COURSE OUTLINE

(1) GENERAL

SCHOOL	Engineering		
DEPARTMENT	Electrical and Computer Engineering		
LEVEL OF STUDY	Undergraduate		
COURSE UNIT CODE	9.015	**SEMESTER**	9th
COURSE TITLE	Computer Systems Security		
COURSEWORK BREAKDOWN		**ΕΒΔΟΜΑΔΙΑΙΕΣ ΩΡΕΣ ΔΙΔΑΣΚΑΛΙΑΣ**	**ΠΙΣΤΩΤΙΚΕΣ ΜΟΝΑΔΕΣ**
Theory (Lectures)		3	2
Practice		1	1
Lab		1	1
TOTAL		**5**	**4**
COURSE UNIT TYPE	Specialized general knowledge/Skills development		
PREREQUISITES	Operating Systems (8.009)		
LANGUAGE OF INSTRUCTION/EXAMS	Greek		
COURSE DELIVERED TO ERASMUS STUDENTS	Yes		
WEB PAGE (URL)	https://eclass.hmu.gr/courses/ECE150		

(2) LEARNING OUTCOMES

Learning Outcomes

A) The **knowledge** which students acquire upon successful completion of the course relates to understanding the design of multilayer protection mechanisms for computing systems, with an emphasis on embedded systems security. Security primitives are examined in detail, including lightweight cryptographic software libraries and hardware security devices (programmable crypto engines, crypto ICs). In addition, security patterns/protocols for efficient access control, data privacy, anonymity, confidentiality, integrity, and availability are examined. Case studies range from device security (cryptos), to memory protection/isolation (ARM Trustzone), to operating system kernel and file system support, to application and system/network security, including high-level security event tracing, correlation, and visualization.

B) The **skills**, which students develop upon successful course completion, relate to:

- Understanding the design and use of public key and symmetric cryptography (lightweight
- Understanding the design and use of digital certificates and signatures
- Designing and implementing protocols and techniques for security and data privacy at device, system/network, and application level

C) The **abilities**, which students develop upon successful course completion, enable problem-solving abilities that relate to

- Integrating security/trust in system/platform design and implementation
- Implementing secure embedded systems using lightweight security primitives/protocols
- Validating security functions and evaluating overheads of at device-, system-, and network-level

General Skills

- Search, analysis and synthesis of data and information, using the necessary technologies
- Adapt solutions to new situations (resource sharing, congestion, contention etc)
- Autonomous work

- Teamwork
- Decision making
- Work in an interdisciplinary environment
- Promoting liberal, creative and inductive/deductive thinking

(3) SYLLABUS

Theoretical Lectures

- History – Classical Cryptography- Mathematical Preliminaries
- System Security, Data Privacy, Anonymity, Legal Framework, GDPR, HIPAA etc
- SW Vulnerabilities, Viruses, Side Channel Attacks & Energy Profiling
- Network Security, Worms, DDoS, Firewall, IPSec, OpenSSL/TLS, OpenVPN, syslog/IDPS
- Symmetric Cryptography, NIST-approved Operating Modes
- Public Key Cryptography (RSA, Diffie Hellmann) & Elliptic Cryptography
- Security Primitives, Protocols, and Services
- Digital Certificates & Signatures
- Message Authenticity - Merkle Trees
- Application Security – Web/Ηλεκτρονικό Ταχυδρομείο (HTTPS, SMTP)
- Embedded Security, Cybersecurity & Safety, e.g. Smart Vehicles, e-Health platforms
- Programmable Crypto Engines – Crypto ICs – Software Libraries
- Domain Isolation, ARM Trustzone, Applications (Secure Boot, File Systems, etc)
- Cloud/IoT Security (Auth protocol vs Kerberos)
- Special Topics (e.g. Blockchains, Steganography, Secret Sharing, Zero-Knowledge Proofs, Oblivious Transfers, Commit Protocols, Homomorphic Security, Quantum Cryptography)

Lab

The student lab focuses on open source hardware/software and Linux system security. Students gain experience in cryptographic mechanisms (AES encryption/decryption, integrity), authentication (SHA3, one-way hash functions), domain isolation, data privacy and anonymity by applying well-established security patterns for device, system/network, and application security. The lab also examines practical use of software tools, cryptographic security libraries, programmable crypto engines, and crypto ICs in experimental platforms and real embedded systems, such as healthcare and automotive.

(4) TEACHING METHODS - ASSESSMENT

MODE OF DELIVERY	In-Class Face-to-Face
USE OF INFORMATION AND COMMUNICATION TECHNOLOGY	▪ Use of ICTs in lecturing and lab ▪ Use of ICTs for the communication with students via the e-class platform
TEACHING ORGANIZATION	

Method description/Activity	Semester Workload
Lectures	39
Demos/Labs	26
Individual Study & Programming (on Server or Laptop/PC using VM or Dual Boot)	55
Total Contact Hours	**120**

ASSESSMENT METHODS	Language for Evaluation: Greek/English (Erasmus) All announcements related to the syllabus, including grading, and complementary reading material are permanently posted in the course web page (ECLASS). The course grade incorporates the following evaluation procedures: 1. Final exam on theoretical/practical problems (50%) 2. Programming exercises (50%) Students with extensive programming experience can opt to replace the Final Exam with a dedicated programming project. This project usually relates to systems/network programming, Linux drivers & kernel modules, RTOS, real-time systems or small software stacks. Students provide a presentation and demonstration at the end of their project.

(5) RECOMMENDED BIBLIOGRAPHY

Recommended Bibliography:

- *P. C. Pfleeger, S. L. Pfleeger, J. Margulies, "Security in Computing", 5th edition, 2018. Prentice Hall, 2018.*
- *D. Basin, P. Schaller, M. Schlaepfer, "A Hands-on Approach", Springer, 2011.*

Other Important Sources

- *Eclass - http://eclass.hmu.gr (notes, examples, open source coce)*
- *Development boards, pirate devices, virtual machines accompanied with open source software and manuals for examining attack and devising protection mechanisms*

Relevant Scientific Journals & Conferences

- *ACM Transactions on Privacy and Security*
- *IEEE Transactions on Dependable and Secure Computing*
- *IEEE Security & Privacy*
- *IEEE Transactions on Information Forensics & Security*
- *IEEE Transactions on Intelligent Transportation Systems*
- *IEEE Transactions on Vehicular Technology*
- *USENIX Security Symposium*
- *IEEE Symposium on Security and Privacy*
- *DEFCON and BLACKHAT conferences*
- *Embedded Security-related conferences, e.g. Embedded Security in Cars (ESCAR), Linux Security Summit, Automotive Linux Summit, Automotive Manufacturing Summit, Automotive World*