UE Information Security

Level
Baccalaureate +5

ECTS
6 credits

European Credit Transfer and Accumulation System (ECTS) Exchange credits
6.0

Component
UFR IM2AG (informatique, mathématiques et mathématiques appliquées)

Semester
Automne

- **Teaching language(s):** English
- **Open to exchange students:** Yes
- **European Credit Transfer and Accumulation System (ECTS) Exchange credits:** 6.0
- **Code d'export Apogée:** GBX9MO80

Presentation

Description

This lecture deals with Information Systems Security and provides several facets, ranging from modeling to deployment in real applications. Information Systems Security refers to the processes and methodologies involved to keep information confidential, available, and assure its integrity. The lecture is divided in two major parts and assisted with several practical labs, allowing the students to model and configure security policies and also to be aware about several kinds of attacks and breaches.

Course content

Part 1: Access Control, or how to prevent unauthorized people from entering or accessing a system?

This part deals with:

- Cryptology for authentication and trust;
  - security needs : confidentiality, availability, integrity, non-repudiation (CAI/DICP);
  - cryptology primitives : private and public key ; trusted infrastructure (PKI and ledgers).
  - zero-knowledge protocols; secret sharing and multiparty computation / or Practical work with Open SSL
- Access control mechanisms (MAC, DAC, RBAC, ABAC) and their implementations
- The detection and remediation of security breaches such as intrusions and insider attacks

- The deployment of control filters in applications and proxies.

The presented approach is built on the model-driven security paradigm (MDS). It refers to the process of modeling security requirements at a high level of abstraction, and generating technical security implementations. Security models are transformed into enforceable security rules including the run-time security management (e.g. entitlements/authorisations). Three labs are planned:

- B4MSecure: we will apply a formal language with animation and model-checking facilities to identify security breaches in Access Control policies.
- Snort: in this practical session you will set a local environment to simulate two machines, the target machine and the attacker. You will learn how to create firewall rules, monitor your network and how to react when an attack is detected.
- Metasploit: you will discover technology intelligence for vulnerabilities through a practical session where you will reproduce an exploit to hack and take control over a web-based server.

Part 2: Overview of modern attacks on systems, protocols, and networks and countermeasures

This part is devoted to modern attacks carried out on the Internet scale, in particular attacks on the DNS system (Domain Name System), such as cache or zone poisoning attacks, reflection and amplification of DDoS attacks (Distributed Denial of Service), IP spoofing - the root cause of DDoS attacks, botnets (e.g., Mirai), domain generation algorithms used for command-and-control communications, modern malware (e.g., Emotet trojan, Avalanche), spam, phishing, and business email compromise (BEC) scams.

The module will discuss preventative measures and security protocols to fight modern attacks, such as DDoS protection services, IP source address validation (SAV) known as BCP 38, Sender Policy Framework, and DMARC protocols as the first line of defense against email spoofing and BEC fraud, and DNSSEC to prevent DNS manipulation attacks. It will also discuss large-scale vulnerability measurements (a case study of the zone poisoning attack) and the challenges of deploying current security technologies by the system and network operators.

This part will be concluded with a practical team assignment in which students will be divided into groups and will have to configure a secure system in a real-world environment. The goal is to secure their system against the various types of discussed attacks and exploit other groups' systems.

Course parts

Lectures	Lectures (CM)	36h

Recommended prerequisites

Java, Web applications, Databases

Useful info

Contacts

Program director

Akram Idani

Akram.Idani@grenoble-inp.fr

Campus

Grenoble - University campus