UNIVERSITY of NICOSIA

Course Syllabus

Course Code	Course Title	ECTS Credits
COMP-431	Computer Security	6
Prerequisites	**Department**	**Semester**
COMP-354	Computer Science	Spring
Type of Course	**Field**	**Language of Instruction**
Required	Computer Science	English
Level of Course	**Lecturer(s)**	**Year of Study**
1st Cycle	Dr Ioanna Dionysiou	4th
Mode of Delivery	**Work Placement**	**Corequisites**
Face-to-face	N/A	None

Course Objectives:

The main objectives of the course are to:

- appreciate the need for computer security and protection
- provide student deep knowledge on computer security technology and principles, including cryptographic tools, user authentication, access control, and formal models for multilevel computer security
- expose students to techniques to manage security of computers and users by means of contemporary host-based intrusion detection/prevention tools, physical security measures, auditing, logging
- explain various operating systems security models, policies.

Learning Outcomes:

After completion of the course students are expected to be able to:

1. discuss and use basic cryptographic techniques
2. critically assess user authentication mechanisms, including choosing strong passwords
3. discuss and utilize access control techniques that could be employed in various operating systems and their impact on users
4. identify vulnerabilities in simple programs and rewrite them to make programs safe
5. identity various types of malicious software and use countermeasure defense/detection tools
6. determine and assess protection policies and mechanisms to secure a personal desktop.

Course Content:

1. Overview of computer security concepts and the scope of computer security
2. Brief introduction to cryptographic tools covering basic security services
3. User authentication (password-based, token-based, biometric) and related security issues
4. Access control principles (DAC, MAC, RBAC), formal multilevel models (Bell-LaPadula, Biba, Chinese Wall) and trusted systems
5. Malicious software including viruses, worms, overflow attacks (stack, buffer) and defences against these attacks
6. Secure programming for handling program input/output and writing safe/robust program code
7. Host-based intrusion systems (e.g. snort, and other open source tools), personal firewalls, anti-virus software, security auditing
8. Physical security threats and recovery from such security breaches
9. Operating systems security

Learning Activities and Teaching Methods:

Lecture, Individual Work, Hands-on Experience with Tools, and Case Studies

Assessment Methods:

Final Exam, Midterm Exam, Assignments, and Project

Required Textbooks / Readings:

Title	Author(s)	Publisher	Year	ISBN
Computer Security: Principles and practice, 3rd Edition	W. Stallings, L. Brown	Prentice Hall	2015	978-0133773927

Recommended Textbooks / Readings:

Title	Author(s)	Publisher	Year	ISBN
Cryptography and Secure Communication	Richard E. Blahut	Cambridge University Press	2014	978-1107014275