

# CS 432 - Computer and Network Security

Spring 2023

This is a 3-credit course that focuses on security applications and cryptographic protocols. An overview of cryptography will be given in the first couple of weeks.

**Prerequisite:** Students are expected to come with undergrad level computer networks and operating systems background. Moreover, computer-programming expertise is necessary. More specifically, CS408 or EE414 is a prerequisite. However, if you have not taken one of these courses but have a background on Computer Networks, feel free to inquiry with the instructor for any possible prerequisite override

**Instructor:** Albert Levi  
FENS 1091, x9563, levi at sabanciuniv.edu

**Assistants:** Emre Ekmekçiöğlü (eekmekcioglu at sabanciuniv.edu), Simge Demir (simgedemir at sabanciuniv.edu), Burcu Tanış (burcutanis at sabanciuniv.edu). Office hours are to be determined. Follow SUCourse for details.

**Schedule:** Lecture: W 16:40 – 17:30 (FENS L045), F 12:40 – 14:30 (I will be streaming from FENS L045).

Zoom link: <https://sabanciuniv.zoom.us/j/97639601149>

Labs: F 16:40 – 18:30. We will start online at least until early April. After that, in accordance with the announcements done by the university administration, the mode of delivery might change. Links and other details of the labs will be posted later. We will not use this hour all the time; you will be informed when there is lab through lab website/SUCourse.

**Text book:** Cryptography and Network Security, 8<sup>th</sup> or 7<sup>th</sup> edition (5<sup>th</sup> or 6<sup>th</sup> also OK), William Stallings

**References:** Computer Security, Dieter Gollmann  
Computer Security: Principles and Practice, William Stallings and Lawrie Brown

## Tentative Outline

- Introduction (1 week)
- Overview of Cryptography (2-3 weeks)
  - Symmetric and Asymmetric Cryptography
  - Key agreement
  - Hash functions
- Authentication and Key Distribution Protocols (1-2 weeks)
- Kerberos and Password Management (1 week)
- TCP/IP Security and IPSec (2 weeks)
- WWW Security, SSL and TLS (1 week)
- E-mail Security (PGP, S/MIME, Domainkeys) (2 weeks)
- PKI and certificate systems, (1 week)
- Access Control (1 week)
- Firewalls and Intrusion Detection Systems (1-2 weeks)

## Student responsibilities and loads (absolutely tentative and might change depending on the announcements made by the administration after early April)

- One midterm and one final exam. See below for details.
- There will be 5 (+/- 1) labs, some may last more than one week. The labs will be dedicated to some practical aspects of the course including programming. Labs will be graded either as in-lab performance or as a separate homework or as after-lab performance. Aside the lab homework assignments, there will be 1-2 lecture related homework assignments. Some homework assignments may require programming. This year we will organize Capture the Flag (CtF) contest as part of homework.
- The labs WILL NOT be direct application of the lectures, but they will be related to each other. We DO NOT aim to use labs as recitations to help the students to get higher marks in the exams.**
- A programming project on a secure networking application. This project will be done in 2 or 3 stages. The project groups will be at most 3 people.

- There will be a couple of Top Hat quizzes every week (will start in week 3), some of the grade will come from attendance and some from correctness. Overall TH grade will be multiplied by 1.25 and normalized to 100. Maximum TH grade that a student can get will not exceed 100. This 25% extra is to cover missing THs due to Internet connection or another reason; we will not provide any make-ups for THs.

### Exam Details and Make-up Policy

There will be one midterm and one final exam. We plan to have **all exams face-to-face**. However, we are waiting for official announcements for these.

No make-up exam will be performed for the midterm exam! If you miss it with a valid reason, I can arrange compensation that might include the options of oral exam, using final exam instead, some extra questions in the final, or any combination of it. If you miss the final exam with a valid reason that I accept as well, compensation mechanism will be determined later.

### Online Lectures and Zoom Etiquette

- Please keep your microphone muted unless you are talking to me or asking a question.
- It is up to you to turn your camera on.
- If you have a question, please speak up and ask. I do not guarantee reading the chat box during the lecture.
- Lectures and labs will not be recorded and videos will NOT be shared. **YOU ARE NOT ALLOWED TO RECORD LECTURES AND LABS EVEN FOR PERSONAL USE.**

### Use of SUCourse+ and Communications

We will make announcements via SUCourse+ that you will also receive as emails. Some announcements may be sent as plain email or the quick ones via WhatsApp group.

We have a WhatsApp group for the class that I also participate (of course you might have another one without me). The invite link for it is <https://chat.whatsapp.com/LofWlQtTjlu8VIfupdA8aa>

All lecture materials, homework and assignments will be posted at SUCourse+. The submissions will also be there unless otherwise stated.

Lecture materials will be posted as powerpoint file without annotations made in class. Each powerpoint file will be shared after it is entirely covered in class.

### Tentative Grading and Timing (subject to change after April)

Midterm Exam	25%	plan is to have on week 9 (April 28, Friday, lecture hour) but finalized after the mode of exam will be cleared (not before early April)
Final Exam	35%	as scheduled by ÖK/SR
Homework, Lab, Project, CtF	35%	deadlines will be determined separately
Top Hat (Quizzes and Attendance)	5%	please see above about how I will use this

## **Plagiarism, Homework Trading, Illegal Local and Remote Help and Cheating will not be tolerated.**

**We may have to revise the course plan according to the countrywide reassessment to be made regarding higher education. This is expected to happen at the beginning of April. The content to be delivered is certain but the method of course delivery, the number and dates of exams, grading scheme and some other details are subject to change.**