UNIVERSITY of NICOSIA

Course Syllabus

Course Code	**Course Title**	**ECTS Credits**
COMP-514DL	Cryptography and Network Security	10
Prerequisites	**Department**	**Semester**
None	Computer Science	Spring
Type of Course	**Field**	**Language of Instruction**
Required	Computer Science	English
Level of Course	**Lecturer(s)**	**Year of Study**
2nd Cycle	Dr Ioanna Dionysiou	1st Year
Mode of Delivery	**Work Placement**	**Corequisites**
Distance Learning	N/A	N/A

Course Objectives:

The main objectives of the course are to:

- appreciate the need for network security practices and information protection.
- provide students with deep knowledge on principles and practice of cryptography.
- provide students with deep knowledge on principles and practice of classical computer and network security paradigms.
- expose students to techniques to manage security threats by means of contemporary host-based and network-based intrusion detection/prevention tools, physical security measures, auditing, logging.
- build foundations to assess contemporary security policies and security mechanisms within organizations and illustrate the balance of the managerial and technical aspects of network security.

Learning Outcomes:

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

1. explain the principles of cryptography.
2. discuss the practical use of cryptography in symmetric/asymmetric encryption, hash functions, MAC, and digital signatures.
3. discuss key management schemes for master, public, and session keys.
4. discuss and explain network authentication protocols (Kerbeors, PKI), Web security paradigms (TLS, SSL, SSH), and IP Security.
5. identify network attacks (denial of service, flooding, sniffing and traffic redirection, inside

attacks, etc.) and basic network defense tools

6. identify various types of malicious software and use countermeasure defense/detection tools
7. appreciate the importance of ethics as a network security practitioner
8. use existing technologies and libraries to achieve security goals

Course Content:

1. Cryptography Principles
   a. Basic Security Services
   b. Classical Encryption Techniques
   c. Symmetric Encryption and Block Ciphers (DES, AES)
   d. Public-Key Cryptography (RSA)
   e. Key Exchange Protocols (Diffie-Hellman Key Exchange)
   f. Cryptographic Hash Functions and Message Authentication Codes
   g. Digital Signatures
   h. Key Management and Distribution
2. Network Security
   a. User authentication (password-based, token-based, biometric) techniques and authentication protocols (Kerberos, PKI)
   b. Network security applications such as IP Security and Web Security
   c. Computer and network threats and attacks: viruses, worms, denial of service attacks, flooding, sniffing and traffic redirection, exploit attacks, infrastructure attacks (DNS hijacking, route blackholing, etc.)
   d. Contemporary network defense countermeasures: as host-based and network-based intrusion systems (e.g. snort, and other open source tools), firewalls, anti-virus software
3. Security Deployment
   a. Information security (technical aspects, informal aspects, and regulatory aspects) from the business perspective
   b. Information systems security framework within enterprises
   c. Information security policy regulations, standards and compliance: sector-specific policies for sectors such as financial, healthcare, critical infrastructures, small businesses
   d. Planning and implementing security policies for an organization

4. Legal, ethical, and professional aspects of security practices

Learning Activities and Teaching Methods:

Lecture, individual work, hands-on experience with tools, case studies

Assessment Methods:

Lab Exercises, Semester Project, Final Exam

Required Textbooks / Readings:

Title	Author(s)	Publisher	Year	ISBN
Cryptography and Network Security: Principles and Practice, Seventh Edition	W. Stallings	Pearson	2016	0134444280
Computer Security: Principles and Practice, Third Edition	W. Stallings, L. Brown	Pearson	2014	0133773922

Recommended Textbooks / Readings:

Title	Author(s)	Publisher	Year	ISBN
Security Engineering: A Guide to Building Dependable Distributed Systems, Second Edition	R. Anderson	John Willey and Sons	2008	0470068523

Software Security Engineering: A Guide for Project Managers	Julia H. Allen, Sean Barnum, Robert J. Ellison ,Gary McGraw, Nancy R. Mead	Addison-Wesley Professional	2008	032150917X
Cryptography and Secure Communication	Richard E. Blahut	Cambridge University Press	2014	9781139013673
Distributed Systems Security: Issues, Processes and Solutions	Abhijit Belapurkar, Anirban Chakrabarti, Harigopal Ponnapalli, Niranjan Varadarajan, Srinivas Padmanabhuni, Srikanth Sundarrajan	John Wiley and Sons	2009	978-0-470-75177-0