System security, hardware security and reverse

ECTS
4 crédits

Hourly volume
54h

Introducing

Objectives

At the end of this module, the student will have understood and be able to explain (main concepts):

- The main protection mechanisms that now exist in the kernel of operating system;
- The main attacks carried out from hardware component and associated contermeasures;
- The internals of the key hardware components for security such as hypervisor and IOMMU;
- The advantages of latest advances in hardware protection carried out by the founders of processors and chipset;
- The logic of physical attacks targeting computer systems;
- Reverse engineering software (reverse engineering) while being able to explain the toolchain of the compilation with the models used by compilers to generate machine code;
- Strategies to make reverse engineering software more difficult to achieve.

The student will be able to:

- Identify the most suitable software components to protect the operating system software against attacks;
- Identify threats from lower layers to higher layers and attack vectors to be considered in a system;
- Obtain an overview of the exchanges between the hardware components of a system to identify critical components and determine the contermeasures to integrate into the operating system;
- Identify threats on the physical components of a system;
- Conduct a reverse engineering of malware to understand their behavior and generate signatures to detect them.

Necessary prerequisites

Good programming skills in C and assembly language;

- A minimum of knowledge about the internals of the OS;
- Bases in algebra and the use of automata theory.

Practical info

Location(s)

Toulouse