COURSE OUTLINE

(1) GENERAL

SCHOOL	Engineering		
DEPARTMENT	Electrical and Computer Engineering		
LEVEL OF STUDY	Undergraduate		
COURSE UNIT CODE	9.018	**SEMESTER OF STUDY**	9th
COURSE TITLE	Networks and Telecommunications Security		

COURSEWORK BREAKDOWN	**TEACHING WEEKLY HOURS**	**ECTS Credits**
Theory (Lectures)	3	2
Tutorial/Project	1	0.5
Laboratory	1	1.5
TOTAL	**5**	**4**

COURSE UNIT TYPE	Specialization/skills development
PREREQUISITES	
LANGUAGE OF INSTRUCTION/EXAMS	Greek
COURSE DELIVERED TO ERASMUS STUDENTS	No
WEB PAGE (URL)	https://eclass.hmu.gr/courses/ECE189/

(2) LEARNING OUTCOMES

Learning Outcomes

The course focuses on Computer Networks and Telecommunication Systems Security, as well as on privacy protection technologies. The approach is based on the OSI network architecture and specifically the security architecture in the Internet model. In addition, cybersecurity and mobile communications security issues are addressed. The course seeks to cultivate to students the culture of security in the networking environments, presenting the various categories of threats, vulnerabilities, countermeasures, and security methods. In addition, it cultivates familiarity with relevant terminology and key privacy technologies.

Upon successful completion of the course the student will be able to:

1. Explain the role and importance of telecommunications and networks security
2. Implement symmetric cryptographic algorithms and public key algorithms
3. Analyze and evaluate the security of telecommunications and networks systems
4. Design and implement secure network systems and applications
5. Evaluate the advantages and disadvantages of alternative security architectures
6. Design and implement blockchain applications.

General Skills

- Search, analysis and synthesis of data and information, using the necessary technologies
- Adaptation to new situations
- Autonomous work
- Teamwork
- Work in an interdisciplinary environment
- Production of new research ideas

(3) SYLLABUS

Theoretical Lecture Units

- Introductory topics of Computer Networks' Security: Threat Categories, Vulnerability Points, Countermeasures
- Network Layer Security, Transport Layer Security, Application Layer Security.
- Firewalls: capabilities and Limitations, Design Issues, firewall Architectures, Network / Application layer firewalls, Hybrid Security firewalls.
- Intrusion Detection and prevention Systems, Deep packet inspection.
- Security in the environment of wireless and mobile communication networks (2/3/4/5 G, IEEE 802.11 and 802.16).
- Risks and uncertainties from the use of cloud computing.
- Privacy protection technologies, anonymity and pseudonymization.
- Security of sensor networks and embedded systems.
- Malware protection.
- Symmetric cryptography and public key cryptography.
- Digital signatures and certificates.
- Security through blockchain architectures.

Laboratory Exercises

In the laboratory part of the course students have the opportunity to practice the concepts of theory using exercises that cover a wide range of material, and gain experience in using security mechanisms in networked computer systems environments, using corresponding tools and software libraries.

(4) TEACHING METHODS - ASSESSMENT

<table>
<tr><td><b>MODE OF DELIVERY</b></td><td>In-Class Face-to-Face</td></tr>
<tr><td><b>USE OF INFORMATION AND COMMUNICATION TECHNOLOGY</b></td><td>• Use of ICTs in lecturing
• Use of ICTs in laboratory-based training
• Use of ICTs for the communication with students via the e-class platform</td></tr>
<tr><td><b>TEACHING ORGANISATION</b></td><td>
<table>
<tr><th>Method description / Activity</th><th>Semester Workload</th></tr>
<tr><td>Lectures</td><td>52</td></tr>
<tr><td>Laboratory work</td><td>13</td></tr>
<tr><td>Non-guided personal study</td><td>17</td></tr>
<tr><td>Project-based assignments</td><td>25</td></tr>
<tr><td>Homework</td><td>13</td></tr>
<tr><td></td><td></td></tr>
<tr><td><b>Total Contact Hours</b></td><td><b>120</b></td></tr>
</table>
</td></tr>
<tr><td><b>ASSESSMENT METHODS</b></td><td><b>Language of Assessment</b>
Greek

<b>Student assessment methods</b>
1. Written final examination (40%)
• with exercises
• with multiple choice questions
2. teamwork assignment for the theoretical part of the course (with written report and oral assessment) (20%).
3. teamwork assignment for the laboratory part of the course (with written report and oral assessment) (30%).
4. Homeworks (10%).

The course evaluation criteria are announced to the students at the beginning of the semester and are posted on the course website in eClass.</td></tr>
</table>

(5) RECOMMENDED BIBLIOGRAPHY

- Recommended Bibliography:

1. *Α. Πομπόρτσης & Γ.Παπαδημητρίου,"Ασφάλεια Δικτύων Υπολογιστών." Τζιόλας, 2002.*
2. *Βασικές Αρχές Ασφάλειας Δικτύων: Εφαρμογές και Πρότυπα, William Stallings, έκδοση 3η, 2008 (μετάφραση).*
3. *Ασφάλεια υπολογιστών: Αρχές και πρακτικές, William Stallings, Lawrie Brown, 3η έκδοση, 2016 (μετάφραση).*
4. *Σ. Γκρίτζαλης, Σ. Κάτσικας, Δ. Γκρίτζαλης, Ασφάλεια Δικτύων Υπολογιστών, Εκδόσεις Παπασωτηρίου, 2004.*
5. *W. Stallings, L. Brown, Ασφάλεια Υπολογιστών: Αρχές και Πρακτικές, Έκδοση 3η Αμερικανική, ISBN 978-960-461-668-8, Εκδόσεις Κλειδάριθμος, 2016.*
6. *Λαμπρινουδάκης, Κ., Μήτρου, Λ., Γκρίτζαλης, Σ., Κάτσικας, Σ., (Eds.), Προστασία της*

Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών: Τεχνικά και Νομικά Θέματα, Παπασωτηρίου, 2009.

7. *OWASP Testing Guide v4.*
8. *"Security Engineering" (2nd Edition), Ross Anderson, Wiley (2008), ISBN: 0470068523*
9. *"Principles of Computer Security, CompTIA Security+", Arthur Conklin and Gregory White, McGraw Hill (2012), ISBN: 9780071786164*
10. *"Hacking Exposed 7: Network Security Secrets & Solutions" (7th Edition), Stuart McClure, Joel Scambray, George Kurtz, McGraw-Hill Osborne (2012)*
11. *NIST Computer Security Resource Center, http://csrc.nist.gov/*
12. *"Cryptography Engineering: Design Principles and Practical Applications", Niels Ferguson, Bruce Schneier, Tadayoshi Kohno, Wiley (2010), ISBN: 9780470474242*

- Relevant Scientific Journals:

- *IEEE Communications Surveys and Tutorials*
- *IEEE Communications Magazine*
- *IEEE Journal on Selected Areas in Communications*
- *IEEE Network*
- *Elsevier Computer Networks*
- *IEEE Access*
- *Network Security - Journal – Elsevier*
- *International Journal of Network Security & Its Applications (IJNSA)*
- *Security and Communication Networks*