Summary
This is an introductory course to computer security and privacy. Its goal is to provide students with means to reason about security and privacy problems, and provide them with tools to confront them.

Content
• History of security and security models; from high confidentiality to high integrity
• Access control: Linux and Android as examples
• Authentication mechanisms: biometrics, tokens, passwords
• Applied cryptography: basic notions and algorithms
• Commonly used security protocols (SSL/TLS, HTTPS, PGP,...)
• Privacy, censorship and surveillance
• Regulatory aspects and standards

Learning Prerequisites
Important concepts to start the course
Basic notions of TCP/IP, basic notions of programms

Learning Outcomes
By the end of the course, the student must be able to:
• Recognize security properties of systems, as well as formulate security policies, and model the threats they may face.

Teaching methods
Lectures with real world examples, and complementary exercises to reinforce basic concepts.

Expected student activities
Attending lectures, solving exercises, reading and demonstrating understanding of provided materials.

Supervision
Office hours: Yes
Assistants: Yes
Forum: No
Prerequisite for

- COM-402 Information security and privacy
- CS-523 Advanced topics on privacy enhancing technologies