COURSE OUTLINE

(1) GENERAL

SCHOOL	ENGINEERING		
ACADEMIC UNIT	INFORMATICS AND COMPUTER ENGINEERING		
LEVEL OF STUDIES	UNDERGRADUATE		
COURSE CODE		**SEMESTER**	**7th and 9th**
COURSE TITLE	Networks and Communications Security		

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	2	
Tutorials	1	
Laboratory Exercises	1	
Add rows if necessary. The organisation of teaching and the teaching methods used are described in detail at (d).	4	5

COURSE TYPE general background, special background, specialised general knowledge, skills development	SPECIALIZED GENERAL KNOWLEDGE, SCIENTIFIC AREA.
PREREQUISITE COURSES:	-
LANGUAGE OF INSTRUCTION and EXAMINATIONS:	GREEK (Instruction and Examination)
IS THE COURSE OFFERED TO ERASMUS STUDENTS	NO
COURSE WEBSITE (URL)	

(2)

(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

The "Networks and Communications Security" course is a core part of the "Computer Networks and Communications" direction and deepens the students' knowledge on security of wired and wireless computer networks and security of communications.

The purpose of the course is to deepen the theoretical and practical knowledge that the student already has acquired in computer networks and in the area of computer security, in order to cover the knowledge framework of the scientific area of Networks and Communications Security, which will add specialized skills to the student and high-level skills necessary for the job market and new research dimension to continue his studies at the next level.

Upon successful completion of the course, the student:

- **will recognize the factors that lead to the required network and communications security.**
- **will be able to identify and categorize specific cases of network attacks.**
- **will be able to identify vulnerabilities in communications and networks.**
- **will be able to design and implement secure network systems and applications.**
- **will be able to recognize advantages and disadvantages of alternative secure network and communications architectures.**
- **will be able to distinguish and compare symmetric and asymmetric cryptosystems and to understand the characteristics of hybrid systems.**
- **will know the tools and techniques for identifying security gaps of network devices and applications and to distinguish the problems and errors due to the insufficient implementation of security mechanisms of devices and insufficient protection of information transmitted through online applications.**
- **will be able to apply his/her knowledge to protect the devices and the transmitted network information from malicious acts of interception, modification, destruction and falsification of the information.**
- **will be able to evaluate the secure operation of networks, identify any security gaps in the access and transmission of information, especially from remote users.**
- **will be able to deal with developments in the field of network and communications security, topics in which he/she will have deepened his/her knowledge.**
- **will have the ability to guide the changes brought about by the developments in technology in this field.**
- **will have the ability to evaluate and distinguish between secure and non-secure network systems and communications across their parts.**
- **will have the ability to systematically apply the acquired knowledge to understand and solve practical problems.**
- **will have the ability to use modern methods to protect network and communication systems.**
- **will have the ability to collaborate with others to solve real problems.**

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	Project planning and management
Adapting to new situations	Respect for difference and multiculturalism
Decision-making	Respect for the natural environment
Working independently	Showing social, professional and ethical responsibility and sensitivity to gender issues
Team work	Criticism and self-criticism
Working in an international environment	Production of free, creative and inductive thinking
Working in an interdisciplinary	……

environment Production of new research ideas	Others… …….

- Examine, retrieve, analyze and synthesize data and information by utilizing necessary technologies
- Decision-Making
- Work independently / Teamwork
- Project planning and management
- Work in an interdisciplinary environment
- Production of new research ideas
- Promoting free, creative and inductive thinking

(3)

(3) SYLLABUS

The course includes the topics described in the following list:

- OSI Architecture, Security Services and Security Mechanisms.
- Network Security Requirements
- Attacks on Networks
- Encryption Systems for Networks
- Models for remote access control (MAC, RBAC, NAC, etc.)
- TCP/IP architecture security:
  - at the Physical level (FHSS, DSSS),
  - at NetworkAccess level (EAP, EAPoL, EAP-TLS)
  - at the Internet level (IPsecVPNs)
  - at Transport level (SSL/TLS)
  - at Application level (email, Web, etc.)
- Internet Security
- Security of Wireless and Mobile Networks
- Internet of Things Security
- Cloud Computing Security
- Security of Wireless Sensor Networks
- Security of Ad-Hoc Networks (MANETs)
- Network Application Security
- Network Intrusion Detection
- Firewalls
- Secure Network Protocols
- Secure Network Architectures
- Secure Communications Trust Models and Uncertainty

(4)

(4) TEACHING and LEARNING METHODS - EVALUATION

DELIVERY Face-to-face, Distance learning, etc.	Face to face
USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY Use of ICT in teaching, laboratory education, communication with students	• Specialized software for the majority of the topics described above. • Use of ICT in Course Teaching • Use of the Open eClass course management system, for distributing lecture notes and exercises for practice, and for communication with students.
TEACHING METHODS The manner and methods of teaching are described in detail. 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. 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	**ActivitySemester workload** Lectures 26 Tutorials 13 Laboratory Exercises 13 Essays / Project 25 Independent Study 48 **Course total 125**
STUDENT PERFORMANCE EVALUATION Description of the evaluation procedure Language of evaluation, methods of evaluation, summative or conclusive, multiple choice questionnaires, short-answer 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.	I. Final theory written exam (100%), which includes: * Questions that combine knowledge and criticism, with complete justification and description of arguments, through which it is established the level of understanding of the topics. - Short answer questions - Problem solving related to Network Security and network applications Security - Comparative evaluation of cases - II. Laboratory examination (30%), that derives from: - Written or oral examination - Laboratory work (individual) over the grade of the final theory written exam, when this is at least 5. For successfully qualifying the course, a minimum grade of 5.0 marks (of 10 in total) is mandatory in both written exams and projects evaluation.

(5)

(5) ATTACHED BIBLIOGRAPHY

- Suggested bibliography:

1. Stallings, Cryptography and Network Security: Principles and Practice, Pearson, 8th edition 2020, ISBN-13: 978-0135764268.
2.
3. J.F. Kurose, K.W. Ross, Computer Networking, A top-Down Approach, 6η Έκδοση, 2013, Pearson, ISBN:978-0-13-285620-1.
4. B. Forouzan, Cryptography & Network Security, 1st Edition, McGraw Hill, 2007, ISBN: 978-0073327532.
5. J.F. Kizza, "Guide to Computer Network Security", Springer, 2017.
6. L. Ertaul, L.H. Encinas and E. El-Sheikh "Computer and Network Security Essentials", Springer, 2017.
7. X. He and H. Dai, "Dynamic Games for Network Security", Springer, 2018.
8. E. Maiwald, "Network Security", Mc Graw Hill, 2013.

(6)