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
The goal of this course is to introduce students to security engineering. The course will help students to think as an adversary so that they can analyse systems and establish security policies. We will cover a number of common security mechanisms at all layers, and learn their properties and limitations.

Core topics:
• Security design principles
• Access control
• Authentication mechanisms
• Applied cryptography
• Software and Network security
• Privacy

Keywords
Security Privacy

Learning Prerequisites

Recommended courses
CS-233a or CS-233b Introduction to Machine Learning (for programming)
COM-208 Computer Networks
CS-323 Introduction to operating systems

Important concepts to start the course
Basic notions TCP/IP
Basic notions programming

Learning Outcomes
By the end of the course, the student must be able to:
• Analyze systems for security
• Decide on security mechanisms to apply
• Establish a security policy

Teaching methods
Pre-recorded lectures
Practical assignments interactively resolved in class using the concepts learned in the lectures
Written exercises to reaffirm the learning of the course
Practical programming homeworks to develop attacks and defenses

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

Assessment methods
• Take home exams (80%)
• Practical homeworks (20%)

Supervision
Office hours Yes
Assistants Yes
Forum Yes

Resources
Bibliography
Computer security by Dieter Gollmann
Security Engineering by Ross Anderson
Computer Security: Principles and Practice by Stallings and Brown

Ressources en bibliothèque
• Security Engineering / Anderson
• Computer Security / Stallings & Brown
• Computer security / Gollmann

Moodle Link
• https://go.epfl.ch/COM-301