Course Title	Network and System Security				
Course Code	ACOE422				
Course Type	Elective				
Level	BSc (Level 1)				
Year / Semester	3rd / 4th (Fall/Spring)				
Teacher's Name	Chrysostomos Chrysostomou				
ECTS	6	Lectures / week	3	Laboratories/week	0
Course Purpose	The purpose of the course is to provide students with the knowledge of the concepts and principles underlying the field of network and system security, and to enable students develop the skills required for examining and analysing network and system security challenges.				
Learning Outcomes	By the end of the course, the students are expected to: 1. outline the underlying principles of system and network security; 2. assess procedures to implement data confidentiality, integrity, availability and security controls; 3. define and illustrate security policies as countermeasures to threats and attacks; 4. recognize, describe and assess the concepts and issues involved in networks security applications; 5. examine and illustrate the cryptographic algorithms and protocols underlying networks security applications; 6. explain the operation of various security models and their application scenarios within an organization; 7. identify system-level security issues, and illustrate the principles of intrusion detection/prevention and firewalls, and describe their characteristics; 8. perform simulation and modeling activities to explore, acquire, reinforce, and expand practical skills.				
Prerequisites	ACOE323, ACSC271	Co-requisites	None		
Course Content	• **Introduction to Security:** Computer security objectives – Confidentiality, Integrity, Availability. Additional concepts – Authenticity, Accountability. Breach of security levels of impact. Examples of security requirements. Computer security challenges. OSI security architecture. Threats and attacks – passive and active. Security services – Authentication, Access control, Data confidentiality, Data integrity, Nonrepudiation. Availability service. Security mechanisms. Model for network security. Standards. Malicious software (Types of malware - Infected content, Vulnerability exploit, Social engineering, Attack agent, Information theft, Stealthing, Countermeasures). • **Cryptography:** Symmetric Encryption and Message Confidentiality				

	(Symmetric encryption principles and algorithms, Cipher block modes of operation, Key distribution). Public-Key Cryptography and Message Authentication (Approaches to message authentication, Secure hash functions and HMAC, Public-key cryptography principles and algorithms, Digital signatures, Certificates, Key management). • **Networks Security Applications:** Authentication Applications (Kerberos, X.509 directory authentication service, Public Key Infrastructure). Web Security (Secure Sockets Layer (SSL), Transport Layer Security (TLS), HTTP over SSL (HTTPS), Secure Shell (SSH)). Electronic Mail Security (PGP, S/MIME). IP Security (IPsec architecture, Authentication header protocol, Encapsulating security payload protocol, Combining security associations, Key management). • **System Security:** High Availability System (Elimination or reduction of single-points of failure, System Resiliency, Fault Tolerance, Asset Management – Risk Analysis, Defence in Depth). Intruders (Intrusion Prevention, Intrusion Detection, Intrusion Response, Password Management). Distributed Denial of Service Attacks. Sniffing. Spoofing. Man-in-the-middle. Access Control Mechanisms. Firewalls (Firewall design principles, Packet filtering firewall, Stateful inspection firewall, Application Level Gateway, Circuit-level Gateway). Operating Systems Security (UNIX Security, Windows Security).
Teaching Methodology	Students are taught the course through lectures by means of computer presentations. Lectures are supplemented with assignments aiming to help students develop practical skills by illustrating the main concepts taught at lectures. The familiarization of computer network simulators and/or packet analysis software has been gained through the ACOE313 course. Lecture/Coursework notes and presentations are available for students to use in combination with the textbooks and references, through the university's e-learning platform.
Bibliography	Textbooks: • W. Stallings, ***Network Security Essentials: Applications and Standards***, Pearson, 6th Ed., 2017 References: • Charles P. Pfleeger, Shari Lawrence Pfleeger, and Jonathan Margulies, ***Security in Computing***, Prentice Hall, 5th Ed., 2015 • Matt Bishop, ***Introduction to Computer Security***, Addison-Wesley Professional, 1st Ed., 2005 • Cisco ***Cybersecurity Essentials*** course, Cisco Networking Academy
Assessment	The assessment of the course includes one written test, multiple-choice quizzes and a final written exam with practical and theoretical questions. Assignments consist of simulation and modeling exercises using networking simulation tool and/or packet analysis software requiring students to illustrate the main concepts taught at lectures. The weights for each assessment component are: • Assignments: 15% • Quizzes: 10%

	• Test: 15% • Final Exam: 60%
Language	English