IoT Security

Academic Year: (2019 / 2020) **Review date: 30-04-2020**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: CAMARA NUÑEZ, MARIA CARMEN

Type: Compulsory ECTS Credits : 3.0

Year : 1 Semester : 2

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

None

OBJECTIVES

Core Competencies
CB6 Possess and understand pieces of knowledge that provides a basis or opportunity to be original in the development and/or application of ideas, often in a research context.
CB7 That students know how to apply the knowledge acquired and their problem-solving ability in new or poorly known environments within broader (or multidisciplinary) contexts related to their area of study.
CB8 That students can integrate knowledge and face the complexity of making judgments based on information that, being incomplete or limited, includes reflections on the social and ethical responsibilities linked to the application of their knowledge and judgments.
CB9 That students know how to communicate their conclusions and the knowledge and ultimate reasons behind them to specialized and non-specialized audiences in a clear and unambiguous manner.

General Competencies
CG2 Ability to compile and analyse existing knowledge in the different areas of IOT, autonomously, and ability to propose possible solutions to the problems raised.
CG7 Ability to communicate (orally and in writing) conclusions - and the knowledge and ultimate reasons behind them - to specialised and non-specialised audiences in a clear and unambiguous manner.

Specific Competencies
CE5 Ability to design, develop, manage and evaluate mechanisms to guarantee security in the treatment and access to information in computationally limited devices and in IoT networks.
CE6 Ability to apply mathematical, statistical and artificial intelligence methods to model, design and develop intelligent applications, services and systems in the field of IoT.
CE10 Ability to integrate the different systems of perception and control of processes both from the hardware and software point of view.
EC13 Capacity to implement IoT legislation, regulation and standardisation.

LEARNING OUTCOMES
The learning outcomes that students should have are:
- Know and apply the law and legal aspects of IoT.
- Know the reference models and structures of IoT.
- Ability to analyse, design and control systems and services
- To know the security risks inherent to an IoT environment.
- To know the physical security measures applicable to mobile devices.
- To know and apply the fundamental techniques for the protection of information stored in mobile devices.
- Master the main existing security protocols for mobile communications and their application spectrum.

DESCRIPTION OF CONTENTS: PROGRAMME

1. Lesson 1. Introduction.
   a. Introduction to Cybersecurity.
   b. Introduction to IoT.

2. Lesson 2. Architectures in IoT
   a. Architectures.

b. Devices.

3. Lesson 3. Security services and mechanisms
a. Security/communications protocols.
b. Authentication.
c. Identification (Biometrics).
d. Cryptographic primitives.

4. Lesson 4. Advanced topics.
a. (Implantable) Medical devices.
b. Forensic analysis of IoT devices.

LEARNING ACTIVITIES AND METHODOLOGY

TRAINING ACTIVITIES IN THE SYLLABUS RELATING TO SUBJECTS
AF1 Theoretical class
AF4 Practical sessions in the lab
AF6 Group work
AF7 Individual Student Work
AF8 Partial and final examinations

Code activity	Nº Total hours	Nº Hours Attendance	% Attendance Student
AF1	26	26	100
AF4	16	16	100
AF6	40	0	0
AF7	64	0	0
AF8	4	4	100
TOTAL SUBJECT MATTER	150	46	31%

TRAINING TEACHING METHODOLOGIES OF THE PLAN RELATING TO MATTERS
MD1 Presentations in the teacher's classroom with a computer and audiovisual support, in which the main concepts of the subject are developed, and the bibliography is provided to complement the students' learning.
MD2 Critical reading of texts recommended by the subject teacher: Press articles, reports, manuals and/or academic articles, either for later discussion in class or to expand and consolidate knowledge of the subject.
MD3 Resolution of practical cases, problems, etc. raised by the teacher individually or in a group.
MD4 Presentation and discussion in class, under the moderation of the professor of topics related to the content of the subject, as well as practical cases.
MD5 Elaboration of works and reports individually or in a group.

ASSESSMENT SYSTEM

The assessment may be continuous assessment or non-continuous assessment:

1. Ordinary sitting - continuous assessment:

A. End of term examination (50% of the final mark)
-A minimum grade of 4.0 is mandatory to pass the subject

B. Periodical assignments (50% of the final mark)
-State of the art on a topic related to the subject.
-Practical cases (e.g. biometric system, forensic analysis of IoT devices).

2. Ordinary sitting - non-continuous assessment:
A. End of term examination (100% of the final mark)
- A maximum grade of 6.0 may be achieved (i.e. 100% = 6.0)
- At least 5.0 marks must be achieved to pass the subject.
- The exam contains specific parts regarding the competencies that have been addressed in the assignments.

3. Extraordinary sitting
In the extraordinary sitting, the following rules apply:

a. If the student followed the continuous assessment method, the exam will have the same relative weight as in the ordinary sitting. The mark of the continuous evaluation is kept.

b. Otherwise, students will have an exam counting for 100% of the final mark. This exam may contain questions related to the proposed assignments. Assignments cannot be re-delivered in this sitting.

c. Even if the student did follow the continuous assessment, he/she has the right to be assessed considering only the mark from the final exam if it is more favourable to him/her.

% end-of-term-examination:	50
% of continuous assessment (assigments, laboratory, practicals…):	50

BASIC BIBLIOGRAPHY

- Aaron Guzman, Aditya Gupta IoT Penetration Testing Cookbook: Identify vulnerabilities and secure your smart devices, Packt Publishing, 2017
- D. Uckelmann, M. Harrison and F. Michahelles Architecting the Internet of Things, Springer-Verlag Berlin Heidelberg, 2011
- Dimitrios Serpanos, Marilyn Wolf Internet-of-Things (IoT) Systems: Architectures, Algorithms, Methodologies, Springer, 2018
- FTC Staff Report Internet of Things: Privacy & Security in a Connected World, FTC, 2015
- Francis daCosta Rethinking the Internet of Things: A Scalable Approach to Connecting Everything, Apress, 2014
- IoT Hackers Handbook IoT Hackers Handbook: An Ultimate Guide to Hacking the Internet of Things and Learning IoT Security , IoT Hackers Handbook, 2017

ADDITIONAL BIBLIOGRAPHY

- N. Jeyanthi, Ajith Abraham, Hamid Mcheick Ubiquitous Computing and Computing Security of IoT, Springer, 2018
- Sunil Cheruvu, Anil Kumar, Ned Smith, David Wheeler Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform security deployment, Apress, 2019