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

2024/25 - 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	2024-25

2. Faculty

2.1. Faculty members with subject teaching role

Name and surname	Office/Room	Email	Tutoring hours *
Maria Luisa Martin Ruiz	A4406	marialuisa.martinr@upm.es	Sin horario.
Mario Vega Barbas (Subject coordinator)	A4418	mario.vega@upm.es	Sin horario.
Maria Dolon Poza	A4411	maria.dolonp@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	Type 1 activities	Type 2 activities	Distant / On-line	Assessment activities
1	**General Security Concepts and Cryptography** Duration: 01:30 Lecture **Security concepts and Primitives** Duration: 02:00 Laboratory assignments			
2	**Security Concepts and Primitives** Duration: 03:10 Laboratory assignments **Test** Duration: 00:20 Additional activities			**Test** Online test Progressive assessment Presential Duration: 00:20
3	**Security Concepts and primitives** Duration: 05:10 Laboratory assignments **Test** Duration: 00:20 Additional activities			**Test** Online test Progressive assessment Presential Duration: 00:20
4	**Security Infrastructure and Protocols** Duration: 03:30 Laboratory assignments			
5	**Security Infrastructure and Protocols** Duration: 03:10 Laboratory assignments **Test** Duration: 00:20 Additional activities			**Test** Online test Progressive assessment Presential Duration: 00:20
6	**Security Infrastructure and Protocols** Duration: 03:30 Laboratory assignments **Test** Duration: 00:20 Additional activities			**Test** Online test Progressive assessment Presential Duration: 00:20
7	**Security Infrastructure and Protocols** Duration: 03:10 Laboratory assignments **Test** Duration: 00:20 Additional activities			**Test** Online test Progressive assessment Presential Duration: 00:20

8	**Infrastructure Protection** Duration: 05:30 Laboratory assignments **Test** Duration: 00:20 Additional activities			**Test** Online test Progressive assessment Presential Duration: 00:20
9	**Infrastructure Protection** Duration: 03:10 Laboratory assignments **Test** Duration: 00:20 Additional activities			**Test** Online test Progressive assessment Presential Duration: 00:20
10	**Infrastructure Protection** Duration: 03:30 Laboratory assignments			
11	**Test** Duration: 00:20 Additional activities **In-class presentation of group work** Duration: 03:10 Additional activities			**Test** Online test Progressive assessment Presential Duration: 00:20 **In-class presentation of group work** Group presentation Progressive assessment Presential Duration: 03:10
12				
13				
14				
15				
16				
17				**Retaking test** Online test Global examination Presential Duration: 03:30

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 schedule is based on an a priori planning of the subject; it might be modified during the academic year, especially considering the COVID19 evolution.

6. Activities and assessment criteria

6.1. Assessment activities

6.1.1. Assessment

Week	Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills
2	Test	Online test	Face-to-face	00:20	8%	0 / 10	CB07 CB08 CT.01 CE.09
3	Test	Online test	Face-to-face	00:20	7%	0 / 10	CB07 CB08 CT.01 CE.09
5	Test	Online test	Face-to-face	00:20	7%	0 / 10	
6	Test	Online test	Face-to-face	00:20	7%	0 / 10	
7	Test	Online test	Face-to-face	00:20	7%	0 / 10	CB07 CB08 CT.01 CE.09
8	Test	Online test	Face-to-face	00:20	7%	0 / 10	CB07 CB08 CT.01 CE.09
9	Test	Online test	Face-to-face	00:20	7%	0 / 10	CB07 CB08 CT.01 CE.09
11	Test	Online test	Face-to-face	00:20	15%	0 / 10	CB07 CT.01 CE.09
11	In-class presentation of group work	Group presentation	Face-to-face	03:10	35%	0 / 10	CB07 CB08 CG01 CG04 CT.01 CT.04 CE.09

6.1.2. Global examination

Week	Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills
17	Retaking test	Online test	Face-to-face	03:30	65%	7 / 10	CB07 CB08 CG01 CG04 CT.01 CT.04 CE.09

6.1.3. Referred (re-sit) examination

Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills
Test	Online test	Face-to-face	02:00	65%	0 / 10	CB07 CG01 CG04 CT.01
Final Work	Individual work	Face-to-face	02:00	35%	0 / 10	CB07 CB08 CG01 CG04 CT.01 CT.04 CE.09

6.2. Assessment criteria

The dates of the different exams of the subject depend on the organisation of the Semester Assessment Plan, coordinated by the SOA, and are published in the School's Annual Teaching Plan. In the event of any discrepancy that may arise between the information published in this guide and that published in the Annual Teaching Plan, the information published in the latter should be taken into account, as it contains the appropriate updates.

Evaluation criteria

General criterion: 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 will apply the following percentages for grading:

- Evaluation test through the Moodle platform: 65% of the grade
- Group work: 35% of the grade.

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

- Evaluation test through the Moodle platform (65% of the grade)
- Presentation of final work with a theme agreed with the teachers of the subject (35% of the grade)

In the case that the student already submitted the group work during the ordinary period of the course, and had a grade higher than 5.0, the group work's mark can be optionally maintained.

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.