University of Nicosia, Cyprus

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

Objectives of the Course:

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 Contents:

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:

Lectures, case studies, hands-on experience with tools, on-site visits to IT departments of Cypriot enterprises, guest lectures by Cypriot IT specialists

Assessment Methods:

Written and programming assignments, team project, midterm exam, final exam

Required Textbooks/Reading:

Authors	Title	Publisher	Year	ISBN
W. Stallings, L. Brown	*Computer Security: Principles and practice*	Pearson Prentice Hall	2008	0136004245

Recommended Textbooks/Reading:

Authors	Title	Publisher	Year	ISBN
M. Bishop	*Computer Security: Art and Science*	Addison-Wesley	2002	0201440997
E. Skoudis, T. Liston	*Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses, 2nd Edition*	Prentice Hall	2006	0131481045
Scambray, McClure, Kurtz	*Hacking Exposed, 5th edition*	McGraw-Hill	2005	0072260815