

COM-506

**Student seminar: security protocols and applications**

Vaudenay Serge

Cursus	Sem.	Type
Computer science	MA2, MA4	Opt.
Cyber security minor	E	Opt.
Cybersecurity	MA2, MA4	Opt.
Data Science	MA2, MA4	Opt.
SC master EPFL	MA2, MA4	Opt.

Language of teaching	English
Credits	3
Session	Summer
Semester	Spring
Exam	During the semester
Workload	90h
Weeks	14
<b>Hours</b>	<b>2 weekly</b>
Courses	2 weekly
<b>Number of positions</b>	

**Summary**

This seminar introduces the participants to the current trends, problems, and methods in the area of communication security.

**Content**

We will look at today's most popular security protocols and new kinds of protocols, techniques, and problems that will play an emerging role in the future. Also, the seminar will cover methods to model and analyze such security protocols. This course will be held as a seminar, in which the students actively participate. The talks will be assigned in the first meeting to teams of students, and each team will have to give a 45 minutes talk, react to other students' questions, and write a 3-4 pages summary of their talk.

**Keywords**

network security, security protocols, cryptography

**Learning Prerequisites****Required courses**

- Computer security (COM-301)
- Cryptography and security (COM-401)

**Learning Outcomes**

By the end of the course, the student must be able to:

- Synthesize some existing work on a security protocol
- Analyze a security protocol
- Present a lecture

**Transversal skills**

- Make an oral presentation.
- Summarize an article or a technical report.

**Expected student activities**

- prepare a lecture (presentation and a 4-page report)
- present the lecture
- attend to others' lectures and grade them

### Assessment methods

- lecture and attendance to others' lectures

### Supervision

Office hours	No
Assistants	Yes
Forum	Yes
Others	Lecturers and assistants are available upon appointment.

### Resources

#### Websites

- <https://lasec.epfl.ch/teaching.php>

#### Moodle Link

- <https://go.epfl.ch/COM-506>

#### Videos

- <https://mediaspace.epfl.ch/channel/COM-506+Student+Seminar+on+Security+Protocols+and+Applications>