

COM-301

Computer security and privacy

Bourgeat Thomas, Stadler Theresa

| Cursus | Sem. | Type |
|-----------------------------|------|------|
| Communication systems minor | H | Opt. |
| Communication systems | BA5 | Obl. |
| Computer science minor | H | Opt. |
| Computer science | BA5 | Obl. |
| Cyber security minor | H | Opt. |
| HES - IC | H | Opt. |

| | |
|----------------------------|-----------------|
| Language of teaching | English |
| Credits | 6 |
| Session | Winter |
| Semester | Fall |
| Exam | Written |
| Workload | 180h |
| Weeks | 14 |
| Hours | 5 weekly |
| Courses | 3 weekly |
| Exercises | 1 weekly |
| Lab | 1 weekly |
| Number of positions | |

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

Learning Prerequisites**Recommended courses**

CS-233 Introduction to Machine Learning (for programming)
CS-202 Computer 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

Max (60% * final + 30% midterm + 10% assignments, 90%*final + 10% assignments)

Resources

Bibliography

Computer security by Dieter Gollmann

Security Engineering by Ross Anderson

Computer Security: Principles and Practice by Stalling and Brown

Ressources en bibliothèque

- [Find the references at the Library](#)

Moodle Link

- <https://go.epfl.ch/COM-301>