INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

5th YEAR THEME SECURITY

Practical info

Location(s)

Toulouse

Security fundamentals

ECTS
5 crédits

Hourly volume
77h

Introducing

Objectives

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

- main concepts of operating systems, TCP/IP networks and language C and assembling programming;
- main concepts of dependability
- main concepts of cryptography

The student will be able to:

- describe the main components of an information system
- describe the main principles of the network protocols, analyse network traces and understand the flow encapsulation
- design and implement basic and advanced language C programs as well as basic assembling programs
- understand the different issues of the safety and security domains and correctly use the associated terminology
- distinguish the different cryptographic tools, understand when and how choose a specific tool, its capabilities and weaknesses
- find the main international cryptographic standards, and understand their content
- deploying high level security tools such as PKI, VPN, IPSEC tools or low-level security tools such as openssl, and choosing purposely the parametrisation of such tools

Practical info

Location(s)

Toulouse

Software security

ECTS
4 crédits

Hourly volume
47h

Introducing

Objectives

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

- The different types of software vulnerabilities that are frequently encountered, especially in programs written in C language;
- The main memories protections to protect software from these types of vulnerabilities;
- The theory related to worms and viruses, especially the algorithms used by these malware to infect computer systems and spread on the internet; the protection against these malicious software and the methods employed by antivirus to detect worms and viruses;
- Best practices for developing software securely.
- Formal methods for security

The student will be able to:

- Develop software taking into account the risks associated with software vulnerabilities;
- Use formal methods to detect software vulnerabilities;
- Appreciate the challenges of viral protection, describe the different types of computer infection, viral and analyze the technical and antiviral éagir in case of infection.

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

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

Networks and protocols security

ECTS
3 crédits

Hourly volume
40h

Introducing

Objectives

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

- the main concepts of network security, main threats targeting these networks and associated protection mechanisms
- the main concepts of non wired network security (Wifi, GSM, GPRS, LTE, UMTS)
- the main weaknesses of the network protocols and how to eliminate these weaknesses

The student will be able to:

- Understand and carry out basic networks attacks in the context of intrusion tests ; identify and imlement protection mechanisms mitigating these attacks, use and install protection infrastructures
- Choose a security solution dedicated to a Wifi access point; carry out intrusion tests on an access point
- Distinguish the security objectives in different cellular networks ; describe authentication mechanisms and key exchange protocols ; describe the different attacks targeting these different technologies ; identify the architectural components of security in operator networks
- Identify the weak protocols currently used in networks ; propose solutions for these weaknesses, through the use of tunnels when this is necessary ; use SSH and its associated functionnalities (file transfers ,proxies, etc) ; describe the good practices for the definition of a secure network protocol

Necessary prerequisites

Knowledges and skills in computer networks and the underlying protocols are required (TCP/IP, routing protocols). The corresponding terminology must be known and the main concepts of cryptography must be clearly understood.

Practical info

Location(s)

Toulouse

Architectures of secured networks

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 concepts associated to the design and the implementation of secure network architectures
- The main tools and technics allowing to implement protection measures, and their usage according to the different contexts and objectives
- The vulnerabilities inherent in system architectures and network and major intrusion techniques;
- The operation of the main vulnerabilities of the web.

The student will be able to:

- Identify the different classes of firewalls as well as their functionalities and weaknesses
- Define and audit a filtering architecture dedicated to a specific network
- Choose, for an IPSEC tunnel, the correct protocols, the correct execution modes and a routing plan adapted to the associated gatewaus
- Implement and audit such an IPSEC tunnel
- Deploy and audit a VPN based on IPSEC, either by configuring ¿by hand¿ the VPN or by using all-in-one preconfigured tools available
- Deploy and audit a network intrusion detection system (or intrusion prevention system)
- Design a complete security architecture for a complex network
- Identify the advantages and limitations of different intrusion detection solutions;
- Position the intrusion detection sensors efficiently;
- Analyze the events collected by the sensors and correlate these events to identify a real threat.
- Identify vulnerabilities in web architectures and propose solutions to achieve effective protection.

Necessary prerequisites

Good knowledge of web architectures, cryptography and networks.

Practical info

Location(s)

Toulouse

[FRANCAIS] Sécurité des systèmes embarqués critiques

ECTS
5 crédits

Hourly volume
31h

Introducing

Objectives

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

- The different techniques used today to secure ground / air communications with satellites;
- Issues related to different types of mission and standards used;
- The means for securing transmissions spread spectrum (TRANSSEC);
- The principles of the computer network for air traffic management (ATM) and related security issues;
- The principles and issues of security management in the context of the DGAC.

The student will be able to:
- Make relevant choice for securing ground / air communications architectures;
- Perform a black box analysis of a critical embedded system

Practical info

Location(s)

Toulouse

[FRANCAIS] SHSJ

ECTS
5 crédits

Hourly volume
42h

Practical info

Location(s)

Toulouse

[FRANCAIS] UE commune M2 RT

ECTS
9 crédits

Hourly volume
45h

Practical info

Location(s)

Toulouse