HARDWARE SECURITY

1. GENERAL

SCHOOL	ENGINEERING		
DEPARTMENT	DEPARTMENT OF INFORMATICS AND COMPUTER ENGINEERING		
LEVEL OF EDUCATION	GRADUATE		
COURSE CODE	CSCYB-201	**SEMESTER OF STUDIES**	**B'**
COURSE TITLE	**HARDWARE SECURITY**		

INDEPENDENT TEACHING ACTIVITIES *in case the credits are awarded in separate parts of the course e.g. Lectures, Laboratory Exercises, etc. If the credits are awarded uniformly for the whole course, indicate the weekly teaching hours and the total number of credits.*	**WEEKLY HOURS OF TEACHING**	**ECTS CREDITS**
Lectures	3	
Practice -Exercises		
Add rows if needed. The teaching organization and teaching methods used are described in detail in 4.	**3**	**8**

COURSE TYPE *Background, General Knowledge, Scientific Area, Skills Development*	*Compulsory, Specialized general knowledge*
ERASMUS STUDENTS	Yes (English)
ONLINE COURSE (URL)	Cscyb.uniwa.gr and eclass (UNIWA Open eClass | Επιλογή μαθημάτων)

2.LEARNING OUTCOMES

Learning outcomes

The learning outcomes of the course are described, the specific knowledge, skills and abilities of an appropriate level that students will acquire after the successful completion of the course.

Refer to Appendix A.

- *Description of the Level of Learning Outcomes for each course according to the Qualifications Framework of the European Higher Education Area*
- *Descriptive Indicators Levels 6, 7 & 8 of the European Qualifications Framework for Lifelong Learning and Annex B*
- *Summary Guide for writing Learning Outcomes*

The aim of this course is to provide post-graduate students with the appropriate knowledge and skills about major topics in hardware security, including hardware security vulnerabilities, attacks, and appropriate protection mechanisms. Upon successful completion of the course the student will be able to:

- Formulate hardware security requirements for a system.
- Describe the types of errors, faults and hazards in a system and how to deal with them, and select appropriate methods to deal with them.
- Describe and apply hardware security analysis methods.
- Describe and apply hardware security assessment methods.
- Design digital circuits for cryptographic applications.
- Design circuits that will contain built-in test structures for easy controllability.
- Check circuits for defects or harmful additional hardware components.

General Abilities

Taking into account the general skills that the graduate must have acquired (as they are listed in the Diploma Supplement and are listed below), which of them is intended for the course ?.

Search, analysis and synthesis of data and information, using the necessary technologies	*Project design and management*
Adaptation to new situations	*Respect for diversity and multiculturalism*
Decision making	*Respect for the natural environment*
Autonomous work	*Demonstration of social, professional and moral responsibility and sensitivity in gender issues*
Teamwork	*Exercise criticism and self-criticism*
Working in an international environment	*Promoting free, creative and inductive thinking*
Work in an interdisciplinary environment	

Production of new research ideas
The course aims to the following general competences: • Search for, analysis and synthesis of data and information, with the use of the necessary technology • Working independently • Team work • Working in an international environment • Decision making

3.COURSE CONTENT

The description contains the material to be covered during 13 lectures.
Lectures 1-2: Introduction and basic concepts, evolution of hardware security, overview and layers of a computing system, types of electronic hardware, hardware security vs. hardware trust, security and test/debug, electronic supply chain.
Lectures 3-4: Introduction to data encryption and security, data encryption standards (DES, AES) and block ciphers, public key cryptography and RSA asymmetric key algorithm.
Lecture 5: Basics of VLSI Design and Test
Lecture 6: Physical attacks
Lectures 7: Hardware Intellectual Property (IP) piracy and reverse engineering
Lecture 8: Side-Channel Attacks
Lecture 9: Hardware Trojans
Lecture 10: Attacks on PCB, RFID and JTAG
Lecture 11-12: Hardware security primitives, physically unclonable functions (PUFs) and true random number generators (TRNGs)

Lecture 13: Hardware metering and digital watermarking

4.TEACHING AND LEARNING METHODS - EVALUATION

METHOD OF DELIVERY *Face to face, Distance education etc.*	This module is taught through a combination of lectures, exercises, computer laboratory sessions, and coursework exercises.
USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES *Use of ICT in Teaching, in Laboratory Education, in Communication with students*	• Use of ICT in Course Teaching • Use of the Open eClass system, with uploaded notes, lectures, exercises for practice and communication with students.
TEACHING ORGANIZATION *The way and methods of teaching are described in detail. Lectures, Seminars, Laboratory Exercise, Field Exercise, Bibliography study & analysis, Tutoring, Internship (Placement), Clinical Exercise, Art Workshop, Interactive teaching , Study visits, Study work, artwork, creation. λπ. The student study hours for each learning activity are indicated as well as the non-guided study hours so that the total workload at the semester level corresponds to the ECTS standards .*	Projection system and presentation capability with the application of the Power Point program, - Internet connection, - Use of bibliography search engines HEAL-LINK, PUBMED, SCOPUS, GOOGLE SCHOLAR - Use of e-mail and the Department's website to communicate with students and keep them informed - Use of the course eclass

STUDENT EVALUATION *Description of the evaluation process* *Assessment Language, Assessment Methods, Formative or Concluding, Multiple Choice Test, Short Answer Questions, Essay Development Questions, Problem Solving, Written Assignment, Report / Report, Oral Examination, Public Presentation, Public Presentation, Others* *Explicitly defined assessment criteria are stated and if and where they are accessible to students.*	I. Project 1 (50%) and II. Project 2 (50%)

4. **RECOMMENDED-BIBLIOGRAPHY**

Essential

- S. Bhuniaand, M. Tehranipoor, Hardware Security: A Hands-on Learning Approach, Morgan Kaufmann–Elsevier, 1st edition, 2018.

Recommended

- Introduction to Hardware Security and Trust, First Edition, Mohammad Tehranipoor and Cliff Wang (Ed.) (2012), Springer, ISBN-13: 978-1-4419-8079-3 or ISBN-10: 1-4419-8079-2 or e-ISBN: 978-1-4419-8080-9.
- Towards Hardware-Intrinsic Security, First Edition, Ahmad-Reza Sadeghi and David Naccache (Eds.) (2010), Springer, ISBN-13: 978-3-642-14451-6 or ISBN-10: 3-642-14451-9 or e-ISBN: 978-3-642-14452-3.
- Fault-Tolerant Systems, First Edition, Israel Koren and C. Mani Krishna (2007), Elsevier Morgan Kaufmann Publishers, ISBN-13: 978-0-12-088525-1 or ISBN-10: 0-12-088525-5
- Fundamentals of Dependable Computing for Software Engineers, John Knight, CRC press, 2012.
- Fault-Tolerant Design, Elena Dubrova, Springer, 2013.
- Building Dependable Distributed Systems, Wenbing Zhao, Willey publications.
- Developing Green Software, Dr. Bob Steigerwald and Abhishek Agrawal, Intel Corporation.
- Dependability benchmarking for Computer Systems, Karama Kanoun and Lisa Spainhower (eds), Willey publications & IEEE Computer Society.
- Dependable Computing: Design and Assessment, Ravishankar K. Iyer, Zbigniew T. Kalbarczyk, Nithin M. Nakka, Wiley, 2016.
- Dependable computer systems, Assen V. Krumov, CreateSpace Independent Publishing Platform, 2013.
- Computer Architecture Techniques For Power-Efficiency, Stefanos Kaxiras and Margaret Martonosi, Morgan & Claypool, 2008.
- System-Level Design Techniques For Energy-Efficient Embedded Systems, Marcus T. Schmitz, Bashir M. Al-Hashimi and Petru Eles, Springer 2009.
- Power-efficient System Design, Preeti Ranjan Panda, B. V. N. Silpa, Aviral Shrivastava, Krishnaiah Gummidipudi, Springer 2010.
- Low power design essentials, J. Rabaey, Springer 2009.