II.2317 / II.2417 – Cybersecurity

General information

Title: Cyber Security
Module identifier: II.2317 / II.2417
Module Leader: Nour EL MADHOUN
ECTS: 5
Average amount of work per student: from 100 to 150 hours, including 42 hours supervised
Teamwork: yes
Keywords :

Presentation

Following the increase in cybercrime, causing considerable economic losses and threatening the reputation or even the survival of companies, securing one's information system and data has become a priority and a strategic issue for all types of companies. The notion of cybersecurity is now part of the fundamental knowledge to be acquired by all engineering profiles. It is a cross-cutting concept involving both hardware and software elements. Securing a system requires above all a methodology and a global understanding of the use cases of the system to be secured, whether at the level of the network, information system, data access or development of applications, especially web applications.

This module introduces the fundamentals of security at the architecture, network, hardware (with a focus on reliability), and with a particular focus on application security.

Educational objectives

The courses given in this module allow students to acquire the following skills:

- Best practices for programming web applications (SQL injection, XSS)
- Management of identifications, authentications
- Access rights management
- Encryption in cryptography

Prerequisite

Prerequisites: Basic notions in networks, and web development.

Content/Program

The lessons taught in this module develop the following concepts:

- Information Systems Security
- Web Application Security
- Network Security (Introduction)
- Introduction to Cryptography
- Reliability, performance and redundancy of equipment and service
- Legal aspects and regulations

Pedagogical methods

Learning methods

Most of the module takes place in a series of lectures/lectures by an expert in the field, interrupted by the restitution of the students' research work on security topics. The module concludes with a practical application around penetration testing.

Evaluation methods

The evaluation of this module is based on:

- Documentary research work on 2 imposed subjects, in teams of 2 or 3, with a written report and presentation of the work to the rest of the class (40 to 60% of the module average),
- An individual assessment in the form of a knowledge test partly MCQ and partly open-ended questions (60 to 40% of the module average).

Language of work

- The materials are in English. The course is also given in English.
- Written presentations and reports may be made in English or French.
- The knowledge test is in English.

Bibliography, Webography, Other sources

- ANSI: https://www.ssi.gouv.fr/
- Course material on Moodle: https://educ.isep.fr/moodle/course/view.php?id=388