COURSE OUTLINE

(1) GENERAL

SCHOOLS	ENGINEERING, NATURAL SCIENCES		
ACADEMIC UNIT/UNITS	DEPARTMENT OF COMPUTER ENGINEERING AND INFORMATICS, DEPARTMENT OF MATHEMATICS		
TITLE OF MASTER'S DEGREE	DATA DRIVEN COMPUTING AND DECISION MAKING (DDCDM)		
LEVEL OF STUDIES	M.Sc.		
COURSE CODE	DDCD###	SEMESTER	WINTER (UPON SELECTIVE)
COURSE TITLE	CYBERSECURITY		

INDEPENDENT TEACHING ACTIVITIES *if credits are awarded for separate components of the course, e.g. lectures, laboratory exercises, etc. If the credits are awarded for the whole of the course, give the weekly teaching hours and the total credits*	WEEKLY TEACHING HOURS	CREDITS
Lectures and Tutorials	3	
Add rows if necessary. The organisation of teaching and the teaching methods used are described in detail at (d).	Total	7.5

COURSE TYPE *general background, special background, specialised general knowledge, skills development*	Specialised general knowledge Skills development
PREREQUISITE COURSES:	-
LANGUAGE OF INSTRUCTION and EXAMINATIONS:	Greek, (English is also possible).
IS THE COURSE OFFERED TO ERASMUS STUDENTS	Yes (In English).
COURSE WEBSITE (URL)	https://eclass.upatras.gr/courses/CEID1228/

(2) LEARNING OUTCOMES

Learning outcomes

The course learning outcomes, specific knowledge, skills and competences of an appropriate level, which the students will acquire with the successful completion of the course are described.

Consult Appendix A

- *Description of the level of learning outcomes for each qualifications cycle, according to the Qualifications Framework of the European Higher Education Area*
- *Descriptors for Levels 6, 7 & 8 of the European Qualifications Framework for Lifelong Learning and Appendix B*
- *Guidelines for writing Learning Outcomes*

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

✓ *have the appropriate knowledge and background on cybersecurity principles, for current and future applications, as well as on cutting edge technologies,*

✓ *understand the cybersecurity integration, as basic target of system's design,*

✓ *understand the basic concepts of design protection, from external breaks and attackers,*

✓ *analyze external attacks on software applications, hardware platforms and implementations, and to get experienced with protection methodologies,*

✓ *implement detection mechanisms, of harmful, additional applications and integrated systems,*

✓ *to be experiences with modern approaches for cybersecurity, such as machine learning, artificial intelligence, dark web.*

General Competences

Taking into consideration the general competences that the degree-holder must acquire (as these appear in the Diploma Supplement and appear below), at which of the following does the course aim?

Search for, analysis and synthesis of data and information, with the use of the necessary technology
Adapting to new situations
Decision-making
Working independently
Team work
Working in an international environment
Working in an interdisciplinary environment
Production of new research ideas

Project planning and management
Respect for difference and multiculturalism
Respect for the natural environment
Showing social, professional and ethical responsibility and sensitivity to gender issues
Criticism and self-criticism
Production of free, creative and inductive thinking
……
Others…
…….

Working independently
Team work
Working in an international environment
Working in an interdisciplinary environment
Production of new research ideas
Production of free, creative and inductive thinking

(3) SYLLABUS

- Introduction to information security: basic principles and good practices.
- Cryptographic engineering.
- Secure Internet of Things (IoT).
- Digital Forensics.
- Ethics and cybercrime.
- Business plan and information management.
- Secure software and dark web.
- Hardware security.
- Cybersecurity in embedded systems.
- Business Information Continuity.
- Threats and attacks: software and hardware perspectives.
- Cyber Incident Analysis and Response.
- Advanced applications and systems: examples and cases.

(4) TEACHING and LEARNING METHODS - EVALUATION

<table>
<tr><td>DELIVERY
<i>Face-to-face, Distance learning, etc.</i></td><td>Face to face</td></tr>
<tr><td>USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY
<i>Use of ICT in teaching, laboratory education, communication with students</i></td><td>Wide use of ICT and more specifically:
▪ The course is backed up by a homepage, providing all course materials. This web page is duly updated.
▪ Course announcements are provided electronically and are available via: online news platform, and e-mail.
▪ The communication with the students is performed electronically: via e-mail. An online course forum, is also supported, for questions/answers, comments etc.</td></tr>
<tr><td>TEACHING METHODS
<i>The manner and methods of teaching are described in detail.</i>
<i>Lectures, seminars, laboratory practice, fieldwork, study and analysis of bibliography, tutorials, placements, clinical practice, art workshop, interactive teaching, educational visits, project, essay writing, artistic creativity, etc.</i>
<i>The student's study hours for each learning activity are given as well as the hours of non-directed study according to the principles of the ECTS</i></td><td>
<table>
<tr><th><i>Activity</i></th><th><i>Semester workload</i></th></tr>
<tr><td>Lectures and Tutorials</td><td>39 hours</td></tr>
<tr><td>Study of relevant bibliography and familiarization with the topic of selected seminars.</td><td>60 hours</td></tr>
<tr><td>Project preparation and writing of the presentation.</td><td>60 hours</td></tr>
<tr><td>Learning about technical writing, publishing and presentation skills.</td><td>25</td></tr>
<tr><td>Exams and project presentation.</td><td>4</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td><i>Course Total</i></td><td><i>188 hours</i></td></tr>
</table>
</td></tr>
<tr><td>STUDENT PERFORMANCE EVALUATION
<i>Description of the evaluation procedure</i>
<i>Language of evaluation, methods of evaluation, summative or conclusive, multiple choice questionnaires, short-answer</i></td><td>The students' assessment is supported in Greek, through a final written examination, twice in each academic year.
The examination is organized by development questions, short answer questions, exercises and problems solving. Within ten days of the examination, scores and indicative answers to the exam questions are announced, and posted electronically.</td></tr>
</table>

questions, open-ended questions, problem solving, written work, essay/report, oral examination, public presentation, laboratory work, clinical examination of patient, art interpretation, other *Specifically-defined evaluation criteria are given, and if and where they are accessible to students.*	It is defined a day and an hour at which students can see their exams' papers about any questions and doubts they may have, as well as to express their disagreement in rating, if they so wish. Then the rating is validated and finalized.

(5) ATTACHED BIBLIOGRAPHY

- Suggested bibliography:

- *Chwan-Hwa (John) Wu, J. David Irwin, Introduction to Computer Networks and Cybersecurity, 1st edition, CRC Press, ISBN: 9781466572133, 2016.*
- *J. Graham, R. Olson, R. Howard, Cyber Security Essentials, 1st edition, CRC Press, ISBN: 9781439851234, 2010.*
- *W. Stallings, Cryptography and Network Security, 6th edition, Upper Saddle River, Pearson, ISBN: 0133354695, 2014.*
- *Fei Hu, Security and Privacy in Internet of Things: Models, Algorithms and Implementations, CRC Press, ISBN: 9781498723183, 2016.*
- *Eoghan Casey, Handbook of Digital Forensics and Investigations, Elsevier, pages 600, ISBN: 9780123742674, 2010.*
- *Eoghan Casey, Digital Evidence and Computer Crime, 3rd Edition, Elsevier, pages 840, ISBN: 9780123742681, 2011.*
- *N. Sklavos, R. Chaves, G. Di Natale, F. Regazzoni, Hardware Security and Trust, Springer, ISBN: 978-3-3194-4318-8, 2017.*
- *A. Sengupta, S. P. Mohanty, IP Core Protection and Hardware-Assisted Security for Consumer Electronics, IET, ISBN: 9781785617997, 2019.*

- Related academic journals:

- *ACM Transactions on Privacy and Security,*
- *ACM Digital Threats: Research and Practice,*
- *IEEE Transactions on Dependable and Secure Computing,*
- *IEEE Transactions on Information Forensics & Security,*
- *IEEE Security and Privacy,*
- *Journal of Hardware and Systems Security, Springer.*