Internet and Security

ECTS
5 crédits

Hourly volume

Introducing

Objectives

At the end of this module, the student will have understood and be able to explain (main concepts):
- Network interconnection part:
o the basic concepts and techniques allowing interconnecting local area networks in the Internet: repeater, bridge, router
o the basic concepts and techniques allowing interconnecting LAN in the Internet : subnetting, CIDR, VLAN, VPN, applicative proxy, NAT
o the main protocols of the TCP/IP Internet architecture : UDP, TCP, IP, ARP/proxy ARP, ICMP, DHCP (Note : RIP, OSPF and BGP are briefly introduced).

- Distributed algorithm part:
o principal characteristics of the distributed systems (asynchronism, distribution of control and the data, absence of common knowledge, dynamicity,¿),
o their specific problems and the difficulty of their solution in a distributed context (mutual exclusion, management of the shared data, distributed choice, diffusion, detection of the termination,¿),
o some generic algorithmic tools allowing to solve them: causality, distributed recursivity (waves) and distributed iteration (phases), specific topological structures.

- Security part:
o principles of computer security through the properties that characterize it as well as the classification of the major threats and the corresponding countermeasures,
o main vulnerabilities of computer networks, in particular the Internet network as well as the corresponding countermeasures,
o main software vulnerabilities as well as some countermeasures.

The student will be able to:
- Network Interconnection part:
o do architecture choices allowing to take into account requirements and constraints associated to a LAN interconnection,
o do basic or complex addressing and routing schemas,
o set up (administrate) Ethernet and IP networks in the basic and advanced interconnection contexts considered in the course.

- Distributed algorithm part:
o solve generic problems involved in the implementation of systems distributed
o handle the most general tools allowing to conceptualize them.

- Security part:
o analyse a computer network and its software in order to identify the main vulnerabilities, from software and network point of view and to propose corresponding countermeasures to improve the security of the whole system.

Necessary prerequisites

Course Introduction to computer networks (3MIC)

Cours de programmation distribuée dans les réseaux (socket API) (3MIC)

Practical info

Location(s)

Toulouse