Ευρωπαϊκό
Πανεπιστήμιο Κύπρου
LAUREATE INTERNATIONAL UNIVERSITIES

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΠΑΡΑΤΗΡΗΣΕΙΣ
για την Έκθεση της Επιτροπής Εξωτερικής Αξιολόγησης του Φορέα Διασφάλισης και Πιστοποίησης της Ποιότητας της Ανώτερης Εκπαίδευσης.

ΓΙΑ ΤΟ ΠΡΟΓΡΑΜΜΑ

«Cybersecurity (M.Sc.)»

12 Οκτωβρίου 2016

Ευρωπαϊκό
Πανεπιστήμιο Κύπρου
LAUREATE INTERNATIONAL UNIVERSITIES

Παρατηρήσεις για την Έκθεση της Επιτροπής Εξωτερικής Αξιολόγησης

«Cybersecurity (M.Sc.)»

Η Σχολή Θετικών Επιστημών του Ευρωπαϊκού Πανεπιστημίου Κύπρου ευχαριστεί θερμά το ΔΙ.Π.Α.Ε. και την Επιτροπή Αξιολόγησης για την αξιολόγηση του μεταπτυχιακού μας προγράμματος «Cybersecurity (M.Sc.)». Τα εποικοδομητικά σχόλια και οι σημαντικές εισηγήσεις της Επιτροπής είναι για μας εργαλείο βελτίωσης και αναβάθμισης του περιεχομένου του προγράμματος.

Θέλουμε να διαβεβαιώσουμε την Επιτροπή ότι λαμβάνουμε πολύ σοβαρά υπόψη **όλες** τις εισηγήσεις που περιλαμβάνονται στην έκθεσή της, τις οποίες υλοποιούμε, όπως παρατίθεται πιο κάτω, αναλυτικά.

1. **Να προστεθεί ένα εισαγωγικό μάθημα που να εισάγει τους φοιτητές στις βασικές έννοιες και τεχνικές cybersecurity.**

   Έχει προστεθεί ένα νέο εισαγωγικό μάθημα 'Introduction to Cybersecurity', το οποίο θα πάρει τη θέση του 'Research Methods and Statistical Analysis' στο πρώτο εξάμηνο. Μπορείτε να δείτε τις αλλαγές στις επισυναπτόμενες περιγραφές μαθημάτων.
   (**Παράρτημα 1**).

2. **Να εμπλουτιστεί το μάθημα του network security με γενικότερες μεθόδους προστασίας και ελέγχου δικτύων - διαδικτύου.**

   Το μάθημα Communications and Network Security έχει εμπλουτιστεί με υλικό πιο στοχευμένο στις μεθόδους προστασίας και αποτροπής επιθέσεων και ελέγχου δικτύων – διαδικτύου. Συγκεκριμένα, στον κάθο τύπο επιθέσεων συμπεριλαμβάνονται και οι αντίστοιχες μέθοδοι προστασίας. Μπορείτε να δείτε τις αλλαγές στις επισυναπτόμενες περιγραφές μαθημάτων (**Παράρτημα 1**).

3. **Το μάθημα Research Methods and Statistical Analysis μπορεί να μεταφερθεί στα μαθήματα επιλογής και να ενισχυθούν αντικείμενα όπως το IT and Law, καθώς επίσης και το database security το οποίο αποτελεί ένα κλασσικό αντικείμενο στην κατεύθυνση αυτή, με ιδιαίτερο πρακτικό ενδιαφέρον.**

   Το μάθημα Research Methods and Statistical Analysis έχει ενσωματωθεί στη διδασκαλία του μαθήματος Master Thesis το οποίο έχει 22 ECTS.

Το εισαγωγικό μάθημα 'Introduction to Cybersecurity' έχει εμπλουτιστεί με ασφάλεια βάσεων δεδομένων καθώς και με άλλα σημαντικά για την εποχή αντικείμενα όπως το IT and Law. Δεδομένου της σημασίας της ασφάλειας των βάσεων δεδομένων, έχουμε προσθέσει σχετικό περιεχόμενο και στο μάθημα 'Cybersecurity Architecture and Operations'.
(Παράρτημα 1)

4. **Το μάθημα Risk Analysis and Management πρέπει να δώσει έμφαση σε information & network security risks και να μην είναι τόσο γενικό όσο περιγράφεται στην αναλυτική περιγραφή του μαθήματος**

   Συμφωνούμε με την άποψη της επιτροπής και για αυτό το λόγο το περιεχόμενο του μαθήματος ‘Risk Analysis and Management ‘ έχει γίνει πιο συγκεκριμένο με αναφορά σε κινδύνους κυβερνοασφάλειας.

5. **Αναφορικά με τα 1.2.6 επισημαίνεται ότι δεν έχει ακόμα προσδιοριστεί και εγκατασταθεί το ειδικό εκείνο λογισμικό που είναι απαραίτητο για τη διδασκαλία ενός τέτοιου αντικειμένου (risk assessment software, access control software, forensic software, etc.).**

   Έχει ετοιμαστεί κατάλογος με το ειδικό λογισμικό που χρειάζεται να εγκατασταθεί στα εργαστήρια, ούτως ώστε να καταστεί δυνατή η βέλτιστη διδασκαλία του κάθε μαθήματος. Αναλυτικά μπορείτε να βρείτε στον κατάλογο που επισυνάπτεται **(Παράρτημα 2)**, ο ειδικός εργαστηριακός εξοπλισμός που χρειάζεται να αγορασθεί, το όνομα του κάθε εξειδικευμένου λογισμικού και τα μαθήματα στα οποία αυτό θα χρησιμοποιηθεί. Έχει ήδη προβλεφθεί στον προϋπολογισμό, προς άμεση ενέργεια, αμέσως μετά από την έγκριση του προγράμματος.

6. **Απαιτείται επίσης πρόσληψη εξειδικευμένου προσωπικού για το χειρισμό τους.**

   Το Πανεπιστήμιο προβαίνει πάντα σε όλες τις προσλήψεις οι οποίες είναι αναγκαίες για την υλοποίηση των Προγραμμάτων του. Και στη συγκεκριμένη περίπτωση, όταν δοθεί η άδεια λειτουργίας του Προγράμματος, θα πραγματοποιηθούν και οι προσλήψεις εξειδικευμένου προσωπικού για το χειρισμό του ειδικού λογισμικού.

....

Δρ Χρήστος Δημόπουλος, Αναπληρωτής Καθηγητής
Κοσμήτορας
Σχολή Θετικών Επιστημών

European
University Cyprus
LAUREATE INTERNATIONAL UNIVERSITIES

Παράρτημα 1

«CYBERSECURITY (M.Sc.)»

GENERAL OBJECTIVES:

- To provide education leading to an academic degree, namely a Master of Science in Cybersecurity.
- To develop the student's capacity to think, write and speak effectively and creatively.
- To develop the student's analytical, decision-making and communication competencies together with those qualities of self-reliance, responsibility, integrity and self-awareness which will promote personal achievement and contribution to organizations.
- To obtain a good grounding in advanced topics in Cybersecurity through the core subjects and attain specialization through the elective courses.
- To provide the student with the advanced skills, necessary for further advancement in an academic and/or professional career.

SPECIFIC OBJECTIVES:

- To intensify and deepen knowledge gained in the Bachelors programs in Computer / Electrical / Electronic Engineering.
- To prepare students for a lifetime career in industry, government and various institutions in the area of Cybersecurity, by establishing a foundation for lifelong learning and development.
- To ensure a learning experience which will provide students with the theoretical background and the applied know-how for practitioners in Cybersecurity to enter any sector of the industry as key personnel.
- To promote cybersecurity / network and information security in Cyprus through education, research and practical experience.
- To expose students to the area of scientific research and independent study and to demonstrate creativity and conduct original research work through the completion of the M.Sc. thesis in a specialized topic in the area of Cybersecurity.
- To analyse and specify the people, process and technology requirements appropriate for a solution to a problem in the area of Cybersecurity.

- To design, implement, and evaluate solutions to Cybersecurity problems, according the desired specifications.
- To apply information security foundations and principles during the modelling, design, and evaluation of preventive, detective and corrective cybersecurity controls, in a way that demonstrates comprehension of the trade-offs involved in design choices.

LEARNING OUTCOMES:

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

- Gain a detailed understanding of the interdisciplinary aspects (technical, business, management, policy) of cybersecurity
- Acquire all the necessary skills to develop a holistic approach to all relevant factors interacting with Cybersecurity.
- Assess the information security risks faced by an organization
- Manage the development, acquisition and evolution of a secure information infrastructure
- Gain expertise in both theory and practice of cybersecurity
- Acquire a detailed understanding of cybersecurity challenges in networks and software systems
- Design and implement networked, software and distributed systems with cybersecurity in mind
- Gain expertise to manage the growing complexities associated with securing data and networks
- Secure both clean and corrupted systems, protecting personal data, securing simple computer networks, and safe Internet usage
- Understand key terms and concepts in cyber law, intellectual property, cybercrime and cyber safety.
- Incorporate approaches to secure networks, firewalls, intrusion detection systems, and intrusion prevention systems
- Examine secure software construction practices
- Understand principles of web security
- Incorporate approaches for incident analysis and response
- Incorporate approaches for risk management and best practices
- Equip students with skills to assume a leadership position in cybersecurity

DEGREE REQUIREMENTS	ECTS
Compulsory courses	52
Elective courses	16
Master Thesis	22
Total ECTS	**90**

DEGREE REQUIREMENTS		ECTS
Compulsory courses		**52**
CYS601	Introduction to Cybersecurity	7
CYS610	Communications and Network Security	7
CYS620	Cryptography	8
CYS640	Cybersecurity Policy, Governance, Law and Compliance	10
CYS650	Cybersecurity Risk Analysis and Management	10
CYS660	Cybersecurity Architecture and Operations	10
Master Thesis		
CYS690	**Master Thesis**	**22**
Elective courses **(Students select two from the following courses)**		**16**
CYS631 - Current Trends in Cybersecurity		8
CYS632 - Machine Learning for Cybersecurity		8
CYS633 - Data Privacy in the era of Data Mining and AI		8
CYS634 - Ethical Hacking and Penetration Testing		8
CYS635 - Incident Response and Forensic Analysis		8
Total ECTS		**90**

Course Title	Introduction to Cybersecurity				
Course Code	CYS601				
Course Type	Compulsory				
Level	Master (2nd cycle)				
Year / Semester	1st Year / 1st Semester				
Teacher’s Name	TBA				
ECTS	7	Lectures / week	3 Hours	Laboratories / week	None
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	Upon succesful completion of this course students should be able to: • Describe the meaning and position of fundamental cybersecurity concepts and terminology • Explain the position of the different topics within cybersecurity and how they fit into a comprehensive cybersecurity model • Classify and describe different cybersecurity components and how they contribute to effective defence • Classify and describe different potential routes for cyber attacks.				
Prerequisites	None	Co-requisites	None		
Course Content	Introduction: 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. History of cybersecurity: important attacks and consequences. Related history (e.g. the important role of cryptography and cryptanalysis in World War II, etc.) Current importance of cybersecurity, 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. Asset protection (including data) as a valuable business operation and its contribution to business survivability. Main principles of cybersecurity – 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. Introduction to the phases of cybersecurity – Identify, Protect, Detect, Respond, Recover. Applicable cybersecurity and IT law Software licensing, Data privacy and security, Electronic signatures, Legal and regulatory risks, cyberattacks, digital forensics, liability issues, trust. Introduction to other courses in this MSc (to aid selection of the elective courses). Introduction to specific cybersecurity topics – database security, secure software development, malware analysis, etc. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on usual network attacks and methods for protection.
Teaching Methodology	Face – to – face
Bibliography	*“Introduction to Computer Networks and Cybersecurity”,* by Chwan-Hwa (John) Wu and J. David Irwin *“Cybersecurity Foundations: An Interdisciplinary Introduction Hardcover”*, by Lee Mark Zeichner IEEE Journals, Magazines and Websites (ISC)^2, ISACA, and other cybersecurity websites

Assessment	Examinations 60% Assignment(s) 40% 100%
Language	English

Course Title	Communications and Network Security				
Course Code	CYS610				
Course Type	Compulsory				
Level	Master (2nd cycle)				
Year / Semester	1st Year / 1st Semester				
Teacher’s Name	Demetris Antoniades				
ECTS	7	Lectures / week	3 Hours	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	Upon succesful completion of this course students should be able to: • Describe the underlying principles of networking layers, architecture, topologies, protocol stacks, 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.				
Prerequisites	None	Co-requisites	None		
Course Content	Introduction: 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. Principles: the network as a route for cyberattacks, how the network can be protected, vulnerabilities, threats. Network Attacks: scanning, malware, (D)DoS, route poisoning, MAC spoofing, sniffing, authentication attacks, man-in-the-midde, session takeover, wiretaps, MAC table flooding, ARP poisoning, ICMP attacks, DNS poisoning, smurf and fraggle attacks, phishing, spam,				

	war-dialing, methods to prevent the network attacks that have been covered (within the discussion of each attack type). Wireless Attacks: 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). General protection, prevention and detection: 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. 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. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on usual network attacks and methods for protection.
Teaching Methodology	Face – to – face
Bibliography	*“Computer Networks (5th Edition)”*, by Andrew S. Tanenbaum and David J. Wetherall *“Network and System Security, Second Edition”*, by John R. Vacca *“Network Security Essentials: Applications and Standards (5th Edition)”*, by William Stallings IEEE Journals and Magazines
Assessment	Examinations 60% Assignment(s) 40% 100%
Language	English

Course Title	Cryptography				
Course Code	CYS620				
Course Type	Compulsory				
Level	Master (2nd cycle)				
Year / Semester	1st Year / 1st Semester				
Teacher's Name	Marina Nikiforou				
ECTS	8	Lectures / week	3 Hours	Laboratories / week	None
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	Upon succesful completion of this course students should be able to: • Describe the underlying principles of cryptography, clear text, plain text, algorithms, and keys. • Explain the different kinds of encryption methods (symmetric, asymmetric) and the differences between them. • Classify and describe a number of different encryption algorithms and the way that they work. • Describe the mathematical principles behind encryption and the mathematical properties of ciphertext. • Describe and evaluate different methods used to crack encryption. • Explain the different uses of encryption methods and the security objectives that they meet.				
Prerequisites	None		Co-requisites	None	
Course Content	Introduction: History of cryptography, early forms, cryptosystem strength, Caesar cipher, one time pad, steganography. Principles: basic cryptographic functions – substitution ciphers and transposition ciphers, symmetric and asymmetric algorithms, block and stream ciphers, hybrid systems.				

	Symmetric systems: DES, 3-DES, AES, IDEA, Blowfish, RC4-5-6, Twofish, Serpent, others, uses and cryptographic services provided. Asymmetric systems: Diffie-Hellman algorithm, RSA, El Gamal, Elliptic Curve systems, zero knowledge proof, SSL/TLS, PGP, S/MIME, Bitcoin. Public key systems: one-way algorithms, public and private keys, public key infrastructure, certificate and trust authorities, distributed trust systems. Other cryptographic services: message and file integrity, hashing, digital certificates, digital signatures, key management. Attacks: known and chosen plaintext attacks, ciphertext attacks, analytical attacks, frequency analysis, statistical attacks, social engineering attacks. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the uses of cryptography in real systems.
Teaching Methodology	Face – to – face
Bibliography	*“Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series)”*, by Jonathan Katz and Yehuda Lindell *“Understanding Cryptography: A Textbook for Students and Practitioners”*, by Christof Paar and Jan Pelzl *“Applied Cryptography: Protocols, Algorithms and Source Code”*, by Bruce Schneier *“Modern Cryptanalysis: Techniques for Advanced Code Breaking”*, by Christopher Swenson IEEE Journals and Magazines
Assessment	Examinations 60% Assignment(s) 40% 100%
Language	English

Course Title	Cybersecurity Policy, Governance, Law and Compliance				
Course Code	CYS640				
Course Type	Compulsory				
Level	Master (2nd cycle)				
Year / Semester	1st Year / 2nd Semester				
Teacher's Name	Ioanna Danidou				
ECTS	10	Lectures / week	3 Hours	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	Upon succesful completion of this course, students should be able to: • State and identify concepts relating to organizational cybersecurity policy, governance mechanisms, applicable legislation and compliance requirements for information security. • State and interpret the different components of a comprehensive organizational cybersecurity policy. • State and interpret the role of security policy within an organization and its position with relation to other controls within a comprehensive cybersecurity environment. • Describe the role of corporate governance with regards to cybersecurity, and the business reasons for implementing a cybersecurity function. • Recognize and explain major applicable legislation and regulatory framework (local, European, international). • Define, explain and exemplify compliance requirements in relation to cybersecurity, information security, data protection (privacy) and critical information infrastructure protection.				
Prerequisites	None	Co-requisites	None		
Course Content	Introduction: 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. Principles: Information security components and concepts, confidentiality, integrity, availability. Policy: definition, role of policy in an organization, statement of management purpose and organizational objectives, description of organizational approach, standards, baselines, guidelines, procedures. Governance: 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. Law: 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. IT and Law: 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. Compliance: Reasons for specific cybersecurity legislation beyond cybercrime, compliance requirements, self-assessment, auditing principles, audit process. 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.
Teaching Methodology	Face – to – face
Bibliography	*“Security Risk Management: Building an Information Security Risk Management Program from the Ground Up”*, by Evan Wheeler

	“Information Security Governance: A Practical Development and Implementation Approach”, by Krag Brotby *“Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats”*, by Scott E. Donaldson *“Cyber Security and IT Infrastructure Protection”*, by John R. Vacca IEEE Journals and Magazines
Assessment	Examinations 60% Assignment(s) 40% 100%
Language	English

Course Title	Cybersecurity Risk Analysis and Management				
Course Code	CYS650				
Course Type	Compulsory				
Level	Master (2nd cycle)				
Year / Semester	1st Year / 2nd Semester				
Teacher's Name	George Stylianou				
ECTS	10	Lectures / week	3 Hours	Laboratories / week	None
Course Purpose and Objectives	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 organizations assets according to the risk appetite of senior management.				
Learning Outcomes	Upon succesful completion of this course students 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.				
Prerequisites	None	Co-requisites	None		

Course Content	Introduction: Definition of cybersecurity risk and associated terminology, the position of risk analysis and management in relation to the other components of a cybersecurity programme. Principles: Assets, vulnerabilities, threats, threat actors, likelihood. Management of risks compared to simple acceptance. Risk treatment options: avoidance, mitigation, transfer, acceptance. Assets: 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. Vulnerabilities: 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. Threats: 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. Risk analysis: 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. Risk management: 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. 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.
Teaching Methodology	Face – to – face
Bibliography	*"Security Risk Management: Building an Information Security Risk*

	Management Program from the Ground Up”, by Evan Wheeler *“How to Measure Anything in Cybersecurity Risk”*, by Douglas W. Hubbard and Richard Seiersen *“The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)”*, by Anne Kohnke and Dan Shoemaker
Assessment	Examinations 60% Assignment(s) 40% 100%
Language	English

Course Title	Cybersecurity Architecture and Operations				
Course Code	CYS660				
Course Type	Compulsory				
Level	Master (2nd cycle)				
Year / Semester	1st Year / 2nd Semester				
Teacher's Name	Ghanan Glezer				
ECTS	10	Lectures / week	3 Hours	Laboratories / week	None
Course Purpose and Objectives	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.				
Learning Outcomes	Upon succesful completion of this course students should be able to: • Identify the various components of a comprehensive cybersecurity architecture within an organization. • Describe the underlying principles of defense in depth and control objectives associated with the outputs of a risk assessment. • Describe and classify controls that meet specific control objectives and to treat identified risks. • 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. • Describe the five phases of cybersecurity operations: Identify, Protect, Detect, Respond, Recover. • Evaluate available controls and the degree to which they mitigate risks. • Select and propose additional controls as appropriate. • Describe and evaluate the processes of vulnerability management, penetration testing, exercising, change management, incident response, and others. • Recognise and explain the differences between normal and				

	emergency operations. • Classify and describe a number of different effects of main cybersecurity controls on the operational environment, e.g. access control. • Evaluate and select appropriate architectural and operational options according to the organizational risk environment.		
Prerequisites	None	Co-requisites	None
Course Content	Introduction: Definition of security objectives: confidentiality, integrity, availability, accountability non-repudiation, authentication. Processes: User provisioning, access control, vulnerability management, penetration testing, exercising, change management, incident response, others. Phases: Phases of cybersecurity operations, in relation to the before and after of an incident: Identify, Protect, Detect, Respond, Recover. Identify: Identification of organizational assets, threats, vulnerabilities and risks (details in risk assessment course), vulnerability management (open databases, CVE, etc.) as an essential process. Protect: 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. Detect: Detection of cybersecurity incidents as they occur, evaluation of impacts, log analysis, IDS/IPS, attack vector analysis, SIEM (security incident and event management), indicatiors of compromise (IOC). Respond: Incident triage and response, CERT/CSIRTs, triggering and implementation of business continuity and disaster recovery plans, corrective controls. Recover: Orderly and planned return to prior operational status and capabilities, lessons learned, evaluation of corrective controls and supporting processes. Specific cybersecurity operations topics: Database security, secure software development, mechanisms for ensuring the security of information at rest, in transit, and during processing, side-channel considerations.		

	Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the practicalities of cybersecurity operations in real environments.
Teaching Methodology	Face – to – face
Bibliography	*“Cybersecurity Operations Handbook”*, by John Rittinghouse and William M. Hancock *“Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”*, by Thomas A. Johnson (Editor) *“The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)”*, by Anne Kohnke and Dan Shoemaker ISO *27002 - Information technology – Security techniques – Code of practice for information security management* COBIT 5 SANS 20 Critical Controls Australia Defense Signals Directorate Top Mitigations IEEE Journals and Magazines
Assessment	Examinations 60% Assignment(s) 40% 100%
Language	English

Course Title	Master Thesis				
Course Code	CYS690				
Course Type	Compulsory				
Level	Master (2nd cycle)				
Year / Semester	2nd Year / 3rd Semester				
Teacher's Name	George Christou				
ECTS	22	Lectures / week	None	Laboratories / week	None
Course Purpose and Objectives	• The student acquires the necessary skills to enable the successful completion of a project. Established research methods for independent research are introduced using methodical processes. This is related to general objectives 5 and 6. • Develop an ability to organize and carry out an extended, independent and novel scientific research work at postgraduate level, employing concepts and methods learned in the program • Synthesize concepts and methods learned in more than one course, and exhibit awareness of previous work in the area of study. • Give a deeper knowledge of the subject at hand and to give an insight into the working processes used within a company, other institutions or within a department. • Extend the knowledge and skills developed in the taught components of the courses of the program • Prepare the student for future independent work as a Master of Science.				
Learning Outcomes	Upon successful completion of this course students should 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.		
Prerequisites	Consent of Instructor	Co-requisites	None
Course Content	Part A: Research Methods: The nature of research: Definitions and types of research; research process; topic selection and scope; feasibility and value. 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. Project management: Methods, techniques and tools for research design, and data collection. Analysis and synthesis: Statistical and qualitative techniques for data analysis; use of appropriate software. Reliability and validity of research projects. Presentation of research findings: Project structure; conventions on citation and quotations; style of writing a report. Part B: Thesis: Students will submit an initial proposal for a project. The project co-coordinator will then allocate an academic supervisor who will liaise with the student to review the initial proposal and to ensure that that the scope of the project is consistent with that of a Masters degree. This will then be followed by an initial report of about 10 pages, which will further expand on: • What the project is intend to achieve. • Why the project is important from an academic and industrial perspective. • How the project will be achieved including proposed methods and techniques. • How the project will be managed.		

	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: **Student:** • To identify and scope a suitable problem • Explain the value of the research • To plan and control the project • To carry out the necessary work • To review and evaluate the work done • To prepare and present the project deliverables • To initiate and maintain contact with the academic supervisor **Academic Supervisor:** • To comment on the suitability of the selected project • To discuss the mapping of the project onto the course requirements • To discuss and approve the intended deliverables • To suggest starting points for consideration of background research • To discuss the nature of the thesis and comment on early drafts • To provide advice on issues associated with the project such as design, implementation, and proof of concept as appropriate. To attend any presentation or demonstration of the project
Teaching Methodology	For Part A: Research Methods there will be research seminars and a number of face–to–face sessions with the instructor. For Part B: Face-to-face
Bibliography	Specified by the instructor Howard, K. & Sharp, J.A., THE MANAGEMENT OF A STUDENT RESEARCH PROJECT, Gower Turk, C. & Kirkman, J., EFFECTIVE WRITING: IMPROVING SCIENTIFIC, TECHNICAL AND BUSINESS COMMUNICATION, Chapman & Hall J. Zobel., WRITING FOR COMPUTER SCIENCE, Springer.

	W. Navidi, Statistics for Engineers and Scientists, McGraw-Hill Science/Engineering/Math; Latest Edition. Statistical Methods for Engineers, by Geoffrey Vining and Scott M. Kowalski, Thomson, Brooks/Cole, Latest Edition. J.G. Paradis, M., Zimmerman,THE MIT GUIDE TO SCIENCE AND ENGINEERING COMMUNICATION, The MIT Press. D. Madsen, SUCCESSFUL DISSERTATIONS AND THESES., A GUIDE TO GRADUATE STUDENT RESEARCH FROM PROPOSAL TO COMPLETION, Jossey Bass. T. Cornford, S. Smithson, PROJECT RESEARCH IN INFORMATION SYSTEMS., A STUDENT'S GUIDE, Macmillian
Assessment	**ASSESSMENT STRATEGY:** The specific deliverables for each individual's project must be discussed and decided upon in consultation with the academic and industrial supervisors. However, each project 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. Projects will be marked in two ways. Firstly, according to the following scheme: • Project justification including its relationship to the current state of the art 10% 20 marks • Ability to select and use appropriate methods and techniques 10% 20 marks • The clarity, coherence and succinctness with which the solution is developed 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 100% 200 marks 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? **ASSESSMENT:** Project: 100%
Language	English

Course Title	Current Trends in Cybersecurity				
Course Code	CYS631				
Course Type	Optional				
Level	Master (2nd cycle)				
Year / Semester	1st or 2nd Year / 2nd or 3rd Semester				
Teacher's Name	Ioanna Danidou				
ECTS	8	Lectures / week	3 Hours	Laboratories / week	None
Course Purpose and Objectives	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.				
Learning Outcomes	Upon succesful 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 Intenet 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		
Prerequisites	None	Co-requisites	None
Course Content	Introduction: 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. Law and Policy: 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. Strategy: 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. Cybersecurity as a factor of growth and the Cybersecurity Ecosystem: 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. The Cyberecurity 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 important role to play in facilitating this goal, in		

	order to achieve a collaborative security in cyberspace Emerging technologies: 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. Safer Internet: 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. Professional Certifications: 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. 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.
Teaching Methodology	Face – to – face
Bibliography	National, European and international cybersecurity strategy, policy and legal documents IEEE Journals, Magazines and Websites (ISC)^2 Journals, Magazines and Websites ISACA Journals, Magazines and Websites Other professional certification information sources
Assessment	Examinations 60% Assignment(s) 40% 100%
Language	English

Course Title	Machine Learning for Cybersecurity				
Course Code	CYS632				
Course Type	Optional				
Level	Master (2nd cycle)				
Year / Semester	1st or 2nd Year / 2nd or 3rd Semester				
Teacher's Name	George Kalogridis				
ECTS	8	Lectures / week	3 Hours	Laboratories / week	None
Course Purpose and Objectives	The course deals with the combination of machine learning and computer security. Approaches for automatically detecting and analyzing security threats are discussed. Topics include anomaly detection, automatic signature generation, classification and clustering of malicious software.				
Learning Outcomes	Upon succesful completion of this course students should be able to: • assess the effectiveness of solutions presented and to question them in an intelligent way; • Understand and implement the most popular learning algorithms; • Perform feature selection and experimental set up on real tasks; • Evaluate multiple learning algorithms across several tasks.				
Prerequisites	None	Co-requisites	None		
Course Content	The massive increase in the rate of novel cyberattacks has made Machine-Learning (ML) techniques a critical component in detecting security threats. The course covers various applications of ML in computer and network security. Topics include: Overview of basic machine learning techniques: supervised and unsupervised learning followed by an overview of the state of information security; malware detection; network and host intrusion detection; web, email, and social network security; authentication and authorization anomaly detection; alert correlation; and potential issues such as privacy issues and adversarial machine learning.				

	• Introduction to Machine Learning: High level analysis of the different approaches to supervised and unsupervised learning. • Supervised Machine Learning: Linear Regression, Logistic Regression, Decision Trees, SVM Vectors. • Unsupervised Machine Learning: Clustering, the k-means algorithm • Density Estimation: Problem Motivation, Gausian Distribution, and the Algorithm • Building an anomaly detection system: Building and Evaluating, Anomaly detection vs Supervised learning. Choosing what features to use. • Introduction to Data Mining for Information Security • Malware Detection: Obfuscation, Polymorphism, Payloadbased detection of worms, Botnet detection/takedown • Network Intrusion Detection: Signature-based solutions (Snort, etc), Data-mining-based solutions (supervised and unsupervised), Deep packet inspection • Host Intrusion Detection: Analysis of shell command sequences, system call sequences, and audit trails, Masquerader/Impersonator/Insider threat detection • Web Security: Anomaly detection of web-based attacks using web server logs, Anomaly detection in web proxy logs • Email: Spam detection, Phishing detection • Social network security: Detecting compromised accounts, detecting social network spam • Authentication: Anomaly detection of Single SignOn (Kerberos, Active Directory), Detecting Pass-the-Hash and Pass-the-Ticket attacks • Automated correlation: Attack trees, Building attack scenarios from individual alerts • Machine learning exploited by both sides: Adversarial machine learning (use of machine learning by attackers, how to make ML algorithms robust/secure against adversaries). • Other potential topics: Fraud detection, IoT/Infrastructure security, Mobile/Wireless security
Teaching Methodology	Face – to – face
Bibliography	Applications of Data Mining in Computer Security, Daniel Barbara and Sushil Jajodia

	Machine Learning and Data Mining for Computer Security, Marcus A. Maloof Data Mining and Machine Learning in Cybersecurity by Sumeet Dua (Editor), Xian Du
Assessment	Examinations 60% Assignment(s) 40% 100%
Language	English

Course Title	Data Privacy in the era of Data Mining and AI				
Course Code	CYS633				
Course Type	Optional				
Level	Master (2nd cycle)				
Year / Semester	1st or 2nd Year / 2nd or 3rd Semester				
Teacher's Name	George Kalogridis				
ECTS	8	Lectures / week	3 Hours	Laboratories / week	None
Course Purpose and Objectives	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. 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.				

Learning Outcomes	Upon succesful completion of this course students should be able to: • Understand privacy-by-design principles. • Get an overview of EU legislative and business regulatory aspects of data handling. • Use cyber security protocols to engineer holistic data privacy system solutions. • Apply fundamental data mining and activity recognition algorithms to run privacy-invansive security tests. • Understand the principles of differential privacy and implement privacy-preserving algorithms. • Design privacy solutions for IoT scenarios, including Smart Grid, Smart Cities and wearable sensor technologies.		
Prerequisites	None	Co-requisites	None
Course Content	IoT scenarios and privacy concerns: Smart meter data collection, wearable and smartphone mobile sensing technologies, data handling and data linking potential risks and system-level analysis. Mathematical privacy metrics and privacy invasion tools: relative entropy, mutual information, cluster classification, regression analysis, residual features, activity recognition, non-intrusive appliance load monitoring, exploratory data mining, differential privacy and atypicality. Cyber-security privacy protection solutions: anonymisation with trusted third party, data aggregation, data splitting, secure multi-party communication protocols, homomorphic encryption, zero-proof cryptosystem, data obfuscation, physical behaviour optimisation. Information-theoretic privacy preserving techniques: privacy-utility trade-off optimisation, privacy-aware data sensing, lossy data compression, rate-distortion function, differentially private billing. Standardisation, regulatory and business aspects: consent-based approaches, ethical aspects of data collection, access control restrictions, business requirements and risks. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the practical privacy scenarios and IoT considerations.		
Teaching Methodology	Face – to – face		

Bibliography	*Larry L Peterson and Bruce S Davie, Computer Networks: A Systems Approach. Morgan Kaufman, 5th edition, 2011.* *Keith M Martin, Everyday Cryptography. Oxford University Press, 2012.* *Agrawal, Rakesh and Srikant, Ramakrishnan, Privacy-preserving Data Mining, SIGMOD Rec., vol. 29, no. 2, pp. 439-450, June 2000.* *Hall, Mark and Frank, Eibe and Holmes, Geoffrey and Pfahringer, Bernhard and Reutemann, Peter and Witten, Ian H., The WEKA Data Mining Software: An Update, SIGKDD Explor. Newsl., vol. 11, no. 1, pp. 10-18, June 2009.* *Sumeet Dua and Xian Du, Data Mining and Machine Learning in Cybersecurity. CRC press, May 2011.*
Assessment	Examinations 60% Assignment(s) 40% 100%
Language	English

Course Title	Ethical Hacking and Penetration Testing				
Course Code	CYS634				
Course Type	Optional				
Level	Master (2nd cycle)				
Year / Semester	1st or 2nd Year / 2nd or 3rd Semester				
Teacher's Name	Ghanan Glezer				
ECTS	8	Lectures / week	3 Hours	Laboratories / week	None
Course Purpose and Objectives	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.				
Learning Outcomes	Upon succesful completion of this course students should be able to: • Define and describe common hacking terminology • Define the different types of hacking and its legal and illegal uses in the cybersecurity world • Identify and evaluate the different type of hacking attacks and how these attacks proceed • Explain the principles of vulnerability research • Describe the ways available to conduct ethical hacking • Describe the different phases of ethical hacking and select appropriate techniques depending on the assignment. • Define and describe the different kinds of penetration testing – black box, grey box, white box.				
Prerequisites	None	Co-requisites	None		
Course Content	Introduction: 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.				

	Hacking phases: The five phases of hacking – reconnaissance, scanning, gaining access, maintaining access, covering tracks. Reconaissance: Discovery of target information, footprinting, competitive intelligence, social engineering, Google hacking, website footprinting, email tracking Scanning: 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 Gaining and maintaining access: 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. Covering tracks: Rootkits, disabling auditing, clearing logs, anonymisers, proxies, hiding files, track covering tools Practical penetration testing: Penetration testing methodology, ethical considerations, assignments and contracts, reporting, relationship to audits and audit techniques. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the practicalities and challenges of penetration testing.
Teaching Methodology	Face – to – face
Bibliography	*“Gray Hat Hacking: The Ethical Hacker's Handbook, Fourth Edition”*, by Daniel Regalado and Shon Harris *“The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy”*, by Patrick Engebretson *“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
Assessment	Examinations 60% Assignment(s) 40% 100%
Language	English

Course Title	Incident Response and Forensic Analysis				
Course Code	CYS635				
Course Type	Optional				
Level	Master (2nd cycle)				
Year / Semester	1st or 2nd Year / 2nd or 3rd Semester				
Teacher’s Name	Ghanan Glezer				
ECTS	8	Lectures / week	3 Hours	Laboratories / week	None
Course Purpose and Objectives	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 this 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.				
Learning Outcomes	Upon succesful 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.		
Prerequisites	None	Co-requisites	None
Course Content	Introduction: 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. Preparation: 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. Identification: Detection, incident triage, information gathering and reporting, incident classification, indicators of compromise (IOC). Containment: Damage limitation, network segment isolation, system isolation, forensic backup and imaging, use of write blockers, temporary fixes, malware spread limitation. Eradication: 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. Recovery: 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. Follow-up: Documenting lessons learned, preparatory activities for similar future incidents, technical training, process improvement. Digital Forensics Investigation Process: Applicable laws, investigation methodology, chain of custody, evidence collection, digital evidence principles, rules and examination process, first responder procedures.		

	Technical forensics tools and techniques: Hard disks, removable media and file systems, Windows forensics, duplication/imaging of 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.) 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.
Teaching Methodology	Face – to – face
Bibliography	*“Incident Response & Computer Forensics, Third Edition”* by Jason T. Luttgens and Matthew Pepe *“Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder”*, by Don Murdoch *“Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response”*, by Leighton Johnson *“The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics”*, by John Sammons *“Digital Forensics with Open Source Tools”*, by Cory Altheide and Harlan Carvey *“Digital Forensics Processing and Procedures”*, by David Lilburn Watson and Andrew Jones IEEE Journals and Magazines
Assessment	Examinations 60% Assignment(s) 40% 100%
Language	English

European
University Cyprus
LAUREATE INTERNATIONAL UNIVERSITIES

Παράρτημα 2

Proposed software / hardware

Introduction

This list of software / hardware has been composed for use within the new MSc in Cybersecurity programme. The choices made were guided with cost in mind, and also with the philosophy of using mostly open source / free tools, which is what most black and white hat hackers use. Additionally, there are many such free tools available that can cover most if not all aspects of cybersecurity. Where specific commercial tools are well known and used, they will also be recommended below. It is recommended that, given that this will be a new course, the tools used are relatively simple and few in number – the list below is provided with the idea of using a single or at most two software tools within a single course for the lab component. As this course is offered to students multiple times, the professors that are teaching each module will be able to recommend further tools and/or infrastructure as new needs become evident, and as teaching maturity in this area increases.

Please note that the following list is a set of recommendations and does not comprise the only tools that are available for the required purpose – there are literally thousands of tools available (see http://sectools.org/ for one out of many lists). The final tools to be used during the cybersecurity course should be ones that the teaching staff will be able to confidently use with their students. Finally, it should be mentioned that some of the courses may not require the use of specific software tools (e.g. Cybersecurity Policy, Governance, Law and Compliance), and that some of the software could be used for many of the courses, even if not mentioned below. The teaching staff will need to make the final decisions.

Also, within the time constraints of individual MSc courses, the depth to which each type of software tool can be explored will necessarily be limited. It is recommended that MSc dissertation projects are designed in such a way so as to require the use of in depth technical work (one or more tools) within a relevant area of specialisation.

Hardware

For security reasons (i.e. to avoid any potential incidents on the main university infrastructure), it is recommended that all of these tools run on a completely separate and isolated network – a couple of powerful servers should be enough for dozens of

VMs (virtual machines) to be run, where students can practice network offence and defence, and use a number of cybersecurity tools in a safe environment. Students should be cautioned about the use of such tools on their personal computing equipment (and applicable legislation will be covered during the course). Additionally, this infrastructure could be made available through the Internet, and thus the relevant students will be able to access the tools with maximum flexibility in terms of location and time. This option should be discussed with relevant IT staff at the university in order to come up with a detailed budget for this separate infrastructure, if it is agreed that this is the best way forward. The estimated cost for this is expected to be in the region of €50,000 - €100,000 (assuming that existing computing labs will be used for accessing this infrastructure and thus no extra equipment will be needed).

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/

Courses it can be used for

Communications and Network Security, Ethical Hacking and Penetration Testing

Price

Free

Dependencies

None – it can be installed on single machines.

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/

Courses it can be used for

Communications and Network Security, Ethical Hacking and Penetration Testing

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).

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.

Nessus

Brief description

Nessus is a widely-deployed vulnerability, configuration, and compliance scanner. Nessus features high-speed discovery, configuration auditing, asset profiling, malware detection, sensitive data discovery, and vulnerability analysis. With the world's largest continuously-updated library of vulnerability and configuration checks, and the support of Tenable's expert vulnerability research team, Nessus sets the standard for speed and accuracy.

Website

https://www.tenable.com/products/nessus/nessus-professional/evaluate

Courses it can be used for

Cybersecurity Architecture and Operations

Price
Free trial, $2200 for a single-user license. The university should contact the company and ascertain whether academic licenses are available. Alternatively, the IT staff should investigate how the VMs on the dedicated infrastructure could be set up so that students could use the free trial edition (7 days) for single labs.

Dependencies
None – it can be installed on a single machine but may operate better in a client-server environment.

Metasploit Community (free) + Metasploitable

Brief description
Metasploit is a tool for developing and executing exploit code against a remote target machine. It offers a semi-automated way of exploiting remote machines that can be configured and run in a controlled environment and is ideally suited for teaching. Intentionally vulnerable images can be used for this purpose (such as Metasploitable - https://sourceforge.net/projects/metasploitable/).

Website
https://www.rapid7.com/products/metasploit/

Courses it can be used for
Communications and Network Security, Ethical Hacking and Penetration Testing

Price
Free (Community Edition)

Dependencies
None – it can be installed on single machines.

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/

Courses it can be used for
Cybersecurity Architecture and Operations, Communications and Network Security

Price
Free

Dependencies
None – it can be installed on single machines.

JCrypTool

Brief description
JCrypTool enables students, teachers, developers, and anyone else interested in cryptography to apply and analyze cryptographic algorithms in a modern, easy-to-use application. The JCT plaform creates a new way of e-learning by not just encouraging users to learn about cryptography and apply the algorithms themselves, but also to develop their own cryptographic plug-ins and extend the JCrypTool platform in new directions.

Website
https://www.cryptool.org/en/jcryptool

Courses it can be used for
Cryptography

Price
Free

Dependencies
None – it can be installed on single machines and doesn't need administrator access to install.

Excel (or LibreOffice)

Brief description
Microsoft Excel is a well known spreadsheet program from Microsoft that is used in most Windows-based computing environments. While not specifically a cybersecurity-related software tool, it is well suited to the organisation and documentation of risk information. The university probably already has Excel (or a free alternative such as LibreOffice) installed on its computers. Note that there are other specialised software

tools available for risk management, but they are not necessary for the purposes of this course.

Website
https://products.office.com/en-us/excel

Courses it can be used for
Risk Analysis and Management

Price
Depends on the type of license. LibreOffice is free.

Dependencies
None – it can be installed on single machines.

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 amount 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/

Courses it can be used for
Communications and Network Security, Ethical Hacking and Penetration Testing, Incident Response and Digital Forensics, Cryptography (for steganography)

Price
Free

Dependencies
Needs to be installed on a physical computer or a VM – it is a standalone OS.

R Project

Brief description
R is a free software environment for statistical computing and graphics. It compiles and runs on a wide variety of UNIX platforms, Windows and MacOS. It includes functionality for machine learning applications (https://cran.r-project.org/web/views/MachineLearning.html).

Website
https://www.r-project.org/

Courses it can be used for
Machine Learning for Cybersecurity, Data Privacy in the era of Data Mining and AI

Price
Free

Dependencies
None – it can be installed on single machines.

MATLAB (with Statistics and Machine Learning Toolbox)

Brief description
MATLAB is a very well known and widely used software tool that is used for many different kinds of mathematics, engineering and computing research. It includes a Statistics and Machine Learning Toolbox, which includes relevant machine learning functionality (http://www.mathworks.com/products/statistics/).

Website
http://www.mathworks.com/products/matlab/

Courses it can be used for
Machine Learning for Cybersecurity, Data Privacy in the era of Data Mining and AI

Price

For educational use, MATLAB and the Statistics Toolbox are priced at $629 and $250 respectively. The equivalent student editions, that the students can use at home for their work (machine learning of this kind involves significant data analysis and cannot be used to instigate cyber attacks), are priced at a total of just $55.

Dependencies

None – it can be installed on single machines.