and explain the process and goals of random assignment in scientific experimentation.

## Key Words

Experimental Design	Factorial Design	Validity
Correlation	Causation	Reliability
Random Assignment		

## Annotated Bibliography

### Basic Material

Edgar, T. W. and Manz, D. O. (2017). Research Methods for Cyber Security. Cambridge, MA: Syngress.

### Supplementary Material

Notes and slides handed out by the instructor of the course.

## **Self-Assessment Exercises**

### **Exercise 7.1**

1. In Tamotsu's sock drawer, there are seven pairs of black socks, three pairs of white socks, two pairs of navy socks, and one pair of pea green socks. (Each pair has been rolled up.)
  - a. If he hurriedly picks a pair of socks, what is the probability that he would randomly select a pair of navy socks?
  - b. If one pair of white socks and two pairs of black socks are being washed, what is the probability that Tamotsu would randomly select the pair of pea green socks?
  - c. When Tamotsu goes away on a trip, he always takes two pairs of socks in his suitcase. If he selects the two pairs randomly, how many different combinations of socks are possible?
2. Market researchers determined that at a particular store in a mall, there is a 50% chance that women passing by will enter the store and a 50% chance they will continue on without entering the store. If E indicates that a woman enters the store and W that she walked by, what is the probability that the following sequence will occur?

E, W, W, W, E, E, E, E, W, W, E

3. A child-care centre has eight different colors of building blocks. How many different combinations of three can a child make?

### **Recommended time for the student to work**

15 hours

# DESCRIPTIVE STATISTICS

8<sup>th</sup> Week

## Summary

During this meeting, students will be introduced to the concepts of descriptive statistics.

## Introductory Remarks

Descriptive statistics are the basic elements upon which one builds an understanding of how any data behaves. It is imperative that the student understands descriptive statistics before moving on to the next meetings, because of the fundamental nature of the presented material.

There are several terms that need to be understood and put to use, in order for the student to receive experience in what each term measures and in which cases each term applies. For this reason, the terms are not explained in the introductory remarks, but rather they are left as an exercise to the reader to do a brief search and find the meaning and use of each. All the terms that are shown in the next section will be discussed during the three-hour meeting, but the students are expected to have done some work on the definition of each term prior to the actual meeting.

## Aim/Objectives

The aim of the meeting is for the students to grasp the concepts of descriptive statistics. As such, the objectives are the following:

1. Explain how to calculate, and explain what each of the following are:
  - a. Measures of central tendency
    - i. Mode
    - ii. Mean
    - iii. Median
  - b. Measures of Range
    - i. Interquartile Range
    - ii. Standard Deviation
    - iii. Range

- iv. Variance
- c. Other measures
  - i. Skewness
  - ii. Kurtosis
- 2. Design the following graphs and plots given data:
  - a. Stem-and-leaf plots
  - b. Box plots
  - c. Time plots
  - d. Scatter diagrams
- 3. Explain how these pertain to the overall understanding of the nature of the data one gathers.

## Learning Outcomes

During the meeting, the students will be introduced to the concepts of descriptive statistics. While these concepts may be basic, they are fundamental to the understanding of more advanced concepts in the analysis of gathered data. For this reason, the students need to perform several exercises that involve the calculation of each of the items mentioned in the “Aims and Objectives” section of this meeting, more preferentially in class.

The students should become familiar with tables and graphs, because these are used to easily summarize gathered data, both for quantitative and qualitative research purposes. The students must be able to create and interpret descriptive statistics along with related graphs and plots that have been seen earlier in the semester. They should be able to distinguish between the differences of different types of distributions, and to recognize these distributions, by looking at the measures of central tendency and through utilizing the measures of range.

Finally, the students are expected to define and explain relationships present in data sets, particularly through the creation and critical assessment of the scatterplot.

## Key Words

Central Tendency	Mode	Mean
Median	Range	Interquartile Range
Standard Deviation	Variance	Skewness
Measures	Kurtosis	Stem-and-leaf plots
Time plots	Scatter diagrams	

## Annotated Bibliography

### Basic Material

Edgar, T. W. and Manz, D. O. (2017). Research Methods for Cyber Security. Cambridge, MA: Syngress.

### Supplementary Material

Notes and slides handed out by the instructor of the course

## Self-Assessment Exercises

### Exercise 8.1

1. In a statistics class, a survey was taken to determine the drinking behavior of students over the course of the previous week. Students were asked to indicate the number of drinks they had consumed over the past week. Results were as follows:

Number of Drinks	<i>f</i>
0	18
1	32
2	6
3	3
4	5

- a. Construct a bar graph for the data given. Use absolute frequency.
  - b. Calculate the mean, median, and mode for the data.
2. In a recent Alberta Survey, respondents were asked what the ideal age was for a woman to have her last child. Responses were as follows:

Age interval	<i>f</i>
45–49	7
40–44	79
35–39	114
30–34	100
25–29	30
20–24	70

- a. Calculate the mean, median, and mode
- b. What is the direction of the skew?
- 3. A new weight-loss drug is being tested on two groups of men: one control group (group A), who takes a placebo, and one test group (group B), who takes the drug. Both groups are following the same diet and exercise plan. Results are tabulated separately for each group. At the end of the trial period, the men in group A lost an average of 8.6 kg, and the men in group B lost an average of 9.3 kg. What is the average weight loss for the entire group? (**Note:** Although both groups originally contained 25 participants, by the end of the trial, group A had 23 participants and group B had 17 participants.)

## Individual Assignment (20 points)

The subject of the individual assignment will be announced at a later stage.

## Recommended time for the student to work

35 hours

# PROBABILITY AND DISTRIBUTIONS

9<sup>th</sup> Week

## Summary

Students will study and grasp the concepts of probability, in describing various types of experiments.

## Introductory Remarks

Descriptive statistics are the basic elements upon which one builds an understanding of how any data behaves. It is imperative that the student understands descriptive statistics before moving on to the next meetings, because of the fundamental nature of the presented material.

There are several terms that need to be understood and put to use, in order for the student to receive experience in what each term measures and in which cases each term applies. For this reason, the terms are not explained in the introductory remarks, but rather they are left as an exercise to the reader to do a brief search and find the meaning and use of each. All the terms that are shown in the next section will be discussed during the three-hour meeting, but the students are expected to have done some work on the definition of each term prior to the actual meeting.

## Aim/Objectives

After the students have been exposed to descriptive statistics, they must now understand and learn to use the tools of statistical inference. As such, students will study the concepts of probability and how these can be used to describe various types of experiments. They must also grasp and apply the concept of probability distribution. Finally, the students will be exposed to the concept of a sampling distribution, and how that pertains to the actual population distribution. Thus, the students will also be presented the concept of random sampling.

## Learning Outcomes

By the end of the three-hour meeting the students should have a firm grasp and be able to use the fundamental laws of probability. The students should also work with the normal distribution, and critically assess how this distribution presents a host of assumptions in statistics, and also

realize that normal distributions cannot be achieved through a sample of the population. In turn, they need to be exposed to the fact that sampling distributions can come close to the actual population distribution. They also need to recognize that even through random sampling, there may be samples that do not correctly represent the actual population.

Students should perform exercises that provide them with examples that show both correct and incorrect methods of sampling, and examine the concept of sampling bias. Finally, the students should become comfortable with the reality of statistical error, both Type-I and Type-II.

## Key Words

Distribution	Laws of Probability	Sampling
Statistical Error	Type-I	Type-II
Normal Distribution	Sample Distribution	

## Annotated Bibliography

### Basic Material

Edgar, T. W. and Manz, D. O. (2017). Research Methods for Cyber Security. Cambridge, MA: Syngress.

### Supplementary Material

Notes and slides handed out by the instructor of the course

## Self-Assessment Exercises

### Exercise 9.1

1. In a science experiment a mouse must find its way through a maze. There are 24 different routes but 18 of these routes lead to dead ends. What is the probability that a mouse will successfully find its way through the maze three out of the 10 times it runs the maze, assuming that the mouse remembers nothing about the maze after each run?
2. In a bouquet of one dozen roses, two are pink, two are white, three are yellow, and five are orange.
  - a. If you close your eyes and pick one rose, what is the probability that it is pink? That it is yellow?

- b. If you pick out one rose and then pick another one without replacement, what is the probability of picking a white rose followed by an orange rose? An orange rose followed by a yellow rose?
- c. How many permutations are possible if you pick out smaller bouquets of three from the large bouquet?
- d. What is the probability of picking an orange, then a white, then a yellow, then another orange rose from the bouquet, without replacement?

### **Exercise 9.2**

1. A survey of auto mechanics in Detroit reveals that, at any given time, 40% of all cars brought in for repairs have problems with the fuel system.
  - a. If you were to select many random samples of 70 cars each, how often would you expect that 25 cars or fewer have problems with the fuel system?
  - b. Selecting many random samples of 100 cars, how often would you expect between 35 and 55 cars to be in for repairs to the fuel system?
2. When selecting random samples of 50 from a population with a mean of 125 and a standard deviation of 8, beyond what two values would the extreme 10% of mean differences fall?
3. When selecting random samples of 15 from the population in exercise 2 with a mean of 125 and a standard deviation of 8, how often would you expect to get means between 122 and 128?

### **Recommended time for the student to work**

15 hours

## HYPOTHESIS TESTING

10<sup>th</sup> Week

### Summary

Students will study in depth how the scientific method works when the results of an experiment are analyzed.

### Introductory Remarks

The three-hour meeting on probability and distributions aims to bring the student closer to understanding how the scientific method works when the results of an experiment are analyzed. The student will become familiar with the concept of **Statistical Error**, and understand why and when statistical error is acceptable. Statistical Error is the unknown difference between what we measure and what is really true. In other words, it is the difference between the population measurement and the sample measurement.

As such, students need to understand **Probability and its Laws**, and understand the different ways that a **Random Sample** can be created, so that we can rely on statistics to tell us that our results do make sense. During the meeting, two types of error will be considered: **Type I** and **Type II**. Type I error occurs when we declare that we have a difference between two samples, when in fact we do not (false positive). On the other hand, Type II error occurs when we have enough evidence to show difference between two samples, and instead we declare that there is no difference (false negative).

While we live in a world where we are used to taking for granted anything that science says is true, we forget that scientific truth only works up to a point, and with specific assumptions and caveats. This is the take-away point of this meeting, but to be clearly elucidated, the point should be presented through an understanding of statistics and different types of distributions.

With this in mind, we will also examine the **Normal Distribution**, a function that represents the distribution of many random variables as a symmetrical bell-shaped graph. The normal distribution is a very useful and versatile tool in the world of statistics, and we will examine how we can use this tool towards analyzing our experiments.

## Aim/Objectives

After the students have been exposed to descriptive statistics, they must now understand and learn to use the tools of statistical inference. As such, students will study the concepts of probability and how these can be used to describe various types of experiments. They must also grasp and apply the concept of probability distribution. Finally, the students will be exposed to the concept of a sampling distribution, and how that pertains to the actual population distribution. Thus, the students will also be presented the concept of random sampling.

## Learning Outcomes

By the end of the three-hour meeting the students should have a firm grasp and be able to use the fundamental laws of probability. The students should also work with the normal distribution, and critically assess how this distribution presents a host of assumptions in statistics, and also realize that normal distributions cannot be achieved through a sample of the population. In turn, they need to be exposed to the fact that sampling distributions can come close to the actual population distribution. They also need to recognize that even through random sampling, there may be samples that do not correctly represent the actual population.

Students should perform exercises that provide them with examples that show both correct and incorrect methods of sampling, and examine the concept of sampling bias. Finally, the students should become comfortable with the reality of statistical error, both Type-I and Type-II.

## Key Words

Distribution	Laws of Probability	Sampling
Statistical Error	Type-I	Type-II
Normal Distribution	Sample Distribution	

## Annotated Bibliography

### Basic Material

Edgar, T. W. and Manz, D. O. (2017). Research Methods for Cyber Security. Cambridge, MA: Syngress.

### Supplementary Material

Notes and slides handed out by the instructor of the course

## Activity (5 points)

### Exercise 10.1

1. In a science experiment a mouse must find its way through a maze. There are 24 different routes but 18 of these routes lead to dead ends. What is the probability that a mouse will successfully find its way through the maze three out of the 10 times it runs the maze, assuming that the mouse remembers nothing about the maze after each run?
2. In a bouquet of one dozen roses, two are pink, two are white, three are yellow, and five are orange.
  - a. If you close your eyes and pick one rose, what is the probability that it is pink? That it is yellow?
  - b. If you pick out one rose and then pick another one without replacement, what is the probability of picking a white rose followed by an orange rose? An orange rose followed by a yellow rose?
  - c. How many permutations are possible if you pick out smaller bouquets of three from the large bouquet?
  - d. What is the probability of picking an orange, then a white, then a yellow, then another orange rose from the bouquet, without replacement?

### Exercise 10.2

1. A survey of auto mechanics in Detroit reveals that, at any given time, 40% of all cars brought in for repairs have problems with the fuel system.
  - a. If you were to select many random samples of 70 cars each, how often would you expect that 25 cars or fewer have problems with the fuel system?
  - b. Selecting many random samples of 100 cars, how often would you expect between 35 and 55 cars to be in for repairs to the fuel system?
2. When selecting random samples of 50 from a population with a mean of 125 and a standard deviation of 8, beyond what two values would the extreme 10% of mean differences fall?
3. When selecting random samples of 15 from the population in exercise 2 with a mean of 125 and a standard deviation of 8, how often would you expect to get means between 122 and 128?

## Recommended time for the student to work

20 hours

## REGRESSION AND CORRELATION

11<sup>th</sup> Week

### Summary

Students will study the interactions that occur only between two variables, see the tools (regression and correlation analysis) and examine the various types of dependence, or interaction, that two variables may have.

### Introductory Remarks

Sometimes the scientific question of an experiment is not to examine whether something applies or not, but to see whether two variables have interaction. Usually this is to examine whether the value of one variable affects the value of another variable, and also, to examine how one value affects the other. This interaction is measured by a method and a statistic called **Correlation** and **Correlation Coefficient** respectively. Given that we have enough data, we can not only calculate the correlation between two interacting variables, but we can also build a statistical **Model**, an equation that shows us how to calculate one value from the other. This is called a **Regression** model.

There are two types of correlation: Pearson and Spearman. We use Pearson correlation only when our data conforms to the normal curve. If they do not, then we use Spearman's coefficient.

### Aim/Objectives

The aim of the meeting is to provide tools that the students can use to examine the interaction between two variables. These tools are called regression and correlation analysis. The students will see the tools and examine the various types of dependence, or interaction, that two variables may have. The scope of this meeting is only to present interactions that occur only between two variables, the independent and the dependent one.

### Learning Outcomes

During the meeting the students will work with Microsoft Excel using guided examples that the instructor will provide. These guided examples will exemplify how regression and correlation analysis are done in a widespread tool.

The students will examine cases where regression analysis is appropriate, and what correlation means. The students will also be given problems to critically assess the strength and direction of correlation between two variables.

The students will then be exposed to the quantification of a model that expresses the relationship between two variables, namely they will solve guided problems that involve the creation of regression equations.

Finally, the students will be exposed to the concept of causation, and how causation can be found through experimentation.

## Key Words

Regression	Correlation	Model
Variables	Causation	Pearson
Spearman		

## Annotated Bibliography

### Basic Material

Howard, K. & Sharp, J.A., The Management Of A Student Research Project, Gower

King, R. S., Research Methods For Information Systems, Dulles: Mercury Learning.

### Supplementary Material

Notes and slides handed out by the instructor of the course

### Suggestions for further reading

Murray, R. (2011). How to Write a Thesis (Vol. 3rd ed). Maidenhead: McGraw-Hill Education.

Goshert, J. C. (2011) Entering the Academic Conversation: Strategies for Research Writing. Boston: Longman.

## Self-Assessment Exercises

### Exercise 11.1

- The Students' Association at a university is interested in determining whether government-funding cuts to the university have affected the number of new research grants obtained by faculty members from outside sources. The Students' Association collected data on the number of research grants awarded to faculty. They gathered data for the past eight years and want to determine the correlation between level of government funding and new research grants acquired by faculty at the university. Do the appropriate analysis to answer the question. How much of variance is accounted for by the correlation?

Funding (\$)	New grants
10000	9
12000	11
9000	11
7000	6
8000	6
7500	5
7500	8
7500	6

- A teacher is interested in determining if there is a relationship between the organizational skills of her 20 students and their mathematical ability. She ranks the students on a scale of 1 to 10 according to their organizational skills and uses their final exam grades to rank their mathematical ability. She finds the correlation between the two ranks to be 0.86. At  $\alpha = .01$ , use a two-tailed alternative to test the hypothesis that there is no correlation between organizational and mathematical ability. Which correlation test did the teacher use? What is your statistical decision? What is your conclusion?

### Exercise 11.2

- The correlation between the scores on Dr. Evans' literacy test and final grade performance is 0.78. How much of the variability in final grade can Dr. Evans claim is associated with differences in ability as assessed by her literacy test?
- The correlation between graduating average and IQ is 0.72. The correlation between graduating average and time spent studying is 0.87. The correlation between IQ and time spent studying is 0.65. What is the correlation between graduating average and IQ if the time spent studying variable is removed?

### Recommended time for the student to work

15 hours

## REVIEW

12<sup>th</sup> Week

### Introductory Remarks

During this meeting you are encouraged to discuss with the instructor about any and all questions you may have prior to the final, and prior to the presentation that will be performed during the next, the final meeting.

### Aim/Objectives

Answer any and all questions students may have about the material in the course.

### Learning Outcomes

Discuss and learn from peers and the instructor, and elucidate any and all concepts and techniques taught in the body of this course.

### Annotated Bibliography

#### Basic Material

Edgar, T. W. and Manz, D. O. (2017). Research Methods for Cyber Security. Cambridge, MA: Syngress.

#### Supplementary Material

Notes and slides handed out by the instructor of the course

### Recommended time for the student to work

15 hours

# PRESENTATION

13<sup>th</sup> Week

## Introductory Remarks

The final meeting's objective is for each group of students to present their scientific findings after they have performed their systematic review of the literature. The students will present as if they are presenting their work at a scientific convention, and receive questions about their work.

## Aim/Objectives

Go through the process of presenting scientific work and defending it in front of a group of their peers.

## Learning Outcomes

Peer-review and feedback

## Annotated Bibliography

### Basic Material

Edgar, T. W. and Manz, D. O. (2017). Research Methods for Cyber Security. Cambridge, MA: Syngress.

### Supplementary Material

Notes and slides handed out by the instructor of the course

## Group Assignment (20 points)

Peer review: Provide feedback to your fellow students about their presentation. This feedback should always be constructive and not demeaning or insulting. Try to help your fellow students towards materializing their best work.

## Recommended time for the student to work

35 hours

## **REVISION AND FINAL EXAMINATION**

The final examination will consist of true/false, multiple-choice questions and a small number of questions.

### **Recommended time for the student to work**

40 hours

**Date/Time of Final Exam: TBD**

## INDICATIVE ANSWERS TO SELF-ASSESSMENT EXERCISES

### WHAT IS RESEARCH – WEEK 1

#### Exercise 1.1

- a) An evaluation research design should be used to evaluate this new social program
- b) A cross-cultural design is appropriate for this research topic.
- c) The physician should conduct a case study of this individual.
- d) This problem is suitable for an experimental approach.
- e) The physician's questions might best be answered with a correlational analysis relating body weight to blood pressure.

### THE LANGUAGE OF STATISTICS – WEEK 2

#### Exercise 2.1

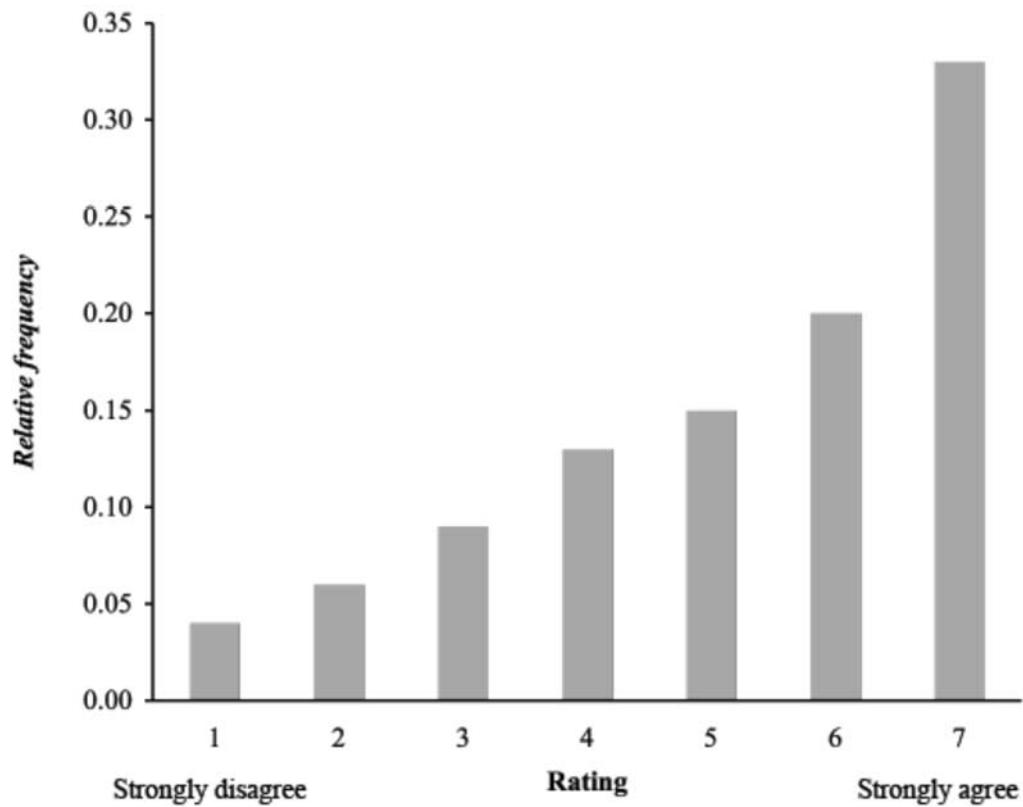
Sampling bias may compromise external validity: Women who go to a private abortion clinic may be different from all women who have abortions. Internal validity may also be compromised. Investigator bias is a potential problem because the funding agency is not impartial. Attrition is a problem with this study as demonstrated by the number of participants remaining after three years. Repeated testing might also threaten internal validity. Safeguards include a pre-study history as a control and random sampling.

### ORGANIZING AND PRESENTING DATA – WEEK 3

#### Exercise 3.1

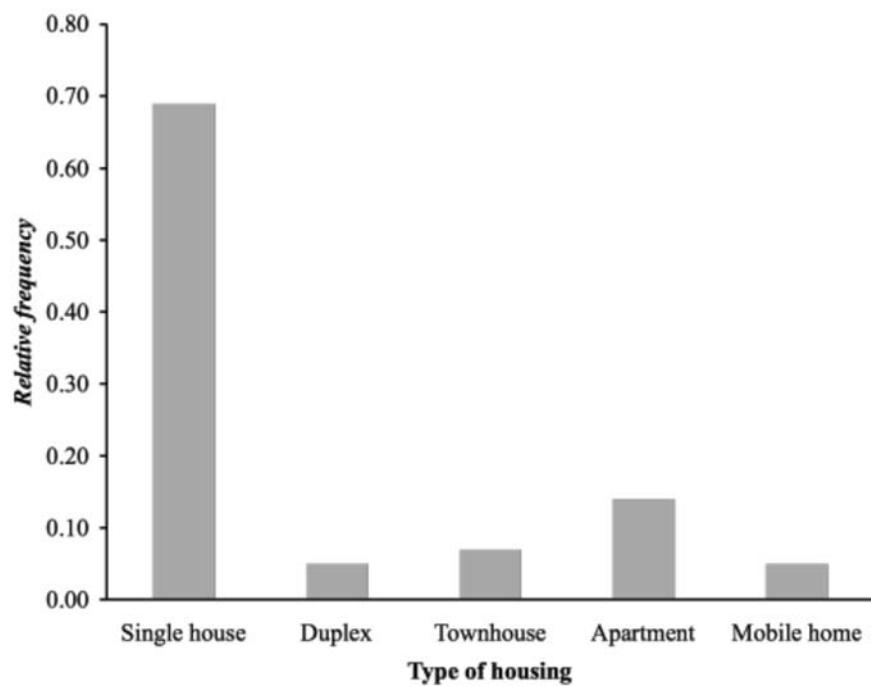
a.

Response	f	rf
7	49	0.33
6	30	0.20
5	23	0.15
4	20	0.13
3	13	0.09
2	9	0.06
1	6	0.04
<b>Sum</b>	<b>150</b>	<b>1</b>

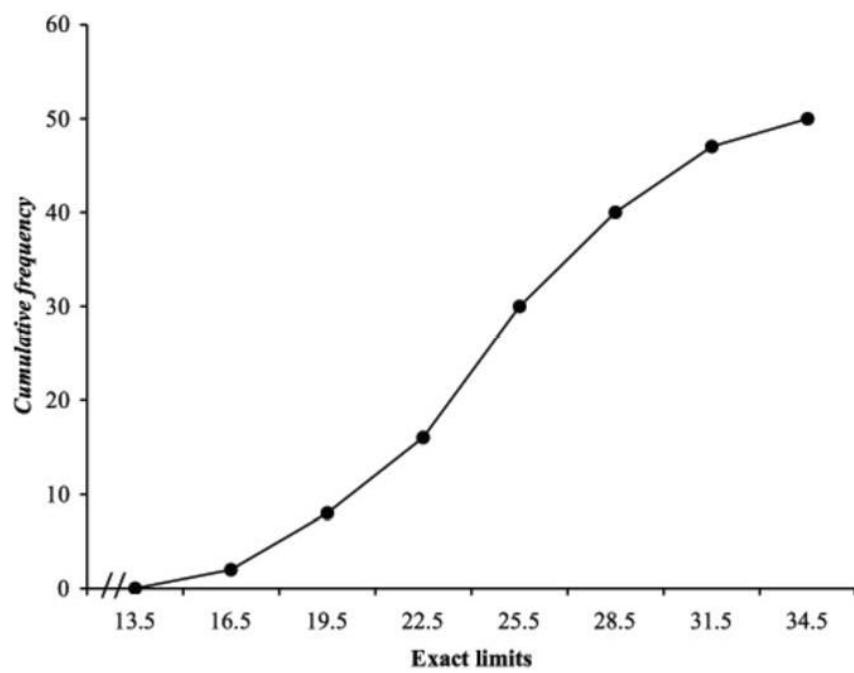


b.

Response	<i>rf</i>
Single house	0.69
Duplex	0.05
Townhouse	0.07
Apartment	0.14
Mobile home	0.05



c.



## THE RESEARCH ARTICLE – WEEK 4 &

## THE RESEARCH ARTICLE CONTINUED – WEEK 5

### Exercises and Activities 4.1 – 5.1

These exercises and activities are focused on the work that the students must perform to understand their research project, and as such, there are no model answers. In fact, only through discussion will the students begin to grasp the method of performing scientific research. Thus, the exercises and activities are geared towards moving the students to the direction of completing their literature review project, which is work that should be guided, but where model answers cannot be provided.

## QUALITATIVE METHODS – WEEK 6

### Exercise 6.1

1. B
2. A
3. C
4. A
5. A
6. D
7. C
8. C
9. B
10. A

## QUANTITATIVE METHODS – WEEK 7

### Exercise 7.1

1.
  - a.  $p(\text{navy}) = 2/13 = 0.154$
  - b.  $p(\text{green}) = 1/10 = 0.10$
  - c.  ${}_{13}C_2 = 78$

$$2. {}_{12}C_7 p^7 q^5 = \frac{12!}{(12-7)!7!} \left(\frac{1}{2}\right)^7 \left(\frac{1}{2}\right)^5 = 0.19$$

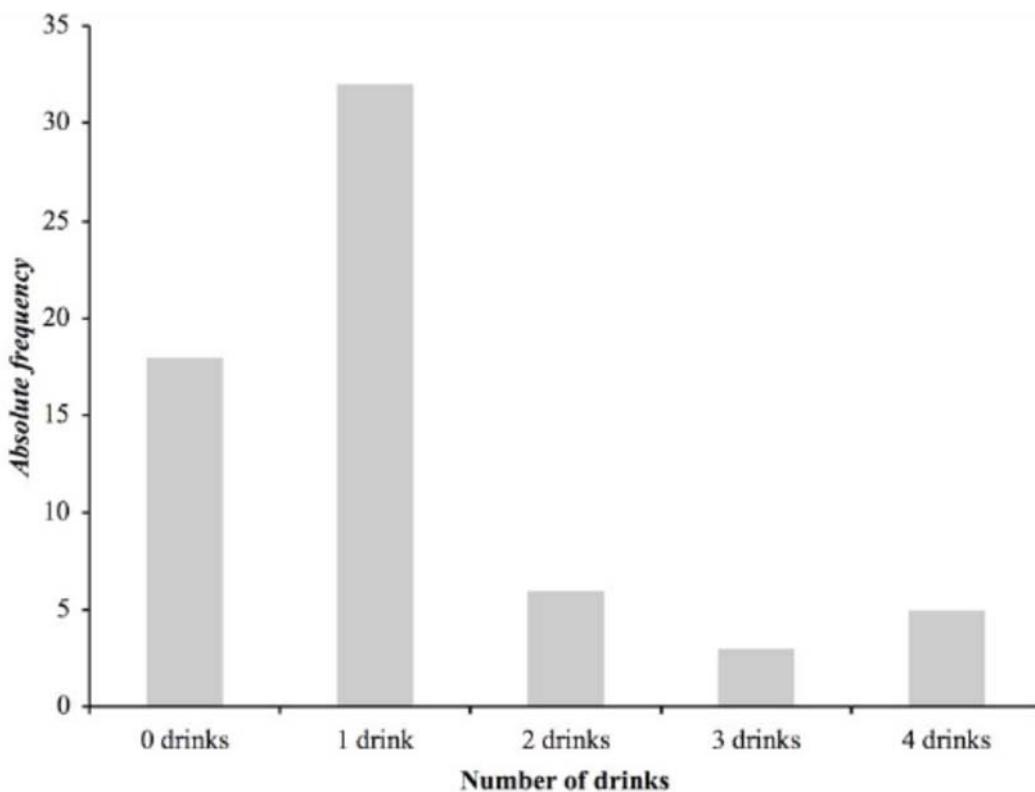
$$3. {}_8C_3 = 56$$

## DESCRIPTIVE STATISTICS – WEEK 8

### Exercise 8.1

1.

a.



b.

Number of Drinks	<i>f</i>	<i>fX</i>
0	18	0
1	32	32
2	6	12
3	3	9
4	5	20
<b>Sum</b>	<b>64</b>	<b>73</b>

$$\mu = \frac{\sum fX}{N} = \frac{73}{64} = 1.14$$

$$\text{Median} = 0.5 + 14/32 = 0.9375$$

Mode = 1

**2.**

**a.**

Age	f	MP ( $X$ )	$fX$
45–49	7	47	329
40–44	79	42	3318
35–39	114	37	4218
30–34	100	32	3200
25–29	30	27	810
20–24	70	22	1540
<b>Sum</b>	<b>400</b>		<b>13415</b>

Mean            33.54

$Mdn$             34.5

$Mo$             37

**b.** Negative skew.

**3.** Mean of combined subgroups.

Group A mean weight loss = 8.6 kg  $N = 23$

Group B mean weight loss = 9.3 kg  $N = 17$

$$\mu_c = \frac{N_A \mu_A + N_B \mu_B}{N_A + N_B} = \frac{23(8.6) + 17(9.3)}{23 + 17} = 8.89$$

## PROBABILITY AND DISTRIBUTIONS – WEEK 9

### Exercise 9.1

$$1. {}_{10}C_3 p^q = \frac{10!}{(10-3)!3!} \left(\frac{1}{4}\right)^3 \left(\frac{3}{4}\right)^7 = 0.25$$

**2.**

**a.**  $p$  (pink) = 2/12 = 0.17  $p$  (yellow) = 3/12 = 0.25

**b.**  $p$  (white and orange) = 2/12 • 5/11 = 0.076

$p$  (orange and white) = 5/12 • 2/11 = 0.075

**c.**  ${}_{12}P_3 = 1320$

**d.**  $p = 5/12 • 2/11 • 3/10 • 4/9 = 0.010$

**3.**

**a.**  $p$  (navy) = 2/13 = 0.154

**b.**  $p(\text{green}) = 1/10 = 0.10$

c.  ${}_{13}C_2 = 78$

### Exercise 9.2

1.

a.  $z = \frac{p - P}{\sqrt{PQ/n}} = \frac{0.357 - 0.40}{\sqrt{(0.40)(0.60)/7}} = -0.734$

About 23% of the time.

b.  $z(35) = -1.02$   $z(55) = 3.06$

Area between  $z$  of 35 and mean = .3461 Area between  $z$  of 55 and mean = .4989

About 85% of the time.

2. Mean differences =  $\pm 1.654$  (1.6) =  $\pm 2.64$

3.  $z = \pm 1.02$  About 69% of the time.

## HYPOTHESIS TESTING – WEEK 10

### Exercise 10.1

1. Directional alternative      Mean difference =  $63 - 59 = 4$

Standard error = 1

$z = 4$  Reject.

The citizens of City A pollute significantly more than the citizens of City B.

2. Non-directional alternative      Sample proportion = 0.286

Standard error = 0.0205

$z = -0.683$  Fail to reject.

There is no evidence that the science students differ from the general population.

### Exercise 10.2

1. Two-tailed  $t$ -test for the difference between independent means

	Group 1	Group 2
$M$	37.5	33
$SS$	1645	2025
$n$	12	15
$df$	25	
$SE$	4.69	
$t$	0.96	Fail to reject

There is no significant difference between the groups.

## 2. One-tailed *t*-test for a single mean

<i>M</i>	1.63
$\mu$	2.14
Numerator	-0.51
<i>SE</i>	0.146
<i>t</i>	-3.5
<i>s</i>	1.02
<i>n</i>	49

Reject the null. Participation has significantly decreased since 2010.

### Exercise 10.3

#### 1. One-way ANOVA: Excel output

Anova: Single Factor SUMMARY

<b>Groups</b>	<b>Count</b>	<b>Sum</b>	<b>Average</b>	<b>Variance</b>
A1	20	1849	92.45	89.734
A2	20	1678	83.90	239.568
A3	20	1611	80.55	297.629

### ANOVA

<b>Source of Variation</b>	<b>SS</b>	<b>df</b>	<b>MS</b>	<b>F</b>	<b>P-value</b>	<b>F<sub>crit</sub></b>
Between Groups	1506.233	2	753.117	3.604	0.034	3.159
Within Groups	11911.700	57	208.977			
Total	13417.933	59				

Reject the null. At least two means were significantly different.

## REGRESSION AND CORRELATION – WEEK 11

### Exercise 11.1

1. Pearson's  $\rho = 0.80 \rho^2 = 0.64$
2. Spearman rank-order correlation test.

$$\text{rho.01} = 0.57$$

$$\text{rhoobt} = 0.86$$

Reject the null. There is a significant correlation between the ranks.

### Exercise 11.2

3. About 61% of the variance is explained by the correlation.

$$4. R_P = \frac{0.72 - (0.87)(0.65)}{\sqrt{1-0.82^2}(1-0.65^2)} = 0.41$$



**FORM: 200.1.3**

**SAMPLE**  
**STUDY GUIDE**

**Course: CYS622 - Special Cybersecurity Topics**

## Course Information

<b>Institution</b>	European University Cyprus		
<b>Programme of Study</b>	Cybersecurity (MSc)		
<b>Course unit</b>	CYS622	Special Cybersecurity Topics	
<b>Level</b>	<i>Undergraduate</i>	<i>Postgraduate</i>	
		<i>Master</i>	<i>PhD</i>
		√	
<b>Language of Instruction</b>	English		
<b>Teaching Methodology</b>	Distance Learning		
<b>Course Type</b>	<i>Compulsory</i>	<i>Optional</i>	
		√	
<b>Number of Group Consultation Meetings/Web-Conferences/ Lectures</b>	<i>Total</i>	<i>Face to Face</i>	<i>Web-Conferences</i>
	14	1	13
<b>Number of Activities/ Assignments</b>	4		
<b>Final Assessment</b>	<i>Assignments</i>	<i>Final Examinations</i>	
	50 %	50 %	
<b>Number of Credits (ECTS)</b>	10		

<b>Study Guide drafted by</b>	Dr Philippos Isaia
<b>Editing and final approval of Study Guide by</b>	Dr Yianna Danidou

## COURSE CONTENTS

		Page
	Introductory Notes	4
	First Group Consultation Meeting	6
1	Introduction ( <a href="#">1<sup>st</sup> Week</a> )	8
2	Major Cyber Attacks / Incidents in Recent Years ( <a href="#">2<sup>nd</sup> Week</a> )	13
3	What to Expect in Cybersecurity Threats ( <a href="#">3<sup>rd</sup> Week</a> )	18
4	European Union Cybersecurity Strategy ( <a href="#">4<sup>th</sup> Week</a> )	24
5	European Union Cybersecurity Act ( <a href="#">5<sup>th</sup> Week</a> )	29
6	Cybersecurity Around the World – Part 1 ( <a href="#">6<sup>th</sup> Week</a> )	34
7	Cybersecurity Around the World – Part 2 ( <a href="#">7<sup>th</sup> Week</a> )	39
8	Cybersecurity and Emerging Technologies ( <a href="#">8<sup>th</sup> Week</a> )	44
9	Cybersecurity as an Engine for Growth ( <a href="#">9<sup>th</sup> Week</a> )	49
10	Future Research Direction in Cybersecurity ( <a href="#">10<sup>th</sup> Week</a> )	54
11	Safer Internet ( <a href="#">11<sup>th</sup> Week</a> )	61
12	Cyber Security Case Studies ( <a href="#">12<sup>th</sup> Week</a> )	65
13	Professional Certifications ( <a href="#">13<sup>th</sup> Week</a> )	70
14	Revision and Final Examination	76
	Indicative answers to Self-Assessment exercises	77

## INTRODUCTORY NOTES

The present Study Guide for **Special Cybersecurity Topics** is a result of collective effort and cooperation of the members of Adjunct Faculty (AF) for this course. Every year this study guide is reviewed and updated based on the changes of the educational material posted on the platform. The Special Cybersecurity Topics course is a first semester **compulsory** course. The course scope is to introduce fundamental concepts of cryptography and its uses in cyber and information security. Beyond the basic uses for keeping information secret and the different methods available, additional forms such as hashes, digital signatures, non-repudiation and steganography are introduced.

Upon successful completion of this course, students should be able to:

- Identify and define the current events in cybersecurity
- Describe the various statistics available on cybersecurity and successful attacks around the world
- Explain recent developments in national, European and international cybersecurity laws and policies
- Define and describe recent developments in the European area and the impact that these may have on the way cybersecurity operations are conducted
- Define and describe the different parts of national and European cybersecurity strategy and how they lead to a holistic approach to the response to cybersecurity threats
- Identify and describe recent developments in the privacy area, and how it is related to and can be protected by proactive cybersecurity operations
- Identify and describe emerging technologies in the cybersecurity field and their applications
- Understand the principles of Safer Internet awareness and how cyber awareness becomes a critical factor of vulnerability for cybersecurity on individual or organizational level.
- Define and describe the various professional certifications that are available in the area of cybersecurity and network and information security, and how they are

applicable to different parts of a comprehensive cybersecurity architecture and related operations. This Study Guide is a necessary and useful tool for the students, especially in the cases that the educational material is not written with open and distance learning methodology. It encourages and facilitates the study and understanding of the issues addressed by the Course.

In addition, through the self-assessment exercises, it stimulates and encourages work at home, providing incentives for further study and contributes to the development of critical thinking.

The Study Guide is structured in a weekly basis and includes summary and brief introductory remarks, purpose and expected outcomes, keywords - basic concepts, annotated references, recommended student study time, self-assessment exercises, critical thinking and case studies, with indicative answers/solutions, aiming at a more meaningful understanding of the content, terms and concepts that each unit deals with.

The recommended weekly working time, apart from studying, includes the follow-up of (tele) meetings and Group Consultation Meeting (GCM), the search for bibliography/references, completion of any coursework, weekly exercises, etc. Although it is sufficiently clear, it should be noted that the study guide does not substitute the educational material posted on the platform that the student needs to read carefully and understand in order to be able to meet the requirements of the program and successfully complete the course.

## 1st GROUP CONSULTATION MEETING

### Programme Presentation

Leading companies today are rethinking the role of information security in their organizations. They realize that in a digital world, cybersecurity is the key to safeguarding their most precious assets—intellectual property, customer information, financial data, and employee records, among others. But far more than a defensive measure, companies also know that cybersecurity can better position their organization with business partners, customers, investors, and other stakeholders.

The European cybersecurity market is about 25% (i.e. about €17bln) of the world market (estimated at €70bln in 2015), with an average yearly growth slightly larger than 6%, when the world market is growing at about 10%/year. Recent study compiled by Europe's cybersecurity industry leaders pointed out that Europe is in danger of falling behind in the international digital economy field.

The Master in Cybersecurity is a cutting-edge program, designed for those wishing to develop a career as a cyber-security professional, or to take a leading technical or managerial role in an organization critically dependent upon data and information communication technology. Students will develop an advanced knowledge of information security and an awareness of the context in which information security operates in terms of safety, environmental, social and economic aspects. They will gain a wide range of intellectual, practical and transferable skills, enabling them to develop a flexible professional career in IT.

Key elements of this postgraduate degree are: the *real life experience* given by the opportunity to apply their theoretical knowledge through specialized virtual and remote security laboratories in which they will be able to carry out activities such as reconnaissance, network scanning and exploitation exercises, and investigate the usage and behavior of security systems such as Intrusion Detection and Prevention Systems thus becoming confident in the practical application of the latest tools; the *high-level insight* that will enhance student's ability to research and design creative cyber security solutions to address business problems; *hands-on skills* through experimentation with security techniques, cryptographic algorithms, cyber forensics building an ethical hacking environment; and *flexibility* since students will also be able to choose either the completion of a Master thesis or to complete a Research methods course and two elective courses.

Students undertake modules to the value of 90 ECTS credits.

## **Recommended Study Time for Students**

Approximately 5 hours for the study of the Study Guide

## INTRODUCTION

1<sup>st</sup> Week

### Summary

In this week we will introduce the course and discuss several up to date trends in Cybersecurity such as cyber incidence report as well as protection for the infrastructure.

### Introductory Remarks

Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services.

A range of traditional crimes are now being perpetrated through cyberspace. This includes the production and distribution of child pornography and child exploitation conspiracies, banking and financial fraud, intellectual property violations, and other crimes, all of which have substantial human and economic consequences.

Cyberspace is particularly difficult to secure due to a number of factors:

- the ability of malicious actors to operate from anywhere in the world
- the linkages between cyberspace and physical systems
- the difficulty of reducing vulnerabilities and consequences in complex cyber networks

Of growing concern is the cyber threat to critical infrastructure, which is increasingly subject to sophisticated cyber intrusions that pose new risks. As information technology becomes increasingly integrated with physical infrastructure operations, there is increased risk for wide scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions/billions of people depend. In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace has become an important mission for several governments/authorities.

## **Securing Networks**

Securing networks is essential in order to prevent several cyber threats including:

- Viruses, Worms and Trojan horses
- Zero-day attacks
- Hacker attacks
- DoS attacks
- Spyware and adware

In addition, as systems are protected, alerts can be issued at machine speed when events are detected to help protect networks across the business or even the whole nation.

## **Protecting Critical Infrastructure**

The protection of critical infrastructure is one of the biggest goals in cybersecurity. Even if almost all the machines/stations in an infrastructure comply with the latest security guidelines, if one of them does not then it poses a threat to the whole network. That is why in the USA, the Department of Homeland Security (DHS) employs a risk-informed, all-hazards approach to safeguarding critical infrastructure in cyberspace that emphasizes protections for privacy and civil liberties, transparent and accessible security processes, and domestic and international partnerships that further collective action.

DHS coordinates with sector specific agencies, other federal agencies, and private sector partners to share information on and analysis of cyber threats and vulnerabilities and to understand more fully the interdependency of infrastructure systems nationwide. This collective approach to prevent, protect against, mitigate, respond to, investigate, and recover from cyber incidents prioritizes understanding and meeting the needs of our partners, and is consistent with the growing recognition among corporate leaders that cyber and physical security are interdependent and must be core aspects of their risk management strategies.

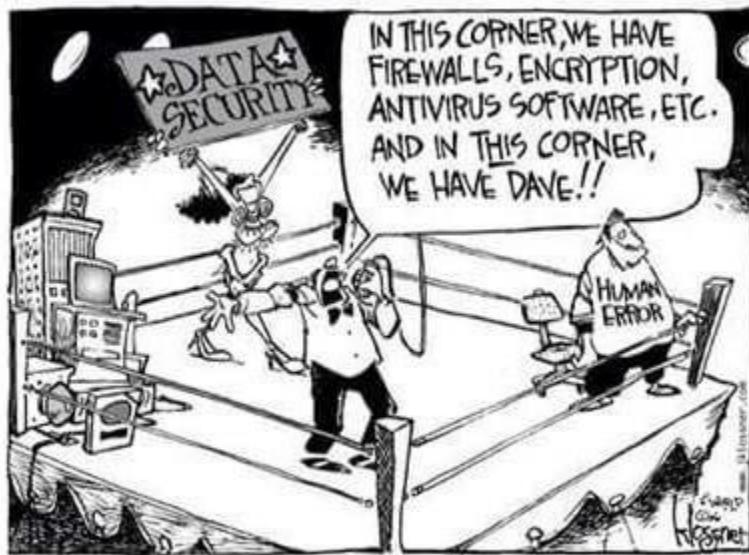


Figure 1 Cyber Security Awareness (Source [www.4itsec.com](http://www.4itsec.com))

## Cyber Incident Response

Incident report is very important when it comes to cybersecurity. Incident response is a way of addressing and managing the aftermath of cyberattacks in a way as to limit the damages and reduce recovery times and costs. Any incident that is not properly contained and handled can escalate into a bigger problem that can ultimately lead to a damaging data breach or system collapse. Responding to an incident quickly will help an organization minimize losses, mitigate exploited vulnerabilities, restore services and processes, and reduce the risks that future incidents pose. Incident response enables an organization to be prepared for the unknown as well as the known and is a reliable method for identifying a security incident immediately when it occurs. Incident response also allows an organization to establish a series of best practices to stop an intrusion before it causes damage.

## Cyber Safety

Being online exposes us to cyber criminals and others who commit identity theft, fraud, and harassment. Every time we connect to the Internet we make decisions that affect our cybersecurity. Emerging cyber threats require engagement from the entire community to create a safer cyber environment, from government and law enforcement to the private sector and, most importantly, members of the public.

## Aim/Objective

The purpose of the 1<sup>st</sup> Week is to introduce to the students the basic concepts and trends in Cybersecurity. Some of the current priorities are explained, as well as examples and case studies of governments and agencies are provided.

## Learning Outcomes

After the successful completion of the 1<sup>st</sup> Week, students should be able to:

- Explain the cybersecurity problems faced by businesses/organisations
- Comprehend the difficulties faced when applying cybersecurity methods
- Explain the importance of securing private and public networks
- List what are the problems faced by critical infrastructure and how it should be protected
- Give the benefits of cyber incident response
- Give examples of security incidents and security measures taken by businesses and governments

## Key Words

Cyberspace	Malicious	Physical Systems
Vulnerabilities	Networks	Infrastructure
Incident Response	Damages	System Collapse

## Annotated Bibliography

### Basic

- E. C. Thompson, *Cybersecurity Incident Response How to Contain, Eradicate, and Recover from Incidents*. Apress, 2018, Chapter 1 “The Significance of Incident Response”

The first Chapter of this book introduces the significance of incident response, something that is important in the current cybersecurity trends. As we see in the following weeks, one of the most important part of every cybersecurity law is the correct and fast incident response.

- J. Jang-Jaccard, S. Nepal, A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences. 2014;80(5):973-993.

This survey paper indicates and explains all the emerging threats in cybersecurity. It covers everything that will be discussed not only in the first week but in the weeks to come.

### **Suggestions for further reading**

- G. Schaub Jr., Understanding Cybersecurity Emerging Governance and Strategy, Rowman & Littlefield, 2018, Chapter 1 “Internet Governance and National Security”

The first chapter of this book covers the importance of cybersecurity and the problems faced at a national security level.

## **Self-Assessment Exercises**

### **Exercise 1.1**

Explain in your own words the terms “Risk”, “Vulnerability” and “Threat”

### **Exercise 1.2**

Using online resources, write an essay (about 400 words) indicating what measures the U.S. government and more specifically DHS decided to take in order to protect the country from cyber-attacks.

## **Recommended time for the student to work**

15 hours

## MAJOR CYBER ATTACKS / INCIDENTS IN RECENT YEARS

2<sup>nd</sup> Week

### Summary

In this week we will introduce some of the major cyber attacks as well as other incidents in recent years and we will discuss how those affected the cyber world in general and how they could have been avoided.

### Introductory Remarks

In the 2<sup>nd</sup> week we will cover some important cybersecurity statistics as well as some cases of recent attacks and incidents in order to understand the importance of cybersecurity as well as analyse the current trends in the area.

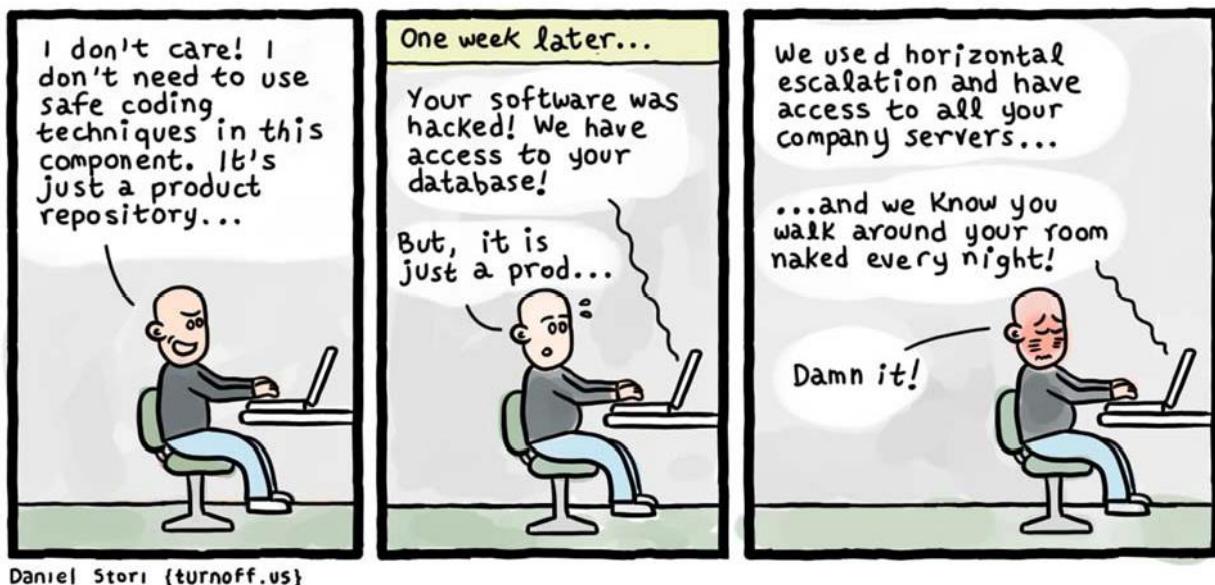


Figure 2 Security is a Serious Matter (Source [www.sheyam.co.in](http://www.sheyam.co.in))

## **National Security Agency (NSA) Hacking Tools**

NSA hacking tools were stolen and leaked by the Shadow Brokers Group. This resulted in a number of cyber-attacks around the world. One of this attack struck networks in Ukraine including the American drug company Merck.

One of those tools which became famous due to its power and the amount of machines it has infected is EternalBlue. EternalBlue is the name of a software vulnerability in Microsoft Windows OS as well as a bug NSA developed to use the bug.

## **National Health Service (NHS) Cyber Attack & Global Ransomware Attacks**

The NHS (UK health services) attack was a global attack which used the WannaCry ransomware (believed to be one of the leaked NSA hacking tools) to affect more than 300000 computers. WannaCry affected machines worldwide, but mostly in Russia, Taiwan, Ukraine and India. In the UK a huge number of hospitals and physicians have been attacked by the ransomware, which caused a huge chaos. In 2017 ransomware attacks have been increased by 36%, with more than 100 new malware families introduced by hackers.

In addition, cyber criminals who have been firmly focused on ransomware for revenue, are now starting to explore other opportunities. Recent astronomical rise in crypto currency values inspired them to shift to coin mining. With the use of malwares, they harvest CPU power from user machines in order to mine crypto currency.

## **French Election Email Dump**

9GB of internal documents from Emmanuel Macron (French Presidential Candidate) have been leaked to the public two days before the French election. No one has claimed responsibility for the data dump, but it's widely thought to be the work of pro-Russian hackers who tried to influence the election in Le Pen's favour. (French Presidential Candidate)

## **Microsoft Presentation on Cybersecurity**

Microsoft claims that the potential cost of cybercrime to the global community is in the range of 500 billion dollars, and the average data breach can cost about 3.8 million dollars to a company. In addition, it claims that more than 63% of network intrusions are due to compromised user credentials. This is due to the fact of password reuse as well as the fact that it takes around 146 days for security engineers to detect that an attacker resides within a network.

## **Juniper Research Predictions**

Juniper research titled “The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation” predicts that the average cost of a data breach will exceed 150 million dollars by 2020 which is a massive 3947% increase from Microsoft’s measurements, and cybercrime will cost businesses over 2 trillion dollars. Juniper also mentions that “we aren’t currently seeing much dangerous mobile or IoT malware because it’s not profitable”. In addition, it says that “The kind of threats we will see of these devices will be either ransomware, with consumers’ devices locked down until they pay the hackers to use their devices, or as part of botnets, where processing power is harnessed as part of a more lucrative hack. With the absence of a direct payout from IoT hacks, there is little motive for criminals to develop the required tools”

## **Aim/Objectives**

The purpose of the 2<sup>nd</sup> Week is to introduce some of the latest attacks and trends in the area of cybersecurity. Students should become familiar with the latest news as well as the shifting trends towards malware and CPU harvesting for crypto currency mining. Finally, students will become familiar with the trends when it comes to the fight against cybercrime.

## **Learning Outcomes**

After the successful completion of the 2<sup>nd</sup> Week, students should be able to:

- Evaluate the NSA hacking tools leak and indicate how they have already been used in cybercrime
- Explain what happened at the NHS attack, as well as the other impacts WannaCry had in the world of computing
- Judge the French election email dump as well as the impact such a cybercrime can have on the community
- Justify Microsoft’s presentation and predictions about the future of cybercrime
- Justify Juniper’s research predictions and the trends of cybercrime, especially when it comes to mobile devices and IoT

## Key Words

NSA Hacking Tools	WannaCry	Ransomware
French Elections	Microsoft Predictions	Juniper Research
CPU Malware	Mobile and IoT Attacks	

## Annotated Bibliography

### Basic

- S. Mohurle, M. Patil, (2017) A brief study of Wannacry Threat: Ransomware Attack 2017, International Journal of Advanced Research in Computer Science; Vol. 8
- A. Tandon, A. Nayyar, (2019) A Comprehensive Survey on Ransomware Attack: A Growing Havoc Cyberthreat, Advances in Intelligent Systems and Computing, vol 839. Springer, Singapore
- Microsoft Cloud-Platform (2018). Advanced Threat Analytics, Microsoft. [online] Available at: <https://www.microsoft.com/en-us/cloud-platform/advanced-threat-analytics> [Accessed 25 Oct. 2018].
- Juniper research: The future of cybercrime & security. Computer Fraud & Security. 2018

### Suggestions for further reading

- NHS cyber-attack: Amber Rudd says lessons must be learnt - BBC News, [Youtube Video], Available at: <https://www.youtube.com/watch?v=gNjc6qD-c6g>
- Introduction to EternalBlue (MS17-010) - Jason Dion [Youtube Video], Available at: <https://www.youtube.com/watch?v=T1Jfz-EQa60>
- WannaCry Ransomware Explained! How to Stay Safe! - C4ETech [Youtube Video], Available at: <https://www.youtube.com/watch?v=GcJaLMrbP10>

## **Self-Assessment Exercises**

### **Exercise 2.1**

Using your own words, explain what are ransomwares, how they work, why do they use crypto currency and what someone can do to lower the chances of getting hit by one. In addition, briefly explain the NHS WannaCry incident and indicate some of the impacts it had on the community.

### **Recommended time for the student to work**

15 hours

## WHAT TO EXPECT IN CYBERSECURITY THREATS

3<sup>rd</sup> Week

### Summary

In this week we will introduce some of the upcoming threats in cybersecurity as well as trends using some of the most important research papers published by the biggest companies in the area of internet, computing and cybersecurity in general.

### Introductory Remarks

Cyber threats are a rapidly increasing trend, that not only changes the scenery of cybersecurity, but it also changes the computing world in general. A report from Herjavec Group, predicts that by 2021 3.5 million new cybersecurity jobs will be opened. Comparing this to the 1 million openings in 2016, and you can see an increase of 350 percent in just five years.

Gartner, Inc. report indicated that in 2017, businesses payed \$86.4 billion in security services/products in order to be protected against cyber threats. That was 7% increase compared to 2016. They also predicted that this number will grow to \$93 billion in 2018.

Looking at these trends as well as upcoming technologies in Internet and computing in general, we can predict the future of cybercrime and cybersecurity.

### Ransomware Evolution

Ransomware is the bane of cybersecurity, IT, data professionals, and executives. Perhaps nothing is worse than a spreading virus that latches onto customer and business information that can only be removed if you meet the cybercriminal's egregious demands. Usually, those demands land in the hundreds of thousands (if not millions) of dollars. Ransomware attacks are one of the areas of cybercrime growing the fastest, too. Sadly, those attacks aren't fading with time, they're even getting stronger. In 2013, there were 500,000 malicious applications. In 2015, that number increased to 2.5 million. In 2017, it sits at 3.5 million. And 77% of those applications are malware according to SophosLabs 2018 Malware Forecast.

Even though, the increase in this type of threats is enormous, there is a large percentage of businesses that do not take cybersecurity seriously. In fact, according to a report from Infrascale,

20% of businesses still do not have a disaster recovery solution. Which means that when a malicious attack comes, one-fifth of businesses have no method or plan for recovering data, applications, customer information, servers, or systems. In addition, Infrascale report goes a step further and states that 42% of the businesses that do have a disaster recovery strategy use a tape-based, outdated backup method. In today's world of evolving ransomware, yesterday's DR strategies no longer work.

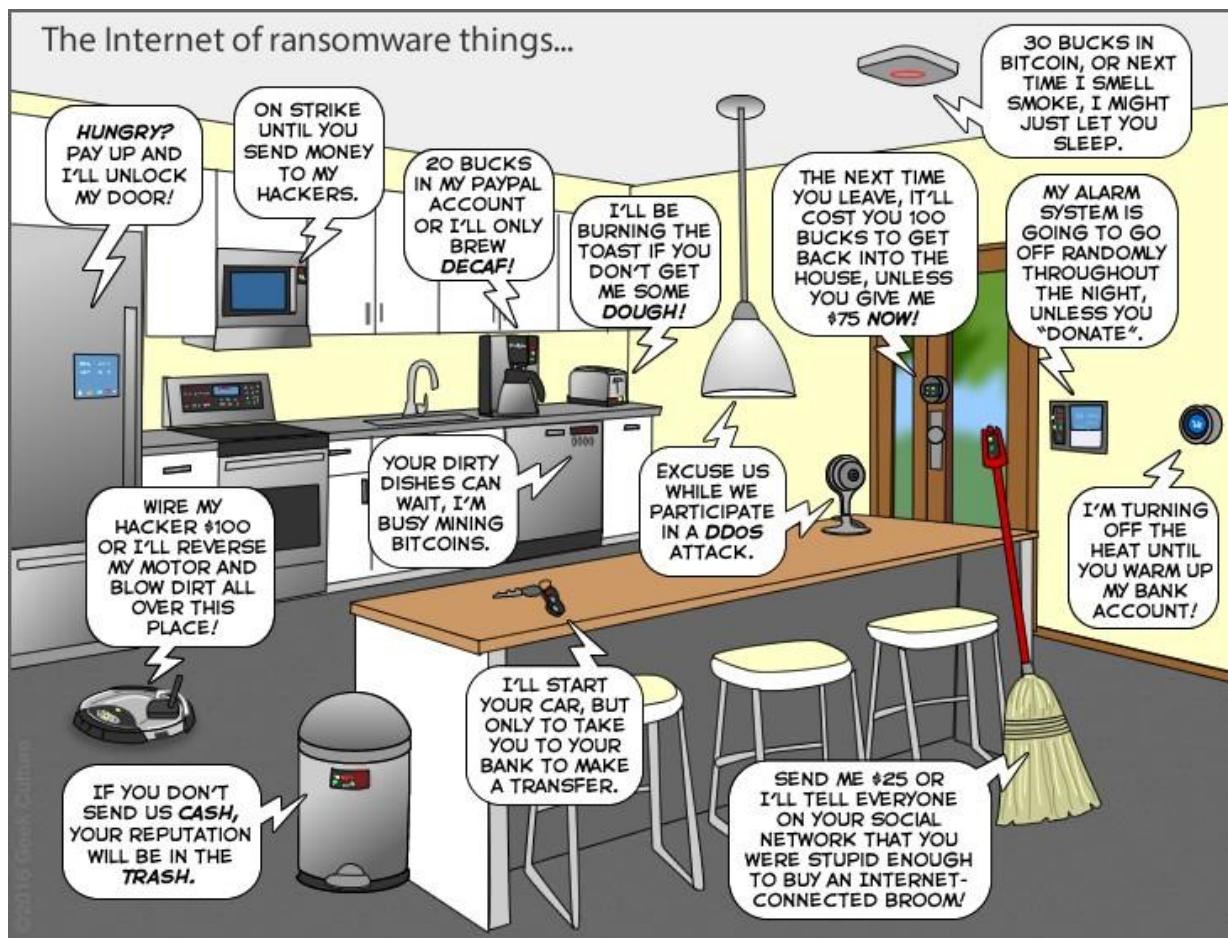


Figure 3 The Internet of Ransomware Things (Source [www.geekculture.com](http://www.geekculture.com))

## AI Expansion

AI might be able to help defend against incoming cyber-attacks. This is a huge development since it will lower the costs against cyber-attacks. First of all, AI does not need hourly payment. In addition, AI can work around the clock, with no breaks, and AI can evolve rapidly. Timing is everything with malware and other vicious data manipulations. If, for instance, you could fight a

virus as it was downloading, you'd have a much better chance of mitigating its forceful impact. But, when you fight against corrupt data after the fact recovery becomes an uphill battle. Traditionally, IT professionals and cybersecurity experts face these attacks once they've already taken place. Since AI doesn't need to sleep, though, they can set defence systems against malware the moment it begins to download.

## **IoT Threats**

The vast majority of humans in first-world countries have a smartphone in their pockets, a computer at work, a smart television at home, and a tablet in their cars. But there is more to come. The Internet of Things (IoT) is making sure that every single device you own is connected. For example, there are now smart refrigerators that can tell you if there is no milk left, there are smart speakers that can talk and listen to you, and order goods online on your command. The fact that everything is connected gives massive benefits to the user, making it so appealing in the first place. You can now control your house from your smart device, or you can ask the virtual assistant (Google Assistant, Siri, Alexa) to do something for you. The problem is that all of that interconnectedness makes consumers highly susceptible to cyberattacks. In fact, one study by Gartner revealed that 70 percent of IoT devices have serious security vulnerabilities. Specifically, insecure web interfaces and data transfers, insufficient authentication methods, and a lack of consumer security knowledge leave users open to attacks. And that truth is compounded by the fact that so many consumer devices are now interconnected. In other words, if you access one device, you've accessed them all. Evidently, with more convenience comes more risk.

## **Blockchain Revolution**

2017 ended with a spectacular rise in the valuation and popularity of cryptocurrencies like Bitcoin and Ethereum. These cryptocurrencies are built upon blockchains, the technical innovation at the core of the revolution, a decentralized and secure record of transactions. But the question is what does blockchain technology have to do with cybersecurity. It's a question that security professionals have only just started asking. While it's difficult to predict what other developments blockchain systems will offer in regards to cybersecurity, professionals can make some educated guesses. Companies are targeting a range of use cases which the blockchain helps enable from medical records management, to decentralized access control, to identity management. As the application and utility of blockchain in a cybersecurity context emerges, there will be a healthy tension but also complementary integrations with traditional, proven, cybersecurity approaches. You will undoubtedly see variations in approaches between public & private

blockchains. With blockchain technology, cybersecurity will likely look much different than it has in the past.

### **Serverless Apps Vulnerability**

Serverless apps can invite cyber-attacks. Customer information is particularly at risk when users access your application off-server, or locally, on their device. This is because on-server, when the data is stored in the cloud rather than the user's device you have control over that information and the security that surrounds it. In other words, you're able to control what security precautions you take to ensure the user's data remains private from identity thieves and other cybercriminals. With serverless applications, however, security precautions are, by and large, the responsibility of the user. Of course, you can integrate software into the application that gives the user the best chance of defeating cybercriminals. But when all's said and done, you, the professional, can't directly defend the customer. Serverless apps are most common as web service and data processing tools. Unfortunately, with all of the vulnerability that serverless apps represent, they don't seem to be going anywhere in the years to come.

### **Aim/Objectives**

The purpose of the 3<sup>rd</sup> Week is to evaluate important cybersecurity threats and show what the predictions for their future are. We go a step further to discuss new threats that might use evolving methodologies to infect or attack a broader audience.

### **Learning Outcomes**

After the successful completion of the 3<sup>rd</sup> Week, students should be able to:

- Evaluate the current state of Cybersecurity and what to expect in the future
- Explain how ransomware evolution might affect the world of cyber business in the future
- Explain the AI expansion and how that might help or affect cybersecurity
- Explain the IOT threats and what the community has to do to prevent such an attack
- Explain blockchain revolution and how that can affect the world of cybersecurity
- Explain what are serverless apps and why they are vulnerable to cyber attacks

## Key Words

Trends	Ransomware	Evolution
AI Expansion	Outdated	IoT
Threats	Blockchain	Serverless

## Annotated Bibliography

### Basic

- Harjavec Group (2017). Cybersecurity Jobs Report. [online] Available at: <https://www.herjavecgroup.com/wp-content/uploads/2018/07/HG-and-CV-The-Cybersecurity-Jobs-Report-2017.pdf> [Accessed 30 Oct. 2018].
- SophosLabs (2017). SophosLabs 2018 Malware Forecast. [online] Available at: <https://www.sophos.com/en-us/en-us/mediabinary/PDFs/technical-papers/malware-forecast-2018.pdf?la=en> [Accessed 30 Oct. 2018].
- Infrascale (2016). 2016 Disaster Recovery as a Service Attitudes & Adoption Report. [online] Available at: <https://www.infrascale.com/wp-content/uploads/pdf/2016-Disaster-Recovery-as-a-Service-Attitudes-and-Adoption-Report.pdf> [Accessed 30 Oct 2018]
- Gartner (2013). Forecast: The Internet of Things, Worldwide, 2013. [Online] Available at: <https://www.gartner.com/doc/2625419/forecast-internet-things-worldwide-> [Accessed 30 Oct 2018]

### Suggestions for further reading

- The Evolution of Ransomware - Symmetry Informatica [Youtube Video], Available at: <https://www.youtube.com/watch?v=cdBhPDdji3Q>
- "Ransomware attacks were on the rise, even before the last episode", The Economist, 15<sup>th</sup> May 2017, Available at: <https://www.economist.com/graphic-detail/2017/05/15/ransomware-attacks-were-on-the-rise-even-before-the-latest-episode> [Accessed 5 Dec 2018]

## Self-Assessment Exercises

### Exercise 3.1

Explain what is the IoT and how it can affect the world of cybersecurity

**Exercise 3.2**

Explain the blockchain revolution, giving your own examples from online resources. (Use appropriate Citations)

**Recommended time for the student to work**

15 hours

## Summary

In this week we will introduce the strategy of the European Union on cybersecurity and we will take a look at the upcoming Cybersecurity Act.

## Introductory Remarks

Securing network and information systems in the European Union is essential to keep the online economy running and to ensure prosperity. The European Union works on a number of fronts to promote cyber resilience across the European Union.

In view of a dynamically evolving threat landscape and building on the review of the 2013 EU cybersecurity strategy, tackling the cybersecurity perils together was one of the three challenges identified in the mid-term review of the Digital Single Market.

On 13 September 2017 the Commission adopted a cybersecurity package. The package builds upon existing instruments and presents new initiatives to further improve EU cyber resilience and response.

### ENISA – the EU cybersecurity agency

The European Union Agency for Network and Information Security (**ENISA**) has a key role to play but is constrained by its current mandate. The Commission presents an ambitious reform proposal, including a permanent mandate for the agency to ensure that ENISA can provide support to Member States, EU institutions and businesses in key areas, including the implementation of the NIS Directive. It will also contribute to stepping up both operational cooperation and crisis management across the EU.

### A single cybersecurity market

The growth of the cybersecurity market in the EU – in terms of products, services and processes – is held back in a number of ways, also due to lack of a cybersecurity certification scheme recognised across the EU. The Commission is therefore putting forward a proposal to set up an EU certification framework with ENISA at its heart. A joint Commission-industry initiative will

also be launched to define a “duty of care” principle to reduce product and software vulnerabilities and promote a “security by design” approach for all connected devices.

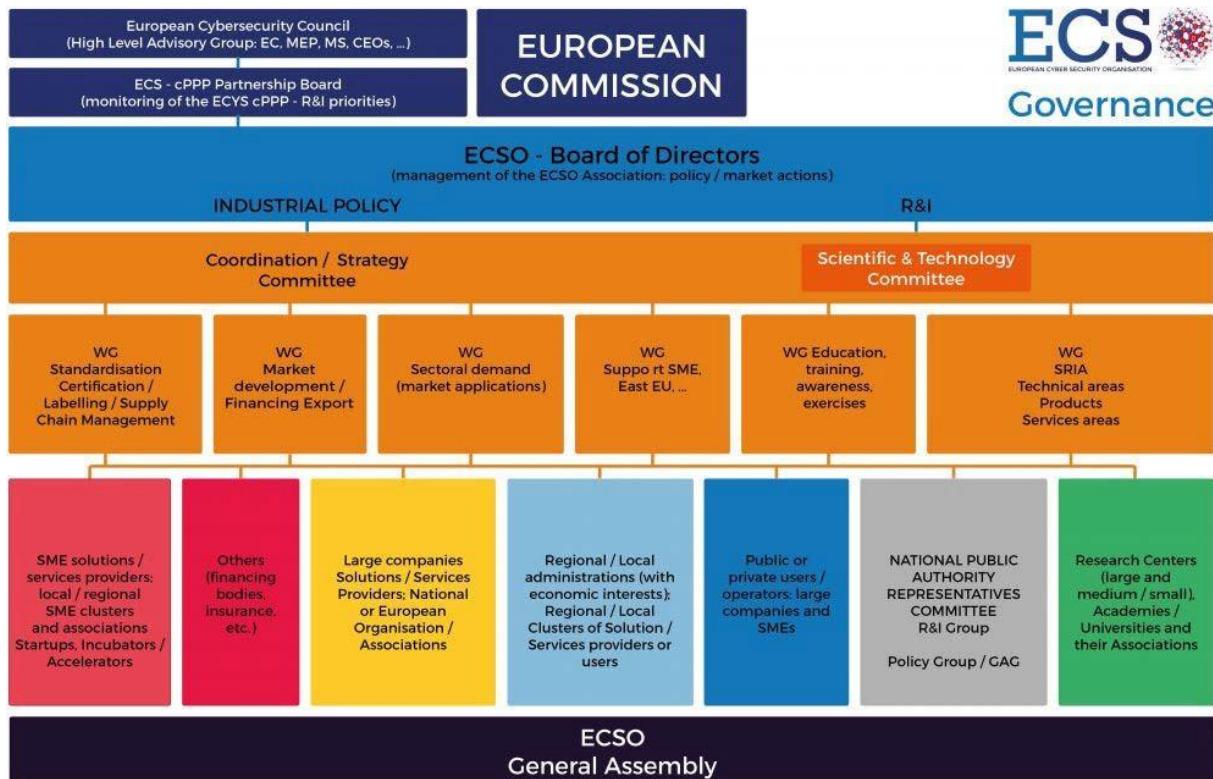


Figure 4 European Cyber Security Organisation (ESCO) (Source [www.ecs-org.eu](http://www.ecs-org.eu))

## The NIS directive

It is necessary to swiftly implement the NIS directive (Directive on security of network and information systems), adopted in July 2016. This will be facilitated thanks to Commission guidance on how the Directive should operate in practice and additional interpretation of specific provisions included in the September 2017 package.

## Blueprint for rapid emergency response

The Commission presents a blueprint so that the EU has in place a well-rehearsed plan in case of a large scale cross-border cyber incident or crisis. It sets out the objectives and modes of cooperation between the Member States and EU Institutions in responding to such incidents and crises, and explains how existing Crisis Management mechanisms can make full use of existing cybersecurity entities at EU level.

## **External relations**

The EU strongly promotes the position that international law, and in particular the United Nations (UN) Charter, applies in cyberspace. As a complement to binding international law, the EU endorses the voluntary non-binding norms, rules and principles of responsible State behaviour that have been articulated by the UN Group of Governmental Experts. It also encourages the development and implementation of regional confidence building measures, both in the Organisation for Security and Co-operation in Europe and other regions. On a bilateral level, cyber dialogues will be further developed and complemented by efforts to facilitate cooperation with third countries to reinforce principles of due diligence and state responsibility in cyberspace.

## **Cyberdefence**

The recently adopted framework for a joint EU diplomatic response to malicious cyber activities (the “cyber diplomacy toolbox”) sets out the measures under the Common Foreign and Security Policy, including restrictive measures which can be used to strengthen the EU's response to activities that harm its political, security and economic interests. Implementation work on the Framework is currently ongoing with Member States and would also be taken forward in close coordination with the Blueprint to respond to large scale cyber incidents.

## **Cybercrime**

The Commission will present concrete proposals in early 2018 to facilitate swift cross-border access to electronic evidence.

### European Factsheet

According to “Resilience, Deterrence and Defence: Building strong cybersecurity in Europe” factsheet, Europeans, with percentages 75%, 64% and 67% believe that digital technologies have a positive impact on economy, society and quality of life respectively. At the same time, 86% of them believe that the risk of becoming a victim of cybercrime is increasing.

## **Aim/Objectives**

The purpose of the 4<sup>th</sup> Week is to evaluate EU cybersecurity strategy. We explain several agencies that have been created, such as ENISA. We then see how cybersecurity affects the market and how EU tackles that. Finally, we see what NIS directive is and how EU handles emergencies as well as external relations.

## Learning Outcomes

After the successful completion of the 4<sup>th</sup> Week, students should be able to:

- Evaluate EUC cybersecurity strategy
- Explain what is ENISA
- Explain the NIS directive
- Explain how the rapid emergency response works
- Explain how EU handles external relations
- Explain how EU handles Cyberdefence and Cybercrime

## Key Words

ENISA	Market	NIS
Blueprint	Emergency Response	External
Cyberdefence	Cybercrime	Rapid

## Annotated Bibliography

### Basic

- European Union Mid-Term Review. Digital Single Market Mid-term Review: Commission calls for swift adoption of key proposals and maps out challenges ahead. [online] Available at: <https://ec.europa.eu/digital-single-market/en/news/digital-single-market-mid-term-review> [Accessed 2 Nov. 2018].
- European Union (2017). Resilience, Deterrence and Defence: Building strong cybersecurity in Europe. [online] Available at: <file:///C:/Users/phili/Downloads/CybersecurityFactsheetA4201709191113.pdf> [Accessed 2 Nov. 2018]

### Suggestions for further reading

- ENISA Cyber Europe 2016 - Are you ready for the next cyber crisis? - ENISAvideos [Youtube Video], Available at: <https://www.youtube.com/watch?v=2wVsB1WCfNg>

## **Self-Assessment Exercises**

### **Exercise 4.1**

Explain what ENISA does in the EU

### **Exercise 4.2**

Explain the EU Cyberdefence and Cybercrime strategies

## **Recommended time for the student to work**

15 hours

## Summary

In this week we will take a closer look at the EU strategy on cybersecurity looking more in depth on Cybersecurity Act and comparing it with related acts implemented in other countries.

## Introductory Remarks

The EU aims at achieving a common high EU level of security for networks and information systems for certain critical sectors (“essential services”) and to establish cooperation between Member States and operators to enhance security. Security requirements are also part of several other sectoral EU laws. The main EU legal acts for cybersecurity are listed below. Most EU acts are directives and therefore require implementation in Member State national laws.

- a. The NIS Directive requires EU Members States to, by 9 May 2018, impose security requirements and notification obligations on their national essential services providers, both public and private (transport, banking, financial market, health and water supply sectors) and introduce penalties for failures. It also creates an incident response team network (“CSIRTs network”).
- b. The EU electronic communications Directive requires operators providing public communication networks or publically available electronic communications services to ensure security.
- c. Directive 2009/140 EC (Telecom Package) requires telecom service providers to ensure integrity and notify incidents.
- d. EU Data privacy rules and ePrivacy Directive also require operators to ensure integrity and protect data.
- e. The eIDAS Regulation establishes an internal market for the use of trust services and electronic identification.

Compared to the US, there is presently, at EU level, a gap in how cybersecurity risks in relation to foreign investment are assessed. As defence and security lies outside the EU's legislative

competence, EU Member States may adopt and act under national defence or national security laws. Reportedly, however, Germany has called for an EU regulation, imposing mandatory reviews to approve or prohibit foreign investments in consideration of possible national security threats. The EU Parliament has also called on the European Commission to draw up such common EU laws on foreign investment review. In addition, in comparison to the US, the EU has not (yet) imposed any economic sanctions related to malicious cyber activities. The EU does have laws on trade and export of information security technology, which restricts export and trade from all EU Member States on items (hardware, software and technology) related to information security.

### **Cybercrime**

Criminal law is normally the competence of each Member State national law, but the EU has through Directive 2013/40/EU established minimum definitions of what shall constitute criminal offences in all EU Member States (e.g. illegal access, illegal system interference, illegal data interference, illegal interception) and directs Member States to enact criminal penalties against these crimes. Also, Member States shall share information and report incidents.

### **Germany**

Beyond what is required by EU law, Germany has some notable national cybersecurity laws touching on cybersecurity. Germany has taken legislative action to enhance IT security of Germany's critical infrastructure and protecting users of the internet. The German IT Security Law requires private and public infrastructure operators to implement minimum information security standards (or face penalties) as well as reporting obligations for suspected attacks (e.g. energy, telecommunication, health, water/food, finance and insurance). The Federal Office of Information Security (BIS) is responsible for investigating cyberattacks. Further, in specific sectors, the competent authority sets minimum IT security standards.

The German government may block foreign investments to ensure that they do not threaten public order or security. The German Foreign Trade Law allows the federal government to block investors from acquiring at least 25% of a company. The Ministry of Economic Affairs conducts mandatory reviews for foreign investments in certain IT security sectors. Reportedly, in 2012, the German national research and education network decided to ban Huawei from tendering for a network update due to security concerns. These rules may be further strengthened if common EU-rules are adopted. Germany also applies the EU dual-use regulation including controls on the export of information security software and hardware (including encryption).

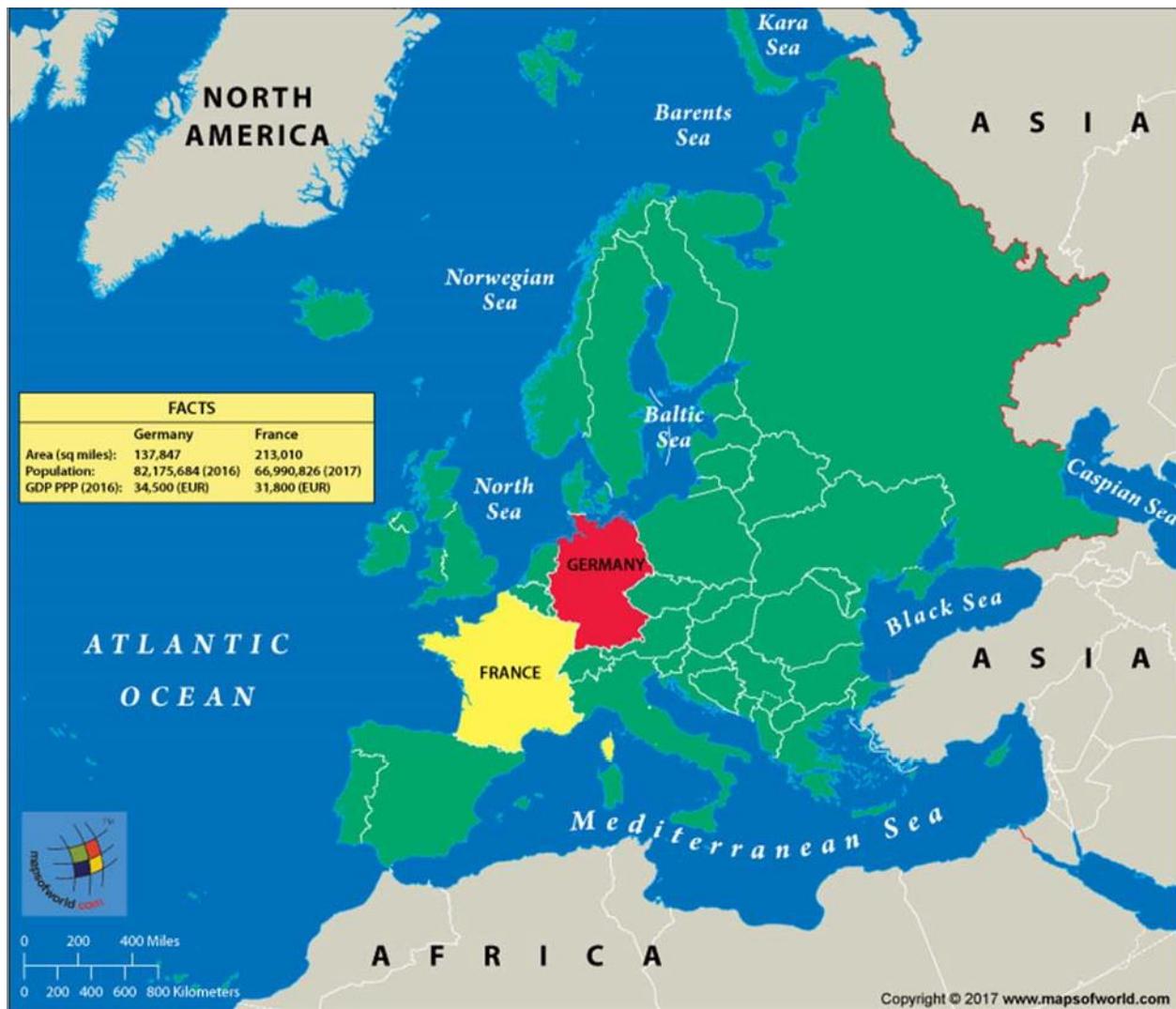


Figure 5 Germany and France Map (Source [www.mapofworld.com](http://www.mapofworld.com))

## France

Beyond what is required by EU law, operators of information systems in critical infrastructure are obliged by the Military Planning Act to protect their information systems. The governmental agency ANSSI has an increasing role in preventing and collecting reports of attacks. Under the Penal Code, France prohibits all forms of supply of certain equipment used to intercept communication, unless specifically authorised. The governmental agency ANSSI is entrusted to handle and grant authorisations for such supplies. France also applies the EU dual-use regulation including controls on the export of information security software and hardware, including encryption. In addition, France controls also supply and import of encryption into France. A general provision in the Defence Code allows French authorities, faced with a threat to e.g. its national interest, to perform any technical operation deemed necessary to attribute or mitigate an

attack by accessing information. France also requires approval of foreign investments in sensitive sectors critical to France's national interest. The Godfrain Law, incorporated into the French Criminal Code, sets out criminal actions associated with e.g. cybercrime. France has fully implemented the Budapest Convention into French Law

## Aim/Objectives

The purpose of the 5<sup>th</sup> Week is to explain and evaluate the proposed Cybersecurity Act of the European Union. We evaluate the act, and we take a look at individual regulations of countries such as Germany and France

## Learning Outcomes

After the successful completion of the 5<sup>th</sup> Week, students should be able to:

- Evaluate the Cybersecurity Act
- Evaluate German Cybersecurity laws
- Evaluate French Cybersecurity laws

## Key Words

Cybersecurity Act	NIS Directive	Legal Acts
Criminal Offences	Illegal Access	Foreign Trade Law
ANSSI	Defence Code	Godfrain Law

## Annotated Bibliography

### Basic

- European Parliament. Cybersecurity Act: Build Trust in Digital Technologies. [online] Available at: <http://www.europarl.europa.eu/news/en/press-room/20180710IPR07605/cybersecurity-act-build-trust-in-digital-technologies> [Accessed 2 Nov. 2018].

### Suggestions for further reading

- Understanding the European NIS Directive by Nathan Martz, [Youtube Video], Available at <https://www.youtube.com/watch?v=isL1xNBfTjA>

- Defence companies target the cyber-security market. The Economist, 26<sup>th</sup> Jul 2018 Available at: <https://www.economist.com/business/2018/07/26/defence-companies-target-the-cyber-security-market> [Accessed 5 Dec 2018].

## Self-Assessment Exercises

### Exercise 5.1

Explain the German Cybersecurity laws

### Activity (5 points)

Activity that includes solving questions related, use online resources to the syllabus covered up to Week 5, as well as applying the knowledge gathered up to discuss and evaluate cybersecurity trends as well as compare the methodologies used by various companies as well as laws applied in several countries.

This activity counts 5% of the final course mark.

You will need approximately 5 hours to solve this Graded Activity.

### Recommended time for the student to work

20 hours

## Summary

In this week we will take a closer look at the cybersecurity strategies of countries such as the United States of America as well as Australia.

## Introductory Remarks

### United States of America

The US is developing industry standards to enhance security for defined “critical infrastructure” and to share information on incidents to strengthen responses. Also, specific standards are being developed for US public authorities. Cybersecurity is also in part found in other sector-specific legislation.

The key legal acts in the US setting down this work are:

- a. For private sector operators, the Cybersecurity Enhancement Act 2014, directs the National Institute of Standards and Technology (NIST) to continue developing industry based standards and best practices for “critical infrastructure”. Also, the Cybersecurity Act 2015, encourages private operators to share information (other operators and the government) about attacks while maintaining confidentiality, privilege and immunity from liability and anti-trust laws. Only defensive, not offensive, security measures are allowed.
- b. For public authorities, the National Cybersecurity Protection Act of 2014 directs the National Cybersecurity and Communications Integration Center of the Department of Homeland Security to collect and share information about risks and incidents with the public and private sector. Federal Cybersecurity Enhancement Act 2016 and Federal Information System Modernization Act of 2014 (FISMA 2014), directs the Department of Homeland Security, e.g. to implement intrusion assessment plans for federal authorities.
- c. For financial institutions, the Gramm-Leach-Bliley Act of 1999, under the Safeguard Rule, requires them to e.g. ensure integrity of data and notifications of breaches of customer information. Similarly, healthcare organisations, under the Health Insurance Portability

and Accountability Act (HIPAA), have to protect information. Further, Electronic Communications Privacy Act (ECPA) prohibits third parties from intercepting or disclosing communications without authorisation

With increasing activity, the US reviews potential foreign investments to ensure that the foreign owners would not pose national interest concerns. Further, trade and export of sensitive information and security technology is restricted in order to prevent dissemination of sensitive technology used to protect against cybersecurity attacks. The US reportedly also imposed (and possibly revoked) requirements through the Appropriations Act on NASA and the Justice Department to buy information security systems only if federal law enforcement officers had given approval of the supplier.

The CFIUS (Committee on Foreign Investment in the United States), is authorised to review, for national security purposes, transactions that could result in control of a US business by a foreign person. CFIUS shall identify any national security risk and may request that the President suspends or prohibits a transaction or take other action. Factors to be considered under such a review include, amongst other, the security effect on the US defence industry, US critical infrastructure and also US technological leadership and critical technologies, particularly if the investment is made by a foreign state-controlled entity. The International Trade in Arms Regulation and Export Administration Regulations, impose restrictions on export on sensitive items used for information security (hardware, software and technology) including encryption items and software. Further, Executive Order 13694, imposes sanctions against significant malicious cyber-enabled activities, and allows the Office of Foreign Assets Control ("OFAC") under the US Treasury Department, to impose asset freezes on persons responsible for cyberattacks that threaten national security, foreign policy, or economic health or financial stability of the United States.

The United States Code (U.S.C.) lists as criminal acts; e.g. online identity theft, hacking, intrusion into computer systems, child pornography, breach of intellectual property. Also, US state laws may impose additional or overlapping offenses.

## Australia

Australia has taken several initiatives similar to those of the US and EU to enhance cybersecurity in critical infrastructure, and in sector specific areas, such as banking, finance and data privacy.

However, at present, these initiatives appear to not be based on legislative action but rather recommendations, guidelines and voluntary industry standards and cooperation (“soft law”) issues by the government.

The Australian Attorney-General has issued a Protective Security Policy Framework applicable in general to Australian governmental authorities. Also, the Australian Government Department of Defence has produced an Information Security Manual (ISM) which applies as a standard for government ICT systems. The government agency, Trusted Information Sharing Network (TINS), provides a platform for sharing information on incidents and increasing resilience against cybersecurity attacks. For example, for banking, the Prudential Practice Guide CPG 235 issued by APRA sets out a standard for managing data risks. Healthcare providers should follow the specific Computer and Information Security Standards.

Australia reviews foreign investments for national interest concerns. Since 2015 the review includes a specific screening to determine whether the foreign investment is made by a foreign government. The Foreign Acquisitions and Takeovers Act 1975 and Regulation 2015, allows the Australian Government Foreign Investment Review Board (FIRB), to review foreign investments in Australia and it advises the Treasurer and Commonwealth Government who may decide that an investment is contrary to national interests. Further, under the Australian Security Intelligence Organisation Act 1976, the Australian Security Intelligence Organisation (“ASIO”) may provide security intelligence to the Australian Government. In 2012, the ASIO advised and the Government blocked Huawei from a public tender of national broadband networks. Also, under The Defence and Strategic Goods List Australia controls export of information security items in a similar manner as the export control rules of the US and the EU.

Various laws implement the Budapest Convention criminalising acts under the Criminal Code Act 1995, Crimes Act 1914. Specific rules exist in the Telecommunications (Interception and Access) Acts, Copyright Act etc. More specifically, the Cybercrime Act 2001.

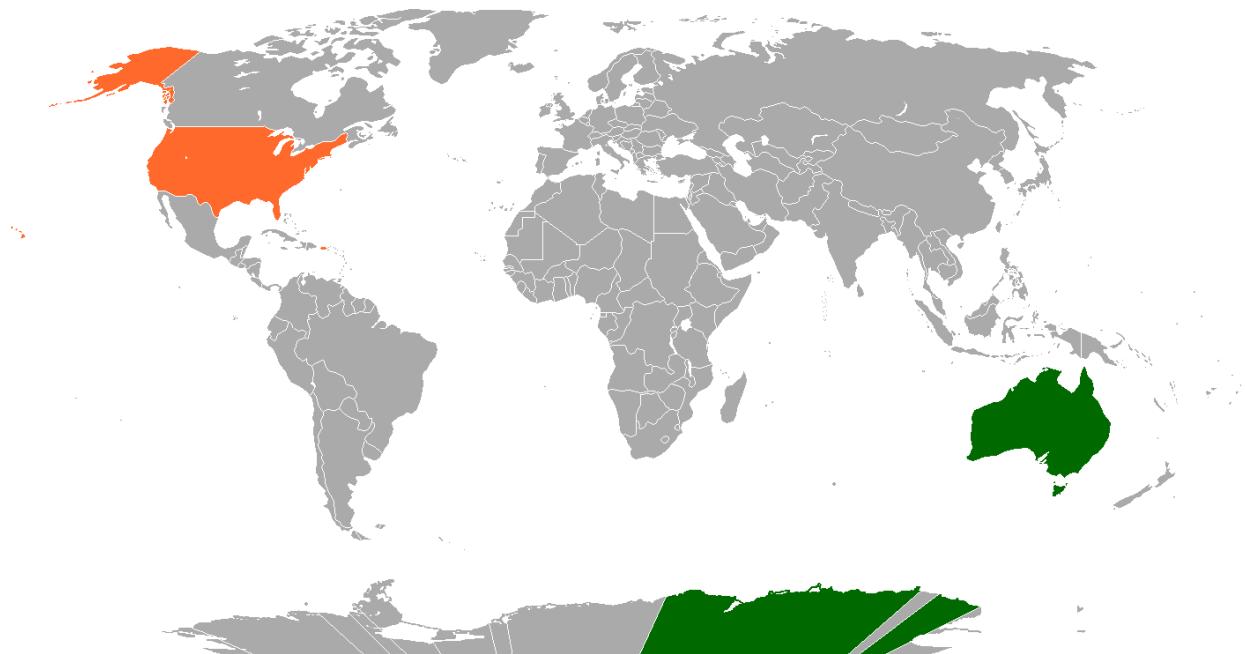


Figure 6 USA (in orange) and Australia (in green) Map (Source Wikipedia)

## Aim/Objectives

The purpose of the 6<sup>th</sup> Week is to introduce the cybersecurity laws of several countries around the world. We introduce the paradigms of United States of America and Australia.

## Learning Outcomes

After the successful completion of the 6<sup>th</sup> Week, students should be able to:

- Evaluate the cybersecurity laws in the United States of America
- Evaluate the cybersecurity laws in Australia

## Key Words

Specific Legislation	Critical Infrastructure	Anti-trust laws
FISMA	Gramm-Leach-Bliley	ECPA
CFIUS	TINS	ISM

## Annotated Bibliography

### Basic

- European Parliament. Cybersecurity Act: Build Trust in Digital Technologies. [online] Available at: <http://www.europarl.europa.eu/news/en/press-room/20180710IPR07605/cybersecurity-act-build-trust-in-digital-technologies> [Accessed 2 Nov. 2018].

### Suggestions for further reading

- How Israel Rules The World of Cyber Security by VICE News, [Youtube Video], Available at <https://www.youtube.com/watch?v=ca-C3voZwpM>
- "How to manage the computer-security threat", The Economist, 8<sup>th</sup> Apr 2017, Available at: <https://www.economist.com/leaders/2017/04/08/how-to-manage-the-computer-security-threat> [Accessed 6 Dec 2018]
- "A large-scale cyber-attack highlights the structural dilemma of the NSA", The Economist, 13<sup>th</sup> May 2017, Available at: <https://www.economist.com/science-and-technology/2017/05/13/a-large-scale-cyber-attack-highlights-the-structural-dilemma-of-the-nsa?zid=291&ah=906e69ad01d2ee51960100b7fa502595> [Accessed 6 Dec 2018]

## Self-Assessment Exercises

### Exercise 6.1

Explain the Australia Cybersecurity laws. How are those compared to the German Cybersecurity laws?

## Recommended time for the student to work

15 hours

### Summary

In this week we will take a closer look at the cybersecurity strategies of countries such as the People's Republic of China, Mexico and Singapore.

### Introductory Remarks

#### People's Republic of China

The PRC Criminal Law broadly prohibits anyone from illegally obtaining personal data of others by stealing or any other means. If the circumstances are serious, the offender could be subject to imprisonment of up to three years and/or a fine. Where any entity commits such offence, it shall be fined, and the person in charge and other responsible personnel of the entity may also be subject to criminal penalties. The Decision of the Standing Committee of the National People's Congress on Strengthening the Protection of Network Information also provides administrative penalties for stealing or otherwise illegally obtaining personal data of others, and selling or otherwise illegally providing personal data of others.

These penalties include warnings, fines, confiscation of illegal gains, revocation of business license, closure of website, prohibition of the responsible personnel from engaging in internet services as well as being recorded on the social credit files and disclosed to the public. In serious cases where the infringement on personal data constitutes acts against public security administration, the offender may be subject to penalties including warnings, fines and/or administrative detention of up to 20 days, according to the Law of the PRC on the Imposition of Penalties in connection with the Administration of Law and Order. Please note that the laws mentioned above do not specify what constitutes "illegally obtaining" personal information. It is possible that under a broad interpretation, the term would cover unauthorised assess of data as well as storage of data depending on the intent of the offender. In addition to criminal and administrative penalties, the PRC Tort Liability Law establishes a private right of action for infringement of one's right to privacy. The infringed party may seek compensation for actual

losses (or profits arising from the infringement if actual losses cannot be determined) and where applicable, damages for emotional distress, in addition to other remedies provided under the law (e.g. cessation of infringement, return of property, apology from the infringer, restoration of reputation, etc.).

Given the potentially broad scope of privacy rights, if a person accessed the personal data of others without authorisation or stored data which has been accessed without authorisation, such person may be subject to civil liabilities for infringement of the privacy rights of others. Where the above infringement is committed by an internet user through the internet, the internet content service provider shall be jointly and severally liable with the internet user if:

- a. after being notified of the infringement, the internet content service provider fails to take necessary actions to remedy the infringement (such as deleting or blocking the infringing web content or disconnecting the link), which causes additional harm to the infringed party, or
- b. if the internet content service provider is aware that the internet user is committing the infringement through its internet services and fails to take necessary measures.

## **Mexico**

There appears to be a significant lack of legislation compared to the other examined jurisdictions. Mexican data privacy rules contain some provisions on cybersecurity measures and there are, reportedly, agencies in Mexico working with incident reporting and governmental cooperation. However, the lack of legislative action reputedly is hampering this work. Mexico is seen as a high-risk country for both inbound and outbound attacks.

Mexico has recently adopted the international Wassenaar Arrangement and therefore implemented export control rules on information security items.

The Federal Criminal Code lists some criminal offences, which appear also to cover cybercrime. Mexico has reportedly adhered to the Budapest Convention, but it is not reported as a signatory. At present, it appears Mexico lacks substantive laws prohibiting cybercrime and attempts to introduce legislation have been scrapped.



Figure 7 China, Mexico and Singapore Map (Source [www.sinoptic.ch](http://www.sinoptic.ch))

## Singapore

Under the Personal Data Protection Act 2012 (PDPA), it is an offence to collect personal data without the data subject's consent, unless an exception applies. It is also an offence under the PDPA for a person to make a request to obtain access to or to change the personal data about another individual, which is in the possession or under control of an organisation, without the authority of that individual. Under the Computer Misuse and Cybersecurity Act (CMCA), it is an offence to knowingly cause a computer to perform any function for the purpose of securing access without authority to any data held in any computer. Further, a plaintiff may make a claim under tort for, amongst others, conversion or breach of a duty of confidentiality. Is there a legal mechanism whereby you can seek access to or retrieve the copy of data which has been accessed without authority? Is there a legal mechanism that enables you find out information about who may have accessed your data without authority and/or how it was used? There are various possible mechanisms, depending on the circumstances:

The matter may be referred to the police for criminal prosecution via a complaint. While the assistance of the police may be sought, the complainant strictly has no control over the conduct of the matter by the police and has no right to request information or documents from the police. It is within the police's discretion whether it chooses to reveal anything to the complainant.

Civil proceedings for, amongst others, breach of confidence may also be commenced. As part of the final relief in such civil proceedings, the complainant may seek an injunction for the delivery

up, return and/or deletion of the data which has been accessed without authority, damages and/or an account of profits. There are also various interim measures or forms of injunctive relief available, for example:

an application for a search and seizure order, for permission to search, inspect and either copy or remove documents in the possession of the defendant(s), when there is (amongst other requirements) a grave danger that the defendant(s) will dispose of or destroy incriminating evidence in his/her possession. These documents which are seized are not ordinarily provided to the plaintiff immediately, but an order may be made for inspection by the plaintiff of those documents;

- a. an application for interim injunction to, amongst other things, restrain the defendant(s) from using and/or disclosing such data pending the final resolution of the civil proceeding;
- b. the process of general and/or specific discovery, interrogatories and/or further and better particulars of pleadings, may be applicable.

If the identity of the person who either committed the data breach or is storing or has stored the data at some point in time is unknown and/or civil proceedings have not been commenced, the complainant may make an application for pre-action discovery or pre-action interrogatories against known parties who may be involved. Such applications, if successful, may require an individual or company to produce documents or answer questions so that either the identity of the potential defendant(s) may be determined or the plaintiff can assess whether there is a case to be made.

## Aim/Objectives

The purpose of the 7<sup>th</sup> Week is to introduce the cybersecurity laws of several countries around the world. We introduce the paradigms of People's Republic of China, Mexico and Singapore.

## Learning Outcomes

After the successful completion of the 7<sup>th</sup> Week, students should be able to:

- Evaluate the cybersecurity laws in the People's Republic of China
- Evaluate the cybersecurity laws in Mexico
- Evaluate the cybersecurity laws in Singapore

## Key Words

Tort Liability Law	Infringement	High-Risk
Criminal Code	Budapest Convention	PDPA
CMCA	Civil Proceedings	Authority

## Annotated Bibliography

### Basic

- Singapore Government. Cybersecurity Act. [online] Available at: <https://www.csa.gov.sg/legislation/cybersecurity-act> [Accessed 2 Nov. 2018].

### Suggestions for further reading

- Cybersecurity and the world: A time to reflect, a time to act, by Microsoft Today in Technology [Youtube Video], Available at <https://www.youtube.com/watch?v=CJO2Lz8dHm8>
- New cyber security centre to boost ASEAN's capabilities [online] Available at: <https://www.straitstimes.com/singapore/new-cyber-security-centre-to-boost-aseans-capabilities> [Accessed 7 Dec 2018]

## Self-Assessment Exercises

### Exercise 7.1

Explain Singapore Cybersecurity laws. What are the differences between Singapore, Australia and Germany when it comes to Cybersecurity laws?

## Recommended time for the student to work

15 hours

## Summary

In this week we will take a look at some emerging technologies, and the positive or negative impact they will have in the area of Cybersecurity.

## Introductory Remarks

The war between security experts charged with the responsibility of protecting information and cyber-criminals who threaten to compromise the integrity of data for different entities has become a cat and mouse game. For instance, as soon as white hats counter one form of malicious behaviour using encryption tools, there is the almost immediate development of yet another malevolent form of threat for information systems.

The increasing digital connectivity and the automation of virtually all processes in the world of business throughout the whole value chain have led to the creation of agility. This has also led to the development of extremely high levels of threat and significantly raised the risk of cybersecurity. The building of cyber-security into applications is critical in addressing such risks, as well as all the devices that are interconnected from the very beginning. In this week, we are going to highlight the emerging technologies that will boost the security of information systems from being compromised by hackers.

### Hardware Authentication

It is a well-known fact that passwords and usernames used by a majority of data users are weak. This makes it easy for hackers to get access to the information systems and compromise sensitive data of a business entity or government agency. In turn, this has exerted pressure on experts of systems security to come up with authentication methods that are more secure. One of the ways that has been used is the development of user hardware authentication. Tech companies have developed a solution in the user authentication process with a new Core vPro processor that

belongs to the sixth generation of processors. The core vPro can combine different hardware components with enhanced factors simultaneously for user identity validation purposes.

The tech company Intel has built on previous experiences and mistakes and dedicated a portion of the processor for security reasons to make a device part of the entire process of authentication. Hardware authentication can be especially important when it comes to the Internet of Things where the network of connected devices ensures that any device that seeks to be connected has the rights for connectivity to that particular network.

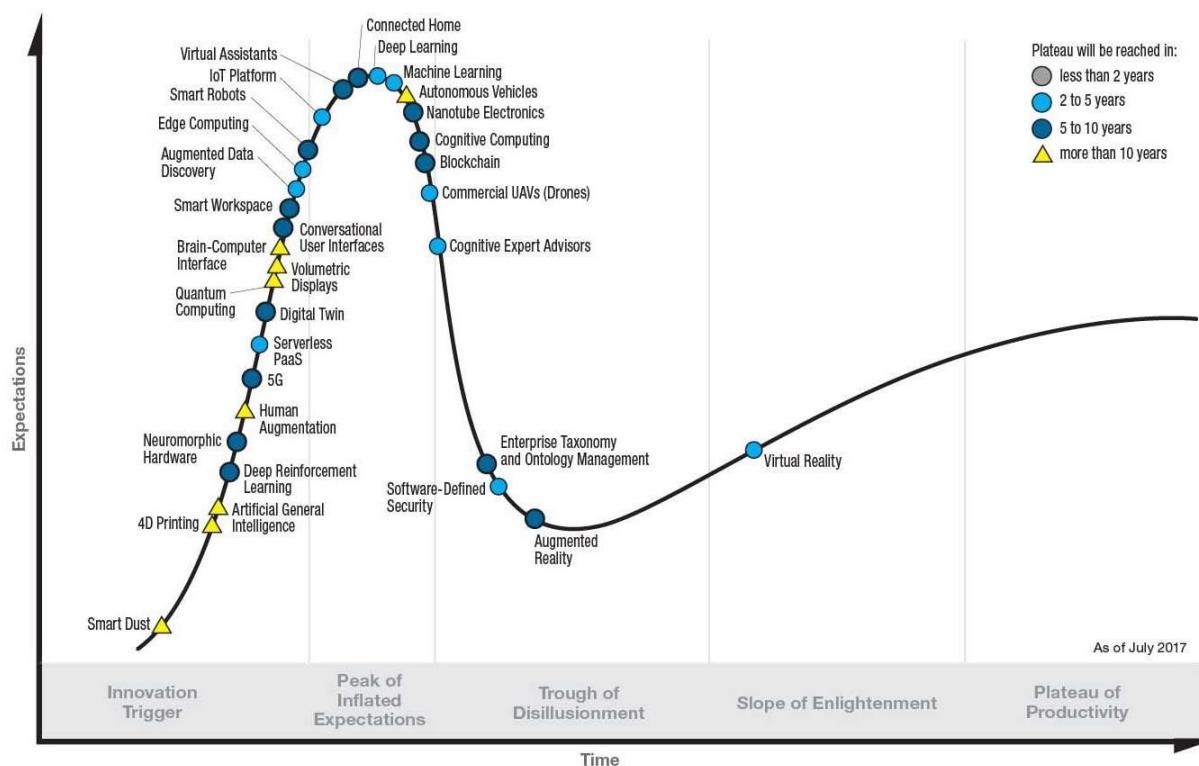


Figure 8 Gartner Hype Cycle for Emerging Technologies in 2017 (Source [www.gartner.com](http://www.gartner.com))

## Cloud Technology

The cloud is set to have a significant impact on the transformation of systems security technology. More business enterprises and government agencies have embraced cloud technology to store the vast amounts of information that they generate on a daily basis. There will be more approaches to information systems security that will be developed for use in the cloud. Techniques for on-premise data storage will be migrated to the cloud. Components such as virtualized intrusion detection and prevention systems, virtualized firewalls and virtualized systems security will now be used from the cloud as opposed to the traditional forms.

For instance, both private and public entities have doubled up their data center security by the use of IaaS services, such as Firehost and Amazon. Another perfect example of certified secure enough services that are based on the cloud is the GSA FedRAMP, which makes it easier for the small to medium-sized business enterprises to have a data security center that is above average.

## **Deep Learning**

Some technologies are encompassed in deep learning, such as machine learning and artificial intelligence. There is a significant deal of interest for purposes of systems security in these technologies.

Deep learning, just like behaviour analytics, focuses on anomalous behaviour. Whenever AI and machine learning systems are fed with the right data regarding potential systems security threats, they can make decisions on how to prevent hacks depending on their immediate environment without any human input.

The system scrutinizes entities instead of users that have access to the information system. The most recent developments in machine learning technology and exact business analytics means that we can now be able to analyse the different entities that are found in the enterprise at both the macro and the micro levels. Business organizations and government agencies can now be able to stamp out any persistent or advanced cyber threats using artificial intelligence and machine learning.

As you can see, attacks can come from any loose end. It is important to keep up with the latest technologies as to not only stay updated but safe, as well. This is not to say that our current security procedures are for naught, however.

We should be leveraging these new technologies with the existing fundamentals that are in place. It is important to remember that a large percent of breaches come from not securing critical security controls. By combining new technologies with fundamental security controls, you will have the confidence that your information is safe and out of reach.

## **Aim/Objectives**

The purpose of the 8<sup>th</sup> Week is to evaluate cybersecurity problems due to emerging technologies. We discuss technologies such as hardware authentication, cloud technology and deep learning.

## Learning Outcomes

After the successful completion of the 8<sup>th</sup> Week, students should be able to:

- Evaluate emerging technologies cybersecurity threats
- Explain hardware authentication and the effects on cybersecurity
- Explain cloud technology and the effects on cybersecurity
- Explain deep learning and the effects on cybersecurity

## Key Words

Interconnected	Compromised	Core vPro
6 <sup>th</sup> Gen Processors	GSA FedRAMP	IaaS
Critical Security	Fundamental	Technologies

## Annotated Bibliography

### Suggestions for further reading

- New Cyber Security Technologies and Cyber Threat Solutions - Check Point Software Technologies, Ltd. [Youtube Video], Available at: <https://www.youtube.com/watch?v=f2-cwx23Kg4>
- Emerging Technologies and Cybersecurity [Online] Available at: <https://www.securityprivacybytes.com/2018/04/emerging-technologies-and-cybersecurity/> [Accessed 6 Dec 2018]

## Self-Assessment Exercises

### Exercise 8.1

Explain hardware authentication and the effects on cybersecurity

## Individual Assignment (20 points)

The individual assignment includes solving questions related to the syllabus covered in this course. The questions can vary from practical ones, to essay style questions asking to use your

current skills in order to describe, evaluate, compare or even propose solutions to existing problems and cyber security uses.

This individual assignment counts 20% of the final course mark.

You will need approximately 20 hours to solve this Individual Assignment.

### **Recommended time for the student to work**

35 hours

### Summary

In this week we will take a look at some examples of companies and countries that have used Cybersecurity in order to grow their business or even the industrial sector of the country.

### Introductory Remarks

Cybersecurity is one of the fastest growing industries in the world. Projections anticipate that global spending on cybersecurity products will reach \$1 trillion cumulatively over the next four years and that cybersecurity unemployment will remain at zero percent over that period of time as job openings continue to outpace supply. With such dramatic growth, the cybersecurity industry has the potential to function as a major driver of economic growth. In regions where cybersecurity industry “clusters” have popped up, this regional concentration can produce substantial contribution to the local economy. Given the positive future projections of the overall need for cybersecurity, national and local governments are actively seeking to attract and develop cybersecurity capacity. As the Christian Science Monitor noted, many localities want to incubate cybersecurity industry clusters, but few have achieved this goal.

In this week, we will look at three different cases (countries) that vary in geography, structure, and stage of development. To explain the emergence of competitive industries and the increased output from a specific region, a branch of development theory has focused on the positive inputs and externalities created by agglomeration economies, otherwise known as “clusters.” The concentration of firms supports the development of regional clusters by:

- a. Lowering input costs, such as skilled talent, capital, and technology through economies of scale; and
- b. Facilitating productivity growth through information sharing and knowledge spillover so each firm produces more output per input.

Existing cluster literature highlights four main pillars of innovation economies: social and business networks, research institutes and universities, relevant industries and sectors, and government policies.



Figure 9 How does your organization manage its cybersecurity risks? (Source [www.connectedfutures.cisco.com](http://www.connectedfutures.cisco.com))

## Israel

Israel Aerospace Industries Ltd. (IAI), the country's largest aerospace and defence company, said it has set up a special division to deal with the cyber business of its subsidiary ELTA Systems Ltd., a defence electronics company. The IAI has appointed Esti Peshin as the general manager of the division. The government-owned company, which manufactures military and civilian aircraft and products, said it ended 2016 with contracts totalling over \$100 million in the fields of cyber-intelligence, cyber-forensics and analysis, and cyberdefense centres.

"We consider cyber to be a strategic field of activity and a growth engine at IAI, and expect it to continue to expand significantly in the coming years," said Joseph Weiss, IAI's president and CEO, in a statement. "The establishment of IAI's Cyber Division serves as infrastructure for continued extensive activity. We will continue to invest in cyber companies and research and

development centres in order to continue to expand in this field." IAI sees cybersecurity as a strategic field and source of growth. The company is developing cyber solutions and advanced capabilities for intelligence, monitoring, identification and accessibility, offering clients tools to tackle cyberthreats. IAI operates R&D and innovation centers in Singapore, Switzerland and Israel. The company also leads the Israel Cyber Company Consortium (IC3) which comprised of leading Israel cyber companies.



Figure 10 Map of Israel (Source [www.worldatlas.com](http://www.worldatlas.com))

Israel is seen as a global leader in cybersecurity. Sixty-five new cyber startups were set up in Israel in 2016, and the nation maintained its leading position as a global center of cybersecurity innovation, a report by the non-profit Start-Up Nation Central revealed. A record \$581 million of capital was raised by cybersecurity startups last year in Israel, a 9 percent increase compared to 2015. This amount was second only to the US, and accounted for 15% of the total venture capital raised by cybersecurity companies globally. At the end of 2016 there were 365 cybersecurity companies active in Israel, compared to 187 in 2012, according to data compiled by Startup Nation's database and PitchBook.

## Singapore

Investing in cyber security would not just reap gains in keeping Singapore secure - it could also be a source of revenue and growth, Minister for Communications and Information Yaacob Ibrahim

told Parliament. By 2020, the cyber security market here could generate \$900 million in revenue, he said in response to a question about how a supportive ecosystem could contribute to cyber security.

"Besides undergirding the digital economy, cyber security is also a growth engine," said Dr Yaacob, who also addressed a concern that Singapore could be a target of cyber attacks due to its connectedness. He also announced Singapore's first cyber security start-up hub, the Innovation Cybersecurity Ecosystem at Block 71 (ICE71), which opened in April 2018. ICE71 cultivates cyber security innovation by providing a supportive ecosystem that helps entrepreneurs develop their ideas and instil in them the knowledge to grow their businesses. Over the next two years, ICE71 aims to train up to 100 people and help 40 start-ups. CSA will also establish a new funding scheme to encourage projects that meet Singapore's cyber security needs. Local companies can qualify for funding of up to \$500,000 in areas such as managed security services, consulting services, forensics and authentication.

According to market research firm IDC, cyber security has been estimated to attract spending of US\$105 billion (S\$138 billion) in Asia Pacific by 2020. Dr Yaacob said 20,000 more training places will be created for the information and communications technology (ICT) workforce, under the Tech Skills Accelerator (TeSA) programme, over the next three years. This will cost \$145 million, and the Government hopes that by 2020, TeSA would have trained 47,000 ICT workers. Introduced in April 2016, TeSA is a SkillsFuture tripartite initiative to train and build the ICT workforce.

Senior Minister of State for Communications and Information Janil Puthucheary said TeSA will work closely with the ICT industry to develop more programmes in "frontier technology areas", including data analytics, artificial intelligence, the Internet of things and cyber security. He said mid-career professionals, managers, executives and technicians (PMETs) will not be left behind. "In line with our commitment to develop our people, TeSA will also strengthen our support for those who might need it most, such as mid-career ICT PMETs in search of new job opportunities as the economy and the ICT job landscape evolve," he added.

## Aim/Objectives

The purpose of the 9<sup>th</sup> Week is to see how cybersecurity can be an engine for economic growth. We explain the cases of Israel as well as Singapore and we observe how cybersecurity changed the scenery in these countries.

## Learning Outcomes

After the successful completion of the 9<sup>th</sup> Week, students should be able to:

- Evaluate how cybersecurity can help on the economic growth of a country
- Evaluate the case of Israel
- Evaluate the case of Singapore

## Key Words

Startups	Input Costs	Skilled Talent
Technology	Economy Scale	Knowledge
Business Network	Research	Industry

## Annotated Bibliography

### Basic

- Steve Morgan. Cybersecurity Industry Outlook 2017-2021 [online] Available at: <https://www.csoonline.com/article/3132722/security/cybersecurity-industry-outlook-2017-to-2021.html> [Accessed 4 Nov. 2018].

### Suggestions for further reading

- New Cyber Security Technologies and Cyber Threat Solutions by Check Point Software Technologies, [Youtube Video], Available at <https://www.youtube.com/watch?v=f2-cwx23Kg4>

## Self-Assessment Exercises

### Exercise 9.1

Evaluate the case of Israel, giving appropriate examples. Try to compare it with other countries and find similarities and/or differences.

## Recommended time for the student to work

15 hours

## Summary

In this week we will take a look at some future research directions in cybersecurity as well as some challenges cybersecurity faces that could be a very important area for research.

## Introductory Remarks

With the tremendous growth in the Internet availability and the advancement of Internet enabled devices, an increasing number of populations use the Internet in all wakes of their lives, often exposing highly sensitive personal information without realizing the consequences of data misuse. We speculate that the issues surrounding the end-user privacy will continuously grow into the future in accordance to the growing volume of personal information over the Internet. In addition, usability issues are gaining more attention as a way to provide end-user focused security mechanism where the users can

intuitively learn and use them, without complexity or deep learning curve, to protect their data. Traditionally the practice in the cybersecurity community has been based on incremental patches which rectify the current security and privacy issues and then moves onto next step. Some believe that this incremental approach has not worked well and will not be able to accommodate future needs since the original Internet was invented for a very different environment than how it is used today. An approach to think “outside box” without relying on the current computing system and the Internet but starting something afresh has been suggested to make a better use of the fast growing demands of the Internet. Anonymous nature of the Internet has been defined as a source of the increasing cyber-attack and difficult to trace the offender. The global scale identity management and traceback techniques have become an active area of research as a strategic plan to thwart increasing number of cyber attackers in the future, especially when the critical infrastructure is involved. We delve into more detailed of these speculated future research directions in the following sections.

## **Focus on privacy**

In recent years, privacy has become a critical issue in the development of IT systems with the widespread of networked systems and the Internet. Now, the Internet is used in all walks of our lives demanding increasing volume of personal information to be entered in the cyberspace. This increase in online shopping suggests that the Internet users are becoming more comfortable sharing their sensitive financial information, such as credit card numbers and shipping addresses. Similarly, professional and social networking sites that connect people with similar interests online have seen an exponential growth in last decade. LinkedIn, a professional networking site founded in May 2003, have 200 million users by January 2013. Facebook, launched in February 2004, have reached 1 billion active users as of September 2012.

These numbers indicate that people increasingly feel comfortable putting personal information about themselves online. Individuals also appear more willing to speak out about what they perceive as invasion of privacy when engaging in online activities. As increasing volume of information is being put in the Internet, the chances of occurrence of compromise of privacy also increase. For example, individual's online visits are watched to infiltrate the information and send advertising based on one's browsing history. The methods of compromise can range from gathering of statistics on users, to more malicious act such as the spreading of spyware. Cyber criminals use the social networking sites to steal personal information to use in fraud and identity theft. To prevent such privacy leakage, several social networking sites provide privacy measures. The goal of privacy-aware security is to enable users and organizations to better express, protect, and control the confidentiality of their private information, even when they choose to (or require to) share it with others. One stream of research in this field concerns with the way data is accessed and disclosed while protecting privacy. A number of researches are conducted to investigate how to selectively disclose the data, how to protect the data that are shared by people, and how to sanitize the data. Another stream of research conducted in this area concerned with the development of specification framework to build and reinforce privacy policy. Development of building a number of specifications for providing privacy guarantees such as languages for specifying privacy policies, specifications for violations of privacy, and detecting violations of privacy is an active research area. Building techniques for data policy for data collection, data sharing and transmission, and dealing with privacy violations are other active areas of research in this category.

## **Next generation secure internet**

There is no doubt that the Internet has been a social phenomenon that has changed, and continues to change how humans communicate, businesses work, how emergencies are handled, and the military operates among many other things. Despite the Internet's critical importance, some portions of the Internet is fragile and the constantly under incessant attacks that range from software exploits to denial-of-service. One of the main reasons for these security vulnerabilities is that the Internet architecture and its supporting protocols were primarily designed for a benign and trustworthy environment, with little or no consideration for security issues. This assumption is clearly no longer valid for today's Internet, which connects millions of people, computers, and corporations in a complex web that spans the entire globe. In the past 30 years, the Internet has been very successful using an incremental approach where a system is moved from one state to another with incremental patches. However, some believe that the entire Internet technology has now reached a point where people are unable to experiment new ideas on the current architecture. For example, a best effort delivery model of IP is no longer considered adequate without added security assurance. Routing is no longer based on algorithmic optimization, but rather has to deal with policy compliance to accommodate a wide range of applications. Protocols designed without concern for energy efficiency cannot integrate energy conscious embedded system networks such as sensor networks. Initial projections about the scale of the Internet have long since been invalidated, leading to the current situation of IP address scarcity.

A new paradigm of architectural design described as "clean-slate design" has been suggested. The theme of "clean-slate design" is to design the system from scratch without being restrained by the existing system, providing a chance to have an unbiased look at the problem space. However, the scale of the current Internet forbids any changes, and it is extremely difficult to convince the stakeholders to believe in a clean-slate design and adopt it. There is simply too much risk involved in the process. The only way to mitigate such risks and to appeal to stakeholders is through actual Internet-scale validation of such designs that show their superiority over the existing systems. Despite the risk, research funding agencies all over the world have realized this pressing need and a world-wide effort to develop the next generation Internet is being carried out. The National Science Foundation (NSF) was among the first to announce a GENI (Global Environment for Networking Innovations) program for developing an infrastructure for developing and testing futuristic networking ideas developed as part of its FIND (Future Internet Design) program. The NSF effort was followed by the FIRE (Future Internet Research and Experimentation) program which support numerous next generation networking projects under

the 7th Framework Program of the European Union, the AKARI program in Japan, and several other similarly specialized programs in China, Australia, Korea, and other parts of the world.

### **Towards trustworthy systems**

Most of today's systems are built out of untrustworthy legacy systems using inadequate architectures, development practices, and tools. Hence, they are typically not well suited to deal with the attacks in cyberspace. Matters get worse as the modern devices are themselves networks of systems and components. They need to interact in complex ways with other components and systems, sometimes producing unexpected and potentially adverse behaviour. Historically, many systems claimed to have a trustworthy computing base (TBC) that was supposed to provide a suitable security foundation to safeguard the critical components. For example, error-correcting codes were developed to overcome unreliable communications and storage media. Encryption has been used to increase confidentiality and integrity despite insecure communication channels. Similarly, firewalls have been used to protect inside assets from outside attacks. However, the idea of having one specific solution to a particular problem has not been successful due to the continuous evolution of attacks.

The term trustworthy systems have been defined by the Department of Homeland Security (DHS) in US as a long-term goal to indicate a computing system that is inherently secure, available, and reliable, despite environmental disruption, human user and operator errors, and attacks by hostile parties. Towards this goal, the author advocates the requirement for secure hardware and software combinations as essential building block towards trustworthy system. In the proposal, systems and devices share provable and standard trust information confirming their trustworthiness, generic security-assured

commodity hardware solutions at all levels, and systems able to determine whether to trust a device, software package, or network based on dynamically acquired trust information rooted in hardware and user defined security policies. Towards this goal, a several threads of research work have been carried away in the areas of trustworthy isolation technique, separation and virtualization in hardware and software, analyses that could greatly simplify evaluation of trustworthiness before putting applications into operation, robust architectures that provide self-testing and self-diagnosing, self-reconfiguring, compromise resilient, and automated remediation.

### **Global-scale identity management and traceback techniques**

Identity management is the task of controlling information about users on computers. Such information includes information that authenticates the identity of a user, information that describes information and actions they are authorize to access and/or perform. It also includes

the management of descriptive information about the user and how and by whom that information can be accessed and modified. Managed entities typically include users, hardware and network resources and even applications. There are many current approaches to identity management. For example, many websites employ logging in process with username and password combination to screen only eligible users to enter into the service. However, many of these are not yet fully interoperable with other services across different organizations and scalable. They are only for single-use or limited in other ways. It has been pointed out that due to the lack of adequate identity management it is often extremely difficult to trace identity theft. Global-scale identity management concerns identifying and authenticating entities such as people, hardware devices, distributed sensors and software applications when accessing critical information technology systems from anywhere. The term global-scale is intended to emphasize the pervasive nature of identities, due to increasing use of mobile phones and embedded sensors in everywhere of our daily life. This also implies the existence of identities in federated systems that may be beyond the control of any single organization.



Figure 11 Phishing Scams (Source [www.dilbert.com](http://www.dilbert.com))

### Usable security

As the range of potential threats over the Internet expands, end users are increasingly find themselves in a position having to make security decisions, for example through configuring security-related settings, responding to security-related events and messages, or enforced to specify security policy and access rights. Unfortunately, experience suggests that although security features are often provided, they are conveyed in a manner that is not understandable or usable for many members of the target audience. As most users unable to comprehend the security features on offer, many security enhancements remain unused leaving the end users in a vulnerable position from malicious attacks. The need for usable security and the difficulties inherent in realizing adequate solutions are increasing being recognized. Many security

technologies have tried to improve the usability aspects; most of which fall short in terms of usability. Password schemes have been believed to be one important parts of usable security. Therefore, several elaborate procedures have been progressed such as frequency of changing, inclusion of non alphabetic characters, or visual and biometric based passwords that users do not have to remember. Despite these attempts, security pitfalls of poorly implemented password schemes have been extensively documented over the years. Users resort to writing them on slips of paper or storing them unencrypted on handheld devices. Mail authentication is another active area where usable security has been studied in a form to authenticate senders of valid emails. Security pop-up dialogs and SSL lock icons also have been proposed. Another issue that makes it difficult to devise an effective usable security scheme is that usability of systems tends to decrease as attempts are made to increase security. For example, some email system requires users to re authenticate in a regular time to assure that they are actually the authorized person. In another example, some web browsers warn users before any script is run. But users may still browse a web server that has scripts on every page causing pop-up alerts to appear on each page. The potential impacts of security that is not usable include increase susceptibility and vulnerable from social engineering type of cyber-attacks.

## Aim/Objectives

The purpose of the 10<sup>th</sup> Week is to evaluate the future research direction when it comes to cybersecurity. We discuss areas such as privacy, next-gen secure internet, trustworthy systems, usable security as well as global-scale identity management.

## Learning Outcomes

After the successful completion of the 10<sup>th</sup> Week, students should be able to:

- Evaluate future research directions in cybersecurity
- Explain the research in the privacy sector
- Explain the research in next-get secure internet

## Key Words

Traceback	Privacy	Cyber Attacks
Social	Complex Web	Clean-Slate Design
Trustworthy	Global-Scale	Usable

## Annotated Bibliography

### Suggestions for further reading

- Top Five Emerging Cybersecurity Challenges, Srinivas Sampalli, TEDxDalhousieU - TEDx Talks [Youtube Video], Available at: [https://www.youtube.com/watch?v=yIxd\\_UwgvJU](https://www.youtube.com/watch?v=yIxd_UwgvJU)

## Self-Assessment Exercises

### Exercise 10.1

Explain the term usable security. What effects does that have both from the scientific/security point of view as well as in users life.

### Activity (5 points)

Activity that includes solving questions related to the syllabus covered in this course, as well as applying the knowledge gathered up to this week in order to solve problems related to cybersecurity and its current trends.

This activity counts 5% of the final course mark.

You will need approximately 5 hours to solve this Graded Activity.

### Recommended time for the student to work

20 hours

## **Summary**

In this week we will take a look at several activities happening around the world as well as in Cyprus in order to raise cybersecurity awareness as well as educate the public.

## **Introductory Remarks**

### **The Cyber Security Month**

The awareness campaign, which first began in the US in 2004 before spreading to the EU in 2012, is part of a major effort to promote cyber security issues and educate the public on the dangers of online attacks.

Cyber security has become an increasingly risky area in recent years, with the World Economic Forum's Global Risks Report 2018 naming cyber attacks as the third top cause of global disruption over the next five years, behind natural disasters and catastrophic weather events. In order to protect against such occurrences, both businesses and individuals are encouraged to increase their awareness of the potential risks in order to improve their safety.

Google also offers a security check-up as part of the campaign. The check-up involves analysing issues within four separate sections: 'Your devices', 'recent security events', 'sign-in and recovery', and 'third-party access'.

Through these sections, Google account holders will be informed of any unusual activity on their account, such as signing in from new devices or sensitive account setting changes.

Google also encourages users to remove old devices with access to their account if they haven't been used for a long period of time.

A number of other organisations and businesses have been participating in the campaigned in Europe and the US, with the Better Business Bureau in the US offering a number of tips for staying safe online throughout the month.

Advice from the bureau includes avoiding suspicious links and attachments, sticking to trustworthy websites, improving the strength of passwords, and updating security protection software on computers and other devices.

Security experts have also issued their own warnings about cyber safety, including Jake Moore from antivirus software firm ESET, who praised Google's initiative.



Figure 12 Safer Internet Day 2018 Flyer (Source [www.saferinternetday.org.uk](http://www.saferinternetday.org.uk))

### **U.S. Department of Homeland Security**

The Department of Homeland Security in the US, has the “Stop. Think. Connect” campaign which is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. They create posters/flyers which they distribute to schools as well as in general public, educating the population on the risks of online exposure as well as ways to be more secure online. They even create videos that are shown in schools to educate the younger population. In addition, they organise the National Security Awareness Month (NCSAM).

### **Cyprus**

eSafeCyprus (in which EUC is a partner) is the national strategy for Internet safety for children, teachers and parents. The design a national strategy for information and education on digital security issues addressed to children, teachers and parents in order to become more critical, creative and responsible users of digital technologies and to develop a culture of safe exploitation of the potential of digital technologies.

eSafeCyprus has several events, presentations as well as it provides helpful information and applications from partners such as the “Safe Internet Filter for Fixed Connections”, and “Cleanfeed”, presentations regarding cyber security at several places and institutes. It also provides training for teachers so they can pass on the information to children and students. In addition it has the “ESafetyLabel” certification.

## Aim/Objectives

The purpose of the 11<sup>th</sup> Week is to indicate that there are several campaigns around the world that are created to educate the public about cybersecurity threats.

## Learning Outcomes

After the successful completion of the 11<sup>th</sup> Week, students should be able to:

- Evaluate USA campaigns
- Explain the need for cybersecurity public education

## Key Words

DHS	Initiative	Campaign
Flyer	Security Tests	Checkup

## Annotated Bibliography

### Basic

- World Economic Forum. The Global Risk Report 2018 [online] Available at: <https://www.weforum.org/reports/the-global-risks-report-2018> [Accessed 4 Nov. 2018].

### Suggestions for further reading

- Accountability & Responsibility in a digital World by Paul Davis, TEDx Talks [Youtube Video], Available at <https://www.youtube.com/watch?v=zaEn0BQS0vY>
- eSafeCyprus, Strategy for safety in the Internet, Available at <https://www.esafecyprus.ac.cy/>

## **Self-Assessment Exercises**

### **Exercise 11.1**

Explain what is the Cybersecurity month. Visit the eSafeCyprus website and find out if they have similar events (i.e. Safer Internet Day), and explain the events organized.

### **Recommended time for the student to work**

15 hours

## CYBER SECURITY CASE STUDIES

12<sup>th</sup> Week

### Summary

In this week we will discuss a cybersecurity case study of a company that works in the area of ships.

### Introductory Remarks

This case study was prepared to show a ‘real life’ snapshot of a company that is a Ship owner, Technical Operations Manager, and Crew Manager and how they, in the early stages, are evaluating and implementing a program of cyber security for their ships with Online Connectivity. They have been asked several general questions on general subjects to help scope how this company is initially viewing cyber security, and their efforts to organise internally by assigning responsibilities and allocating resources of staff and budget. They have been purposely general in nature to help identify certain concepts that may be of help. It should be recognised that this is not an all-inclusive guidance or evaluation, and does not critically assess their efforts. It is rather intended to contribute to the greater discussion of maritime cyber security by exposure to what is likely a typical case and find some value to their cyber security efforts.

The company owns and/or operate over 100 ships which include tankers, bulkers, and container ships. They employ directly over 3,000 employees in seven offices worldwide. The company operates as an owner and technical operator, including crewing services. Driving this shipping company’s cyber security initiatives is the increasing awareness of the invasive nature of cyber-criminal activity in the shipping industry. Cyber threat has imposed an elevated cyber security related risk awareness from ship owners, the company board of directors, cargo owners, and legal / regulatory bodies such as TMSA, IMO and USCG to name some, as well as P&I club coverage.

- a. “Reducing the risk should be the main deliverable of the company’s cyber security strategy and outcome of the risk assessment decided by senior management. At a technical level,

this would include the necessary actions to be implemented to establish and maintain an agreed level of cyber security.

- b. Ships entering / leaving management pose added challenge to maintaining a uniform application of a cyber security program as each ship differs in communication systems, ship technology, and operations budget. Efforts to establish a fleet wide standard cyber security strategy is an efficient way to maintain a consistent and effective level of defense and response across a fleet. “A further complexity is that shipping lines operate a mix of vessels which they either own or charter for a short period of time...” .
- c. Company employees, port agents, service vendors, equipment manufacturers, and crewing services do introduce a significant cyber security risk for a ship’s commercial operations due to the large number of persons routinely visiting the ship or joining as crew. These ship visitors are often routine in nature and are left minimally monitored while they complete their tasks onboard. There is no company cybersecurity policy in place for ship related services that use the ships network.
- d. Knowing who is using your ship network and for what purpose is important and a real concern relating to cyber security. Discovering early malicious intent, unintentional mistakes, or poor cyber security practices are a risk that needs to be addressed. Ship network monitoring and analysis is one way to have this capability.
- e. There is a need to have a clear policy and practical procedures for all crew and visitors who use the ship’s network in the cyber security policy and proper use expectations.
- f. Cyber Incident insurance coverage will grow in importance as a part of a company’s risk management strategy. Underwriters will require certain cyber security standards and routine audits for coverage. Using their assessment and audit standards is a good start and should be reviewed for applicability to your cyber security strategy and for possible future insurance coverage.

“Currently, the company is undergoing a transition from the current Fleet Broadband communication services to a higher broadband capable VSAT system. This ‘open to the internet’ situation will drive the company towards more vigilance and the need for a Cyber security program to be put in place

- a. “The rapid development in maritime broadband satellite coverage combined with the introduction of highly sophisticated equipment, such as computer controlled engine systems, has changed the structural risks to maritime vessels. Ships are no longer

protected by an air-gap from external systems. Today, an estimated 30,000 vessels globally have equipment providing them with constant internet access, which is an increase from only 6,000 in 2008. Even if networks on board are separated between systems for ship operation, crew welfare and remote access to suppliers, separations can over time be compromised by ad hoc interventions by the crew or suppliers, for instance in connection to maintenance...”.

- b. “Cyber security refers to the security of information networks and control systems and the equipment and systems that communicate, store and act on data. Cyber security encompasses systems, ships and offshore assets, but includes third parties – subcontractors, technicians, suppliers – and external components such as sensors and analytic systems that interface with networks and data systems. This includes human interaction of crews and other Company personnel, customers and potential threat players. In such a dynamic system, cyber security is an evolving set of capabilities inside the Company, developing and adapting as technology and threats evolve.”

A cyber security committee has been established, and is in the process of creating ship and office procedures with regards to cyber security. This will be an ongoing and constantly updated procedure

- a. In this case the Board of Directors (BoD) has made cyber security a priority for the office and fleet and tasked the management to formulate a strategy starting with a Cyber security Committee to communicate with the BoD, study cyber security ‘best practices’, provide recommendations, and implement approved actions.
- b. It is a good start that the ship and office are working together as there is a common threat risk from one to the other. It is a challenge if there is the passing on of cyber security to an unprepared crew without reasonable guidance, assigned responsibility, and at least basic knowledge of the ships networks and hardware.
- c. When implementing ‘best practices’, cyber security policy and procedures it should be incorporated into the Quality and Safety Management system to ensure ongoing improvement.
- d. Cyber security implementation on ships, not supported by clear and understandable policy, procedures, and audit will lessen the effectiveness of the cyber security program. Assigning responsibility and direct communication channels is essential.

- e. A clear message of the company policy and expectations from senior management to all of the company staff and crews and especially its vendors and suppliers is critical to set an acceptable level of cyber security companywide. The risk is that over time the trap of a lethargic message will lead to a weak cyber security culture.
- f. Approval of a strategy and a budget are a must and should be addressed at the highest management level of the company.
- g. "Company plans and procedures for cyber risk management should be seen as complementary to existing security and safety risk management requirements contained in the International Safety Management Code (ISM) Code1 and the International Ship and Port Facility Security (ISPS) Code2. Cyber security should be considered at all levels of the company, from senior management ashore to crew on board, as an inherent part of the safety and security culture necessary for safe and efficient ship operations."

## Aim/Objectives

The purpose of the 12<sup>th</sup> Week is to evaluate a case study of a company and how cybersecurity has helped/affected the company

## Learning Outcomes

After the successful completion of the 12<sup>th</sup> Week, students should be able to:

- Explain the advantages/disadvantages cybersecurity brings to a company

## Key Words

Ships	Reduce Risks	Strategy
Communication Systems	Routines	Insurance
Rapid Development	Threats	BoD

## Annotated Bibliography

### Suggestions for further reading

- Cyber Crime Case Study by Fujitsu in the UK & Ireland, [Youtube Video], Available at <https://www.youtube.com/watch?v=1mTviSphUDU>

## **Self-Assessment Exercises**

### **Exercise 12.1**

Explain the need for a cybersecurity program.

## **Group Assignment (20 points)**

The group assignment includes solving questions related to the syllabus covered in this course. The questions can vary from practical ones, to essay style questions asking to use your current skills as a group in order to describe existing laws applied in several countries, or even propose your own solutions giving the appropriate context to discuss and defend them.

This assignment counts 20% of the final course mark.

You will need approximately 20 hours to solve this Group Assignment.

## **Recommended time for the student to work**

35 hours

## PROFESSIONAL CERTIFICATIONS

13<sup>th</sup> Week

### Summary

In this week we will discuss some important certifications in the area of cybersecurity that are useful and sometimes necessary for a successful industry career.

### Introductory Remarks

#### CompTIA Network+

Network+ ensures an IT professional has the knowledge and skills to design and implement functional networks. Configure, manage, and maintain essential network devices, use devices such as switches and routers to segment network traffic and create resilient networks. Identify benefits and drawbacks of existing network configurations. Implement network security, standards, and protocols as well as troubleshoot network problems. Support the creation of virtualized networks. CompTIA Network+ has been updated and reorganized to address the current networking technologies with expanded coverage of several domains by adding:

- a. Critical security concepts to helping networking professionals work with security practitioners. Key cloud computing best practices and typical service models
- b. Coverage of newer hardware and virtualization techniques
- c. Concepts to give individuals the combination of skills to keep the network resilient

#### CompTIA Security+

CompTIA Security+ is the first security certification IT professionals should earn. It establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs. Security+ incorporates best practices in hands-on trouble-shooting to ensure security professionals have practical security problem-solving skills. Cybersecurity professionals with Security+ know how to address security incidents – not just identify them.

The CompTIA Security+ exam will certify the successful candidate has the knowledge and skills required to install and configure systems to secure applications, networks, and devices; perform threat analysis and respond with appropriate mitigation techniques; participate in risk mitigation

activities; and operate with an awareness of applicable policies, laws, and regulations. The successful candidate will perform these tasks to support the principles of confidentiality, integrity, and availability.

### **CompTIA CySA+**

CompTIA Cybersecurity Analyst (CySA+) is an IT workforce certification that applies behavioral analytics to networks and devices to prevent, detect and combat cybersecurity threats. CySA+ is the only intermediate high-stakes cybersecurity analyst certification with performance-based questions covering security analytics, intrusion detection and response. High-stakes exams are proctored at a Pearson VUE testing center in a highly secure environment. CySA+ is the most up-to-date security analyst certification that covers advanced persistent threats in a post-2014 cybersecurity environment.

As attackers have learned to evade traditional signature-based solutions, such as firewalls, an analytics-based approach within the IT security industry is increasingly important for most organizations. The behavioral analytics skills covered by CySA+ identify and combat malware, and advanced persistent threats (APTs), resulting in enhanced threat visibility across a broad attack surface.

CompTIA CySA+ is for IT professionals looking to gain the following security analyst skills:

- a. Perform data analysis and interpret the results to identify vulnerabilities, threats and risks to an organization.
- b. Configure and use threat-detection tools.
- c. Secure and protect applications and systems within an organization.

CompTIA CySA+ meets the ISO 17024 standard and is approved by U.S. Department of Defense to fulfill Directive 8570.01-M requirements. It is compliant with government regulations under the Federal Information Security Management Act (FISMA). Regulators and government rely on ANSI accreditation because it provides confidence and trust in the outputs of an accredited program. Over 1.3 million CompTIA ISO/ANSI-accredited exams have been delivered since January 1, 2011.

### **CompTIA PenTest+**

CompTIA PenTest+ is for cybersecurity professionals tasked with penetration testing and vulnerability management. CompTIA PenTest+ is the only penetration testing exam taken at a Pearson VUE testing center with both hands-on, performance-based questions and multiple-choice, to ensure each candidate possesses the skills, knowledge, and ability to perform tasks on

systems. PenTest+ exam also includes management skills used to plan, scope, and manage weaknesses, not just exploit them.

PenTest+ is unique because our certification requires a candidate to demonstrate the hands-on ability and knowledge to test devices in new environments such as the cloud and mobile, in addition to traditional desktops and servers.

- a. CompTIA PenTest+ assesses the most up-to-date penetration testing, and vulnerability assessment and management skills necessary to determine the resiliency of the network against attacks.
- b. Successful candidates will have the intermediate skills required to customize assessment frameworks to effectively collaborate on and report findings.
- c. Candidates will also have the best practices to communicate recommended strategies to improve the overall state of IT security.

### **CompTIA CASP**

CompTIA Advanced Security Practitioner (CASP) is the ideal certification for technical professionals who wish to remain immersed in technology as opposed to strictly managing. CASP is the only hands-on, performance-based certification for practitioners - not managers - at the advanced skill level of cybersecurity. While cybersecurity managers help identify what cybersecurity policies and frameworks could be implemented, CASP-certified professionals figure out how to implement solutions within those policies and frameworks.

The CompTIA Advanced Security Practitioner certification validates advanced-level competency in risk management; enterprise security operations and architecture; research and collaboration; and integration of enterprise security. Successful candidates will have the knowledge required to:

- a. Enterprise Security domain expanded to include operations and architecture concepts, techniques, and requirements
- b. More emphasis on analyzing risk through interpreting trend data and anticipating cyber defense needs to meet business goals
- c. Expanding security control topics to include Mobile and small form factor devices, as well as software vulnerability
- d. Broader coverage of integrating cloud and virtualization technologies into a secure enterprise architecture
- e. Inclusion of implementing cryptographic techniques, such as Blockchain- Cryptocurrency and Mobile device encryption

## **CISSP**

The Certified Information Systems Security Professional (CISSP) is an advanced-level certification for IT pros serious about careers in information security. Offered by the International Information Systems Security Certification Consortium, known as (ISC)<sup>2</sup> and pronounced "ISC squared," this vendor-neutral credential is recognized worldwide for its standards of excellence. CISSP credential holders are decision-makers who possess expert knowledge and technical skills necessary to develop, guide and then manage security standards, policies and procedures within their organizations. The CISSP continues to be highly sought after by IT professionals and well recognized by IT organizations. It is a regular fixture on most-wanted and must-have security certification surveys.

CISSP is designed for experienced security professionals. A minimum of five years of experience in at least two of (ISC)<sup>2</sup>'s eight Common Body of Knowledge (CBK) domains, or four years of experience in at least two of (ISC)<sup>2</sup>'s CBK domains and a college degree or an approved credential, is required for this certification. The CBK domains are Security and Risk Management, Asset Security, Security Engineering, Communications and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security.

(ISC)<sup>2</sup> also offers three CISSP concentrations targeting specific areas of interest in IT security:

- a. Architecture (CISSP-ISSAP)
- b. Engineering (CISSP-ISSEP)
- c. Management (CISSP-ISSMP)

## **CISM**

The Certified Information Security Manager (CISM) is a top credential for IT professionals responsible for managing, developing and overseeing information security systems in enterprise-level applications, or for developing best organizational security practices. The CISM credential was introduced to security professionals in 2003 by the Information Systems Audit and Control Association (ISACA).

ISACA's organizational goals are specifically geared toward IT professionals interested in the highest quality standards with respect to audit, control and security of information systems. The CISM credential targets the needs of IT security professionals with enterprise-level security management responsibilities. Credential holders possess advanced and proven skills in security risk management, program development and management, governance, and incident management and response.

Holders of the CISM credential, which is designed for experienced security professionals, must agree to ISACA's Code of Professional Ethics, pass a comprehensive examination, possess at least five years of security experience, comply with the Continuing Education Policy and submit a written application. Some combinations of education and experience may be substituted for the experience requirement.

## **CEH**

Hackers are innovators and constantly find new ways to attack information systems and exploit system vulnerabilities. Savvy businesses proactively protect their information systems by engaging the services and expertise of IT professionals skilled in beating hackers at their own game (often called "white hat hackers" or simply "white hats"). Such professionals use the very skills and techniques hackers themselves use to identify system vulnerabilities and access points for penetration to prevent hackers' unwanted access to network and information systems.

The Certified Ethical Hacker (CEH) is an intermediate-level credential offered by the International Council of E-Commerce Consultants (EC-Council). It's a must-have for IT professionals pursuing careers in ethical hacking. CEH credential holders possess skills and knowledge on hacking practices in areas such as footprinting and reconnaissance, scanning networks, enumeration, system hacking, Trojans, worms and viruses, sniffers, denial-of-service attacks, social engineering, session hijacking, hacking web servers, wireless networks and web applications, SQL injection, cryptography, penetration testing, evading IDS, firewalls, and honeypots.

## **Aim/Objectives**

The purpose of the 13<sup>th</sup> Week is to show some of the best and most known security certifications.

## **Learning Outcomes**

After the successful completion of the 13<sup>th</sup> Week, students should be able to:

- Evaluate several security certifications and understand which are the suitable ones according to the situation

## Key Words

Network+	Security+	CySA+
PenTest+	CASP	CISSP
CISM	CEH	

## Annotated Bibliography

### Basic

- CompTIA Website. [online] Available at: <https://www.comptia.org/> [Accessed 15 Nov. 2018].
- Cisco Training & Certifications [online] Available at: <https://www.cisco.com/c/en/us/training-events/training-certifications/certifications.html> [Accessed 15 Nov. 2018].

### Suggestions for further reading

- The Most in Demand Certifications in Cybersecurity by CyberTraining 365, [Youtube Video], <https://www.youtube.com/watch?v=N5MjxTMGbvs>

## Self-Assessment Exercises

### Exercise 13.1

Explain what CEH certification is?

## Recommended time for the student to work

15 hours

## **REVISION AND FINAL EXAMINATION**

The final examination will consist of a series of questions covering the material covered in this course.

Those questions will be in the form of multiple choice, essay style questions (mainly for methods and laws explained in the course) as well as more logic thinking questions such as discussing the advantages or disadvantages of some laws as well as proposing your own solutions.

The Final Examinations counts 50% of the final course mark.

### **Recommended time for the student to work**

40 hours

## INDICATIVE ANSWERS SELF-ASSESSMENT EXERCISES

### Introduction (1<sup>st</sup> Week)

#### Exercise 1.1

Vulnerability (weakness) is a gap in the protection efforts of a system, a threat is an attacker who exploits that weakness. Risk is the measure of potential loss when that the vulnerability is exploited by the threat e.g. Default username and password for a server – An attacker can easily crack into this server and compromise it.

#### Exercise 1.2

DHS and other U.S. agencies work together to conduct high-impact criminal investigations to disrupt and defeat cyber criminals. In addition, they provide training of technical experts, develop standardized methods, and broadly share cyber response best practices and tools.

The U.S. Secret Service maintains Electronic Crimes Task Forces, which focus on identifying and locating international cyber criminals connected to cyber intrusions, bank fraud, data breaches, and other computer-related crimes. The U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Cyber Crimes Center (C3) delivers computer-based technical services to support domestic and international investigations into cross-border crime.

In addition, DHS has created several programs in order to secure federal networks. This is because the federal enterprise networks face large and diverse cyber threats that range from unsophisticated hackers to technically competent intruders using state-of-the-art intrusion techniques. To tackle that, DHS created the National Cybersecurity Protection System (NCPS). Its mission is to improve cybersecurity to federal departments, agencies and partners by developing and establishing the services needed to secure the networks. These services include intrusion detection, advanced analytics, information sharing and intrusion prevention capabilities, that combat and mitigate cyber threats to the federal networks.

DHS's National Cybersecurity and Communications Integration Center (NCCIC) is a 24/7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the federal government, intelligence community, and law enforcement. The NCCIC shares information among the public and private sectors to provide

greater understanding of cybersecurity and communications situation awareness of vulnerabilities, intrusions, incidents, mitigation, and recovery actions.

Finally, it has created many public awareness campaigns such as the Stop.Think.Connect. A national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. The Campaign provides free resources available to everyone that are tailored to multiple demographics, including small businesses, students, educators and parents, and many others.

The Stop.Think.Connect. Campaign also has opportunities for academic colleges/universities, federal and local agencies, and non-profit organizations to collaborate with the Campaign. This no-fee partnership allows organizations and agencies to communicate with each other through various mediums and allows various stakeholders to expand the Stop.Think.Connect. message. A good resource is the website <https://www.dhs.gov/topic/combating-cyber-crime>

## **Major Cyber Attacks / Incidents in Recent Years (2<sup>nd</sup> Week)**

### **Exercise 2.1**

A ransomware is a type of malware that prevents or limits users from accessing their system. This could either be done by locking the system's screen or by locking the users' files unless a ransom is paid. More recent ransomware families, now commonly known as crypto-ransomware, have the capability to encrypt numerous file types on infected systems and coerces users to pay the ransom in exchange for the decrypt key needed to regain access to the affected files.

Most ransomware attacks use crypto currency methods of payment. This is due to the fact that such a system does not have a central authority to control this form of currency, therefore it keeps the transaction anonymous. Recent ransomware variants have also listed alternative payment options such as iTunes and Amazon gift cards, which are easily monetized. In June 2016, bitcoin exchange via Paypal was also seen, which was an interesting choice given that transactions made on the platform can be traced.

When it comes to ransomwares, there is no way that can guarantee 100% safety. But some precaution measures can be used, such as:

- Avoid opening unverified emails or clicking links embedded in them. If the email came from an unknown source, refrain from clicking or opening them. If the email claims to have come from someone you know, always verify if it did come from them.
- Back up important files using the 3-2-1 rule—create 3 backup copies on 2 different media with 1 backup in a separate location. Losing one's database of important files and

documents remains as the biggest lure of cybercriminals to make victims pay for the ransom. Having a backup of your important files keeps damages to a minimum.

- Remember to regularly update software, programs, and applications to reduce the risks posed by vulnerabilities which can be exploited to install malware such as ransomware.

WannaCry attack led to disruption in one third of hospital trusts in England. NHS England data shows that at least 80 out of 236 trusts were affected. As part of its incident response the NHS enacted its “mutual aid” processes in some parts of the country. This meant that where one A&E could no longer take patients, nearby A&Es stepped up to take their demand. During the incident, some patients from five hospitals travelled further for emergency treatment than normal. 1.2 % (6,912) first appointments were cancelled and re-arranged at later dates. NHS England’s EPRR review identified at least 139 patients who had an urgent appointment for potential cancer cancelled, representing approximately 0.4% of urgent cancer referrals. During and after the attack, evening and weekend clinics in GP practices were impacted due to the lack of availability of electronic patient records and clinical systems

## What to Expect in Cybersecurity Threats (3<sup>rd</sup> Week)

### Exercise 3.1

The vast majority of humans in first-world countries have a smartphone in their pockets, a computer at work, a smart television at home, and a tablet in their cars. But there is more to come. The Internet of Things (IoT) is making sure that every single device you own is connected. For example, there are now smart refrigerators that can tell you if there is no milk left, there are smart speakers that can talk and listen to you, and order goods online on your command. The fact that everything is connected gives massive benefits to the user, making it so appealing in the first place. You can now control your house from your smart device, or you can ask the virtual assistant (Google Assistant, Siri, Alexa) to do something for you. The problem is that all of that interconnectedness makes consumers highly susceptible to cyberattacks. In fact, one study by Gartner revealed that 70 percent of IoT devices have serious security vulnerabilities. Specifically, insecure web interfaces and data transfers, insufficient authentication methods, and a lack of consumer security knowledge leave users open to attacks. And that truth is compounded by the fact that so many consumer devices are now interconnected. In other words, if you access one device, you’ve accessed them all. Evidently, with more convenience comes more risk.

### **Exercise 3.2**

2017 ended with a spectacular rise in the valuation and popularity of cryptocurrencies like Bitcoin and Ethereum. These cryptocurrencies are built upon blockchains, the technical innovation at the core of the revolution, a decentralized and secure record of transactions. But the question is what does blockchain technology have to do with cybersecurity. It's a question that security professionals have only just started asking. While it's difficult to predict what other developments blockchain systems will offer in regards to cybersecurity, professionals can make some educated guesses. Companies are targeting a range of use cases which the blockchain helps enable from medical records management, to decentralized access control, to identity management. As the application and utility of blockchain in a cybersecurity context emerges, there will be a healthy tension but also complementary integrations with traditional, proven, cybersecurity approaches. You will undoubtedly see variations in approaches between public & private blockchains. With blockchain technology, cybersecurity will likely look much different than it has in the past. For the second part of the question (i.e. giving examples with appropriate citations), students can find uses of blockchain technology online and explain what breakthrough does the technology bring and why it is used. One example can be the blockchain mobile phone.

## **European Union Cybersecurity Strategy (4<sup>th</sup> Week)**

### **Exercise 4.1**

The European Union Agency for Network and Information Security (**ENISA**) has a key role to play but is constrained by its current mandate. The Commission presents an ambitious reform proposal, including a permanent mandate for the agency to ensure that ENISA can provide support to Member States, EU institutions and businesses in key areas, including the implementation of the NIS Directive. It will also contribute to stepping up both operational cooperation and crisis management across the EU.

### **Exercise 4.2**

#### **Cyberdefence**

The recently adopted framework for a joint EU diplomatic response to malicious cyber activities (the “cyber diplomacy toolbox”) sets out the measures under the Common Foreign and Security

Policy, including restrictive measures which can be used to strengthen the EU's response to activities that harm its political, security and economic interests. Implementation work on the Framework is currently ongoing with Member States and would also be taken forward in close coordination with the Blueprint to respond to large scale cyber incidents.

## **Cybercrime**

The Commission will present concrete proposals in early 2018 to facilitate swift cross-border access to electronic evidence.

### European Factsheet

According to "Resilience, Deterrence and Defence: Building strong cybersecurity in Europe" factsheet, Europeans, with percentages 75%, 64% and 67% believe that digital technologies have a positive impact on economy, society and quality of life respectively. At the same time, 86% of them believe that the risk of becoming a victim of cybercrime is increasing.

## **European Union Cybersecurity Act (5<sup>th</sup> Week)**

### **Exercise 5.1**

Beyond what is required by EU law, Germany has some notable national cybersecurity laws touching on cybersecurity. Germany has taken legislative action to enhance IT security of Germany's critical infrastructure and protecting users of the internet. The German IT Security Law requires private and public infrastructure operators to implement minimum information security standards (or face penalties) as well as reporting obligations for suspected attacks (e.g. energy, telecommunication, health, water/food, finance and insurance). The Federal Office of Information Security (BIS) is responsible for investigating cyberattacks. Further, in specific sectors, the competent authority sets minimum IT security standards.

The German government may block foreign investments to ensure that they do not threaten public order or security. The German Foreign Trade Law allows the federal government to block investors from acquiring at least 25% of a company. The Ministry of Economic Affairs conducts mandatory reviews for foreign investments in certain IT security sectors. Reportedly, in 2012, the German national research and education network decided to ban Huawei from tendering for a network update due to security concerns. These rules may be further strengthened if common EU-rules are adopted. Germany also applies the EU dual-use regulation including controls on the export of information security software and hardware (including encryption).

For the second part students should compare the law with any other country giving differences or similarities. Countries such as Israel, Singapore, Australia or EU in general can be used.

## Cybersecurity Around the World – Part 1 (6<sup>th</sup> Week)

### Exercise 6.1

Australia has taken several initiatives similar to those of the US and EU to enhance cybersecurity in critical infrastructure, and in sector specific areas, such as banking, finance and data privacy. However, at present, these initiatives appear to not be based on legislative action but rather recommendations, guidelines and voluntary industry standards and cooperation (“soft law”) issues by the government.

The Australian Attorney-General has issued a Protective Security Policy Framework applicable in general to Australian governmental authorities. Also, the Australian Government Department of Defence has produced an Information Security Manual (ISM) which applies as a standard for government ICT systems. The government agency, Trusted Information Sharing Network (TINS), provides a platform for sharing information on incidents and increasing resilience against cybersecurity attacks. For example, for banking, the Prudential Practice Guide CPG 235 issued by APRA sets out a standard for managing data risks. Healthcare providers should follow the specific Computer and Information Security Standards.

Australia reviews foreign investments for national interest concerns. Since 2015 the review includes a specific screening to determine whether the foreign investment is made by a foreign government. The Foreign Acquisitions and Takeovers Act 1975 and Regulation 2015, allows the Australian Government Foreign Investment Review Board (FIRB), to review foreign investments in Australia and it advises the Treasurer and Commonwealth Government who may decide that an investment is contrary to national interests. Further, under the Australian Security Intelligence Organisation Act 1976, the Australian Security Intelligence Organisation (“ASIO”) may provide security intelligence to the Australian Government. In 2012, the ASIO advised and the Government blocked Huawei from a public tender of national broadband networks. Also, under The Defence and Strategic Goods List Australia controls export of information security items in a similar manner as the export control rules of the US and the EU.

Various laws implement the Budapest Convention criminalising acts under the Criminal Code Act 1995, Crimes Act 1914. Specific rules exist in the Telecommunications (Interception and Access) Acts, Copyright Act etc. More specifically, the Cybercrime Act 2001.

## Cybersecurity Around the World – Part 2 (7<sup>th</sup> Week)

### Exercise 7.1

Under the Personal Data Protection Act 2012 (PDPA), it is an offence to collect personal data without the data subject's consent, unless an exception applies. It is also an offence under the PDPA for a person to make a request to obtain access to or to change the personal data about another individual, which is in the possession or under control of an organisation, without the authority of that individual. Under the Computer Misuse and Cybersecurity Act (CMCA), it is an offence to knowingly cause a computer to perform any function for the purpose of securing access without authority to any data held in any computer. Further, a plaintiff may make a claim under tort for, amongst others, conversion or breach of a duty of confidentiality. Is there a legal mechanism whereby you can seek access to or retrieve the copy of data which has been accessed without authority? Is there a legal mechanism that enables you find out information about who may have accessed your data without authority and/or how it was used? There are various possible mechanisms, depending on the circumstances:

The matter may be referred to the police for criminal prosecution via a complaint. While the assistance of the police may be sought, the complainant strictly has no control over the conduct of the matter by the police and has no right to request information or documents from the police. It is within the police's discretion whether it chooses to reveal anything to the complainant.

Civil proceedings for, amongst others, breach of confidence may also be commenced. As part of the final relief in such civil proceedings, the complainant may seek an injunction for the delivery up, return and/or deletion of the data which has been accessed without authority, damages and/or an account of profits. There are also various interim measures or forms of injunctive relief available, for example:

an application for a search and seizure order, for permission to search, inspect and either copy or remove documents in the possession of the defendant(s), when there is (amongst other requirements) a grave danger that the defendant(s) will dispose of or destroy incriminating evidence in his/her possession. These documents which are seized are not ordinarily provided to the plaintiff immediately, but an order may be made for inspection by the plaintiff of those documents;

an application for interim injunction to, amongst other things, restrain the defendant(s) from using and/or disclosing such data pending the final resolution of the civil proceeding;

the process of general and/or specific discovery, interrogatories and/or further and better particulars of pleadings, may be applicable.

If the identity of the person who either committed the data breach or is storing or has stored the data at some point in time is unknown and/or civil proceedings have not been commenced, the complainant may make an application for pre-action discovery or pre-action interrogatories against known parties who may be involved. Such applications, if successful, may require an individual or company to produce documents or answer questions so that either the identity of the potential defendant(s) may be determined or the plaintiff can assess whether there is a case to be made.

## Cybersecurity and Emerging Technologies (8<sup>th</sup> Week)

### Exercise 8.1

It is a well-known fact that passwords and usernames used by a majority of data users are weak. This makes it easy for hackers to get access to the information systems and compromise sensitive data of a business entity or government agency. In turn, this has exerted pressure on experts of systems security to come up with authentication methods that are more secure. One of the ways that has been used is the development of user hardware authentication. Tech companies have developed a solution in the user authentication process with a new Core vPro processor that belongs to the sixth generation of processors. The core vPro can combine different hardware components with enhanced factors simultaneously for user identity validation purposes.

The tech company Intel has built on previous experiences and mistakes and dedicated a portion of the processor for security reasons to make a device part of the entire process of authentication. Hardware authentication can be especially important when it comes to the Internet of Things where the network of connected devices ensures that any device that seeks to be connected has the rights for connectivity to that particular network.

## Cybersecurity as an Engine for Growth (9<sup>th</sup> Week)

### Exercise 9.1

Israel Aerospace Industries Ltd. (IAI), the country's largest aerospace and defence company, said it has set up a special division to deal with the cyber business of its subsidiary ELTA Systems

Ltd., a defence electronics company. The IAI has appointed Esti Peshin as the general manager of the division. The government-owned company, which manufactures military and civilian aircraft and products, said it ended 2016 with contracts totalling over \$100 million in the fields of cyber-intelligence, cyber-forensics and analysis, and cyberdefense centres.

"We consider cyber to be a strategic field of activity and a growth engine at IAI, and expect it to continue to expand significantly in the coming years," said Joseph Weiss, IAI's president and CEO, in a statement. "The establishment of IAI's Cyber Division serves as infrastructure for continued extensive activity. We will continue to invest in cyber companies and research and development centres in order to continue to expand in this field." IAI sees cybersecurity as a strategic field and source of growth. The company is developing cyber solutions and advanced capabilities for intelligence, monitoring, identification and accessibility, offering clients tools to tackle cyberthreats. IAI operates R&D and innovation centers in Singapore, Switzerland and Israel. The company also leads the Israel Cyber Company Consortium (IC3) which comprised of leading Israel cyber companies.

Israel is seen as a global leader in cybersecurity. Sixty-five new cyber startups were set up in Israel in 2016, and the nation maintained its leading position as a global center of cybersecurity innovation, a report by the non-profit Start-Up Nation Central revealed. A record \$581 million of capital was raised by cybersecurity startups last year in Israel, a 9 percent increase compared to 2015. This amount was second only to the US, and accounted for 15% of the total venture capital raised by cybersecurity companies globally. At the end of 2016 there were 365 cybersecurity companies active in Israel, compared to 187 in 2012, according to data compiled by Startup Nation's database and PitchBook.

## Future Research Direction in Cybersecurity (10<sup>th</sup> Week)

### Exercise 10.1

As the range of potential threats over the Internet expands, end users are increasingly find themselves in a position having to make security decisions, for example through configuring security-related settings, responding to security-related events and messages, or enforced to specify security policy and access rights. Unfortunately, experience suggests that although security features are often provided, they are conveyed in a manner that is not understandable or usable for many members of the target audience. As most users unable to comprehend the security features on offer, many security enhancements remain unused leaving the end users in a vulnerable position from malicious attacks. The need for usable security and the difficulties

inherent in realizing adequate solutions are increasing being recognized. Many security technologies have tried to improve the usability aspects; most of which fall short in terms of usability. Password schemes have been believed to be one important parts of usable security. Therefore, several elaborate procedures have been progressed such as frequency of changing, inclusion of non alphabetic characters, or visual and biometric based passwords that users do not have to remember. Despite these attempts, security pitfalls of poorly implemented password schemes have been extensively documented over the years. Users resort to writing them on slips of paper or storing them unencrypted on handheld devices. Mail authentication is another active area where usable security has been studied in a form to authenticate senders of valid emails. Security pop-up dialogs and SSL lock icons also have been proposed. Another issue that makes it difficult to devise an effective usable security scheme is that usability of systems tends to decrease as attempts are made to increase security. For example, some email system requires users to re authenticate in a regular time to assure that they are actually the authorized person. In another example, some web browsers warn users before any script is run. But users may still browse a web server that has scripts on every page causing pop-up alerts to appear on each page. The potential impacts of security that is not usable include increase susceptibility and vulnerable from social engineering type of cyber-attacks.

## Safer Internet (11<sup>th</sup> Week)

### Exercise 11.1

The awareness campaign, which first began in the US in 2004 before spreading to the EU in 2012, is part of a major effort to promote cyber security issues and educate the public on the dangers of online attacks.

Cyber security has become an increasingly risky area in recent years, with the World Economic Forum's Global Risks Report 2018 naming cyber attacks as the third top cause of global disruption over the next five years, behind natural disasters and catastrophic weather events. In order to protect against such occurrences, both businesses and individuals are encouraged to increase their awareness of the potential risks in order to improve their safety.

Google also offers a security checkup as part of the campaign. The checkup involves analysing issues within four separate sections: 'Your devices', 'recent security events', 'sign-in and recovery', and 'third-party access'.

Through these sections, Google account holders will be informed of any unusual activity on their account, such as signing in from new devices or sensitive account setting changes.

Google also encourages users to remove old devices with access to their account if they haven't been used for a long period of time.

A number of other organisations and businesses have been participating in the campaigned in Europe and the US, with the Better Business Bureau in the US offering a number of tips for staying safe online throughout the month.

Advice from the bureau includes avoiding suspicious links and attachments, sticking to trustworthy websites, improving the strength of passwords, and updating security protection software on computers and other devices.

Security experts have also issued their own warnings about cyber safety, including Jake Moore from antivirus software firm ESET, who praised Google's initiative.

## Cyber Security Case Studies (12<sup>th</sup> Week)

### Exercise 12.1

The company is undergoing a transition from the current Fleet Broadband communication services to a higher broadband capable VSAT system. This 'open to the internet' situation will drive the company towards more vigilance and the need for a Cyber security program to be put in place

- a. "The rapid development in maritime broadband satellite coverage combined with the introduction of highly sophisticated equipment, such as computer controlled engine systems, has changed the structural risks to maritime vessels. Ships are no longer protected by an air-gap from external systems. Today, an estimated 30,000 vessels globally have equipment providing them with constant internet access, which is an increase from only 6,000 in 2008. Even if networks on board are separated between systems for ship operation, crew welfare and remote access to suppliers, separations can over time be compromised by ad hoc interventions by the crew or suppliers, for instance in connection to maintenance..." .
- b. "Cyber security refers to the security of information networks and control systems and the equipment and systems that communicate, store and act on data. Cyber security encompasses systems, ships and offshore assets, but includes third parties – subcontractors, technicians, suppliers – and external components such as sensors and analytic systems that interface with networks and data systems. This includes human interaction of crews and other Company personnel, customers and potential threat

players. In such a dynamic system, cyber security is an evolving set of capabilities inside the Company, developing and adapting as technology and threats evolve."

## Professional Certifications (13<sup>th</sup> Week)

### Exercise 13.1

Hackers are innovators and constantly find new ways to attack information systems and exploit system vulnerabilities. Savvy businesses proactively protect their information systems by engaging the services and expertise of IT professionals skilled in beating hackers at their own game (often called "white hat hackers" or simply "white hats"). Such professionals use the very skills and techniques hackers themselves use to identify system vulnerabilities and access points for penetration to prevent hackers' unwanted access to network and information systems.

The Certified Ethical Hacker (CEH) is an intermediate-level credential offered by the International Council of E-Commerce Consultants (EC-Council). It's a must-have for IT professionals pursuing careers in ethical hacking. CEH credential holders possess skills and knowledge on hacking practices in areas such as footprinting and reconnaissance, scanning networks, enumeration, system hacking, Trojans, worms and viruses, sniffers, denial-of-service attacks, social engineering, session hijacking, hacking web servers, wireless networks and web applications, SQL injection, cryptography, penetration testing, evading IDS, firewalls, and honeypots.



**FORM: 200.1.3**

## **STUDY GUIDE**

**Course: CYS623 - Cybersecurity Risk Analysis and Management**

## Course Information

<b>Institution</b>	European University Cyprus		
<b>Programme of Study</b>	Cybersecurity (MSc)		
<b>Course unit</b>	CYS623	Cybersecurity Risk Analysis and Management	
<b>Level</b>	<i>Undergraduate</i>	<i>Postgraduate</i>	
		<i>Master</i>	<i>PhD</i>
		√	
<b>Language of Instruction</b>	English		
<b>Teaching Methodology</b>	Distance Learning		
<b>Course Type</b>	<i>Compulsory</i>		<i>Optional</i>
			√
<b>Number of Group Consultation Meetings/Web-Conferences/ Lectures</b>	<b>Total</b>	<b>Face to Face</b>	<b>Web-Conferences</b>
	14	1	13
<b>Number of Activities/ Assignments</b>	4		
<b>Final Assessment</b>	<i>Assignments</i>		<i>Final Examinations</i>
	50 %		50 %
<b>Number of Credits (ECTS)</b>	10		

<b>Study Guide drafted by</b>	Dr George Kioumourtzis
<b>Editing and final approval of Study Guide by</b>	Dr Yianna Danidou

## COURSE CONTENTS

		Page
	Introductory Notes	4
	First Group Consultation Meeting	5
1	Week 1 - Cyber-Systems and Cyber Security	8
2	Week 2 - Cyber Security Standards and Best Practices	14
3	Week 3 - Cyber Security Frameworks	20
4	Week 4 – Risk Management	26
5	Week 5 - Cyber Risk Management	32
6	Week 6 - Risk Assessment Concepts	39
7	Week 7 - Risk Assessment Process	44
8	Week 8 - Risk Assessment Approaches	50
9	Week 9 - Risk Analysis and Treatment	59
10	Week 10 - Threat and Vulnerability Management	68
11	Week 11 – Security Incident Management	75
12	Week 12 - Business Continuity	83
13	Week 13 - Security Monitoring and Improvement	91
14	Revision and Final Examination	97
	Indicative Answers to Self-Assessment Exercises	98

## INTRODUCTORY NOTES

The Cybersecurity Risk Analysis and Management course is fundamental is course is compulsory with a special position among the other courses in the Cybersecurity master program.

The Study Guide, a tool that is necessary and useful for students, especially in those cases where the training material is not written with the methodology of open and distance learning, encourages and facilitates the study and understanding of the issues addressed by the thematic module. In addition, through self-assessment exercises, it stimulates and encourages work at home, provides incentives for further study, and contributes to the development of your critical thinking. The Study Guide is structured on a weekly basis and includes a summary and some very brief introductory remarks, purpose and expected outcome, key words - basic concepts, annotated literature, recommended student's time, self-assessment exercises, critical thinking and case studies, with indicative answers in the end, aiming at a more meaningful understanding of the content, terms and concepts that each unit deals with. The recommended weekly working time includes, apart from the study, the follow-up of teleconferences and OSS, bibliography search, two weekly exercises, etc. Although it is self-evident, it should be noted that the study guide does not substitute to the minimum the educational material on the platform that the student needs to read carefully and assimilate in order to be able to meet the requirements of the program and to successfully complete the thematic module them.

## 1st GROUP CONSULTATION MEETING

### Programme Presentation

Leading companies today are rethinking the role of information security in their organizations. They realize that in a digital world, cybersecurity is the key to safeguarding their most precious assets—intellectual property, customer information, financial data, and employee records, among others. But far more than a defensive measure, companies also know that cybersecurity can better position their organization with business partners, customers, investors, and other stakeholders.

The European cybersecurity market is about 25% (i.e. about €17bln) of the world market (estimated at €70bln in 2015), with an average yearly growth slightly larger than 6%, when the world market is growing at about 10%/year. Recent study compiled by Europe's cybersecurity industry leaders pointed out that Europe is in danger of falling behind in the international digital economy field.

The Master in Cybersecurity is a cutting-edge program, designed for those wishing to develop a career as a cyber-security professional, or to take a leading technical or managerial role in an organization critically dependent upon data and information communication technology. Students will develop an advanced knowledge of information security and an awareness of the context in which information security operates in terms of safety, environmental, social and economic aspects. They will gain a wide range of intellectual, practical and transferable skills, enabling them to develop a flexible professional career in IT.

Key elements of this postgraduate degree are: the *real life experience* given by the opportunity to apply their theoretical knowledge through specialized virtual and remote security laboratories in which they will be able to carry out activities such as reconnaissance, network scanning and exploitation exercises, and investigate the usage and behavior of security systems such as Intrusion Detection and Prevention Systems thus becoming confident in the practical application of the latest tools; the *high-level insight* that will enhance student's ability to research and design creative cyber security solutions to address business problems; *hands-on skills* through experimentation with security techniques, cryptographic algorithms, cyber forensics building an ethical hacking environment; and *flexibility* since students will also be able to choose either the completion of a Master thesis or to complete a Research methods course and two elective courses.

Students undertake modules to the value of 90 ECTS credits.

## COURSE PRESENTATION THROUGH THE STUDY GUIDE

This course is compulsory with a special position among the other courses in the Cybersecurity master program. The course consists of the following parts:

In the first three weeks we will study and explain the main concepts of cyber systems and security, the cyber security standards and the guidance principles. We will provide a high-level overview cyber security frameworks and methodologies along with the European Union Agency for Network and Information Security (ENISA) NIS Directive and the Cybersecurity Framework of the National Institute of Standards and Technology (NIST), USA. During the third week, you will be requested to make a comparison between these two major cybersecurity frameworks. This will enable to better grasp the concept of cyber risk assessment and management in the upcoming weeks.

Cyber risk assessment concepts, management, processes, approaches, analysis and treatment will be discussed from week four to week eleven. In these weeks we will dig deeper in all the above topics and you will be given the most important concepts of cyber risk management. During the eighth week you will be requested to study a major International standard related to risk assessment, the ISO 27005, which describes a systematic approach to managing information security risk, particularly in the context of ISO 27001, ISMS Requirements.

The following last two weeks we will discuss business continuity, and how we can improve cyber security performance on how we can improve the security of an ingratitudo or a business area via security monitoring and audits. In the twelfth week, you will be given a group assignment related to most important and widely used cyber security frameworks.

There will be also two activities to improve your knowledge in the weeks fifth and tenth.

In addition to the above, each week you are provided with self-assessment exercises to test and identify your level of understanding. The study guide will also provide supplementary reading, interesting scientific publications and multimedia content that we suggest you visit. These materials will improve your knowledge and your understanding of the course.

Upon successful completion of this course you should be able to:

- Describe the underlying principles of risk analysis and management and the purpose and benefits behind such activities
- Explain the terms used, such as risk, analysis, management, vulnerability, threats, actors, impact, risk matrix, etc.
- Recognise the difference between vulnerabilities and threats.
- Classify and describe a number of different risk assessment/management methodologies.

- Classify and describe different assets and their values (including tangible and intangible assets).
- Identify and explain various threat sources and the impacts that their materialization may manifest.
- Describe the risk management process, as it pertains to the protection of assets.
- Evaluate and select appropriate risk treatment options according to the combination of impacts and probabilities that the risk analysis has produced.

### **Recommended time for the student to work**

Approximately 5 hours for the study guide

# CYBER SYSTEMS AND CYBER SECURITY

1<sup>st</sup> Week

## Summary

In this first week, we will deal with the basic definitions and concepts of cyberspace and cyber security.

Our definitions will be based on updated literature and international standards.

## Introductory Remarks

A useful definition of cyberspace comes from the National Research Council's publication at the Nexus of Cybersecurity and Public Policy [1]:

- **Cyberspace** consists of artifacts based on or dependent on computer and communications technology; the information that these artifacts use, store, handle, or process; and the interconnections among these various elements.

A reasonably comprehensive definition of cybersecurity is provided in ITU-T (International Telecommunication Union Telecommunication Standardization Sector) Recommendation X.1205:

- **Cybersecurity** is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that are used to protect the cyberspace environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyberspace environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyberspace environment. The general security objectives comprise the following: availability; integrity, which may include authenticity and non-repudiation; and confidentiality.

Two related terms should be mentioned:

- **Information security:** Preservation of confidentiality, integrity, and availability of information. In addition, other properties—such as authenticity, accountability, non-repudiation, and reliability—can also be involved.
- **Network security:** Protection of networks and their services from unauthorized modification, destruction, or disclosure and provision of assurance that the network performs its critical functions correctly and that there are no harmful side effects.

Cybersecurity encompasses information security, with respect to electronic information, and network security. Information security also is concerned with physical (for example, paper-based) information. However, in practice, the terms cybersecurity and information security are often used interchangeably.

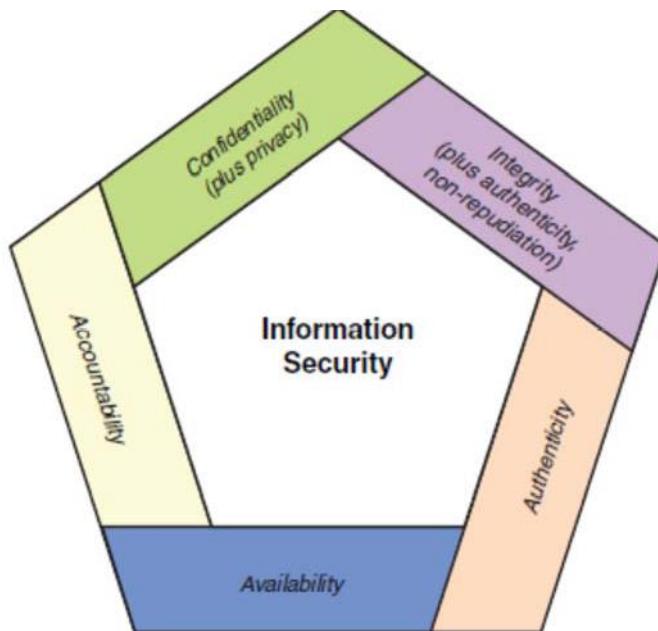


Figure 1 - Essential Cybersecurity Objectives

A more extensive list of cybersecurity objectives includes the following:

- **Availability:** The property of a system or a system resource being accessible or usable or operational upon demand, by an authorized system entity, according to performance specifications for the system; that is, a system is available if it provides services according to the system design whenever users request them.
- **Integrity:** The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.
- **Authenticity:** The property of being genuine and being able to be verified and trusted. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

- **Non-repudiation:** Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
- **Confidentiality:** The property that data is not disclosed to system entities unless they have been authorized to know the data.
- **Accountability:** The property of a system or system resource ensuring that the actions of a system entity may be traced uniquely to that entity, which can then be held responsible for its actions.

Cybersecurity Dilemmas: Technology, Policy, and Incentives [2] summarizes the challenges in developing an effective cybersecurity system as follows:

- **Scale and complexity of cyberspace:** The scale and complexity of cyberspace are massive. Cyberspace involves mobile devices, workstations, servers, massive data centers, cloud computing services, Internet of Things (IoT) deployments, and a wide variety of wired and wireless networks. The variety of individuals and applications requiring some level of access to these resources is also huge. Further, the challenges to achieving cybersecurity constantly change as technologies advance, new applications of information technologies emerge, and societal norms evolve.
- **Nature of the threat:** Organizational assets in cyberspace are under constant and evolving threat from vandals, criminals, terrorists, hostile states, and other malevolent actors. In addition, a variety of legitimate actors, including businesses and governments, are interested in collecting, analyzing, and storing information from and about individuals and organizations, potentially creating security and privacy risks.
- **User needs versus security implementation:** Users want technology with the most modern and powerful features, that is convenient to use, that offers anonymity in certain circumstances, and that is secure. But there is an inherent conflict between greater ease of use and greater range of options on the one hand and robust security on the other. In general, the simpler the system, and the more its individual elements are isolated from one another, the easier it is to implement effective security. But over time, people demand more functionality, and the greater complexity that results makes systems less secure. Users or groups within an organization that feel inconvenienced by security mechanisms will be tempted to find ways around those mechanisms or demand relaxation of the security requirements.
- **Difficulty estimating costs and benefits:** It is difficult to estimate the total cost of cybersecurity breaches and, therefore, the benefits of security policies and mechanisms. This complicates the need to achieve consensus on the allocation of resources to security.

Because of these challenges, there is an ongoing effort to develop best practices, documents, and standards that provide guidance to managers charged with making resource allocation decisions as well as those charged with implementing an effective cybersecurity framework. The focus of this book is on the broad consensus that has been reached, as expressed in such documents. The volume and variety of these documents is very broad, and the goal of this book is to consolidate that material and make it accessible.

Let us see now in which way cybersecurity is related to information security. Information security is the preservation of confidentiality, integrity, and availability of information. Information can come in any form, be it electronic or material, or even as the knowledge of personnel. Cybersecurity, however, is not limited to the protection of information assets alone. As we discuss below, it often concerns the protection of infrastructure.

Infrastructure security, in particular critical infrastructure protection (CIP) and critical information infrastructure protection (CIIP), is concerned with the prevention of the disruption, disabling, destruction, or malicious control of infrastructure [3], [4]. Such infrastructures include, for example, telecommunication, transportation, finance, power supply, water supply, and emergency services. How cybersecurity relates to information security and CIP is illustrated in the Venn diagram in Figure 2. From the diagram we see that while cybersecurity may involve both information security and CIP, the former is not simply a combination of the latter two.

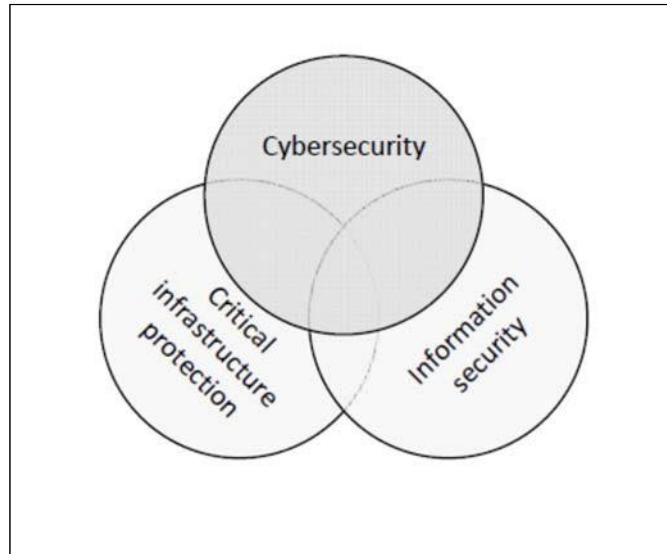


Figure 2 - Essential Cybersecurity Objectives

Let us see now the relation between safety and cybersecurity. Safety can be defined as the protection of life and health by the prevention of physical injury caused by damage to property or to the environment [5], [6]. One of the main differences between safety and cybersecurity is that while safety focuses on system incidents that can harm the surroundings, cybersecurity focuses on threats that cause harm via a cyberspace. A further difference is that the assets that are considered with respect to safety are usually limited to human life and health, as well as environmental assets, while the assets of concern with respect to cybersecurity can be anything that needs to be protected.

## Aim/Objectives

The scope of this week is to provide with the definition of cyber systems and cybersecurity and the objectives of cybersecurity. We will look in which cybersecurity is related to information security and to Critical Infrastructure Protection (CIP). Finally, we will also look at the relation between cybersecurity and safety.

## Learning Outcomes

Upon successful completion of this course, students should be able to:

- Explain what cyber system is.
- Explain what cybersecurity is.
- Explain in which way cybersecurity is related to the protection of critical infrastructure
- Explain the difference between information security and cybersecurity.
- Discuss the challenges in developing an effective cybersecurity system.
- Define the Essential Cybersecurity Objectives

## Key Words

Cyber systems	cybersecurity	Information security
Network security	Availability	Integrity
Confidentiality	Critical Infrastructure Protection (CIP)	Non-repudiation

## Annotated Bibliography

### Basic

Atle Refsdal, Bjørnar Solhaug, Ketil Stølen, “**Cyber-Risk Management**”, ISSN 2191-5768 ISBN 2191-5776 (electronic), SpringerBriefs in Computer Science, ISBN 978-3-319-23569-1 ISBN 978-3-319-23570-7 (eBook), DOI 10.1007/978-3-319-23570-7, Library of Congress Control Number: 2015950450, 2015.

Available to all EUC students via the <https://www.openathens.net/> service.

This week is based on the above book and more specifically on Chapters 3 and 4. The book provides a short and focused introduction to risk management, with particular emphasis on cybersecurity and cyber-risk assessment, building on best practices from industry. This book builds on and is complementary to established standards in several respects. First, the book defines and explains the background of the terminology to give a more thorough understanding of the domain of cyber-risk management. Second, the book has a pragmatic orientation in that it explains not only what cyber risk management is (as the standards do), but also how to do it. Third, the book gives a running example that illustrates the various tasks of cyber-risk assessment and how to conduct them. Fourth, the book addresses several of the typical challenges that assessors of cyber-risk encounter and provides advice on how to tackle them. The intended target audience is practitioners, as well as graduate and undergraduate students, in particular within the ICT domain.

## **Supplementary**

Power point presentation slides available in the platform

Video: [City, University of London: Professor Chris Hankin - 'The Science of Cyber Security'](#)

## **Suggestions for further reading**

- [1] Clark, D., Berson, T., & Lin, H. (Eds.), At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues. National Research Council, National Academy of Sciences, 2014. European Commission Decision C (2014)4995 of 22 July 2014.
- [2] Cicerone, R., & Nurse, P. (Eds.), Cybersecurity Dilemmas: Technology, Policy, and Incentives. National Academy of Sciences, 2014.
- [3] European Commission: COM (2011) 163 final – On critical information infrastructure protection – Achievements and next steps: Towards global cyber-security (2011)
- [4] International Organization for Standardization / International Electrotechnical Commission: ISO/IEC 27032 – Information technology – Security techniques – Guidelines for cybersecurity (2005).
- [5] Avižienis, A., Laprie, J.C., Randell, B., Landwehr, C.: Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing 1, 11–33 (2004).
- [6] International Electrotechnical Commission: IEC/TR 61508-0 – Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 0: Functional safety and IEC 61508 (2005).

## **Self-Assessment Exercises**

### **Exercise 1.1**

Explain briefly each of the following terms from the perspective of cybersecurity: availability, integrity, authenticity, non-repudiation, and confidentiality.

### **Exercise 1.2**

Explain the three key challenges in developing an effective cybersecurity system.

## **Recommended time for the student to work**

15 hours

## CYBER SECURITY STANDARDS AND BEST PRACTICES

2<sup>nd</sup> Week

### Summary

In this week we will overview the main security standards and best practices. We will present you the major international players in the cyber security field and the related ISO cyber security standards.

### Introductory Remarks

The development, implementation, and management of a cybersecurity system for an organization are extraordinarily complex and difficult. However, there is a great deal of thought, experimentation, and implementation experience that have gone already into the development of policies, procedures, and overall guidance for cybersecurity system management teams. A number of organizations, based on wide professional input, have developed best practices types of documents as well as standards for implementing and evaluating cybersecurity. On the standards side, the most prominent player is the National Institute of Standards and Technology (NIST). NIST has a huge number of security publications, including nine Federal Information Processing Standards (FIPS) and well 100 active Special Publications (SP) that provide guidance on virtually all aspects of cybersecurity. Other organization that have produced cybersecurity standards and guidelines include the ITU-T, International Organization for Standardization (ISO), and the Internet Society (ISOC).

The European Union Agency for Network and Information security (ENISA) is working on the National Cyber Security Strategies (NCSS) for the EU-28-member states. ENISA's work in supporting these strategies has focused on the analysis of existing NCSS; on the development and implementation of NCSS; on outlining and raising awareness of good practice to provide guidance and practical tools to the Member States for evaluating their NCSS. A common objective of every European national cyber security strategy is collaboration to enhance cyber security across all levels, from threat information sharing to awareness raising. Collaboration is often achieved through two formal structures: Information Sharing and Analysis Centres (ISACs) and Public Private Partnerships (PPPs).

A wide variety of technical approaches are involved, including cryptography, network security protocols, operating system mechanisms, database security schemes, and malware identification. The areas of concern are broad, including stored data, data communications, human factors, physical asset and property security, and legal, regulatory, and contractual concerns.

In addition, a number of professional and industry groups have produced best practices documents and guidelines. The most important such document is the Standard of Good Practice for Information Security, produced by the Information Security Forum (ISF). This 300-plus-page document provides a wide range of

best practices representing the consensus of industry and government organizations. Other respected organizations, including the Information Systems Audit and Control Association (ISACA) and the Payment Card Industry (PCI), have produced a number of similar documents.

There is an ongoing need to maintain high confidence in the cybersecurity capability in the face of evolving IT systems, relationships with outside parties, personnel turnover, changes to the physical plant, and the ever-evolving threat landscape.

The ISF is an independent, not-for-profit association of leading organizations from around the world. ISF members fund and cooperate in the development of a practical research program in information security. The most significant activity of the ISF is the ongoing development of the Standard of Good Practice for Information Security (SGP). This document is a business-focused, comprehensive guide to identifying and managing information security risks in organizations and their supply chains. The development of the standard is based on the results of four main groups of activities, shown in Figure 3.

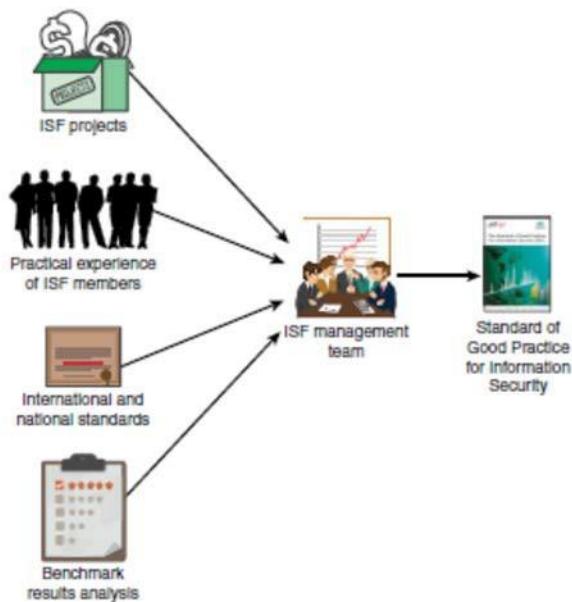


Figure 3 - Basis for the ISF Standard of Good Practice for Information Security

The SGP is organized into 17 categories, each of which is broken down into two areas. Each area is further broken down into a number of topics, or business activities, for a total of 132 topics. It is informative to consider the 17 SGP categories as being organized into three principal activities (see Figure 4):

1. Planning for cybersecurity: Developing approaches for managing and controlling the cybersecurity function(s); defining the requirements specific to a given IT environment; and developing policies and procedures for managing the security function
2. Managing the cybersecurity function: Deploying and managing the security controls to satisfy the defined security requirements

3. Security assessment: Assuring that the security management function enables business continuity; monitoring, assessing, and improving the suite of cybersecurity controls

The arrows in Figure 4 suggest that these activities occur an ongoing process.

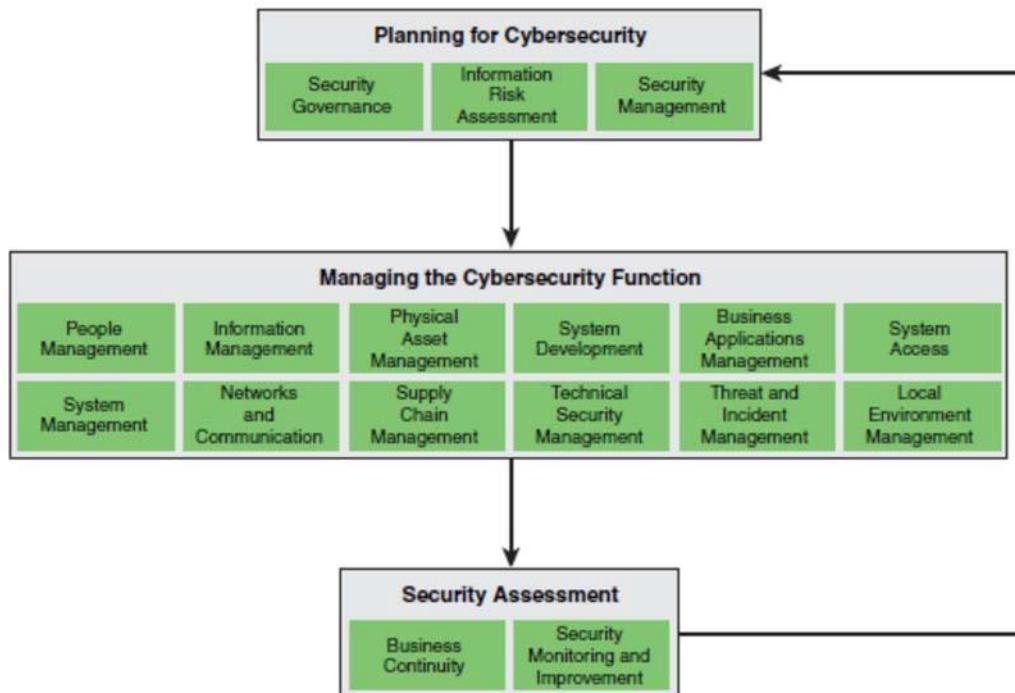


Figure 4 - Categories in the Standard of Good Practice for Information Security

ISMS overview and vocabulary	ISMS requirements		ISMS guidelines		ISMS sector-specific guidelines	
27000 ISMS overview	27001 ISMS requirements	27006 Audit and certification of ISMS	27002 Code of practice for IS controls	27003 ISMS implementation	27010 Intersector/interorganizational comms	27011 Telecomms organizations
	27009 Sector-specific application		27004 ISM measurement	27005 IS risk management	27015 Financial services	27017 IS controls for cloud services
			27007 ISMS auditing	TR 27008 Auditors on IS control	27018 Protection of PII in public clouds	27019 Energy utility industry PCS
			27013 Integrated implementation of 27001/20000	27014 Governance of IS		
			TR 27016 Organizational economics	27036 IS for supplier relationships		

ISMS = Information Security Management System  
PII = personally identifiable information  
PCS = process control systems

Figure 5 - ISO 27000 ISMS Family of Standards

**The ISO/IEC 27000 Suite of Information Security Standards:** Perhaps the most important set of standards for cybersecurity is the ISO 27000 suite (Figure 5) of information security standards. The ISO is an international agency for the development of standards on a wide range of subjects. It is a voluntary, nontreaty organization whose members are designated standards bodies of participating nations as well as nonvoting observer organizations. Although the ISO is not a government body, more than 70% of ISO member bodies are government standards institutions or organizations incorporated by public law. Most of the remainder have close links with the public administrations in their own countries.

**ISO 27001:** Although ISO 27001 is brief, it is an important document for organizational executives with security responsibility. It is used to define the requirements for an ISMS in such a way that it serves as a checklist for certification. Certification gives credibility to an organization, demonstrating that a product or service meets the expectations of the organization's customers.

**ISO 27002:** Although ISO 27001 lays out the requirements for an ISMS, it is rather general, and the specification of the requirements is only nine pages long. Of equal importance is ISO 27002, Code of Practice for Information Security Controls, which provides the broadest treatment of ISMS topics in the ISO 27000 series and comprises 90 pages.

## Aim/Objectives

The scope of this week is to provide the student with the major standards of cyber security. The importance of International standards is discussed with an emphasis on ISO/IEC 27000 suite. It is essential for the student to be aware that cyber security requires a well-defined approach that is based on well-accepted standards such as the ISO/IEC 27000 suite.

## Learning Outcomes

Upon successful completion of this course, students should be able to:

- Explain the need for standards and best practices documents in cybersecurity.
- Present an overview of the Standard of Good Practice for Information Security.
- Explain the difference between ISO 27001 and ISO 27002.
- Discuss the role of the National Institute of Standards and Technology (NIST)
- Cybersecurity Framework and how it differs from the objectives of ISO 27002.
- Discuss the role of the European Union agency for network and information security (ENISA).

## Key Words

National Institute of standards and Technology (NIST)	European Union agency for network and information security (ENISA)	ISO 27000
ISO 27001	ISO 27002	cybersecurity system

## Annotated Bibliography

### Basic

**Effective Cybersecurity: A Guide to Using Best Practices and Standards** 1st Edition, 2019, Willian Stallings, ISBN-13: 978-0134772806, ISBN-10: 0134772806

This week is based on Chapter 1 of the book that is related to the most significant sources and documentation for effective cybersecurity management and a discussion of the effective use of standards and best practices documents. This is a new book for effective cyber security with emphasis on the understanding of the main concepts of cyber security risk analysis and management. The book is addressed to people in both IT and security management, people tasked with maintaining IT security, and a wide range of others interested in cybersecurity and information security.

### Supplementary

Power point presentation slides available in the platform

[NIST Cybersecurity Site](#): A range of resources related to NIST programs and documents on cybersecurity.

[Information Security Forum](#): Many resources, including the Standard of Good Practice. Many of these require that you be a member but there are some useful free resources.

[ITU-T Recommendations](#): The complete collection of Recommendations, most of which are free.

[Center for Internet Security](#): Provides a collection of controls, best practices, and threat reports.

[ISACA](#): Good collection of documents and other resources.

[ENISA](#): Home page for the EU Agency for Network and Information Security. Excellent collection of documents.

[Communications Security Establishment](#): Home page for the Government of Canada's national cryptologic agency. A number of useful documents.

## **Suggestions for further reading**

- [7] Center for Internet Security, The CIS Critical Security Controls for Effective Cyber Defense version 7. 2018. <https://www.cisecurity.org>

## **Self-Assessment Exercises**

### **Exercise 2.1**

In your opinion why security standards are so important?

### **Exercise 2.2**

What is the most significant activity of the Information Security Forum (ISF)?

## **Recommended time for the student to work**

15 hours

## CYBER SECURITY FRAMEWORKS

3<sup>rd</sup> Week

### Summary

In this week, we will discuss on the European and international cyber security frameworks. The most important cybersecurity frameworks that have been adopted by many countries worldwide are those defined by the National Institute of Standards and Technology (NIST), USA and the European Union Agency for Network and Information Security (ENISA).

### Introductory Remarks

In this week, we will discuss on the European and international cyber security frameworks. The National Institute of Standards and Technology (NIST), USA, provides a policy framework of computer security guidance for how private sector organizations in the United States can assess and improve their ability to prevent, detect, and respond to cyber-attacks. The framework has been translated to many languages and is used by the governments of Japan and Israel, among others. It "provides a high level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes."

Despite their national scope, NIST Federal Information Processing Standards (FIPS) and Special Publications (SP) have a worldwide impact. In the area of information security, the NIST Computer Security Resource Center (CSRC) is the source of a vast collection of documents that are widely used in the industry. The NIST Cybersecurity Framework consists of three components (see Figure 6):

- Core: Provides a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors.
- Implementation tiers: Provide context on how an organization views cybersecurity risk and the processes in place to manage that risk.
- Profiles: Represents the outcomes based on business needs that an organization has selected from the Framework Core categories and subcategories.

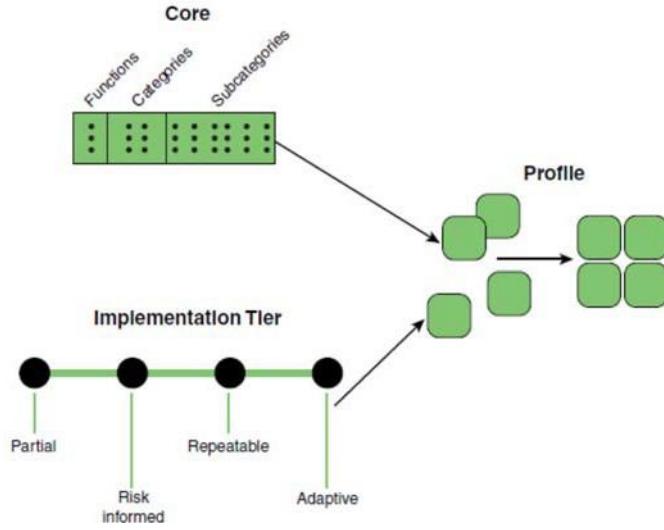


Figure 6 - NIST Cybersecurity Framework Components

**ENISA:** The European Union Agency for Network and Information Security (ENISA) is a centre of expertise for cyber security in Europe. The Agency is located in Greece with its seat in Heraklion Crete and an operational office in Athens. ENISA is actively contributing to a high level of **network and information security (NIS)** within the Union, since it was set up in 2004, to the development of a culture of NIS in society and in order to raise awareness of NIS, thus contributing to proper functioning of the internal market. The Agency works closely together with Members States and private sector to deliver advice and solutions. This includes, the pan-European Cyber Security Exercises, the development of National Cyber Security Strategies, CSIRTs cooperation and capacity building, but also studies on secure Cloud adoption, addressing data protection issues, privacy enhancing technologies and privacy on emerging technologies, eIDs and trust services, and identifying the cyber threat landscape, and others. ENISA also supports the development and implementation of the European Union's policy and law on matters relating to NIS. ENISA's approach is illustrated below by presenting its activities in three areas (Figure 7):

- Recommendations.
- Activities that support policymaking and implementation.
- 'Hands On' work, where ENISA collaborates directly with operational teams throughout the EU.



Figure 7 – ENISA approach

**The CIS Critical Security Controls for Effective Cyber Defense:** The Center for Internet Security (CIS) is a nonprofit community of organizations and individuals seeking actionable security resources. The CIS identifies specific security techniques and practices that the CIS group of experts agree are important. A major contribution of CIS is The CIS Critical Security Controls for Effective Cyber Defense (CSC) [CIS18]. CSC focuses on the most fundamental and valuable actions that every enterprise should take. Value here is determined by knowledge and data—the ability to prevent, alert, and respond to the attacks plaguing enterprises today.

**COBIT 5 for Information Security:** Control Objectives for Business and Related Technology (COBIT) is a set of documents published by ISACA, which is an independent, nonprofit, global association engaged in the development, adoption, and use of globally accepted, industry-leading knowledge and practices for information systems. COBIT 5, the fifth version of the set of documents to be released, is intended to be a comprehensive framework for the governance and management of enterprise IT. Of particular concern for this course is the section of COBIT 5 that deals with information security.

**Payment Card Industry Data Security Standard (PCI DSS):** The PCI-DSS, a standard of the PCI Security Standards Council, provides guidance for maintaining payment security. The standard sets the technical and operational requirements for organizations accepting or processing payment transactions and for software developers and manufacturers of applications and devices used in those transactions.

**ITU-T Security Documents:** The International Telecommunication Union (ITU) is a United Nations specialized agency—hence the members of ITU-T are governments. The U.S. representation is housed in the Department of State. The ITU's charter states that it is “responsible for studying technical, operating, and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.” Its primary objective is to standardize, to the extent necessary, techniques and operations in telecommunications to achieve end-to-end compatibility of international telecommunication connections, regardless of the countries of origin and destination. The ITU Telecommunication Standardization Sector (ITU-T) fulfills the purposes of the ITU relating to telecommunications standardization by studying technical, operating, and tariff questions and adopting recommendations on them with a view to standardizing telecommunications on a worldwide basis.

## Aim/Objectives

The scope of this week is to provide the student with the major cyber security frameworks worldwide. Two of them and the most important are presented; the USA-based NIST framework and the EU-based ENISA framework. It is essential for the student to be aware of these two major cybersecurity frameworks, along with best practices that are followed by governments and Industry sectors.

## Learning Outcomes

Upon successful completion of this course, students should be able to:

- Present an overview of the Standard of Good Practice for Information Security.
- Explain the difference between ISO 27001 and ISO 27002.
- Discuss the role of the National Institute of Standards and Technology (NIST)
- Discuss the role of the European Union agency for network and information security (ENISA).
- Explain the value of the Center for Internet Security (CIS) Critical Security Controls.

## Key Words

National Institute of standards and Technology (NIST)	European Union agency for network and information security (ENISA)	ISO 27000
PCI DSS	COBIT5	National Cyber Security Strategies (NCSS)

## Annotated Bibliography

### Basic

**Effective Cybersecurity: A Guide to Using Best Practices and Standards** 1st Edition, 2019, Willian Stallings, ISBN-13: 978-0134772806, ISBN-10: 0134772806

This week is based on Chapter 1 of the book that is related to the most significant sources and documentation for effective cybersecurity management and a discussion of the effective use of standards and best practices documents. This is a new book for effective cyber security with emphasis on the understanding of the main concepts of cyber security risk analysis and management. The book is

addressed to people in both IT and security management, people tasked with maintaining IT security, and a wide range of others interested in cybersecurity and information security.

## **Supplementary**

Power point presentation slides available in the platform

Video: [The Cybersecurity Framework - National Institute of Standards and Technology](#)

Video: [European Network and Information Security Agency](#)

[NIST Cybersecurity Site](#): A range of resources related to NIST programs and documents on cybersecurity.

[NIST Computer Security Resource Center](#): This is an essential resource. Provides access to CSRC projects, news, huge publications library, and an extensive glossary.

[Information Security Forum](#): Many resources, including the Standard of Good Practice. Many of these require that you be a member but there are some useful free resources.

[PCI Security Standards Council](#): Provides free access to PCI-DSS, other standards, and supporting documents.

[ITU-T Recommendations](#): The complete collection of Recommendations, most of which are free.

[Center for Internet Security](#): Provides a collection of controls, best practices, and threat reports.

[ISACA](#): Good collection of documents and other resources.

[ENISA](#): Home page for the EU Agency for Network and Information Security. Excellent collection of documents.

[Communications Security Establishment](#): Home page for the the Government of Canada's national cryptologic agency. A number of useful documents.

## **Suggestions for further reading**

- [8] Center for Internet Security, The CIS Critical Security Controls for Effective Cyber Defense version 7. 2018. <https://www.cisecurity.org>

## **Self-Assessment Exercises**

### **Exercise 3.1**

What is the main role of ENISA?

**Exercise 3.2**

Explain briefly the five core functions in the NIST Cybersecurity Framework.

**Recommended time for the student to work**

15 hours

### Summary

This week will discuss about **risk management** in general. We begin by explaining what risk is and presenting the terminology we need in order to obtain a better understanding on the topic. Thereafter we introduce risk management and explain what it involves for an organization to manage risk in a systematic and effective manner. Subsequently, we look more into the details of the risk management process and its sub-processes.

### Introductory Remarks

Let us start with the definition of what risk is. ***Risk is the potential that something goes wrong and thereby causes harm or loss.*** The gravity of a risk depends on its likelihood to occur and its consequence. The consequence is the impact on an asset, and an asset is an object of value that we want to protect. In order to convey more precisely, what this definition means, we need to explain the concepts it refers to, namely incident, likelihood, consequence, and asset. Figure 8 below depicts the risk concept and we can identify its main elements.

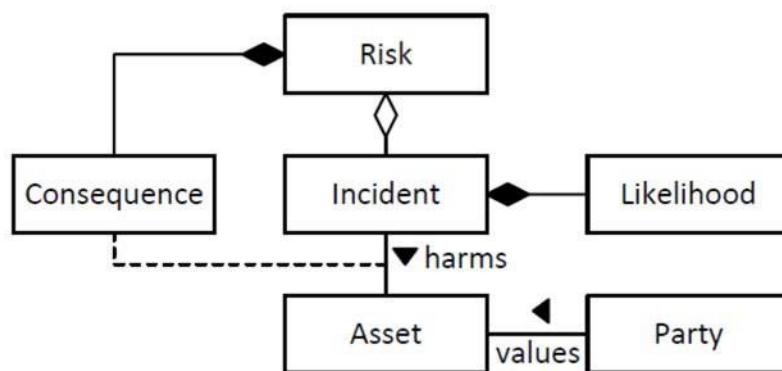


Figure 8 – Risk concepts

Now let us take a closer look at the risk management. All organizations are exposed to risk, and most organizations do some kind of risk management. However, if we aim to precisely understand the kinds

and nature of the risks, and to manage them in a systematic and effective manner, we need a well-defined process for risk management. We moreover need to understand the underlying principles and framework for the risk management process.

In order to convey more precisely, what this definition means, we need to explain the concepts it refers to, namely **incident**, **likelihood**, **consequence**, and **asset**. We start with the notion of incident. When we discuss or assess risk, we need to be careful to distinguish between its causes and the potential occurrence of the incident that constitutes the risk. The definition of the term “incident” makes it clear that risk is about the occurrence of harmful events. For a risk management process to be adequate, efficient, and effective, it should be based on a risk management framework. This framework should in turn comply with the basic principles for risk management.

The **risk management framework** must comply with the basic principles for risk management. The principles apply to all kinds of risk management, but organizations need to understand what the principles mean for them and for their own framework for risk management. **ISO 31000** lists eleven such principles. Among others, these include the principles that risk management shall create and protect value, that risk management shall be an integral part of all organizational processes, that risk management shall be part of decision-making, and that risk management shall be based on the best available information.



Figure 9 – Risk management process

Figure 9 presents the risk management process in more detail. **Risk assessment** is a finite process that organizations conduct on a regular basis. The two others, namely communication and consultation and monitoring and review, are continuous activities.

By **communication and consultation**, we mean activities aiming to provide, share, or obtain information and to interact with stakeholders regarding the management of risk. A stakeholder in a risk management context is a person or organization that may affect or be affected by the organization that is the subject of the risk management.

By **risk assessment**, we mean activities aiming to understand and document the risk picture for specific parts or aspects of a system or an organization. The assessment includes the estimation of the risk level, as well as the identification of options for risk treatment. The results serve as a decision basis for risk management, including the decision of which controls and measures to implement to mitigate risk. The risk assessment process is divided into five steps, as illustrated in Figure 10.

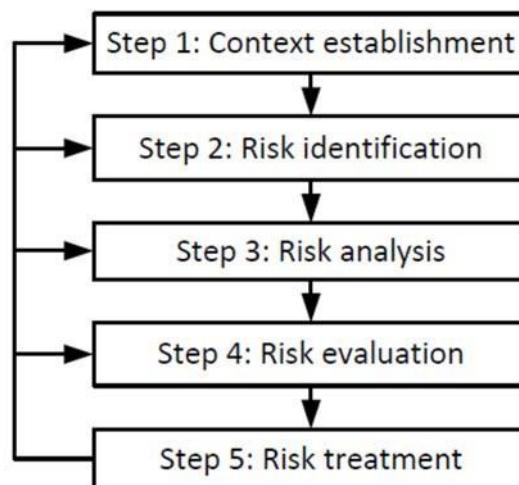


Figure 10 – Risk assessment process

**Monitoring and review** apply both to the underlying risk management framework and to the risk management process, but specifically also to the identified risks and to the measures that the organization implements in order to treat risks. Monitoring is the continual checking, supervising, critically observing, or determining the current status in order to identify deviations from the expected or required status.

The review activity is to determine the suitability, adequacy, and effectiveness of the risk management process and framework, as well as risks and treatments. The main purposes of the monitoring and review process are as follows [13]:

- Ensure that controls are effective and efficient
- Obtain further information to improve risk assessment
- Analyze and learn lessons from incidents, changes, trends, successes, and failures

- Detect changes
- Identify emerging risks

## Aim/Objectives

The scope of this week is to introduce the student with the fundamental knowledge of risk management. We start our discussion with the definition of risk management based on the International Organization for Standardization (ISO) definitions. We will see what the main elements of a risk management are and will analyse each one of them. We will also discuss the risk management processes namely risk assessment, communication and consultation and monitoring and review. It is very important for the student to be able to define and explain these topics because these is the fundament knowledge for cybersecurity risk analysis and management.

## Learning Outcomes

Upon successful completion of this course, students should be able to:

- State and explain what incident is.
- Explain how risks can be defined.
- State and explain what risk management framework is.
- State what Risk management process is.
- State what Risk assessment process is.

## Key Words

incident	risk management framework	Information security
communication and consultation	risk assessment	Monitoring and review
likelihood	consequence	asset

## Annotated Bibliography

### Basic

Cyber-Risk Management, Atle Refsdal, Bjørnar Solhaug, Ketil Stølen, ISSN 2191-5768 ISSN 2191-5776 (electronic), Springer Briefs in Computer Science, ISBN 978-3-319-23569-1 ISBN 978-3-319-23570-7 (eBook), DOI 10.1007/978-3-319-23570-7, Library of Congress Control Number: 2015950450.

Available to all EUC students via the <https://www.openathens.net/> service.

This week we will follow and study Chapter 2 “Risk Management”.

## **Supplementary**

Power point presentation slides available in the platform

Video: [Risk management basics by David Hillson](#)

## **Suggestions for further reading**

The terminology introduced in this chapter is largely based on the risk management vocabulary of ISO Guide [14]. The presentation of the risk management process and how this process relates to the risk management framework and principles is based on the ISO 31000 risk management standard [13]. This standard also makes use of the vocabulary of ISO Guide.

Note that ISO 31000 refers to risk assessment as the three activities of risk identification, risk analysis, and risk evaluation. In this chapter, we use the term “risk assessment” in a broader sense. It also includes the activities of context establishment and risk treatment. There are two reasons for this: First, ISO 31000 offers no term denoting the process consisting of these five activities. Second, in our view, this better reflects how the term “risk assessment” is used in practice.

In addition to these ISO standards, we refer the interested reader to the ISO/IEC 27005 [15] standard on information security risk management. This standard is much more limited than ISO 31000 as it concerns information security risks, but because it builds closely on the latter, it gives some good insights into many principles of risk management in general.

For a useful and quite comprehensive overview and classification of risk assessment techniques, the reader is referred to IEC 31010 [16]. The overview includes techniques for risk identification, risk analysis, and risk evaluation.

## **References**

- [9] International Organization for Standardization: ISO 31000 – Risk management – Principles.
- [10] International Organization for Standardization: ISO Guide 73 – Risk management – Vocabulary (2009).
- [11] International Organization for Standardization / International Electrotechnical Commission: ISO/IEC 27005 – Information technology – Security techniques – Information security risk management (2011).

- [12] International Organization for Standardization / International Electrotechnical Commission: ISO/IEC 31010 – Risk management – Risk assessment techniques (2009).
- [13] International Organization for Standardization: ISO 31000 – Risk management – Principles.
- [14] International Organization for Standardization: ISO Guide 73 – Risk management – Vocabulary (2009).
- [15] International Organization for Standardization / International Electrotechnical Commission: ISO/IEC 27005 – Information technology – Security techniques – Information security risk management (2011).
- [16] International Organization for Standardization / International Electrotechnical Commission: ISO/IEC 31010 – Risk management – Risk assessment techniques (2009).

## **Self-Assessment Exercises**

### **Exercise 4.1**

Explain the stages of the risk management process.

### **Exercise 4.2**

State the five steps of the risk assessment process.

## **Recommended time for the student to work**

15 hours

## CYBER-RISK MANAGEMENT

5<sup>th</sup> Week

### Summary

In this week, we will discuss about risk management in the domain of cyber-systems. We will highlight what is special about cyber-systems and cyber-threats from a risk management perspective, focusing in particular on the nature of cyber-risks and the options and means we have for managing them. First, we will explain what we mean by cyber-risk. Thereafter we will specialize the three main processes of risk management to cope with cyber risk.

### Introductory Remarks

Let us start our discussion with the meaning of cyber-risk. We have to understand that cyberspace has considerable impact on the kind and nature of the threats and the risks that may appear, as well as on the procedures and techniques to conduct risk management and risk assessment. One striking aspect of cyberspace is that it is potentially extremely far-reaching. This means that the possible threat sources can reside anywhere in the world, yet with the potential of causing damage deep inside the cyber-system of our concern. Another crucial aspect is that a substantial share of cyber-threats are malicious; they are caused by adversaries with motives and intentions. On the other hand, there are also non-malicious cyber-threats.

**Cyber-risk management** is concerned with risks caused by cyber-threats. A **cyber-risk** is a risk that is caused by a cyber-threat. Although we are concerned with cyber-systems, it is important to understand that cyber-risk is not the same as any risk that a cyber-system can be exposed to. Cyber risks are limited to the risks that are caused by cyber-threats. The risk of a server on which our cyber-system is running being damaged by water flooding, for example, is not a cyber-risk unless a cyber-threat is a contributing factor. Confidentiality breaches due to virus attacks via cyberspace and loss of availability due to DoS attacks, however, are examples of cyber-risks.

Next, in order to understand the nature of cyber-risks and how to manage them we distinguish between malicious cyber-risk and non-malicious cyber-risk. We say that a cyber-risk is malicious if it is (at least partly) caused by a malicious threat and non-malicious otherwise.

Please notice that by this definition some cyber-risks are both malicious and non-malicious. These cyber-risks can be caused by either a malicious threat or a non-malicious threat. Consider, for example, an incident of unauthorized access to some sensitive data. A potential occurrence of this incident as caused by a hacker is a malicious cyber-risk, while a potential occurrence that is caused by accidental posting of the data on an open website is a non-malicious cyber-risk.

There are also incidents that happen only due to the combined occurrence of a malicious and a non-malicious threat. An example of this is an intrusion that occurs while the intrusion detection and prevention system is down due to an accidental failure. We classify these as malicious cyber-risks since they cannot occur without the malicious threat.

The Venn diagram of Figure 11 provides a summary: Cyber-risks are the union of malicious and non-malicious cyber-risks, and cyber-risks are only a subset of the risks that cyber-systems can be exposed to. Moreover, the intersection between malicious and non-malicious cyber-risk represents the cyber-risks that can be caused by either a malicious threat or a non-malicious threat.

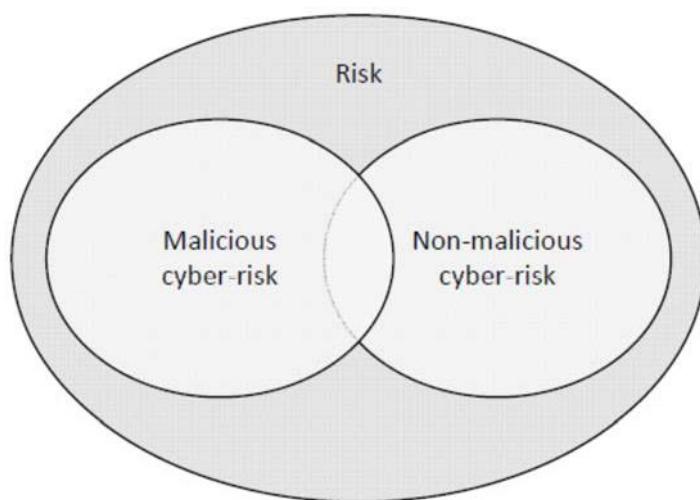


Figure 11 – Malicious and non-malicious cyber-risk

Let us recall now what we discussed the previous week. The process of communication and consultation described in the previous week for risk management in general is equally suited to the narrower domain of cyber-risk. There are, however, certain issues imposed by cyberspace that require particular attention.

First, due to the nature of cyberspace, cyber-systems may potentially have stakeholders everywhere. These stakeholders may be consumers of services or information provided by the cyber-system of our concern, or they may be providers of services to this cyber-system. It is important to consider all stakeholders, both individuals and organizations, when determining relevant sources of information and identifying who may be affected by cyber-risks. We moreover need plans and procedures for how to provide, share, obtain, and make use of the information of relevance.

Second, also due to cyberspace, there may potentially be adversaries everywhere, and any major incident somewhere in the world may have considerable impact on our cyber-system. Coping with these numerous parameters requires increased focus on information collection by monitoring and surveillance.

For the process to be efficient, it is necessary to establish a classification and categorization of information. For the purpose of representing and understanding relevant information, organizations may use established standards or repositories. The objective is to maintain a repository of up-to-date information regarding, for example, cyber-threats, vulnerabilities and incidents, potential and confirmed adversary profiles, current strategies and mechanisms for cyber-risk mitigation, and so forth. The classification and categorization may also include characterizations of cyber-systems, including, for example, assets and cyber-system profiling.

Concerning cyber-risk assessment, there are two things in particular that distinguish risk assessment in the context of cyber-systems from the general case. First, the potentially far-reaching extent of a cyberspace implies that also the origins of threats are widespread, possibly global. Second, the number of potential threat sources and threats, both malicious and non-malicious, is very large. In combination, this means that the search area and the number of sources of potentially relevant information about cyber-risk are extremely large and may seem overwhelming. We therefore need procedures and techniques that provide guidance and direction.

Figure 12 shows the specialization of the risk assessment process to cybersystems. The most obvious difference from the general case is that the risk identification step is divided into two separate steps: Step 2a focusing on malicious cyber-risks and Step 2b focusing on non-malicious cyber-risks. We make this distinction because the nature of threats, threat sources, and vulnerabilities, and how to approach their identification, is highly dependent on whether we are dealing with malicious intent or not.

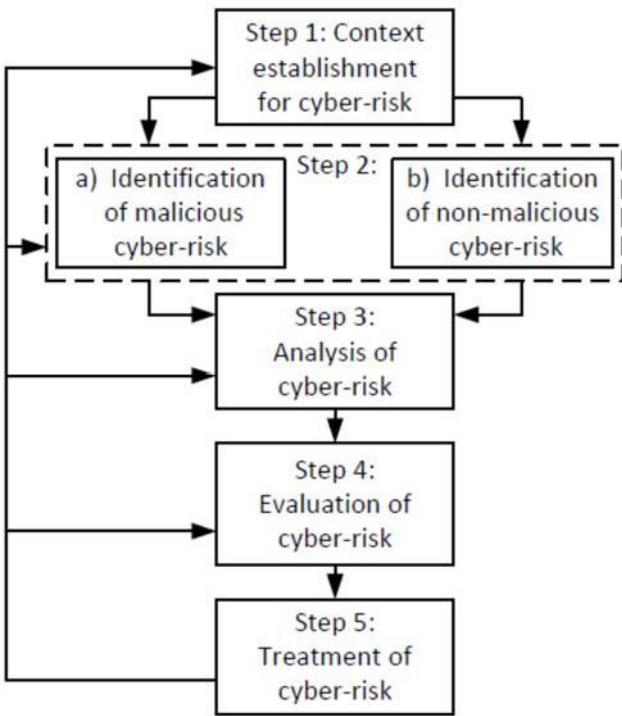


Figure 12 – Process for cyber risk assessment

The aim of Step 2a is to identify risks based on the potential ways in which such a game can play out. The motives, intentions, abilities, skills, resources, and so forth of the adversary are essential in this context. A good starting point in the identification of cyber-risks caused by malicious threats is therefore the identification and characterization of potential threat sources. In conducting Step 2b we recommend instead to start from the assets and the ways in which they may be harmed. In this way, we make sure that we focus strictly on what we seek to protect, and that we proceed in a manner that is both effective and efficient.

The process of monitoring and review as described in Risk Management makes a clear distinction between

- monitoring and review of risk, and
- monitoring and review of risk management

In the first case, we are concerned with the system in question; in the second case, we focus on the implementation and operation of the risk management process for the system in question. This distinction is of course also relevant within cyber-risk management.

We benefit from the fact that cyber-systems are computerized, at least to a large degree. The options for monitoring and surveying cyber-risks are numerous. We can, for example, keep logs of the number and frequency of detected attacks or viruses, monitor the network traffic to detect irregularities, gather information from firewalls and intrusion detection systems.

In order to maximize the value of the cyber-risk information that we gather by system monitoring, risk assessments and open repositories, we need efficient and useful means for representing the information. One option is to establish a classification and categorization of information as mentioned previously. An additional option is to establish a risk register where the information is available to all relevant stakeholders.

## Aim/Objectives

The scope of this week is for the student to be able to define the process of cyber risk assessment and identify the five steps of this procedure. The student will be able to distinguish between the malicious and non-malicious cyber risks. It is important for the student to be able to identify the various cyber risks and apply this knowledge in a specific domain/area of interest.

## Learning Outcomes

Upon successful completion of this course, students should be able to:

- Explain what Cyber-risk management is
- State what cyber risk is in the context of cyberspace
- Distinguish between malicious and non-malicious cyber threats
- Define the process for cyber risk assessment
- Elaborate on the importance of monitoring and review of cyber risks.

## Key Words

Cyber Risk	Risk assessment	Malicious cyber risk
Cyber-risk management	Non-malicious cyber risk	Cyber risk review

## Annotated Bibliography

### Basic

Cyber-Risk Management, Atle Refsdal, Bjørnar Solhaug, Ketil Stølen, ISSN 2191-5768 ISSN 2191-5776 (electronic), Springer Briefs in Computer Science, ISBN 978-3-319-23569-1 ISBN 978-3-319-23570-7 (eBook), DOI 10.1007/978-3-319-23570-7, Library of Congress Control Number: 2015950450.

Available to all EUC students via <https://www.openathens.net/> service

This week will focus on Chapter 5 of this book and we will discuss the main concept of the cyber risk management.

## **Supplementary**

Power point presentation slides available in the platform

Video: [What is Cyber Risk? Steve Culp](#)

Video: [Managing Cyber-risk: Unlocking the Mystery of the Boardroom](#)

ENISA has generated an inventory of Risk Management / Risk Assessment tools. A total of 12 tools have been considered. Similarly to the inventory of methods, each tool in the inventory has been described through a template. The template used consists of 22 attributes that describe characteristics of tools. You can find the complete list of these tools (most of them are free tools) in this [Inventory of Risk Management / Risk Assessment Tools](#)

## **Suggestions for further reading**

For up-to-date information about cyber-threats, vulnerabilities, and incidents there are several open lists and repositories that can be used such as the MITRE attack patterns [17] and vulnerability lists [18], as well as the lists of security risks. Such overviews often come with estimates of attack likelihood, vulnerability severity, and incident consequence. There are also several organizations that regularly publish statistics on cyber-incidents and top cyber-risks, such as the open web application security project [19].

Some standards and guidelines on ICT security offer lists of threat sources, threats, and vulnerabilities that can be used as input to the cyber-risk identification. This includes, for example, ISO 27005 [20], ISO 27032 [21] and NIST SP 800-30 [22]. The same kinds of standards and guidelines often offer advice on options for cyber-risk treatment. There is also literature and guidance on attacker modeling, for example as provided by OWASP [23] or the Common Criteria [24].

## **References**

- [17] MITRE: Common attack pattern enumeration and classification (CAPEC). Online: <https://capec.mitre.org/>
- [18] MITRE: Common weakness enumeration (CWE). Online: <http://cwe.mitre.org/>
- [19] OWASP: The open web application security project. Online: <http://www.owasp.org>
- [20] International Organization for Standardization / International Electrotechnical Commission: ISO/IEC 27005 – Information technology – Security techniques – Information security risk management (2011)
- [21] International Organization for Standardization / International Electrotechnical Commission: ISO/IEC 27032 – Information technology – Security techniques – Guidelines for cybersecurity (2005)
- [22] National Institute of Standards and Technology: Guide for conducting risk assessments, special publ. 800-30 (2012).
- [23] OWASP: Testing guide, v4.0 (2013)
- [24] OWASP: Testing guide, v4.0 (2013) Common Criteria: Common methodology for information technology security evaluation – Evaluation methodology, v3.1, rev. 4 (2012).

## **Self-Assessment Exercises**

### **Exercise 5.1**

What cyber risk is? Give a definition.

### **Exercise 5.2**

What are the four steps of the cyber-risk assessment process?

## **Activities**

Nowadays, cyber security management is a serious component of any organization. Consider you are conducting an interview with a Chief Information Security Officer (CIO) in a large organization. What would be the five key questions you were considering to ask? Justify your answer.

## **Recommended time for the student to work**

20 hours

## RISK ASSESSMENT CONCEPTS

6<sup>th</sup> Week

### Summary

This week will go into the core functions of cyber risk management. That is, the risk assessment concepts and how they contribute in the evaluation of cyber vulnerabilities and threats.

### Introductory Remarks

The ultimate objective of risk assessment is to enable organization executives to determine an appropriate budget for security and, within that budget, implement security controls to optimize the level of protection. This objective is met by providing an estimate of the potential cost to the organization of security breaches, coupled with an estimation of the likelihood of such breaches.

While the utility of risk assessment should be obvious, and indeed, it must be considered essential, it is well at the outset to recognize its limitations, which are clearly summarized in Foundational Cybersecurity Research: Improving Science, Engineering, and Institutions. If the scale of the effort is too ambitious, projects become large, complicated, and unreviewable, with a tendency to leave out things that are not easily quantified. On the other hand, if effective ways of calculating risk are not employed, managers tend to underestimate the magnitude of the risk and choose to invest in other areas that are understood better and lead to clear payoffs. Thus, responsible executives need to develop a plan for risk assessment that is balanced between too much and too little. Fortunately, relying on well-accepted best practices, such as those in the Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP), makes it possible to develop a systematic approach that incorporates best practices that are reasonable for a given organization.

**Risk assessment is a complex subject that is more art than science and calls for considerable management judgment.** A good way to begin looking at risk assessment is to consider the terminology on definitions in ISO 27005, Information Security Risk Management System Implementation Guidance. Nearly identical terminology is used in two other important documents: SP 800-30, Guide for Conducting Risk Assessments, and X.1055, Risk Management and Risk Profile Guidelines for Telecommunication Organizations.

Threats and vulnerabilities need to be considered together. A **threat** is the potential for a threat agent to intentionally or accidentally exploit a vulnerability, which is a weakness in a system's security procedures, design, implementation, or internal controls. A threat acting on a vulnerability produces a security violation, or breach. The level of risk is a measure that an organization can use in assessing the need for and the expected cost of taking remedial action in the form of risk treatment. Figure 13 illustrates in general terms a universally accepted method for determining the level of risk.

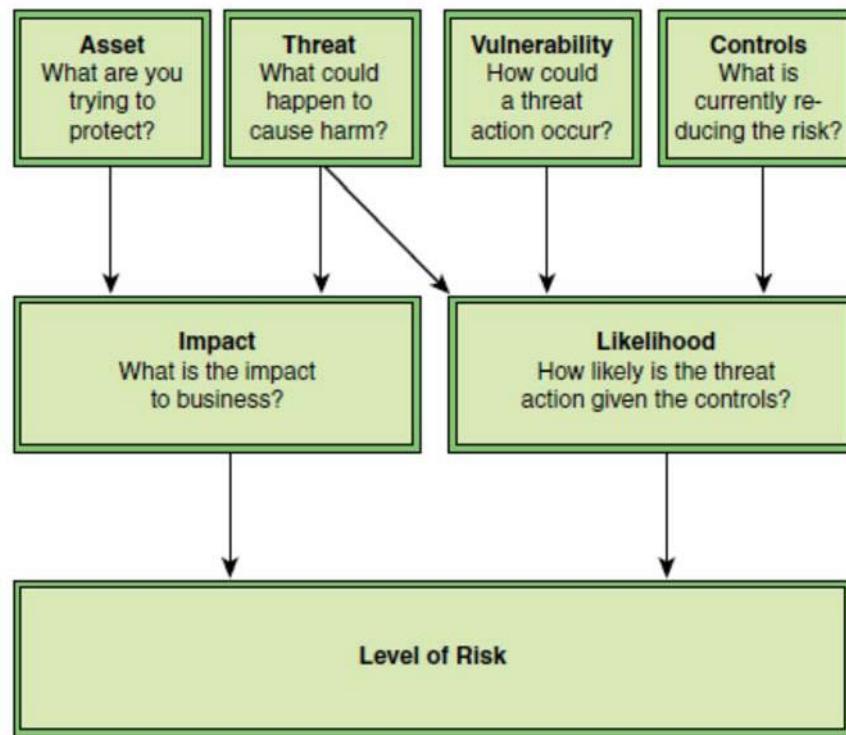


Figure 13 – Determining Information Security Risk

Two main threads, impact and likelihood, should be pursued in parallel. An organization pursues the following tasks related to these threads:

- **Impact:** Consider these two elements in determining impact:
  - Assets: Develop an inventory of the organization's assets, which includes an itemization of the assets and an assigned value for each asset. These include intangible assets such as reputation and goodwill, as well as tangible assets, such as databases, equipment, business plans, and personnel.
  - Threat: For each asset, determine the possible threats that could reduce the value of that asset.

Then, for each asset, determine the impact to the business, in terms of cost or lost value, of a threat action occurring.

- **Likelihood:** Consider the three elements in determining likelihood:
  - Threat: For each asset, determine which threats are relevant and need to be considered.

- Vulnerability: For each threat to an asset, determine the level of vulnerability to the threat. That is, determine specifically for an asset how a threat action could be achieved.
- Controls: Determine what security controls are currently in place to reduce the risk.

### Risk Assessment Challenges

An organization faces enormous challenges in determining the level of risk. In general terms, these challenges fall into two categories: the difficulty of estimating and the difficulty of predicting. Consider first the problem of estimation of each of the four elements that contribute to determining risk:

- **Asset:** An organization needs to put a value on individual assets and how that value may be reduced by a specific threat—in other words, the impact value.
- **Threat:** In determining the threats facing an organization, there is past experience to go on and, as discussed subsequently, numerous publicly available reports list current threats and their corresponding frequencies. Even so, it should be clear that it is difficult to determine the entire range of threats that are faced as well as the likelihood of any threat being realized.
- **Vulnerability:** An organization may face security vulnerabilities that it is not aware of. For example, software vendors have been known to delay revealing a security vulnerability until a patch is available or even delaying releasing a patch to a portion of a vulnerability until a complete patch is available. Further, a patch may introduce new vulnerabilities. As another example, a company may have a fireproof barrier constructed around a data center enclosure. But if the contractor does not install a barrier that meets the specification, there may be no way for the company to know this.
- **Controls:** Controls are implemented to reduce vulnerability and therefore reduce the likelihood of particular threats being realized. However, it may be very difficult to assess the effectiveness of given controls, including software, hardware, and personnel training. For example, a particular threat action may be relatively unlikely, but controls may be introduced because of the high impact in the event that the threat action succeeds. But, if the event rarely occurs, the organization has difficulty in determining whether the control has the desired effect. The threat action may be artificially generated to test the system, but this artificial action may not be realistic enough to get a true picture of how effective a control is.

Another challenge in risk assessment is the difficulty of predicting future conditions. Again, considering the four elements, the following problems emerge.

- **Asset:** Whether the planning period is one year, three years, or five years, changes in the value of an organization's assets complicate the effort to estimate the impact of a security threat. Company expansion, software or hardware upgrades, relocation, and a host of other factors may come into play.
- **Threat:** It is difficult at best to assess the current threat capability and intentions of potential adversaries. Future projections are even more subject to uncertainty. Entire new types of attack may emerge in a very short period of time. And, of course, without complete knowledge of the threat, it is impossible to provide a precise assessment of impact.
- **Vulnerability:** Changes within the organization or its IT assets may create unexpected vulnerabilities. For example, if an organization migrates a substantial portion of its data assets to a cloud service provider, the degree of vulnerability of that provider may not be known to the organization with a high level of confidence.

- **Controls:** New technologies, software techniques, or networking protocols may provide opportunities for strengthening an organization's defenses. But it is difficult to predict the nature of these new opportunities, much less their cost, and so resource allocation over the planning period may not be optimal.

## Aim/Objectives

The scope of this week is to introduce the risk assessment concept. It is important for the student to be able to explain the main concept of the risk assessment process with the use of internationally accepted methods on risk assessment.

## Learning Outcomes

Upon successful completion of this course, students should be able to:

- Explain the purpose of the risk assessment process
- Understand the methodology of the of the risk assessment process
- Describe what threat is in the context of cyber security
- Describe the method for determining the level of risk
- Describe the main risk assessment challenges

## Key Words

Threat	Impact	likelihood
Vulnerability	Controls	ISO 27005

## Annotated Bibliography

### Basic

**Effective Cybersecurity: A Guide to Using Best Practices and Standards** 1st Edition, 2019, Willian Stallings, ISBN-13: 978-0134772806, ISBN-10: 0134772806

This week is based on Chapter 3 of the book.

### Supplementary

Power point presentation slides available in the platform

Video: [Conducting a cybersecurity risk assessment](#)

### **Suggestions for further reading**

- [25] Ashok, I., "Hackers Spied and Stole from Millions by Exploiting Word Flaw as Microsoft Probed Bug for Months." International Business Times, April 27, 2017.
- [26] Keizer, G., "Experts Contend Microsoft Canceled Feb. Updates to Patch NSA Exploits." Computer World, April 18, 2017.

### **Self-Assessment Exercises –**

#### **Exercise 6.1**

Why is risk assessment needed in an organization?

#### **Exercise 6.2**

Describe the risk assessment challenges that an organization faces.

### **Recommended time for the student to work**

15 hours

## RISK ASSESSMENT PROCESS

7<sup>th</sup> Week

### Summary

After we have seen the risk assessment concepts in the previous week, we will discuss in this week the risk assessment process. It is important to understand how to identify the assets in an organization and the associated threats and vulnerabilities.

### Introductory Remarks

#### Asset Identification

Risk identification is the identification of the assets, threats, existing controls, vulnerabilities, and impacts relevant to the organization and that serve as inputs to risk analysis. A first step in risk assessment is to document and determine values for the organization's assets. An **asset is anything of value to the business that requires protection, including hardware, software, information, and business assets**. Many assets of various types can be identified, and the challenge is to develop a uniform way of documenting the assets, the security implications of each, and the costs associated with security incidents related to each. Asset valuation relates directly to business needs. Accordingly, the input for asset valuation needs to be provided by owners and custodians of assets, not by members of the risk assessment team. A generic list of assets is provided below:

- Hardware Assets
- Software Assets
- Information Assets
- Business Assets

#### Threat Identification

Threat identification is the process of identifying threat sources with the potential to harm system assets. Threat sources are categorized into three areas:

- Environmental: Examples include floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and power failure.

- Business resources: Examples include equipment failure, supply chain disruption, and unintentional harm caused by employees.
- Hostile actors: Examples include hackers, hacktivists, insider threats, criminals, and nation-state actors.

The **STRIDE Threat Model**: STRIDE is a threat classification system developed by Microsoft that is a useful way of categorizing attacks that arise from deliberate actions [HERN06]. It involves the following categories:

- Spoofing identity
- Tampering with data
- Repudiation
- Information disclosure
- Denial of service
- Elevation of privilege

**Verizon Data Breach Investigations Report**: Perhaps the most important source of information that an organization can consult is the annual Verizon Data Breach Investigations Report (DBIR). This authoritative and highly respected report is based on data on security incidents systematically collected from a wide variety of organizations. The results in the 2018 report are based on data from more than 53,000 security incidents and over 2,200 data compromises from 65 countries and 67 organizations. The results are broken down by 20 industry sectors, such as accommodation, entertainment, finance, healthcare, manufacturing, public, and utilities.

**Threat Horizon Report**: A useful complement to the DBIR is the annual Threat Horizon Report from the ISF. It differs from the DBIR in two ways. First, it is a more broad-brush treatment, identifying key threat trends rather than detailed threats and detailed target profiles. Second, the Threat Horizon Report attempts to project the likely major threats over the next two years.

**ENISA Threat Landscape Report**: Another very useful source of information is several threat documents from European Union Agency for Network and Information Security (ENISA). One of these is the ENISA Threat Taxonomy (2016), which provides a very detailed breakdown of potential cybersecurity threats. It is organized into a three-level hierarchy of high-level threats, threats, and threat details, and defines dozens of individual threat categories. It provides is a useful checklist for ensuring that an organization considers the full range of threats.

## **Control Identification**

Controls for cybersecurity include any process, policy, procedure, guideline, practice, or organizational structure that modifies information security risk. Controls are administrative, technical, management, or legal in nature. Control identification is defined in ISO 27005 as the process of identifying existing and planned security controls, and suggests the following steps:

1. Review documents containing information about the controls (for example, risk treatment implementation plans). If the processes of information security management are well documented, all existing or planned controls and the status of their implementation should be available.
2. Check with the people with responsibility related to information security (e.g., security manager, building manager, and operations manager) and the users about which controls are really implemented for the information process or information system under consideration.
3. Conduct an on-site review of the physical controls, comparing those implemented with the list of what controls should be there, and checking those implemented to determine whether they are working correctly and effectively.
4. Review results of audits.

## **Vulnerability Identification**

Vulnerability identification is the process of identifying vulnerabilities that can be exploited by threats to cause harm to assets. A vulnerability is a weakness or a flaw in a system's security procedures, design, implementation, or internal controls that could be accidentally triggered or intentionally exploited when a threat is manifested. Vulnerabilities occur in the following areas:

- Technical vulnerabilities: Flaws in the design, implementation, and/or configuration of software and/or hardware components, including application software, system software, communications software, computing equipment, communications equipment, and embedded devices.
- Human-caused vulnerabilities: Key person dependencies, gaps in awareness and training, gaps in discipline, and improper termination of access.
- Physical and environmental vulnerabilities: Insufficient physical access controls, poor siting of equipment, inadequate temperature/humidity controls, and inadequately conditioned electrical power.
- Operational vulnerabilities: Lack of change management, inadequate separation of duties, lack of control over software installation, lack of control over media handling and storage, lack of control

over system communications, inadequate access control or weaknesses in access control procedures, inadequate recording and/or review of system activity records, inadequate control over encryption keys, inadequate reporting, handling and/or resolution of security incidents, and inadequate monitoring and evaluation of the effectiveness of security controls.

- Business continuity and compliance vulnerabilities: Misplaced, missing, or inadequate processes for appropriate management of business risks; inadequate business continuity/contingency planning; and inadequate monitoring and evaluation for compliance with governing policies and regulations.

**Current Description**  
An issue was discovered in the Cisco WebEx Extension before 1.0.7 on Google Chrome, the ActiveTouch General Plugin Container before 106 on Mozilla Firefox, the GpcContainer Class ActiveX control plugin before 10031.6.2017.0126 on Internet Explorer, and the Download Manager ActiveX control plugin before 2.1.0.10 on Internet Explorer. A vulnerability in these Cisco WebEx browser extensions could allow an unauthenticated, remote attacker to execute arbitrary code with the privileges of the affected browser on an affected system. This vulnerability affects the browser extensions for Cisco WebEx Meetings Server and Cisco WebEx Centers (Meeting Center, Event Center, Training Center, and Support Center) when they are running on Microsoft Windows. The vulnerability is a design defect in an application programming interface (API) response parser within the extension. An attacker that can convince an affected user to visit an attacker-controlled web page or follow an attacker-supplied link with an affected browser could exploit the vulnerability. If successful, the attacker could execute arbitrary code with the privileges of the affected browser.

Source: MITRE   Last Modified: 02/01/2017   [View Analysis Description](#)

**CVSS Severity (version 3.0):** [+] Quick Info  
**CVSS v3 Base Score:** 8.8 High  
**Vector:** CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H  
**Impact Score:** 5.9  
**Exploitability Score:** 2.8  
**CVE Dictionary Entry:** [CVE-2017-3823](#)  
**Original release date:** 02/01/2017  
**Last revised:** 04/04/2017  
**Source:** US-CERT/NIST

**CVSS Version 3 Metrics:**  
**Attack Vector (AV):** Network  
**Attack Complexity (AC):** Low  
**Privileges Required (PR):** None  
**User Interaction (UI):** Required  
**Scope (S):** Unchanged  
**Confidentiality (C):** High  
**Integrity (I):** High  
**Availability (A):** High

Figure 14 – NVD Scoring Example

In the area of technical vulnerabilities, it is possible to be more precise and exhaustive. An outstanding resource is the NIST National Vulnerability Database (NVD) and the related Common Vulnerability Scoring System (CVSS), described in NISTIR 7946, CVSS Implementation Guidance. The NVD is a comprehensive list of known technical vulnerabilities in systems, hardware, and software. Figure 14 provides an example of one of the vulnerability entries in the NVD.

## Aim/Objectives

The scope of this week is to explain the various steps of the risk assessment process. We start our discussion with the identification of critical assets of an organization and the explanation of the process for threat identification. We introduce in the discussion the STRIDE Threat Model and its related categories. Threat reports are discussed including those with the highest impact to society. We also discuss and explain the meaning and context of vulnerability and where they occur.

## Learning Outcomes

Upon successful completion of this course, students should be able to:

- Explain the meaning of assets in the context of cyber risk assessment
- Define the main asset categories in the context of cyber risk assessment
- Explain the importance of control identification
- Present an overview of threat identification techniques
- Explain the STRIDE threat model
- Present an overview of vulnerability identification techniques

## Key Words

Scripting languages	Server-side scripting	client-side scripting
Common Gateway Interface (CGI)	Web Script Security	Browser attack

## Annotated Bibliography

### Basic

**Effective Cybersecurity: A Guide to Using Best Practices and Standards** 1st Edition, 2019, Willian Stallings, ISBN-13: 978-0134772806, ISBN-10: 0134772806

This week is based on Chapter 3 of the book.

### Supplementary

Power point presentation slides available in the platform

Presentation: [Threat Modeling with STRIDE](#)

### **Suggestions for further reading**

2017 was the year in which incidents in the cyber threat landscape have led to the definitive recognition of some omnipresent facts. We have gained unwavering evidence regarding monetization methods, attacks to democracies, cyber-war, transformation of malicious infrastructures and the dynamics within threat agent groups. Read more on [ENISA Threat Landscape Report 2017](#)

National Institute of Standards and Technology (NIST). Read this [Guide for Conducting Risk Assessments](#)

### **Self-Assessment Exercises –**

#### **Activities**

##### **Exercise 7.1**

Explain the STRIDE threat model and provide an example

##### **Exercise 7.2**

What are the different types of assets from a risk assessment point of view?

### **Recommended time for the student to work**

15 hours

## RISK ASSESSMENT APPROACHES

8<sup>th</sup> Week

### Summary

In this week, we will focus on how we can conduct risk assessment by using both qualitative and quantitative methods. We will also discuss an important contribution to risk assessment, which is Factor Analysis of Information Risk (FAIR) that was first introduced in 2005.

### Introductory Remarks

#### Quantitative Versus Qualitative Risk Assessment

**Impact** and **likelihood** are two factors of risk assessment that can be treated either quantitatively or qualitatively. For impact, if it seems feasible to assign a specific monetary cost to each of the impact areas, then the overall impact can be expressed as a monetary cost. Otherwise, qualitative terms, such as low, moderate, and high, are used. Similarly, the likelihood of a security incident may be determined quantitatively or qualitatively. The quantitative version of likelihood is simply a probability value, and again the qualitative likelihood can be expressed in such categories as low, medium, and high.

#### Quantitative Risk Assessment

If all factors are expressed quantitatively, it is possible to develop a formula such as the following:

$$\text{Level of risk} = (\text{Probability of adverse event}) \times (\text{Impact value})$$

This is a measure of the cost of security breaches, expressed numerically. It can also be expressed as a residual risk level as follows:

$$\text{Residual risk level} = \frac{(\text{Probability of adverse event})}{(\text{Mitigation factor})} \times (\text{Impact value})$$

In this equation, the mitigation factor reflects the reduction in the probability of an adverse event due to the implementation of security controls. Thus, the residual risk level is equivalent to the expected cost of security breaches with the implementation of controls. If the various factors can be quantified with a

reasonable degree of confidence, then these equations should be used to guide decisions concerning how much to invest in security controls. Figure 15 illustrates this point: As new security controls are implemented, the residual probability of an adverse event declines and, correspondingly, the cost of security breaches declines. However, at the same time, the total cost of security controls increases as new controls are added. The upper curve represents the total security cost, consisting of the cost of security breaches plus the cost of security controls. The optimal cost point occurs at the lowest point of the total cost curve. This represents a level of risk that is tolerable and cannot be reduced further without the expenditure of costs that are disproportionate to the benefit gained.

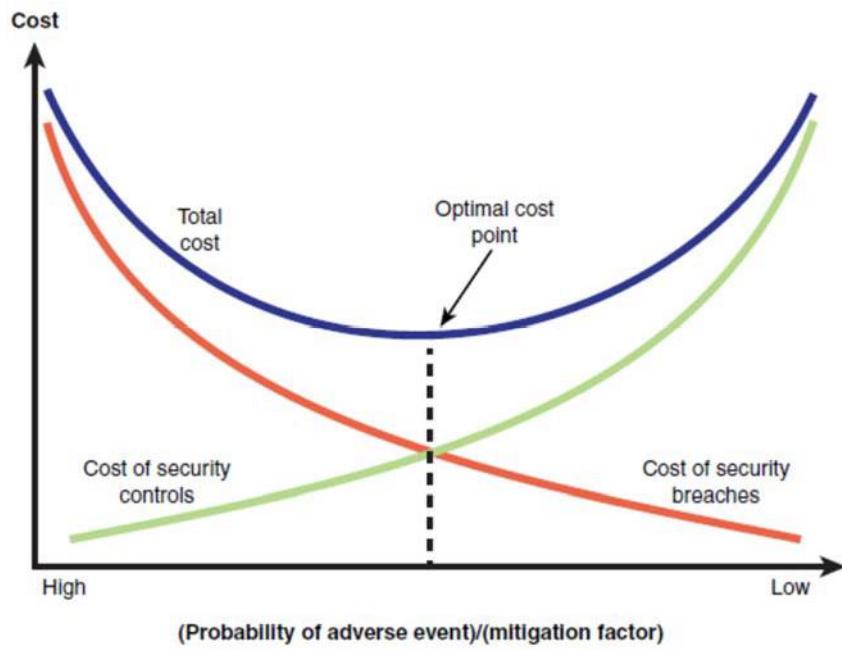


Figure 15 – Cost Analysis for Risk Assessment

### **Qualitative Risk Assessment**

It is not reasonable to suppose that all impact costs and likelihoods can with confidence be expressed quantitatively. Security breaches are rare, and organizations are reluctant to reveal them. Consequently, security incidence information is typically anecdotal or based on surveys and cannot be used to develop reliable or accurate probability or frequency values. At the same time, the total cost or potential loss due to a security breach is hard to quantify. The cost may depend on a variety of factors, such as length of

downtime, amount and effect of adverse publicity, cost to recover, and other factors that are difficult to estimate. Table 1 compares quantitative and qualitative risk assessment.

Table 1 - Comparison of Quantitative and Qualitative Risk Assessment

	Quantitative	Qualitative
<b>Benefits</b>	<ul style="list-style-type: none"> <li>■ Risks are prioritized by financial impact; assets are prioritized by financial values.</li> <li>■ Results facilitate management of risk by return on security investment.</li> <li>■ Results can be expressed in management-specific terminology (for example, monetary values and probability expressed as a specific percentage).</li> <li>■ Accuracy tends to increase over time as the organization builds historic record of data while gaining experience.</li> </ul>	<ul style="list-style-type: none"> <li>■ It enables visibility and understanding of risk ranking.</li> <li>■ It is easier to reach consensus.</li> <li>■ It is not necessary to quantify threat frequency.</li> <li>■ It is not necessary to determine financial values of assets.</li> <li>■ It is easier to involve people who are not experts on security or computers.</li> </ul>
<b>Drawbacks</b>	<ul style="list-style-type: none"> <li>■ Impact values assigned to risks are based on subjective opinions of participants.</li> <li>■ The process to reach credible results and consensus is very time-consuming.</li> <li>■ Calculations can be complex and time-consuming.</li> <li>■ Results are presented in monetary terms only, and they may be difficult for nontechnical people to interpret.</li> <li>■ The process requires expertise, so participants cannot be easily coached through it.</li> </ul>	<ul style="list-style-type: none"> <li>■ There is insufficient differentiation between important risks.</li> <li>■ It is difficult to justify investing in control implementation because there is no basis for a cost/benefit analysis.</li> <li>■ Results are dependent upon the quality of the risk management team that is created.</li> </ul>

An organization needs some clearly defined categories of impact, threat, and vulnerability. For impact, FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, defines three security categories based on the potential impact on an organization should certain events occur that jeopardize the IT assets needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. The categories are as follows:

- **Low:** Expected to have a limited adverse effect on organizational operations, organizational assets, or individuals, including the following:
  - Cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced
  - Result in minor damage to organizational assets
  - Result in minor financial loss
  - Result in minor harm to individuals
- **Moderate or medium:** Expected to have a serious adverse effect on organizational operations, organizational assets, or individuals, including the following:
  - Cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced
  - Result in significant damage to organizational assets
  - Result in significant financial loss
  - Result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries
- **High:** Expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals, including the following:
  - Cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions
  - Result in major damage to organizational assets
  - Result in major financial loss
  - Result in severe or catastrophic harm to individuals, involving loss of life or serious life-threatening injuries

**FIPS 199, Standards for Security Categorization of Federal Information and Information Systems,** provides a number of examples of qualitative impact assessment. The resulting security category, SC, of this information type is expressed as:

SC investigative information = {(confidentiality, HIGH), (integrity, MODERATE),  
(availability, MODERATE)}.

Similarly, ranges of probability are assigned to qualitative likelihood categories. SP 800-100, Information Security Handbook: A Guide for Managers, suggests the following categories:

- Low:  $\leq 0.1$
- Medium: 0.1 to 0.5
- High: 0.5 to 1.0

With these categories in mind, Figure 16 illustrates the use of matrices to determine risk. The vulnerability to a particular threat is a function of the capability, or strength, of the threat and the resistance strength of a system or an asset to that particular threat. Then, the likelihood of an adverse security event causing a particular threat is a function of the frequency, or likelihood, of the threat occurring and the vulnerability to that threat. Impact is determined as a function of asset class and the exposure to loss that a particular threat could cause. For example, assets can be classified in terms of the business impact of a loss.

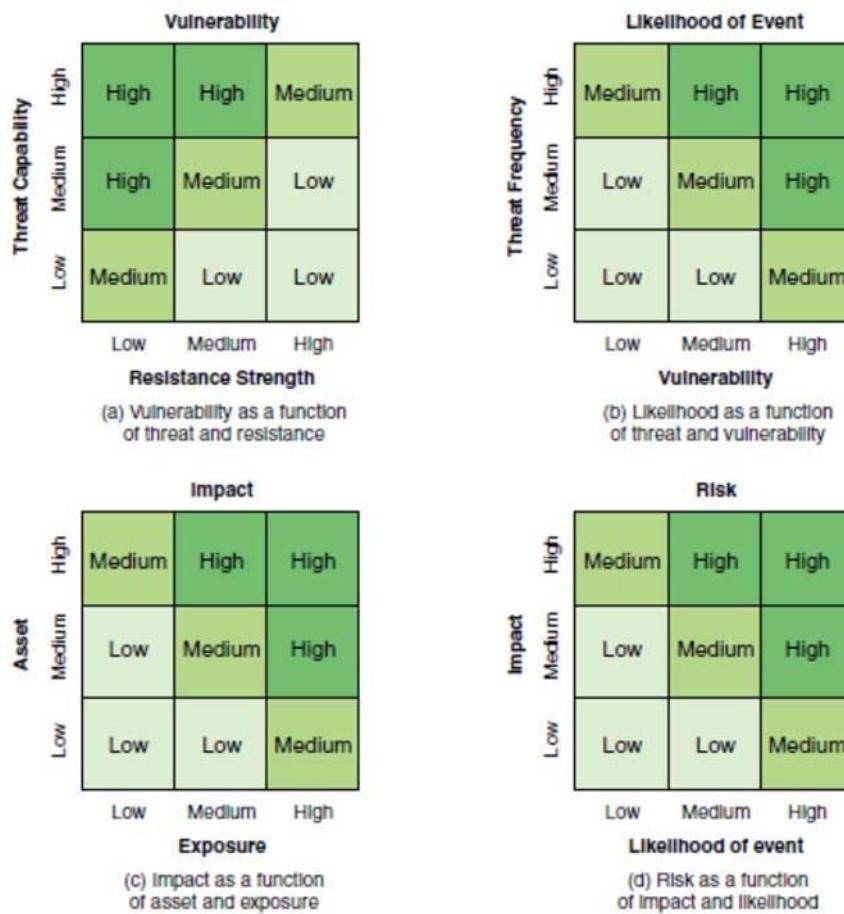


Figure 16 – Qualitative Risk Determination

## Factor Analysis of Information Risk

An important contribution to risk assessment is Factor Analysis of Information Risk (FAIR), first introduced in 2005. FAIR, which has been standardized by The Open Group, has received wide acceptance. Its relationship to International Organization for Standardization (ISO) risk standards are summarized as follows:

- ISO 27001 describes a general process for creating an information security management system (ISMS).
  - In that context, ISO 27005 defines the approach to managing risk.
  - FAIR provides a methodology for analyzing risk.

Thus, FAIR provides more specific guidance that can be used within the framework defined by ISO 27005. Figure 17 illustrates the relationships between the three risk assessment tasks in ISO 27005 and the detailed definitions of those tasks in FAIR. FAIR provides a more detailed set of guidelines for all aspects of risk assessment. For example, FAIR provides definitions of the key terms that are less vague and more specifically tied to the risk analysis process than does ISO 27005.

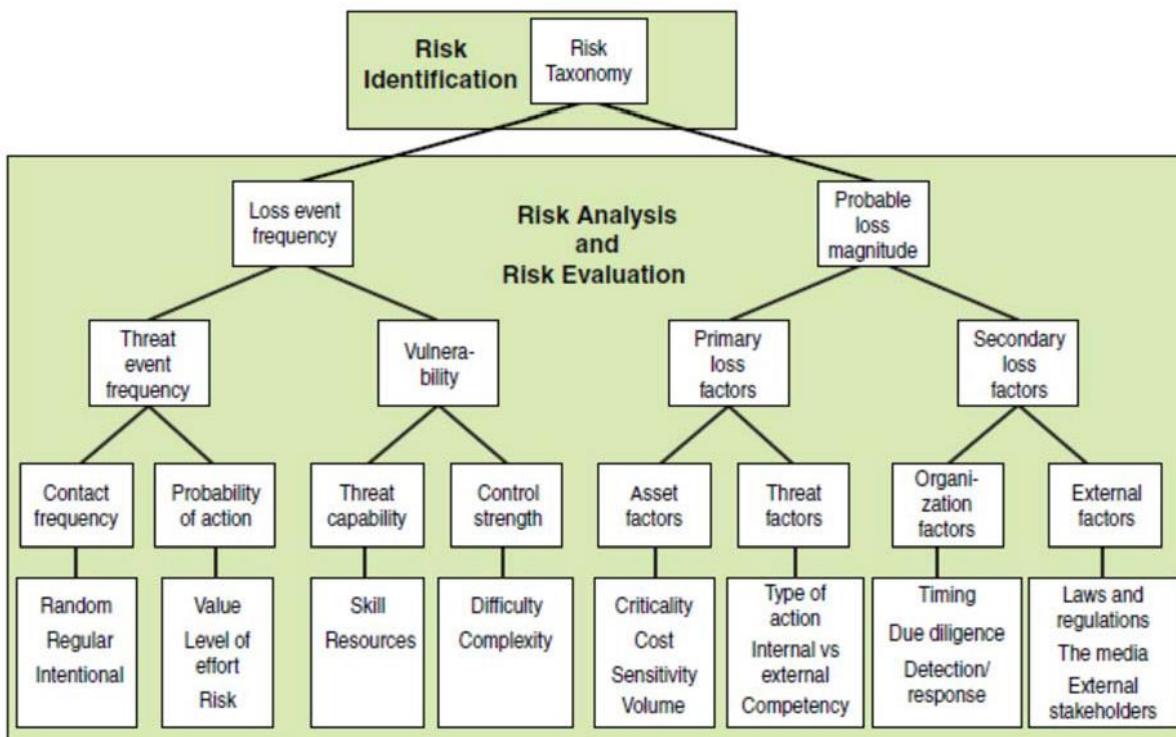


Figure 17 – Risk Assessment Using FAIR

The key FAIR definitions are as follows:

- Asset: Any data, device, or other component of the environment that supports information-related activities that can be illicitly accessed, used, disclosed, altered, destroyed, and/or stolen, resulting in loss.
- Risk: The probable frequency and probable magnitude of future loss.
- Threat: Anything that is capable of acting in a manner resulting in harm to an asset and/or organization—for example, acts of God (weather, geologic events, and so on), malicious actors, errors, and failures.
- Vulnerability: The probability that an asset will be unable to resist actions of a threat agent.

The FAIR methodology is based on a belief that subjective qualitative analysis is inadequate in most situations and that all risk, tangible and intangible, is measurable and quantifiable. The actual quantitative analysis results are delivered using calibrated, probabilistic estimates based on ranges of probabilities, accurate comparisons, and PERT calculations run through Monte Carlo simulations.

## Aim/Objectives

We start this week with a discussion of the distinction between quantitative and qualitative risk assessment. This will be followed by a presentation of a simple approach to risk assessment. Therefore, the main objective of this week is to introduce the student with the most practical and well-accepted risk assessment approaches. We base the risk assessment approaches on International standards such as the ISO 27005 and the FAIR approach for risk assessment.

## Learning Outcomes

Upon successful completion of this course, students should be able to:

- Explain the difference between quantitative and qualitative Risk Assessment
- Compare Quantitative and Qualitative Risk Assessment
- Explain the purpose and approach of Factor Analysis of Information Risk.
- Understand the key elements of risk analysis.
- Explain what Factor Analysis of Information Risk (FAIR) is and where it is used
- Describe the key FAIR definitions

## Key Words

FAIR	quantitative	qualitative
Risk Assessment	Residual risk level	Risk level

## Annotated Bibliography

### Basic

**Effective Cybersecurity: A Guide to Using Best Practices and Standards** 1st Edition, 2019, Willian Stallings, ISBN-13: 978-0134772806, ISBN-10: 0134772806

This week is based on Chapter 3 of the book.

### Supplementary

1. Power point presentation slides available in the platform
2. Factor Analysis of Information Risk (FAIR) has emerged as the standard Value at Risk (VaR) framework for cybersecurity and operational risk. The FAIR Institute is a non-profit professional organization dedicated to advancing the discipline of measuring and managing information risk. It provides information risk, cybersecurity and business executives with the standards and best practices to help organizations measure, manage and report on information risk from the business perspective. The FAIR Institute and its community focus on innovation, education and sharing of best practices to advance FAIR and the information risk management profession. Read more on [FAIR](#)
3. [Short presentation of Open FAIR Risk Analysis Tool](#)

### Suggestions for further reading

[ISO/IEC 27005:2018](#) provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of this document. This document is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that can compromise the organization's information security.

## **Self-Assessment Exercises**

### **Exercise 8.1**

How does FAIR define key terms related to risk assessment? Is it more or less specific than ISO 27005 in its definitions pertaining to risk analysis?

### **Exercise 8.2**

According to ISO 27005, what are viable options for any system that treats risk?

## **Individual Assignment**

### **ISO 27005, Information Security Risk Management**

While a simple risk analysis worksheet may be suitable for smaller organizations, for larger organizations, a broader framework to guide risk assessment is advisable. The most important such framework is ISO 27005, which describes a systematic approach to managing information security risk, particularly in the context of ISO 27001, ISMS Requirements.

After you have studied the course materials and already have an understanding of the most important concepts and methodology concerning cyber risks and management, in this assignment you are requested to:

1. Present the overall risk management process defined in ISO 27005.
2. Explain the various separate activities that constitute the risk management process.

There is no page limit in this assignment. However, a 10 to 15 pages document is considered as adequate for this assignment.

## **Recommended time for the student to work**

35 hours

## RISK ANALYSIS AND TREATMENT

9<sup>th</sup> Week

### Summary

In the previous two weeks, we discussed risk identification and assessment. This week we will concentrate on the following important topics, namely i) Likelihood assessment, ii) Impact assessment, iii) Risk determinations, iv) risk evaluation, and v) risk treatment.

### Introductory Remarks

#### Likelihood assessment

Likelihood assessment does not yield a numerical value subject to calculation using probability theory. Rather, it is the process of developing some sort of agreed-upon likelihood score that estimates the chance of a threat action. A likelihood assessment considers the presence, tenacity, and strengths of threats as well as the presence of vulnerabilities and the effectiveness of security controls already in place. This assessment is applied to each identified potential threat action.

The essence of likelihood assessment for a given threat to a given asset is shown in the following steps:

**Step 1.** Determine the likelihood that a threat event will occur. That is, determine the likelihood that this threat will develop into an attack on the given asset.

**Step 2.** Determine the degree of vulnerability of the asset to the threat.

**Step 3.** Based on Step 1 and Step 2, determine the likelihood that a security incident will occur.

This analysis needs to be repeated for every threat to every asset. ISO 27005 and other ISO documents provide limited guidance on how to perform this function. FAIR provides detailed guidance on how to systematically characterize event likelihood, referred to in the FAIR documents as loss event frequency.

FAIR adopts a top-down approach to determining loss event frequency. At the top level, it may be possible, based on historical data, to develop an estimate of loss event frequency, simply on the basis of how frequently a loss event has occurred in the past. It is not necessary, and indeed not possible, to derive an exact frequency or probability. For one thing, a security event in the past may remain undetected at the

time of the risk assessment. In addition, the past cannot be considered an exact predictor of the future. The examples in the FAIR documents use five levels (very low, low, moderate, high, very high) with an order of magnitude change between levels,

**Estimating Threat Event Frequency:** The assessment of threat event frequency involves two aspects: determining the frequency with which a threat agent will come in contact with an asset and the probability that, once in contact, the threat agent will act against the asset. Contact can be physical or logical.

**Estimating Vulnerability:** As with the estimation of threat event frequency, the estimation of vulnerability involves assigning relative values to two dimensions. In the case of vulnerability, the two dimensions are the threat capability and the control strength. FAIR defines threat capability as the capability of the threat community to act against an asset using a specific threat.

Estimating vulnerability involves looking at two factors:

- **Skill:** The knowledge and experience of the threat agent are critical factors in the severity of the threat action. Skill is reflected in the manner in which a threat agent is able to act, such as performing social engineering or bypassing logon or other access barriers. In the case of malware, the skill applied to constructing and propagating the malware determine the severity of the threat.
- **Resources:** The other important factor is the resources, such as the time, financial resources, and materials that a threat agent can bring to bear.

For a given threat to a given asset, once an analyst has developed estimates of threat capability and resistance strength, these two dimensions can be combined to produce a measure of vulnerability. This is done using the matrix shown in Figure 18.

		Vulnerability (Vuln)				
		VH	VH	VH	H	M
Threat Capability (TCap)	VH	VH	VH	H	M	M
	H	VH	VH	H	M	L
	M	VH	H	M	L	VL
	L	H	M	L	VL	VL
	VL	M	L	VL	VL	VL
		VL	L	M	H	VH

Resistance Strength (RS)

$Vuln = f_1(RS, TCap)$

(a)

		Primary Loss Event Frequency (PLEF)				
		VH	M	H	VH	VH
Threat Event Frequency (TEF)	VH	M	H	VH	VH	VH
	H	L	M	H	H	H
	M	VL	L	M	M	M
	L	VL	VL	L	L	L
	VL	VL	VL	VL	VL	VL
		VL	L	M	H	VH

Vulnerability (Vuln)

$PLEF = f_2(Vuln, TEF)$

$SLEF = f_2(SLP, PLEF)$

(b)

		Primary Risk				
		VH	M	H	VH	VH
Primary Loss Magnitude	VH	M	H	VH	VH	VH
	H	L	M	H	VH	VH
	M	VL	L	M	H	VH
	L	VL	VL	L	M	H
	VL	VL	VL	VL	L	VH
		VL	L	M	H	VH

Primary Loss Event Frequency (PLEF)

$Primary Risk = f_3(PLEF, Primary Loss Magnitude)$

$Secondary Risk = f_3(SLEF, Secondary Loss Magnitude)$

(c)

		Overall Risk				
		VH	VH	VH	VH	VH
Secondary Risk	VH	H	H	H	H	VH
	H	M	M	M	H	VH
	M	L	L	M	H	VH
	L	VL	L	M	H	VH
	VL	VL	L	M	H	VH
		VL	L	M	H	VH

Primary Risk

$Risk = f_4(Primary Risk, Secondary Risk)$

(d)

Figure 18 – Sample FAIR Risk Assessment Matrices

It is worth making a distinction here between an estimated parameter and a derived parameter. Threat capability and resistance strength are parameters whose values are estimated by an analyst, which involves analytic effort. Once these two parameters are estimated, the analyst simply plugs them into the matrix to derive the desired vulnerability rating. The matrix defines a qualitative function  $f_1$ , that is expressed as:

$$Vulnerability = f_1(Resistance\ strength, Threat\ capability)$$

**Loss Event Frequency:** The likelihood of a loss, referred to as loss event frequency in the FAIR documents, is derived from the threat event frequency and vulnerability by using the matrix shown in Figure 18b. This matrix defines a function  $f_2$ :

$$Primary\ loss\ event\ frequency = f_2(Vulnerability, Threat\ event\ frequency)$$

This derived quantity is also referred to as the primary loss event frequency, to contrast it with the secondary loss event frequency discussed subsequently.

## Impact Assessment

Impact assessment is the process of developing some sort of agreed-upon impact score or cost value that estimates the magnitude or the adverse consequence of a successful threat action. The essence of impact assessment is that, for a given threat to a given asset, you determine the impact (cost or relative magnitude of impact) on the asset if the threat were to become an actual security incident. This analysis needs to be repeated for every threat to every asset. ISO 27005 and other ISO documents provide limited guidance on how to perform this function. The FAIR documents note that this is one of the most difficult aspects of risk assessment. FAIR provides detailed guidance on how to systematically characterize impact. This guidance, although clear, is rather complex, so this section provides an overview.

Table 2 - FAIR Loss Categories

Loss Category	Loss Factors	Forms of Loss
Primary loss	<ul style="list-style-type: none"><li>■ <b>Asset:</b> Includes the value/liability characteristics of an asset and the volume of assets at risk</li><li>■ <b>Threat:</b> Includes type of action, whether internal or external, and threat competence.</li></ul>	<ul style="list-style-type: none"><li>■ <b>Productivity:</b> The reduction in an organization's ability to generate its primary value proposition (for example, income, goods, services).</li><li>■ <b>Response:</b> Associated with managing a loss event (for example, internal or external person-hours, logistical expenses).</li><li>■ <b>Replacement:</b> The intrinsic value of an asset. Typically represented as the capital expense associated with replacing lost or damaged assets (for example, rebuilding a facility, purchasing a replacement laptop).</li></ul>
Secondary loss	<ul style="list-style-type: none"><li>■ Secondary loss event frequency</li><li>■ Secondary loss magnitude</li></ul>	<ul style="list-style-type: none"><li>■ <b>Organization:</b> Includes timing, due diligence, type of response, and detection capability.</li><li>■ <b>External:</b> Entities that can inflict a secondary form of harm upon the organization as a result of an event.</li></ul> <ul style="list-style-type: none"><li>■ <b>Competitive advantage:</b> Losses associated with diminished competitive advantage; associated with assets that provide competitive differentiation between the organization and its competition. Examples include trade secrets and merger and acquisition plans.</li><li>■ <b>Fines/judgments:</b> Legal or regulatory actions levied against an organization.</li><li>■ <b>Reputation:</b> Associated with an external perception that an organization's value proposition is reduced or leadership is incompetent, criminal, or unethical.</li></ul>

FAIR impact analysis depends on two categories of loss, as shown Figure 17 and Table 2.

The two loss categories are:

**Primary loss:** Occurs directly as a result of the threat agent's action upon the asset. The owner of the affected assets is considered the primary stakeholder in an analysis. This event affects the primary stakeholder in terms of productivity loss, response costs, and so on.

**Secondary loss factors:** Occurs as a result of secondary stakeholders (for example, customers, stockholders, regulators) reacting negatively to the primary event. The reactions of the secondary stakeholders may, in turn, act as new threat agents against the organization's assets (such as reputation, legal fees, and so on), which, of course, affects the primary stakeholder.

### Risk Determination

Once the loss magnitude is estimated and the loss event frequency derived, it is a straightforward process to derive an estimate of risk. This is done separately for primary and secondary losses, and then the two are combined

The primary risk determination is illustrated in Figure 18c and is expressed as:

$$\text{Primary risk} = f_3(\text{Primary loss event frequency}, \text{Primary loss magnitude})$$

The same  $f_3$  calculation is applied to secondary loss to determine the secondary risk. The two risks are

then combined to determine an overall risk using the matrix in Figure 18d, which is expressed as:

$$\text{Overall risk} = f_4(\text{Primary risk}, \text{Secondary risk})$$

Again, the individual matrix values are a matter of judgment. For example, a conservative view might be that if both primary and secondary risk are at the same level, the overall risk should be raised to the next level. In that case, if both risks are rated high, the overall risk is rated very high. A less conservative strategy is indicated in function  $f_4$ .

## Risk Evaluation

Once a risk analysis is done, senior security management and executives can determine whether to accept a particular risk and if not determine the priority in assigning resources to mitigate the risk. This process, known as risk evaluation, involves comparing the results of risk analysis with risk evaluation criteria.

The advice provided for risk evaluation, both by ISO 27005 and the FAIR documents, is general as the criteria developed vary significantly from one organization to another. ISO does make a distinction between risk evaluation criteria and risk acceptance criteria. Evaluation criteria focus on the importance of various business assets and the impact that can be caused to the organization by various security events. The goal is to be able to specify priorities for risk treatment. Risk acceptance criteria relate to how much risk the organization can tolerate and provide guidance on how much budget can be allocated for risk treatment. SP 800-100 provides some general guidance for evaluating risk and prioritizing action based on a three-level model:

- **High:** If an observation or a finding is evaluated as high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
- **Moderate:** If an observation is rated as moderate risk, corrective actions are needed, and a plan must be developed to incorporate these actions within a reasonable period of time.
- **Low:** If an observation is described as low risk, the system's authorizing official must either determine whether corrective actions are still required or decide to accept the risk.

## Risk Treatment

Once the risk assessment process is complete, management should have a list of all the threats posed to all assets, with an estimate of the magnitude of each risk. In addition, a risk evaluation provides input in terms of the priority and urgency with which each threat should be addressed. The response to the set of identified risks is referred to as risk treatment (or risk response), as shown in Figure 19.

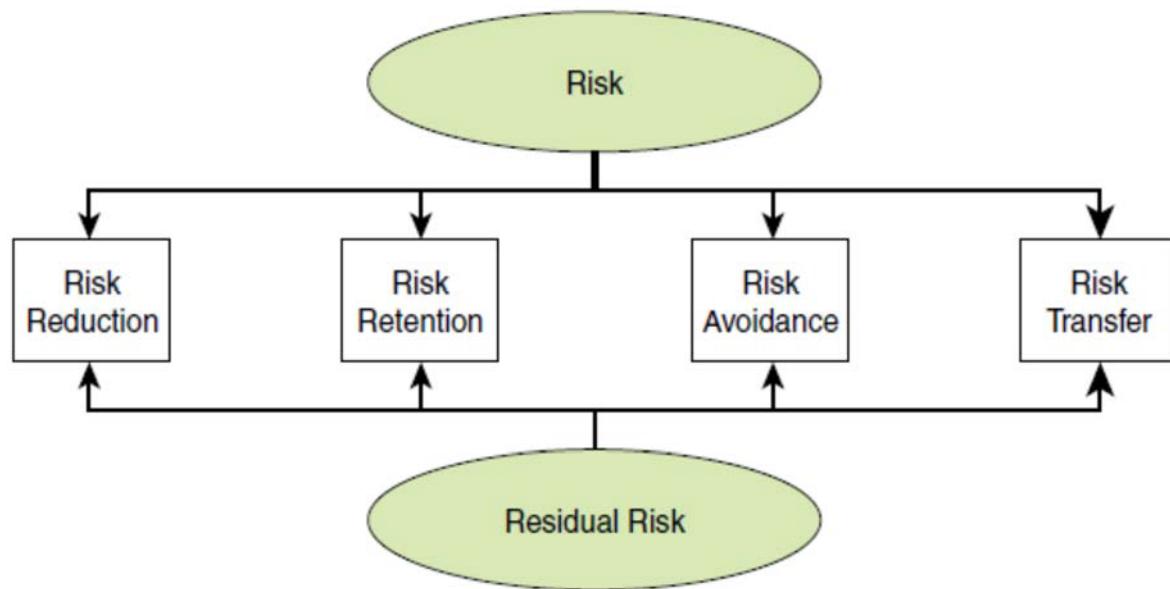


Figure 19 – Risk Treatment

## Aim/Objectives

The scope of this week is to introduce the student with the important topics of risk analysis and treatment. We explain how risk analysis is conducted with the Likelihood and Impact assessment and risk determination. The student will follow the same steps of both ISO 27005 and FAIR, which was discussed in the previous week

## Learning Outcomes

Upon successful completion of this course, students should be able to:

- Define the steps of likelihood assessment
- Explain how the Impact assessment can be conducted
- Explain the risk determination procedure
- Understand the context of high, medium and low risk
- Explain the importance of risk treatment

## Key Words

Likelihood assessment	Impact assessment	Risk determination
risk evaluation	risk treatment	risk assessment levels

## Annotated Bibliography

### Basic

**Effective Cybersecurity: A Guide to Using Best Practices and Standards** 1st Edition, 2019, Willian Stallings, ISBN-13: 978-0134772806, ISBN-10: 0134772806

This week is based on Chapter 3 of the book.

### Supplementary

1. Power point presentation slides available in the platform
2. Webminar: [An Overview of Risk Assessment According to ISO 27001 and ISO 27005](#)

### Suggestions for further reading

1. NIST: Information Security Handbook: A Guide for Managers

This Information Security Handbook provides a broad overview of information security program elements to assist managers in understanding how to establish and implement an information security program. Typically, the organization looks to the program for overall responsibility to ensure the selection and implementation of appropriate security controls and to demonstrate the effectiveness of satisfying their stated security requirements. The topics within this document were selected based on the laws and regulations relevant to information security, including the ClingerCohen Act of 1996, the Federal Information Security Management Act (FISMA) of 2002, and Office of Management and Budget (OMB) Circular A-130. The material in this handbook can be referenced for general information on a particular topic or can be used in the decision-making process for developing an information security program. National Institute of Standards and Technology (NISTIR) Interagency Report 7298 provides a summary glossary for the basic security terms used throughout this document. While reading this handbook, please consider that the guidance is not specific to a particular agency. Agencies should tailor this guidance according to their security posture and business requirements. Read more [here](#)

## Self-Assessment Exercises

### Exercise 9.1

Explain what likelihood assessment is and define the four steps for a given threat.

### Exercise 9.2

What is the model of SP 800-100 for evaluating risk and prioritizing action?

**Recommended time for the student to work**

15 hours

## THREAT AND VULNERABILITY MANAGEMENT

10<sup>th</sup> Week

### Summary

This week we will discuss about threats and vulnerabilities and how can we manage them. We will see the various steps of vulnerability management and explain what threat intelligence is and how it contributes in the whole concept of cyber security risk management.

### Introductory Remarks

**Technical vulnerability management**, usually referred to simply as vulnerability management, is a security practice specifically designed to proactively mitigate or prevent the exploitation of technical vulnerabilities that exist in a system or an organization. The process involves the **identification**, **classification**, **remediation**, and **mitigation** of various vulnerabilities in a system. It is an integral part of cybersecurity and is practiced together with risk management as well as other security practices. Figure 20 illustrates the five key steps involved in vulnerability management.

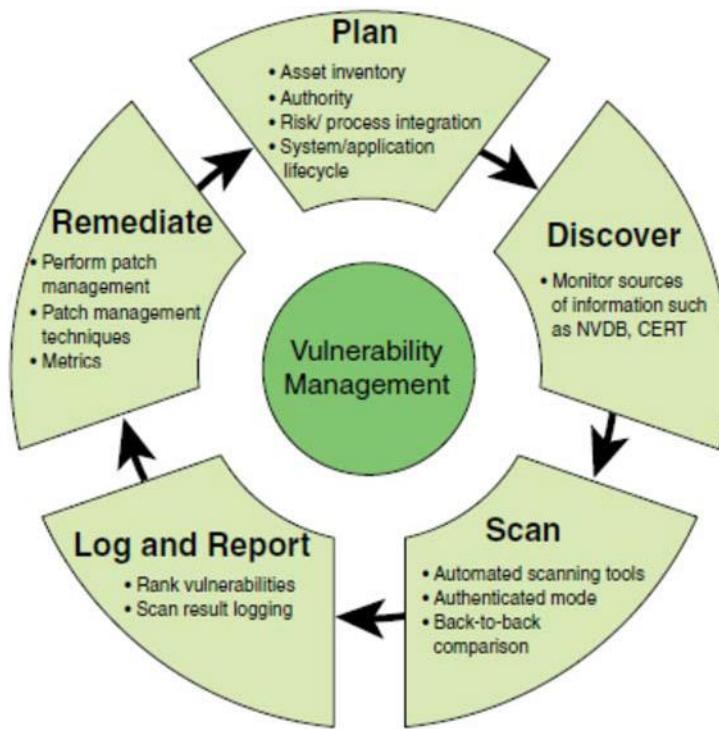


Figure 20 – Vulnerability Management Steps

Effective management of technical vulnerabilities begins with planning. Key aspects of the planning process include the following:

- **Risk and process integration:** Technical vulnerability review is an operational aspect of an overall information security risk management strategy. A vulnerability analysis must consider the relative risk impacts, including those related to the potential for operational disruption. These risks must also have a clear reporting path that allows for appropriate management awareness of risk factors and exposure. Vulnerability management should also provide input into change management and incident management processes.
- **Integration with asset inventory:** As discussed in the previous weeks, asset identification is an integral part of risk assessment. The resulting asset inventory allows for action to be taken once a technical vulnerability is reviewed and a mitigation strategy agreed on. By integrating the asset inventory with the vulnerability management system, an enterprise can prioritize high-risk systems where the impact of technical vulnerabilities can be greatest.
- **Establishment of clear authority to review vulnerabilities:** Because probing a network for vulnerabilities can disrupt systems and expose private data, an enterprise needs to have in place a policy and buy-in from top management before performing vulnerability assessments. The

enterprise's acceptable use policy must have users and system managers consent to vulnerability scanning as a condition of connecting to the network. Awareness training should clarify that the main purpose of seeking vulnerabilities is to defend against attacks. There is also a need for policies and ethical guidelines for those who have access to data from vulnerability scans. These individuals need to understand the appropriate action when illegal materials are found on their systems during a vulnerability scan.

- **System and application life cycle integration:** The review of vulnerabilities must be integrated in system release and software development planning to ensure that potential weaknesses are identified early to both lower risks and manage costs of finding these issues prior to identified release dates.

**Threat Intelligence**, also known as **cyber threat intelligence (CTI)**, or **cyber intelligence**, is the knowledge established as a result of analyzing information about potential or current attacks that threaten an organization. The information is taken from a number of internal and external sources, including application, system, and network logs; security products such as firewalls and intrusion detection systems; and dedicated threat feeds.

A number of organizations have published taxonomies or catalogs of threat types. NIST provides a catalog consisting of 83 adversarial threat events and 18 non-adversarial threat events in SP 800-30, Guide for Conducting Risk Assessments. The European Union Agency for Network and Information Security (ENISA) Threat Taxonomy [28] lists 177 separate threats. The Web Application Security Consortium (WASC) Threat Classification [29] lists 34 threat types. The Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP) list 22 adversarial threats, 11 accidental threats, and 13 environmental threats.

Therefore, the **primary purpose of threat intelligence** is to help organizations understand the risks of the most common and severe external threats, such as **advanced persistent threats (APTs)**, **exploits**, and **zero-day** threats. Although threat actors also include internal (or insider) and partner threats, the emphasis is on the types of external threats that are most likely to affect a particular organization's environment. Threat intelligence includes in-depth information about specific threats to help an organization protect itself against the types of attacks that could do them the most damage.

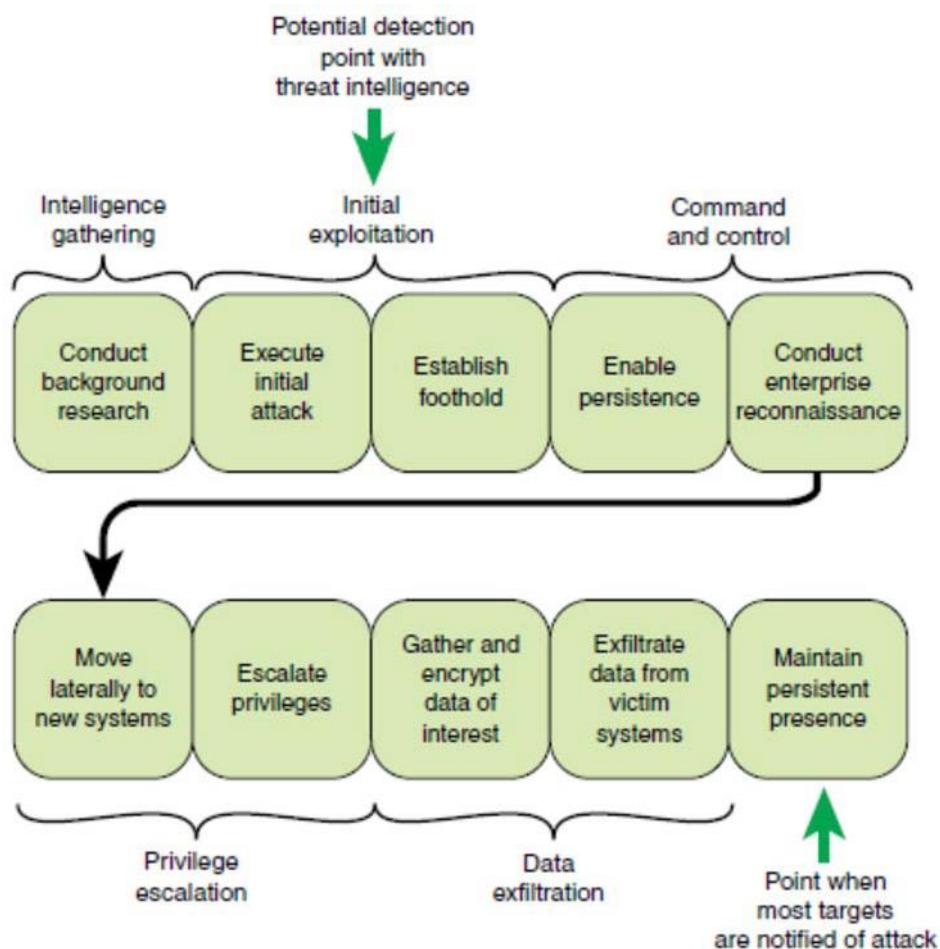


Figure 21 – Potential Benefit of Threat Intelligence

As an example of the **importance of threat intelligence**, Figure 21, based on one in the Information Systems Audit and Control Association's (ISACA's) Responding to Targeted Cyberattacks [30], illustrates the impact of threat intelligence on an advanced persistent threat (APT) attack.

A typical APT attack proceeds through the following steps:

1. *Conduct background research.* An APT attack begins with research on potential targets to identify specific avenues of attack. This maximizes the chance of the target reacting as desired.
2. *Execute the initial attack.* Typically, the initial attack targets one or more specific individuals through some form of social engineering.
3. *Establish a foothold.* The APT establishes an initial foothold into the target environment by using customized malware.

4. *Enable persistence.* One of the primary objectives of the APT is to establish persistent command and control over compromised computers in the target environment.
5. *Conduct enterprise reconnaissance.* After establishing persistent access to the target environment, the APT typically attempts to find the servers or storage facilities holding the targeted information.
6. *Move laterally to new systems.* Part of enterprise reconnaissance necessarily includes moving laterally to new systems to explore their contents and understand the new parts of the enterprise accessed from the new systems.
7. *Escalate privileges.* As the attackers conduct reconnaissance and move around the network using the compromised credentials of their first few targets, they inevitably seek to escalate from local user to local administrator to higher levels of privilege in the environment
8. *Gather and encrypt data of interest.* Having found the data of interest to the attackers, the APT generally gathers the data into an archive and then compresses and encrypts the archive.
9. *Exfiltrate data from victim systems.* The APT uses a variety of tools and protocols to transfer data from the target systems.
10. *Maintain persistent presence.* An APT seeks to attain what its controllers have tasked it to do: maintain access to the target environment. It is not uncommon for the APT to sit undetected in an enterprise network for lengthy periods before being activated.

As Figure 21 indicates, threat intelligence enables a security team to become aware of a threat well before the point of typical notification, which is often after the real damage is done. Even if an early opportunity is lost, threat intelligence reduces the time it takes to discover that an attack has already succeeded and therefore speeds up remediation actions to limit the damage.

## Aim/Objectives

The scope of this week is for the student to understand the steps of the vulnerability management process and the effective management of technical vulnerabilities. The primary purpose of the effective management of technical vulnerabilities are discussed and we concentrate on current cyber threats such as the advanced persistent threats (APTs), exploits, and zero-day threats.

## Learning Outcomes

Upon successful completion of this course, students should be able to:

- Present an overview of the process of managing technical vulnerabilities.
- Appreciate the importance of security event logging to the event management process.
- Explain the nature and purpose of threat intelligence.
- Define the key aspects for effective management of technical vulnerabilities.
- Elaborate on **advanced persistent threats** (APTs), **exploits**, and **zero-day** threats
- Explain the potential benefit of threat intelligence in enterprises.

## Key Words

Vulnerability Management	identification	cyber threat intelligence (CTI)
classification	remediation	mitigation

## Annotated Bibliography

### Basic

**Effective Cybersecurity: A Guide to Using Best Practices and Standards** 1st Edition, 2019, Willian Stallings, ISBN-13: 978-0134772806, ISBN-10: 0134772806

This week is based on Chapter 15 of the book.

### Supplementary

Power point presentation slides available in the platform

Video: [8 Most Common Cybersecurity Threats](#)

### Suggestions for further reading

1. A cyberattack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. Usually, the attacker seeks some type of benefit from disrupting the victim's network. You can read more on the most common cyberattacks in this [Cisco release](#).

### References

- [27] Committee on National Security Systems. National Information Assurance (IA) Glossary, April 2010.
- [28] European Union Agency for Network and Information Security, ENISA Threat Taxonomy—A Tool for Structuring Threat Information. January 2016, <https://www.enisa.europa.eu>
- [29] Web Application Security Consortium, WASC Threat Classification. January 2010. <http://www.webappsec.org/>

[30] IISACA, Responding to Targeted Cyberattacks. 2008. [www.isaca.org](http://www.isaca.org)

## Self-Assessment Exercises

### Exercise 10.1

What are the most common processes in a technical vulnerability management?

### Exercise 10.2

Why threat intelligence is considered an essential process for the protection of our cyber space.

## Activities

ENISA publishes each year the top 15 cyber threats. After studying ENISA reports over the last five years provide a paper with a short description of each one threat, defining its severity and how they are evolving.

## Recommended time for the student to work

20 hours

## SECURITY INCIDENT MANAGEMENT

11<sup>th</sup> Week

### Summary

In this week, we will deal explicitly with the security event management (SEM) and security incident management processes. We will also see a number of standards that are relevant to the implementation of security incident management.

### Introductory Remarks

The **security event management (SEM)** is the process of identifying, gathering, monitoring, analyzing, and reporting security-related events. The objective of SEM is to extract from a large volume of security events those events that qualify as incidents. SEM takes data input from all devices/nodes and other similar applications, such as log management software. The collected events data is analyzed with security algorithms and statistical computations to trace out any vulnerability, threat, or risk, as shown in Figure 22.

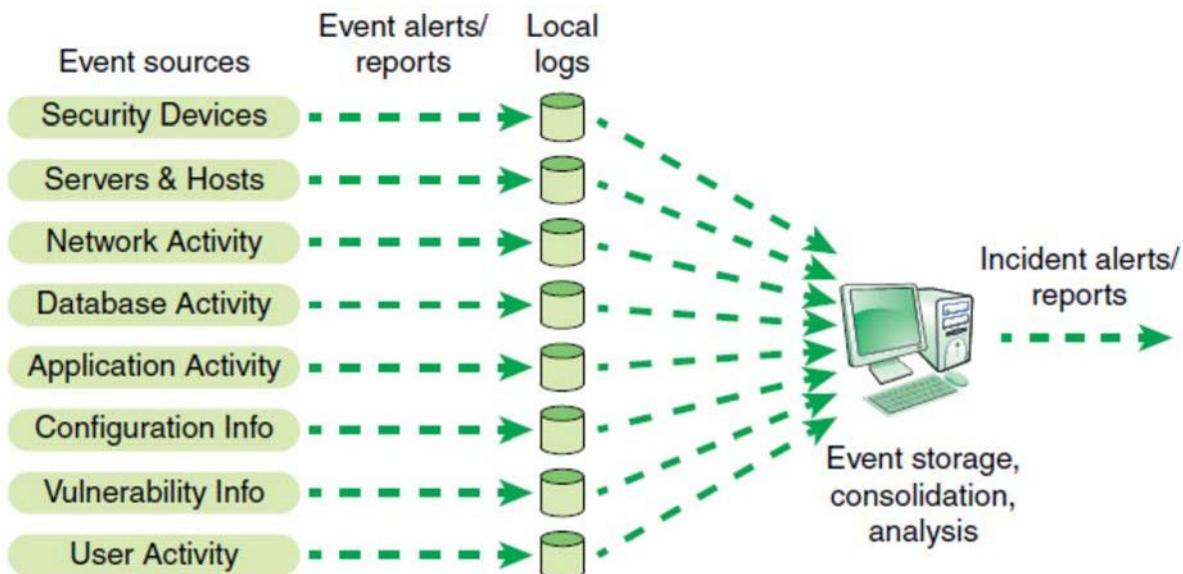


Figure 22 – Security Event Management

Incident management we need to have a place a framework. We can check in ISO 27000 suite that defines information security incident management as consisting of processes for **detecting, reporting, assessing, responding to, dealing with, and learning** from information security incidents. Therefore, we will examine the management framework for security information management, which comprises the relevant individuals, information, and tools required by the organization's information security incident management process. Figure 23 highlights the four key elements of an incident response framework, which are discussed subsequently in this week. **The purpose of the framework is to ensure the availability of resources that are required to help resolve information security incidents quickly and effectively.**

Next, we examine the security incident management process.

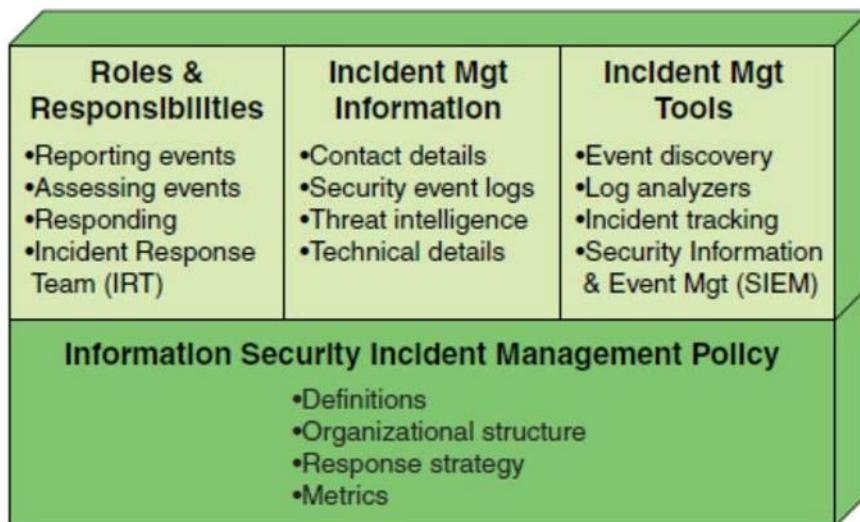


Figure 23 – Security Information Management Framework

A number of standards are relevant to the implementation of security incident management, including the following:

- **ISO 27002, Code of Practice for Information Security Controls:** Provides a comprehensive checklist of management practices for incident response.
- **ISO 27035-1, Information Security Incident Management—Part 1: Principles of Incident Management:** Presents basic concepts and phases of information security incident management and how to improve incident management. This part combines these concepts with principles in a structured approach to detecting, reporting, assessing, and responding to incidents and applying lessons learned.

- **ISO 27035-2, Information Security Incident Management—Part 2: Guidelines to Plan and Prepare for Incident Response:** Describes how to plan and prepare for incident response. Provides a very detailed discussion of what should go into an information security incident management plan.
- **ITU-T X.1056, Security Incident Management Guidelines for Telecommunications Organizations:** Provides practical guidance on how to respond to incidents effectively and efficiently.

### **Objectives of Incident Management**

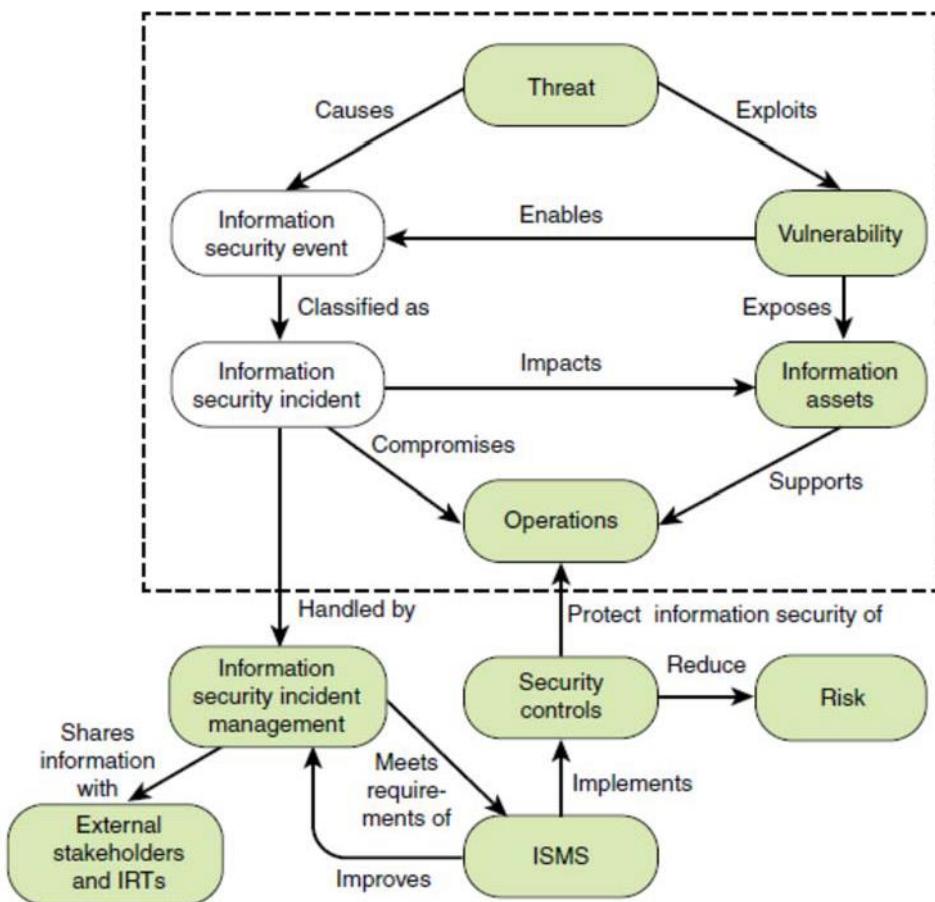
ISO 27035-1 lists the following as the objectives for security incident management:

- Information security events are detected and dealt with efficiently, in particular deciding when they are to be classified as information security incidents.
- Identified information security incidents are assessed and responded to in the most appropriate and efficient manner.
- The adverse effects of information security incidents on the organization and its operations are minimized by appropriate controls as part of incident response.
- A link is established with relevant elements from crisis management and business continuity management through an escalation process.
- Information security vulnerabilities are assessed and dealt with appropriately to prevent or reduce incidents.
- Lessons are learned quickly from information security incidents, vulnerabilities, and their management. This feedback mechanism increases the chances of preventing future information security incidents from occurring, improves the implementation and use of information security controls, and improves the overall information security incident management plan.

### **Relationship to Information Security Management System**

Figure 24, adapted from figures in ISO 27035-1, indicates the relationship between information security incident management and an information security management system (ISMS). The upper part of the figure, bounded by dashed lines, illustrates the relationships among objects in an information security incident.

A threat causes a security event by exploiting a vulnerability, which enables the threat to create the event. The event is potentially an incident that impacts information assets exposed by vulnerabilities and compromises the operations supported by the information assets. In the upper part of the figure, the shaded objects are preexisting and affected by the unshaded objects.



IRT = incident response team  
ISMS = information security management system

Figure 24 – Security Incident Management in Relation to ISMS and Applied Controls

The lower part of Figure 24 indicates the bigger picture, showing how security incident management relates to risk management and an ISMS.

### **Incident Management Policy**

Essential to successful incident management is a documented incident management policy. Such a policy should have sections that deal with overall management, including the following topics:

- A specification of internal and external interested parties
- An agreed-on definition of incident and guidelines to identify a security incident
- A definition of incident response/handling and its overall objectives and scope

- A statement of management intent, supporting the goals and principles of incident response/handling

### **Security Incident Management Process**

Many organizations react in an ad hoc manner when a security incident occurs. Because of the potential cost of security incidents, it is cost-beneficial to develop a standing capability for quick discovery and response to such incidents. This capability also serves to support the analysis of past security incidents with a view to improving the ability to prevent and respond to incidents.

SP 800-61 defines a four-phase incident management process, as shown in Figure 25 that serves as a useful way of structuring the discussion.

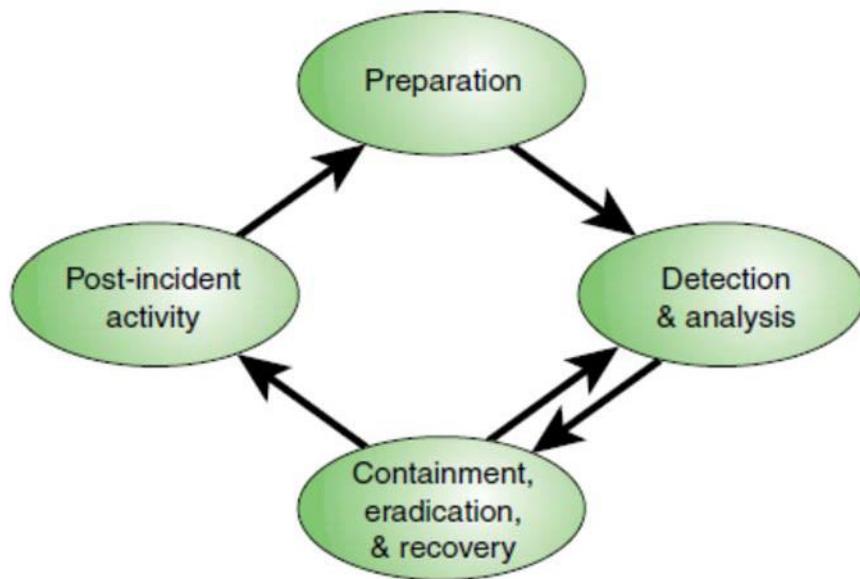


Figure 25 – Incident Response Life Cycle

### **Emergency Fixes**

Security incident emergencies must be handled with a greater sense of urgency than other security incidents. An emergency response may entail making an emergency fix to temporarily eliminate ongoing damage until a more permanent response is provided. Implementing an emergency fix can also require that an information security officer be temporarily given access privileges not normally authorized.

### **Forensic Investigations**

NIST SP 800-96, Guide to Integrating Forensic Techniques into Incident Response, defines computer forensics, or digital forensics, as the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data. Computer forensics seeks to answer several critical questions. Figure 26 illustrates the typical phases in the digital forensics process, which are discussed in detail in the following sections.

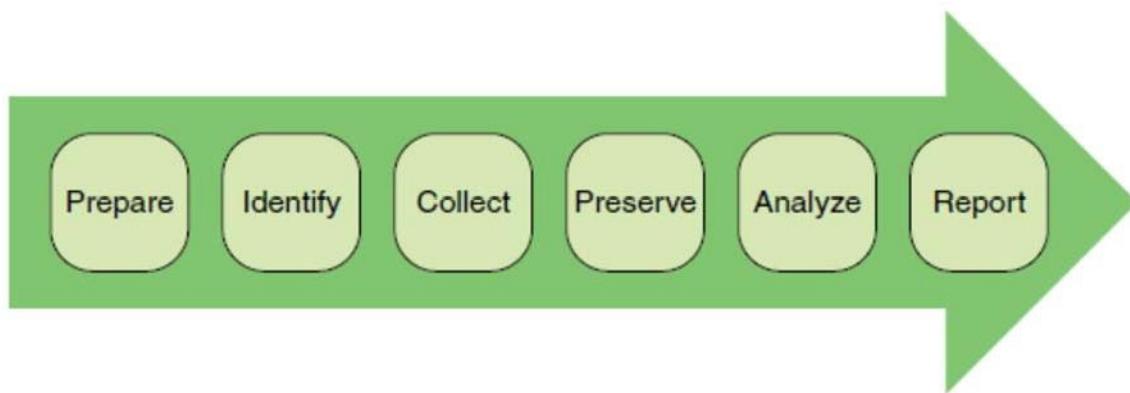


Figure 26 – Phases of Digital Forensics Process

## Aim/Objectives

The scope of this week is for the student to understand the importance of the security incident management and the related ISO frameworks. Another objective for the student is to be able to explain the importance of the incident management policy and the incident response life cycle. Last but not least, forensics investigations are discussed as an essential element for post-incident analysis and future response.

## Learning Outcomes

Upon successful completion of this course, students should be able to:

- Explain what the security event management (SEM) is.
- Define the main elements of the Security Information Management Framework
- Explain the importance of security incident management
- Define the various steps of the security incident management
- Explain what incident management policy is
- Explain the importance of digital forensics

## Key Words

security event management  
(SEM)

security information and  
event management (SIEM)

security event

security incident

Digital forensics

Forensic Investigations

## Annotated Bibliography

### Basic

**Effective Cybersecurity: A Guide to Using Best Practices and Standards** 1st Edition, 2019, Willian Stallings, ISBN-13: 978-0134772806, ISBN-10: 0134772806

This week is based on Chapter 15 of the book.

### Supplementary

Power point presentation slides available in the platform

Video: [8 Most Common Cybersecurity Threats](#)

### Suggestions for further reading

1. A cyberattack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. Usually, the attacker seeks some type of benefit from disrupting the victim's network. You can read more on what are the most common cyberattacks in this [Cisco release](#).

### References

- [31] Committee on National Security Systems. National Information Assurance (IA) Glossary, April 2010.
- [32] European Union Agency for Network and Information Security, ENISA Threat Taxonomy—A Tool for Structuring Threat Information. January 2016, <https://www.enisa.europa.eu>
- [33] Web Application Security Consortium, WASC Threat Classification. January 2010. <http://www.webappsec.org/>
- [34] IISACA, Responding to Targeted Cyberattacks. 2008. [www.isaca.org](http://www.isaca.org)

## Self-Assessment Exercises

### Exercise 11.1

Provide the definition of the security event management.

### **Exercise 11.2**

Why the collection of digital forensics is considered an essential step in the Incident Response Life Cycle

#### **Recommended time for the student to work**

15 hours

## BUSINESS CONTINUITY

12<sup>th</sup> Week

### Summary

A fundamental concern for all organizations is business continuity. An organization needs to perform essential functions during an emergency situation that disrupts normal operations and resume normal operations in a timely manner after the emergency has ended. This week we will discuss the methodology to keep up with the core functions of any business area even though it has experienced a serious cyber-attack.

### Introductory Remarks

The International Organization for Standardization (ISO) has published a family of standards for business continuity management that enterprise security managers should be familiar with:

- **ISO 22300**, Security and Resilience—Vocabulary: Provides a glossary of relevant terms.
- **ISO 22301**, Business Continuity Management Systems—Requirements: Specifies requirements for setting up and managing an effective business continuity management system (BCMS). This is the first international standard focused exclusively on business continuity.
- **ISO 22313**, Business Continuity Management Systems—Guidance: Provides guidance, where appropriate, on the requirements specified in ISO 22301 and provides recommendations (“should”) and permissions (“may”) in relationship to them.
- **ISO 22317**, Business Continuity Management Systems: Guidelines for Business Impact Analysis (BIA): Provides guidelines (based on good international practice) for performing a business impact analysis (BIA), which is a requirement of ISO 22301 (clause 8.2). It provides guidance for establishing, implementing, and maintaining a formal and documented process for business impact analysis. It is applicable to all organizations, regardless of type, location, size, and nature of the organization.
- **ISO 22318**, Business Continuity Management Systems: Guidelines for Business Impact Analysis (BIA): Provides guidelines for supply chain continuity.

Two additional useful guidance documents are:

**National Institute of Standards and Technology** (NIST) SP 800-34, Contingency Planning Guide for Federal Information Systems: Provides a detailed description of the planning process.

**European Union Agency for Network and Information Security**' s (ENISA's) IT Business Continuity Management: An Approach for Small and Medium Sized Organizations: Provides a detailed list of controls for implementing business continuity plans.

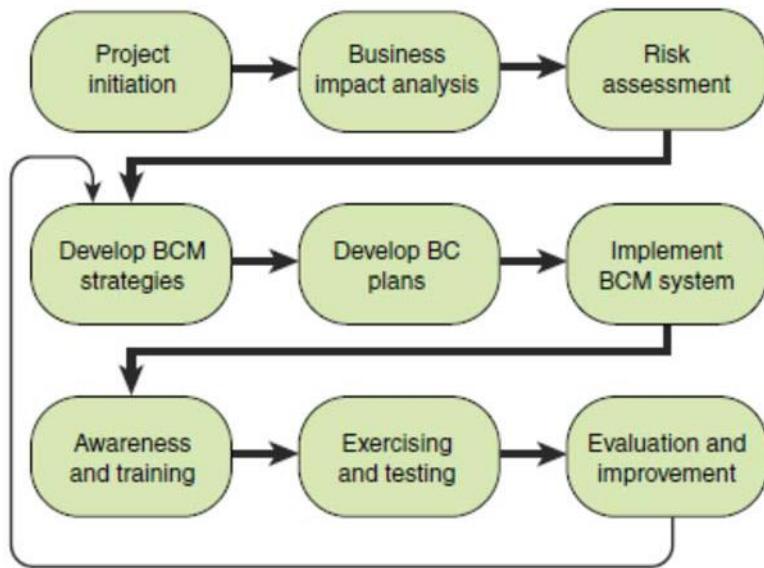


Figure 27 – ISO 22301 Methodology for BCM

### Business Continuity Concepts

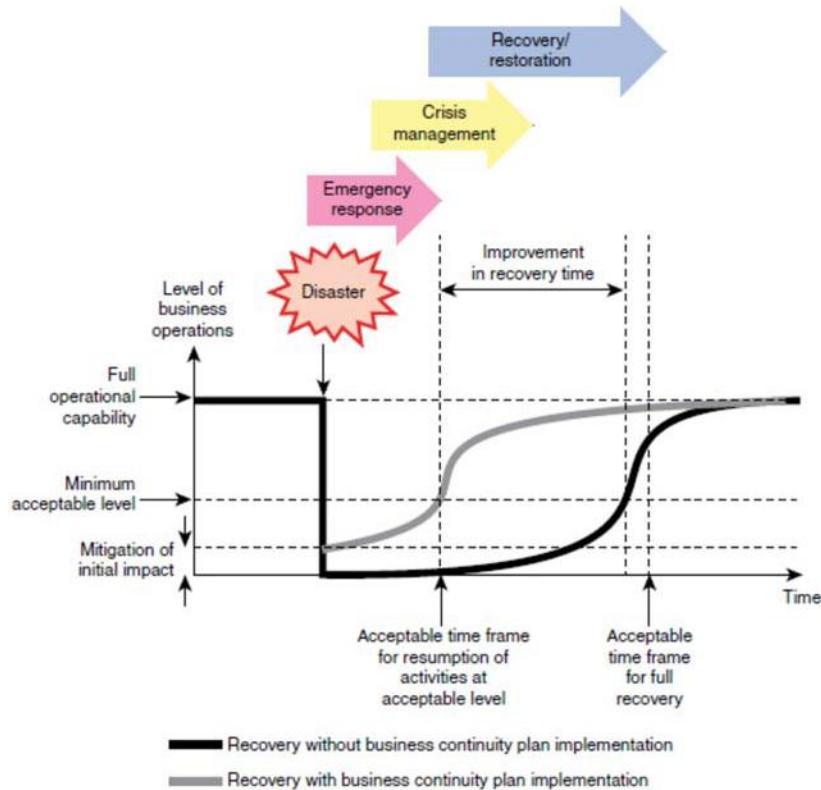


Figure 28 – Effectiveness of Business Continuity Management

In essence, business continuity management is concerned with mitigating the effects of disasters. Figure 28, based on figures in ISO 22313, illustrates the two ways in which business continuity management achieves that mitigation. The relative distances depicted in the figure imply no specific time scales. The gray curve shows the pace of recovery from a disaster with a business continuity plan in place, and the black curve shows the typical recovery pace without a business continuity plan.

When a disaster occurs, the worst-case scenario is that it has the potential to bring some business processes or functions to a complete halt. A business continuity plan includes resilience properties and quick or instantaneous switchover mechanisms that mitigate this initial impact. A business continuity plan also calls for the implementation of capabilities and procedures that result in more rapid restoration of operational capability. Figure 28 also depicts that the recovery process goes through three overlapping stages.

### **Business Continuity Program**

Please recall that an information security program consists of the management, operational, and technical aspects of protecting information and information systems. It encompasses policies, procedures, and management structure and mechanism for coordinating security activity. A business continuity program, as defined in the beginning of this chapter, encompasses these considerations, although it is not limited to just ICT systems but covers the broader business continuity area. The business continuity program requires a business continuity strategy to be in place. This is a conceptual summary of preventive and recovery strategies that must be carried out between the occurrence of a disaster and the time when normal operations are restored. Strategy design involves understanding the requirements gathered during the business impact analysis and risk assessment and effectively translating them into actionable strategies. Furthermore, it involves considering the costs/benefits of any proposed strategy.

Figure 29 illustrates the type of trade-off that management needs to consider. The cost of disruption derives from the business impact analysis and risk assessment. Against that is the cost of resources to implement a business continuity program. Typically, the longer a disruption continues, the more costly it becomes for the organization. But the shorter the RTO, the more costs are incurred. For example, for short recovery times, an organization may require a mirror data site that is always active and updated, whereas a longer RTO may enable the enterprise to rely on a less costly tape backup system. ISO 22301 divides business continuity strategy into three categories: determination and selection, resource requirements, and protection and mitigation.

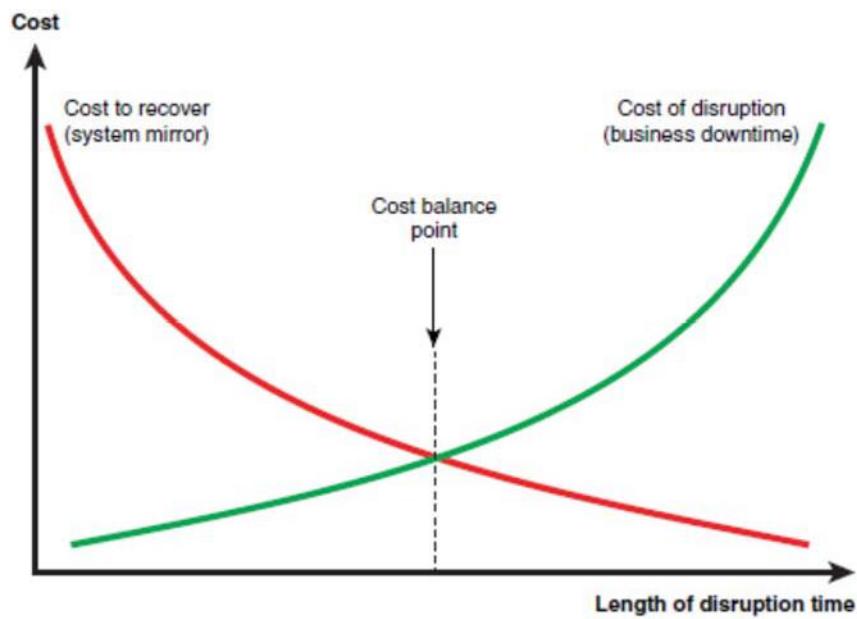


Figure 29 – Cost Balancing for Business Continuity Management

### **Business Continuity Readiness**

Business continuity readiness, refers to the capability of an organization and its assets to respond to, manage, and recover from a disruptive event. The Business continuity readiness consists of the following actions:

- Awareness program
- Training
- Resilience
- Control Selection
- Business Continuity Plan
- Exercising and Testing
- Performance Evaluation

### **Business Continuity Operations**

Business continuity operations constitutes the foundation layer for business continuity management. In response to a disruptive event, the business continuity process proceeds in three overlapping phases (see Figure 30):

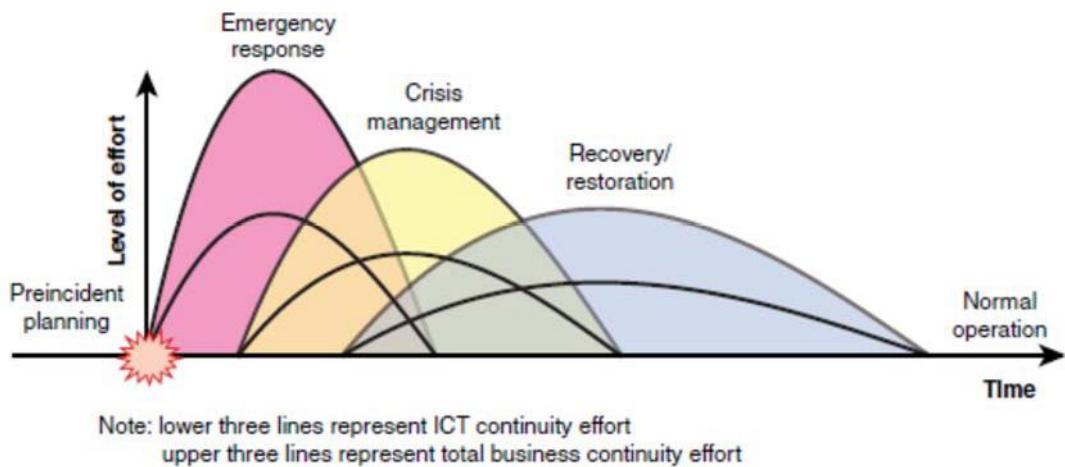
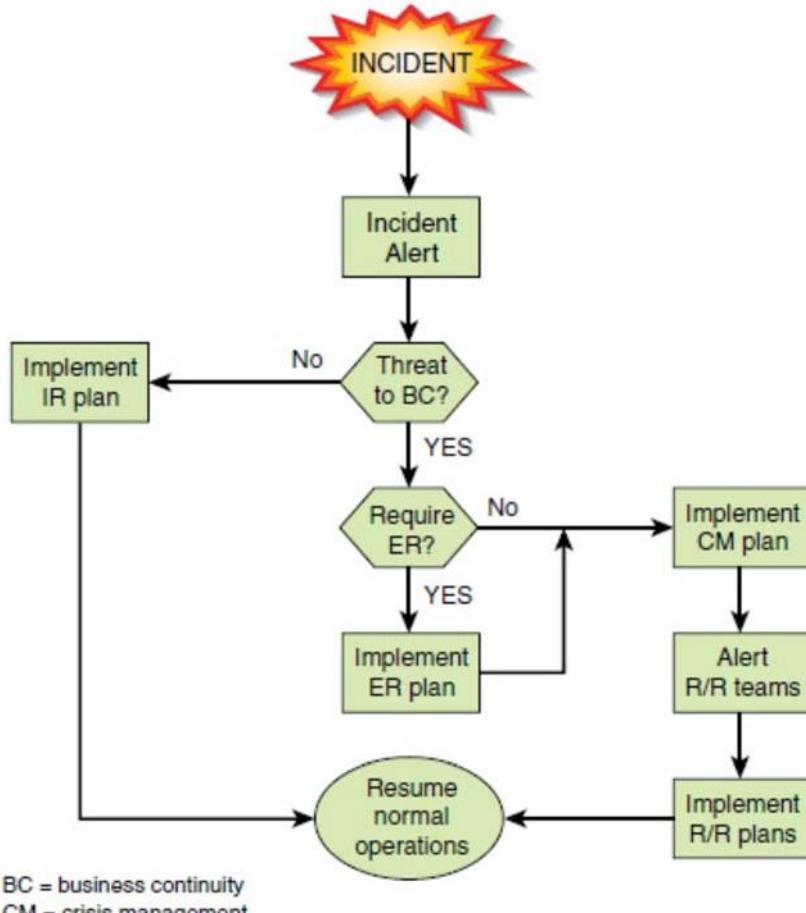


Figure 30 – Business Continuity Process

1. Emergency response: Focused on arresting or stabilizing an event
2. Crisis management: Focused on safeguarding the organization
3. Business recovery/restoration

The flowchart in Figure 31 provides a general picture of the relationship between security incident management, emergency response, crisis management, and recovery/ restoration.

The Information Security Forum's (ISF's) Standard of **Good Practice for Information Security (SGP)** breaks down the best practices in the business continuity category into two areas and seven topics and provides detailed checklists for each topic.



BC = business continuity  
 CM = crisis management  
 ER = emergency response  
 IR = incident response  
 R/R = recovery/restoration

Figure 31 – Incident Response and Business Continuity

## Aim/Objectives

The scope of this week is to introduce the key concepts of business continuity management (BCM). We provide a useful three-layer model for BCM, covering governance and policy, readiness, and operations and we are going through these areas. We also present flow between the major elements, as suggested in ISO 22301. BCM is a broad area that deals with all sorts of disasters, including natural disasters, health and safety incidents, and cyber-attacks. ISO 27002, Code of Practice for Information Security Controls, specifically focuses on threats to information assets and information and communications technology (ICT) systems. This week describes BCM in general terms, with specific reference to information assets and ICT systems, where appropriate.

## Learning Outcomes

Upon successful completion of this course, students should be able to:

- Present an overview of business continuity concepts, including the operation of business continuity management systems, the objectives for business continuity, and the essential components for maintaining business continuity.
- Understand the key elements of a business continuity program.
- Explain the concept of resilience in the context of business continuity.
- Outline the elements of a business continuity plan.
- Discuss performance analysis of a business continuity management system.
- Describe the phases of business continuity operation following a disruptive event.
- Present an overview of business continuity best practices.

## Key Words

business continuity management (BCM)	emergency response	business continuity
business continuity program	business continuity readiness	business continuity strategy

## Annotated Bibliography

### Basic

**Effective Cybersecurity: A Guide to Using Best Practices and Standards** 1st Edition, 2019, Willian Stallings, ISBN-13: 978-0134772806, ISBN-10: 0134772806

This week is based on Chapter 17 of the book.

### Supplementary

Power point presentation slides available in the platform

Video: [ISO 22301 Business Continuity Management](#)

### Suggestions for further reading

1. The Standard of Good Practice for Information Security 2016 (the Standard) provides comprehensive controls and guidance on current and emerging information security topics enabling organisations to respond to the rapid pace at which threats, technology and risks evolve. [Read full story](#).

## Self-Assessment Exercises

### Exercise 12.1

Describe the three key elements of business continuity.

### Exercise 13.2

According to ISO 22301, what are three key areas to consider while developing a business continuity strategy?

## Group Assignment

As part of the EU Cybersecurity strategy, the European Commission proposed the EU Network and Information Security directive. The NIS Directive (see [EU 2016/1148](#)) is the first piece of EU-wide cybersecurity legislation. The goal is to enhance cybersecurity across the EU. The NIS directive was adopted in 2016 and subsequently, because it is an EU directive, every EU member state has started to adopt national legislation, which follows or ‘transposes’ the directive. EU directives give EU countries some level of flexibility to take into account national circumstances, for example to re-use existing organizational structures or to align with existing national legislation. The deadline for national transposition by the EU member states is 9 May 2018.

On the other hand, the United States of America released the [Cybersecurity Framework Version 1.1](#). This Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization’s risk management processes. The Framework consists of three parts: the Framework Core, the Implementation Tiers, and the Framework Profiles. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure.

In this assignment, after you study both the EU NIS Directive and the USA NIST Cybersecurity Framework Version 1.1 you are requested to elaborate the following:

1. Provide a short overview of the main points of the NIS Directive.
2. Provide a short overview of the USA NIST Cybersecurity Framework Version 1.1
3. Compare and present the main differences between the two frameworks

Limit your report in 20-25 pages and concentrate on the most important aspects in both frameworks.

## Recommended time for the student to work

35 hours

## SECURITY MONITORING AND IMPROVEMENT

13<sup>th</sup> Week

### Summary

This final week we will concentrate on the importance concept of audits. We will discuss both the internal and external audits and how they contribute to safeguard any business area from malicious internal or external actions.

### Introductory Remarks

In general terms, an audit in an enterprise is an independent inspection of enterprise records to determine compliance with a standard or policy. More specifically, **a security audit relates to security policies and the mechanisms and procedures used to enforce that policy**. A security audit trail is an important component of a security audit.

X. **6, Security Audit and Alarms Framework**, lists the following objectives for a security audit:

- Allows the adequacy of the security policy to be evaluated
- Aids in the detection of security violations
- Facilitates making individuals accountable for their actions (or for actions by entities acting on their behalf)
- Assists in the detection of misuse of resources
- Acts as a deterrent to individuals who might attempt to damage the system X.816 has developed a model that shows the elements of the security auditing function and their relationships to security alarms (see Figure 32).

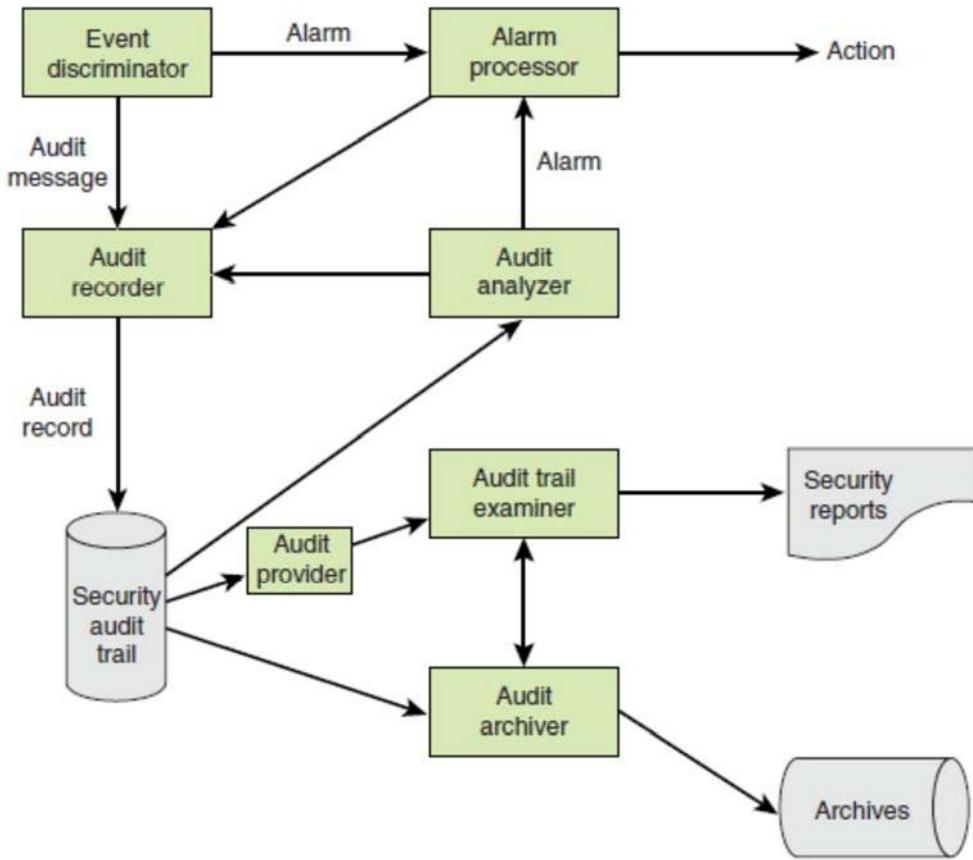


Figure 32 – Security Audit and Alarms Model

In terms of the individual security services, the following **security-related events** are important:

- Authentication: Verify success and verify fail
- Access control: Decide access success and decide access fail
- Non-repudiation: Non-repudiable origination of message, non-repudiable receipt of message, unsuccessful repudiation of event, and successful repudiation of event
- Integrity: Use of shield, use of unshield, validate success, and validate fail
- Confidentiality: Use of hide and use of reveal
- Audit: Select event for auditing, deselect event for auditing, and change audit event selection criteria

A sound auditing policy includes both **internal security audits and external security audits**. Internal audits are carried out by the organization itself, typically on a quarterly basis or after a significant security event. External audits are carried out by someone from outside, typically on annual basis.

**Security performance** is the measurable result of security controls applied to information systems and supporting information security programs. The Information Security Forum's (ISF's) Standard of Good Practice for Information Security (SGP) defines the security performance function as comprising three areas:

- Security monitoring and reporting: Consists of monitoring security performance regularly and reporting to specific audiences, such as executive management
- Information risk reporting: Consists of producing reports relating to information risk and presenting reporting to executive management on a regular basis
- Information security compliance monitoring: Consists of information security controls derived from regulatory and legal drivers and contracts, used to monitor security compliance

An essential element of security performance assessment is the selection of security performance metrics. This section looks first at the topic of security performance metrics and then treats the three areas previously listed. National Institute of Standards and Technology (NIST) IR 7564, Directions in Security Metrics Research, lists the following as the main broad uses of security metrics:

- **Strategic support:** Assessments of security properties can be used to aid in different kinds of decision making, such as program planning, resource allocation, and product and service selection.
- **Quality assurance:** Security metrics can be used during the software development life cycle to eliminate vulnerabilities, particularly during code production, by performing functions such as measuring adherence to secure coding standards, identifying vulnerabilities that are likely to exist, and tracking and analyzing security flaws that are eventually discovered.
- **Tactical oversight:** Monitoring and reporting of the security status or posture of an IT system can be carried out to determine compliance with security requirements (for example, policies, procedures, regulations), gauge the effectiveness of security controls and manage risk, provide a basis for trend analysis, and identify specific areas for improvement.

Figure 33, from **SP 800-55**, illustrates the process of developing information security metrics. It shows how this process takes place within a larger organizational context and demonstrates that information security metrics are used to progressively measure implementation, efficiency, effectiveness, and the business impact of information security activities within organizations or for specific systems.

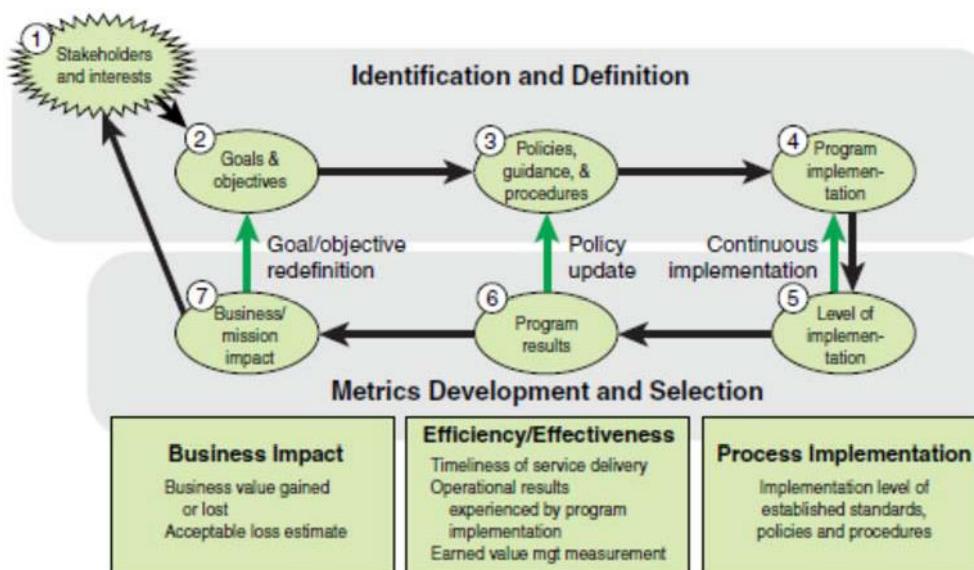


Figure 33 – Information Security Metrics Development Process

SP 800-55 provides a view of implementing the monitoring and reporting function based on the security performance metrics, shown in Figure 34.

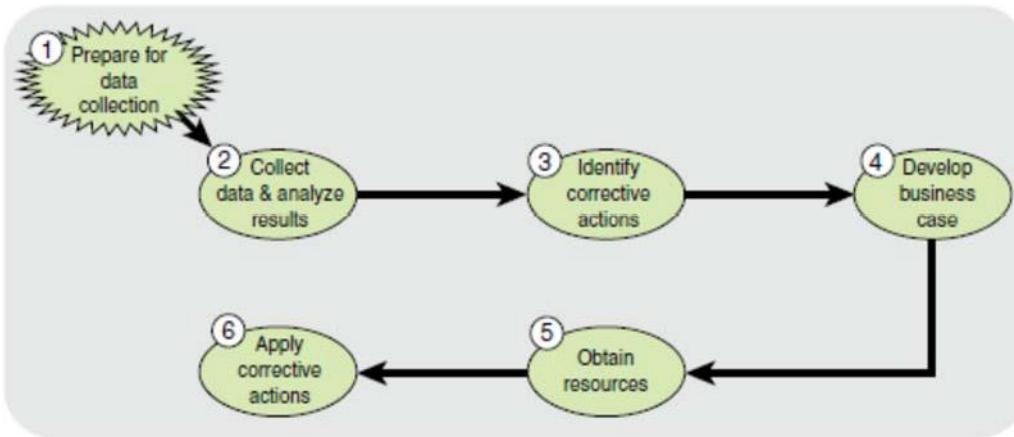


Figure 34 – Information Security Metrics Program Implementation Process

This process proceeds in six steps:

1. Prepare for data collection. In essence, this step involves the metrics development process shown in Figure 33.
2. Collect data and analyze results. The analysis should identify gaps between actual and desired performance, identify reasons for undesired results, and identify areas that require improvement.

3. Identify corrective actions. Based on step 2, determine appropriate corrective actions and prioritize them based on risk mitigation goals.
4. Develop business case. This involves developing a cost model for each corrective action and making a business case for taking that action.
5. Obtain resources. Obtain the needed budget and resource allocation.
6. Apply corrective actions. These actions may include adjustments in management, technical, and operational areas.

Concerning best practices, one can check that the SGP breaks down the best practices in the security monitoring and improvement category into two areas and eight topics and provides detailed checklists for each topic.

## Aim/Objectives

The scope of this week is to introduce the techniques and related standards for auditing and monitoring the performance of cybersecurity controls, with a view to spotting gaps in the system and devising improvements.

## Learning Outcomes

Upon successful completion of this course, students should be able to:

- Present the X.816 model of security audit and alarms.
- List useful information to collect in security audit trails.
- Discuss security audit controls.
- Understand the use of metrics in security performance monitoring.
- Describe the essential elements of information risk reporting.
- Discuss what is involved in information security compliance monitoring.
- Present an overview of security monitoring and improvement best practices.

## Key Words

external security audit	internal security audit	activity
security audit control	security performance metric	security report

## Annotated Bibliography

### Basic

**Effective Cybersecurity: A Guide to Using Best Practices and Standards** 1st Edition, 2019, Willian Stallings, ISBN-13: 978-0134772806, ISBN-10: 0134772806

This week is based on Chapter 18 of the book.

### Supplementary

Power point presentation slides available in the platform

Video: Watch this webinar related to [Process of Auditing Information Systems](#)

### Suggestions for further reading

1. ITU- Information technology X816: Open Systems Interconnection - Security frameworks for open systems: Security audit and alarms framework. Read more on this standard in this [link](#)
2. SP 800-55 provides guidance on how an organization, through the use of metrics, identifies the adequacy of in-place security controls, policies, and procedures. It provides an approach to help management decide where to invest in additional security protection resources or when to research the causes of nonproductive controls. It explains the metric development and implementation process and how it can also be used to adequately justify security control investments. The results of an effective metric program can provide useful data for directing the allocation of information security resources and should simplify the preparation of performance-related reports. Read more in this [link](#)

## Self-Assessment Exercises

### Exercise 13.1

Briefly define the terms security audit and security audit trail.

### Exercise 13.2

What are some of the auditable items suggested in the X.816 model of security audits and alarms?

## Recommended time for the student to work

15 hours

## **STUDY WEEK AND FINAL EXAMS**

The final examination will consist of true/false, multiple-choice questions and a small number of questions

### **Recommended time for the student to work**

40 hours

**Date/Time of Final Exam: TBD**

## ANSWERS TO REVIEW QUESTIONS

### CYBER SYSTEMS AND CYBER SECURITY - 1<sup>st</sup> Week

**Exercise 1.1:** The following terms are defined from a cybersecurity perspective:

**Availability**—The property of a system or a system resource being accessible, or usable, or operational upon demand by an authorized system entity, according to performance specifications for the system. Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed, and maintaining a correctly functioning operating system environment that is free of software conflicts.

**Integrity**—This means maintenance of consistency, accuracy, and trustworthiness of data over its entire life cycle. There should not be any change in data in transit, such as unauthorized people altering data (for example, in a breach of confidentiality). These measures include encryption, file permissions, and user access controls.

**Authenticity**—This is simply the property of being genuine and being able to be verified and trusted. It is a technological concept and can be solved by cryptography. Authenticity is about one party, Alice, interacting with another, Bob to convince Bob that some data really comes from Alice.

**Non-repudiation**—This is a legal assurance that the sender of information is provided with proof of delivery, and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. For example, non-repudiation is about Alice showing to Bob a proof that some data really comes from Alice, such that not only is Bob convinced, but Bob also gets the assurance that he could show the same proof to Charlie, and Charlie would be convinced, too, even if Charlie does not trust Bob.

**Confidentiality**—This, in lay terms, is privacy. It is a set of rules that limits access to information from reaching the wrong people, while making sure that the right people can in fact get it. Data encryption is a common method of ensuring confidentiality. User IDs and passwords constitute a standard procedure; two-factor authentication is becoming the norm. Other options include biometric verification and security tokens, key fobs, or soft tokens.

**Exercise 1.2:** Three key challenges in developing an effective cybersecurity system are as follows:

- Scale and complexity of cyberspace—Many telecom companies, such as Ericsson, are working to connect all devices and people to each other to make a fully connected society by next decade. It would cut across wired, wireless, and satellite networks and would consist of mobile devices, PDAs, laptops, wearables, cars, Internet of Things (IOT) devices, the cloud, and so on. The challenges to achieving cybersecurity will change with each technological advancement because new applications of information technology will emerge, which will trigger massive changes in societal norms.
- Nature of threat—It will come from both internal sources and external sources. Common actors involved are vandals, criminals, terrorists, hostile states, and other malevolent actors. The desire to collect, analyze, and store individual information by both government agencies and corporations will create security and privacy risks.
- Trade-off between user needs and security implementation—It is a heavily debated topic that involves huge trade-offs because users want to use the most recent technology without caring for overall security, whereas an enterprise wants security and continuity at all costs. For example, employees prefer to connect their personal devices to the office network and share content, but this might introduce potent viruses and malware that could infect the whole system in a short time.

## CYBER SECURITY STANDARDS AND BEST PRACTICES – 2<sup>nd</sup> Week

**Exercise 2.1:** This is a judgment question. The student is requested to provide a justification for the answer.

**Exercise 2.2:** The most significant activity of the ISF is the ongoing development of the Standard of Good Practice for Information Security (SGP). This document is a focused reference guide for enterprises to identify and manage information security risks in their operations and supply chains. This document is well researched, with input from its members, as well as an analysis of the leading standards on cybersecurity, information security, and risk management.

## CYBER SECURITY FRAMEWORKS– 3<sup>rd</sup> Week

**Exercise 3.1:** ENISA is actively contributing to a high level of network and information security (NIS) within the Union, since it was set up in 2004, to the development of a culture of NIS in society and in order to raise awareness of NIS, thus contributing to proper functioning of the internal market. The Agency works

closely together with Members States and private sector to deliver advice and solutions. This includes, the pan-European Cyber Security Exercises, the development of National Cyber Security Strategies, CSIRTs cooperation and capacity building, but also studies on secure Cloud adoption, addressing data protection issues, privacy enhancing technologies and privacy on emerging technologies, eIDs and trust services, and identifying the cyber threat landscape, and others. ENISA also supports the development and implementation of the European Union's policy and law on matters relating to NIS.

**Exercise 3.2:** Five core functions mentioned in the NIST framework are as follows:

- Identification – This implies development of organizational understanding of management of cybersecurity risk to systems, assets, data, and capabilities.
- Protection–This implies development and implementation of appropriate safeguards for ensuring delivery of critical infrastructure services.
- Detection–This implies development and implementation of appropriate activities for identification of any occurrence of a cybersecurity event.
- Response–This implies development and implementation of appropriate activities for taking action regarding a detected cybersecurity event.
- Recovery–This implies development and the appropriation of activities needed for maintenance of plans for resilience and for restoration of capabilities or services impaired due to a cybersecurity event.

## RISK MANAGEMENT – 4<sup>th</sup> Week

**Exercise 4.1:** The stages of risk management process are described as follows:

- Risk assessment—Here you identify the risk to analyze it thoroughly and then to evaluate the risk against establish metrics to categorize it for further action.
- Risk communication and consultation—This is the continual and iterative processes an organization follows to provide, share, or obtain information about the risk and to keep updating or taking feedback from the key stakeholders regarding the management of risk.
- Risk monitoring and review—This stage involve continuous monitoring and review of all risk information obtained from the risk management activities.

**Exercise 4.2:** The five steps of the risk assessment process are as follows:

- Context Establishment
- Risk Identification
- Risk analysis
- Risk evaluation
- Risk treatment

## CYBER-RISK MANAGEMENT – 5<sup>th</sup> Week

**Exercise 5.1:** Cyber risk means any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems.

**Exercise 5.2:** i) Context establishment, ii) identification of cyber risk, iii) analysis of cyber risk, iv) evaluation of cyber risk, v) treatment of cyber risk

## RISK ASSESSMENT CONCEPTS – 6<sup>th</sup> Week

### Exercise 6.1

Fair and accurate risk assessment enables an organization to determine an appropriate budget for security and implement appropriate security controls that optimize the level of protection while not overshooting the budget. Risk assessment enumerates potential security breaches, fair estimates of their cost, and the likelihood of their occurrence. Without risk assessment, an organization cannot formulate a cost-effective strategy to secure itself.

### Exercise 6.2

An organization faces enormous challenges in determining the level of risk. In general terms, these challenges fall into two categories: the difficulty of estimating and the difficulty of predicting. Another challenge in risk assessment is the difficulty of predicting future conditions.

## RISK ASSESSMENT PROCESS - 7<sup>th</sup> Week

### Exercise 7.1

STRIDE is a threat classification system developed by Microsoft to categorize deliberately planned attacks. It includes identity spoofing, data tampering, repudiation, information disclosure to non-authorized entities, denial-of-service (DoS), privilege elevation, and so on. For example, imagine that a bright engineering team of company X is working on a new high-end mobile phone. The product is announced, and the CEO of X describes its capabilities and fixes its release date. All is going fine until a key member of the design team voluntarily discloses design specifications (for extra money and a better job than his current one) and implementation-level details to the company's key competitor, say Y. As a result, Y improves the specifications, adds more capability, and, following an Agile go-to-market strategy, it announces an earlier release date. This results in X's image being downgraded, its share price crashing, investors losing confidence, and a complete panic in the design team. This is a classic case of involuntary information disclosure.

### Exercise 7.2

Regarding risk assessment, you consider the following types of assets:

- **Hardware assets**—This includes physical servers, workstations, laptops, mobile devices, removable media, PDA devices, television sets, and networking and telecommunications equipment.
- **Software assets**—This includes applications, operating systems and other system software, virtual machine and container virtualization software, software for software defined networks (SDNs) and network function virtualization (NFV), database management systems (DBMSs), decision support systems (DSS), and analytic engine (AEs).
- **Information assets**—This includes assets directly connected with information or its storage (for example, databases, file systems, cloud storage, routing information). This category of asset depends on the nature of work done by the organization.
- **Business assets**—This category includes all other organization assets (such as human capital, business processes, and factory location) that don't fit in preceding categories of assets. It also includes intangible assets, such as organization control, know-how, reputation, and image of the organization.

## RISK ASSESSMENT APPROACHES – 8<sup>th</sup> Week

### Exercise 8.1

FAIR defines the key terms as follows:

- Asset—Any data, device, or other component of the environment that involves information and that can be illicitly accessed, used, disclosed, altered, destroyed, and/or stolen, resulting in loss
- Risk—The probable frequency and probable impact of future loss
- Threat—Any entity capable of harming an asset and/or organization partially or permanently
- Vulnerability—The probability of an asset's inability to resist actions of a threat agent FAIR definitions are much more specific than ISO 27005 definitions pertaining to risk analysis.

### Exercise 8.2

ISO 27005 lists four options for treating risk:

- Risk reduction or mitigation—This implies actions taken to lessen the probability and/ or negative consequences associated with a risk.
- Risk retention—This implies acceptance of the cost from a risk.
- Risk avoidance—This implies a decision not to become involved in or an action to withdraw from a risk situation.
- Risk transfer or sharing—This implies sharing the burden of loss from a risk with a third party, such as an insurance agency.

## RISK ANALYSIS AND TREATMENT – 9<sup>th</sup> Week

### Exercise 9.1

Likelihood assessment does not yield a numerical value subject to calculation using probability theory. Rather, it is the process of developing some sort of agreed-upon likelihood score that estimates the chance of a threat action. A likelihood assessment considers the presence, tenacity, and strengths of threats as well as the presence of vulnerabilities and the effectiveness of security controls already in place. This assessment is applied to each identified potential threat action.

The essence of likelihood assessment for a given threat to a given asset is shown in the following steps:

**Step 1.** Determine the likelihood that a threat event will occur. That is, determine the likelihood that this threat will develop into an attack on the given asset.

**Step 2.** Determine the degree of vulnerability of the asset to the threat.

**Step 3.** Based on Step 1 and Step 2, determine the likelihood that a security incident will occur.

### Exercise 9.2

SP 800-100 provides some general guidance for evaluating risk and prioritizing action based on a three-level model:

- **High:** If an observation or a finding is evaluated as high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
- **Moderate:** If an observation is rated as moderate risk, corrective actions are needed, and a plan must be developed to incorporate these actions within a reasonable period of time.
- **Low:** If an observation is described as low risk, the system's authorizing official must either determine whether corrective actions are still required or decide to accept the risk.

## THREAT AND VULNERABILITY MANAGEMENT-10<sup>th</sup> Week

### Exercise 10.1

**Technical vulnerability management**, usually referred to simply as vulnerability management, is a security practice specifically designed to proactively mitigate or prevent the exploitation of technical vulnerabilities that exist in a system or an organization. The process involves the **identification, classification, remediation, and mitigation** of various vulnerabilities in a system. It is an integral part of cybersecurity and is practiced together with risk management as well as other security practices.

### Exercise 10.2

This is a judgment question. The student is requested to provide a justification for the answer.

## SECURITY INCIDENT MANAGEMENT 11<sup>th</sup> Week

### Exercise 11.2

The **security event management** (SEM) is the process of identifying, gathering, monitoring, analyzing, and reporting security-related events. The objective of SEM is to extract from a large volume of security events

those events that qualify as incidents. SEM takes data input from all devices/nodes and other similar applications, such as log management software. The collected events data is analyzed with security algorithms and statistical computations to trace out any vulnerability, threat, or risk.

### **Exercise 11.2**

This is a judgment question. The student is requested to provide a justification for the answer.

## **BUSINESS CONTINUITY -12<sup>th</sup> Week**

### **Exercise 12.1**

Business continuity is the ability of an organization to maintain essential functions during and after a disaster has occurred. Business continuity includes three key elements:

- Resilience—Critical business functions and the supporting infrastructure must be designed in such a way that they are materially unaffected by relevant disruptions (for example, through the use of redundancy and spare capacity).
- Recovery—Arrangements have to be made to recover or restore critical and less critical business functions that fail for some reason.
- Contingency—The organization must establish a generalized capability and readiness to cope effectively with whatever major incidents and disasters occur, including those that were not, and perhaps could not have been, foreseen.

### **Exercise 12.2**

According to ISO 22301, three key areas to be considered while developing business continuity strategy are as follows:

- Protecting prioritized activities – For activities deemed significant for maintaining continuity, the organization should look at the general strategic question of how each activity is carried out. The goal is to determine a strategy that reduces the risk to the activity.

- Stabilizing, continuing, resuming, and recovering prioritized activities and their dependencies and supporting resources—The next step is to provide more detailed options for managing each prioritized activity during the business continuity process.
- Mitigating, responding to, and managing impacts—In this step, the organization should spell out the strategies that attempt to contain the damage to the organization from disasters.

## **SECURITY MONITORING AND IMPROVEMENT – 13<sup>th</sup> Week**

### **Exercise 13.1**

A security audit is an independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures. The key objective of a security audit is to assess the security of the system's physical configuration and environment, software, information handling processes, and user practices.

A security audit trail is a chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a security-relevant transaction from inception to final results. Its key objective is to provide a historical record of progression based on a sequence of events to provide proof of compliance and operational integrity.

### **Exercise 13.2**

Some of the auditable items suggested in the X.816 model of security audits and alarms are as follows:

- Security-related events related to a specific connection, such as connection request/confirmation.
- Security-related events related to the use of security services, such as security service requests.
- Security-related events related to management, such as management operations/notifications.
- Events such as access denials, authentication, and attribute changes.
- Individual security services such as authentication results, access control results, non-repudiation, and integrity responses.



**FORM: 200.1.3**

## **STUDY GUIDE**

**Course: CYS624 - Data Privacy in the era of Data  
Mining and AI**

## Course Information

<b>Institution</b>	European University Cyprus		
<b>Programme of Study</b>	Cybersecurity (MSc)		
<b>Course unit</b>	CYS624 Data Privacy in the era of Data Mining and AI		
<b>Level</b>	<b><i>Undergraduate</i></b>	<b><i>Postgraduate</i></b>	
		<b><i>Master</i></b>	<b><i>PhD</i></b>
		√	
<b>Language of Instruction</b>	English		
<b>Teaching Methodology</b>	Distance Learning		
<b>Course Type</b>	<b><i>Compulsory</i></b>		<b><i>Optional</i></b>
			√
<b>Number of Group Consultation Meetings/ Web-Conferences/ Lectures</b>	<b>Total</b>	<b>Face to Face</b>	<b>Web-Conferences</b>
	14	1	13
<b>Number of Activities/ Assignments</b>	4		
<b>Final Assessment</b>	<b><i>Assignments</i></b>	<b><i>Final Examinations</i></b>	
	50 %	50 %	
<b>Number of Credits (ECTS)</b>	10		

<b>Study Guide drafted by</b>	Dr Yianna Danidou
<b>Editing and final approval of Study Guide by</b>	Dr Yianna Danidou

## COURSE CONTENTS

		Page
	<b>Error! Reference source not found.</b>	<b>Error! Bookmark not defined.</b>
1	Week 1 - INTRODUCTION TO CYBERSECURITY DATA MINING  <b>1st Week</b>	9
2	Week 2 - SOCIAL BIG DATA APPLICATIONS  <b>2nd Week</b>  <b>Summary</b>	17
3	Week 3 - BIG CONCEPTS IN DATA MINING  <b>3rd Week</b>  <b>Summary</b>	2224
4	Week 4 - CLASSICAL MACHINE – LEARNING PARADIGMS FOR DATA MINING  <b>4th Week</b>	27

5	Week 5 - PRIVACY AND DATA MINING	<b>5th Week</b>	33
<b>Summary</b>			
6	Week 6 - PRIVACY-PRESERVING DATA MINING	<b>6th Week</b>	40
<b>Summary</b>			
7	Week 7 - EMERGING CHALLENGES IN CYBERSECURITY	<b>7th Week</b>	48
<b>Summary</b>			
8	Week 8 - DATA MINING FOR THE INTERNET OF THINGS: LITERATURE REVIEW AND CHALLENGES	<b>8th Week</b>	57
<b>Summary</b>			
9	Week 9 - AI-BASED PRIVACY MECHANISM FOR PERSONAL DATA IN THE INTERNET OF THINGS	<b>9th Week</b>	65
<b>Summary</b>			
10	Week 10 - Error! Reference source not found.		74
11	Week 11 - BEYOND CONSENT-BASED PRIVACY PROTECTION		83

	11th Week	
	<b>Summary</b>	
12	Week 12 - INVITED LECTURE	91
	<b>11th &amp; 12th Week</b>	
13	Week 13 - INVITED LECTURE	91
	<b>11th &amp; 12th Week</b>	
14	<b>Error! Reference source not found.</b>	92
	Indicative answers to Self-Assessment exercises	93

## 1st GROUP CONSULTATION MEETING

### Programme Presentation

Leading companies today are rethinking the role of information security in their organizations. They realize that in a digital world, cybersecurity is the key to safeguarding their most precious assets—intellectual property, customer information, financial data, and employee records, among others. But far more than a defensive measure, companies also know that cybersecurity can better position their organization with business partners, customers, investors, and other stakeholders.

The European cybersecurity market is about 25% (i.e. about €17bln) of the world market (estimated at €70bln in 2015), with an average yearly growth slightly larger than 6%, when the

world market is growing at about 10%/year. Recent study compiled by Europe's cybersecurity industry leaders pointed out that Europe is in danger of falling behind in the international digital economy field.

The Master in Cybersecurity is a cutting-edge program, designed for those wishing to develop a career as a cyber-security professional, or to take a leading technical or managerial role in an organization critically dependent upon data and information communication technology. Students will develop an advanced knowledge of information security and an awareness of the context in which information security operates in terms of safety, environmental, social and economic aspects. They will gain a wide range of intellectual, practical and transferable skills, enabling them to develop a flexible professional career in IT.

Key elements of this postgraduate degree are: the *real life experience* given by the opportunity to apply their theoretical knowledge through specialized virtual and remote security laboratories in which they will be able to carry out activities such as reconnaissance, network scanning and exploitation exercises, and investigate the usage and behavior of security systems such as Intrusion Detection and Prevention Systems thus becoming confident in the practical application of the latest tools; the *high-level insight* that will enhance student's ability to research and design creative cyber security solutions to address business problems; *hands-on skills* through experimentation with security techniques, cryptographic algorithms, cyber forensics building an ethical hacking environment; and *flexibility* since students will also be able to choose either the completion of a Master thesis or to complete a Research methods course and two elective courses.

Students undertake modules to the value of 90 ECTS credits.

## COURSE PRESENTATION THROUGH THE STUDY GUIDE

The CYS624 course is an elective course. Data collection and data analysis have become ubiquitous in modern world. Along with this trend, the need to protect private and sensitive information in data has become an important issue. This course will study a few state-of-the-art techniques in protecting data privacy and data security when the data is released to public or is subject to computer-based analysis, such as data mining.

This course introduces students to concepts and methods for creating technologies and related policies with provable guarantees of privacy protection while allowing society to collect and share person-specific information for many worthy purposes. Methods include those related to the identifiability of data, record linkage, data profiling, data fusion, data anonymity, de-identification,

policy specification and enforcement and privacy-preserving data mining. Students also learn to be "data protectors" by assessing privacy protocols, algorithms and anonymity protection schemes to protect inferences in shared data.

Students are required to attend bi- weekly virtual classes to submit discussion posts, reading assignment case studies, media content review and exams.

On successful completion, the student will have the knowledge and skills to:

- Display a comprehensive understanding of different data mining tasks and the algorithms most appropriate for addressing them;
- Evaluate models/algorithms with respect to their accuracy;
- identify and articulate some basic ethical and policy-based frameworks;
- understand the relationship between data, ethics, and society; and
- be able to critically assess their own work and education in the area of data science. In particular, course assignments will emphasize researcher and practitioner reflexivity, allowing students to explore their own social and ethical commitments as future data scientists and information professionals

This study guide has been prepared collectively by the academic staff teaching in the program of study this course belongs to and by the Distance Education Unit Director. The guide has been approved by the relevant Department Chair and the Distance Education Unit Director. The study guide is based on the syllabus and learning material (provided through the online learning platform) of the course CYS624. The guide consists of a basic tool of the learning process for this course and it has been designed to use it along with the course learning material. The aim of this guide is to direct students on how to use the learning material of this course in order to understand and comprehend it. The guide aims to provide the necessary support needed for distance learning. The guide is continuously updated to keep in accord with the course learning material and to meet the aim of the course. Although the study guide provides extensive information related to the course, it does not substitute in any way the learning material provided on the learning platform. It is imperative that the studying of the learning material and executing the rest of the activities of the course (e.g. attending online lectures, completing coursework) are very important for the successful completion of the course.

This guide consists of a number of units, divided in 13 weeks, each one comprised of the summary and introductory remarks, aim, learning outcomes, keywords, required learning material, recommended further learning material, self-assessment activities and expected time for self-

study. At the end of this study guide, students can find suggested solutions and proposed answers to all the self-assessment activities of this guide. It is very important that students carry out the suggested self-assessment activities because it will assist them to understand in a practical way the theoretical material they study for this course. In addition, the self-assessment activities help to motivate and encourage students to carry out their self-study and to develop their analytical and critical thinking skills. The self-assessment activities together with the model answers to the self-assessment activities serve as a kind of a self-assessment for students. The expected time for self-study of each unit includes the expected time spent on studying the learning material and carrying out the self-assessment activities of each unit. The expected time for self-study does not include the expected time for attending online lectures, coursework preparation, final examination preparation, and final examination itself.

### **Recommended time for the student to work**

Approximately 5 hours for comprehending the study guide.

# INTRODUCTION TO CYBERSECURITY DATA MINING

1<sup>st</sup> Week

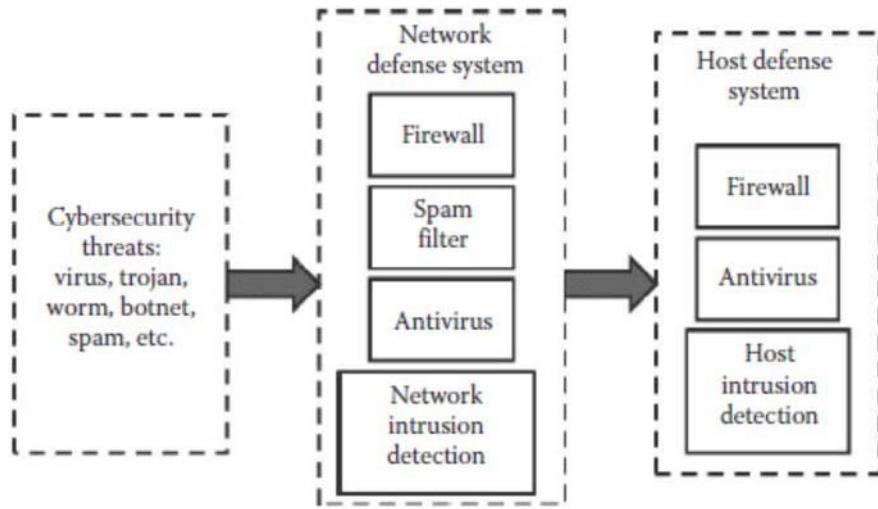
## Summary

Vulnerabilities in cyberinfrastructure can be attacked horizontally or vertically. Hence, cyber threats can be evaluated horizontally from the perspective of the attacker(s) or vertically from the perspective of the victims. First, we look at cyber threats vertically, from the perspective of the victims. A variety of adversarial agents such as nation-states, criminal organizations, terrorists, hackers, and other malicious users can compromise governmental homeland security through networks.

## Introductory Remarks

Next, we look at cyber threats horizontally from the perspective of the victims. We consider any malicious activity in cyberspace as a cyber threat. A cyber threat may result in the loss of or damage to cyber components or physical resources. Most cyber threats are categorized into one of three groups according to the intruder's purpose: stealing confidential information, manipulating the components of cyberinfrastructure, and/or denying the functions of the infrastructure. If we evaluate cyber threats horizontally, we can investigate cyber threats and the subsequent problems.

To secure cyberinfrastructure against intentional and potentially malicious threats, a growing collaborative effort between cybersecurity professionals and researchers from institutions, private industries, academia, and government agencies has engaged in exploiting and designing a variety of cyber defense systems. Cybersecurity researchers and designers aim to maintain the confidentiality, integrity, and availability of information and information management systems through various cyber defense systems that protect computers and networks from hackers who may want to intrude on a system or steal financial, medical, or other identity-based information



As shown in this Figure, conventional cybersecurity systems address various cybersecurity threats, including viruses, Trojans, worms, spam, and botnets. These cybersecurity systems combat cybersecurity threats at two levels and provide network- and host-based defenses. Network-based defense systems control network flow by network firewall, spam filter, antivirus, and network intrusion detection techniques. Host-based defense systems control upcoming data in a workstation by firewall, antivirus, and intrusion detection techniques installed in hosts. Conventional approaches to cyber defense are mechanisms designed in firewalls, authentication tools, and network servers that monitor, track, and block viruses and other malicious cyber attacks. For example, the Microsoft Windows operating system has a built-in Kerberos cryptography system that protects user information. Antivirus software is designed and installed in personal computers and cyberinfrastructures to ensure customer information is not used maliciously. These approaches create a protective shield for cyberinfrastructure.

Data-capturing tools, such as Libpcap for Linux, Solaris BSM for SUN, and Winpcap for Windows, capture events from the audit trails of resource information sources (e.g., network). Events can be host-based or network-based depending on where they originate. If an event originates with log files, then it is categorized as a host-based event. If it originates with network traffic, then it is categorized as a network-based event. A host-based event includes a sequence of commands executed by a user and a sequence of system calls launched by an application, e.g., send mail. A network-based event includes network traffic data, e.g., a sequence of internet protocol (IP) or transmission control protocol (TCP) network packets. The data-preprocessing module filters out the attacks for which good signatures have been learned.

Proactive approaches anticipate and eliminate vulnerabilities in the cyber system, while remaining prepared to defend effectively and rapidly against attacks. To function correctly, proactive security solutions require user authentication (e.g., user password and biometrics), a system capable of avoiding programming errors, and information protection [e.g., privacy-preserving data mining (PPDM)]. PPDM protects data from being explored by data-mining techniques in cybersecurity applications. We will discuss this technique in detail in later weeks. Proactive approaches have been used as the first line of defense against cybersecurity breaches.

It is not possible to build a system that has no security vulnerabilities. Vulnerabilities in common security components, such as firewalls, are inevitable due to design and programming errors.

The second line of cyber defense is composed of reactive security solutions, such as intrusion detection systems (IDSs). IDSs detect intrusions based on the information from log files and network flow, so that the extent of damage can be determined, hackers can be tracked down, and similar attacks can be prevented in the future.

Due to the availability of large amounts of data in cyberinfrastructure and the number of cyber criminals attempting to gain access to the data, data mining, machine learning, statistics, and other interdisciplinary capabilities are needed to address the challenges of cybersecurity. Because IDSs use data mining and machine learning, we will focus on these areas. Data mining is the extraction, or “mining,” of knowledge from a large amount of data. The strong patterns or rules detected by data-mining techniques can be used for the nontrivial prediction of new data. In nontrivial prediction, information that is implicitly presented in the data, but was previously unknown is discovered. Data-mining techniques use statistics, artificial intelligence, and pattern recognition of data in order to group or extract behaviors or entities. Thus, data mining is an interdisciplinary field that employs the use of analysis tools from statistical models, mathematical algorithms, and machine learning methods to discover previously unknown, valid patterns and relationships in large data sets, which are useful for finding hackers and preserving privacy in cybersecurity.

Data mining is also an integral part of knowledge discovery in databases (KDDs), an iterative process of the nontrivial extraction of information from data and can be applied to developing secure cyberinfrastructures.

Data-mining techniques are used to aid in the development of predictive models that enable a real-time cyber response after a sequence of cybersecurity processes, which include real-time

data sampling, selection, analysis and query, and mining peta-scale data to classify and detect attacks and intrusions on a computer network

Learning user patterns and/or behaviors is critical for intrusion detection and attack predictions. Learning these behaviors is important, as they can identify and describe structural patterns in the data automatically and theoretically explain data and predict patterns. Automatic and theoretic learning require complex computation that calls for abundant machine-learning algorithms.

Traditionally, proactive security solutions (Canetti et al., 1997; Barak et al., 1999) are designed to maintain the overall security of a system, even if individual components of the system have been compromised by an attack. Recently, the improvement of data-mining techniques and information technology brings unlimited chances for Internet and other media users to explore new information. The new information may include sensitive information and, thus, incur a new research domain where researchers consider data-mining algorithms from the viewpoint of privacy preservation. This new research, called PPDM is designed to protect private data and knowledge in data mining. PPDM methods can be characterized by data distribution, data modification, data-mining algorithms, rule hiding, and privacy preservation techniques.

Cyber intrusion is defined as any unauthorized attempt to access, manipulate, modify, or destroy information or to use a computer system remotely to spam, hack, or modify other computers. An IDS intelligently monitors activities that occur in a computing resource, e.g., network traffic and computer usage, to analyse the events and to generate reactions. In IDSs, it is always assumed that an intrusion will manifest itself in a trace of these events, and the trace of an intrusion is different from traces left by normal behaviors. To achieve this purpose, network packets are collected, and the rule violation is checked with pattern recognition methods. An IDS system usually monitors and analyzes user and system activities, accesses the integrity of the system and data, recognizes malicious activity patterns, generates reactions to intrusions, and reports the outcome of detection.

### *Misuse/Signature Detection*

Misuse detection, also called signature detection, is an IDS triggering method that generates alarms when a known cyber misuse occurs. A signature detection technique measures the similarity between input events and the signatures of known intrusions. It flags behavior that shares similarities with a predefined pattern of intrusion. Thus, known attacks can be detected immediately and realizable with a lower false-positive rate. However, signature detection cannot detect novel attacks.

### *Anomaly Detection*

Anomaly detection triggers alarms when the detected object behaves significantly differently from the predefined normal patterns. Hence, anomaly detection techniques are designed to detect patterns that deviate from an expected normal model built for the data. In cybersecurity, anomaly detection includes the detection of malicious activities, e.g., penetrations and denial of service. The approach consists of two steps: training and detection. In the training step, machine-learning techniques are applied to generate a profile of normal patterns in the absence of an attack. In the detection step, the input events are labeled as attacks if the event records deviate significantly from the normal profile. Subsequently, anomaly detection can detect previously unknown attacks. However, anomaly detection is hampered by a high rate of false alarms.

### *Hybrid Detection*

Most current IDSs employ either misuse detection techniques or anomaly detection techniques. Both of these methods have drawbacks: misuse detection techniques lack the ability to detect unknown intrusions; anomaly detection techniques usually produce a high percentage of false alarms. To improve the techniques of IDSs, researchers have proposed hybrid detection techniques to combine anomaly and misuse detection techniques in IDSs.

### *Scan Detection*

Scan detection generates alerts when attackers scan services or computer components in network systems before launching attacks. A scan detector identifies the precursor of an attack on a network, e.g., destination IPs and the source IPs of Internet connections. Although many scan detection techniques have been proposed and declared to be able to detect the precursors of cyber attacks, the high false-positive rate or the low scan detection rate limits the application of these solutions in practice.

### *Profiling Modules*

Profiling modules group similar network connections and search for dominant behaviors using clustering algorithms.

## **Aim/Objectives**

This week aims to introduce students in the most important components of cybersecurity, data mining, and machine learning. We have provided an overview of types of cyber attacks and cybersecurity solutions and explained that cyber attacks compromise cyberinfrastructures in three

ways: They help cyber criminals steal information, impair componential function, and disable services. We have briefly defined cybersecurity defense strategies, which consist of proactive and reactive solutions. We highlighted proactive PPDM, and the reactive misuse detection, anomaly detection, and hybrid detection techniques. PPDM is rising in popularity as operative computation and data sharing in cyber space creates more concerns about privacy leaks, and misuse detection, anomaly detection, and hybrid detection techniques compose many IDSs. Misuse detection methods attempt to match test data with the profiled anomalous patterns, while anomalous detection solutions profile normal patterns to search for outliers. Hybrid detection systems combine misuse and anomalous detection techniques to improve the detection rate and reduce the false-alarm rate. In addition, we discuss two specific research areas in cybersecurity: scan detection and network profiling. Scan detection is used to detect the precursor of attacks, such that its use can lead to the earlier deterrence of attacks or defenses. Profiling networks facilitate the administration and monitoring of cybersecurity through extraction, aggregation, and visualization tools.

## Learning Outcomes

On completion of this course students should have gained a good understanding of the basic concepts, principles and techniques of data mining. Specifically, students should be able to:

- Define knowledge discovery and data mining.
- Recognize the key areas and issues in data mining in cybersecurity.
- Determine proactive and reactive security solutions.

## Key Words

Data capturing tools	PPDM	IDS
Data mining	Machine learning	Nontrivial prediction
Artificial Intelligence	KDDs	Attack prediction
Anomaly detection		

## Annotated Bibliography

### Required Materials

To achieve the educational needs of this unit the following material is used:

#### Primary Material

Chapter 1 of Dua, S. and Du, X., 2016. *Data mining and machine learning in cybersecurity*. Auerbach Publications.

In this chapter, the authors introduced what are the most important components of cybersecurity, data mining, and machine learning. They provide an overview of types of cyber attacks and cybersecurity solutions and explain that cyber attacks compromise cyberinfrastructures in three ways: They help cyber criminals steal information, impair componential function, and disable services.

#### Supportive material

Adams, N., Heard, N., Adams, N. and Heard, N., 2014. *Data analysis for network cyber-security*. World Scientific Publishing Co., Inc..

Dua, S. and Du, X., 2011. Classical machine-learning paradigms for data mining. *Data Mining and Machine Learning in Cybersecurity*, pp.23-56.

Brij Bhooshian Gupta, Quan Z. Sheng, Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices, 2019

## Self-Assessment Exercises

### Exercise 1.1

You are opening an online store in a cloud environment. What are three security controls you might use to protect customers' credit card information? Assume that the information will need to be stored.

### Exercise 1.2

Humans are said to be the weakest link in any security system. Give an example for each of the following:

- a) a situation in which human failure could lead to a compromise of encrypted data

- b) a situation in which human failure could lead to a compromise of identification and authentication
- c) a situation in which human failure could lead to a compromise of access control

### **Recommended time for the student to work**

15 hours

# SOCIAL BIG DATA APPLICATIONS

2<sup>nd</sup> Week

## Summary

Before discussing the applications of social media, the differences between social media and generic Web (i.e., surface Web, but not deep Web) will be discussed by focusing on the natures of the respective users. As discussed below, the types of user interactions with the systems are very different in the generic Web and social media. In generic Web and social media, the types of data that can be used in the analysis also differ depending on the differences of the types of such interactions.

## Introductory Remarks

### *Differences between Generic Web and Social Media as Subjects of Analysis*

First, the interactions in generic Web are considered. The users of generic Web are roughly classified into end users and site administrators. Creation, modification, and deletion as to the contents (i.e., pages and links) are explicitly done by the administrator on the generic Web. On the other hand, the end user interactions are mainly browsing the Web pages and the users' click streams are recorded in the Web site as user access histories. Indeed, in some sites other actions such as input of search terms can be done through some kinds of forms. However, the Web sites that demand the user accounts or allow the users to query the backend databases are the deep Web, not the surface Web. In a word, the end users are anonymous because they cannot be identified only from the IP address. Therefore, pages and links inside and outside the sites as explicit relationships and the users' click streams as implicit relationships are important as the subject of the analysis on the generic Web. Only the site administrator can use the access histories basically.

On the other hand, there exist explicit users who can be identified by the account names in addition to the administrators in social media. The profiles of the users can also be accessed by other users. The users can perform various interactions with social media sites, which include browsing and creation of social data. Primary contents such as articles and photos, secondary contents for the primary contents such as tags or evaluations, and access histories as results of

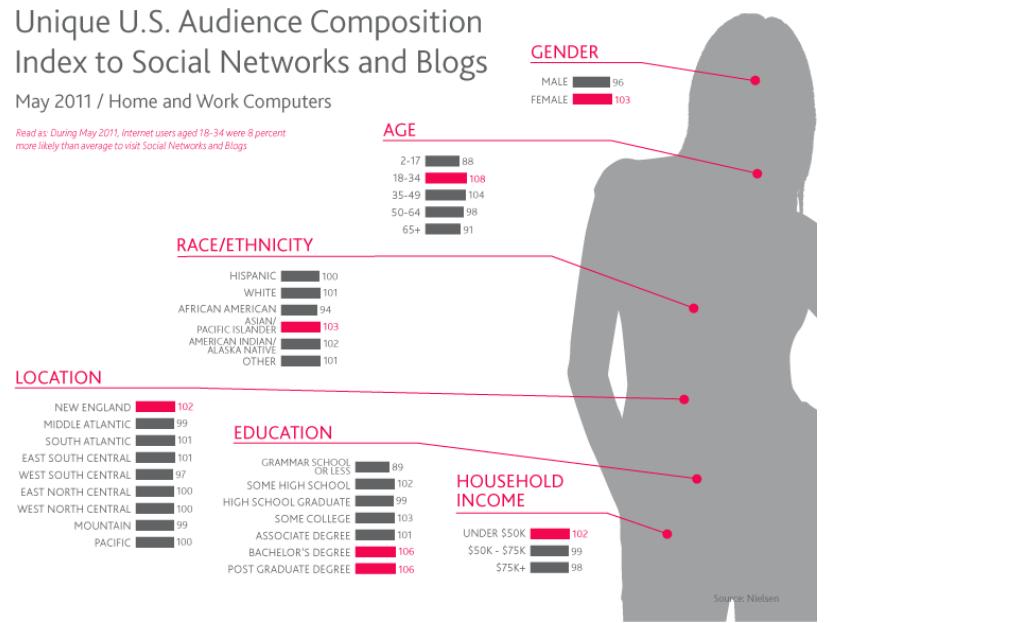
such interactions constitute social data. In course of time, the relationships between the users, those between the intra-site contents, those between the inter-site contents, and those between the users and contents are created. In addition to the contents directly or indirectly created by the users, the diverse histories and relationships created in this way are important subjects of analysis in social media. Social media are different from generic Web in that most of these data are available through the Web services API provided by social media sites.

### *Classification of Social Media Applications based on the Purposes*

Referring to a book on social data mining [Graubner-Mueller 2011], this section will explain promising business fields based on analysis of social media including the applications described above. As each step of business processes can be considered to correspond to a specific purpose, applications will be enumerated for each purpose. In general, needless to say, business applications are not contrary to individual interests. Rather, such applications are also useful to customers through providing improved services and products in many cases. In addition, in consideration of usefulness, applications using the generic Web will also be included for reference.

#### *(1) Research and development*

- *Trend scouting:* A trend survey about a certain known topic which the users frequently describe in social media as well as latent topics with potential values is conducted in order to explore the business environments surrounding development of new products.
- *Consumer behavior analysis:* Investigation of consumer needs, wishes, attitudes, and motives is conducted as to products, product categories, and brands. Since the users' opinions about products, product categories, and brands at large are described in social media irrespective of whether they purchase the products or not, this analysis is useful both for improvement of existing products and development of completely new products which fulfill potential needs.

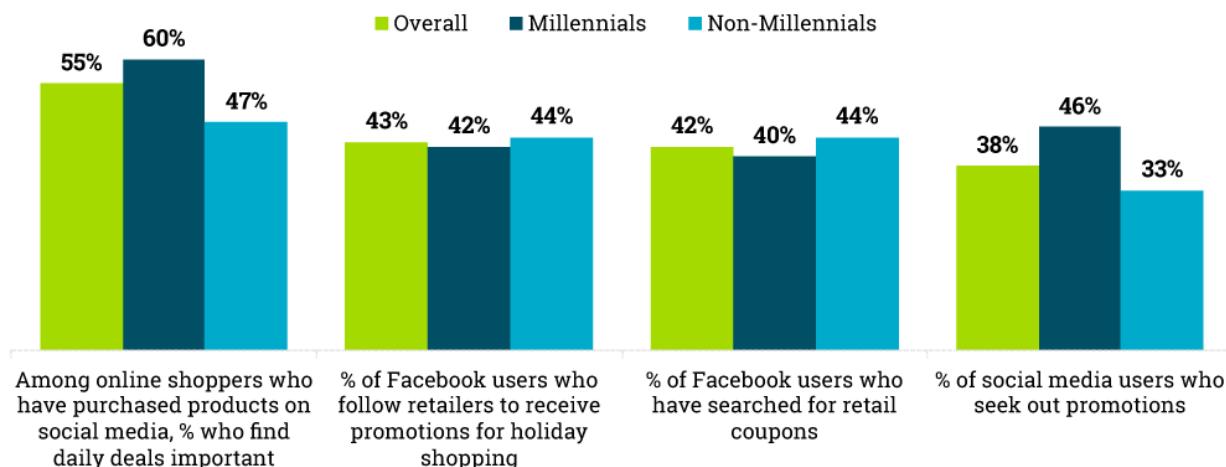


- *Technology Intelligence:* When a company intends to innovate some product, the company conducts a trend survey on related technologies against specialized technical information repositories on the Web such as patent databases and digital libraries. This is equivalent to investigation of researches by preceding rivals or that of exploratory researches with potential values in research and development of products.

## (2) Marketing and sales

- *Product and brand image analysis:* The reputations, sentiments, and opinions about concrete products and brands are analyzed. Indeed, these can be known by conducting a post-purchase survey to users who purchased products. However, since not only the motives and related comments of users who actually purchased the products but also the reasons and opinions of users who thought to purchase the products but did not in reality are described in social media data, analysis of such data is useful for strengthening and changing the current sales strategy.
- *Campaign evaluation:* Some campaigns performed towards users are described by the users in social media data according to the impacts. By analyzing such social data, the effectiveness of marketing can be measured or optimized.
- *Community and opinion leader discovery:* If a community related to a certain product on social media can be discovered, it will be a target of promotion of the product. Moreover, if opinion leaders with large influence in the community can be discovered, it is possible to influence other customers by using channels including the detected opinion leaders in marketing.

## Online Shoppers' Use of Social Media for Retail Promotions



Published on MarketingCharts.com in October 2017 | Data Source: UPS / comScore

Based on a survey of more than 5,189 qualified comScore panelists who made at least two online purchases in a typical three-month period

### (3) Distribution

- Site and location planning:* Most of information about a certain area as well as customers and rivals within the area has already been published by geographic information services on the Web. On the other hand, reputations about the area or rivals may be described by social media data. By combining such pieces of information, it is possible to accurately choose promising places for opening-a-shop of the company.

### (4) Customer services

- Product recommendation:* Data such as sales histories of a certain commercial product are stored in in-house databases. On the other hand, the ranks and reputations about the product and its relationships with other products are described in social media data. Unifying such data for recommending the product can raise the conversion ratio of the customer as to the product.
- Customer feedback analysis:* Formal customer feedback is obtained by conducting questionnaires to the users who actually purchased the product. Some dissatisfaction, improvement suggestions, and unexpected uses are described as social data, which can be considered as informal customer feedback. Analyzing such feedback can help to improve the product.

### (5) Procurement

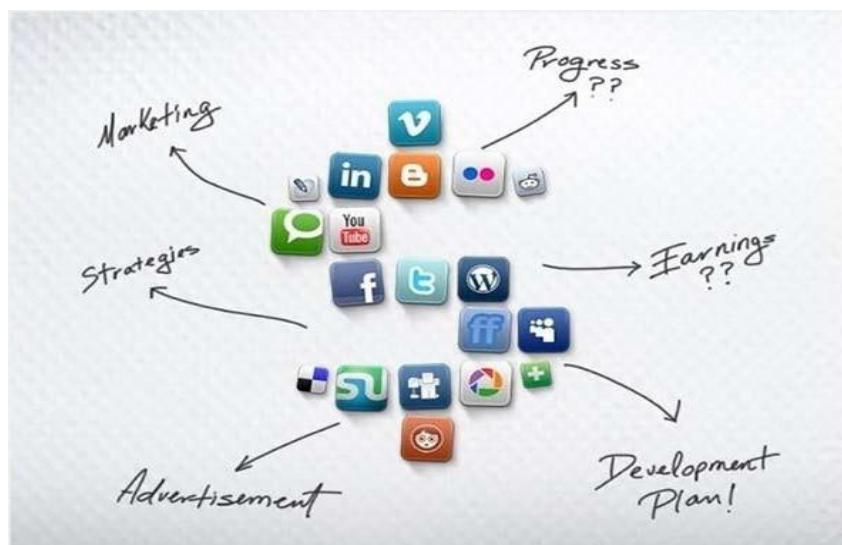
- *Content acquisition*: Data in the same categories, such as products, services, and news, spanning over two or more sites are extracted by using Web Service API of each site and aggregated into the unified results.
- *Supplier and price monitoring*: Two or more sites are monitored in an integrated manner so as to compare the suppliers and prices of components for effective supply.

#### (6) Risk and public relation management

- *Investor sentiment analysis*: It is possible to collect and analyze investors' sentiments as to a specific company through analysis of social media data.
- *Fraud detection*: It is expected that issues that pose a risk to a company such as copyright infringement are uncovered by monitoring file sharing related sites such as BitTorrent sites.
- *Media intelligence*: Collection and analysis of mainstream news of a specific company in generic Web sites and social news and rumors about the company in social media are conducted for customer relationship management. In particular, if bad reputations about the company are discovered in social media in the early stage, they can be used for taking measures so that the situation may not become very serious.

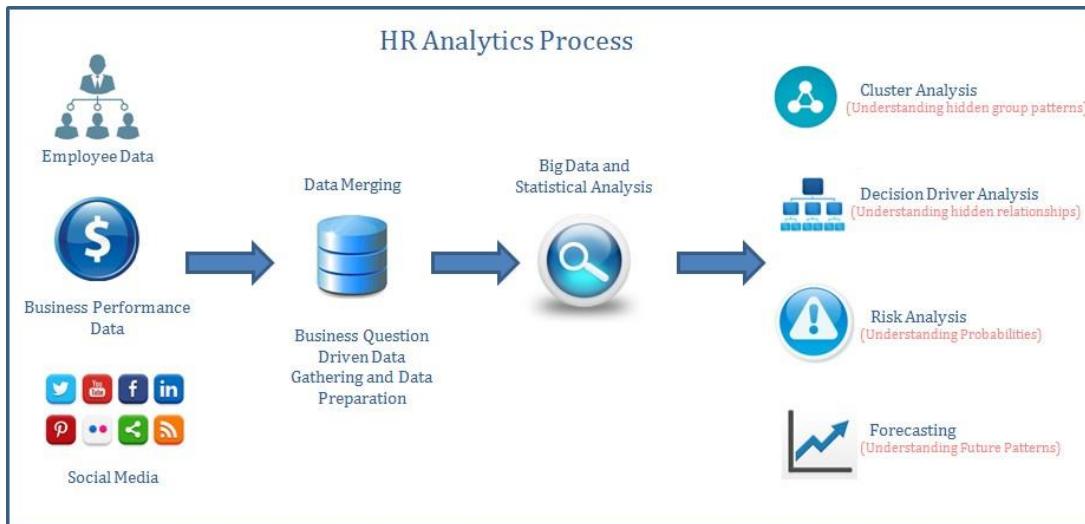
#### (7) Strategic management

- *Competitive and stakeholder analysis*: For surveillance and analysis of competitors and stakeholders, investigation and analysis are conducted based on data such as management information and news which are published on the official sites and other Web sites.



#### (8) Human resource management

- *Employer reputation*: The reputation of a company as an employer is investigated based on analysis of social media.
- *Labor market intelligence*: Based on analysis of data on recruitment sites, the labor market relevant to a company is investigated.



## Aim/Objectives

In this week we explore web data mining and social big data mining, pointing out security aspects of both. Data mining is closely related to the concept of big data, which involves the collection of massive amounts of data, often not intended to be databases or structured as such and we see the classification of social media applications based on their purpose. The emphasis is on the term “big,” for example, the set of all index entries for search engines.

## Learning Outcomes

By the end of this chapter, students should be able to:

- understand the current challenges in processing big data
- be aware of the technologies available for handling big data
- understand how big data are generated in different industries
- understand the ideas behind data mining methods targeted for big data

## Key Words

Social media analytics	Web site analytics	Technology intelligence
------------------------	--------------------	-------------------------

## Annotated Bibliography

### Required Materials

To achieve the educational needs of this unit the following material is used:

#### Primary Material

Graubner-Müller, A., 2011. Web Mining in Social Media: Use Cases, Business Value, and Algorithmic Approaches for Corporate Intelligence (No. 3). BoD–Books on Demand.

This book is on social data mining and this section explains promising business fields based on analysis of social media.

#### Supportive material

Katal, A., Wazid, M. and Goudar, R.H., 2013, August. Big data: issues, challenges, tools and good practices. In Contemporary Computing (IC3), 2013 Sixth International Conference on (pp. 404-409). IEEE.

Zeng, D., Chen, H., Lusch, R. and Li, S.H., 2010. Social media analytics and intelligence. IEEE Intelligent Systems, 25(6), pp.13-16.

Russell, M.A., 2013. Mining the Social Web: Data Mining Facebook, Twitter, LinkedIn, Google+, GitHub, and More. " O'Reilly Media, Inc. ".

Brij Bhooshian Gupta, Quan Z. Sheng, Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices, 2019

## Self-Assessment Exercises

### Exercise 2.1

Sketching Your Data Double:

In this brief personal essay (300 words), students will identify a data-intensive online service they regularly use (i.e., Facebook, Google, reddit, etc...) and describe how the site “sees” them, that is, students should offer a description of who or what the site “thinks” they are like.

## Recommended time for the student to work

15 hours

# BIG CONCEPTS IN DATA MINING

3<sup>rd</sup> Week

## Summary

Data mining is, in a nutshell, to discover frequent patterns and meaningful structures appearing in a large amount of data used by applications.

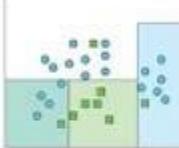
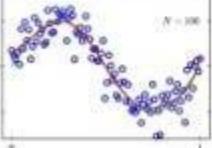
## Introductory Remarks

One of the basic techniques for data mining is association rule mining, also known as association analysis. It is to discover frequent co-occurrences between structured data used in business applications, which are usually managed by database management systems (DBMS) such as relational database systems. An algorithm called *Apriori* is used in many cases for that purpose. Association rules are made from frequent combinations of items discovered by the algorithm. Based on association rules, a lot of application systems recommend a set of items by revising arrangements of them. Association rule mining is extended and applied to the history of product purchases and the history of click streams on the Web pages in order to discover the frequent patterns of series data. Mining historical data is called historical data mining in particular.

On the other hand, a classifier is learned based on data whose classes (i.e., categories) are known in advance. Then, if there is new data, classes to which they should belong are determined by using the learned classifier. This task called *classification* is one of the basic data mining techniques. Naïve Bayes and decision trees are used as typical classifiers. Classification is used by such a variety of applications as determination of promising customers, detection of spam e-mails and determination of categories of new specimens in science or medicine. Determination of continuous values such as temperatures and stock prices is also called prediction of future values. *Prediction* requires methods such as regression analysis as a basic approach or multivariate analysis as a more advanced approach. Indeed, these analytical approaches have been developed more or less independently from data mining. However, they are considered a kind of extensions of data mining and will be described as one of the key technologies for social big data mining. Based on a combination of two or more existing classifiers, ensemble learning creates a more accurate classifier than each of the original ones. It may be possible to define the

degrees of *similarity* between data even if the categories of the data are not known in advance. The opposite concept of similarity is *dissimilarity* or distance. Based on the defined similarity, grouping data into the same group which are similar to each other in a collection of data is called cluster analysis or clustering, which is also one of the basic technologies of data mining. Unlike classification, *clustering* doesn't demand that the names and characteristics of clusters are known in advance. Techniques such as a hierarchical agglomerative method and a nonhierarchical  $k$ -means method are often used for clustering. Promising applications of clustering include discovery of groups of similar customers for marketing.

## Data mining methods

Predictive methods	Descriptive methods
<b>Classification</b>  Learns a method for predicting the instance class from pre-labeled (classified) instances	<b>Clustering</b>  Finds "natural" grouping of instances given un-labeled data
<b>Regression</b>  An attempt to predict a continuous attribute	<b>Association Rules</b>  Method for discovering interesting relations between variables in large DBs

A data mining task which can detect exceptional values or values different from standard values is called *outlier detection*. There are methods for outlier detection based on statistical models, data distances, and data densities. There are alternative ways to find outliers using clustering and classification. Outlier detection has been used for applications, such as detection of credit card frauds or network intrusions. A database is a mechanism for efficiently managing and accessing a large amount of data which social big data applications use. Descriptors for data structures, operations, and constraints dedicated to databases are collectively called a data model. Networks (or graphs) and hierarchical structures (or trees) have often been used as data models since the early days. The former and the latter are called a network data model and a hierarchical data model, respectively. Generally, based on the analysis of textual contents of documents,

classification and clustering of documents can be performed. Such technologies are collectively called text mining or more generally contents mining. On the other hand, analysis of link structures of Web pages is called structure mining or link mining.

With regards to the processing performance of big data, there is another issue called high dimensionality in addition to scalability. In some cases data mining represent target data as objects with many attributes or vectors of many dimensions.

What data mining considers as emergent issues is not confined to the increase in the size of data or number of dimensions. The complexity of data structures to treat also becomes a problem along with the wide spread of the application fields of big data. Although conventional data mining has mainly targeted structured data, an opportunity to treat graphs or networks (e.g., Web) and semi-structured data (i.e., XML) is increasing along with the development of the Internet. Moreover, the data produced every moment from sensor networks are essentially time series data and positional information is added to time series data if GPS (Global Positioning System) is used. It can be considered that Tweets (i.e., articles in Twitter) are also a kind of time series data. Unstructured multimedia data such as photos, videos, and sounds are also the target of data mining. Furthermore, in a case where the target data of data mining are distributed, issues such as communication costs, data integration, and security are also caused.

As mentioned above, the main tasks of data mining include the following:

- Association rule mining
- Clustering
- Classification and prediction
- Outlier detection

The relations among data mining, database systems, information retrieval, and Web search have already been explained.

Data mining can be positioned in the context of broader technologies *called knowledge discovery in database (KDD)*. Thus data mining is one of the essential steps in the process of knowledge discovery. In addition, KDD is not a one-way process but is usually accompanied by feedback loops to any prior step based on the so far acquired knowledge.

## Aim/Objectives

This chapter describes basic concepts in data mining, typical tasks for data mining, and basic data structures as targets of data mining. Here the relationships between data mining and its peripheral technologies will be summarized in order to better understand the features of data mining.

## Learning Outcomes

At the end of this chapter, students will be able to:

- describe the main tasks of data mining
- comprehend the knowledge discovery in databases.

## Key Words

<i>Apriori</i> algorithm	Association rule mining	Classification and prediction
Clustering	Degrees of similarity	Knowledge discovery in database (KDD)
Outlier detection	Big data mining	

## Annotated Bibliography

### Required Materials

To achieve the educational needs of this unit the following material is used:

#### Primary Material

Chapter 5 of Ishikawa, H., 2015. *Social big data mining*. CRC Press.

This chapter describes basic concepts in data mining, typical tasks for data mining, and basic data structures as targets of data mining.

## **Supportive material**

Wu, X., Zhu, X., Wu, G.Q. and Ding, W., 2014. Data mining with big data. IEEE transactions on knowledge and data engineering, 26(1), pp.97-107.

Fan, W. and Bifet, A., 2013. Mining big data: current status, and forecast to the future. ACM SIGKDD Explorations Newsletter, 14(2), pp.1-5.

Clarence Chio, David Freeman, Machine Learning and Security: Protecting Systems with Data and Algorithms, 2018

Tan, P.N., 2007. Introduction to data mining. Pearson Education India.

## **Self-Assessment Exercises**

### **Exercise 3.1**

Give an application example where global outliers, contextual outliers, and collective outliers are all interesting. What are the attributes, and what are the contextual and behavioral attributes? How is the relationship among objects modeled in collective outlier detection?

## **Recommended time for the student to work**

15 hours

# CLASSICAL MACHINE – LEARNING PARADIGMS FOR DATA MINING

4<sup>th</sup> Week

## Summary

Data mining flourishes because the information influx in ubiquitous applications calls for data management, pattern recognition and classification, and knowledge discovery. Cyberinfrastructures generate peta-scale data sets for daily monitoring and pattern profiling in cybersecurity models. To facilitate the application of datamining techniques in cybersecurity protection systems, we comprehensively study the classic data-mining and machine-learning paradigms. Machine learning is the computational process of automatically inferring and generalizing a learning model from sample data. Learning models use statistical functions or rules to describe the dependences among data and causalities and correlations between input and output.

## Introductory Remarks

Machine learning for data-mining applications in cybersecurity face challenges due to the amount and complexity of growing data in cyberinfrastructures. Intrusions (e.g., network anomalies) are moving targets and are difficult to detect precisely and in a predefined way. Meanwhile, large false alarms make analysis overwhelming due to the lack of labels for intrusion.

### *Challenges in Data Mining*

The challenges are classified into four areas for data-mining applications in cybersecurity: modelling large-scale networks, intrusion discovery, network dynamics, and privacy preserving in data mining.

### *Modelling Large-Scale Networks*

Modelling a cyberinfrastructure is challenging, as many common graph measures are difficult to compute for the underlying networks. It is difficult to build the explanatory model of networks due to the requirements for accurate learning and prediction: Realistic networks at different scales are simulated for testing algorithms for defense, and anomalies that do not conform to the model and potentially represent an intrusion or other network problem are detected.

A network model can be extracted partially and amenably for advanced analysis, and a network can be built in a real-world, meaningful way but may not follow the assumption of iid random variables. Moreover, challenges exist in the computation of graphic measures in the network model. Examples of these graphic models have the dynamic network of telecommunications, e-mail communication networks through which viruses spread, and the network of hyperlinks between Web sites. One example of a graphic measure is the graph diameter, i.e., the greatest distance between two nodes in a graph. The computation difficulties call for a data-mining model that discovers the nature of real data using a simpler model.

#### *Discovery of Threats*

Data-mining cyberinfrastructure for the discovery of threats suffers from the sheer volume and heterogeneous network data, the dynamic change of threats, and the severe imbalanced classes of normal and anomalous behaviors. The above challenges call for the methods that can aggregate information dynamically and locally and across the networks to detect complex multistage attacks and predict potential and rare threats based on the behavior analysis of network event data. The most employed methods for detecting malicious code or behavior use rule-based or statistical models to identify threats in real-time, using adaptive threat detection with temporal data modelling and missing data. The sampling of big-scale network data has to be adaptive to the uncertainty of physical changes of networks, malicious code, and malicious behavior. Adaptive and dynamic modelling is necessary for the temporally evolving data structure and features.

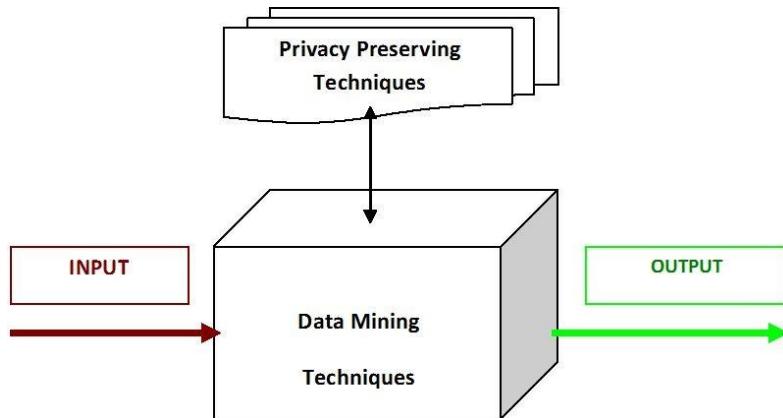
#### *Network Dynamics and Cyber Attacks*

Many cyber attacks spread malware to vulnerable computers. Due to the conditions triggering the malware, the malware may infect computers in a network in varying degrees. Once the cyber defenders detect the malware, the spread of malware infections is investigated to build the protection system. Novel data-mining methods are necessary to predict future attacks by constantly evolving malware and launch defenses correspondingly. However, the detailed structure of the network is unknown, limiting the knowledge of infection evolution.

#### *Privacy Preservation in Data Mining*

Data-mining techniques are critical for discovering intrusions in cybersecurity systems. However, data mining can also be used maliciously in cyberinfrastructures to breach privacy. In principle, the more complete data is available for data mining, the more accurate the mining result that will be obtained. However, the comprehensive and accurate data may also raise privacy breach

issues. Furthermore, the data-mining result can potentially reveal private information. Privacy preserving data mining (PPDM) protects private data from being stolen or misused by malicious users, while allowing the other data to be extracted for use.



#### *Online Learning Methods for Dynamic Modelling of Network Data*

The most employed method for finding the temporal or sequential patterns of an audit data stream is to slide a window across the audit trace and determine whether the short sequence within the sliding window is anomalous or not. Sequences of the same window size are used in training and testing. The primary difficulty with using this method is selecting the appropriate window size for anomaly detection using a good learning method instead of trial-and-error. Information-theoretic measures have been proposed to describe the regularity of an audit data set and determine the best sliding window size based on the conditional entropy and information cost measures. However, a simple trained detector based on instance cannot be generalized, and the conditional entropy does not affect the appropriate window size. Consequently, a good learning method is needed to find the optimum window size for sequence learning in anomaly detection and dynamic modelling in network.

#### *Research Directions*

Many fundamental problems await solutions, and the complexity of cybersecurity problems present new research challenges in the domains of machine learning and data mining. The complexity of many learning problems in cybersecurity goes well beyond the capabilities of current machine-learning methods.

In the cybersecurity area, the machine-learning technologies that are being used are not adequate to handle challenges from the huge amount of dynamic and severely imbalanced network data.

Machine-learning technologies should be revolutionized so that their potential can be leveraged to address those challenges in cybersecurity.

#### *Understanding the Fundamental Problems of Machine-Learning Methods in Cybersecurity*

Most of the research efforts in machine-learning applications in cybersecurity focus on specific machine-learning algorithms and case studies; only a limited number of principal and consequence theories have been investigated.

#### *Incremental Learning in Cyberinfrastructures*

Theoretically, there is an inadequate understanding of the characteristics and normal behavior of an attack. Without this information, it is difficult to detect excursions from the norm. However, cyberinfrastructure contains a huge amount of data streaming continuously and dynamically. These data are required for incremental learning. Dynamic information challenges machine-learning modelling, whereas “time” adds important information for the understanding and learning of anomalies.

New machine-learning principles, methodologies, algorithms, and tools are required for such dynamic modelling to transform raw data into the useful information about their own normal and anomaly behaviors.

#### *Feature Selection/Extraction for Data with Evolving Characteristics*

Feature selection/extraction methods partially solve the problems that cybersecurity encounters with imbalanced data sets. However, the existing feature selection/extraction methods extract static information without perturbation. Cyberinfrastructure is characterized with a large amount of evolving dynamic information. This evolving information requires feature selection/extraction, not only to reduce the dimensionality for machine learning, but also to capture the evolving characteristics. To discover the evolving patterns in data, machine-learning methods have to be combined into feature selection. New machine-learning and feature selection techniques are required to identify continuous behavior in data.

#### *Privacy-Preserving Data Mining*

PPDM techniques address concerns that the broad use of data mining will threaten the privacy of individuals, industries, and even countries. Meanwhile, PPDM opens opportunities for data mining to protect private data from disclosure. The interaction between legally protected data and data mining has never been explored. PPDM is relatively new and has not been adopted in real-world applications. At this point, it is not clear how much or little private information data-mining methods

can disclose. Thus, machine-learning and data-mining methods should be fundamentally investigated to answer this question. Meanwhile, the developed PPDM methods need to be evaluated for researchers to determine how much privacy they can protect.

## Aim/Objectives

In this week, we introduce the fundamental concepts of machine learning. Since malicious behaviors occur either rarely or infrequently among cyberinfrastructures, classic machine-learning techniques must adopt machine-learning techniques to perform unbalanced learning accurately. We address several challenges that arise when we apply the classic data-mining and machine-learning methods to discovering cyberinfrastructures. Finally, we summarize the emerging research directions in machine learning for cybersecurity.

## Learning Outcomes

By the end of this week, students will be able to:

- Describe the fundamental concepts of machine learning
- Judge which machine learning technique is needed to perform unbalance learning
- Address several challenges arising from the classic data-mining and machine learning methods

## Key Words

Machine learning	Intrusion discovery	Privacy preservation
Incremental Learning	Privacy-Preserving Mining	Data

## Annotated Bibliography

### Required Materials

To achieve the educational needs of this unit the following material is used:

## **Primary Material**

Chapter 2 of Dua, S. and Du, X., 2016. Data mining and machine learning in cybersecurity. Auerbach Publications.

In this chapter, we find the fundamental background of machine learning and provided a brief overview of machine-learning formulations and methods for data mining in cybersecurity. It discusses challenging and critical problems that occur when machine-learning methods are applied in the huge amount of temporal and unbalanced network data.

## **Supportive material**

Witten, I.H., Frank, E., Hall, M.A. and Pal, C.J., 2016. *Data Mining: Practical machine learning tools and techniques*. Morgan Kaufmann.

Fawcett, T. and Provost, F.J., 1996, December. Combining Data Mining and Machine Learning for Effective User Profiling. In KDD (pp. 8-13).

Kochurov, M., Garipov, T., Podoprikhin, D., Molchanov, D., Ashukha, A. and Vetrov, D., 2018. Bayesian Incremental Learning for Deep Neural Networks. arXiv preprint arXiv:1802.07329.

Clarence Chio, David Freeman, Machine Learning and Security: Protecting Systems with Data and Algorithms, 2018

## **Self-Assessment Exercises**

### **Exercise 4.1**

Research the different algorithms existing for incremental machine learning and write a report of 2 pages max.

### **Recommended time for the student to work**

15 hours

## PRIVACY AND DATA MINING

5<sup>th</sup> Week

### Summary

Data mining has emerged as a significant technology for gaining knowledge from vast quantities of data. However, there has been growing concern that use of this technology is violating individual privacy. This has led to a backlash against the technology.

### Introductory Remarks

Does this mean that data mining (at least when used to develop generalized knowledge) does not pose a privacy risk? In practice, the answer is no. Perhaps the largest problem is not with data mining, but with the infrastructure used to support it. The more complete and accurate the data, the better the data mining results. The existence of complete, comprehensive, and accurate data sets raises privacy issues regardless of their intended use.

While much of the data is already accessible, the fact that data is distributed among multiple databases, each under different authority, makes obtaining data for misuse difficult. The same problem arises with building data warehouses for data mining. Even though the data mining itself may be benign, gaining access to the data warehouse to misuse the data is much easier than gaining access to all of the original sources. A second problem is with the results themselves. The census community has long recognized that publishing summaries of census data carries risks of violating privacy. Summary tables for a small census region may not identify an individual, but in combination (along with some knowledge about the individual, e.g., number of children and education level) it may be possible to isolate an individual and determine private information. There has been significant research showing how to release summary data without disclosing individual information. Data mining results represent a new type of "summary data"; ensuring privacy means showing that the results (e.g., a set of association rules or a classification model) do not inherently disclose individual information.

The data mining and information security communities have recently begun addressing these issues. Numerous techniques have been developed that address the first problem - avoiding the potential for misuse posed by an integrated data warehouse. In short, techniques that allow

mining when we aren't allowed to see the data. This work falls into two main categories: Data perturbation, and Secure Multiparty Computation. *Data perturbation* is based on the idea of not providing real data to the data miner - since the data isn't real, it shouldn't reveal private information. The data mining challenge is in how to obtain valid results from such data. The second category is based on separation of authority: Data is presumed to be controlled by different entities, and the goal is for those entities to cooperate to obtain valid data-mining results without disclosing their own data to others. The second problem, the potential for data mining results to reveal private information, has received less attention. This is largely because concepts of privacy are not well-defined - without a formal definition, it is hard to say if privacy has been violated. Despite the fact that this field is new, and that privacy is not yet fully defined, there are many applications where privacy-preserving data mining can be shown to provide useful knowledge while meeting accepted standards for protecting privacy. As an example, consider mining of supermarket transaction data. Most supermarkets now offer discount cards to consumers who are willing to have their purchases tracked. Generating association rules from such data is a commonly used data mining example, leading to insight into buyer behavior that can be used to redesign store layouts, develop retailing promotions, etc.



This data can also be shared with suppliers, supporting their product development and marketing efforts. Unless substantial demographic information is removed, this could pose a privacy risk. Even if sufficient information is removed and the data cannot be traced back to the consumer, there is still a risk to the supermarket. Utilizing information from multiple retailers, a supplier may be able to develop promotions that favor one retailer over another, or that enhance supplier revenue at the expense of the retailer. Instead, suppose that the retailers collaborate to produce globally valid association rules for the benefit of the supplier, without disclosing their own contribution to either the supplier or other retailers. This allows the supplier to improve product and marketing (benefiting all retailers), but does not provide the information needed to single out one retailer. Also notice that the individual data need not leave the retailer, solving the privacy problem raised by disclosing consumer data!

The goal of privacy-preserving data mining is to enable such win-win win situations: The knowledge present in the data is extracted for use, the individual's privacy is protected, and the data holder is protected against misuse or disclosure of the data.

There are numerous drivers leading to increased demand for both data mining and privacy. On the data mining front, increased data collection is providing greater opportunities for data analysis. At the same time, an increasingly competitive world raises the cost of failing to utilize data. At the same time, the costs of failing to protect privacy are increasing.

The goal of privacy-preserving data mining - analyzing data while limiting disclosure of that data - has numerous applications. A standard dictionary definition of privacy as it pertains to data is "freedom from unauthorized intrusion"<sup>1</sup>. With respect to privacy-preserving data mining, this does provide some insight. If users have given authorization to use the data for the particular data mining task, then there is no privacy issue. However, the second part is more difficult: If use is not authorized, what use constitutes "intrusion"? Common standard among most privacy laws (e.g., European Community privacy guidelines<sup>2</sup> or the U.S. healthcare laws<sup>3</sup>) is that privacy only applies to "individually identifiable data". Combining *intrusion* and *individually identifiable* leads to a standard to judge privacy-preserving data mining: A privacy-preserving data mining technique

---

<sup>1</sup> Merriam-Webster online dictionary.

<sup>2</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities*, No L(281):31-50, Oct. 24 1995.

<sup>3</sup> Standard for privacy of individually identifiable health information. *Federal Register*, 67(157):53181-53273, Aug. 14 2002.

must ensure that any information disclosed 1) cannot be traced to an individual; or 2) does not constitute an intrusion. Formal definitions for both these items are an open challenge. At one extreme, we could assume that any data that does not give us completely accurate knowledge about a specific individual meets these criteria. At the other extreme, any improvement in our knowledge about an individual could be considered an intrusion. The latter is particularly likely to cause a problem for data mining, as the goal is to improve our knowledge. Even though the target is often groups of individuals, knowing more about a group does increase our knowledge about individuals in the group. This means we need to *measure* both the knowledge gained and our ability to relate it to a particular individual, and determine if these exceed thresholds.

The U.S. Healthcare Information Portability and Accountability Act (HIPAA) defines *individually nonidentifiable data* as data "that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual"<sup>4</sup>. The regulation requires an analysis that the risk of identification of individuals is very small in any data disclosed, *alone or in combination with other reasonably available information*. A real example of this is given in<sup>5</sup>: Medical data was disclosed with name and address removed. Linking with publicly available voter registration records using birth date, gender, and postal code revealed the name and address corresponding to the (presumed anonymous) medical records. This raises a key point: Just because the individual is not identifiable in the data is not sufficient; joining the data with other sources must not enable identification.

One proposed approach to prevent this is *k-anonymity*. The basic idea behind *k-anonymity* is to group individuals so that any identification is only to a group of *k*, not to an individual. This requires the introduction of a notion of *quasi-identifier*: information that can be used to link a record to an individual. With respect to the HIPAA definition, a quasi-identifier would be anything that would be present in "reasonably available information". The disclosure problem is that combining this data with small cells in other tables (e.g., a table that reports salary by size of household, and a table reporting salary by racial characteristics) may reveal that only one possible salary is consistent with the numbers in all of the tables. Several methods are used to combat this. One is by introducing noise into the data; Other techniques include cell suppression, in which counts

---

<sup>4</sup> Standard for privacy of individually identifiable health information. Technical report, U.S. Department of Health and Human Services Office for Civil Rights, Aug. 2003.

<sup>5</sup> L. Sweeney, k-anonymity: a model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, (5):557-570, 2002.

smaller than a threshold are not reported at all; and generalization, where cells with small counts are merged.

Generalization and suppression are also used to achieve *k-anonymity*. How does this apply to privacy-preserving data mining? If we can ensure that disclosures from the data mining generalize to large enough groups of individuals, then the size of the group can be used as a metric for privacy protection. This is of particular interest with respect to data mining results: When does the result itself violate privacy? The "size of group" standard may be easily met for some techniques; e.g., pruning approaches for decision trees may already generalize outcomes that apply to only small groups and association rule support counts provide a clear group size.

An unsolved problem for privacy-preserving data mining is the cumulative effect of multiple disclosures. While building a single model may meet the standard, multiple data mining models in combination may enable deducing individual information. To violate privacy, disclosed information must both be linked to an individual, and constitute an intrusion. While it is possible to develop broad definitions for individually identifiable, it is much harder to state what constitutes an intrusion. Release of some types of data, such as date of birth, pose only a minor annoyance by themselves. But in conjunction with other information date of birth can be used for identity theft, an unquestionable intrusion. Determining intrusiveness must be evaluated independently for each domain, making general approaches difficult. What can be done is to measure the amount of information about a privacy sensitive attribute that is revealed to an adversary. As this is still an evolving area, we give only a brief description of several proposals rather than an indepth treatment. It is our feeling that measuring intrusiveness of disclosure is still an open problem for privacy-preserving data mining; readers interested in addressing this problem are urged to consult the papers referenced in the following overview.

#### *Protected from disclosure.*

Sometimes disclosure of certain data is specifically proscribed. We may find that *any* knowledge about that data is deemed too sensitive to reveal. For specific types of data mining, it may be possible to design techniques that limit ability to infer values from results, or even to control what results can be obtained.

### *Indirect disclosure.*

Techniques to analyze a classifier to determine if it discloses sensitive data were explored in<sup>6</sup>. Their work made the assumption that the disclosure was a "black box" classifier - the adversary could classify instances, but not look inside the classifier.

## Aim/Objectives

This chapter describes the foundations for privacy in regards to data mining on the Web. In particular, we discuss the problems in defining privacy and how privacy can be violated in data mining. Then, we describe the basis of PPDM including the historical roots, the definition of privacy preservation in data mining, and the general parameters that characterizes scenarios in PPDM.

## Learning Outcomes

By the end of this chapter students should be able to:

- Describe what PPDM is about
- Define misuse, disclosure and data perturbation

## Key Words

Misuse	Disclosure	Data perturbation
privacy-preserving data mining	k-anonymity	defines individually nonidentifiable data
quasi-identifier	intrusiveness	Generalization and suppression

---

<sup>6</sup> M. Kantarcioglu, J. Jin, and C. Clifton. When do data mining results violate privacy? In *Proceedings of the 2004 ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 599- 604, Seattle, WA, Aug. 22-25 2004.

## Annotated Bibliography

### Required Materials

To achieve the educational needs of this unit the following material is used:

#### Primary Material

Chapters 1 and 2 of Vaidya, J., Clifton, C.W. and Zhu, Y.M., 2006. *Privacy preserving data mining* (Vol. 19). Springer Science & Business Media.

These two chapters discuss a while perhaps too extreme - as a hypothetical example, would data mining of equipment failure to improve maintenance schedules violate privacy? – the concern is real. There is growing concern over information privacy in general, with accompanying standards and legislation. This is discussed in more detail in Chapter 2.

#### Supportive material

Vaidya, J. and Clifton, C., 2004. Privacy-preserving data mining: Why, how, and when. *IEEE Security & Privacy*, 2(6), pp.19-27.

Agrawal, R. and Srikant, R., 2000. *Privacy-preserving data mining* (Vol. 29, No. 2, pp. 439-450). ACM.

Lindell, Y. and Pinkas, B., 2000, August. Privacy preserving data mining. In Annual International Cryptology Conference(pp. 36-54). Springer, Berlin, Heidelberg.

## Activity (5 points)

Graded activity carrying 5% of the final grade. Suppose a telephone company-maintained records on every telephone call it handled, showing the calling phone number, the called phone number, and the time, date, and duration of the call. What uses might the telephone company make of those records? What uses might commercial marketers make? What uses might a rival telephone company make? What uses might a government make? Which of those uses violate individuals' privacy rights?

## Recommended time for the student to work

Estimated 20 hours

### Summary

In the previous chapters we have focused on data-mining and machine-learning applications and on techniques for profiling cyberinfrastructures to safeguard cyberspace against the attacks from anomalous users. Data mining, machine learning, and related statistical methods help researchers to learn and mine user patterns from the information collected in cyberspace. These statistical methods mine the user information, and detection ability protects the privacy and security of the cyber communities. Ironically, malicious users can employ these powerful data-mining and machine-learning techniques to learn or mine the confidential information of private sectors, corporations, and national departments. Instead of stealing vital personal information directly, our adversaries can deduce the private information from information available on public databases.

### Introductory Remarks

To preserve privacy, people generally ask that private records be used in one of three ways: without disclosure of any information, with disclosure of some information, with disclosure of modified information. In the above example, randomly swapped medical or voter data would have prevented Sweeney from deducing exact private information through the three features.

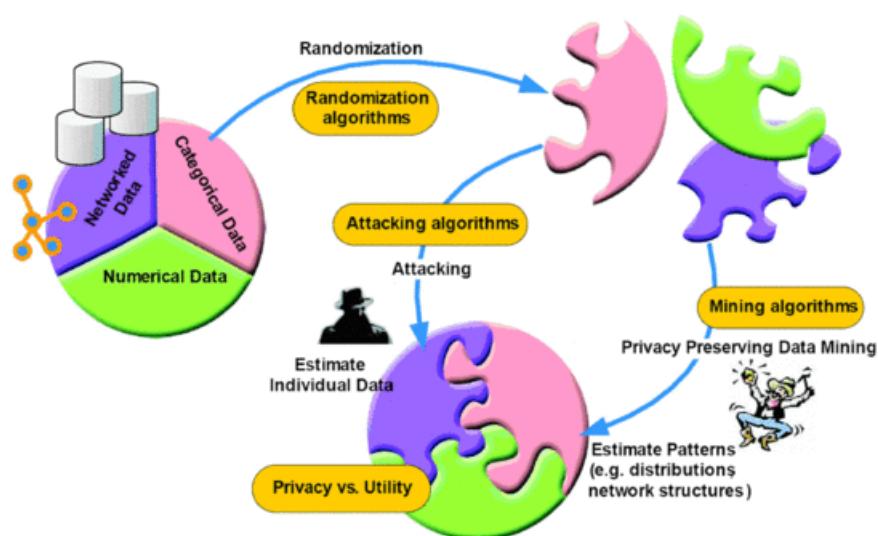
Preserving privacy is nearly ubiquitous in various informatics disciplines, including but not limited to bioinformatics, homeland security, and financial analysis. It influences cybersecurity significantly with the recent development of information collection and dissemination technologies. The unlimited explosion of new information through the Internet and other media have inaugurated a new era of research where data-mining algorithms should be considered from the viewpoint of privacy preservation, called privacy-preserving data mining (PPDM).

The ubiquitous applications of data-mining and machine-learning algorithms allow malicious users to employ data mining to obtain private information and, hence, raises the following questions: will data mining compromise privacy and should data mining be limited in some applications. This concern can be addressed from two aspects: ethical and technological.

Legitimate use of private data would benefit the data-mining users and private owners. Various countries have produced regulations and legislation to protect the data owners, control the dissemination of private data, and regulate the accuracy of a database. A variety of issues have to be involved in these semantic systems, such as the definition of privacy, the compromise level in data mining, the accurate boundaries between data users and data owners, the responsibility of data users, etc. An elaborative privacy protection regulation can prohibit the misuse of sensitive information and avoid intrusion of human rights. While regulations can protect private data from misuse, the technological solutions can proactively provide solutions to the application of various data-mining algorithms without compromising privacy.

## Scope

---



PPDM reduces unauthorized access of private information, while retaining the same functions as a normal data-mining method for discovering useful knowledge. Privacy-preserving methods generally alter the integrity of data, so that the generally employed data-mining methods cannot discover the same knowledge from the modified data as completely and correctly as from the original data. For example, scientists need private information from banks to mine for fraudulent activities.

### *Privacy Preservation in Data Mining*

The objective of PPDM is to prevent unauthorized users from accessing private information, such as private data-mining or machine-learning results. Privacy preservation and data mining worked in parallel, until Aggrawal et al. defined the specific research area in data mining concerning privacy protection in 2000. In PPDM, researchers adopt a large number of privacy preservation techniques in data-mining and machine-learning algorithms to preserve knowledge security. The complexity in PPDM algorithms raises several research topics other than privacy preservation and data mining. Verykios et al. (2004a) classified the existing PPDM techniques by considering five views: horizontal or vertical data distribution, data modification methods, data-mining algorithms, rule confusion, and privacy preservation.

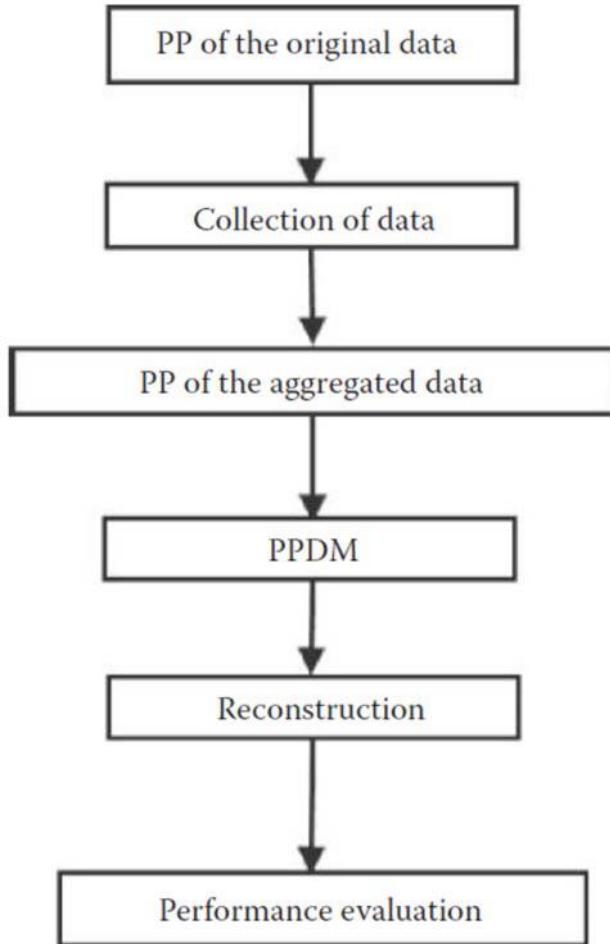
Most data distributions are horizontal or vertical.

Privacy is the designation of confidential information for entities (e.g., personal) that is not supposed to be publicly known. There is no exact definition of privacy for any entities due to the complicated categorization of information in different situations by different entities. Similarly, we can attribute privacy breaches to various causes, such as data mining, inference from the legitimate responses to database queries, disclosed data in cooperative computations and analysis, and the poor privacy preservation systems. To solve the above privacy violations, respective solutions include PPDM, privacy constraint processing, multilevel encryption, secure multiparty computation (SMC), and more advanced privacy protection.

According to the definition of privacy and possible causes of privacy leaks, we summarize two purposes for privacy preservation: to keep private information anonymous or to control valid information leaks. Valid information counters sensitive information that represents the entity privacy. The sensitive information can be obtained directly from available data sets or inferred indirectly from computational methods, such as data mining or machine learning.

As shown in Figure that follows, PPDM methods consist of six procedures: modification of the original data for privacy preservation, collection of data, modification of the aggregated data for privacy preservation, PPDM algorithms, reconstruction of the mining results for individual data points, and performance evaluation of the PPDM result. The modification of the original data points attempts to avoid the breach of sensitive information in the individual data points or the privacy violation of participants. In contrast to the commonly employed data-mining or machine learning methods, PPDM requires the input to be modified. After collecting the data, the

aggregated data needs to be further processed so that the data source ID or other private information is blocked.



PPDM algorithms focus on the privacy problems caused by data-mining results and methods. Researchers identified the use of unmodified data-mining and machine-learning methods as the primary cause of privacy leaks. In these classic data-mining and machine-learning methods, centralized data are required as input. As explained previously, malicious users violate the single data repository in a facile manner. The solutions to this problem include hiding all of the sensitive information in the data and distributing the data for computation, e.g., SMC. The former solution removes detailed information from the original data and reduces the completeness of input. The latter solution poses new challenges, such as how to reduce the computation and communication

cost caused by the information flow in the distributed network, and how to preserve sensitive information in the net flow.

Another privacy issue is the possibility of data-mining results inferring privacy. This problem occurs in secure multiparty computation (MPC) and SMC. In MPC, each participant holds one subset of the whole data set, and hides its sensitive information in the collaborative computation. Given an accurate data-mining result in SMC, a participant is able to infer the other participant's private information.

### *Performance Evaluation of PPDM Algorithms*

With the influx of a huge number of electronic data in corporations, researchers have studied a variety of PPDM algorithms extensively to sanitize the information involved. A unique performance criterion cannot measure all of the quality aspects of various PPDM algorithms. For example, the strong data perturbation can enable users to protect their privacy 100%, but may compromise the mining of the insensitive information. While the preliminary requirements vary among PPDM applications, a set of quality measures can guarantee the most appropriate selection of PPDM algorithms for miners. Broadly speaking, these PPDM-related metrics characterize information security, mining accuracy, and computation efficiency.

Information security includes the privacy hiding quality and transversal preservation. To measure privacy hiding ability, we identify the possible vulnerabilities in PPDM operations. We consider the sensitive information leaks at three levels: the uncertainty of original data privacy preservation, the disclosure of aggregated privacy, and the privacy violation of mining results. The uncertainty of privacy preservation in original data originates in the limitation of data modification or hidden approaches, such as the privacy preservation techniques.

### *Data-Mining and Machine-Learning Applications in PPDM*

The objective of PPDM is to keep private data and private knowledge safe once the mining on the data has been completed. PPDM methods can be analyzed from the perspectives of data distribution, data modification, data mining algorithms, data or rule hiding, or privacy preservation. We categorize the principle PPDM methods, according to data-mining algorithms and present their privacy preservation methods. In particular, the privacy preservation technique is the most important for the selective modification of the data, which are classified into three groups: heuristic-based techniques, cryptography-based techniques, and reconstruction-based techniques.

## **Anonymity networks**

An anonymous communication system is a peer-to-peer distributed application in which the nodes or participants are anonymous or pseudonymous. Anonymity of participants is usually achieved by special routing overlay networks that hide the physical location of each node from other participants.

Interest in anonymous P2P systems has increased in recent years for many reasons, ranging from the desire to share files without revealing one's network identity and risking litigation to distrust in governments, concerns over mass surveillance and data retention, and lawsuits against bloggers.

The ethical issues surrounding privacy, anonymity and mass-surveillance are complicated, with compelling arguments for and against, due in part to the fact that privacy and anonymity are desired by criminals and terrorists, not just individuals who care about their privacy.

## **Aim/Objectives**

In this chapter, we introduce PPDM. We discuss the privacy-preserving techniques in an extensive PPDM research area. We further analyze several PPDM applications and research studies to understand the details of the state-of-the-art methods for preserving privacy in data mining and machine learning. We have defined PPDM and explain related research topics, such as privacy-preserving techniques, multiparty computation (MPC), cryptography, and the performance evaluation of PPDM algorithms. We categorized privacy preserving and PPDM methods according to data modification methods. We outline the workflow of PPDM. We discuss the difference between general data-mining and machine-learning techniques, and PPDM to understand why privacy leaks occur in data-mining and machine learning applications. We analyzed several applications of PPDM in-depth and compare them to various machine-learning techniques, which face challenges of sensitive outputs. We will also briefly introduce other PPDM frameworks. We also discuss major anonymity networks and ethical consideration that these can raise.

## **Learning Outcomes**

By the end of this chapter, students should be able to:

- Analyse the PPDM applications in order to preserve privacy in data mining and machine learning

- Outline and categorize privacy preserving methods according to data modification methods.
- Apply their skills to identify and handle ethics issues

## Key Words

Preserving privacy	Unauthorized access	Privacy violations
multilevel encryption	Secure multiparty computation (SMC)	Data perturbation
Information Sensitivity	Anonymity networks	Ethics

## Annotated Bibliography

### Required Materials

To achieve the educational needs of this unit the following material is used:

#### Primary Material

Chapter 8 of Dua, S. and Du, X., 2016. Data mining and machine learning in cybersecurity. Auerbach Publications.

This chapter discusses a number of data-mining and machine-learning algorithms have to be redesigned to address growing concerns with privacy protection. The chapter presents the applications of privacy preservation association rules, privacy preservation decision-tree model, privacy preservation KNN, privacy preservation  $k$ -means clustering, and privacy preservation BN. The privacy preservation concerns mostly concentrate on the reformation of original input data, the redesigning of the datamining algorithm for the hidden data source and for the prevention of information leakage during computation and communication of data sharing, and privacy preservation of the data-mining results.

#### Supportive material

Agrawal, R. and R. Srikant. Privacy-preserving data mining. In: *Proceedings of the ACM SIGMOD Conference on Management of Data*, Dallas, TX, 2000, pp. 439–450.

Aggarwal, C.C. and P.S. Yu. *Privacy-Preserving Data Mining: Models and Algorithms*. New York: Springer, 2008.

Verykios, V.S., E. Bertino, I.N Fovino, L.P. Provenza, Y. Saygin, and Y. Theodoridis. State-of-the-art in privacy preserving data mining. *ACM SIGMOD Record* 33 (1) (2004a): 50–57.

Verykios, V.S., A. Elmagamid, E. Bertino, Y. Saygin, and E. Dasseni. Association rule hiding. *IEEE Transactions on Knowledge and Data Engineering* 16 (4) (2004b): 434–447.

Aggarwal, C.C. and Yu, P., 2008. A general survey of privacy-preserving data mining models and algorithms. In Privacy-preserving data mining (pp. 11-52). Springer, Boston, MA.

Hamish Haughey, Gregory Epiphaniou, Haider M Al-Khateeb, Anonymity networks and the fragile cyber ecosystem, Network Security, Volume 2016, Issue 3.

## **Self-Assessment Exercises**

### **Exercise 6.1**

Describe a situation in which the source of information is more sensitive than the information itself. Explain why the sum of sensitive data might also be sensitive.

## **Recommended time for the student to work**

15 hours

# EMERGING CHALLENGES IN CYBERSECURITY

7<sup>th</sup> Week

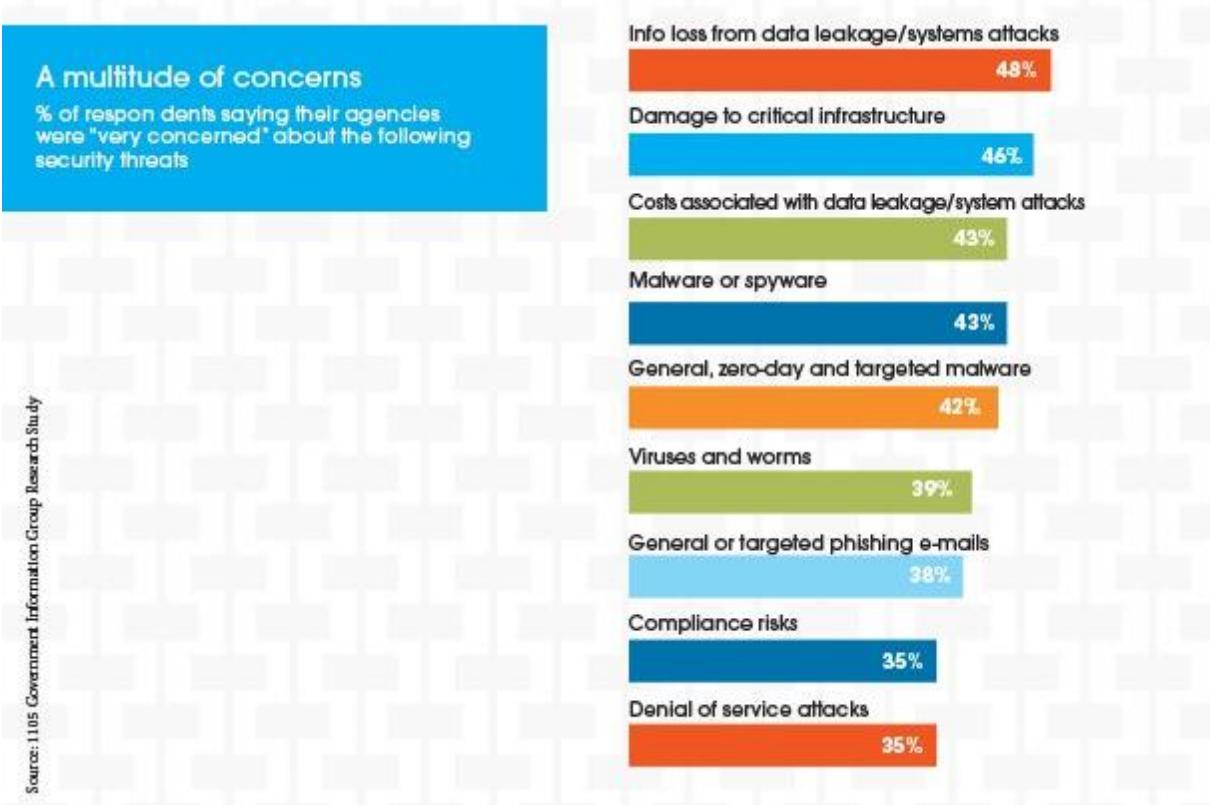
## Summary

Information technologies facilitate human activities, including communication, commerce, travel, study, work, voting, and policy dissemination. Cyberspace is no longer a place that exists on the fringe of society. We live in cyberspace, and it seems every activity has a paired terminology starting with e- or cyber-, such as cyber crime, cyber attack, cyber thieves, and e-commerce. As with our physical world, we benefit and suffer from activities conducted in cyberspace. Cyberinfrastructures may provide us with access to faster and more convenient modes of communication; likewise, we can suffer from cyber crimes and cyber warfare. In previous weeks, we have mentioned many cyber protection techniques to combat malicious cyber activities. However, we cannot cover all levels of cyber attacks and prevention, as the area is vast, complex, and constantly growing. To broaden readers' views of cyberspace in the years ahead, we summarize the emerging challenges in cybersecurity, focusing on cyber threats, network monitoring and privacy protection, and network intrusion detection.

## Introductory Remarks

### *Emerging Cyber Threats*

Mustaque et al. (2008) reported five emerging cyber threats that will challenge cybersecurity in the years ahead: malware, botnets, cyber warfare attacks, threats to mobile communication, and cyber crimes using various attack methods.



### *Threats from Malware*

Hackers use malware programs, such as phishing scams, to steal private information or for other malicious purposes. They deliver malware by leveraging the vulnerability of Web site structures, social network systems, and document transmissions that do not scan for such threats. With the widespread use of social network tools such as MySpace, MSN Messenger, and Facebook, social networking systems are becoming the dominant targets for malicious users. For example, MSN Messenger links users via the Internet, and video messages shared between MSN Messenger users can be convenient conduits for cyber attacks and malware. Taking advantage of the vulnerabilities of the computer systems, the malware will be able to track and record the user's keystrokes, spy on the user's browsing habits, alternate any browsing page to a phishing Web site, and send private information, such as a social security number, to an attacker. To repair the vulnerable points in the software, a number of software vendors provide patch-update versions of their software periodically.

### *Threats from Botnets*

Botnets are a group of bots, which make use of bots that attackers can run in groups using remote control systems. The master communicates with the bots to launch the botnet attack like an army.

The bots' mechanisms and their capabilities can be updated via this communication to evade intrusion detection.

One possible method of detecting botnets is to collect malware and track botnets so that the master and bots can be destroyed or blocked. However, this approach requires a system capable of understanding and responding to the request and command in a group of bot syntax. The growing and enriching features in the syntax, especially the incorporation of anti-detection techniques, exacerbate the difficulties of tracking the bot masters. The other solutions require monitoring the network systems and detecting the anomaly behavior of botnets through learning the patterns of network traffic flows. The biggest impediment to the accurate and efficient monitoring of network traffic lies in the huge amount of streaming data that must be processed.

#### *Threats from Cyber Warfare*

Cyber attacks are critical military actions. Instead of physically engaging in combat, attacks may come from cyberspace. The rapid development of digital information technologies makes national infrastructures, such as financial structures, utility transmission, and media communication, run efficiently in cyberspace. This dependence on cyberinfrastructures leaves a large number of vulnerabilities for cyber warriors to exploit for military activity. Cyber warfare has accompanied physical war in the past, and may come from sources that are not organized enough to fight a physical war. A recent example of cyber warfare occurred during the Russia/Georgia conflict of 2008.

Whereas traditional, physical warfare is expensive and closed to many members of a society, cyber warfare is inexpensive and is open to anyone who can launch a malicious program. Therefore, cyber defense against cyber attacks is an inevitable but challenging goal of military forces around the world. An efficient cyber defense requires collaboration between countries, states, institutions, and industrial societies, because cyber attacks can be launched through various routes at a large number of optional sites. The variety of attack options also discloses vulnerability in a cyber world that has no established rules of conduct. The lack of international cyber laws makes cyber defense challenging.

#### *Threats from Mobile Communication*

Researchers have put a great deal of effort in combating cyber attacks in terms of silent data types. They use silent signals to represent voices, images, and other media information. Mobile devices are linked to the Internet to facilitate everyday communications and activities, such as making purchases and checking bank balances. A variety of companies can provide services

through mobile networks, including the traditional mobile phone and Voice over Internet protocol (VoIP) infrastructures. The good calling quality and reliable service entices more companies to offer mobile services and attract more customers to use them. The investigations have shown that even financial transactions appear in mobile services. These services on mobile devices provide a number of opportunities for hackers to steal valuable information from the digital voice communication.

### *Cyber Crimes*

Cyber fraud, stealing, phishing, and other malicious behaviors are enriching the terminologies of cyber crimes in the years ahead. The term cyber crime does not have a set definition because of the evolution of cyberspace and its subsequent problems. For example, the constant evolution of cyberinfrastructures makes it difficult to identify and catch cyber criminals. Different jurisdictions define cyber crimes as they correlate to local situations. As we discussed above, ubiquitous cyber tools facilitate everyday life along with a large number of cyber services via computers, mobile devices, wireless networks, and so on. Cyber crimes refer to the malicious activities to block, read, or interfere with these services. The motivations of cyber criminals include gaining economic benefit, compromising cyberinfrastructure (e.g., in cyber warfare), and self-satisfaction. Undoubtedly, prosperous e-commerce or online business entices cyber criminals. Motivated by huge profits, cyber criminals can purchase malware tools from professional cyber experts and conduct economic crimes, such as gaining credit card and social security numbers, and electronic money laundering. The cooperation between the owners of cyber attack platforms and cyber criminals promotes malware delivery in networks. Vulnerabilities in the e-commerce or online services provide opportunities for cyber crimes in the economy. Combating cyber crimes requires more than updating patches for vulnerabilities. Many cyber crimes leave no detectable evidence, since cyber criminals can easily destroy evidence before being captured. Because of the lack of evidence, cyber police cannot quantify malicious behaviors. In some cases, cyber criminals have encryption and concealment tools to cover up their malicious activities. It is also challenging to aggregate corroborative evidence from the third parties in cyber crimes. Moreover, the borderless cyber world and its limited number of laws constrain the analysis and determination of cyber crimes. Thus, combating cyber crimes requires effort in two perspectives. First, uniform cyber laws need to be enacted. Second, advanced intrusion detection technology based on data-mining and machine-learning methods need to be developed to defend against criminals. While new laws can protect victims, computer and mobile phone users can also implement self-protection

methods. Furthermore, highly developed intrusion detection techniques can help cyber police detect crime evidence.

#### *Network Monitoring, Profiling, and Privacy Preservation*

In practice, attackers are interested in more than the data communicated between users. For example, attackers can learn an individual's or a group's intent when they observe the communication between parties. PP network traffic monitoring and profiling is emerging as a new research direction in cybersecurity. In this new research domain, monitoring and profiling programs attempt to collect traffic traces in the cyberinfrastructures to perform routine administration and operations and detect anomalous behavior in traffic flows. However, such programs are responsible for preserving the private information of network users in traffic flows. Thus, the PP processing has to take effect in the data collection process, of the monitoring and profiling of personal traffic flows, and the sensitive profiling results.

#### *Privacy Preservation of Original Data*

First, protection of private data by cryptographic, anonymous, and any other effective operation plays a preliminary but always effective role in privacy preservation. The earlier the users implement protective operations on the sensitive data, the less possible it is that attackers will breach user privacy.

Privacy-preservation methods are also specifically designed for different data types, e.g., the vertically and horizontally portioning of data sets in SMC. In literature, the proposed privacy preservation methods solve specific problems one-by-one, but maintain no preparation for the upcoming specific data breaching issues.

#### *Privacy Preservation in the Network Traffic Monitoring and Profiling Algorithms*

Second, we need to re-devise the monitoring and profiling programs for the privacy preservation data. As we showed in the application studies datamining and machine-learning methods are adapted to various privacy preservation data types, as a preprocessor of monitoring and profiling programs. How to extract the desired knowledge from the encrypted data poses the first challenge. Network traffic flows differentiate from normal PPDM data types in the dynamic streams and huge amount of influx. The scalability and computation requirements for the monitoring programs exacerbate the difficulty in designing applicable privacy preservation monitoring methods. As a new field, network traffic monitoring and profiling has challenging problems, such as the accuracy of mining, the coverage of profiling, and the scalability and

computation complexity in face of the huge and streaming network traffic flows. However, privacy preservation and PPDM remains a cybersecurity issue.

#### *Privacy Preservation of Monitoring and Profiling Data*

Third, we need privacy preservation algorithms to process the monitoring and profiling results of network traffic data. Similar to PPDM algorithms, original monitoring, and profiling rules, or learned models, indicate a correlation between users or hosts in the network. Sensitive rules or patterns have to be removed or hidden for privacy preservation. Network traffic monitoring and profiling poses a similar problem. The huge amount of traffic flows result in a large number of rules, and we must determine which of these rules are sensitive and how to identify and preserve them before reporting. To accurately monitor and profile cyberinfrastructures, the rules should be elucidative and representative.

For privacy preservation, the results should not disclose any informative clues for malicious users to know the rules and their correlations.

#### *Regulation, Laws, and Privacy Preservation*

The United States and European countries have acknowledged the protection of private data as a fundamental human right, whereas the emerging privacy breaches call forth the elaborate definitions and legislation specific for PPDM and privacy preservation network monitoring and tracking. The powerful data-mining and machine-learning techniques offer criminals not only the chance to invade private databases, but also the tools to discover the network user profiles. Hence, related regulation has to address the elaborate degree of network monitoring and profiling tools. Conversely, a reasonable elaboration of user behaviors supports network administrators in detecting malicious users.

An elaborate intrusion detection result can help police detect criminals and find evidence. The elaborate results may relate to the log history of criminals or other malicious users. This evidence collection raises two more privacy issues: how long the log records should be kept for users and how much information should be included in the records.

#### *Emerging Challenges in Intrusion Detection*

We have discussed a variety of data-mining and machine-learning techniques to improve intrusion detection and prevention. These techniques secure cyberinfrastructures ranging from specific applications to various scales of operating systems, such as host-based or network-based IDS. Researchers have formulated these systems in data-mining and machine-learning models, or in

other mathematical forms, based on specific assumptions on the anomalous data and normal data.

These assumptions have facilitated the formulation of intrusion detection problems with regard to the objective of detection and the constraints on the data description in the formulation.

Most commercial products contain signature-based detection techniques. These techniques work, because all malicious or misuse behaviors have been profiled in signatures in a set of features. Extracting or selecting the features among the given data set promotes signature matching. However, missing features or insufficient profiling can cause these techniques to miss unknown attacks. The likelihood of missing unknown attacks hampers the abilities of these techniques to combat the miscellaneous novelties of cyber attacks. Anomaly detection techniques, including hybrid systems involving signature-based techniques, have occupied the research domain of intrusion detection in the past years. These techniques assume that, given the profile of all normal behaviors in cyberinfrastructures, outlying behaviors are anomalous. Such profiling techniques statistically aggregate the normal data into feature subsets or data clusters, which enable the flexibility and adaptability of anomaly detection to novel attack paradigms. Unfortunately, such techniques depend on accurate and precise boundaries between normal and anomalous data points. The current machine-learning classification and clustering methods result in a high false-alarm rate when applied in anomaly detection systems. The high falsepositive rate hampers the application of anomaly detection techniques in real-world data sets. The high false- alarm rate can make an anomaly detection system ineffective.

When an IDS detects more false alarms than true attacks, the true attacks are easily lost. In worst-case scenarios, the detected alarms are all false instead of true attacks.

### *Privacy Issues in Network Anomaly Detection*

Privacy issues in network anomaly detection can be approached from two methodologies: the identification of useful encrypted traffic packets and/or the privacy preservation problems in distributed anomaly detection. Cryptography techniques have been applied in networks to solve privacy preservation problems, as well as randomization, permutation, and other data protection methods. Privacy protection processed data, such as encrypted traffic packets, prevent malicious users from accessing private information. The traditional anomaly detection techniques lack the ability to decrypt the encrypted packets. Since the traditional anomaly detection techniques cannot read these valuable encrypted packets, they will remove them and reduce the useful traffic

information for anomaly detection. A desired solution would be to maintain these data without compromising the detection ability of IDS.

## Aim/Objectives

This chapter contains an overview of emerging topics and recent cases in cybersecurity, such as botnet attacks, economic cyber crimes, privacy protection in cyber monitoring systems, cyber warfare, and intrusion detection for multilevel wireless communication systems. In this chapter, we first summarize the emerging threats in various attack methods. We present several privacy-preserving (PP) problems in cyber monitoring and profiling infrastructures, including PP data, PPDM, legislation, and PP traffic in networks. We present the challenges of using network intrusion detection systems (IDSs), which are caused by the fast aggregating network traffic flows. We highlight the difficulties in designing and validating efficient IDSs. We summarize the challenges ahead and recommend research directions for data-mining and machine-learning applications in cybersecurity.

## Learning Outcomes

By the end of this chapter, students should be able to:

- List the emerging topics and recent cases in cybersecurity
- List the emerging threats in different attack methods
- Identify the challenges of using IDSS as well as proper validation of efficient IDSs

## Key Words

Cyber threats	anomaly behavior	Cyber Warfare
Evidence	PP network traffic monitoring and profiling	Network Anomaly Detection

## Annotated Bibliography

### Required Materials

To achieve the educational needs of this unit the following material is used:

## **Primary Material**

Chapter 9 of Dua, S. and Du, X., 2016. Data mining and machine learning in cybersecurity. Auerbach Publications.

This chapter points out that we must consider cybersecurity and privacy-protection issues when we design and promote innovative tools in cyberspace. In the near future, new tools and legislation for privacy protection will significantly enhance the challenges and opportunities for data-mining and machine-learning techniques for cybersecurity.

## **Supportive material**

Ahamad, M., Amster, D., Barrett, M., Cross, T., Heron, G., Jackson, D., King, J., Lee, W., Naraine, R., Ollmann, G. and Ramsey, J., 2008. Emerging cyber threats report for 2009.

## **Self-Assessment Exercises**

### **Exercise 7.1**

Select one of the emerging topics analysed during this week and find a real case/ example. Discuss critical issues on the case you have selected as well as the proper reaction to respond to such a case. Write your answer in 2 pages max.

### **Recommended time for the student to work**

15 hours

# DATA MINING FOR THE INTERNET OF THINGS: LITERATURE REVIEW AND CHALLENGES

8<sup>th</sup> Week

## Summary

The Internet of Things (IoT) and its relevant technologies can seamlessly integrate classical networks with networked instruments and devices. IoT has been playing an essential role ever since it appeared, which covers from traditional equipment to general household objects and has been attracting the attention of researchers from academia, industry, and government in recent years.

## Introductory Remarks

There is a great vision that all things can be easily controlled and monitored, can be identified automatically by other things, can communicate with each other through internet, and can even make decisions by themselves. In order to make IoT smarter, lots of analysis technologies are introduced into IoT; one of the most valuable technologies is data mining. Data mining involves discovering novel, interesting, and potentially useful patterns from large data sets and applying algorithms to the extraction of hidden information. Many other terms are used for data mining, for example, knowledge discovery (mining) in databases (KDD), knowledge extraction, data/pattern analysis, data archaeology, data dredging, and information harvesting. The objective of any data mining process is to build an efficient predictive or descriptive model of a large amount of data that not only best fits or explains it, but is also able to generalize to new data. Based on a broad view of data mining functionality, data mining is the process of discovering interesting knowledge from large amounts of data stored in either databases, data warehouses, or other information repositories.

On the basis of the definition of data mining and the definition of data mining functions, a typical data mining process includes the following steps (see Figure 1).

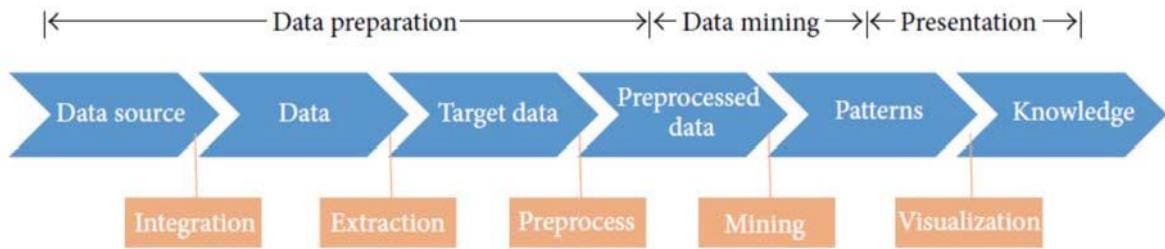


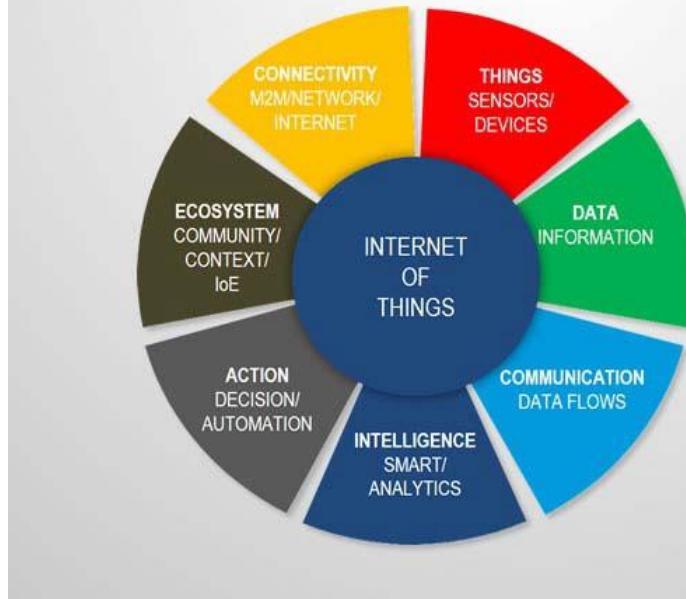
FIGURE 1: The data mining overview.

- (i) Data preparation: prepare the data for mining. It includes 3 substeps: integrate data in various data sources and clean the noise from data; extract some parts of data into data mining system; preprocess the data to facilitate the data mining.
- (ii) Data mining: apply algorithms to the data to find the patterns and evaluate patterns of discovered knowledge.
- (iii) Data presentation: visualize the data and represent mined knowledge to the user.

We can view data mining in a multidimensional view.

- (i) In knowledge view or data mining functions view, it includes characterization, discrimination, classification, clustering, association analysis, time series analysis, and outlier analysis.
- (ii) In utilized techniques view, it includes machine learning, statistics, pattern recognition, big data, support vector machine, rough set, neural networks, and evolutionary algorithms.
- (iii) In application view, it includes industry, telecommunication, banking, fraud analysis, biodata mining, stockmarket analysis, text mining, web mining, social network, and e-commerce.

## DEFINING IOT: 7 CHARACTERISTICS



### *Data Mining Functionalities*

Data mining functionalities include classification, clustering, association analysis, time series analysis, and outlier analysis.

- (i) Classification is the process of finding a set of models or functions that describe and distinguish data classes or concepts, for the purpose of predicting the class of objects whose class label is unknown.
- (ii) Clustering analyzes data objects without consulting a known class model.
- (iii) Association analysis is the discovery of association rules displaying attribute-value conditions that frequently occur together in a given set of data.
- (iv) Time series analysis comprises methods and techniques for analyzing time series data in order to extract meaningful statistics and other characteristics of the data.
- (v) Outlier analysis describes and models regularities or trends for objects whose behavior changes over time.

### *Data Mining Applications*

#### Data Mining in e-Commerce.

Data mining enables the businesses to understand the patterns hidden inside past purchase transactions, thus helping in planning and launching new marketing campaigns in prompt and

cost-effective way. e-commerce is one of the most prospective domains for data mining because data records, including customer data, product data, users' action log data, are plentiful; IT team has enriched datamining skill and return on investment can be measured. Researchers leverage association analysis and clustering to provide the insight of what product combinations were purchased; it encourages customers to purchase related products that they may have been missed or overlooked. Users' behaviors are monitored and analyzed to find similarities and patterns in Web surfing behavior so that theWeb can be more successful in meeting user needs.

#### Data Mining in Industry.

Datamining can highly benefit industries such as retail, banking, and telecommunications; classification and clustering can be applied to this area. One of the key success factors of insurance organizations and banks is the assessment of borrowers' creditworthiness in advance during the credit evaluation process. Credit scoring becomes more and more important and several data mining methods are applied for credit scoring problem. Retailers collect customer information, related transactions information, and product information to significantly improve accuracy of product demand forecasting, assortment optimization, product recommendation, and ranking across retailers and manufacturers.

#### Data Mining in Health Care.

In health care, data mining is becoming increasingly popular, if not increasingly essential. Heterogeneous medical data have been generated in various health care organizations, including payers, medicine providers, pharmaceuticals information, prescription information, doctor's notes, or clinical records produced day by day. These quantitative data can be used to do clinical text mining, predictive modelling, survival analysis, patient similarity analysis, and clustering, to improve care treatment and reduce waste. In health care area, association analysis, clustering, and outlier analysis can be applied.

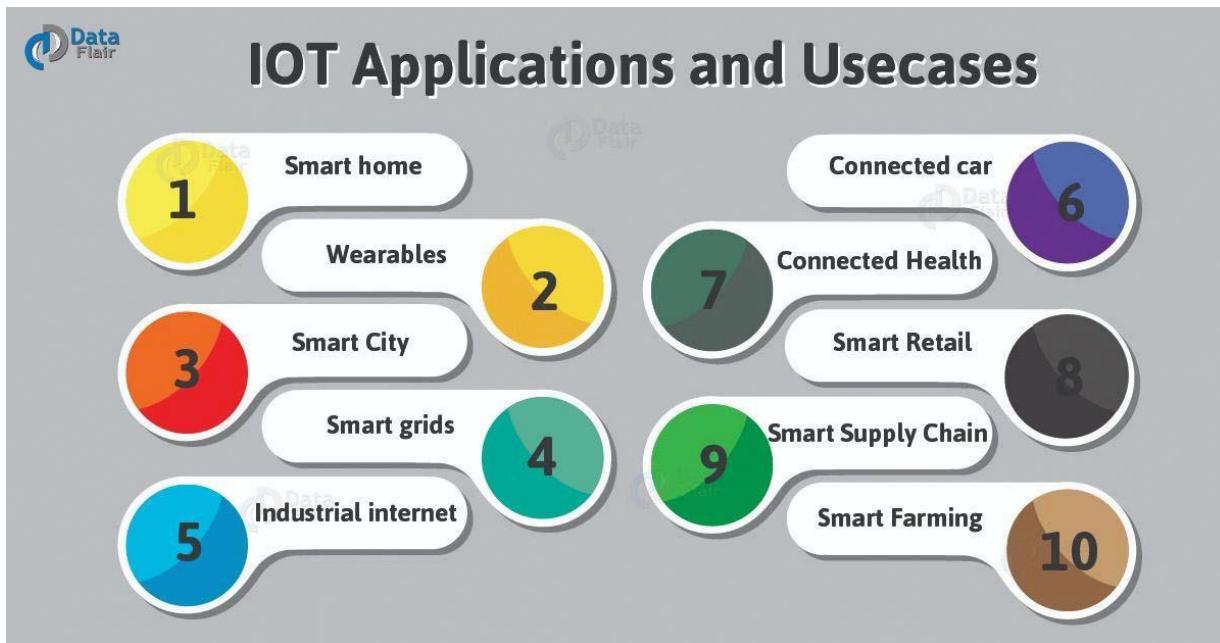
#### Data Mining in City Governance.

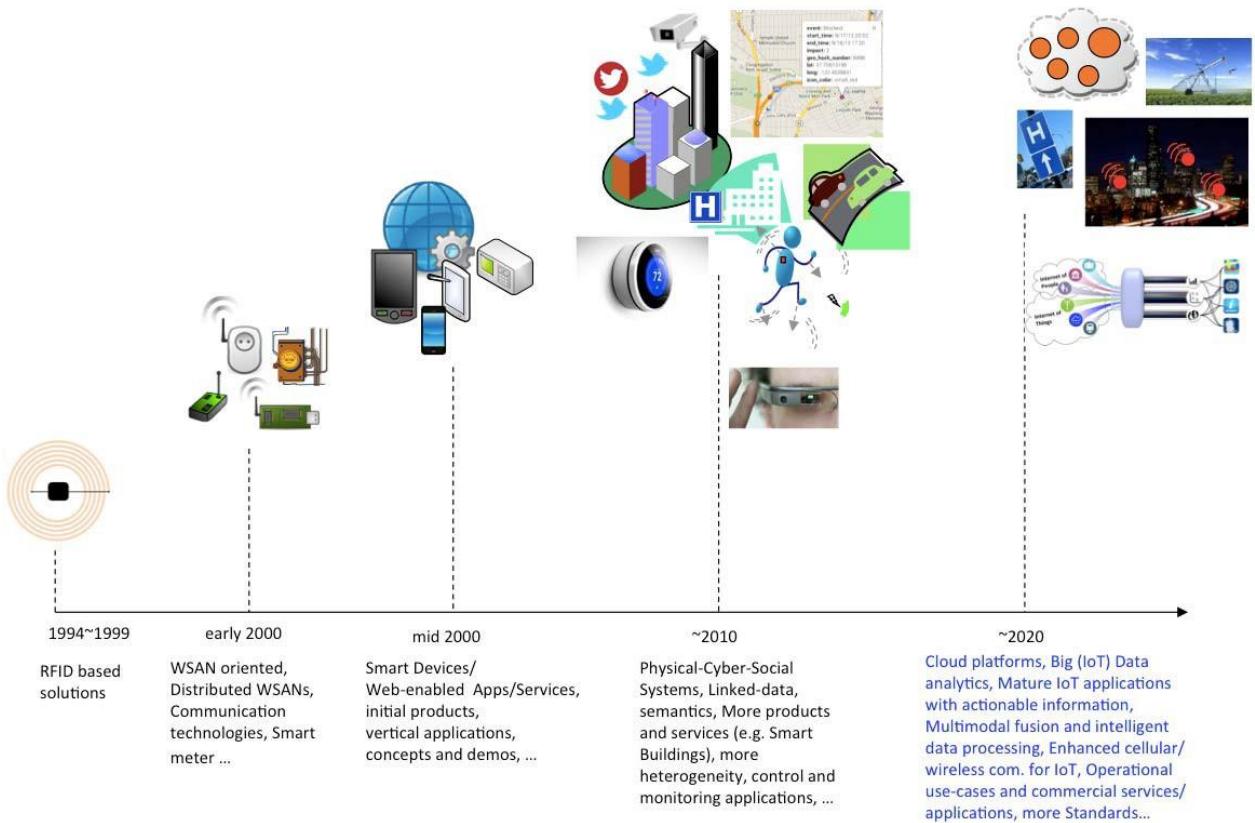
In public service area, data mining can be used to discover public needs and improve service performance, decision making with automated systems to decrease risks, classification, clustering, and time series analysis which can be developed to solve this area problem.

E-government improves quality of government service, cost savings, wider political participation, and more effective policies and programs, and it has also been proposed as a solution for increasing citizen communication with government agencies and, ultimately, political trust. A

major challenge for the government and law enforcement is how to quickly analyze the growing volumes of crime data.

In transport system, data mining can be used for map refinement according to GPS traces, and based on multiple users' GPS trajectories researchers discover the interesting locations and classical travel sequences for location recommendation and travel recommendation.





### Challenges and Open Research Issues in IoT and Big Data Era

With the rapid development of IoT, big data, and cloud computing, the most fundamental challenge is to explore the large volumes of data and extract useful information or knowledge for future actions. The key characteristics of the data in IoT era can be considered as big data; they are as follows.

- (i) Large volumes of data to read and write: the amount of data can be TB (terabytes), even PB (petabytes) and ZB (zettabyte), so we need to explore fast and effective mechanisms.
- (ii) Heterogeneous data sources and data types to integrate: in big data era, the data sources are diverse; for example, we need to integrate sensors data, cameras data, social media data, and so on and all these data are different in format, byte, binary, string, number, and so forth. We need to communicate with different types of devices and different systems and also need to extract data from web pages.
- (iii) Complex knowledge to extract: the knowledge is deeply hidden in large volumes of data and the knowledge is not straightforward, so we need to analyze the properties of data and find the association of different data.

### *Challenges.*

There are lots of challenges when IoT and big data come; the quantity of data is big but the quality is low and the data are various from different data sources inherently possessing a great many different types and representation forms, and the data is heterogeneous, as-structured, semistructured, and even entirely unstructured.

### *Open Research Issues.*

In big data era, there are some open research issues including data checking, parallel programming model, and big data mining framework.

### *Recent Works of Big Data Mining System for IoT.*

In datamining system area, many large companies as Facebook, Yahoo, and Twitter benefit and contribute works to open source projects.

## **Aim/Objectives**

In this unit we raise some issues emerging in the field of computer security. By emerging we mean that these areas are starting to be recognized outside the security community, although we do not mean there are solutions or even approaches to the security problems. Instead we raise these as interesting things to watch over time. In this week we discuss the so-called Internet of Things (the trend toward embedding Internet connected computing technology in new technology), economics of cybersecurity, electronic voting, and what many call cyber warfare (use of computers in political conflicts).

## **Learning Outcomes**

By the end of this chapter, students should be able to:

- Describe issues emerging in the field of computer security and more specifically the IoT.

## **Key Words**

Cyber warfare	Big Data Mining	Open Research Issues
E-governance	Health care data mining	e-commerce data mining

## Annotated Bibliography

### Required Materials

To achieve the educational needs of this unit the following material is used:

#### Primary Material

Chen, F., Deng, P., Wan, J., Zhang, D., Vasilakos, A.V. and Rong, X., 2015. Data mining for the internet of things: literature review and challenges. *International Journal of Distributed Sensor Networks*, 11(8), p.431047.

The massive data generated by the Internet of Things (IoT) are considered of high business value, and data mining algorithms can be applied to IoT to extract hidden information from data. In this paper, we give a systematic way to review data mining in knowledge view, technique view, and application view, including classification, clustering, association analysis, time series analysis and outlier analysis. And the latest application cases are also surveyed. As more and more devices connected to IoT, large volume of data should be analyzed, the latest algorithms should be modified to apply to big data. In this article these algorithms are reviewed; and challenges and open research issues are discussed. At last a suggested big data mining system is proposed.

#### Supportive material

Tsai, C.W., Lai, C.F., Chiang, M.C. and Yang, L.T., 2014. Data mining for Internet of Things: A survey. *IEEE Communications Surveys and Tutorials*, 16(1), pp.77-97.

IoT Applications | Top 10 Uses of Internet of Things <https://data-flair.training/blogs/iot-applications/>

## Individual Assignment (20 points)

Individual Assignment carrying 20% of the total grade. Research on Data mining for the Internet of Things listing possible applications, as well as the advantages and challenges posed by this emerging technology. Use 6-8 pages maximum.

## Recommended time for the student to work

35 hours

# AI-BASED PRIVACY MECHANISM FOR PERSONAL DATA IN THE INTERNET OF THINGS

9<sup>th</sup> Week

## Summary

Privacy is a very broad and diverse notion for which literature offers many definitions and perspectives. With the increasing use and efficiency of electronic data processing, data privacy has become the predominant issue today, especially for the IoT. Data privacy is suitably defined as the appropriate use of data. When companies and merchants use data or information that is provided or entrusted to them, the data should be used according to the agreed purposes. The differences and relations between security and privacy is that security provides protection for all types of information, in any form, so that the information's confidentiality, integrity, and availability are maintained whereas privacy assures that personal information (and sometimes corporate confidential information as well) are collected, processed (used), protected and destroyed legally and fairly.

## Introductory Remarks

The evolving nature of the IoT regarding technologies and features and the emerging new ways of interaction with the IoT lead to specific privacy threats and challenges. Generally, data privacy in the IoT is the threefold guarantee to the subject for:

- Awareness of privacy risks imposed by smart things and services surrounding the data subject
- Individual control over the collection and processing of personal information by the surrounding smart things
- Awareness and control of subsequent use and dissemination of personal information by those entities to any entity outside the subject's personal control sphere.

Data privacy in the IoT captures in essence the idea of informational self-determination by enabling the subject (i) to assess its personal privacy risks, (ii) to take appropriate action to protect its privacy, and (iii) to be assured that it is enforced beyond its immediate control sphere. Data Privacy has been a hot research topic in different technology and application areas that are important enablers of the IoT vision.

Despite considerable contributions from research communities, arising privacy issues in the IoT have not been efficiently dealt. This is because the composition of a growing number of technologies and a range of changing features with an explosion in the number of smart things, interactions and inter-communications among users and things in the IoT. These new features of the IoT will aggravate privacy issues and introduce unforeseen threats that pose challenging technical problems.

In the complex IoT environment, privacy problems cannot be optimally solved due to their complexity. In these situations, AI has proven to be extremely useful and well-fitted to solve these problems. Artificial neural networks, evolutionary computation, clustering, fuzzy sets, multi-agent systems, data mining and pattern recognition are just a few examples of AI techniques that can be successfully used to solve some relevant privacy and security problems.

#### *Requirements related to IoT environment*

Privacy includes the concealment of personal data as well as the ability to control what happens with this data. The right to privacy can be considered as either a basic and inalienable human right, or as a personal right or possession. There are two main approaches for dealing with privacy challenges in the IoT:

- Privacy enhancing technologies (PET): PET refers to specific methods that act in accordance with the laws of data protection. PET is a system of ICT that measures the protection of informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data. The fulfilment of customer privacy requirements is quite difficult. A number of technologies have been developed in order to achieve privacy goals. PET can be any mechanisms that enhance the privacy.
- Legal course of action: Privacy legislation tries to draw boundaries to the evermore data-hungry business models of many Internet enterprises (e.g., data market places, advertising networks and e-commerce sites) and to define mandatory practices and processes for privacy protection.

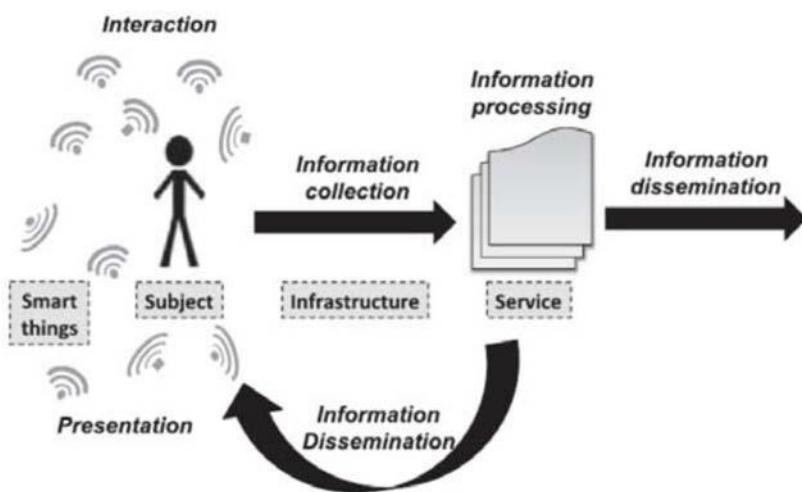
#### *Privacy Principles*

The concepts of privacy and data protection must not be reduced to protection of data. In fact, the concepts have to be understood more broadly: they address the protection of human beings and their personal rights as well as democratic values of society. Keeping this in mind, privacy and data protection require safeguards concerning specific types of data since data processing may severely threaten informational privacy.

Several terms have been introduced to describe types of data that need to be protected. A term very prominently used by industry is “personally identifiable information (PII)”, i.e., data that can be related to an individual. Similarly, the European data protection framework centres on “personal data”. However, some authors argue that this falls short since also data that is not related to a single individual might still have an impact on the privacy of groups, e.g., an entire group might be discriminated with the help of certain information.

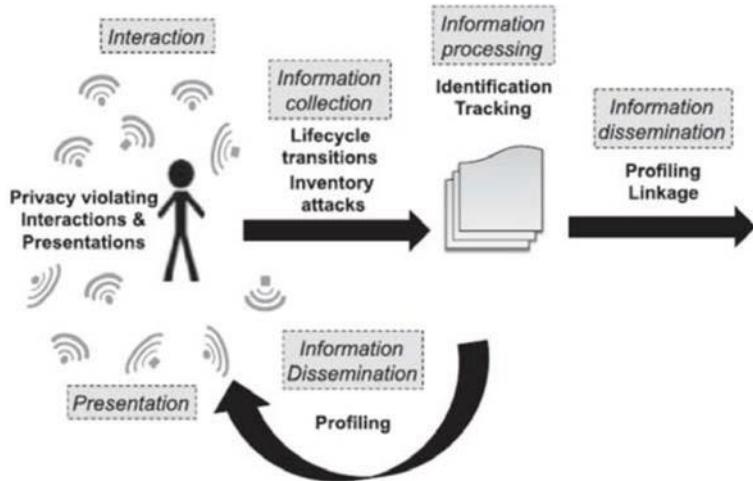
### *Privacy reference model*

The privacy reference model is considered based on the IoT reference model proposed by ITU and IoT European Research Council (IERC) visions. Here in the privacy model, there are 4 main types of entities namely: Smart Things, Subject, Infrastructure and Services with 5 different data flows including Interaction, Collection, Processing, Dissemination and Presentation.



### *Privacy Threats and Challenges in the Internet of Things*

The evolving nature of the IoT regarding technologies and features and the emerging new ways of interaction with the IoT lead to specific privacy threats and challenges.



### *Identification*

Identification denotes the threat of associating a (persistent) identifier, for example, a name and address or a pseudonym of any kind, with an individual and data about him. The threat thus lies in associating an identity to a specific privacy-violating context, and it also enables and aggravates other threats, for example, profiling and tracking of individuals or combination of different data sources. The threat of identification is currently most dominant in the information processing phase at the backend services of our reference model, where huge amounts of information are concentrated in a central place outside of the subject's control. In the IoT, also the interaction and collection phase will become relevant because the impact of the evolving technologies and interconnection and interaction features aggravates the threat of identification. Identity protection and, complementary, protection against identification is a predominant topic in RFID privacy, but has also gained much attention in the areas of data anonymization<sup>41</sup>, and privacy enhancing identity management. Those approaches (i.e., data anonymization, privacy enhancing identity management) are difficult to fit to the IoT: Most data anonymization techniques can be broken using auxiliary data, which are likely to become available at some point during the IoT evolution. Identity management solutions, besides relying heavily on expensive crypto-operations, are mostly designed for very confined environments, such as enterprise or home networks, and thus difficult to fit to the distributed, diverse, and heterogeneous environment of the IoT.

### *Localization and Tracking*

Localization and tracking is the threat of determining and recording a person's location through time and space. Tracking requires identification of some kind to bind continuous localizations to one individual. Already today, tracking is possible through different means, for example, GPS,

internet traffic, or cell phone location. Many concrete privacy violations have been identified related to this threat, for example, GPS stalking, disclosure of private information such as an illness, or generally the uneasy feeling of being watched. However, localization and tracking of individuals is also an important functionality in many IoT systems. The location privacy is the protection of location information of user's sensitive information such as residence location, behaviour, health status and other sensitive information. IoT devices have a builtin GPS system for positioning of location information. The user may issue a query to location based services (LBS) for location information. The query may be for a location of interest—for example, the nearest restaurant, hospital, park or other places. The query contains the identity and location of the user. The convenience of using LBS services creates issues of privacy risk. Based on the provided information, an adversary could easily link the identity and location of the user to get more private information. Security and privacy are a critical measure to consider for information gathering and broadcasting. This information and data must be secure from illegal and unauthorized access.

### *Profiling*

Profiling denotes the threat of compiling information dossiers about individuals to infer interests by correlation with other profiles and data. Profiling methods are mostly used for personalization in ecommerce (e.g., in recommender systems, newsletters, and advertisements) and also for internal optimization based on customer demographics and interests. Existing approaches to preserve privacy include client-side personalization, data perturbation, obfuscation and anonymization, distribution, and working on encrypted data

### *AI-based Privacy Techniques and Mechanisms*

Successful security success is about having the right combination of people, process, policy and technology. This can be achieved by developing a network management systems capable of intellectual reasoning, dynamic real time decision making, and self-adaptation and improvement based on experiences. The design of such efficient, dynamic and automated social network management framework requires support from the field of AI. Dealing with uncertainty and inconsistency has been a part of AI since its origins.

### *Traditional Privacy Preserving Approaches*

In order to address the privacy concerns of end-users and privacy considerations of service providers, several approaches have been proposed by the research community:

- a) Cryptographic techniques and information manipulation: Although researchers have spent many years proposing novel privacy-preserving schemes, cryptography is still the most dominant solution. However, due to limited storage and computation resources, cryptography often cannot offer adequate security protocols to safeguard end-users' data.
- b) Privacy awareness or context awareness: The solutions for the lack of privacy awareness have been primarily focused on relying individual applications to provide a basic privacy terms and conditions to the end-users. This practice is common among devices such as smart TVs, wearable fitness devices, and health monitor systems. For instance, in a recent research, a framework called SeCoMan was proposed to act as a trusted third party for the users as applications might not be reliable enough with the location information that they manage.
- c) Access control: Access control is one of the viable solutions to be used in addition to encryption and raising privacy awareness. This gives users the power to manage their own data.
- d) Data minimization: The principle of "data minimization" means that the IoT service providers should limit the collection of personal information to what is directly relevant. They should also retain the data only for as long as it is necessary to fulfill the purpose of the services. In other words, they should collect only the personal data they really need and should keep it only for as long as they need it.

### *Prospective AI-based Privacy Preserving*

Capabilities of AI can be leveraged to deal with privacy challenges in the IoT.

#### AI-based Identification Management

- AI - is it the answer for identity management?
- Could AI improve identity management and security?

Identity and Access Management (IAM) is already a key weapon in the security arsenal of many organisations as a way to mitigate against data breaches and manage the additional risks that come with remote working and Bring Your Own Device (BYOD). And the take up of IAM solutions is set to gain even more momentum. IAM solutions enable a network or system to authenticate the identity of a user against a set of pre-prescribed credentials. Depending on the system being accessed, these can range from a simple username and password to digital certificates, physical tokens, biometric passwords (such as fingerprints, iris scans, or facial recognition), or a combination of these features.

Traditionally, the strength of the authentication required depends on the sensitivity of the material being accessed, as well as the impact should these resources fall into unauthorised hands. Public information might require little or no authentication, while proprietary or classified data or accounts with administrative privileges will require stronger authentication, preferably using multiple factors.

While the above still holds true, recent thinking around best practice in IAM has moved on. The focus has shifted from authenticating identity to controlling access based on the principle of least privilege access. In practice, what that means is that every user – whether an individual, a device, a programme or a process – is given access only to the resources needed to fulfil their role.

But how might AI help? So often with data breaches it's not the management of the identity that causes the breach, but the transfer of credentials to some unknown party. While least privilege access control does afford some protection here, there are clearly insufficient. Identity management and access control have always been two sides of a coin, but in the future AI will be the glue to bind them together to much greater effect.

Moving on to biometric passwords, it's not difficult to conceive that AI could identify a user by using sight and sound. Rather than checking pre-defined credentials, a machine would be able to identify whether a person using visual and aural clues, granting access to this person accordingly.

AI also offers the potential for intelligent, real-time security by implementing fine-grained access control. Just because a user proved who they were at log on two minutes ago, should the system continue to believe they are who they say they are? Visual images and voice could obviously still play a part here, constantly monitoring users as they move around the network. However, in addition to behavioural factors and real-time, risk analysis can also come into play.

Working within a user's access permissions, AI systems could monitor in real-time whether a user is accessing or trying to access a part of the system they never normally would or suddenly downloading more documents than they generally would. The rhythm of a user's keyboard and mouse movements could be observed to identify irregular or unusual patterns. Taking this a step further it's not inconceivable that insights from an individual's online identity and activity – their social profile, groups they are part of, people they follow, websites they visit – could be used to determine a risk score. Drawing this data together, actions taken by the AI system could range from an alert being triggered, to specific areas of a corporate system being switched off for a user, to access being instantly revoked.

## Aim/Objectives

This week aims to enhance students' perception of privacy regarding the AI. Students will be acquainted with privacy principles and privacy reference models as well as major privacy threats and challenges in the IoT and AI.

## Learning Outcomes

By the end of this chapter, students should be able to:

- present a Privacy reference model for the IoT
- introduce major privacy threats and challenges in the IoT
- describe some state-of-the-art approaches based on AI for dealing with such data privacy issues

## Key Words

Artificial intelligence	IoT	Privacy reference model
Data and privacy issues	Identification	Localization and tracking
Profiling		

## Annotated Bibliography

### Required Materials

To achieve the educational needs of this unit the following material is used:

#### Primary Material

Internet of Things European Research Cluster (IERC). *The Internet of Things 2012—New Horizons*, 3rd edn.: Halifax, UK, 2012.

In this book you will find many answers to the questions which are being asked today - After considering the content of this book the reader might well ask what will come next. What is happening on a world-wide scale in the domain of the Internet of Things? What are the results and achievements so far in Europe on several dedicated aspects like architecture but also on

identification and standardisation issues? What should be understood by IoT Governance and what ideas exist for a potential model? What are the future research challenges and road-mapping building blocks? How are current Internet of Things business perspectives perceived by regional and international players?

International Organization for Standardization. Information technology security techniques privacy framework, iso/iec 29100, 2011.

OECD. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. OECD Publishing, 2002

D. Wright and C. Raab. Privacy principles, risks and harms. International Review of Law, Computers & Technology, 28(3):277–298, 2014.

## **Self-Assessment Exercises**

### **Exercise 9.1**

Find a case of data mining in regards to AI and briefly explain the concerns that it may raise, as well as your own critical view on the matter. Use 2-3 pages.

### **Recommended time for the student to work**

15 hours

## PRIVACY METRICS AND PRIVACY INVASION TOOLS

10<sup>th</sup> Week

### Summary

During this week we will see some privacy metrics. The Patterns (behaviour profiling) can be revealed if we answer questions like Watching too much TV? Or Another microwave meal? Real-time surveillance like monitoring if you Were you home last night? Or Did your friend move in? can reveal information as well. Non-grid use of data like Advertising and spam, Insurance and Appliance warranties gather significant amount of information that can lead to Information leakage including phishing, pharming, fraud.

### Introductory Remarks

Security does not guarantee privacy. Remote switching off capability of smart meters opens up new vulnerabilities (Stuxnet type cyber-attacks). Meters can be hacked by consumers or third parties to reduce/increase energy bill. A utility in Puerto Rico lost \$400 million in annual revenue after criminals hacked into smart meters to under-report electricity usage. Smart meters are made to last (15-20 years). In many cases encryption mechanisms are not adaptive and cannot last as long. Highly connected advanced metering infrastructure (AMI) allows spread of malware. Wireless transmission of meter readings is prone to eavesdropping and data injection attacks

Security Measures against Attackers are Authentication and authorisation, Secure networks and communication links, Secure data storage, Secure multi-party computing, Encrypted functions, Trusted platform module, and Physically unclonable functions. Are these measures sufficient to protect privacy? We also need Confidentiality and Authorisation vs. Privacy. By Confidentiality we refer to set of rules that limit access or place restrictions on disclosure of some information, e.g., by means of encryption. Confidentiality ensures that access to information is restricted to authorized entities. Authorisation limits access to certain entities. Authorization is usually coupled with authentication. In smart meters, privacy is not only against third parties/ attackers, but also against the legitimate/ authorised receiver of data.

To protect privacy we first need to measure it.

Privacy Metrics for Smart Meters include:

- Relative entropy / Mutual information: used for computing bounds on the achievable level of privacy, independent of technologic and computational capabilities of an attacker.
- Cluster classification: input data classified into clusters; known and hidden load cluster comparison may yield a possible privacy gain.
- Regression analysis: known and hidden loads are shifted until they align to their point of maximum cross-correlation.
- Residual features: features that appear both in the known and hidden profiles (i.e., an energy transition).
- Exploratory Data Mining & Interestingness: ensures that interesting data mining patterns (e.g. atypical TV or sleep patterns) remain hidden.
- Differential privacy: ensures that adding a single entry to a database (or deleting one from it) does not significantly change the answer given to some queries.

Interestingness of a pattern may be assessed as a trade-off between the self-information and the description length. Self-information: this may be calculated by calculating the entropy of mutually exclusive subsets of the pattern. Description length: this measures how concisely the pattern conveys this information.

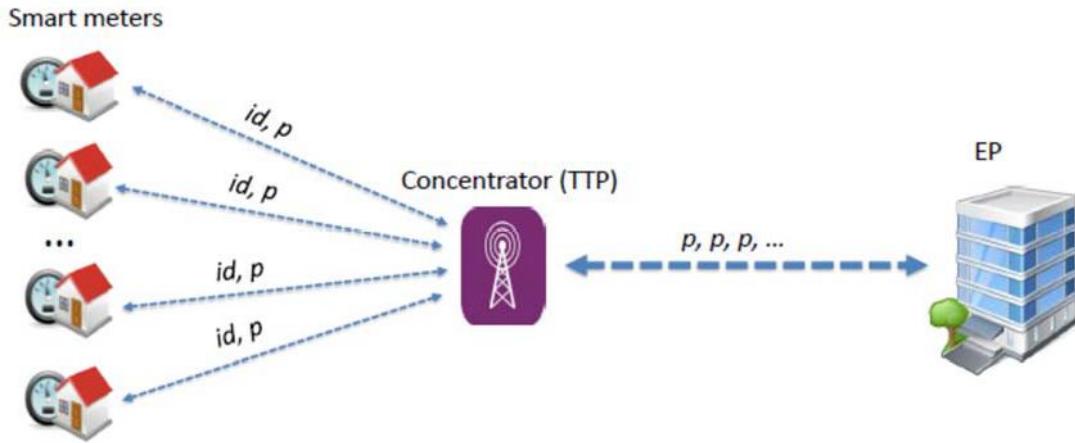
### *Differential Privacy*

- Introduced to privately release statistical queries on data sets
- Differential privacy measures privacy by parameter that bounds the log-likelihood ratio of the output for two databases that differ in only a single entry.

### *Machine Learning & Knowledge extraction*

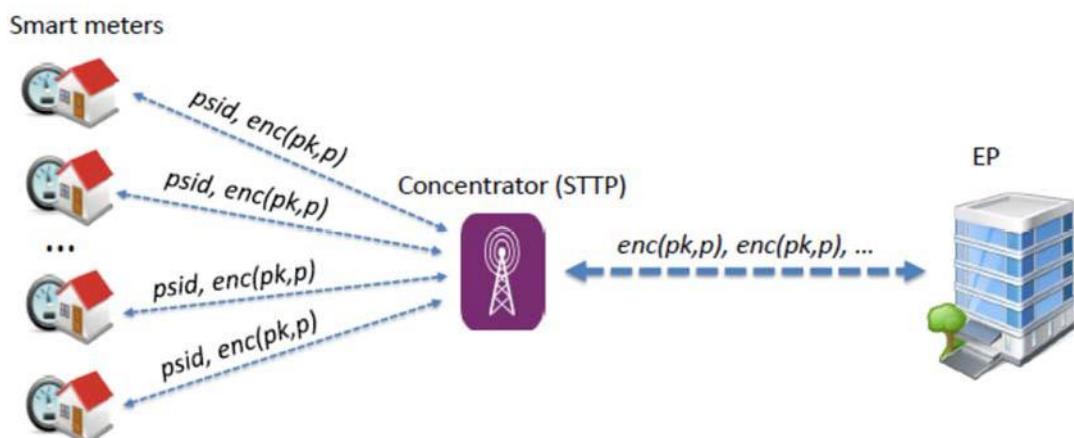
- The fundamental privacy metrics may also apply after smart metering data is processed to extract knowledge.
- For example, knowledge may simply be represented as a categorical table with multiple dimensions (columns).
- A particularly important knowledge, from a privacy perspective, concerns metering data at an appliance level.
- This leads us to the problem of appliance disaggregation, the alter ego of privacy protection.
- This is also known as Non-intrusive Appliance Load Monitoring (NIALM) and may be further distinguished into low frequency NIALM and high frequency NIALM.

### Anonymization with Trusted Third Party (TTP)



- SM readings sent to a TTP over secure links.
- TTP removes the identities of users from the tuples received and sends only the SM readings to EP.
- EP learns the SM readings, but not their origin.
- However, TTP learns the SM readings too.

### Anonymization with STTP



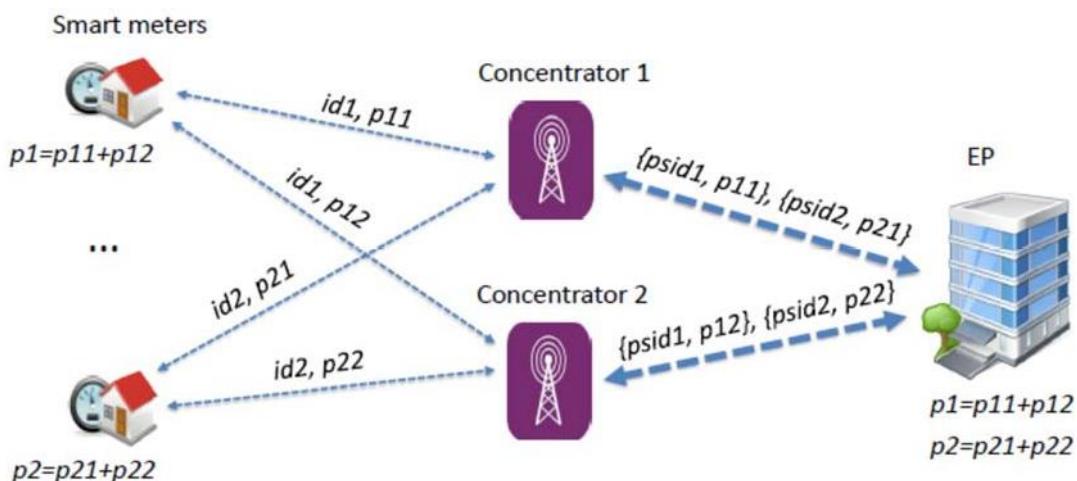
- SM readings are encrypted with the public key of EP.
- Instead of real identities, users use pseudonyms.

- STTP sends only the encrypted SM readings to EP.
- EP decrypts and learns the SM readings, but not their origin.
- STTP does not learn the SM readings nor the real identities of users.

#### *Anonymisation: Customer Data vs. Technical data*

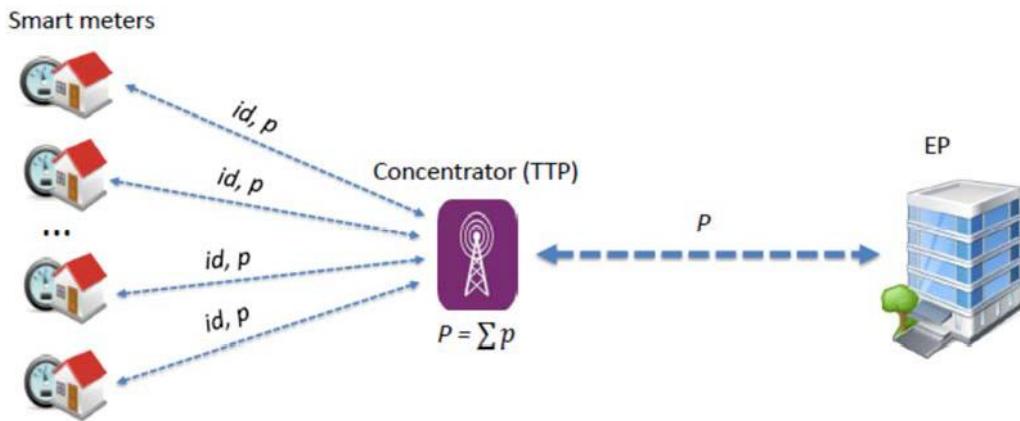
- EU SM standards recommendation to define two types of data for smart metering:
- Customer data: Attributable data, e.g. for billing and account management purposes. Low-frequency data, e.g. every few days/weeks.
- Technical data: “Anonymous” data, e.g. for power network management and demand response. High-frequency data, e.g. every few minutes.
- There is no real reason why the high-frequency data can't be anonymous and still serve the purposes of the utility and the power distribution network.
- Smart meter uses both eponymous and anonymous IDs (and related crypto keys) for customer and technical data, respectively.
- The utility knows that the anonymous ID is located within a certain area, but not which specific house.

#### *Anonymization & Data Splitting*



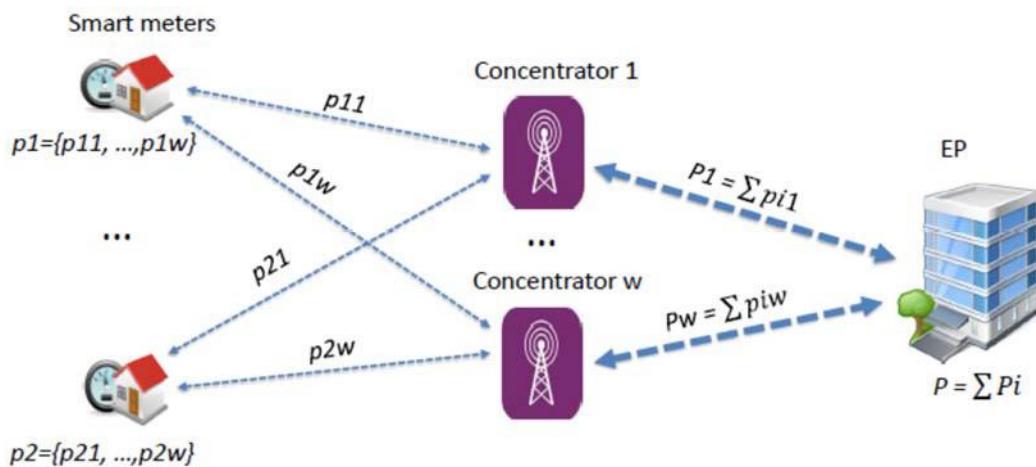
- Each SM splits its data into shares and sends each share to a different concentrator.
- Each concentrator replaces the real ID of the user with a pseudonym and forwards the data to EP.
- EP sums all the shares attached with the same pseudonym.
- EP knows the SM readings, but not their origin.

### Aggregation with Trusted Third Party (TTP)



- SM readings sent to a TTP over secure links.
- TTP reports to EP:
- sum consumption for a group of SMs (e.g., neighbourhood),
- sum consumption of each user over billing period.
- EP learns exactly what it needs to learn, not more.
- TTP does not need to know real identities of users, but has to be trusted.

### Aggregation & Data Splitting



- Each SM splits its data into  $w$  shares using  $(w, t)$  secret sharing scheme; sends each share to a different concentrator.
- Each concentrator sums the received shares and sends the aggregated shares to EP.

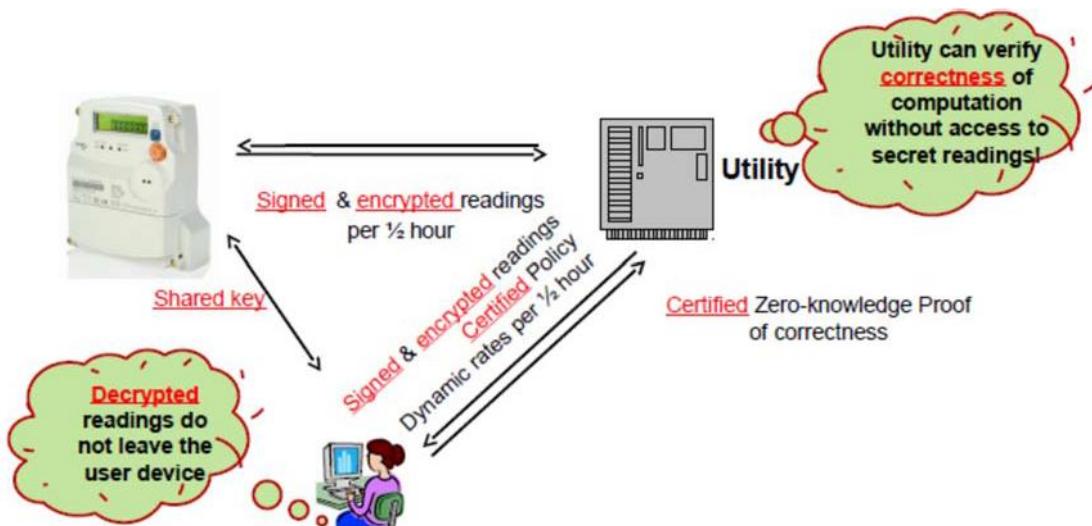
- EP sums at least  $t$  of the received aggregated shares to obtain the aggregated data of all SMs.

### *Aggregation without Trusted Third Party (TTP)*

- How to add a user's data to the aggregate without revealing it to other users?
- SMs have trusted elements (e.g., smart card or secure USB stick) that cannot be controlled by the grid operator (i.e., it cannot change keys remotely).
- These trusted elements provide secure storage and basic cryptographic functionality
- Common tool: homomorphic encryption, thanks to its additive homomorphic property.
- Proposed approaches differ mainly in: Who performs the aggregation, and how keys are managed.

### *Zero-proof SM cryptosystem*

## Yet another fancy cryptosystem



- Computations executed by the customer without disclosing raw meter readings.
- Correctness can be guaranteed.
- If the raw data is needed, secure aggregation can be used.

### *Obfuscation*

Users add zero-mean independent noise to their readings before forwarding to EP. Average sum consumption remains same at each period. The goal is low confidence for individual

measurements (high variance noise component), and high-confidence for total consumption (too many uses aggregated together: 99.9% confidence requires aggregating 3.8 million users.) Meters should be tamper-proof.

## Aim/Objectives

In this chapter we overview some important data mining notions with the help of smart meters – providing reliable and secure source for real-time data on energy consumption and power supply quality. We review differential privacy, privacy metrics, data splitting, anonymization, aggregation, zero-proof and obfuscation.

## Learning Outcomes

By the end of this chapter, students should be able to:

- Analyse privacy implications of using smart meters in IoT
- Recognize privacy metrics
- Explain anonymization, aggregation, zero-proof, data splitting and obfuscation

## Key Words

Smart meters	Knowledge extraction	Differential Privacy
Privacy metrics	Data Splitting	Anonymization
Aggregation	Zero-proof	Obfuscation

## Annotated Bibliography

### Required Materials

To achieve the educational needs of this unit the following material is used:

#### Primary Material

Kalogridis, D.G.G. and Mustafa, M.A., 2015, November. Privacy in Smart Metering Systems. In *Information Forensics and Security (WIFS), IEEE in 7th International Workshop on, Rome, Italy*.

This tutorial will provide a comprehensive overview of growing privacy threats to SMs and the smart grid in general. Potential attacks and their impact on the grid, and various privacy preservation solutions will be reviewed. It provides both an academic and an industry perspective on the future of SMs, and the tools that can be employed to guarantee advanced SM functionality without threatening user privacy.

### **Supportive material**

"Guidelines for Smart Grid Cyber Security," National Institute of Standards and Technology (NIST), Privacy and the Smart Grid, vol. 2, NIST IR 7628 Rev. 1, Sep. 2014.

Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, "Private memoirs of a smart meter," in ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building, New York, 2010, pp. 61-66.

R. Petrlík, "A privacy-preserving concept for smart grids," in Sicherheit in vernetzten Systemen 18. DFN Workshop, ser. Books on Demand GmbH, 2010, pp. 1-14.

C. Rottondi, G. Mauri, and G. Verticale, "A data pseudonymization protocol for smart grids," in IEEE GreenCom Conference, Sept. 2012, pp. 68-73.

J.-M. Bohli, C. Sorge, and O. Ugus, "A privacy model for smart metering," in IEEE Int'l Conf. on Comm. Workshops, Cape Town, South Africa, May 2010, pp. 1-5.

C. Rottondi, G. Verticale, and A. Capone. "Privacy-preserving smart metering with multiple data consumers." Computer Networks 57, no. 7, 2013, 1699-1713.

A. Rial, G. Danezis, "Privacy-preserving smart metering", Proceedings of the 10th annual ACM workshop on Privacy in the electronic society, pp 49–60, 2011.

Danidou, Y. and Schafer, B., 2012. Legal environments for digital trust: trustmarks, trusted computing and the issue of legal liability. *J. Int'l Com. L. & Tech.*, 7, p.212.

### **Activity (5 points)**

Graded activity carrying 5% of the final grade. Research extensively on the privacy implications caused by the IoT in terms of the extreme size of data gathered by the different devices. Use 4-7 pages to support your research using proper citations.

## **Recommended time for the student to work**

Estimated 20 hours

## BEYOND CONSENT-BASED PRIVACY PROTECTION

11<sup>th</sup> Week

### Summary

The circumstances have changed fundamentally since privacy was conceptualized as “individuals in control of their personal information” over forty years ago. Individuals constantly provide personal information. The Internet now reaches billions of people around the world and serves as a virtual marketplace for products, information, and ideas. The fluidity of personal information collections has increased as the scope and goals of such data continuously evolve. Business models are increasingly based on the notion of greater customization and various products and services are offered for free, as they may be partially supported by advertising revenue. Companies also wish to use analytic solutions in order to better understand their customers, as well as to improve or develop new products and services.

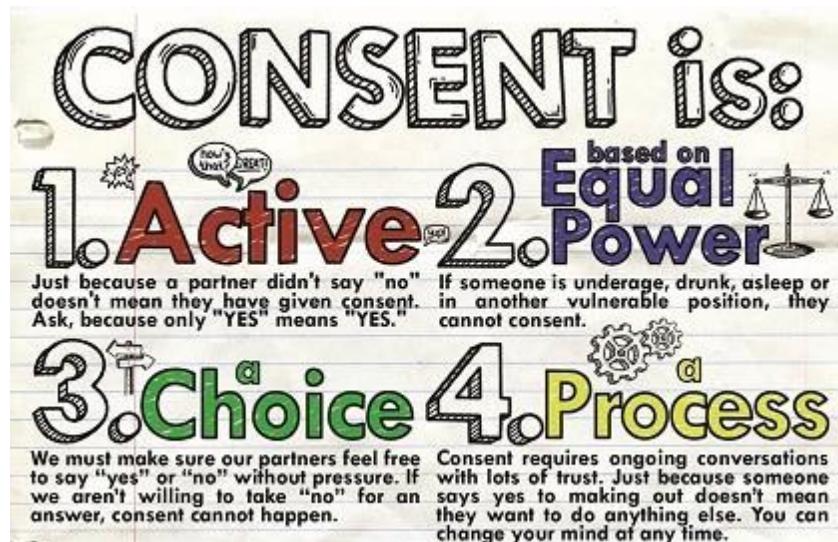
### Introductory Remarks

The second generation of the Internet made possible greater interaction and connectedness among online users, and individuals are becoming increasingly involved in managing their own data through online social networks. There are also recent technological developments triggering the emergence of new identification tools, which allow for easier identification of individuals.

Recent technologies are presenting additional challenges to consent-based privacy protection frameworks. With the Internet of Things (IoT), seemingly mundane everyday devices are fitted with microchips, sensors, and wireless communication capabilities. All of these devices are networked together to provide a seamless user experience. They are intended to collect data, aggregate them, communicate them to other devices in the network (*machine-to-machine* communication or M2M) and respond according to predetermined outcomes. Every device, of course, has its own producer and therefore its own privacy policy dictating who owns and gets access to the data and how it may be used – including data that comes from M2M communication. A study by Cisco shows that by 2020, 37 billion intelligent devices will be connected and communicating – three times the number of such devices being used in 2015. Wearable technologies collect data about all of the user’s daily activities and communicate them

automatically to an online data management system, aggregating the data and ensuring feedback to the user. The more data the user allows the device to accumulate, the more useful it may become. Moreover, more and more devices record, stream or upload a constant feed of images or movies. CCTV is one example; Google Glass is another. Almost everyone nowadays owns a smartphone with which we constantly take pictures, share them on social networks, and comment on them.

Many have, for quite some time, criticized the notion of meaningful consent which is central in any legislation based on the FIPPs, as it allegedly no longer provides a realistic approach. Solove reports that “people will be given consent forms with vague fine-print discussions of the contractual default privacy rules that they are waiving, and they will sign them without thought.” Schwartz questions whether individuals are in fact able to exercise meaningful choices with regard to the handling of their personal information, given disparities in knowledge and power when bargaining over the transfer of their information. Nissenbaum has articulated the view that it is no longer clear whether individuals are always capable of making informed choices and therefore, meaningful privacy notices and valid consent may be considered as illusory. In this section, the inadequacy of privacy policies as a means to communicate choices, as well as the fact that consent is now challenged by technological changes, will be discussed.



### Vagueness and Complexity of Privacy Policies

There are several reasons why privacy policies are ineffective. It is reported that it is difficult for individuals to understand such policies, because they are often complex and use specialized terms.

Policies are often written by specialized professionals, without considering the audience that may include users who are “below basic” literacy. Privacy policies, for instance, tend to be written at a college level; whereas the average reading level of an individual may typically be somewhere between that of eighth and ninth grade pupils. Similarly, privacy policies are often written in English, which is not everyone’s first language. Privacy policies may also be very long, discouraging users from reading them. Users are not generally capable of processing all the information they contain. Privacy policies may not always include sufficient or complete information to allow for a truly informed decision on the part of the consumer. Privacy policies may also often be vague about what information is collected, how the information will be used and how it will be disclosed.

Privacy policies may also be purposefully vague as to the uses which will eventually be made of the data to avoid limiting future uses. For example, organizations may claim to use the data collected for broad purposes, such as improving their products and services, developing new ones or enhancing the customer’s experience. Organizations do not necessarily have bad intentions when they use broad language in their policy; they may simply wish to be flexible so as to accommodate future actions without changing their policy, but the implication is that potential future uses of the information are too vast to enable individuals to make an adequate evaluation.

Finally, these privacy policies may also be nebulous when it comes to those with whom the data will be shared. Businesses often share this information with their marketing partners (as well as corporate affiliates and subsidiaries), in order to build more complete profiles about individual consumers; and often do so quietly. Many privacy policies will use terms like “partners” or “affiliates” to describe potential recipients of user data. According to some, these terms are “elastic”, because they can encompass different meanings in different contexts.

In many instances, consent to data collection activities is granted, despite the possibility – completely unbeknownst to the particular user in question -- that personal information already on file may be correlated or aggregated with new data, in order to form a more complete user profile. Cohen notes that “a comprehensive collection of data about an individual is vastly more than the sum of its parts.”

### *Privacy Policies Fatigue*

The issue with a consent or choice-based approach is the fact that, with the volume of data exchanges and collections taking place in modern society, individuals would be faced with the prospect of constantly reviewing privacy policies and consenting to them throughout any given

day. It has been recently estimated that to read the privacy policies for all the websites an Internet user visits annually would take about 244 hours per year. Researchers at Carnegie Mellon once calculated that it would cost \$781 billion in worker productivity, if everyone were to read all of the privacy policies they encountered online in one year. It is not reasonable to expect average individuals to devote large portions of their time in order to process and provide meaningful responses to consent requests. Most users do not read privacy policies: A recent White House report stated, “Only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent.” To further illustrate the fact businesses know that users do not read privacy policies, it was reported a few years ago that a videogame company from the United Kingdom included a provision in its statement that, unless the user opted out, the company would retain rights to the user’s eternal soul.

### *Incentive for Data Collection and Retention*

Business models are increasingly based on the notion of greater customization of services and products. Due to the global dimension of its potential audience, the Internet has become an increasingly attractive forum for advertisers, who can target their campaigns more precisely and effectively than by advertising in other media. Technology now makes it possible to gather a lot of information to profile individuals and track their conduct, in order to send personalised advertising or tailored websites, products or services accordingly. Behavioural advertising provides benefits to consumers in the form of free web content and personalized advertisements. Many online service providers are offering services, information, and entertainment free of charge to online users, as long as they agree to receive advertising and allow their online behaviour to be tracked. Various services are offered for free online, as they may be partially supported by advertising revenue, including online social services such as Facebook and Google’s web service Gmail. Additionally, more individuals are able to access newspaper content on the Internet for free, because it is subsidized by online advertising. Certain studies even show that individuals do not want and do not expect to be paying for web services.

With Big Data, organizations have an incentive to collect more personal information and keep such information for longer. These examples simply illustrate the shared incentive for businesses to collect a large quantity of personal information and to remain vague in framing their privacy policies. Froomkin suggests that: “In theory, the parties to a transaction can always contract for confidentiality. This is unrealistic due because consumers suffer from privacy myopia: they will sell their data too often and too cheaply”.

### *Consent Challenged by Technological Changes*

The previous section illustrates how ineffective current privacy policies are a means to communicate choices, as these statements are rarely ever read, are often confusing and are incapable of capturing the complexity of modern data-handling practices. As a result, individuals typically have little meaningful choice about the use of their personal information. This section will discuss how the notion of consent is being challenged, in light of the increase in the number of players providing new products and services, the dynamic aspect of privacy policies and business models, the ubiquity of data collection and sharing practices, as well as because technology is becoming increasingly sophisticated, so as to enable individuals to properly evaluate the risks related to their consent to a given data-handling activity.

### *Ever-increasing Number of Players Involved*

In Europe, the interaction between data controllers and data processors is essential in the application of certain data protection laws such as GDPR, since they influence who will be responsible for compliance with data protection rules and how individuals can exercise their rights. The increasing complexity of the environment in which these concepts are used has given rise to new and difficult issues, such that the Article 29 Working Party recently issued an opinion emphasizing the need to allocate responsibility between data controllers and data processors, so that compliance with data protection laws can be enforced sufficiently.



### *Dynamic Aspect of Privacy Policies and Business Models*

Many organizations and industry players may change their privacy policies, making it even more difficult to keep track (i.e. "control") of data handling practices. Privacy policies often reserve the right to change their terms and conditions unilaterally, so if users want to know the precise nature

of any such modification, it is often up to them to refer back to the new version, which is unrealistic. This practice of unilaterally modifying privacy policies makes it even more difficult for individuals to keep control over their information and provide meaningful consent.

#### *Ubiquity of Data Collection and Sharing*

Challenges the validity of consent. For instance, when the consumer browses for products and services online, advertisers may choose to collect and share information about the consumer's activity, search history, websites visited, etc. When participating in an OSN, third-party applications are likely to have access to the user's information pertaining to his posts. When using location-enabled devices, various third party application providers and entities may thus ascertain the consumer's precise whereabouts. If a consumer uses loyalty cards at a grocery store or sends in a product warranty card, his name, address, and information about his purchase may be shared with data brokers and combined with other data.

More recently, certain wearable things are likely to be adopted quickly, as they extend the usefulness of everyday objects familiar to the individual. They may be embedded in cameras, microphones and sensors that can record and transfer data to the device manufacturer.<sup>70</sup> The Article 29 Working Party has raised the concern that such wearable things, kept in close proximity to users, result in the availability of a range of other identifiers, such as the MAC addresses of other devices, which could be useful to generate a fingerprint allowing location tracking.

### **Aim/Objectives**

This chapter introduces students to the new data protection regulation GDPR and the aspects of it that are related to data mining like data collection and retention, consent, and of course privacy. We aim to broaden the knowledge of students on these important subjects to help them acquire full knowledge of all the legal implications that data mining in the new era is carrying.

### **Learning Outcomes**

By the end of this chapter, students should be able to:

- demonstrate knowledge and understanding of key concepts, tools and approaches for data mining on complex unstructured data sets
- describe theoretical concepts and the motivations behind different data-mining approaches

## Key Words

Machine-to-machine communication or M2M	Privacy policies	Data collection and retention
GDPR		

## Annotated Bibliography

### Required Materials

To achieve the educational needs of this unit the following material is used:

#### Primary Material

Gratton, E.,(2016), "Beyond Consent-Based Privacy Protection"

This paper is meant to provide guidance on some of the issues raised, such as whether legislative changes are required as well as on potential solutions which would be helpful in addressing consent challenges. In the first section, the paper illustrates how, in the context of new Internet technologies, the “notice and choice” approach is challenged. This is in part due to the current volume of data collections and vagueness of privacy policies, the increase in the numbers of players involved, the dynamic aspect of privacy policies and business models and the ubiquity of data collections and exchanges. It is also due to the fact that with technology becoming increasingly sophisticated, individuals may have a hard time understanding what kind of information is being collected about them and how their information will in fact be used. The fact that seeking consent may not always be practical to obtain, and is sometimes even impossible with recent business models and innovative technologies, will also be discussed.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Article 29 Data Protection Working Party, “Opinion 1/2010 on the concepts of “controller” and “processor””, 00264/10/EN WP 169, available at: European commission, available at:  
[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf)

Nissenbaum, H., 2011. A contextual approach to privacy online. *Daedalus*, 140(4), pp.32-48.

Solove, D.J., 2000. Privacy and power: Computer databases and metaphors for information privacy. Stan. L. Rev., 53, p.1393.

Schwartz, P.M., 1999. Privacy and democracy in cyberspace. Vand. L. Rev., 52, p.1607.

### **Supportive material**

Carmichael, L., Stalla-Bourdillon, S. and Staab, S., 2016. Data mining and automated discrimination: a mixed legal/technical perspective. IEEE Intelligent Systems, (6), pp.51-55.

Kumar, V. and Reinartz, W., 2018. Customer relationship management: Concept, strategy, and tools. Springer.

## **Self-Assessment Exercises**

### **Exercise 11.1**

Choose any subject area that uses or can start using IoT device (e.g. healthcare, transportation, critical infrastructures etc) and research on what kind of data they are collected, how these data are handled and discuss any potential privacy concerns this may raise. Use 5-7 pages.

### **Recommended time for the student to work**

15 hours

## INVITED LECTURE

11<sup>th</sup> & 12<sup>th</sup> Week

### Summary

Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Invited lectures aim to keep the connection with the industry and get real world examples on issues discussed during the course as well as current research issues.

### Introductory Remarks

Possible invited organisations:

- Office of the Commissioner for Personal Data Protection
- Cyprus Robotics team
- IEEE CIS Cyprus Chapter Drone Artificial Intelligence School

### Annotated Bibliography

### Required Materials

To achieve the educational needs of this unit, all the relevant material will be at student's disposal in Blackboard for further studying.

### Group Assignment (20 points)

Group assignment carrying 20% of the total grade.

Students (in pairs) will write an extended essay (4000 words) on the topic of their choosing (so long as the topic relates to ethics and data, data mining, Artificial intelligence, IoT, broadly construed). Students should have a clear idea of their intended audience and will receive guidance on how to write persuasively in that direction. Overall, the assignment is intended to help students learn to communicate ethical ideas and critical issues outside of the classroom.

### Recommended time for the student to work

Week 12: 35 hours and Week 13: 15 hours

## **REVISION WEEK AND FINAL EXAMINATION**

The final exam will contain multiple choice questions, open ended questions, closed ended questions and case studies.

### **Recommended time for the student to work**

40 hours

**Date/Time of Final Exam: TBD**

## INDICATIVE ANSWERS TO SELF-ASSESSMENT EXERCISES

### INTRODUCTION TO CYBERSECURITY DATA MINING – WEEK 1

#### Exercise 1.1

The answer should move around these three pillars.

- (a) Passwords
- (b) Encryption: Using the cloud services that provide local encryption and decryption of sensitive data.
- (c) Backup data

#### Exercise 1.2

The answer could vary according to the student. Indicative answers are given below.

- a) People are neglecting to change the key, by this they are given a chance to hack the data.
- b) The identification and authentication of the user data are done sometimes by forgetting the access code or wrong entry of the code.
- c) The access control is allowed when employees forget to log off the server for example and allow access to bad actors.

### SOCIAL BIG DATA APPLICATIONS – WEEK 2

#### Exercise 2.1

Each student will provide his own answer.

### BASIC CONCEPTS IN DATA MINING – WEEK 3

#### Exercise 3.1

An important aspect of an outlier detection technique is the nature of the desired outlier. Outliers can be classified into following three categories:

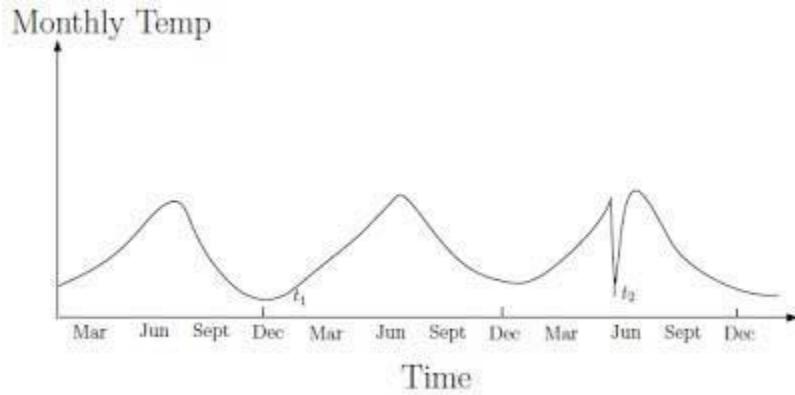
1. Point Outliers
2. Contextual Outliers
3. Collective Outliers.

**Point Outliers:**

If an individual data instance can be considered as anomalous with respect to the rest of data, then the instance is termed as a point outlier. This is the simplest type of outlier and is the focus of majority of research on outlier detection. For example, in Figure 1, points o1 and o2 as well as points in region O3 lie outside the boundary of the normal regions, and hence are point outliers since they are different from normal data points. As a real life example, if we consider credit card fraud detection with data set corresponding to an individual's credit card transactions assuming data definition by only one feature: amount spent. A transaction for which the amount spent is very high compared to the normal range of expenditure for that person will be a point outlier.

**Contextual Outliers:**

If a data instance is anomalous in a specific context (but not otherwise), then it is termed as a contextual outlier (also referred to as conditional outlier). The notion of a context is induced by the structure in the data set and has to be specified as a part of the problem formulation. Each data instance is defined using two sets of attributes: Contextual attributes. The contextual attributes are used to determine the context (or neighborhood) for that instance. For example, in spatial data sets, the longitude and latitude of a location are the contextual attributes. In time series data, time is a contextual attribute which determines the position of an instance on the entire sequence. Behavioral attributes. The behavioral attributes define the non-contextual characteristics of an instance. For example, in a spatial data set describing the average rainfall of the entire world, the amount of rainfall at any location is a behavioral attribute. The anomalous behavior is determined using the values for the behavioral attributes within a specific context. A data instance might be a contextual outlier in a given context, but an identical data instance (in terms of behavioral attributes) could be considered normal in a different context. This property is key in identifying contextual and behavioral attributes for a contextual



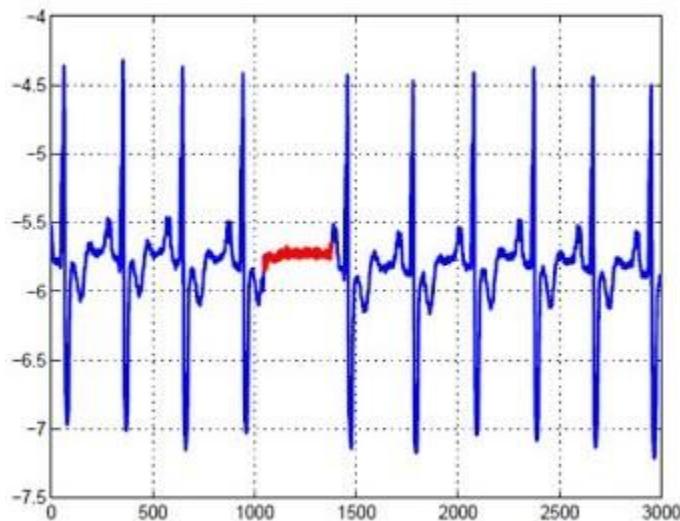
Contextual outlier  $t_2$  in a temperature time series. Temperature at time  $t_1$  is same as that at time  $t_2$  but occurs in a different context and hence is not considered as an outlier. Contextual outliers have been most commonly explored in time-series data and spatial data . Figure 3 shows one such example for a temperature time series which shows the monthly temperature of an area over last few years. A temperature of 35F might be normal during the winter (at time  $t_1$ ) at that place, but the same value during summer (at time  $t_2$ ) would be an outlier. A six ft tall adult may be a normal person but if viewed in context of age a six feet tall kid will definitely be an outlier. A similar example can be found in the credit card fraud detection with contextual as time of purchase. Suppose an individual usually has a weekly shopping bill of \$100 except during the Christmas week, when it reaches \$1000. A new purchase of \$1000 in a week in July will be considered a contextual outlier, since it does not conform to the normal behavior of the individual in the context of time (even though the same amount spent during Christmas week will be considered normal).

The choice of applying a contextual outlier detection technique is determined by the meaningfulness of the contextual outliers in the target application domain. Applying a contextual outlier detection technique makes sense if contextual attributes are readily available and therefore defining a context is straightforward. But it becomes difficult to apply such techniques if defining a context is not easy.

### **Collective Outliers:**

If a collection of related data instances is anomalous with respect to the entire data set, it is termed as a collective outlier. The individual data instances in a collective outlier may not be outliers by themselves, but their occurrence together as a collection is anomalous. Figure 4 illustrates an example which shows a human electrocardiogram output. The highlighted region denotes an outlier because the same low value exists for an abnormally long time (corresponding to an Atrial

Premature Contraction). It may be noted that low value by itself is not an outlier but its successive occurrence for long time is an outlier.



Collective outlier in an human ECG output corresponding to an Atrial Premature Contraction.

As another illustrative example, consider a sequence of actions occurring in a computer as shown below: ..... http-web, buffer-overflow, http-web, http-web, smtp-mail, ftp, http-web, ssh, smtp-mail, http-web, ssh, buffer-overflow, ftp, http-web, ftp, smtp-mail, httpweb..... The highlighted sequence of events (buffer-overflow, ssh, ftp) correspond to a typical web based attack by a remote machine followed by copying of data from the host computer to remote destination via ftp. It should be noted that this collection of events is an outlier but the individual events are not outliers when they occur in other locations in the sequence. Collective outliers have been explored for sequence data, graph data, and spatial data. It should be noted that while point outliers can occur in any data set, collective outliers can occur only in data sets in which data instances are related. In contrast, occurrence of contextual outliers depends on the availability of context attributes in the data. A point outlier or a collective outlier can also be a contextual outlier if analyzed with respect to a context. Thus a point outlier detection problem or collective outlier detection problem can be transformed to a contextual outlier detection problem by incorporating the context information.

# **CLASSICAL MACHINE – LEARNING PARADIGMS FOR DATA MINING**

## **– WEEK 4**

### **Exercise 4.1**

This is a research question that each student will answer differently.

## **PRIVACY AND DATA MINING – WEEK 5**

### **Exercise 5.1**

- Possible telephone company use: Capacity planning; billing; ideas for new services.
- Possible marketer use: Data mining to advertise to the caller/recipient. Possible rival telephone company use: Market research to woo customers.
- Possible government use: Looking for suspicious communications; criminal prosecution.
- All of these might violate individuals' privacy rights depending on how they are executed.

## **PRIVACY PRESERVING DATA MINING – WEEK 6**

### **Exercise 6.1**

Information sensitivity is the control of access to information or knowledge that might result in loss of an advantage or level of security if disclosed to others. Loss, misuse, modification, or unauthorized access to sensitive information can adversely affect the privacy or welfare of an individual, trade secrets of a business or even the security and international relations of a nation depending on the level of sensitivity and nature of the information.

- Removing identifying information from data doesn't work
  - Even if the overtly identifying information can be removed, identification from remaining data is often possible
- Data perturbation
  - Data perturbation can limit the privacy risks associated with the data without impacting analysis results
  - Data mining often focuses on correlation and aggregation, both of which can generally be reliably accomplished with perturbed data

One possible situation is when the source of information is a secret, such as a police informant or covert surveillance program. Sometimes patterns of insensitive data can become extremely

sensitive. For instance, seeing a person in a supermarket reveals insensitive data about that person's whereabouts at a given time, but tracking that person's movements for an extended period of time, aggregates that same kind of information into a set of sensitive data about that person's life.



**FORM: 200.1.3**

## **STUDY GUIDE**

**Course: CYS625 - Incident Response and Forensic Analysis**

## Course Information

<b>Institution</b>	European University Cyprus		
<b>Programme of Study</b>	Cybersecurity (MSc)		
<b>Course unit</b>	CYS625	Incident Response and Forensic Analysis	
<b>Level</b>	<b>Undergraduate</b>	<b>Postgraduate</b>	
		<b>Master</b>	<b>PhD</b>
		√	
<b>Language of Instruction</b>	English		
<b>Teaching Methodology</b>	Distance Learning		
<b>Course Type</b>	<b>Compulsory</b>	<b>Optional</b>	
		√	
<b>Number of Group Consultation Meetings/ Web-Conferences/ Lectures</b>	<b>Total</b>	<b>Face to Face</b>	<b>Web-Conferences</b>
	14	1	13
<b>Number of Activities/ Assignments</b>	4		
<b>Final Assessment</b>	<b>Assignments</b>	<b>Final Examinations</b>	
	50 %	50 %	
<b>Number of Credits (ECTS)</b>	10		

<b>Study Guide drafted by</b>	Dr Olga Angelopoulou
<b>Editing and final approval of Study Guide by</b>	Dr Yianna Danidou

## COURSE CONTENTS

		Page
	Introductory notes	4
	First group consultation meeting	5
1	Week 1 – Introduction to incident response and digital forensics	7
2	Week 2 – Planning and handling incident response	12
3	Week 3 – The Incident Reporting Process	17
4	Week 4 – Cybercrimes and digital investigations	22
5	Week 5 – Digital Investigations	28
6	Week 6 – Data collection and principles (I)	34
7	Week 7 – Data collection and principles (II)	34
8	Week 8 – Forensic Science to Networks and Volatile Data Preservation Process	37
9	Weeks 9 – Digital Evidence on the Internet	41
10	Week 10 – Evidence analysis and handling (I)	45
11	Week 11 – Evidence analysis and handling (II)	45
12	Week 12 - Reporting and presenting (I)	50
13	Week 13 - Reporting and presenting (II)	50
14	Revision and Final Examination	52

## INTRODUCTORY NOTES

Incident Response and Forensic Analysis is an elective unit of the MSc in Cybersecurity programme. The main goal of this unit is to cover the principles and practises of incident response and the digital forensic investigation.

This is a new unit that has been exclusively designed to be offered as part of the MSc in Cybersecurity. The main goal during the design phase of the unit is to maintain content flexibility for the development phase. It does not represent the material the learners will be provided with for the delivery of the unit, but it indicates the unit's aims, the topics that will be covered and the relevant individual activities.

This study guide is structured to provide a weekly content of the unit. It outlines the topic of study and the learning outcomes the online learners are expected to achieve every week. It expands on relevant keywords and the bibliography that the learners can refer to in order to expand their critical understanding of the topic. Also, a range of self-assessment exercises, activities and tutorials are provided the learners to practise the topics that are covered every week. Some weeks have been grouped together since they cover topics that require an expanded depth and breadth of learning aiming to enhance the learners' conceptualisations of the provided material of a specific topic.

## 1st GROUP CONSULTATION MEETING

### Programme Presentation

Leading companies today are rethinking the role of information security in their organizations. They realize that in a digital world, cybersecurity is the key to safeguarding their most precious assets—intellectual property, customer information, financial data, and employee records, among others. But far more than a defensive measure, companies also know that cybersecurity can better position their organization with business partners, customers, investors, and other stakeholders.

The European cybersecurity market is about 25% (i.e. about €17bln) of the world market (estimated at €70bln in 2015), with an average yearly growth slightly larger than 6%, when the world market is growing at about 10%/year. Recent study compiled by Europe's cybersecurity industry leaders pointed out that Europe is in danger of falling behind in the international digital economy field.

The Master in Cybersecurity is a cutting-edge program, designed for those wishing to develop a career as a cyber-security professional, or to take a leading technical or managerial role in an organization critically dependent upon data and information communication technology. Students will develop an advanced knowledge of information security and an awareness of the context in which information security operates in terms of safety, environmental, social and economic aspects. They will gain a wide range of intellectual, practical and transferable skills, enabling them to develop a flexible professional career in IT.

Key elements of this postgraduate degree are: the *real life experience* given by the opportunity to apply their theoretical knowledge through specialized virtual and remote security laboratories in which they will be able to carry out activities such as reconnaissance, network scanning and exploitation exercises, and investigate the usage and behavior of security systems such as Intrusion Detection and Prevention Systems thus becoming confident in the practical application of the latest tools; the *high-level insight* that will enhance student's ability to research and design creative cyber security solutions to address business problems; *hands-on skills* through experimentation with security techniques, cryptographic algorithms, cyber forensics building an ethical hacking environment; and *flexibility* since students will also be able to choose either the completion of a Master thesis or to complete a Research methods course and two elective courses.

Students undertake modules to the value of 90 ECTS credits.

## COURSE PRESENTATION THROUGH THE STUDY GUIDE

The objective of this course is to introduce concepts and techniques related to the topics of incident response and forensic analysis. An incident is a matter of when, not if, a compromise or violation of an organization's security will happen. Today's cyber threats have become very complex and require additional resources and skills to mitigate detect analyse and respond to.

The uniqueness and complexity of these threats is often beyond the capabilities of ordinary IT teams. Detecting these incidents therefore requires additional skills such as forensics, malware analysis and threat detection which help decipher how this threat operates and therefore how they can be prevented and mitigated.

Forensic analysis techniques are introduced, along with standard tools that are used to carry out computer forensic investigations, with emphasis on digital evidence acquisition, handling and analysis in a forensically sound way.

Upon successful completion of this course students should be able to:

- Define and describe the main phases of incident response
- Evaluate incident data and indicators of compromise (IOC) to determine the correct responses to an incident
- Identify different kinds of attacks methods to counter their effects
- Describe the different phases of incident response – preparation, identification, containment, eradication, recovery, follow-up
- Explain the principles of evidence collection and the chain of custody
- Identify and evaluate key forensic analysis techniques
- Describe the application of such techniques to real situations and the connection with incident response
- Describe the ways in which cybercrime investigations use forensic analysis and legal issues regarding evidence collection.

## Recommended time for the student to work

Approximately 5 hours for the study guide

## INTRODUCTION TO INCIDENT RESPONSE AND DIGITAL FORENSICS

1<sup>st</sup> Week

### Summary

The introductory unit allows the students to familiarise themselves with the concepts of incident response and digital forensics. Incident response is employed in order to recover from a cybersecurity breach. The identification, containment, and management of a security breach require adequate preparation from an organisational perspective. The principles and goals of incident response are presented and the role of digital forensics when responding to an incident is discussed.

Digital forensics techniques and procedures are adopted, when an organisation responds to a cybersecurity incident. Therefore, the second part of this unit presents the principles and objectives of digital forensics as well as the code of conduct in digital investigations. The students will also be introduced to the properties of digital evidence in order to develop an understanding on the nature and sensitivity of digital evidence.

### Introductory Remarks

Not every crime committed with a computer is a computer crime. If someone steals a telephone access code and makes a long-distance call, the code he has stolen is checked by a computer before the call is processed. Nevertheless, such a case is more appropriately treated as “toll fraud,” not computer crime. It would, however qualify as cyber crime if the code was obtained as a result of hacking into a computer system. Although this example appears straightforward, many cases are not so neatly categorized. A bank employee who steals money from a cash drawer is embezzling. A bank employee who writes a computer program to randomly steal very small amounts from numerous accounts may also be embezzling, yet committing (and prosecuting) this offense may require a working knowledge of the bank’s computer system. As a result, such a crime may reasonably be characterized as a computer offense.

According to the U.S. Department of Justice, computers generally play three distinct roles in a criminal case. First, a computer can be the target of an offense. This occurs when conduct is designed to take information without authorization from, or cause damage to, a computer or computer network. The Melissa and Explore.Zip.Worm viruses, along with hacks into the

White House and other Web sites, are examples of this type of offense. Second, a computer can be incidental to an offense yet still be significant in terms of law enforcement purposes. For example, drug traffickers may store transactional data (such as names, dates, and quantities) on computers, rather than in paper form. Finally, a computer can be the tool used for committing an offense (such as fraud or the unlawful sale of prescription drugs over the Internet).

For the purposes of this text, *digital evidence* is defined as any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi (adapted from Chisum, 1999). The data referred to in this definition are essentially a combination of numbers that represent information of various kinds, including text, images, audio, and video.

Forensic Science provides a large body of proven investigative techniques and methods. By forensic we mean a characteristic of evidence that satisfies its suitability for admission as fact and its ability to persuade based upon proof (or high statistical confidence).

Analyzing the aftermath of a computer intrusion takes far longer than it takes a perpetrator to commit the crime. It is often the speed of the response that determines the outcome; and the more prepared an organization is when an incident first occurs, the quicker it can respond in the incident's wake. With the ever-increasing use of information technology (IT), organizations around the globe are facing the challenge of protecting valuable resources from a never-ending onslaught of threats. Computers, and the networks that connect them, process, store, and transmit information that is crucial for successful day-to-day operations and are therefore inviting targets for hackers and malicious code. The protection of critical IT resources requires not only adopting reasonable precautions for securing these systems and networks, but also the ability to respond quickly and efficiently when system and network security defenses have been breached. Unfortunately, responding to computer security incidents is generally not an easy endeavor. Proper incident response requires technical knowledge, communication, and coordination among personnel in charge of the response process. In information technology, incident refers to an adverse event in an information system and/or network or the threat of the occurrence of such an event. Examples of incidents include unauthorized use of another user's account, unauthorized use of system privileges, and execution of malicious code that destroys data. Other adverse events include floods, fires, electrical outages, or excessive heat that results in system crashes. Adverse events such as natural disasters and powerrelated disruptions, though certainly undesirable incidents, are not generally within the scope of xx Introduction a526367 FM.qxd 3/21/03 3:37 PM Page xx incident response teams and are better addressed by an organization's business continuity (contingency) plans. For the

purpose of incident response, therefore, the term incident refers to an adverse event that is related to information security.

In order to be useful in an investigation, digital evidence must be preserved and examined in a forensically sound manner. Some practitioners of digital forensics think that a method of preserving or examining digital evidence is only forensically sound if it does not alter the original evidence source in any way. This is simply not true. Traditional forensic disciplines such as DNA analysis show that the measure of forensic soundness does not require the original to be left unaltered. When samples of biological material are collected, the process generally scrapes or smears the original evidence. Forensic analysis of the evidential sample further alters the sample because DNA tests are destructive. Despite the changes that occur during preservation and processing, these methods are considered forensically sound and DNA evidence is regularly admitted as evidence. In digital forensics, the routine task of acquiring data from a hard drive, even when using a hardware write-blocker, alters the original state of the hard drive. Such alterations can include making a hidden area of the hard drive accessible, or updating information maintained by Self-Monitoring, Analysis, and Reporting Technology (S.M.A.R.T.) on modern hard drives. Furthermore, most methods of acquiring the contents of memory on live computer systems and mobile devices alter or overwrite portions of memory, but this is a generally accepted practice in digital forensics. In fact, courts are starting to compel preservation of volatile computer data in some cases, which requires digital investigators to preserve data on live systems.

Digital evidence as a form of physical evidence creates several challenges for digital forensic analysts. First, it is a messy, slippery form of evidence that can be very difficult to handle. For instance, a hard drive platter contains a messy amalgam of data—pieces of information mixed together and layered on top of each other over time. Only a small portion of this amalgam might be relevant to a case, making it necessary to extract useful pieces, fit them together, and translate them into a form that can be interpreted. Second, digital evidence is generally an abstraction of some digital object or event. When a person instructs a computer to perform a task such as sending an e-mail, the resulting activities generate data remnants that give only a partial view of what occurred (Venema & Farmer, 2000).

## Aim/Objectives

This course allows the students to familiarise themselves with the concepts of incident response and digital forensics.

## Learning Outcomes

After the successful completion of this week, students should be able to:

- Familiarise with the importance of incident response
- Develop a critical understanding of the incident response lifecycle
- Develop a background in the fundamentals of digital forensics
- Identify the basic purposes and priorities of digital forensics
- Familiarise with the concept of digital evidence in the context of incident response

## Key Words

Incident response	Business continuity	Disaster recovery	Digital forensics
Code of conduct	Lifecycle	Investigation	Digital Evidence

## Annotated Bibliography

### Basic

Chapter 1 of Casey, E, 2011. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. Academic Press Inc (London) Ltd.

The Internet is the largest operating computer network in the world. Because it is largely a public network, threats may come from all corners of the globe. To protect themselves against the constant threat of hackers, crackers, and malicious code, organizations often make use of firewalls, antivirus software, and intrusion detection systems. Despite sophisticated defensive measures, however, computers and the networks that connect them are still subject to frequent attacks. As a result of this unfortunate fact, organizations and governments around the world must remain prepared to respond to a variety of threats by any computer security incident that circumvents security measures.

Kruse WG II, Heiser JG, Computer Forensics Incident Response Essentials, Addison Wesley 2001

Lillard VT, 2010, Digital Forensics for Network, Internet, and Cloud Computing: A Forensic Evidence Guide for Moving Targets and Data, Elsevier Inc.

### Supplementary

- PowerPoint Presentation: Introduction to incident response and digital forensics

### Suggestions for further reading

- Prosite C and Mandia K, 2014, Incident Response and Computer Forensics, The McGraw-Hill Companies, 3<sup>rd</sup> edition
- Chisum, J. W. (1999). Crime reconstruction and evidence dynamics. Presented at the Academy of Behavioral Profiling Annual Meeting. Monterey, CA.
- Venema, W., & Farmer, D. (2000). Forensic computer analysis: an introduction. Doctor Dobb's Journal. Available from <http://www.ddj.com/documents/s=881/ddj0009f/0009f.htm>.
- Schweitzer D, Incident Response, Computer Forensics Toolkit, Wiley
- Cranor L F, 2008, A framework for reasoning about the human in the loop. In Proceedings of the 1st Conference on Usability, Psychology, and Security, pages 1–15, Berkeley, CA, USA, USENIX Association
- CREST Incident Response Guide, 2013, <https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf>

## **Self-Assessment Exercises**

### **Exercise 1.1**

Presentation/ Critical discussion on the Introduction to incident response and digital forensics

### **Exercise 1.2**

Case study group discussion on incident response: *The students are provided with a case study related to an incident response scenario. They are required to work on a predefined set of questions and participate in an online discussion forum to exchange their views and discuss the answers to the questions.*

## **Recommended time for the student to work**

15 hours

## PLANNING AND HANDLING INCIDENT RESPONSE

2<sup>nd</sup> Week

### Summary

This unit material aims to provide the students with an in-depth set of material to familiarise with common defensive technologies and their role to planning and handling an incident. The current intrusion detection and prevention mechanisms are discussed, as well as firewalls, darknets and honeypots.

The administrative and technical controls are compared, and the physical security controls are evaluated. After the detection methods, the response process is analysed, and the different roles involved in organisations during an incident response. At this stage the preparation for disaster recovery is also introduced to the students.

### Introductory remarks

Prior to the early 1990s, threats to computer security (besides human errors) were mainly physical and environmental, consisting of physical damage and insider attacks, such as fire, water, or theft. These types of threats are understood fundamentally and are easily controlled through the use of traditional methods and contingency planning. Today, a new category of computer security threats has become equally as important to understand and control. These threats include transgressions by unauthorized intruders and users who exploit system vulnerabilities, computer viruses, worms, and Trojan horses. Several factors have contributed to the growing presence of these threats, such as the following:

- Society's increased reliance on computers. Today, nearly every organization, both public and private, relies on computers and networks for communication. Because of this increased reliance, many agencies would suffer great losses to productivity should their systems become unavailable. Due to system complexity, reliance on computer systems often presents unanticipated risks and vulnerabilities.
- Malicious code. Computer viruses, Internet mail worms, and Trojan horses in particular, continue to wreak havoc in personal computer security. As bad as this problem is at present, malicious code difficulties will only get worse. This is primarily a result of the proliferation of personal computers (with minimal built-in security controls), LANs, and a

blatant disregard for safe computing practices. The number of variants and copycats of viruses has also increased and shows no signs of abating.

- Wide area networks (WANs). The use of WANs, linking governments, businesses, and educational institutions, continues to grow. An efficient response to a computer security incident is important for agencies linked via large networks such as an intranet or the Internet. Because of their interconnectivity, a compromise of one computer can affect other systems that are connected to the network but are located in different organizations, resulting in possible legal or financial ramifications. Incident response teams are aware that intruder attempts to penetrate systems occur daily at numerous sites throughout the United States, yet many organizations remain unaware that their systems have been penetrated or have been used as springboards for attacks on other systems. Reduced barriers to hacking. Computing power is readily available, as is broadband connectivity. Hackers can download tools readily from the Internet, so relatively unskilled attackers can launch very sophisticated attacks.

Today, being prepared to handle a computer security incident has become a top priority for most system administrators. As businesses increase their online presence and their dependency on information systems' assets, the number of computer incidents also rises. These organizations are finally recognizing their need to adapt their security positions accordingly. This is accomplished in three stages.

First, organizations must develop and implement security plans and controls in a proactive effort. Second, they must work to ensure that their plans and controls are effective by continually reviewing and modifying them to guarantee that appropriate security is always in place. Finally, when controls are bypassed, either intentionally or unintentionally, organizations must be prepared to act quickly and effectively to minimize the impact of these lapses.

The prime objective of these security measures is to prevent an operational security problem from becoming a business problem that impacts revenue. Administrators and other users can obtain guidelines in this book to preplan a response to incidents and minimize any negative impact to a business. Waiting until an incident has occurred is naturally too late to begin planning how to address such an event. Incident response planning requires maintaining both administrative and technical roles. Each party must be familiar with the other's role, responsibilities, and capabilities.

Having a computer security incident response capability means that an organization is prepared to detect and counter computer security incidents in a skilled and efficient manner.

Such a capability is a combination of technically skilled people, policies, and techniques with the aim of constituting a proactive approach to handling computer security incidents.

Having an incident response capability with traditional computer security elements can provide organization-wide protection from damaging incidents, saving the organization valuable resources and permitting it to take better advantage of the latest computer technology. Many businesses, organizations, and government agencies have implemented incident response capabilities with great success, generally focusing on the following areas:

- Efficient response. Efficiency is one of the most important aspects of a computer security incident response capability. Without an efficient capability, incident response is disorganized and ineffective, with the organization maintaining higher expenses and leaving vulnerabilities open and unprotected. For example, uneducated responses to small outbreaks of computer viruses can actually make their effects far worse, resulting in hundreds of computers being infected by the response team itself. A proper computer security incident response capability helps in the management of incident response expenses that are otherwise difficult to track, makes risk assessment more accurate, and improves user training and awareness with regard to computer security. Conversely, an inefficient incident response effort can perpetuate existing problems and even exacerbate them.
- Centralization. A security incident response capability must utilize centralized means for reporting and handling incidents. While this undoubtedly increases efficiency, it also permits a more accurate assessment of the incidents, such as whether they are related (in order to more quickly avert possible widespread damage). By virtue of centralization, incident response capability expenses and overhead can be kept down, and duplication of effort can be reduced (possibly eliminated entirely). Organizations may find a significant cost savings as a result.
- Improved user awareness. The benefits of an incident response capability include enhanced user awareness of threats and knowledge of appropriate controls. An incident response capability will help an organization identify vulnerabilities and issue computer security alerts. Information regarding security awareness can be disseminated throughout the organization by using a variety of mechanisms such as a company intranet, seminars, and training workshops. Such information greatly improves the users' ability to manage their systems efficiently and securely.

## Aim/Objectives

This unit material aims to provide the students with an in-depth set of material to familiarise with common defensive technologies and their role to planning and handling an incident.

## Learning Outcomes

After the successful completion of this week, students should be able to:

- Develop a critical understanding of incident handling by using appropriate methods
- Compare and contrast defensive technologies
- Develop a critical understanding on securing systems with intrusion detection systems
- Critically discuss the different types of network-based evidence
- Familiarise with the issues involving network investigations
- Identify the importance of intrusion detection systems in network investigations

## Key Words

Incident response	Detection Methods	Incident Reporting	Incident Response Plan
Incident Response Process	Intrusion Detection	Intrusion Prevention	Investigative Procedure
Disaster recovery	First Response		

## Annotated Bibliography

### Basic

- Oriyano SP and Solomon M G, 2014, *Hacker Techniques, Tools, and Incident Handling*, Jones & Bartlett Learning, 2<sup>nd</sup> edition.

### Supplementary

- PowerPoint Presentation on planning and handling incident response that covers the material for weeks 3 and 4.

### Suggestions for further reading

- Nikkel B.J., 2005, Generalizing sources of live network evidence, *Digital Investigation*, Volume 2, Issue 3, pp. 193–200

- Turner P, 2007, Applying a forensic approach to incident response, network investigation and system administration using Digital Evidence Bags, *Digital Investigation*, Volume 4, Issue 1, pp. 30-35
- Schneier B, 2014, The Future of Incident Response, *IEEE Security & Privacy*, Volume 12, Issue 5, p 96
- Stallings, W., 2017. Network security essentials: applications and standards. Pearson Education India, 6<sup>th</sup> edition
- Chappell L and Combs G, 2017, *Wireshark 101: Essential Skills for Network Analysis*, Second Edition, Chappell University, ISBN: 978-1893939752

## **Self-Assessment Exercises**

### **Exercise 2.1**

Online group discussion on the roles and processes involved in incident response in various organisations.

### **Exercise 2.2**

Practical exercise: Introduction to Wireshark. The students will be provided with a network capture to familiarise with the packet inspection and analysis with Wireshark.

## **Recommended time for the student to work**

15 hours

## THE INCIDENT REPORTING PROCESS

3<sup>rd</sup> Week

### Summary

Despite sophisticated defensive measures, however, computers and the networks that connect them are still subject to frequent attacks. As a result of this unfortunate fact, organizations and governments around the world must remain prepared to respond to a variety of threats by any computer security incident that circumvents security measures.

### Introductory remarks

All organizations need to establish and implement an internal incident response capability. Intrusions are only one form of computer security incident.

Remember, a computer security incident is any adverse event wherein some aspect of a computer system is threatened. This could include loss of data confidentiality, disruption of data integrity, and disruption or denial of service. The types of incidents are classified into low, medium, or high levels depending on their severity.

Low-level incidents are the least severe and should be resolved within one working day after the event occurs. These include

- Loss of passwords
- Suspected unauthorized sharing of accounts
- Misuse of computer hardware
- Unintentional computer actions
- Unsuccessful scans or probes

Mid-level incidents are more serious and should be handled the same day the event occurs (normally within two to four hours of the event). These include

- Property destruction related to a computer incident
- Illegal download of copyrighted music/unauthorized software
- Violation of special access
- Unauthorized use of a system for processing or storing personal data
- An act resulting from unfriendly employee termination
- Illegal building access
- Personal theft (moderate in value) related to a computer incident

High-level incidents are the most serious. Because of the gravity of these situations and the likelihood of damage resulting to the organization's bottom line, these types of incidents should be handled immediately. They include

- Property destruction related to a computer incident
- Child pornography
- Pornography
- Personal theft (higher in value than a mid-level incident) related to a computer incident
- Suspected computer break-in
- Denial of Service (DoS) attacks
- Illegal software download
- Malicious code (for example, viruses, worms, Trojan horses, and malicious scripts)
- Unauthorized use of a system for processing or storing of prohibited data
- Changes to system hardware, firmware (for example, BIOS), or software without the system owner's authorization
- Any violation of the law

Other types of incidents may include isolated cases of viruses or misuse of computer equipment,

unintentional actions, and common, unsuccessful scans or probes. When faced with a security incident, an organization should be able to respond in a manner that both protects its own information and helps protect the information of others that might be affected by the incident.

### **Assessment and Containment**

Every organization needs to develop internal reporting procedures that define the actions that must be taken in responding to and reporting computer security incidents. At a minimum, internal procedures should include the organization chain of authority or hierarchy and require the involvement of all of the organization's computer security personnel. These procedures also require the following:

- Preservation of evidence
- Assessment
- Containment and recovery actions
- Damage determination
- Report documentation
- Lessons learned

- Identification of corrective actions required by the organization's security programs

Organizations should distribute computer security procedures to all appropriate personnel responsible for identifying, reporting, or handling high-level incidents. Responsible parties should be instructed to read and become familiar with the incident reporting policy. Individuals assigned to incident handling or reporting may be organized into a response team that becomes active when a breach is identified.

All organizational networks must be monitored on an ongoing basis. It is not necessary to obtain and install intrusion detection devices or software for every server. Only the most critical locations need to have intrusion detection installed. As soon as suspicious activity is detected, qualified personnel designated to respond must be notified to take immediate action.

The upper-level management personnel authorized to take containment actions should assess the event and take appropriate action. This may include shutting down a system within a reasonable time after discovery of an intrusion to contain any future damage. In extreme instances, if the incident response team fails to adequately respond or if the problem is not contained in a timely manner (usually 12 hours), the organization's chief information officer (CIO) or designate may issue an order to bring the entire system down. Reporting directly to the CIO or upper-level management should occur in cases where a preliminary assessment indicates that significant damage to organizational resources may have occurred. Upon confirmation, the incident response actions must be implemented immediately. The unavailability of any official in the reporting chain should not delay the continuation of the incident notification or response process.

Powering down a computer system in a manner that will not corrupt the integrity of existing files is a complicated computer security procedure. In the event of a suspected computer incident, great care must be taken to preserve evidence in its original state. While it may seem that simply viewing files on a system would not result in alteration of the original media, merely opening a file changes it. In a legal sense, it is no longer the original evidence and at that point may be inadmissible in any subsequent legal or administrative proceedings.

Opening a file also alters the time and date it was last accessed. On the surface this may not seem an important issue; however, it could later become extremely important in the determination of who committed the violation and when it occurred. Isolation of the computer system is ideal, but if this cannot be accomplished due to operational requirements, no attempts should be made to recover or view files at the local level.

The isolation of a computer system so that evidence is not lost is of the utmost importance.

Consideration must also be given to other storage media, handwritten notes, and documents found in the vicinity of the computer involved. These items can be of value in an ensuing investigation. Computer disks, CD-ROMs, tape storage media, and/or additional hard drives found in the area of the computer also must be isolated and protected.

### **Building an Incident Response/Forensic Toolkit**

There are two important issues when it comes to collecting digital evidence: authenticity and integrity. You need to be able to demonstrate that the evidence is what you say it is, came from where you say it came from, and has not been modified since you obtained it. How you collect and document evidence to preserve its authenticity and reliability depends on the circumstances and the computer systems you are dealing with. A dependable set of tools is invaluable for those in charge of incident response.

### **Aim/Objectives**

This chapter aims to introduce students with the basic steps that all organizations should take to prepare their response to incidents.

### **Learning Outcomes**

After the successful completion of this week, students should be able to:

- Describe the basic steps all organizations should follow in preparation for responding to incidents
- Verify that a security incident has occurred while preserving key evidence
- Use specific types of response measures useful against modern day attacks
- Recognise the importance of building a forensic toolkit

### **Key Words**

Incident response	Forensic toolkit	Key evidence	
-------------------	------------------	--------------	--

### **Annotated Bibliography**

#### **Basic**

Chapter 1 of Schweitzer, D., 2003. *Incident response: computer forensics toolkit* (p. 26). New York: Wiley.

In this chapter students will learn to recognize the signs of an incident, the steps required to prepare for an incident, the process of incident verification, preservation of key evidence, specific response measures and how to build a toolkit.

### **Suggestions for further reading**

- Nikkel B.J., 2005, Generalizing sources of live network evidence, Digital Investigation, Volume 2, Issue 3, pp. 193–200
- Turner P, 2007, Applying a forensic approach to incident response, network investigation and system administration using Digital Evidence Bags, Digital Investigation, Volume 4, Issue 1, pp. 30-35
- Schneier B, 2014, The Future of Incident Response, IEEE Security & Privacy, Volume 12, Issue 5, p 96
- Stallings, W., 2017. Network security essentials: applications and standards. Pearson Education India, 6<sup>th</sup> edition
- Chappell L and Combs G, 2017, Wireshark 101: Essential Skills for Network Analysis, Second Edition, Chappell University, ISBN: 978-1893939752

### **Recommended time for the student to work**

15 hours

## CYBERCRIMES AND DIGITAL INVESTIGATIONS

4<sup>th</sup> Week

### Summary

This unit aims to cover two weeks. It introduces cybercrimes and their nature, then expands on the relevant terminology and the different types of cybercrimes. Computers can be the target for attack and penetration, the tool to perform a cybercrime or the storage area to save cybercrime related information.

The role of technology in cybercrime evolution is presented and the different types of cybercrimes are analysed.

This section also aims to cover international procedures, best practices and compliance in relation to the investigation of cybercrimes. The case management to maintain the chain of custody is discussed in depth leading to the essential background knowledge required for the establishment and management of a digital forensics' laboratory.

### Introductory remarks

#### Computer-Integrity Crimes

The first category of offenses concerns "hard-core" cybercrime, criminalizing offenses against the confidentiality, integrity, or availability of computer data or computer systems.

The Council of Europe Convention on Cybercrime introduces the following five offenses against the confidentiality, integrity, and availability of computer data and systems:

1. Illegal access, that is, intentional access to the whole or any part of a computer system without right (Article 2)
2. Illegal interception, being the intentional interception without right made by technical means of nonpublic transmissions of computer data to, from, or within a computer system (Article 3)
3. Data interference, that is, the intentional damaging, deletion, deterioration, alteration, or suppression of computer data without right (Article 4)
4. System interference, being intentionally seriously hindering without right the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data (Article 5) and

5. Misuse of devices, that is, the production, sale, procurement for use, import, distribution, or otherwise making available of a device or password or access code with the intent that it be used for the purpose of committing any of the offenses established in articles 2-5 (Article 6).

“Computer system” is defined as “any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data,” and “computer data” is defined as meaning “any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.”

The second category of offenses addressed by the Cybercrime Convention are computer-assisted crimes. Contrary to computer-integrity crimes, which are effectively new forms of crime that cannot be committed in the absence of computers or computer networks, and where the computer usually is the target of the crime, computer-assisted crimes are traditional crimes in which the computer is “merely” a tool. They nevertheless merit attention from the legislator, if traditional crimes are formulated in a way that precludes their application to the digital world.

The third category of offenses in the Cybercrime Convention relates to content related crimes. They are similar to the computer-assisted crimes in that they relate to traditional offenses and that computers are tools rather than targets, but they differ from them in that it is the content of data rather than the result of an action that is the core of the offence. The only content-related offence that the parties involved in drafting the Convention could agree upon was child pornography.

### **Computer-Integrity Crimes**

The first and most obvious cybercrime is hacking or, in the Convention’s term, “illegal access”: the intentional “access to the whole or any part of a computer system without right” (article 2 Convention; similarly, article 2 Framework Decision). When implementing this provision, states may provide that hacking is only punishable when security measures are infringed, when committed with dishonest intent, or when the computer is part of a network.

Article 3 of the Convention criminalizes the intentional “interception without right, made by technical means, of nonpublic transmissions of computer data to, from or within a computer system.”

Data interference is the intentional “damaging, deletion, deterioration, alteration or suppression of computer data without right” (art. 4 Convention). Parties may pose a requirement of serious harm for this conduct to be punishable. A typical example is computer viruses that alter in any way certain data in a computer. Data interference is also covered by

art. 4 of the EU Framework Decision, which uses similar language, with the addition of “rendering inaccessible” computer data as an act of data interference.

System interference refers to the intentional “serious hindering without right of the functioning of a computer system” through computer data (art. 5 Convention). This comprises computer sabotage, but also denial-of-service (DoS) attacks that block access to a system. It does not, however, criminalize spam—sending unsolicited, commercial, or other email—except “where the communication is intentionally and seriously hindered”; parties may, however, go further in sanctioning spam, for example by making it an administrative offence, according to the Explanatory Report (§ 69). System interference is also covered by art. 3 of the EU Framework Decision.

Article 6 of the Convention criminalizes “misuse of devices,” which includes hardware as well as software and passwords or access codes. It is aimed at combating the subculture and black market of trade in devices that can be used to commit cybercrimes, such as virus-making or hacking tools. “To combat such dangers more effectively, the criminal law should prohibit specific potentially dangerous acts at the source, preceding the commission of offenses” (Explanatory Report, § 71). Article 6 is a complex provision, establishing as criminal offenses under its domestic law, when committed intentionally and without right

- a) the production, sale, procurement for use, import, distribution or otherwise making available of
  - i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offenses established in accordance with the above Articles 2 through 5;
  - ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offenses established in Articles 2 through 5; and
- b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offenses established in Articles 2 through 5.

### **Computer-Assisted Crimes**

Art. 7 of the Cybercrime Convention criminalizes computer-related forgery:

the intentional and unlawful “input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible.” Parties may pose a requirement of dishonest intent.

Like forgery, fraud can also be committed with the assistance of computers: the intentional and unlawful “causing of a loss of property to another person by [interfering with computer data or a computer system] with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person” (art. 8 Convention). The term “loss of property” is used here as a broad notion, comprising loss of money, tangibles, and intangibles with an economic value (§ 88 Explanatory Report).

### **Content-Related Cybercrimes**

Offences relating to the possession and distribution of child pornography are probably the most litigated and certainly the most notorious of cyber offenses. Art. 9 of the Convention stipulates that the production, making available, distribution, procurement, and possession of child pornography should be criminalized when committed through use of computers. Parties can, however, decide not to criminalize procurement or possession. The age limit for child pornography advised by the Convention is 18 years; it must in any case be at least 16 years (art. 9(3)). An important innovation is that also “virtual child pornography” is criminalized: computer-generated or computer-morphed images made to look like child pornography, in the Convention’s terminology: “realistic images representing a minor engaged in sexually explicit conduct” (art. 9(2)). The rationale of this is not so much direct protection against child abuse, as no children need to be actually abused for virtual images, but to prevent that such images “might be used to encourage or seduce children into participating in such acts, and hence form part of a subculture favoring child abuse” (§ 102 Explanatory Report).

The court set out specific factors which were capable of aggravating the seriousness of a particular offence:

- 1) The images had been shown or distributed to a child
- 2) There were a large number of images
- 3) The way in which a collection of images was organized on a computer might indicate a more or less sophisticated approach on the part of the offender to, say, trading
- 4) Images were posted on a public area of the Internet 5. If the offender was responsible for the original production of the images, especially if the child or children were family members or located through the abuse of the offender’s position of trust, for example, as a teacher
- 5) The age of the children involved

## Aim/Objectives

This chapter tackles the challenge in giving a European perspective of cybercrime law by presenting the two major initiatives to increase consistency across countries specifically, the European legal framework—in particular the Cybercrime Convention—and relevant national legislation. We start with a brief overview of the sources of European and national cybercrime law. We then focus on the various cybercrime offenses—computer-integrity crimes, computer-assisted crimes, content-related crimes, and some other offenses.

## Learning Outcomes

After the successful completion of this week, students should be able to:

- Develop a critical understanding about the different types of cybercrime and how traditional criminological theories are applied to cybercrime analysis.
- Familiarise with relevant legislation, processes and procedures

## Key Words

Cybercrime	Cybercrime Convention	Legal trends	Legislation
------------	--------------------------	--------------	-------------

## Annotated Bibliography

### Basic

Chapter 5 of Casey, E, 2011. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. Academic Press Inc (London) Ltd.

Watson D and Jones A, 2013. Digital Forensics Processing and Procedures: Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements. Syngress Publishing.

### Supplementary

- Presentation on cybercrimes and digital investigations that covers the material for weeks 5 and 6.

## **Suggestions for further reading**

- Jones A and Valli C, 2008, Building a Digital Forensic Laboratory. Butterworth-Heinemann, Newton, MA, USA.
- NIJ Guide, 2001, Electronic Crime Scene Investigation: A Guide for First Responders by The National Institute of Justice
- Angelopoulou O, Vidalis S, 2013, Towards 'Crime Specific' Digital Investigation Methodologies, Cyberforensics 2013, Cardiff, UK
- Silde A, Angelopoulou O, 2014, Digital Forensic Cyberstalker Profiling Methodology, Proceedings of INCoS 2014: Intelligent Networking and Collaborative Systems, Salerno, Italy
- Angelopoulou O, Vidalis S, Robinson I, 2012, Who are you today? Profiling the ID theft fraudster, Proceedings of the 11th ECIW: European Conference on Information Warfare and Security, Laval, France
- Casey E, 2011, Digital Evidence and Computer Crime; Forensic Science, Computers and the Internet, Eoghan, Academic Press
- Maras M.H., 2012, Computer Forensics, Cybercriminals, Laws and Evidence, ISBN: 1449600727
- Stephenson, P., 2002, Collecting Evidence of a Computer Crime, Computer Fraud & Security, Volume 2002, Issue 11, Pages 17-19
- Holt TJ, Bossler AM, Seigfried-Spellar K C, 2018, Cybercrime and Digital Forensics. London: Routledge.

## **Self-Assessment Exercises**

### **Exercise 4.1**

Practical task that aims to familiarise the students with the Autopsy interface in Kali Linux. The students will practise with the tool, create a case and run a basic analysis of an image.

## **Recommended time for the student to work**

15 hours

## Summary

This section also aims to cover international procedures, best practices and compliance in relation to the investigation of cybercrimes. The case management to maintain the chain of custody is discussed in depth leading to the essential background knowledge required for the establishment and management of a digital forensics' laboratory.

## Introductory remarks

The goal of any investigation is to uncover and present the truth. Although this chapter will deal primarily with truth in the form of digital evidence, this goal is the same for all forms of investigation whether it be in pursuit of a murderer in the physical world or trying to track a computer intruder online. As noted in the Introduction, when evidence is presented as truth of an allegation, it can influence whether people are deprived of their livelihoods and liberties, and potentially whether they live or die. This is reason enough to seek to use trusted methodologies and techniques to ensure that the analysis, interpretation, and reporting of evidence are reliable, objective, and transparent.

Digital investigations inevitably vary depending on technical factors such as the type of computing or communications device, whether the investigation is in a criminal, civil, commercial, military, or other context, and case-based factors such as the specific claims to be investigated. Despite this variation, there exists a sufficient amount of similarity between the ways digital investigations are undertaken that commonalities may be observed. These commonalities tend to be observed from a number of perspectives, with the primary ways being process, principles, and methodology.

## Digital Investigation Process Models

Early attempts to describe how one conducted a digital investigation tended to focus on practical stepwise approaches to solving particular investigative challenges, within the context of particular technical computing environments. Numerous subsequent efforts determined that, when attempting to conceive of a general approach to describe the investigation process within digital forensics, one should make such a process generalizable. This led to the proposal of a number of models for describing investigations, which have come to be known as "process models."

The motivations for developing process models are numerous. Such process models serve as useful points of reference for reflecting on the state and nature of the field, as a framework for training and directing research, and for benchmarking performance against generally accepted practice. Using a formalized methodology encourages a complete, rigorous investigation, ensures proper evidence handling, and reduces the chance of mistakes created by preconceived theories, time pressures, and other potential pitfalls. Another purpose of these models is to refine our understanding of what is required to complete a comprehensive and successful investigation in a way that is independent of a particular technology in corporate, military, and law enforcement environments. An effective process model identifies the necessary steps to achieve goals and can be applied to new technologies that become a source of digital evidence. Finally, these models are useful for the development of case management tools, Standard Operating Procedures (SOPs), and investigative reports.

Ultimately, these process models are intended to serve digital investigations, and not to dictate. Every investigation is unique and can bring unforeseeable challenges, so process models and other methodologies should not be viewed as an end-point but rather as a framework or foundation upon which to build. Furthermore, as with any tool, investigative process models can be useful under certain circumstances but have limitations. Therefore, it is important to be familiar with the various process models and the extent to which they apply to a given situation.

The most common steps for conducting a complete and competent digital investigation are:

- Preparation: Generating a plan of action to conduct an effective digital investigation, and obtaining supporting resources and materials.
- Survey/Identification: Finding potential sources of digital evidence (e.g., at a crime scene, within an organization, or on the Internet). Because the term identification has a more precise meaning in forensic science relating to the analysis of an item of evidence, this process can be more clearly described as survey of evidence. Survey is used throughout this chapter when referring to this step.
- Preservation: Preventing changes of in situ digital evidence, including isolating the system on the network, securing relevant log files, and collecting volatile data that would be lost when the system is turned off. This step includes subsequent collection or acquisition.<sup>1</sup>
- Examination and Analysis: Searching for and interpreting trace evidence. Some process models use the terms examination and analysis interchangeably.
- Presentation: Reporting of findings in a manner which satisfies the context of the investigation, whether it be legal, corporate, military, or any other.

## Chain of Custody

One of the most important aspects of authentication is maintaining and documenting the chain of custody (a.k.a. continuity of possession) of evidence. Each person who handled evidence may be required to testify that the evidence presented in court is the same as when it was processed during the investigation. Although it may not be necessary to produce at trial every individual who handled the evidence, it is best to keep the number to a minimum and maintain documentation to demonstrate that digital evidence has not been altered since it was collected. A sample chain of custody form is shown in the following Figure , recording the transfer of evidence, when, where, and why.

cmdLabs Continuity of Possession Form				
Case Number:	2010-05-27-00X	Client/Case Name: Digifinger Intrusion		
Evidence Type:	hard drive	Evidence Number: 0023		
Details:	Mac storage <network share>			
Date of Transfer	Transferred From	Transferred To	Location of Transfer	Action Taken by Recipient
5/27/10	signature print name <b>Sam Spade</b>	signature print name <b>Philip Marlowe</b>	Digifinger HQ Linthicum MD	Collected evidence for examination
	signature print name	signature print name		

Without a solid chain of custody, it could be argued that the evidence was handled improperly and may have been altered, replaced with incriminating evidence, or contaminated in some other fashion. Potential consequences of breaking the chain of custody include misidentification of evidence, contamination of evidence, and loss of evidence or pertinent elements.

Chain of custody and integrity documentation are important for demonstrating the authenticity of digital evidence. Proper chain of custody demonstrates that digital evidence was acquired from a specific system and/or location, and that it was continuously controlled since it was collected. Thus, proper chain of custody documentation enables the court to link the digital evidence to the crime. Incomplete documentation can result in confusion over where the digital evidence was obtained and can raise doubts about the trustworthiness of the digital evidence.

Integrity documentation helps demonstrate that digital evidence has not been altered since it was collected. In situations where the hash value of digital evidence differs from the original, it may be possible to isolate the altered portions and verify the integrity of the remainder. For example, bad sectors on a hard drive generally cause the hash value calculated for the drive

to change each time it is computed. Documenting the location of bad sectors will help a digital investigator determine whether they are allocated to files that are important to the case. In addition, the hash values of individual files that are important to the case can be compared with those on the original hard drive to ensure that specific files are not impacted by the bad sectors.

In addition to presenting findings, digital investigators may be required to explain how the evidence was handled and analyzed to demonstrate chain of custody and thoroughness of methods. Digital investigators may also be asked to explain underlying technical aspects in a relatively nontechnical way, such as how files are deleted and recovered and how tools acquire and preserve digital evidence. Simple diagrams depicting these processes are strongly recommended.

It can be difficult to present digital evidence in even the simplest of cases. In direct examination, the attorney usually needs to refer to digital evidence and display it for the trier of fact (e.g., judge or jury). This presentation can become confusing and counterproductive, particularly if materials are voluminous and not well arranged. For instance, referring to printed pages in a binder is difficult

for each person in a jury to follow, particularly when it is necessary to flip forward and backward to find exhibits and compare items. Such disorder can be reduced by arranging exhibits in a way that facilitates understanding and by projecting data onto a screen to make it visible to everyone in the court.

Displaying digital evidence with the tools used to examine and analyze it can help clarify details and provide context, taking some of the weight of explaining off the digital investigator. Some digital investigators place links to exhibits in their final reports, enabling them to display the reports onscreen during testimony and efficiently display relevant evidence when required. However, it is important to become familiar with the computer that will be used during the presentation to ensure a smooth testimony. Visual representations of timelines, locations of computers, and other fundamental features of a case also help provide context and clarity. Also, when presenting technical aspects of digital evidence such as how files are recovered or how log-on records are generated, first give a simplified, generalized example and then demonstrate how this applies to the evidence in the case.

## Aim/Objectives

This chapter compares several methodologies, highlighting commonalities and providing practical perspectives on approaches to uncover truths to serve justice. This chapter then covers how the scientific method can be applied in each step of a digital investigation.

## Learning Outcomes

After the successful completion of this week, students should be able to:

- Discuss cybercrime and digital investigations
- Discuss the challenges faced by the digital forensic investigators
- Develop an understanding of crime scene principles

## Key Words

Digital forensic investigations	Crime scene principles	International procedures	Chain of custody
---------------------------------	------------------------	--------------------------	------------------

## Annotated Bibliography

### Basic

Chapter 6 of Casey, E, 2011. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. Academic Press Inc (London) Ltd.

Watson D and Jones A, 2013. Digital Forensics Processing and Procedures: Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements. Syngress Publishing.

### Supplementary

- Presentation on cybercrimes and digital investigations that covers the material for weeks 5 and 6.

### Suggestions for further reading

- Jones A and Valli C, 2008, Building a Digital Forensic Laboratory. Butterworth-Heinemann, Newton, MA, USA.
- NIJ Guide, 2001, Electronic Crime Scene Investigation: A Guide for First Responders by The National Institute of Justice

- Angelopoulou O, Vidalis S, 2013, Towards 'Crime Specific' Digital Investigation Methodologies, Cyberforensics 2013, Cardiff, UK
- Silde A, Angelopoulou O, 2014, Digital Forensic Cyberstalker Profiling Methodology, Proceedings of INCoS 2014: Intelligent Networking and Collaborative Systems, Salerno, Italy
- Angelopoulou O, Vidalis S, Robinson I, 2012, Who are you today? Profiling the ID theft fraudster, Proceedings of the 11th ECIW: European Conference on Information Warfare and Security, Laval, France
- Casey E, 2011, Digital Evidence and Computer Crime; Forensic Science, Computers and the Internet, Eoghan, Academic Press
- Maras M.H., 2012, Computer Forensics, Cybercriminals, Laws and Evidence, ISBN: 1449600727
- Stephenson, P., 2002, Collecting Evidence of a Computer Crime, Computer Fraud & Security, Volume 2002, Issue 11, Pages 17-19
- Holt TJ, Bossler AM, Seigfried-Spellar K C, 2018, Cybercrime and Digital Forensics. London: Routledge.

### **Activity (5 points)**

Online quiz on the analysis of cybercrimes and digital investigations, based on the content material. The quiz is an assessed task and weights 5% of the overall module. The students should complete it and submit their answers by the end of week 7.

### **Recommended time for the student to work**

20 hours

## DATA COLLECTION AND PRINCIPLES

6<sup>th</sup> & 7<sup>th</sup> Week

### Summary

Develop an understanding on the digital forensic investigation phases and discuss the principles.

### Introductory Remarks

A digital investigation focuses on the system and the human aspect at the same time. This is a distinctive characteristic of cyber investigations, since the human factor is involved. The digital forensic investigators follow specific procedures during an investigation in order to maintain the chain of custody and preserve the digital evidence. There are methodologies and procedures that are broad and try to cover all different aspects of investigations; whereas others are specific and aim to support the investigation of targeted and sophisticated cyber incidents.

The aim of this unit is to develop an understanding on the digital forensic investigation phases and discuss the principles. The focus is on both data and network collection and the good practise for the analysis of the collected evidence. Students will also familiarise with the challenges of collecting digital evidence and the order of evidence collection according to the volatility of the item. The main concepts around the examination and analysis of the digital evidence are also covered in this unit.

### Aim/Objectives

The aim of this unit is to develop an understanding on the digital forensic investigation phases and discuss the principles.

### Learning Outcomes

After the successful completion of this week, students should be able to:

- Describe the digital forensic methodology
- Critically evaluate scientific methods to collecting and protecting evidence
- Critically discuss the digital evidence categories and the investigative practise
- Develop a critical understanding on data collection and analysis principles

- Develop a critical understanding on network collection and analysis principles
- Familiarise with the different types of digital forensic tools

## Key Words

Digital forensics methodology	Acquisition	Examination	Analysis
Preservation	Anti-forensics	Unallocated space	Temporary data
Volatile data	Logical analysis	Physical analysis	Data recovery
Packet capture	Encryption	Hidden data	Deleted partitions
Deleted files	Hash		

## Annotated Bibliography

### Basic

Easttom C, 2017, System Forensics, Investigation and Response (3rd ed.). Jones and Bartlett Publishers, Inc., USA.

Sammons J, 2014, The Basics of Digital Forensics, Second Edition: The Primer for Getting Started in Digital Forensics, 2nd ed., Syngress Publishing.

Prosise C and Mandia K, 2014, Incident Response and Computer Forensics, The McGraw-Hill Companies, 3<sup>rd</sup> edition

### Supplementary

- Presentation on data collection and principles that covers the material for weeks 7, 8 and 9.

### Suggestions for further reading

- Jones A, Angelopoulou O, Vidalis S, Janicke H, 2017, The 2016 Hard Disk Study on Information Available on the Second-Hand Market in the UK, Proceedings of the 16th ECCWS: European Conference on Information Warfare and Security, Dublin, Ireland
- Casey E, Fellows G, Geiger M, Stellatos G, 2011, The growing impact of full disk encryption on digital forensics, Digital Investigation, Volume 8, Issue 2, Pages 129-134, ISSN 1742-2876

- Ab Rahman NH, Cahyani NDW, Choo K-KR, 2017, Cloud incident handling and forensic-by-design: cloud storage as a case study. *Concurrency Computation: Practice and Experience*, 29: e3868.
- Carrier B, 2003, Defining digital forensic examination and analysis tools using abstraction layers. *International Journal of digital evidence*, 1(4), 1-12.

## **Self-Assessment Exercises**

### **Exercise 6.1**

- Online group discussion on the overview of digital forensic analysis techniques.

### **Exercise 6.2**

- Practical task that aims to familiarise the students with the digital media acquisition process. The students will populate a device with data and create a forensic image.

### **Exercise 7.1**

- Tutorial on the analysis on the identification of partition tables.

### **Exercise 7.2.**

- Tutorial on the file signatures.

## **Activity (5 points)**

The students are required to research and develop a list of tools they should include in their toolkit as digital forensics analysts together with a justification of their decision to include a specific tool. The activity is an assessed task and weights 5% of the overall module. The students should complete it and submit their answers by the end of week 11.

## **Recommended time for the student to work**

Week 6: 15 hours & Week 7: 20 hours

# **FORENSIC SCIENCE TO NETWORKS AND VOLATILE DATA PRESERVATION PROCESS**

**8<sup>th</sup> Week**

## **Summary**

The aim of this unit is to develop an understanding on the digital forensic investigation phases and discuss the principles. The focus is on both data and network collection and the good practise for the analysis of the collected evidence. Students will also familiarise with the challenges of collecting digital evidence and the order of evidence collection according to the volatility of the item. The main concepts around the examination and analysis of the digital evidence are also covered in this unit.

## **Introductory remarks**

A typical process that digital investigators follow to preserve volatile data from a single system is outlined below.

1. Perform an initial physical inspection of the target device, including photographing or noting the physical condition of the device, external markings such as serial numbers, etc. While doing this, the digital investigator notes the input/output options available on the device.
2. Authenticate to the console (monitor and keyboard as opposed to remote access) of the device using administrative credentials. Administrative credentials are typically required to execute some volatile data collection commands.
3. Note the contents of the screen after logon, including any windows that may be open or were opened automatically during logon. Should there be no obvious destructive processes active, the digital investigator will continue.
4. Insert a forensically prepared “clean” toolkit (created from trusted sources in such a way that it minimizes calls to libraries on the system). In this example, consider this toolkit to be on a CD.
5. Locate and identify the trusted shell executable on the CD, and start that shell (e.g., cmd.exe). Running a trusted shell as opposed to the local command line shell helps to circumvent interference by less sophisticated rootkits.

6. Execute a command to change the path variable for the shell, so that the operating system will look on the toolkit CD for programs and libraries before turning to the local system where executables and libraries are not trusted.
7. Insert a wiped and formatted USB drive that will serve as the destination for any volatile data collection output. When dealing with systems that contain large amounts of memory, care must be taken to use a USB device large enough to store the full contents of memory.
8. Execute a command that will extract and present the date and time of the system. This date and time should be recorded in documentation and compared with a trusted time source, noting any discrepancy.
9. Execute a script that will perform the following actions:
  - a. Execute a command that will collect a memory dump and output it to the destination USB drive
  - b. Execute a series of targeted commands that will collect data types
  - c. Create and record hash values for all outputs.
10. Close the trusted shell and eject all media used in the collection and note the date and time in documentation. At this stage, the volatile data preservation process is completed. Depending upon conditions and investigative requirements, the digital investigator may choose to shut the system down to collect a forensic duplicate of the internal storage or may leave the system running for a variety of reasons.

### **Forensic Science to Networks**

Processing a hard drive for evidence is a relatively well-defined procedure. When dealing with evidence on a network, however, digital investigators face a number of unpredictable challenges. Data on networked systems are dynamic and volatile, making it difficult to take a snapshot of a network at any given instant. Unlike a single computer, it is rarely feasible to shut a network down because digital investigators often have a responsibility to secure evidence with minimal disruption to business operations that rely on the network. Besides, shutting down a network will result in the destruction of most of the digital evidence it contains. Also, given the diversity of network technologies and components, it is often necessary to apply best evidence collection techniques in unfamiliar contexts.

Additionally, unlike crime in the physical world, a criminal can be in several places on a network at any given time. This distribution of criminal activity and associated digital evidence makes it difficult to isolate a crime scene.

## Aim/Objectives

The aim of this unit is to develop an understanding on the digital forensic investigation phases and discuss the principles.

## Learning Outcomes

After the successful completion of this week, students should be able to:

- Describe the digital forensic methodology
- Critically evaluate scientific methods to collecting and protecting evidence
- Critically discuss the digital evidence categories and the investigative practise
- Develop a critical understanding on data collection and analysis principles
- Develop a critical understanding on network collection and analysis principles
- Familiarise with the different types of digital forensic tools

## Key Words

Digital forensics methodology	Acquisition	Examination	Analysis
Preservation	Anti-forensics	Unallocated space	Temporary data
Volatile data	Logical analysis	Physical analysis	Data recovery
Packet capture	Encryption	Hidden data	Deleted partitions
Deleted files	Hash		

## Annotated Bibliography

### Basic

- Easttom C, 2017, System Forensics, Investigation and Response (3rd ed.). Jones and Bartlett Publishers, Inc., USA.
- Sammons J, 2014, The Basics of Digital Forensics, Second Edition: The Primer for Getting Started in Digital Forensics, 2nd ed., Syngress Publishing.
- Prosise C and Mandia K, 2014, Incident Response and Computer Forensics, The McGraw-Hill Companies, 3<sup>rd</sup> edition

## **Supplementary**

- Presentation on data collection and principles that covers the material for weeks 7, 8 and 9.

## **Suggestions for further reading**

- Jones A, Angelopoulou O, Vidalis S, Janicke H, 2017, The 2016 Hard Disk Study on Information Available on the Second-Hand Market in the UK, Proceedings of the 16th ECCWS: European Conference on Information Warfare and Security, Dublin, Ireland
- Casey E, Fellows G, Geiger M, Stellatos G, 2011, The growing impact of full disk encryption on digital forensics, Digital Investigation, Volume 8, Issue 2, Pages 129-134, ISSN 1742-2876
- Ab Rahman NH, Cahyani NDW, Choo K-KR, 2017, Cloud incident handling and forensic-by-design: cloud storage as a case study. Concurrency Computation: Practice and Experience, 29: e3868.
- Carrier B, 2003, Defining digital forensic examination and analysis tools using abstraction layers. International Journal of digital evidence, 1(4), 1-12.

## **Recommended time for the student to work**

15 hours

### Summary

The growth of the Internet has greatly increased the number of ways that computers can be involved in a crime, creating many potential sources of digital evidence. Feeling protected by some level of anonymity, individuals often do things on the Internet that they would only imagine in the physical world and express thoughts that they would otherwise keep to themselves. What many people do not realize is that eavesdropping on a network is elementary and servers on the Internet retain a significant amount of information about individuals' activities, creating a cybertrail similar to a paper trail in the physical world.

### Introductory remarks

The Internet provides the infrastructure for many different services. Most people are familiar with services such as e-mail and the World Wide Web (WWW). Although many of us use these Internet services, we rarely access them directly. Instead we use applications (computer programs) that make it easier to use the services on a network. For example, many people use the Netscape Navigator application to access Web pages stored on distant Web servers. Similarly, Eudora is an application used to access e-mail on distant e-mail servers. The underlying services are comprised of application layer protocols, many of which are defined in Request For Comment (RFC) documents. Although there are thousands of Internet services and applications, the process of understanding the Internet can be simplified by considering its seven main services:

- World Wide Web (or Web)
- E-mail
- Social Networking
- Synchronous (Live) Chat Networks
- Peer-to-Peer (P2P)
- Virtual Worlds
- Newsgroups (a.k.a. Asynchronous Discussion Groups)

### The Internet as an Investigative Tool

An important aspect of following the cybertrail in an investigation is to search for related information on the Internet such as a victim's Web pages or Usenet messages, an offender's

e-mail address or telephone number, and personal data in various online databases. Because the Internet contains so much loosely ordered information, searching for something in particular can be like looking for a needle in a haystack. This is why it is crucial to learn how to search the Internet effectively. In addition to becoming familiar with various search tools, it is necessary to develop search strategies.

Given the popularity of social networking sites like Facebook, and the wealth of personal information that they contain, digital investigators will often find useful information on these sites. Some of the information on social networking sites can be searched and accessed by anyone on the Internet, but there can be substantial amounts of information on these sites with access restricted to friends and family. In some cases, digital investigators may be able to obtain information, including backups of past pages and communications, from the social network provider.

### **Online Anonymity and Self-Protection**

It is important for investigators to become familiar with online anonymity to protect themselves, and to understand how criminals use anonymity to avoid detection. In addition to concealing obvious personal information like name, address, and telephone number, some offenders use IP addresses that cannot be linked to them. Such IP addresses can be obtained by using free ISPs that allow individuals to dial into the Internet without requiring them to identify themselves. Other ISPs unintentionally provide this type of free, anonymous service when one of their customer's dial-up account is stolen and used by the thief to conceal his/her identity while he/she commits crimes online. Public library terminals and Internet cafes are other popular methods of connecting to the Internet anonymously.

Investigators should use anonymity to protect themselves while searching for criminals on the Internet, particularly when conducting an undercover investigation. Online undercover investigations can be used in many types of criminal activities including online gambling. When investigating online gambling, it is necessary to create several undercover identities to make transactions and gather intelligence into the supporting organizations and networks. Undercover identities are also used to purchase drugs on the Internet and stolen hardware through online auction sites. In child exploitation cases, undercover investigators may pose as children or as pedophiles to gather evidence. Computer intruders can be tracked on IRC, counterfeiters can be ferreted out, and fraudsters can be apprehended, all with the assistance of online undercover identities.

## Aim/Objectives

This chapter focuses on investigating criminal activity on the application layer of the Internet. Case examples are used to give a practical understanding of how the main services on the Internet can be involved in criminal activity and how they can be a source of digital evidence. The discussions of the Internet's application layer in this chapter can be generalized to any network, such as a company's internal network. Collecting digital evidence at the application layer is like taking a surface scraping of a network. For every piece of digital evidence found at the application layer, there are more related data in other layers of the network that can be obtained as discussed in previous chapters.

## Learning Outcomes

After the successful completion of this week, students should be able to:

- Describe the digital forensic methodology
- Critically evaluate scientific methods to collecting and protecting evidence
- Critically discuss the digital evidence categories and the investigative practise
- Develop a critical understanding on data collection and analysis principles
- Develop a critical understanding on network collection and analysis principles
- Familiarise with the different types of digital forensic tools

## Key Words

Digital forensics methodology	Acquisition	Examination	Analysis
Preservation	Anti-forensics	Unallocated space	Temporary data
Volatile data	Logical analysis	Physical analysis	Data recovery
Packet capture	Encryption	Hidden data	Deleted partitions
Deleted files	Hash		

## Annotated Bibliography

### Basic

- Easttom C, 2017, System Forensics, Investigation and Response (3rd ed.). Jones and Bartlett Publishers, Inc., USA.
- Sammons J, 2014, The Basics of Digital Forensics, Second Edition: The Primer for Getting Started in Digital Forensics, 2nd ed., Syngress Publishing.
- Prosise C and Mandia K, 2014, Incident Response and Computer Forensics, The McGraw-Hill Companies, 3<sup>rd</sup> edition

### **Supplementary**

- Presentation on data collection and principles that covers the material for weeks 7, 8 and 9.

### **Suggestions for further reading**

- Jones A, Angelopoulou O, Vidalis S, Janicke H, 2017, The 2016 Hard Disk Study on Information Available on the Second-Hand Market in the UK, Proceedings of the 16th ECCWS: European Conference on Information Warfare and Security, Dublin, Ireland
- Casey E, Fellows G, Geiger M, Stellatos G, 2011, The growing impact of full disk encryption on digital forensics, Digital Investigation, Volume 8, Issue 2, Pages 129-134, ISSN 1742-2876
- Ab Rahman NH, Cahyani NDW, Choo K-KR, 2017, Cloud incident handling and forensic-by-design: cloud storage as a case study. Concurrency Computation: Practice and Experience, 29: e3868.
- Carrier B, 2003, Defining digital forensic examination and analysis tools using abstraction layers. International Journal of digital evidence, 1(4), 1-12.

### **Individual Assignment (20 points)**

*Research report, 20% of the overall mark*

Your task is to critically discuss the important elements of an incident response plan. You should produce a word-processed report of approximately 1000 words, justify your decisions and refer to specific technical terms related to incident response. You are encouraged to make use of tables and figures where appropriate.

### **Recommended time for the student to work**

35 hours

## EVIDENCE ANALYSIS AND HANDLING

10<sup>th</sup> & 11<sup>th</sup> Week

### Summary

Different types of incidents leave behind different traces of evidence. However, the examination phase of the investigation should explain the evidence origin and significance, while looking for information that may be hidden or obscured. The analysis phase of the investigation tests the outcome of the examination for its relevance to the existing case and evaluates the recovered artefacts.

This unit aims to discuss the analysis techniques and file systems. The focus is on Windows and Linux forensic investigations. Windows is the most popular operating system for desktop and laptop computers, while variants of Linux are the most popular systems for servers. The techniques on evaluating incident data and the significance of indicators of compromise are also covered in this unit.

### Introductory remarks

There are few events in the field of computer security as satisfying or worthwhile as a successful courtroom experience. If a computer security incident you have investigated leads to a court proceeding, the digital evidence and documents you obtained are likely to be used as exhibits in the trial. Special rules exist to ensure that the exhibits are genuine and exactly what they purport to be. Therefore, during adverse civil or criminal proceedings, your collection, handling, and storage of electronic media, paper documents, equipment, and any other physical evidence can be challenged by an adversary.

It is important that you follow and enforce evidence-handling procedures that will meet the requirements of the judging body and withstand any challenges. However, it is equally important that your evidence procedures do not create so much overhead that they become too cumbersome and difficult to implement at your organization.

One of the most common mistakes made by computer security professionals is failure to adequately document when responding to a computer security incident. Critical data might not ever be collected, the data may be lost, or the data's origins and meaning may become unknown. Added to the technical complexity of evidence collection is the fact that the properly

retrieved evidence requires a paper trail. Such documentation is seemingly against the natural instincts of the technically savvy individuals who often investigate computer security incidents.

The FRE, as well as the laws of many state jurisdictions, define computer data as “writings and recordings.” Documents and recorded material must be authenticated before they may be introduced into evidence. Authentication, defined in FRE 901(a), basically means that whomever collected the evidence should testify during direct examination that the information is what the proponent claims. In other words, the most common way to authenticate evidence is to have a witness who has personal knowledge as to the origins of that piece of evidence provide testimony.

If evidence cannot be authenticated, it is usually considered inadmissible, and that information cannot be presented to the judging body. You meet the demands of authentication by ensuring that whomever collected the evidence is a matter of record. It is important to develop some sort of internal document that records the manner in which evidence is collected. Maintaining the chain of custody requires that evidence collected is stored in a tamper-proof manner, where it cannot be accessed by unauthorized individuals. A complete chain-of-custody record must be kept for each item obtained. Chain of custody requires that you can trace the location of the evidence from the moment it was collected to the moment it was presented in a judicial proceeding.

To meet chain-of-custody requirements, many police departments and federal law enforcement agencies have property departments that store evidence (the best evidence) in a secure place. Experts and law enforcement officers must “check-out” the evidence whenever they need to review it, and then “check-in” the evidence each time it is returned to storage.

Another challenge is to ensure that the data you collected is identical to the data that you present in court. It is not uncommon for several years to pass between the collection of evidence and the production of evidence at a judicial proceeding. Your organization can meet the challenge of validation by ensuring MD5 hashes of the original media match those of the forensic duplication. MD5 hash values should also be generated for every file that contributes to the case (every file that is evidence).

When handling evidence during an investigation, you will generally adhere to the following procedures:

1. If examining the contents of a hard drive currently placed within a computer, record information about the computer system under examination.
2. Take digital photographs of the original system and/or media that is being duplicated.

3. Fill out an evidence tag for the original media or for the forensic duplication (whichever hard drive you will keep as best evidence and store in your evidence safe).
4. Label all media appropriately with an evidence label.
5. Store the best evidence copy of the evidence media in your evidence safe.
6. An evidence custodian enters a record of the best evidence into the evidence log. For each piece of best evidence, there will be a corresponding entry in the evidence log.
7. All examinations are performed on a forensic copy of the best evidence, called a working copy.
8. An evidence custodian ensures that backup copies of the best evidence are created. The evidence custodian will create tape backups once the principal investigator for the case states that the data will no longer be needed in an expeditious manner.
9. An evidence custodian ensures that all disposition dates are met. The dates of evidence disposition are assigned by the principal investigator.
10. An evidence custodian performs a monthly audit to ensure all of the best evidence is present, properly stored, and labeled.

## Aim/Objectives

This chapter explains how to ensure that all the information you obtain is collected, handled, and stored in an appropriate manner. Effective and efficient evidence-handling procedures are presented, with guidelines for implementing these procedures in an organization.

## Learning Outcomes

After the successful completion of this week, students should be able to:

- Develop an understanding of the digital forensic investigation process
- Identify digital evidence sources
- Develop an understanding on different file systems under a digital forensics analysis perspective

## Key Words

Digital evidence	File systems	Data carving	File analysis
Log analysis	Indicators of compromise	Windows registry	Linux shell

## Annotated Bibliography

### Basic

- Easttom C, 2017, System Forensics, Investigation and Response (3rd ed.). Jones and Bartlett Publishers, Inc., USA.
- Prosise C and Mandia K, 2014, Incident Response and Computer Forensics, The McGraw-Hill Companies, 3<sup>rd</sup> edition
- Carvey H, 2012, Windows Forensic Analysis Toolkit, 4th Edition: Advanced Analysis Techniques for Windows 8, Syngress Publishing

### Supplementary

- Presentation on evidence analysis and handling that covers the material for weeks 10 and 11.

### Suggestions for further reading

- Vidalis S, Angelopoulou O, 2014, Assessing Identity Theft in the Internet of Things, IT CoNvergence PRACTICE - INPRA, Volume 2, Issue 1, March 2014, pp. 15-21, <http://isyu.info/inpra/papers/inpra-v2n1-02.pdf>
- Carvey H, 2016, Windows Registry Forensics, Advanced Digital Forensic Analysis of the Windows Registry, 2<sup>nd</sup> ed, Syngress
- Carrier B, 2005, File System Forensic Analysis, Addison-Wesley Professional.

## Self-Assessment Exercises

### Exercise 10.1

- Practical task that aims to familiarise the students with the analysis of the NTFS Master File Table.

### Exercise 10.2

- Practical task that aims to familiarise the students with the viewing and analysis of email.

### Activity 11.1

- Online group discussion on comparing Windows and Linux forensic investigations.

### **Tutorial 11.1**

- Tutorial on the analysis of the Windows registry

### **Recommended time for the student to work**

30 hours (15 hours/week)

## REPORTING AND PRESENTING

12<sup>th</sup> &13<sup>th</sup> Week

### Summary

Focus on the final phase of a forensic examination, which is reporting the findings.

### Introductory Remarks

The final phase of a forensic examination is reporting the findings. The report should be well organised and presented in a format that the target audience understands. The reports communicate the results of the analysis and are presented to technical and non-technical individuals. Therefore, they must be factual, simple and concise. The report should convey the work of the analyst to the decision makers no matter if it is written as the outcome of an incident response or a digital forensic investigation.

### Aim/Objectives

This unit aims to discuss the best practices in writing a report, define the different types of reports and present the testimony practices to the students. The cross-examination of an expert witness is also covered in this unit.

### Learning Outcomes

After the successful completion of this week, students should be able to:

- Evaluate the best practices for writing an incident response and a digital forensics report
- Discuss and identify the different types of reports
- Critically discuss how to apply the scientific method to the report
- Develop an understanding of cross examination.

### Key Words

Digital forensics report	Technical report	Expert witness	Cross examination
Documentary evidence	Expert testimony		

## Annotated Bibliography

### Basic

- Carvey H, 2012, Windows Forensic Analysis Toolkit, 4th Edition: Advanced Analysis Techniques for Windows 8, Syngress Publishing

### Supplementary

- Presentation on reporting and presenting that covers the material for weeks 12.

### Suggestions for further reading

- Caviglione L, Wendzel S and Mazurczyk W, 2017, The Future of Digital Forensics: Challenges and the Road Ahead, IEEE Security & Privacy, vol. 15, no. 6, pp. 12-17
- Schroeder SC, 2005, How to be a digital forensic expert witness, First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05), Taipei, Taiwan, pp. 69-85
- F-Secure, 2018, Incident response report, <https://fsecurepressglobal.files.wordpress.com/2018/02/f-secure-incident-response-report.pdf>

## Self-Assessment Exercises

### Exercise 12.1

- Practical task on crafting an evidentiary case report from a digital forensics' suite.

### Activity 12.1

- Online group discussion on good practise for report writing.

## Group Assignment (20 points)

*Group Practical task, 20% of the overall mark – Deadline on week 13*

You are required to carry out a forensic examination of the evidence file that you have been provided with and forensically examine its contents. You will need to produce a technical report that describes the formal investigation methodology that you followed and presents your findings.

## Recommended time for the student to work

50 hours (for both weeks)

## **REVISION AND FINAL EXAMINATION**

### **Summary**

The final examination consists of two parts of essay type and short answer questions. The final exam weights 50% of the overall mark. In detail:

- Part a. Essay type: Four questions out of which the students should select and answer two. Each answer is awarded 25 marks.
- Part b. Short answer: Six questions out of which the students should select and answer five. Each answer is awarded 10 marks.

### **Recommended time for the student to work**

40 hours

**Date/Time of Final Exam: TBD**



**FORM: 200.1.3**

## **STUDY GUIDE**

**Course: CYS695 - Master Thesis**

## Course Information

<b>Institution</b>	European University Cyprus		
<b>Programme of Study</b>	Cybersecurity (MSc)		
<b>Course unit</b>	CYS695	Master Thesis	
<b>Level</b>	<i>Undergraduate</i>	<i>Postgraduate</i>	
		<i>Master</i>	<i>PhD</i>
		√	
<b>Language of Instruction</b>	English		
<b>Teaching Methodology</b>	Distance Learning		
<b>Course Type</b>	<i>Compulsory</i>		<i>Optional</i>
		√	
<b>Number of Group Consultation Meetings/Web-Conferences/Lectures</b>	<i>Total</i>	<i>Face to Face</i>	<i>Web-Conferences</i>
	14	1	13
<b>Number of Assignments</b>			
<b>Final Assessment</b>	<i>Assignments</i>		<i>Oral Presentation</i>
	80 %		20 %
<b>Number of Credits (ECTS)</b>	30		

<b>Study Guide drafted by</b>	Dr George Christou
<b>Editing and final approval of Study Guide by</b>	Dr Yianna Danidou

## COURSE CONTENTS

		Page
	Introductory Notes	4
	First Group Consultation Meeting	9
1	Week 1 – What is Research	12
2	Week 2 - Discussion of the Research Proposal	14
3	Week 3 – The Literature Review	17
4	Week 4 – The Literature Review continued	20
5	Week 5 – The Literature Review continued	23
6	Week 6 – Methodology and Data Gathering – Qualitative Methods	26
7	Week 7 – Methodology and Data Gathering – Quantitative Methods	29
8	Week 8 – Analysis and Discussion – Descriptive Statistics	32
9	Week 9 – Analysis and Discussion – Probability and Distributions	36
10	Week 10 – Analysis and Discussion – Hypothesis Testing	40
11	Week 11 – Analysis and Discussion – Regression and Correlation Analysis	44
12	Week 12 – The Conclusion	47
13	Week 13 – Presentation and Mock Defense	49
	Preparation, Writing and Defense of the Master Thesis	51
	Indicative answers to Self-Assessment Exercises	52
	Annexes 1-5	58

## INTRODUCTORY NOTES

### 1.1 Instructor and Communication

The instructor for this course is Dr. George Christou. You can contact Dr. Christou through email – [g.christou@euc.ac.cy](mailto:g.christou@euc.ac.cy), during his office hours face-to-face at his office located at Room 114, or through the phone at +357-22713104. You can also use blackboard to arrange for an online meeting whenever the need arises.

However, thesis topics are submitted by many instructors from the Department of Computer Science and Engineering, and this is what makes this course unique. While the students may ask any procedure questions to the instructor who is assigned the course, it is the thesis supervisor who is in charge of the subject matter. As such, when students require help with the content of their thesis, they should contact the thesis supervisor.

*Students are encouraged to communicate with the instructor throughout the duration of this course. The students should not only communicate with the instructor, but should also use blackboard's course forum to communicate with each other, exchange ideas, and collaborate in solving and clarifying their questions. Collaboration is what drives scientific enquiry, and even though each student will create a unique thesis, several questions about the research and the writing are common to everyone. As such, the students should feel free to post and answer questions on the course forum, and utilize the instructor to the fullest extent. The contact details and ways of contacting the instructor are described in the first part of this guide.*

### 1.2 Short course description and objectives:

This course will guide you to the completion of your Master's Thesis. A thesis is required for the completion of your degree as per the degree requirements. The course is designed to give you the necessary skills to enable the successful completion of this project. You will learn established research methods for independent research using methodical processes. Through this course, you will also develop an ability to organize and carry out an extended, independent and novel scientific research work at postgraduate level, employing concepts and methods learned during your study in the program. You will acquire skills that will enable you to synthesize concepts and methods learned in your other courses, and exhibit awareness of previous work in the area of study. Through the research and write-up of your thesis you will gain deeper knowledge of the subject at hand and to gain insight into the working processes used within a company, other institutions or within a department. Your skills and knowledge will be extended through the taught

components of the courses of the program and you will become prepared for future independent work as a Master of Science.

### **1.3 Learning outcomes**

After the completion of this course you will be able to:

- Demonstrate written and oral technical research skills.
- Select and justify a research topic.
- Use various resources to carry out a literature search.
- Structure and format the project to agreed conventions.
- Design, execute, interpret and report results from empirical research projects.
- Manage a project and explain the relevant techniques and tools needed in order to complete it successfully on time and within budgeted resources.
- Identify real-world problems to which academic concepts and methods can be realistically applied to improve or resolve the problem situation.
- Select and use effectively the methods and techniques appropriate for particular cases.
- Plan and manage their work.
- Evaluate a proposed solution and prove its worth to the client.
- Critically evaluate the project and the proposed solution.
- Recognise and describe legal, social or ethical obligations.

### **1.4 Course Timeline**

*The Thesis Topics Catalogue becomes available on the first day of the first week of the semester. The students receive the catalogue via a personal email sent to them by the course instructor, and they are also available on the departmental website. If the students do not receive an email by the end of the first day of the semester, they should immediately contact the course instructor.*

*Once the students receive the topics, they have two weeks (by the second Friday of the semester) to choose a topic. Topics are assigned on a First-Come, First-Served basis, given that the students have passed all the pre-requisite courses for a specific topic. Two weeks are given to the students so that they can examine the topics in detail and contact the associated topic supervisors for the topics they select. It is advisable that each student selects more than one topic, so that if one topic becomes unavailable, the student will have options to select another topic.*

*Once a topic is selected and agreed upon with the associated supervisor, the course follows the weekly breakdown structure as that is provided later in the study guide. However, the student should know that the course is broken down into 13 weeks and the week of presentation, which may or may not directly follow the 13 weeks of instruction.*

*Although this course does not have a final exam, the written thesis is defended during a public defense at a place and time that is suitable and agreed upon by the thesis advisor, the course instructor and any other instructors involved in helping the student during his thesis write-up. The instructors involved are called the Evaluation Committee, and they should all be present during the thesis defense.*

*The thesis is orally defended through teleconference software, preferably through the Blackboard software, before the student's assessment board, as noted above. The defense process is open to the academic community, and any people that want to observe the defense should communicate this to the thesis advisor at least one week prior to the defense day, so that the advisor will have ample time to provide access codes to the teleconference. It is advised that the defense be recorded, but for this to occur, the student and the Evaluation Committee need to provide their explicit consent.*

*According to the departmental guidelines for thesis submission, a final draft of the thesis should be sent to the Evaluation Committee at least four weeks before the deadline of the submission of the final thesis. This allows the Evaluation Committee members to examine the thesis and provide their comments. The comments of the Evaluation Committee should be taken into account by the student, who should edit and possibly amend the thesis with the appropriate corrections, before the submission of the final thesis. The final thesis is the only document that is graded in the way discussed in the grading section of this guide.*

## **1.5 Course Assessment**

*The specific deliverables for each individual's thesis must be discussed and decided upon in consultation with the academic and, if they exist, industrial supervisors. However, each thesis must involve deliverables falling into the following general categories:*

- a) A proposed solution to a real-world problem.
- b) A proof of concept, which demonstrates the validity of the proposed solution.
- c) Clear indication of knowledge of relevant work by others in the field.
- d) The selection and application of appropriate theoretical concepts and methods.
- e) A project thesis of between 12,000 to 16,000 words.

*The course is graded in two parts. One part which carries 80% of the total grade of the course is allocated to the actual written thesis. The second part, which carries 20% of the total grade of the course is allocated to the thesis presentation. The guidelines for the grading of both the thesis and the presentation are shown below.*

*The written thesis is graded according to the following scheme:*

<b>Description</b>	<b>Grade Percentage</b>	<b>Actual Marks</b>
<i>Project justification including its relationship to the current state of the art</i>	10%	<i>20 points</i>
<i>Ability to select and use appropriate methods and techniques</i>	10%	<i>20 points</i>
<i>The clarity, coherence and succinctness with which the solution is developed</i>	30%	<i>60 points</i>
<i>Novelty. Does the work improve significantly the current state of the art?</i>	30%	<i>60 points</i>
<i>Ability to critically review the project and assess its implications for future work in view of the project recommendations and conclusions</i>	10%	<i>20 points</i>
<i>Project Management: Ability to plan and control the project</i>	10%	<i>20 points</i>

*The total amount of actual points a student may accumulate for the written thesis is 200.*

*In addition, the oral presentation is graded according to the following table:*

<b>Description</b>	<b>Grade Percentage</b>	<b>Actual Marks</b>
<i>Ability and presence of mind of the presenter to answer to all questions pertaining to the thesis</i>	40%	<i>20 points</i>
<i>Clear and correct presentation of the subject matter with good organization and structure</i>	30%	<i>15 points</i>

<i>Correct use of slides, charts, and tables to justify the thesis main objective</i>	30%	15 points
---	-----	-----------

*The total amount of actual points a student may accumulate for the presentation are 50.*

*The calculation of the final grade for the student is as follows:*

*The written thesis is worth 80% of the final grade of the course, while the presentation accounts for the other 20%. For example, if a student accumulates 160 points for the written thesis and 30 points of the final, the student's final grade will be:*

$$160/200 * 80/100 = 0.64 \text{ or } 64\% \text{ of the final grade}$$

*Added with*

$$30/50 * 20/100 = 0.12 \text{ or } 12\% \text{ of the final grade.}$$

*Thus, the final grade is 76% and the student is awarded the letter grade of C+.*

### **1.6 Method of Teaching**

*The Master's Thesis course is slightly different from all other distance learning courses in the student's degree. As such, the course requires the students to have regularly scheduled meetings with their thesis supervisor. Through the use of the blackboard platform, both the students and the supervisors can upload articles that are relevant to the thesis topic, and provide links to video and presentation material that can be used to further the students' knowledge towards gaining the specific skills required to complete their thesis.*

*A second tool that the students are urged to learn how to use is the European University Cyprus' online library. The library offers access to a significant amount of online libraries from the ACM and other publishers that specialize in publishing targeted material in Computer Science and, more importantly, in the field of Cybersecurity.*

*Again, students are urged to collaborate through the Blackboard platform in order to solve generic questions and to use private consultations with their thesis supervisor to solve specific subject matter questions. In any case, it is the students' responsibility to leverage all resources that the university offers to train them in the use of the online tools that the university offers.*

## 1st GROUP CONSULTATION MEETING

### Programme Presentation

Leading companies today are rethinking the role of information security in their organizations. They realize that in a digital world, cybersecurity is the key to safeguarding their most precious assets—intellectual property, customer information, financial data, and employee records, among others. But far more than a defensive measure, companies also know that cybersecurity can better position their organization with business partners, customers, investors, and other stakeholders.

The European cybersecurity market is about 25% (i.e. about €17bln) of the world market (estimated at €70bln in 2015), with an average yearly growth slightly larger than 6%, when the world market is growing at about 10%/year. Recent study compiled by Europe's cybersecurity industry leaders pointed out that Europe is in danger of falling behind in the international digital economy field.

The Master in Cybersecurity is a cutting-edge program, designed for those wishing to develop a career as a cyber-security professional, or to take a leading technical or managerial role in an organization critically dependent upon data and information communication technology. Students will develop an advanced knowledge of information security and an awareness of the context in which information security operates in terms of safety, environmental, social and economic aspects. They will gain a wide range of intellectual, practical and transferable skills, enabling them to develop a flexible professional career in IT.

Key elements of this postgraduate degree are: the *real life experience* given by the opportunity to apply their theoretical knowledge through specialized virtual and remote security laboratories in which they will be able to carry out activities such as reconnaissance, network scanning and exploitation exercises, and investigate the usage and behavior of security systems such as Intrusion Detection and Prevention Systems thus becoming confident in the practical application of the latest tools; the *high-level insight* that will enhance student's ability to research and design creative cyber security solutions to address business problems; *hands-on skills* through experimentation with security techniques, cryptographic algorithms, cyber forensics building an ethical hacking environment; and *flexibility* since students will also be able to choose either the completion of a Master thesis or to complete a Research methods course and two elective courses.

Students undertake modules to the value of 90 ECTS credits.

## COURSE PRESENTATION THROUGH THE STUDY GUIDE

During the first group consultation, the students will meet with the course instructor (not their topic supervisor) to discuss the various thesis topics that are provided by the members of the department in the Thesis Topics Catalogue.

The students will also become familiar with the online features of the university's library system, and will learn about the structure of the Master's Thesis. They will also learn about the various methods of referencing, such as APA, Harvard, MLA, Chicago, ACM, etc.

Generally, the structure of the Master's Thesis includes the following:

1. **Introduction:** The introduction to the thesis is used to present the topic of the thesis, position the thesis in the general knowledge framework of the subject (in this case in the context of Cybersecurity), and to specifically describe the scientific question that the thesis will try to answer. The rest of the introduction provides a brief description of the following chapters in the thesis, and concludes with a wrap-up of why the scientific question needs to be answered.
2. **Literature Review:** The second chapter of the thesis provides a brief and concise review of the existing literature. Scientific journal articles, articles published in the proceedings of scientific conferences, and books that pertain to the topic of the thesis are reviewed in this chapter. The goal of this chapter is to provide the reader the background to understand how the scientific question that was described in the introduction was formed.
3. **Methodology:** The third chapter of the thesis provides a discussion of the scientific apparatus used to perform any experiments described in the thesis, and discusses how the apparatus is unbiased. The chapter should also describe the methodology and the procedure used to guide the research. In this chapter, students should justify why the apparatus, methodology, and procedure are valid and credible. Any experiments should be described in this chapter, and it should be shown how they conform to the methodology described.
4. **Results and Discussion:** The fourth chapter should present the results of the experiments using relevant charts and tables. The student is urged to include any extensive data tables and large statistics results in an Appendix instead of cluttering the chapter with them. The main results should be analyzed and discussed, and the answer to the scientific question should be clearly outlined and explained here.
5. **Conclusion:** The fifth and final chapter of the main thesis should reiterate the scientific question, and provide a succinct answer. The conclusion should also include discussion on further questions that the answer may possibly open, as well as describe any future work that may stem from the thesis.
6. **References:** The scientific literature which was cited in the thesis is included here, following the selected method of citing (APA, ACM, Harvard, etc.)

7. **Appendices:** This part includes any relevant information that supplements the thesis, such as large statistics tables, the data extracted from the experiments, sample questionnaires and/or other data collection methods used, but that was not included in any of the previous chapters.

## Time for the student to work

During the first week, the student is recommended to take as much time as required to study this guide, and to attend the online training to become familiarized with the Blackboard platform and the Library's online functions. The approximate time required is about five (5) hours of study.

The student should also consult with the topic supervisors, to gain the information to allow the student to make an intelligent choice on which topic to choose for his or her master's thesis.

## WHAT IS RESEARCH

1<sup>st</sup> Week

### Summary

After the completion of the three-hour meeting, the students should be able to critically assess and compare the two major types of research, quantitative and qualitative, discuss how academic discourse works, and be able to suggest what type of research they should use in their selected project.

### Introductory Remarks

During the second meeting of the semester, the students will discuss and become exposed to the major paradigms of **research**. Research is the investigation or experimentation aimed at the discovery and interpretation of facts, revision of accepted theories or laws in the light of new facts, or practical application of such new or revised theories or laws. The students will compare these paradigms, and critically discuss how research takes place in the context of **academic discourse**, or academic dialogue, the inclusion of all lingual material for a specific topic. They will also assess the **ethical**, **legal**, and **social** implications of the performance of a research project, given its particular objectives and scientific questions. The students will further delve into a discussion on the differences between **qualitative research** and **quantitative research**. Qualitative research is a scientific method that is based on gathering non-numerical data, such as notes, bodies of text, etc. whereas quantitative research is a scientific method that requires the gathering and analysis of numerical data.

### Aim/Objectives

The aim of this meeting will be for the students to be able to critically discuss the various types of research that they can use.

### Learning Outcomes

After the completion of the three hour meeting, the student should begin to grasp the method of how to select and justify a research topic. The student will be able to discuss the ethical, legal

and social implications of research, and be able to critically assess these implications for his or her selected project.

## Key Words

Academic Discourse	Research	Research Paradigm
Qualitative Research	Quantitative Research	Social Issues in Research
Ethics in Research	Legal Issues in Research	

## Annotated Bibliography

### Basic Material

Howard, K. & Sharp, J.A., The Management Of A Student Research Project, Gower

### Supplementary Material

Notes and slides handed out by the instructor of the course

### Suggestions for further reading

Murray, R. (2011). How to Write a Thesis (Vol. 3rd ed). Maidenhead: McGraw-Hill Education.

Manuals of Referencing Scientific Research.

## Self Assessment Exercises

### Exercise 1.1

Describe what type of research your selected research topic should be treated with, and provide the reasons that have led you to this choice. Critically assess your topic, and provide a preliminary research question that is raised in that topic that must be answered.

## Recommended time for the student to work

The recommended amount of time outside of the three-hour meeting for this week is approximately 15 hours including the studying of the required and further reading, as well as answering the self-assessment exercise.

## DISCUSSION OF THE RESEARCH PROPOSAL

2<sup>nd</sup> Week

### Introductory Remarks

During the second meeting of the semester, the students will discuss and learn how to compose their **Research Proposal**. The Research Proposal is a short article that describes a topic with problems that have not been answered yet, or they have been answered in ways that may not yield optimal answers. The proposal contains a **Scientific Question**, a question that when answered will move the field closer to answering the problems described in the Research Proposal. It also includes the way that the researchers will proceed with the examination, data gathering and testing of the scientific question. This is called the **Methodology** of the research to be conducted. Finally, to create a solid plan for performing the research in question, the researchers provide a timeframe for its conclusion. This is the **Timeline for completion** of the project, and must include specific **Milestones** and **Deadlines**. A milestone is a significant event towards the completion of the research project, such as finishing up the data gathering, or finishing up the analysis of part of the data. A deadline on the other hand is a firm date upon which the researcher will have finished some part of the research. Finally, the proposal includes a section which examines the existing knowledge in the field about the particular topic and about the specific scientific question. This section is called the **Literature Review** of the proposal, in which the researcher corroborates through the work of others, that the problem to be studied is indeed an important one.

### Aim/Objectives

The aim of this meeting is to provide the students the method and scope of their Research Proposal.

### Learning Outcomes

At the end of the three hour meeting, the students should have clear goals in mind. In fact, the students should understand that they should hand in their Preliminary Research Proposal in exactly one week from the end of the meeting, and that the Research Proposal should have the following structure:

1. Introduction: The introduction should help the reader understand why the suggested topic is interesting and requires investigation, as well as explain what the scientific question is. The students should collaborate closely with their supervisor in order to explicitly define their scientific question. This is one of the key characteristics of a successful thesis. Defining correctly the scientific question will allow the students to proceed with the most appropriate methods of enquiry, and push them towards the correct choice in the type of research that they will choose
2. Brief literature review: The literature review part should highlight the seminal papers that will be used towards defining the scientific question. In other words, the review should at least include the articles that discuss research that exactly leads to the scientific question at hand. These articles should be tied together in a coherent argument, and shown that they do indeed point to the scientific question that is proposed in the introduction. The literature review is by no means the completed literature review chapter that will be submitted later on in the semester, because there is not enough time to perform the systematic review required for the final thesis.
3. Brief explanation of the methodology to be used: From the literature review and the nature of the scientific question the students should propose the method that most likely will allow them to provide an answer. The students should explain why the methodology that they describe is the appropriate one for the given question, and provide a plan upon which they will design experiments for data gathering and analysis.
4. References: This final section will include references to all the in-text cited articles that the students have referred to in their preliminary research proposal.

## Key Words

Research Proposal	Scientific Question	Methodology
Timeline for completion	Milestones and Deadlines	Literature Review
Seminal Paper		

## Annotated Bibliography

### Basic Material

Howard, K. & Sharp, J.A., The Management Of A Student Research Project, Gower

## **Supplementary Material**

Notes and slides handed out by the instructor of the course

## **Suggestions for further reading**

Murray, R. (2011). How to Write a Thesis (Vol. 3rd ed). Maidenhead: McGraw-Hill Education.

Goshert, J. C. (2011) Entering the Academic Conversation: Strategies for Research Writing. Boston: Longman.

Manuals of Referencing Scientific Research.

## **Activity**

### **Activity 2.1**

You have one week to submit your preliminary thesis proposal. This proposal must include the justification for the scientific question you plan to pursue in the context of the chosen thesis topic. It should also include the recommended course of action for answering this question. The recommended course of action should consist of a preliminary methodology discussion, as well as a skeleton of the experiments that you should perform in order to gather the data that will allow you to answer the question.

## **Recommended time for the student to work**

The recommended amount of time outside of the three-hour meeting for this week is approximately 30 hours, including the studying of the required and further reading, as well as writing up the activity.

## THE LITERATURE REVIEW

3<sup>rd</sup> Week

### Introductory Remarks

The **Literature Review** is one of the primary ways that one becomes deeply involved with the specific material of his/her scientific question. Thus, understanding how to perform a well-defined, systematic literature review provides the student with a tool that can not only allow him/her to find **relevant** information, but also allows the student to drop information that may seem interesting but is tangential or irrelevant to the topic of the scientific question.

A literature review is a summary of the publications written on a specific topic. These publications, also called articles, are published through **Academic Publishers**. These are companies that print or post online scientific work that has gone through a **peer-review process**. Peer-review is the process of having multiple experts in the field of the publication read and decide whether it is worthy of publication or if it needs more work to become part of the scientific dialogue on its topic.

When the literature review follows a specific methodology, also called a **Review Protocol**, that tries to encompass the whole of a topic, it becomes a **Systematic Review**. The systematic review is no longer a summary of a topic, but it is focused on a specific question, and reviews all the literature around that specific question, coming to a conclusion about whether a definitive answer exists or not.

In both cases, the most common way of finding scientific articles is through the use of a **Search Engine**, an online machine that only focuses on scientific articles, rather than the whole of the World Wide Web.

### Aim/Objectives

The aim of the meeting is to provide the students of a clear plan of action on how to write a systematic literature review, based on the presentation of existing systematic reviews in the literature.

## Learning Outcomes

The literature review is one of the required chapters in the Master's Thesis. During this week and the next, the students will learn how to assemble material according to the specific guidelines of their supervisors. They will then synthesize a coherent piece of work that describes the existing knowledge in the field and that critically examines this knowledge. Through the critical examination, the students will then extract the need for an answer to their scientific question.

A literature review consists of assembling together the relevant existing knowledge about a topic into a coherent story which concludes with the scientific question that will be answered in the final thesis of the student. More specifically, a literature review is used to summarize existing knowledge about a treatment or technology, to identify gaps in the existing knowledge, thus identifying scientific questions that need an answer, and to provide the backdrop upon which an existing research activity takes place.

A systematic review is a thorough and fair review of the existing literature, and not a vague selection of pieces of literature whose only purpose is to guide the reader to believe that the scientific question that is posed is important. As such, the methodology for performing a systematic review is another important piece in the understanding of the research question. It provides strong evidence towards the scientific question, evidence that when treated fairly will withstand the test of peer-review.

Thus, a systematic review requires a plan of action, much like it is required for the writing of the Master's Thesis. This plan of action is usually called the Review Protocol, and it is through the careful design of this protocol that the readers will be convinced that the review is a fair treatment of the existing knowledge that is considered within.

During the three-hour meeting the students will analyse existing systematic reviews taken from the recent literature, so that they will have tangible examples of the creation of a Review Protocol, and a clear understanding of how a systematic review binds together the research that it cites into a coherent whole that leads to the required result.

## Key Words

Literature Review	Systematic Review	Search Engine
Academic Publishers	Peer-Reviewed Publications	Review Protocol

## Annotated Bibliography

### Basic Material

Howard, K. & Sharp, J.A., The Management Of A Student Research Project, Gower

### Supplementary Material

Notes and slides handed out by the instructor of the course

### Suggestions for further reading

Murray, R. (2011). How to Write a Thesis (Vol. 3rd ed). Maidenhead: McGraw-Hill Education.

Goshert, J. C. (2011) Entering the Academic Conversation: Strategies for Research Writing. Boston: Longman.

Various Systematic Review articles gathered from the recent literature.

## Activity

### Activity 3.1

Study the provided systematic reviews and critically assess the Review Protocol, the synthesis of information, and the analysis provided in each. Create a small presentation that will discuss one of the provided reviews to be presented during the next class meeting

### Activity 3.2

Begin gathering literature for preparing your own literature review chapter.

## Recommended time for the student to work

The recommended amount of time outside of the three-hour meeting for this week is approximately 15 hours, including the studying of the required and further reading, as well as the creation of the presentation.

## THE LITERATURE REVIEW - CONTINUED

4<sup>th</sup> Week

### Introductory Remarks

During this week the students will present their own assessment of the provided systematic reviews as per the previous week's assignment.

### Aim/Objectives

The goal of this meeting is to allow the students to discuss an existing systematic review, thus through its deconstruction to understand the style, the structure and the flow of the argumentation in such reviews.

### Learning Outcomes

The literature review is one of the required chapters in the Master's Thesis. During this week and the next, the students will learn how to assemble material according to the specific guidelines of their supervisors. They will then synthesize a coherent piece of work that describes the existing knowledge in the field and that critically examines this knowledge. Through the critical examination, the students will then extract the need for an answer to their scientific question.

A literature review consists of assembling together the relevant existing knowledge about a topic into a coherent story which concludes with the scientific question that will be answered in the final thesis of the student. More specifically, a literature review is used to summarize existing knowledge about a treatment or technology, to identify gaps in the existing knowledge, thus identifying scientific questions that need an answer, and to provide the backdrop upon which an existing research activity takes place.

A systematic review is a thorough and fair review of the existing literature, and not a vague selection of pieces of literature whose only purpose is to guide the reader to believe that the scientific question that is posed is important. As such, the methodology for performing a systematic review is another important piece in the understanding of the research question. It provides strong evidence towards the scientific question, evidence that when treated fairly will withstand the test of peer-review.

Thus, a systematic review requires a plan of action, much like it is required for the writing of the Master's Thesis. This plan of action is usually called the Review Protocol, and it is through the careful design of this protocol that the readers will be convinced that the review is a fair treatment of the existing knowledge that is considered within.

During the three-hour meeting the students will analyse existing systematic reviews taken from the recent literature, so that they will have tangible examples of the creation of a Review Protocol, and a clear understanding of how a systematic review binds together the research that it cites into a coherent whole that leads to the required result.

## Key Words

Literature Review	Systematic Review	Search Engine
Academic Publishers	Peer-Reviewed Publications	Review Protocol

## Annotated Bibliography

### Basic Material

Howard, K. & Sharp, J.A., The Management Of A Student Research Project, Gower

### Supplementary Material

Notes and slides handed out by the instructor of the course

### Suggestions for further reading

Murray, R. (2011). How to Write a Thesis (Vol. 3rd ed). Maidenhead: McGraw-Hill Education.

Goshert, J. C. (2011) Entering the Academic Conversation: Strategies for Research Writing. Boston: Longman.

Various Systematic Review articles gathered from the recent literature.

## Activity

### Activity 4.1

You must by now have accumulated a number of scientific articles that pertain to your scientific question. You will have one week to provide the first draft of your systematic review chapter for review by your supervisors.

## **Recommended time for the student to work**

The recommended amount of time outside of the three-hour meeting for this week is approximately 25 hours.

## THE LITERATURE REVIEW - CONTINUED

5<sup>th</sup> Week

### Introductory Remarks

This week marks the last week that students will dedicate to their literature review. The week prior, students submitted their first draft of the literature review to their supervisors, and must have discussed it with them as well. Thus, students should have a good idea about what they need to edit and amend to their literature review.

### Aim/Objectives

The goal of this meeting is to allow the students ample time to discuss their own literature review with the course instructor, given the feedback they received from their supervisors. The students should then be able to provide a second re-write of the literature review that takes into account the comments they have received, as well as feedback by the course instructor.

### Learning Outcomes

The literature review is one of the required chapters in the Master's Thesis. During this week and the next, the students will learn how to assemble material according to the specific guidelines of their supervisors. They will then synthesize a coherent piece of work that describes the existing knowledge in the field and that critically examines this knowledge. Through the critical examination, the students will then extract the need for an answer to their scientific question.

A literature review consists of assembling together the relevant existing knowledge about a topic into a coherent story which concludes with the scientific question that will be answered in the final thesis of the student. More specifically, a literature review is used to summarize existing knowledge about a treatment or technology, to identify gaps in the existing knowledge, thus identifying scientific questions that need an answer, and to provide the backdrop upon which an existing research activity takes place.

A systematic review is a thorough and fair review of the existing literature, and not a vague selection of pieces of literature whose only purpose is to guide the reader to believe that the

scientific question that is posed is important. As such, the methodology for performing a systematic review is another important piece in the understanding of the research question. It provides strong evidence towards the scientific question, evidence that when treated fairly will withstand the test of peer-review.

Thus, a systematic review requires a plan of action, much like it is required for the writing of the Master's Thesis. This plan of action is usually called the Review Protocol, and it is through the careful design of this protocol that the readers will be convinced that the review is a fair treatment of the existing knowledge that is considered within.

During the three-hour meeting the students will analyse existing systematic reviews taken from the recent literature, so that they will have tangible examples of the creation of a Review Protocol, and a clear understanding of how a systematic review binds together the research that it cites into a coherent whole that leads to the required result.

## Key Words

Literature Review	Systematic Review	Search Engine
Academic Publishers	Peer-Reviewed Publications	Review Protocol

## Annotated Bibliography

### Basic Material

Howard, K. & Sharp, J.A., The Management Of A Student Research Project, Gower

### Supplementary Material

Notes and slides handed out by the instructor of the course

### Suggestions for further reading

Murray, R. (2011). How to Write a Thesis (Vol. 3rd ed). Maidenhead: McGraw-Hill Education.

Goshert, J. C. (2011) Entering the Academic Conversation: Strategies for Research Writing. Boston: Longman.

Various Systematic Review articles gathered from the recent literature.

## **Activity**

### **Activity 5.1**

You need to re-write your literature review, taking into account the feedback you have received both by your academic supervisor, and by the course instructor.

## **Recommended time for the student to work**

The recommended amount of time outside of the three-hour meeting for this week is approximately 20 hours depending on the amount of feedback each student has accumulated by their supervisor and course instructor.

# METHODOLOGY AND DATA GATHERING – QUALITATIVE METHODS

6<sup>th</sup> Week

## Introductory Remarks

Once the student has completed their literature review, he/she is ready to move on to the design of the methodology and experiments that need to be performed to gather data to answer the scientific question. The next four weeks are dedicated towards this objective.

Over the course of these four weeks the students will be exposed to two major paradigms of research: Qualitative and Quantitative. **Qualitative Research** is mostly research that aims to explore a topic rather than to provide a specific answer to a specific question. It is usually performed to provide insights into a problem or to help towards creating questions that can then be answered through **Quantitative Research**. Quantitative Research on the other hand, is used when the problem has become structured, and we can assign measures and metrics towards its solution. It is used to quantify statistical variables that can be used to measure specific aspects of the problem to be studied.

Qualitative Research uses various data collection methods, such as **Interviews** and **Focus Groups**. Interviews are one-on-one question and answer sessions, and vary in that if the interviewer does not deviate at all from the questions that must be asked, then we call this the **Fully Structured Interview**. If the interviewer is allowed to deviate from the question structure to explore things that the interviewee mentions and seem interesting, then we have a **Semi-Structured Interview**. Finally, if the interviewer is allowed to completely forget the question structure and ask about anything, then the interview becomes an **Open Interview**. One may create a **focus group** as well, a group of people that are brought together in a room, to provide opinion on a specific product or service.

The discussions in both cases are recorded, and then the researcher **Codifies**, or creates a group of patterns that have been talked about throughout the interview. This allows the researcher to see the patterns of structures that lead to specific items that may be studied through quantitative research.

## Aim/Objectives

The aim of this week is to introduce students to the writing of their methodology chapter. The students will dissect various methods of data gathering, such as questionnaires, focus groups and interviews for qualitative assessment.

## Learning Outcomes

The students will be exposed to the various methods of data gathering. The students will examine the methodology of building a validated questionnaire and the ways of using existing questionnaires from the literature to gather data.

The students will also be introduced to how a focus group is used to extract data, and how to codify the verbal answers of the group into data that can be analysed using statistical methods.

Finally, the students will examine three types of interviews, fully structured, semi-structured, and open interviews, in order to understand their differences, and how each type of interview may lead to the introduction of scientific questions, or provide data towards the answer of a specific scientific question.

Thus, the focus of the three hour meeting falls on the understanding and examination of qualitative techniques.

## Key Words

Qualitative Research	Focus Group	Interview
Codification	Open Interview	Fully-structured interview
Semi-structured Interview		

## Annotated Bibliography

### Basic Material

Howard, K. & Sharp, J.A., The Management Of A Student Research Project, Gower

### Supplementary Material

Notes and slides handed out by the instructor of the course

## **Suggestions for further reading**

Murray, R. (2011). How to Write a Thesis (Vol. 3rd ed). Maidenhead: McGraw-Hill Education.

Goshert, J. C. (2011) Entering the Academic Conversation: Strategies for Research Writing. Boston: Longman.

Articles from the literature that use qualitative methods to gather data towards answering their research question

## **Activity**

### **Activity 6.1**

The students should prepare a short methodology chapter that describes how they may use qualitative methods of research in order to gather data towards answering their scientific question. The students are urged to critically evaluate qualitative method tools so that they may reject this type of research as most suitable for their scientific question. In any case, the students should provide a clear and concise argument as to why they would either use or reject qualitative methods as a way of answering their scientific question. This argument is more important than simply explaining how they could leverage qualitative research methods for their thesis.

## **Recommended time for the student to work**

The recommended amount of time outside of the three-hour meeting for this week is approximately 15 hours to become familiar with the qualitative research methods, as well as to write the argument in the recommended activity.

# METHODOLOGY AND DATA GATHERING – QUANTITATIVE METHODS

7<sup>th</sup> Week

## Introductory Remarks

Quantitative methods differ from qualitative ones. Whereas in qualitative research one is looking at data that cannot be put into numbers, such as bodies of text and answers to questions, quantitative methods seek to find relationships between numerical data. As such, questionnaires that ask questions that can be answered through the ascription of a number to a particular concept, are treated as a quantitative method.

Quantitative methods require some understanding of probabilities and statistics. Over the course of the next few meetings, our aim will be to become familiar with this type of analysis. Students will be provided with the required knowledge to design their own experiments and to carry out their own statistical analysis using appropriate statistics techniques and methods.

The students will begin by looking at various types of **Experimental Designs**, in other words, how to setup two or more groups of participants so that they can compare different types of effects on each group. The students will see types of **Factorial Designs**, an experimental design that compares many different groups that each may have more than one effect placed upon them by the experiment.

The experimental designs should be valid. **Validity** is the manner in which the different effects on each group of participants interacts with other effects. On the other hand, **Reliability** expresses the random error that can occur when choosing a set of participants, or any other error that can happen during the process of an experiment. To reduce random error, we do not assign participants to each experimental group specifically. Rather, we use a random process to place them in groups, called **Random Assignment**.

Finally, students need to understand the necessary ingredients for **Causation**, which is the expressed reliance of one experimental effect on another. In statistics, it is generally difficult to show causation, so instead we show **Correlation**. Correlation is a measure that shows that if one experimental effect varies, then another experimental effect varies together with the first one.

## Aim/Objectives

The aim of this meeting is for students to dissect the concept of an experiment, and toy with the idea of NxN experimental design.

## Learning Outcomes

Having completed this three hour meeting, the student will be able to differentiate experimental and nonexperimental designs. The student will also be able to critically assess a scientific question that requires quantitative evaluation, and provide a preliminary experimental design which should uphold structure, content, construct, and internal validity. The student should also be able to describe the factors needed to assess causation between variables, and perform and explain the process and goals of random assignment in scientific experimentation.

## Key Words

Experimental Design	Factorial Design	Validity
Correlation	Causation	Reliability
Random Assignment		

## Annotated Bibliography

### Basic Material

Howard, K. & Sharp, J.A., *The Management Of A Student Research Project*, Gower

### Supplementary Material

Notes and slides handed out by the instructor of the course

### Suggestions for further reading

King, R. S., *Research Methods For Information Systems*, Dulles: Mercury Learning.

## **Activity**

### **Activity 7.1**

The students should start forming their own conceptual framework towards examining the scientific question that is posed together with their supervisors. After this meeting the students must meet with their supervisors and decide which methods are suitable for data gathering depending on their thesis topic, and begin the development of an execution plan.

### **Recommended time for the student to work**

The recommended amount of time outside of the three-hour meeting for this week is approximately 15 hours, excluding the meeting with the students' supervisors.

## ANALYSIS AND DISCUSSION – DESCRIPTIVE STATISTICS

8<sup>th</sup> Week

### Introductory Remarks

Descriptive statistics are the basic elements upon which one builds an understanding of how any data behaves. It is imperative that the student understands descriptive statistics before moving on to the next meetings, because of the fundamental nature of the presented material.

There are several terms that need to be understood and put to use, in order for the student to receive experience in what each term measures and in which cases each term applies. For this reason, the terms are not explained in the introductory remarks, but rather they are left as an exercise to the reader to do a brief search and find the meaning and use of each. All the terms that are shown in the next section will be discussed during the three-hour meeting, but the students are expected to have done some work on the definition of each term prior to the actual meeting.

### Aim/Objectives

The aim of the meeting is for the students to grasp the concepts of descriptive statistics. As such, the objectives are the following:

1. Explain how to calculate, and explain what each of the following are:
  - a. Measures of central tendency
    - i. Mode
    - ii. Mean
    - iii. Median
  - b. Measures of Range
    - i. Interquartile Range
    - ii. Standard Deviation
    - iii. Range
    - iv. Variance
  - c. Other measures
    - i. Skewness
    - ii. Kurtosis

2. Design the following graphs and plots given data:
  - a. Stem-and-leaf plots
  - b. Box plots
  - c. Time plots
  - d. Scatter diagrams
3. Explain how these pertain to the overall understanding of the nature of the data one gathers.

## Learning Outcomes

During the meeting, the students will be introduced to the concepts of descriptive statistics. While these concepts may be basic, they are fundamental to the understanding of more advanced concepts in the analysis of gathered data. For this reason, the students need to perform several exercises that involve the calculation of each of the items mentioned in the "Aims and Objectives" section of this meeting, more preferentially in class.

The students should become familiar with tables and graphs, because these are used to easily summarize gathered data, both for quantitative and qualitative research purposes. The students must be able to create and interpret descriptive statistics along with related graphs and plots. They should be able to distinguish between the differences of different types of distributions, and to recognize these distributions, by looking at the measures of central tendency and through utilizing the measures of range.

Finally, the students are expected to define and explain relationships present in data sets, particularly through the creation and critical assessment of the scatterplot.

## Key Words

Central Tendency	Mode	Mean
Median	Range	Interquartile Range
Standard Deviation	Variance	Skewness
Measures	Kurtosis	Stem-and-leaf plots
Time plots	Scatter diagrams	

## Annotated Bibliography

### Basic Material

Howard, K. & Sharp, J.A., The Management Of A Student Research Project, Gower

King, R. S., Research Methods For Information Systems, Dulles: Mercury Learning.

### Supplementary Material

Notes and slides handed out by the instructor of the course

### Suggestions for further reading

Murray, R. (2011). How to Write a Thesis (Vol. 3rd ed). Maidenhead: McGraw-Hill Education.

Goshert, J. C. (2011) Entering the Academic Conversation: Strategies for Research Writing. Boston: Longman.

## Self-Assessment Exercises

### Exercise 8.1

For the following, present the data in the appropriate figure. Explain your choice. Label all axes.

- a. Survey respondents were asked to respond to the statement: "More money should be spent on health care for the elderly." Responses were on a scale of 1 (strongly disagree) to 7 (strongly agree).

Response	f
7	49
6	30
5	23
4	20
3	13
2	9
1	6

- b. Respondents are asked to indicate the type of dwelling in which they live.

Response	f
Single house	87
Duplex	6
Townhouse	9
Apartment	18
Mobile home	6

- c. A small company has each of its employees participate in a 5 km run, and their times are recorded.

Time (min)	<i>cf</i>
32–34	50
29–31	47
26–28	40
23–25	30
20–22	16
17–19	8
14–16	2

### Recommended time for the student to work

The recommended amount of time outside of the three-hour meeting for this week is approximately 25 hours.

## ANALYSIS AND DISCUSSION – PROBABILITY AND DISTRIBUTIONS

9<sup>th</sup> Week

### Introductory Remarks

The three-hour meeting on probability and distributions aims to bring the student closer to understanding how the scientific method works when the results of an experiment are analyzed. The student will become familiar with the concept of **Statistical Error**, and understand why and when statistical error is acceptable. Statistical Error is the unknown difference between what we measure and what is really true. In other words, it is the difference between the population measurement and the sample measurement.

As such, students need to understand **Probability and its Laws**, and understand the different ways that a **Random Sample** can be created, so that we can rely on statistics to tell us that our results do make sense. During the meeting, two types of error will be considered: **Type I** and **Type II**. Type I error occurs when we declare that we have a difference between two samples, when in fact we do not (false positive). On the other hand, Type II error occurs when we have enough evidence to show difference between two samples, and instead we declare that there is no difference (false negative).

While we live in a world where we are used to taking for granted anything that science says is true, we forget that scientific truth only works up to a point, and with specific assumptions and caveats. This is the take-away point of this meeting, but to be clearly elucidated, the point should be presented through an understanding of statistics and different types of distributions.

With this in mind, we will also examine the **Normal Distribution**, a function that represents the distribution of many random variables as a symmetrical bell-shaped graph. The normal distribution is a very useful and versatile tool in the world of statistics, and we will examine how we can use this tool towards analyzing our experiments.

### Aim/Objectives

After the students have been exposed to descriptive statistics, they must now understand and learn to use the tools of statistical inference. As such, students will study the concepts of probability and how these can be used to describe various types of experiments. They must also grasp and apply the concept of probability distribution. Finally, the students will be exposed to the

concept of a sampling distribution, and how that pertains to the actual population distribution. Thus, the students will also be presented the concept of random sampling.

## Learning Outcomes

By the end of the three-hour meeting the students should have a firm grasp and be able to use the fundamental laws of probability. The students should also work with the normal distribution, and critically assess how this distribution presents a host of assumptions in statistics, and also realize that normal distributions cannot be achieved through a sample of the population. In turn, they need to be exposed to the fact that sampling distributions can come close to the actual population distribution. They also need to recognize that even through random sampling, there may be samples that do not correctly represent the actual population.

Students should perform exercises that provide them with examples that show both correct and incorrect methods of sampling, and examine the concept of sampling bias. Finally, the students should become comfortable with the reality of statistical error, both Type-I and Type-II.

## Key Words

Distribution	Laws of Probability	Sampling
Statistical Error	Type-I	Type-II
Normal Distribution	Sample Distribution	

## Annotated Bibliography

### Basic Material

Howard, K. & Sharp, J.A., *The Management Of A Student Research Project*, Gower

King, R. S., *Research Methods For Information Systems*, Dulles: Mercury Learning.

### Supplementary Material

Notes and slides handed out by the instructor of the course

### Suggestions for further reading

Murray, R. (2011). *How to Write a Thesis* (Vol. 3rd ed). Maidenhead: McGraw-Hill Education.

Goshert, J. C. (2011) Entering the Academic Conversation: Strategies for Research Writing. Boston: Longman.

## Self-Assessment Exercises

### Exercise 9.1

1. In a science experiment a mouse must find its way through a maze. There are 24 different routes but 18 of these routes lead to dead ends. What is the probability that a mouse will successfully find its way through the maze three out of the 10 times it runs the maze, assuming that the mouse remembers nothing about the maze after each run?
2. In a bouquet of one dozen roses, two are pink, two are white, three are yellow, and five are orange.
  - a. If you close your eyes and pick one rose, what is the probability that it is pink? That it is yellow?
  - b. If you pick out one rose and then pick another one without replacement, what is the probability of picking a white rose followed by an orange rose? An orange rose followed by a yellow rose?
  - c. How many permutations are possible if you pick out smaller bouquets of three from the large bouquet?
- d. What is the probability of picking an orange, then a white, then a yellow, then another orange rose from the bouquet, without replacement?

### Exercise 9.2

1. A survey of auto mechanics in Detroit reveals that, at any given time, 40% of all cars brought in for repairs have problems with the fuel system.
  - a. If you were to select many random samples of 70 cars each, how often would you expect that 25 cars or fewer have problems with the fuel system?
  - b. Selecting many random samples of 100 cars, how often would you expect between 35 and 55 cars to be in for repairs to the fuel system?
2. When selecting random samples of 50 from a population with a mean of 125 and a standard deviation of 8, beyond what two values would the extreme 10% of mean differences fall?
3. When selecting random samples of 15 from the population in exercise 2 with a mean of 125 and a standard deviation of 8, how often would you expect to get means between 122 and 128?

## **Recommended time for the student to work**

The recommended amount of time outside of the three-hour meeting for this week is approximately 25 hours.

## ANALYSIS AND DISCUSSION – HYPOTHESIS TESTING

10<sup>th</sup> Week

### Introductory Remarks

The scientific method is partial to always have a specific goal when performing any analysis or experiment. This goal is called a **Hypothesis**. A hypothesis is the opinion of the scientist on what the result of the experiment performed should be. As such, there can be several types of hypotheses, but only two types of results: one that supports the hypothesis or one that rejects it. Usually the hypothesis is defined in terms of no change, and this is called the **Null Hypothesis**. The Null Hypothesis states that there will be no difference to the results prior the scientific intervention and after it. However, we also create the **Alternative Hypothesis**, which is the hypothesis that states the type of change we are looking for. As such, there may be several alternative hypotheses. For example we may be looking to see whether one sample's mean is strictly greater than the other's. This is a **One-Sided** hypothesis. Or we may be looking to see that one sample's mean is either greater or less than the other's. This is a **Two-Sided** hypothesis.

To examine an effect, we usually create **Independent samples**, different groups of participants that will undergo different treatments, and from which we will take different measurements and compare them. The comparison occurs through a statistical test called a **T-Test**. This test compares the means of the two samples and tells us how far apart they are, and whether this difference is statistically significant or not. However, if we have more than two samples, then we use a different type of test that gives us the **F-Statistic**, another measure of difference, but this time for more than two samples.

During this three-hour meeting the students will go through an experimental design session with the creation of several hypotheses, so that they can see functionally how an experiment is set up, when a hypothesis exists prior to the experiment. The students will then be familiarized with the ways that hypothesis testing occurs, and will experience first-hand how a hypothesis is rejected or not.

### Aim/Objectives

The overarching aim of this meeting is for the students to understand the effects of a hypothesis on the result of an experiment. The specific objectives are for the students to be able to create

correct hypotheses, and to state null and alternative hypotheses given a specific scientific question. The students must also be able to critically assess the results of their data analysis to provide statistical reasons for why a null hypothesis can be rejected.

## Learning Outcomes

At the end of this meeting the students should be able to correctly setup experiments together with null and alternative hypotheses. They should also be able to critically assess their analysis results as they were presented in the previous week to reject the null hypothesis. To do this, they must be able to choose confidence intervals, be they one- or two-sided. The students must be able to apply appropriate statistical tests using the t-distribution for single population means, as well as use the F statistic for independent samples.

## Key Words

T-test	Hypothesis	Null Hypothesis
Alternative Hypothesis	Independent samples	One-sided
Two-sided	F-statistic	

## Annotated Bibliography

### Basic Material

Howard, K. & Sharp, J.A., *The Management Of A Student Research Project*, Gower

King, R. S., *Research Methods For Information Systems*, Dulles: Mercury Learning.

### Supplementary Material

Notes and slides handed out by the instructor of the course

### Suggestions for further reading

Murray, R. (2011). *How to Write a Thesis* (Vol. 3rd ed). Maidenhead: McGraw-Hill Education.

Goshert, J. C. (2011) *Entering the Academic Conversation: Strategies for Research Writing*. Boston: Longman.

## Self-Assessment Exercises

### Exercise 10.1

1. National car emission statistics report that the mean level of emissions is 72 with a standard deviation of 5. A random sample of 50 cars from each of two cities is tested for emissions. The mean emission level for the sample from City A is 63. The mean level for the cars from City B is 59. Determine if the citizens of City A pollute more than those of City B. Use a .01 level of significance.
2. At a university, 30% of the population express an affiliation with a religious group. A sample of 500 students in the Faculty of Science reveals that 143 express an affiliation with a religious group. Using an alpha level of .05, determine if the students in the Faculty of Science are different from the general university population?

### Exercise 10.2

1. A survey conducted among 12 runners randomly selected from running clubs indicated that members ran, on average, 37.5 kilometers per week during the regular training season. A researcher wants to find out if this survey is representative of runners in Boulder. He selects a random sample of 15 runners from the local running club and tracks their weekly kilometers over a period of eight months. He finds that this group of runners averages 33 kilometers per week. Test the hypothesis at  $\alpha = .05$ . (**Note:** SS<sub>1</sub> = 1645; SS<sub>2</sub> = 2025).
2. American colleges and universities conducted a survey in 2010 that indicated that students participated in and/or watched varsity sports an average of 2.14 hours per week. A Students' Association representative at the local community college is certain that participation in varsity sports has decreased significantly since then. She surveys a sample of 49 students across the country to test her hypothesis. She finds that students now participate in and/or watch varsity sports an average of 1.63 hours per week. Test her hypothesis at  $\alpha = .05$ . (**Note:** s = 1.02).

### Exercise 10.3

1. A social psychologist was interested in how the presence of others affects performance on a timed test of mechanical aptitude. She randomly selected 60 participants and randomly assigned twenty to each of three treatment groups. A<sub>1</sub> participants completed the aptitude test alone. A<sub>2</sub> participants completed the test with one other test-taker present, and A<sub>3</sub> participants were in the presence of three other test-takers. Conduct the appropriate ANOVA to see if the presence of others made a difference in aptitude scores. Use an alpha level of .05.

**Alone (A<sub>1</sub>):** 105, 91, 79, 102, 85, 101, 96, 74, 101, 104, 90, 90, 102, 101, 81, 100, 83, 82, 94, 88

**One Other Present (A<sub>2</sub>):** 62, 93, 101, 60, 99, 72, 64, 107, 104, 93, 85, 79, 90, 73, 78, 107, 68, 91, 67, 85

**Three Others Present (A3):** 90, 111, 103, 66, 79, 74, 84, 92, 47, 74, 76, 108, 55, 76, 82, 88, 73, 101, 75, 57

### **Recommended time for the student to work**

The recommended amount of time outside of the three-hour meeting for this week is approximately 25 hours.

# ANALYSIS AND DISCUSSION – REGRESSION AND CORRELATION ANALYSIS

11<sup>th</sup> Week

## Introductory Remarks

Sometimes the scientific question of an experiment is not to examine whether something applies or not, but to see whether two variables have interaction. Usually this is to examine whether the value of one variable affects the value of another variable, and also, to examine how one value affects the other. This interaction is measured by a method and a statistic called **Correlation** and **Correlation Coefficient** respectively. Given that we have enough data, we can not only calculate the correlation between two interacting variables, but we can also build a statistical **Model**, an equation that shows us how to calculate one value from the other. This is called a **Regression** model.

There are two types of correlation: Pearson and Spearman. We use Pearson correlation only when our data conforms to the normal curve. If they do not, then we use Spearman's coefficient.

## Aim/Objectives

The aim of the meeting is to provide tools that the students can use to examine the interaction between two variables. These tools are called regression and correlation analysis. The students will see the tools and examine the various types of dependence, or interaction, that two variables may have. The scope of this meeting is only to present interactions that occur only between two variables, the independent and the dependent one.

## Learning Outcomes

During the meeting the students will work with Microsoft Excel using guided examples that the instructor will provide. These guided examples will exemplify how regression and correlation analysis are done in a widespread tool.

The students will examine cases where regression analysis is appropriate, and what correlation means. The students will also be given problems to critically assess the strength and direction of correlation between two variables.

The students will then be exposed to the quantification of a model that expresses the relationship between two variables, namely they will solve guided problems that involve the creation of regression equations.

Finally, the students will be exposed to the concept of causation, and how causation can be found through experimentation.

## Key Words

Regression	Correlation	Model
Variables	Causation	Pearson
Spearman		

## Annotated Bibliography

### Basic Material

Howard, K. & Sharp, J.A., The Management Of A Student Research Project, Gower

King, R. S., Research Methods For Information Systems, Dulles: Mercury Learning.

### Supplementary Material

Notes and slides handed out by the instructor of the course

### Suggestions for further reading

Murray, R. (2011). How to Write a Thesis (Vol. 3rd ed). Maidenhead: McGraw-Hill Education.

Goshert, J. C. (2011) Entering the Academic Conversation: Strategies for Research Writing. Boston: Longman.

## Self-Assessment Exercises

### Exercise 11.1

1. The Students' Association at a university is interested in determining whether government-funding cuts to the university have affected the number of new research grants obtained by faculty members from outside sources. The Students' Association collected data on the number of research grants awarded to faculty. They gathered data for the past eight years and want to determine the correlation between level of government funding and new

research grants acquired by faculty at the university. Do the appropriate analysis to answer the question. How much of variance is accounted for by the correlation?

Funding (\$)	New grants
10000	9
12000	11
9000	11
7000	6
8000	6
7500	5
7500	8
7500	6

2. A teacher is interested in determining if there is a relationship between the organizational skills of her 20 students and their mathematical ability. She ranks the students on a scale of 1 to 10 according to their organizational skills and uses their final exam grades to rank their mathematical ability. She finds the correlation between the two ranks to be 0.86. At  $\alpha = .01$ , use a two-tailed alternative to test the hypothesis that there is no correlation between organizational and mathematical ability. Which correlation test did the teacher use? What is your statistical decision? What is your conclusion?

### Exercise 11.2

1. The correlation between the scores on Dr. Evans' literacy test and final grade performance is 0.78. How much of the variability in final grade can Dr. Evans claim is associated with differences in ability as assessed by her literacy test?
2. The correlation between graduating average and IQ is 0.72. The correlation between graduating average and time spent studying is 0.87. The correlation between IQ and time spent studying is 0.65. What is the correlation between graduating average and IQ if the time spent studying variable is removed?

### Recommended time for the student to work

The recommended amount of time outside of the three-hour meeting for this week is approximately 25 hours.

# THE CONCLUSION

12<sup>th</sup> Week

## Introductory Remarks

Once a whole project is completed, and when the analysis and discussion sections are written, the thesis closes with a section called **Conclusions**. Here, the author presents succinctly once more what the whole point of the thesis was, presenting an **argument summary**, to remind the reader why the thesis topic is important, and why anyone should learn from the thesis. The thesis then, provides directions for **future research** with questions that are opened because of the thesis' results.

## Aim/Objectives

The students are exposed to the importance of the conclusion chapter in a thesis.

## Learning Outcomes

A good conclusion in a thesis reminds the reader what the significance of the research in the thesis was. It also reminds the reader what the original scientific question was, and why it was important in the first place. Finally a good conclusion extends the scientific conversation by presenting new questions that stem from the new research presented in the thesis.

Writing a good conclusion is not a talent but a skill. The aim of the one-to-last meeting is to provide the students with the tools to synthesize a good and memorable conclusion

## Key Words

Conclusion	Future Work	Argument Summary
------------	-------------	------------------

## Annotated Bibliography

### Basic Material

Howard, K. & Sharp, J.A., The Management Of A Student Research Project, Gower

## **Supplementary Material**

Notes and slides handed out by the instructor of the course

## **Suggestions for further reading**

Murray, R. (2011). How to Write a Thesis (Vol. 3rd ed). Maidenhead: McGraw-Hill Education.

Goshert, J. C. (2011) Entering the Academic Conversation: Strategies for Research Writing. Boston: Longman.

## **Recommended time for the student to work**

The recommended amount of time outside of the three-hour meeting for this week is approximately 25 hours.

## PRESENTATION AND MOCK DEFENSE

13<sup>th</sup> Week

### Introductory Remarks

The students should work autonomously, with the guidance of their thesis supervisor, to provide a first draft of their completed thesis.

### Aim/Objectives

The students will present their rough drafts to receive feedback from their peers and the instructor of the course.

### Learning Outcomes

Peer-review and feedback

### Annotated Bibliography

#### Basic Material

Howard, K. & Sharp, J.A., The Management Of A Student Research Project, Gower

#### Supplementary Material

Notes and slides handed out by the instructor of the course

#### Suggestions for further reading

Murray, R. (2011). How to Write a Thesis (Vol. 3rd ed). Maidenhead: McGraw-Hill Education.

Goshert, J. C. (2011) Entering the Academic Conversation: Strategies for Research Writing. Boston: Longman.

### Activity

Peer review: Provide feedback to your fellow students about their master's thesis. This feedback should always be constructive and not demeaning or insulting. Try to help your fellow students towards materializing their best work.

## **Recommended time for the student to work**

The recommended amount of time outside of the three-hour meeting for this week is approximately 35 hours.

## **PREPARATION, WRITING AND DEFENSE OF THE MASTER THESIS**

### **Recommended time for the student to work**

450 hours

## INDICATIVE ANSWERS TO SELF-ASSESSMENT EXERCISES

**WHAT IS RESEARCH – WEEK 1 &**  
**DISCUSSION OF THE RESEARCH PROJECT – WEEK 2 &**  
**THE LITERATURE REVIEW – WEEK 3 &**  
**THE LITERATURE REVIEW – CONTINUED – WEEK 4 & 5 &**  
**METHODOLOGY AND DATA GATHERING – QUALITATIVE METHODS – WEEK 6&**  
**METHODOLOGY AND DATA GATHERING – QUANTITATIVE METHODS – WEEK 7**

### **Exercises and Activities 1.1 – 7.1**

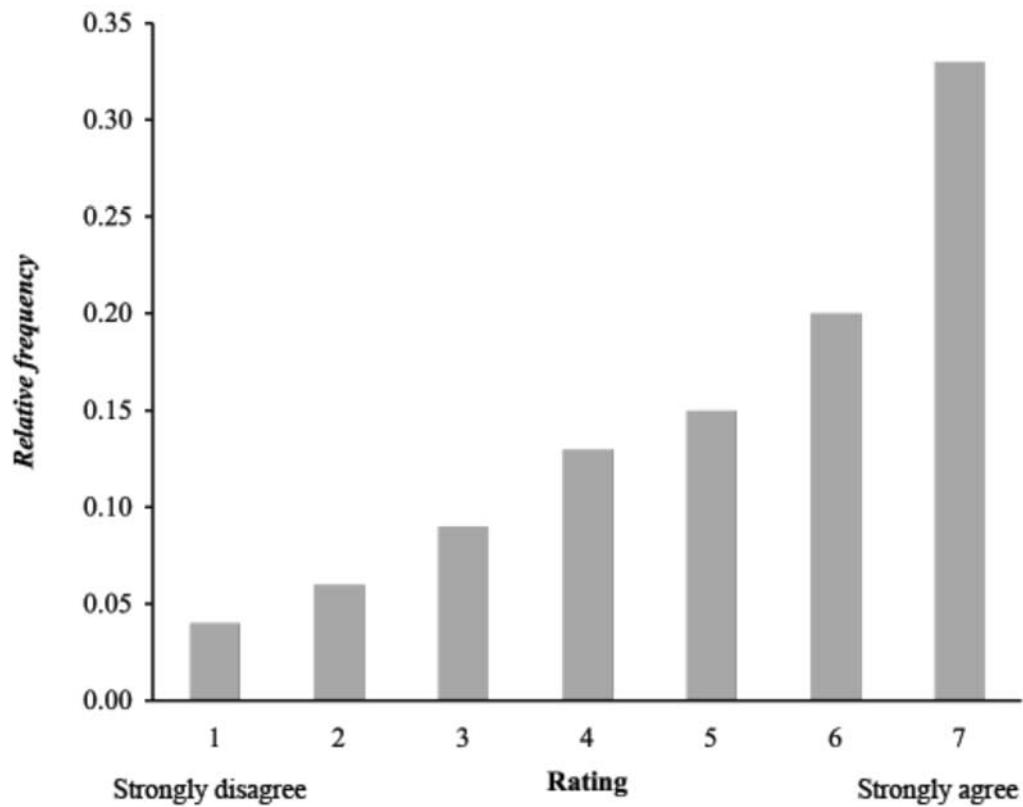
These exercises and activities are focused on the work that the student must perform to understand his or her research project, and as such, there are no model answers. In fact, only through the discussion with the Thesis supervisor will the student begin to grasp the method of performing scientific research. Thus, the exercises and activities are geared towards moving the student to the direction of completing several of his or her thesis chapters, which is work that should be guided, but where model answers cannot be provided.

### **ANALYSIS AND DISCUSSION – DESCRIPTIVE STATISTICS – WEEK 8**

#### **Exercise 8.1**

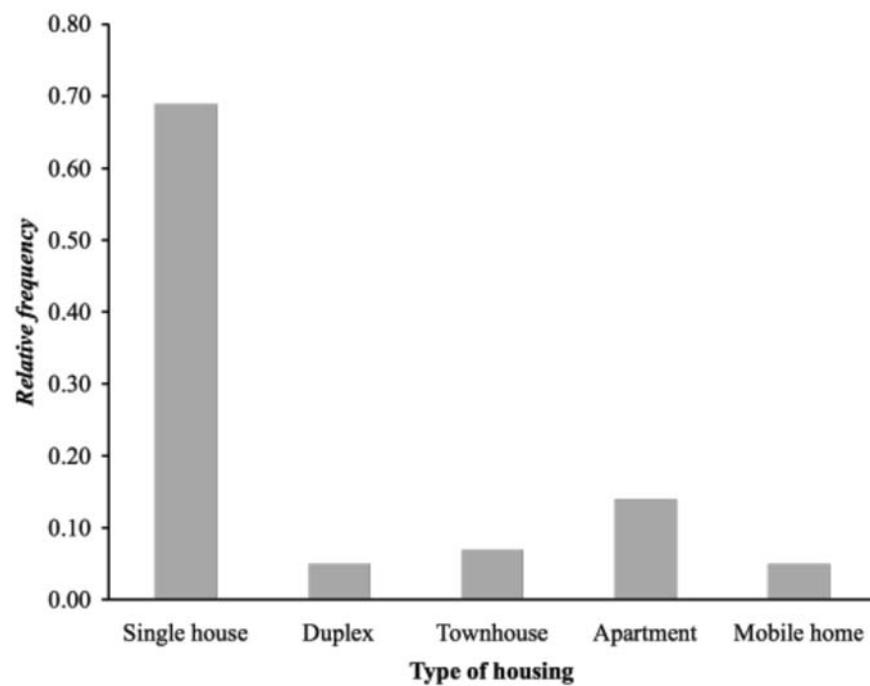
a.

Response	f	rf
7	49	0.33
6	30	0.20
5	23	0.15
4	20	0.13
3	13	0.09
2	9	0.06
1	6	0.04
<b>Sum</b>	<b>150</b>	<b>1</b>

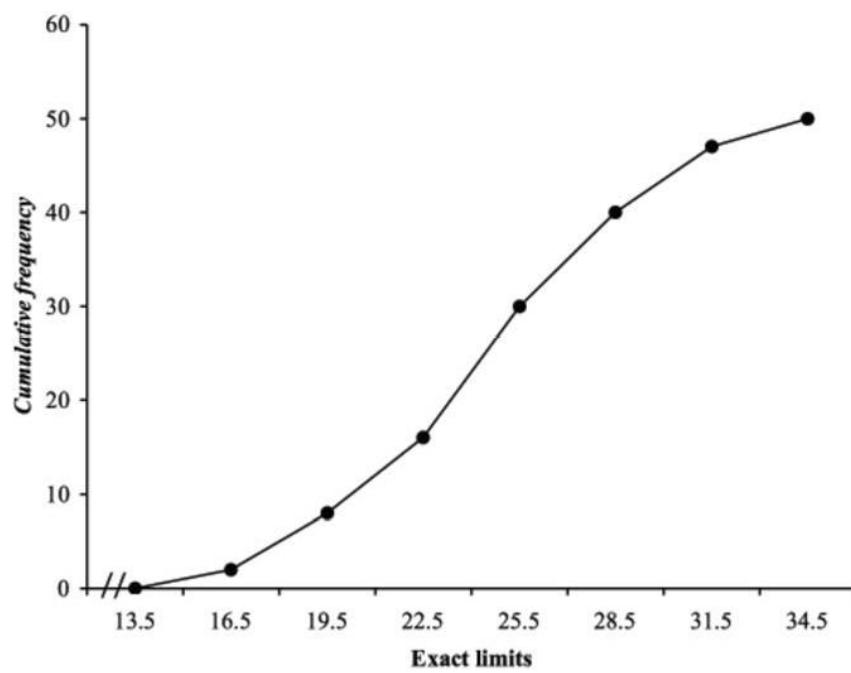


b.

Response	<i>rf</i>
Single house	0.69
Duplex	0.05
Townhouse	0.07
Apartment	0.14
Mobile home	0.05



c.



## ANALYSIS AND DISCUSSION – PROBABILITY AND DISTRIBUTIONS – WEEK 9

### Exercise 9.1

$$1. {}_{10}C_3 p^3 q^7 = \frac{10!}{(10-3)!3!} \binom{10}{3} \binom{7}{4} = 0.25$$

2.

a.  $p(\text{pink}) = 2/12 = 0.17$   $p(\text{yellow}) = 3/12 = 0.25$

b.  $p(\text{white and orange}) = 2/12 \cdot 5/11 = 0.076$

$p(\text{orange and white}) = 5/12 \cdot 2/11 = 0.075$

c.  ${}_{12}P_3 = 1320$

d.  $p = 5/12 \cdot 2/11 \cdot 3/10 \cdot 4/9 = 0.010$

3.

a.  $p(\text{navy}) = 2/13 = 0.154$

b.  $p(\text{green}) = 1/10 = 0.10$

c.  ${}_{13}C_2 = 78$

### Exercise 9.2

1.

a.  $z = \frac{p - P}{\sqrt{PQ/n}} = \frac{0.357 - 0.40}{\sqrt{(0.40)(0.60)/7}} = -0.734$

About 23% of the time.

b.  $z(35) = -1.02$   $z(55) = 3.06$

Area between  $z$  of 35 and mean = .3461 Area between  $z$  of 55 and mean = .4989

About 85% of the time.

2. Mean differences =  $\pm 1.654$  (1.6) =  $\pm 2.64$

3.  $z = \pm 1.02$  About 69% of the time.

## ANALYSIS AND DISCUSSION – HYPOTHESIS TESTING – WEEK 10

### Exercise 10.1

1. Directional alternative      Mean difference =  $63 - 59 = 4$

Standard error = 1

$z = 4$  Reject.

The citizens of City A pollute significantly more than the citizens of City B.

2. Non-directional alternative      Sample proportion = 0.286

Standard error = 0.0205

$z = -0.683$  Fail to reject.

There is no evidence that the science students differ from the general population.

### Exercise 10.2

1. Two-tailed  $t$ -test for the difference between independent means

	Group 1	Group 2
$M$	37.5	33
$SS$	1645	2025
$n$	12	15
$df$	25	
$SE$	4.69	
$t$	0.96	Fail to reject

There is no significant difference between the groups.

2. One-tailed  $t$ -test for a single mean

$M$	1.63
$\mu$	2.14
Numerator	-0.51
$SE$	0.146
$t$	-3.5
$s$	1.02
$n$	49

Reject the null. Participation has significantly decreased since 2010.

### Exercise 10.3

1. One-way ANOVA: Excel output

## Anova: Single Factor SUMMARY

<b>Groups</b>	<b>Count</b>	<b>Sum</b>	<b>Average</b>	<b>Variance</b>
A1	20	1849	92.45	89.734
A2	20	1678	83.90	239.568
A3	20	1611	80.55	297.629

## ANOVA

<b>Source of Variation</b>	<b>SS</b>	<b>df</b>	<b>MS</b>	<b>F</b>	<b>P-value</b>	<b>F<sub>crit</sub></b>
Between Groups	1506.233	2	753.117	3.604	0.034	3.159
Within Groups	11911.700	57	208.977			
Total	13417.933	59				

Reject the null. At least two means were significantly different.

## ANALYSIS AND DISCUSSION – REGRESSION AND CORRELATION – WEEK 11

### Exercise 11.1

1. Pearson's  $\rho = 0.80 \rho^2 = 0.64$
2. Spearman rank-order correlation test.

$$\rho_{0.01} = 0.57$$

$$\rho_{0.05} = 0.86$$

Reject the null. There is a significant correlation between the ranks.

### Exercise 11.2

3. About 61% of the variance is explained by the correlation.

$$4. R_P = \frac{0.72 - (0.87)(0.65)}{\sqrt{1 - 0.82^2}(1 - 0.65^2)} = 0.41$$

## ANNEX 1

(COVER PAGE)



TITLE (AND SUBTITLE IF APPLICABLE)  
OF MASTER THESIS

BY

(Student's name)

**MASTER OF SCIENCE  
IN CYBERSECURITY**

**NICOSIA**

Month, Year

## **ANNEX 2**

(TITLE PAGE)

TITLE (AND SUBTITLE IF APPLICABLE)

BY

(Student's Name)

(Student's Reg. No.)

**Master Thesis**

**Submitted in partial fulfilment of the requirements for the Degree of**

**Master in Cybersecurity**

**NICOSIA**

Month, Year

## **ANNEX 3**

**EUROPEAN UNIVERSITY CYPRUS  
SCHOOL OF SCIENCES**

**DECLARATION OF ACCEPTANCE**

The Master Thesis with title ". ....", which was prepared by ..... to obtain a postgraduate degree in Cybersecurity

approved on ..... following the suggestion of the Members of the Evaluation Committee:

- 1.
- 2.

**DEAN OF SCHOOL OF SCIENCES**

---

Date and Stamp

---

## **ANNEX 4**

### **DECLARATION**

I ..... (student's name) hereby declare that the present master's thesis with title "....." (title of thesis) was composed by myself and that the work contained herein is my own. I also confirm that I have only used the specified resources. All formulations and concepts taken verbatim or in substance from printed or unprinted material or from the Internet have been cited according to the rules of good scientific practice and indicated by footnotes or other exact references to the original source.

I understand that the provision of incorrect information may have legal consequences.

**Candidate**

---

(student's signature)

## **ANNEX 5**

**EUROPEAN UNIVERSITY CYPRUS  
SCHOOL OF SCIENCES**

**EVALUATION OF MASTER THESIS**

Author Name: .....

Reg. No.: .....

Thesis Title

.....  
.....  
.....  
.....

**GRADE:**

a) Supervisor:

Report: ..... Oral Defense: .....

b) 2<sup>nd</sup> member

Report: ..... Oral Defense: .....

c) 3<sup>rd</sup> member

Report: ..... Oral Defense: .....

Total Grading: Number:..... Letter:.....

### **Comments of the Evaluation Committee:**

## **The Evaluation Committee:**

Supervisor: .....

2<sup>nd</sup> member: .....

3<sup>rd</sup> member: .....

Date: .....