Student seminar: security protocols and applications
Oechslin Philippe, Vaudenay Serge

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
• Network 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
• do the final exam

Assessment methods
• lecture and attendance to others' lectures (50%)
• final exam (50%)

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

Resources
Websites
• http://lasec.epfl.ch/teaching.shtml