Computer Security Fall 2024/25

Syllabus

September 16, 2024

Course Description

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.

Classes

Classes will take place on Mondays 12:00-14:00. Classes will take place in Level B of the IMDEA Software Institute building. IMDEA Software is located in the Campus de Montegancedo, about 5 minutes walk from the School of Computer Science. Directions to the building are available here: `https://software.imdea.org/contact_and_directions/directions.html`

Classes will by physical. We will not retransmit the lessons online, unless needed (e.g., if a class needs to be moved or a pandemic re-appears). If a class needs to be re-scheduled due to a holiday or some other event, the new time will be agreed with the students.

Course Material

Since the course teachers are not UPM faculty, we do not use UPM's systems.
Instead, course material will be provided at the following URL:
`https://cloud.software.imdea.org/index.php/s/XXejicgCxbgySzH`
Password: `s3cUrityR0cks`

Communication

We will use a mailing list for communication regarding the course. You should have received an invitation through your UPM account. Let us know otherwise. You can handle your subscription (e.g., register another address, unregister, ...) at:
`http://software.imdea.org/cgi-bin/mailman/listinfo/computer-security-2024-2025`

For direct questions, you can also contact the professors through their email:

- Juan Caballero: juan.caballero@imdea.org
- Alessandra Gorla: alessandra.gorla@imdea.org
- Marco Guarnieri: marco.guarnieri@imdea.org
- Srdjan Matic: srdjan.matic@imdea.org
- Georgios Portokalidis: georgios.portokalidis@imdea.org

Office Hours

We do not have fixed times for office hours, but hold them upon request. If you have questions about a module drop the teacher of that module an email to request an appointment.

Overview of Modules

#	Module	Lecturer	Timeline
1	Network Security	Srdjan Matic, Juan Caballero	16.09 – 07.10
2	Software Analysis	Alessandra Gorla	14.10 – 28.10
3	Software Exploitation	Georgios Portokalidis	11.11 – 25.11
4	Physical Security	Marco Guarnieri	02.12 – 16.12

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.

Course Evaluation

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 cover the whole course material. For the final exam, the students can choose whether to answer the questions for the first two modules or use instead their grade from the

Date	Module	Professor	Notes
Monday, September 16th	Introduction to Computer Security	Srdjan Matic	
Monday, September 23rd	Network Security	Srdjan Matic	
Monday, September 30th	Network Security	Juan Caballero	
Monday, October 7th	Network Security	Juan Caballero	
Monday, October 14th	Software Analysis	Alessandra Gorla	
Monday, October 21st	Software Analysis	Alessandra Gorla	
Monday, October 28th	Software Analysis	Alessandra Gorla	
Monday, November 4th	Mid-term Exam	All	
Monday, November 11th	Software Exploitation	Georgios Portokalidis	
Monday, November 18th	Software Exploitation	Georgios Portokalidis	
Monday, November 25th	Software Exploitation	Georgios Portokalidis	
Monday, December 2nd	Physical Security	Marco Guarnieri	
Monday, December 9th	Physical Security	Marco Guarnieri	
Monday, December 16th	Physical Security	Marco Guarnieri	
Monday, January 13th	Final Exam	All	Exam will take place at 11:00
Monday, June 30th	Extra Exam	All	Exam will take place at 11:00

Table 1: Course schedule.

mid-term exam. If they answer any part of the first half their final course grade would be that of the final exam. Otherwise, the final course grade would be the grade of the mid-term exam (50%) plus the grade of the second part of the final exam (50%).