ANX-PR/CL/001-01

LEARNING GUIDE

SUBJECT

103000738 - Computer Security

DEGREE PROGRAMME

10AM - Master Universitario En Ingenieria Del Software

ACADEMIC YEAR & SEMESTER

2024/25 - Semester 1

Index

Learning guide

1. Description

1.1. Subject details

Name of the subject	103000738 - 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	10AM - Master Universitario en Ingenieria del Software
Centre	10 - Escuela Tecnica Superior De Ingenieros Informaticos
Academic year	2024-25

2. Faculty

2.1. Faculty members with subject teaching role

Name and surname	Office/Room	Email	Tutoring hours *
Julio Mariño Carballo	D-2308	julio.marino@upm.es	Tu - 15:00 - 17:00 W - 12:30 - 13:30 Th - 15:00 - 17:00 F - 12:30 - 13:30 Please get in touch with the instructor to get an appointment in order to check his availability.

Manuel Carro Liñares (Subject coordinator)	2303	manuel.carro@upm.es	F - 15:00 - 19:00 Please send an e-mail to set up an appointment before going to the instructor's office.

* 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
Juan Caballero	Juan.caballero@imdea.org	IMDEA Software Institute
Srdjan Matic	srdjan.matic@imdea.org	IMDEA Software Institute
Alessandra Gorla	alessandra.gorla@imdea.org	IMDEA Software Institute
Georgios Portokalidis	georgios.portokalidis@imdea.org	IMDEA Software

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

CE13 - Tener una visión de los distintos aspectos específicos y emergentes de la ingeniería del software, y profundizar en algunos de ellos

CE14 - Comprender lo que pueden y no pueden conseguir las prácticas actuales de ingeniería del software, y sus limitaciones y su posible futura evolución.

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 (RD)

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

CG14 - Conocimiento y comprensión de la informática necesaria para la creación de modelos de información, y de los sistemas y procesos complejos

CG3 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades (RD)

CG7 E - Especificación y realización de tareas informáticas complejas, poco definidas o no familiares

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

4.2. Learning outcomes

RA80 - 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 will focus on providing the students with a global view of the field of computer security. Classes will be divided in 4 independent blocks of lectures, each lasting 3-4 weeks and taught by different teachers. Each block provides basic concepts in a core area of computer security: network security, software exploitation, software analysis, and physical security. Each block will comprise lectures to provide the student with basic concepts and a homework to practice and demonstrate the learned concepts.

Module 1: Introduction to Security + Network 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.). Then, it will introduce basic concepts of network security covering topics such as HTTPS/TLS/SSL, network scanning, and denial-of-service protection.

Module 2: Software Analysis

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).

Module 3: Software Exploitation

This module will introduce students to techniques used to exploit software vulnerabilities, and the defenses that have been introduced to protect against such attacks. It will cover the basics of memory corruption vulnerabilities, such as buffer overflows, and how they can be exploited to gain control of a program and perform arbitrary code execution. We will look at how defenses, like address space layout randomization and stack canaries aim to prevent such attacks and how they can be bypassed. We will also cover more advanced exploitation techniques, such as return-oriented programming and recent additions to the defensive landscape, such as control-flow integrity.

Module 4: 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. Network security

3. Software Analysis

4. Software Exploitation

5. Physical Security

6. Schedule

6.1. Subject schedule*

Week	Type 1 activities	Type 2 activities	Distant / On-line	Assessment activities
1	**Course Overview** Duration: 02:00 Lecture			
2	**Introduction to Computer Security** Duration: 02:00 Lecture			
3	**Network security** Duration: 02:00 Lecture			
4	**Network security** Duration: 02:00 Lecture			
5	**Network security** Duration: 02:00 Lecture			
6	**Software Analysis** Duration: 02:00 Lecture			
7	**Software Analysis** Duration: 02:00 Lecture			
8	**Software Analysis** Duration: 02:00 Lecture			
9	**Additional security topics** Duration: 01:00 Additional activities			**Midterm exam** Written test Progressive assessment Presential Duration: 01:00
10	**Software exploitation** Duration: 02:00 Lecture			
11	**Software exploitation** Duration: 02:00 Lecture			
12	**Software exploitation** Duration: 02:00 Lecture			
13	**Physical security** Duration: 02:00 Lecture			

14	**Physical security** Duration: 02:00 Lecture			
15	**Physical security** Duration: 02:00 Lecture			
16				
17				**Resit of modules 1 and 2** Written test Global examination Presential Duration: 01:00 **Exam of modules 3 and 4** Written test Progressive assessment Presential Duration: 01:00

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.

7. Activities and assessment criteria

7.1. Assessment activities

7.1.1. Assessment

Week	Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills
9	Midterm exam	Written test	Face-to-face	01:00	50%	2 / 10	CG7 E CG9 CG13 CG14 CE14 CG3 CG1 CG8 CE13
17	Exam of modules 3 and 4	Written test	Face-to-face	01:00	50%	2 / 10	CG13 CG14 CE14 CG3 CG1 CG8 CE13 CG7 E CG9

7.1.2. Global examination

Week	Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills
17	Resit of modules 1 and 2	Written test	Face-to-face	01:00	50%	2 / 10	CG13 CG14 CE14 CG3 CG1 CG8 CE13 CG7 E CG9

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	

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 midterm and 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.
- The evaluation will be based on two exams: mid-term and final.
- The mid-term exam will cover the first two modules.
- The final exam will have two parts: one of them will cover the first two modules and the other one will cover the last two modules.
- Students wishing to pass the course using progressive evaluation should make the mid-term and the part of the final exam covering the last two modules, and their grade will be calculated as 50% from the mid-term and 50% from the part of the final exam covering the last two modules.
- Students wishing to pass the course using global evaluation, regardless of whether they made the mid-term, should make the two parts of the final exam and their grade will be calculated with 50% from the part covering the first two modules and 50% from the part covering the last two modules, regardless of whether the student made the mid-term exam.
- Any student that submits any answer (even partial) from the part of the final exam covering the two first modules will be considered to have switched to global evaluation.
- The July (resit) evaluation will consist of a single global exam covering all the material given during the course.

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