Computer Security Fall 2023/24

Syllabus

September 12, 2023

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: cryptography, network security, software security, 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/zQweKHLpadbJyPE`
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-2023-2024`

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

- Juan Caballero: juan.caballero@imdea.org
- Ignacio Cascudo: ignacio.cascudo@imdea.org
- Dario Fiore: dario.fiore@imdea.org
- Alessandra Gorla: alessandra.gorla@imdea.org

- Marco Guarnieri: marco.guarnieri@imdea.org
- Srdjan Matic: srdjan.matic@imdea.org
- Pedro Moreno-Sanchez: pedro.moreno@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
-	Course Overview	All lecturers	11.09
1	Cryptography	Dario Fiore, Ignacio Cascudo	18.09 – 16.10
2	Network Security	Srdjan Matic, Juan Caballero	23.10 – 06.11
3	Software Security	Alessandra Gorla, Juan Caballero	13.11 – 27.11
4	Physical Security	Marco Guarnieri	04.12 – 18.12

Module 1: Introduction to Security + Cryptography

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 cryptography, including notions of private key and public key cryptography, encryption, and digital signatures.

Module 2: 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.

Module 3: 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).

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.

Date	Module	Professor	Notes
Monday, September 11th	Course Overview	All	
Monday, September 18th	Cryptography	Dario Fiore	
Monday, September 25th	Cryptography	Dario Fiore	
Monday, October 2nd	Cryptography	Ignacio Cascudo	
Monday, October 16th	Cryptography	Ignacio Cascudo	
Monday, October 23rd	Network Security	Srdjan Matic	
Monday, October 30th	Network Security	Srdjan Matic	
Monday, November 6th	Network Security	Juan Caballero	
Monday, November 13th	Software Security	Juan Caballero	
Monday, November 20th	Software Security	Alessandra Gorla	
Monday, November 27th	Software Security	Alessandra Gorla	
Monday, December 4th	Physical Security	Marco Guarnieri	
Monday, December 11th	Physical Security	Marco Guarnieri	
Monday, December 18th	Physical Security	Marco Guarnieri	
Wednesday, January 17th	Exam	All	Exam will take place at 18:00

Table 1: Course schedule.

Course Evaluation

The evaluation will be based on homeworks. There will be 4 homeworks, one for each module. Each homework will correspond to 25% of the grade. Each homework will be released after the module ends and students will submit the completed homework through email.

For students that do not achieve a passing grade through the homeworks, there will be a final exam on January 17th, 2024 at 18:00.