ANX-PR/CL/001-01

LEARNING GUIDE

SUBJECT

593000508 - Security For Iot Applications

DEGREE PROGRAMME

59AH - Master Universitario en Internet Of Things (iot)

ACADEMIC YEAR & SEMESTER

2019/20 - Semester 2

Index

Learning guide

1. Description

1.1. Subject details

Name of the subject	593000508 - Security For Iot Applications
No of credits	4.5 ECTS
Type	Compulsory
Academic year ot the programme	First year
Semester of tuition	Semester 2
Tuition period	February-June
Tuition languages	English
Degree programme	59AH - Master Universitario en Internet Of Things (iot)
Centre	59 - Escuela Tecnica Superior de Ingenieria y Sistemas de Telecomunicacion
Academic year	2019-20

2. Faculty

2.1. Faculty members with subject teaching role

Name and surname	Office/Room	Email	Tutoring hours *
Ivan Pau De La Cruz (Subject coordinator)	A4404	ivan.pau@upm.es	Sin horario.
Maria Luisa Martin Ruiz	A4406	marialuisa.martinr@upm.es	Sin horario.

* The tutoring schedule is indicative and subject to possible changes. Please check tutoring times with the faculty member in charge.

3. Skills and learning outcomes *

3.1. Skills to be learned

CB07 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio

CB08 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios

CE.09 - Analizar, implementar y evaluar los mecanismos de seguridad mas adecuados para dispositivos y redes usados en cada aplicación específica de IoT

CG01 - Los alumnos demostrarán tener una visión del estado actual, las necesidades y los problemas que se plantean en el mundo de la IoT, así como de las arquitecturas y estándares más utilizados

CG04 - Los alumnos tendrán la capacidad de aplicar criterios de eficiencia, escalabilidad, fiabilidad y seguridad en distintos ámbitos de aplicaciones inteligentes y sistemas ciberfísicos, tales como Smart Living, Smart Cities o eHealth

CT.01 - Capacidad de uso de la lengua inglesa para el trabajo en contextos internacionales

CT.04 - Capacidad para la elaboración, planificación, coordinación y gestión técnica y económica de proyectos siguiendo criterios éticos, de calidad y medioambientales

3.2. Learning outcomes

RA32 - To manage relevant information on security, including the search, study, synthesis and preparation of new documents

RA30 - To design simple and complex firewall systems, as well as barrier defense, intrusion detection and hacking attack defense systems

RA33 - To use semantic information models to describe IoT devices and services

RA28 - To configure secure web servers by applying encryption systems

RA29 - To apply security mechanisms in wireless networks and mobile devices

RA31 - To audit networks from the point of view of defense and security against attacks, both internal and external

* The Learning Guides should reflect the Skills and Learning Outcomes in the same way as indicated in the Degree Verification Memory. For this reason, they have not been translated into English and appear in Spanish.

4. Brief description of the subject and syllabus

4.1. Brief description of the subject

The IoT Security course has as main objective the presentation of the problems and existing techniques when making designs and secure deployments of IoT-based solutions. The course will follow a learning methodology based on activities. This method proposes actions, as problems to solve, that must be carried out and whose development implies the need to learn new concepts that are aligned with the proposed objectives of the course.

In addition to the development of the activities, students must prepare a work related to some aspect of IoT security. This work can be exploratory of some concrete technology, of investigation in some type of solution or of direct application to some solutions previously contemplated by the students.

4.2. Syllabus

1. Introduction to the Course

2. Security Concepts and Primitives

3. Security Protocols

4. Infrastructure Protection

5. Schedule

5.1. Subject schedule*

Week	Face-to-face classroom activities	Face-to-face laboratory activities	Other face-to-face activities	Assessment activities
1	**General Security Concepts and Cryptography** Duration: 05:30			
2		**General Security Concepts and Cryptography** Duration: 03:10		**Test** Continuous assessment and final examination Duration: 00:20
3	**Security Infrastructure and Protocols** Duration: 03:10			**Test** Continuous assessment and final examination Duration: 00:20
4	**Security Infrastructure and Protocols** Duration: 03:10			**Test** Continuous assessment and final examination Duration: 00:20
5		**Security Infrastructure and Protocols** Duration: 05:10		**Test** Continuous assessment and final examination Duration: 00:20
6		**Developing a Protected IoT Solution** Duration: 03:10		**Test** Continuous assessment and final examination Duration: 00:20
7		**Developing a Protected IoT Solution** Duration: 03:10		
8				**"Challenges of IoT" work delivery** Continuous assessment and final examination Duration: 00:00 **In-class presentation of group work** Continuous assessment and final examination Duration: 02:40

9				
10				
11				
12				
13				
14				
15				
16				
17				

The independent study hours are training activities during which students should spend time on individual study or individual assignments.

Depending on the programme study plan, total values will be calculated according to the ECTS credit unit as 26/27 hours of student face-to-face contact and independent study time.

* The subject schedule is based on a previous theorical planning of the subject plan and might go to through experience some unexpected changes along throughout the academic year.

6. Activities and assessment criteria

6.1. Assessment activities

6.1.1. Continuous assessment

Week	Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills
2	Test		Face-to-face	00:20	10%	0 / 10	CT.01 CE.09 CB07 CB08
3	Test		Face-to-face	00:20	10%	0 / 10	CT.01 CE.09 CB07 CB08
4	Test		Face-to-face	00:20	10%	0 / 10	CT.01 CE.09 CB07 CB08
5	Test		Face-to-face	00:20	10%	0 / 10	CB07 CB08 CT.01 CE.09
6	Test		Face-to-face	00:20	10%	0 / 10	CB07 CB08 CT.01 CE.09
8	"Challenges of IoT" work delivery		Face-to-face	00:00	15%	0 / 10	CB08 CT.01 CG01
8	In-class presentation of group work		Face-to-face	02:40	35%	0 / 10	CG04 CT.01 CT.04 CE.09 CB07

6.1.2. Final examination

Week	Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills

2	Test		Face-to-face	00:20	10%	0 / 10	CT.01 CE.09 CB07 CB08
3	Test		Face-to-face	00:20	10%	0 / 10	CT.01 CE.09 CB07 CB08
4	Test		Face-to-face	00:20	10%	0 / 10	CT.01 CE.09 CB07 CB08
5	Test		Face-to-face	00:20	10%	0 / 10	CB07 CB08 CT.01 CE.09
6	Test		Face-to-face	00:20	10%	0 / 10	CB07 CB08 CT.01 CE.09
8	"Challenges of IoT" work delivery		Face-to-face	00:00	15%	0 / 10	CB08 CT.01 CG01
8	In-class presentation of group work		Face-to-face	02:40	35%	0 / 10	CG04 CT.01 CT.04 CE.09 CB07

6.1.3. Referred (re-sit) examination

Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills
Test		Face-to-face	02:00	50%	0 / 10	CG04 CT.01 CG01 CB07
Final Work		Face-to-face	02:00	50%	0 / 10	CG04 CT.01 CT.04 CE.09 CG01 CB07 CB08

6.2. Assessment criteria

As a general criterion, it is considered that the subject is passed if after adding all the evaluation items, the students take a grade equal to or higher than 5.0 points (out of 10).

The evaluation of only final examination consists in the same number of test performed in the continuous evaluation. In addition the student should deliver also the "Challenges for IoT Security" work and make a presentation with an individual work that must be previously agreed with the docents of the subject.

Both, continuous and final evaluation, will apply the next percentages for grading:

- Evaluation test through the Moodle platform: 50% of the grade.
- "Challenges for IoT Security" work: 15% of the grade.
- Final work: 30% of the grade.

The evaluation of the extraordinary call will be based on two in-class tests:

- Evaluation test through the Moodle platform (50% of the grade)
- Presentation of a final work with a theme agreed with the teachers of the subject (50% of the grade)

In the event that the student has already submitted the group work during the ordinary period of the course, and has a grade higher than 5.0, the grade of that work will be maintained and should make a shorter work to complete this part of the evaluation (15% of the grade).

7. Teaching resources

7.1. Teaching resources for the subject

Name	Type	Notes
Moodle space of the Subject	Web resource	In the moodle space of the subject will be published relevant information both for the contents of the course and to deepen in the area.