# ANX-PR/CL/001-01

# LEARNING GUIDE

## SUBJECT

**103000590 - Computer Security**

## DEGREE PROGRAMME

10AK - Master Universitario En Software Y Sistemas

## ACADEMIC YEAR & SEMESTER

2023/24 - Semester 1

# Index

## Learning guide

# 1. Description

## 1.1. Subject details

| | |
|---|---|
| **Name of the subject** | 103000590 - Computer Security |
| **No of credits** | 4 ECTS |
| **Type** | Optional |
| **Academic year ot the programme** | First year |
| **Semester of tuition** | Semester 1 |
| **Tuition period** | September-January |
| **Tuition languages** | English |
| **Degree programme** | 10AK - Master Universitario en Software y Sistemas |
| **Centre** | 10 - Escuela Tecnica Superior De Ingenieros Informaticos |
| **Academic year** | 2023-24 |

# 2. Faculty

## 2.1. Faculty members with subject teaching role

| Name and surname | Office/Room | Email | Tutoring hours * |
|---|---|---|---|
| Manuel Carro Liñares (Subject coordinator) | 2303 | manuel.carro@upm.es | F - 15:00 - 19:00<br>Please send an e-mail to set up an appointment before going to the instructor's office. |
| Julio Mariño Carballo | D-2308 | julio.marino@upm.es | Tu - 15:00 - 17:00<br>W - 12:30 - 13:30<br>Th - 15:00 - 17:00<br>F - 12:30 - 13:30<br>Please get in touch |

| | | | |
|---|---|---|---|
| | | | with the instructor to get an appointment in order to check his availability. |

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

### 2.3. External faculty

| Name and surname | Email | Institution |
|---|---|---|
| Marco Guarnieri | marco.guarnieri@imdea.org | IMDEA Software Institute |
| Pedro Moreno | pedro.moreno@imdea.org | IMDEA Software Institute |
| Dario Fiore | Dario.Fiore@imdea.org | IMDEA Software Institute |
| Juan Caballero | Juan.caballero@imdea.org | IMDEA Software Institute |
| Ignacio Cascudo | ignacio.cascudo@imdea.org | IMDEA Software Institute |
| Srdjan Matic | srdjan.matic@imdea.org | IMDEA Software Institute |
| Alessandra Gorla | alessandra.gorla@imdea.org | IMDEA Software Institute |

## 3. Prior knowledge recommended to take the subject

### 3.1. Recommended (passed) subjects

The subject - recommended (passed), are not defined.

### 3.2. Other recommended learning outcomes

- An undergraduate level course on computer security is desired but not required. Some demonstrable knowledge on the basic principles of computer security is necessary.

# 4. Skills and learning outcomes *

## 4.1. Skills to be learned

CG1 - 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.

CG13 - Apreciación de los límites del conocimiento actual y de la aplicación práctica de la tecnología más reciente.

CG4 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

CG8 - Planteamiento y resolución de problemas también en áreas nuevas y emergentes de su disciplina

CG9 - Aplicación de los métodos de resolución de problemas más recientes o innovadores y que puedan implicar el uso de otras disciplinas

CGI20 - Adquirir conocimientos científicos avanzados del campo de la informática que le permitan generar nuevas ideas dentro de una línea de investigación.

CGI23 - Capacidad de leer y comprender publicaciones dentro de su ámbito de estudio/investigación, así como su catalogación y valor científico

## 4.2. Learning outcomes

RA12 - Be familiar with examples of real applications and research trends and lines

RA112 - Identify computer security threats and decide the best proactive and reactive measures against them

* 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.

# 5. Brief description of the subject and syllabus

## 5.1. Brief description of the subject

This course gives students a general view of Computer Security. Lectures are divided in independent blocks which provide basic concepts in Computer Security, such as cryptography, software security, network security, or physical security. Each block includes a theory part to give students the basic concepts and a practical exercise to demonstrate and fix the presented concepts. The particular order and length of the topics in the blocks will ultimately depend on the schedule of the instructors.

- **Introduction to Security.** This module will first cover a general introduction to computer security (what is security, why it is important, what areas of computer science does it draw on, etc.).
- **Cryptography.** Here we will introduce basic concepts of cryptography, including notions of private key and public key cryptography, encryption, and digital signatures.
- **Network Security**. The Internet and other communication networks are critical for most of our daily tasks. This block will discuss problems and solutions in securing Internet-connected communication networks. The block will cover topics such as HTTPS/TLS/SSL, intrusion detection, and denial-of-service protection.
- **Software Security**. Whether you want to understand if your code is vulnerable to possible exploits or rather you want to understand if some third party code is malicious, you have to *analyze* a software artifact. This module will present different static and dynamic analysis techniques that can give a better understanding of a software artifact. Some of the techniques that we will see include symbolic execution, taint analysis, and fuzz testing. We will see that these techniques can be used for different purposes and can work for different platforms (e.g., desktop, Web, mobile).
- **Physical Security**. This module will provide an introduction to the physical aspects of information security. We will discuss so-called side-channel attacks, which exploit secret-dependent variations of a program's execution time, network use, or power consumption. We will start by focusing on side-channel attacks that exploit different in execution time caused by memory caches. Next, we will focus on recent speculative execution attacks such as Spectre, which exploit a CPU optimization called speculative execution to compromise the security of bug-free programs. We will study how speculative execution attacks work and how one can reason about them.

## 5.2. Syllabus

1. Introduction to Security

2. Cryptography

3. Network security

4. Software Security

5. Physical Security

# 6. Schedule

## 6.1. Subject schedule*

| Week | Classroom activities | Laboratory activities | Distant / On-line | Assessment activities |
|---|---|---|---|---|
| 1 | **Introduction to Computer Security**<br>Duration: 02:00<br>Lecture | | | |
| 2 | **Cryptography**<br>Duration: 02:00<br>Lecture | | | |
| 3 | **Cryptography**<br>Duration: 02:00<br>Lecture | | | |
| 4 | **Cryptography**<br>Duration: 02:00<br>Lecture | | | |
| 5 | **Cryptography**<br>Duration: 02:00<br>Lecture | | | **Practical problem / exercise on Cryptography**<br>Individual work<br>Continuous assessment<br>Not Presential<br>Duration: 04:00 |
| 6 | **Network security**<br>Duration: 02:00<br>Lecture | | | |
| 7 | **Network security**<br>Duration: 02:00<br>Lecture | | | |
| 8 | **Network security**<br>Duration: 02:00<br>Lecture | | | **Practical problem / exercise on Network Security**<br>Individual work<br>Continuous assessment<br>Not Presential<br>Duration: 04:00 |
| 9 | **Software security**<br>Duration: 02:00<br>Lecture | | | |
| 10 | **Software security**<br>Duration: 02:00<br>Lecture | | | |
| 11 | **Software security**<br>Duration: 02:00<br>Lecture | | | |
| 12 | **Software security**<br>Duration: 02:00<br>Lecture | | | **Practical problem / exercise on Software Security**<br>Individual work<br>Continuous assessment<br>Not Presential<br>Duration: 04:00 |

| | | | | |
|---|---|---|---|---|
| 13 | **Physical security**<br>Duration: 02:00<br>Lecture | | | |
| 14 | **Physical security**<br>Duration: 02:00<br>Lecture | | | |
| 15 | **Physical security**<br>Duration: 02:00<br>Lecture | | | **Practical problem / exercise on Physical Security**<br>Individual work<br>Continuous assessment<br>Not Presential<br>Duration: 04:00 |
| 16 | | | | |
| 17 | | | | **Global exam**<br>Written test<br>Final examination<br>Presential<br>Duration: 02:00 |

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.

# 7. Activities and assessment criteria

## 7.1. Assessment activities

### 7.1.1. Assessment

| Week | Description | Modality | Type | Duration | Weight | Minimum grade | Evaluated skills |
|---|---|---|---|---|---|---|---|
| 5 | Practical problem / exercise on Cryptography | Individual work | No Presential | 04:00 | 25% | 2 / 10 | CG1<br>CG4<br>CG8<br>CG9<br>CG13<br>CGI20<br>CGI23 |
| 8 | Practical problem / exercise on Network Security | Individual work | No Presential | 04:00 | 25% | 2 / 10 | CG1<br>CG4<br>CG8<br>CG9<br>CG13<br>CGI20<br>CGI23 |
| 12 | Practical problem / exercise on Software Security | Individual work | No Presential | 04:00 | 25% | 2 / 10 | CG1<br>CG4<br>CG8<br>CG9<br>CG13<br>CGI20<br>CGI23 |
| 15 | Practical problem / exercise on Physical Security | Individual work | No Presential | 04:00 | 25% | 2 / 10 | CG1<br>CG4<br>CG8<br>CG9<br>CG13<br>CGI20<br>CGI23 |

### 7.1.2. Global examination

| Week | Description | Modality | Type | Duration | Weight | Minimum grade | Evaluated skills |
|---|---|---|---|---|---|---|---|
| 17 | Global exam | Written test | Face-to-face | 02:00 | 100% | 5 / 10 | CG1<br>CG4<br>CG8<br>CG9<br>CG13<br>CGI20<br>CGI23 |

### 7.1.3. Referred (re-sit) examination

| Description | Modality | Type | Duration | Weight | Minimum grade | Evaluated skills |
|---|---|---|---|---|---|---|
| Comprehensive exam | Written test | Face-to-face | 02:00 | 100% | 5 / 10 | CG1<br>CG8<br>CG9<br>CG13<br>CGI20<br>CGI23 |

## 7.2. Assessment criteria

- No mandatory activities are necessary to pass via the global exam.
- The minimum grade to pass the course is 5 over 10 (either when it is calculated as the weighted sum of individual homework or when it is the grade of a single comprehensive exam).
- The global exams, both regular and extraordinary, will be made in person.
- Copying from any source (either textbooks, the Internet, another student, or any other source) with or without the permission of the author of the source, as well as other types of academic fraud, can lead to a 'fail' grade in the course and / or being reported to the academic authorities, who will decide whether to take additional authoritative measures. In particular, in case of non-ethical or fraudulent behavior, the Law 3/2022 of February 24th will be applied, as well as the corresponding UPM regulations. Article 12 and 14 of Law 3/2022 states that a serious fault may mean, among other outcomes, failing the corresponding sitting.
- There are no learning blocks whose earned grades can be carried over to future academic courses.
- Failure to deliver the homework at the time and in the form stated by the instructor(s) may result in a failure for that exercise.
- Active participation in the course can be taken into account to fine-tune the student's final grade.

# 8. Teaching resources

## 8.1. Teaching resources for the subject

| Name | Type | Notes |
|---|---|---|
| Various | Others | Will be decided based on the selected topics. |

# 9. Other information

## 9.1. Other information about the subject