CS 432/532 - Computer and Network Security

Spring 2022

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.

This is a code-shared course with both graduate (CS532) and undergraduate (CS432) codes. However, the topics are undergraduate topics and the exams/homework assignments will be designed with the assumption of being an undergraduate course. Graduate students (CS532 takers) will have relatively more load as compared to undergraduate students (CS432 takers). Project grouping rules will be different. Graduate students will have an extra (but small) takehome exam. Midterm and final exams, and homework assignments will mostly be common (see the explanations below), but the letter grades will be determined separately.

Catalogue Data: Overview of Cryptography, Identification and Authentication, Access Control, Operating System Security, Key Distribution, TCP/IP Security, IPSec, DNSSEC, WWW Security, SSL and TLS, E-mail Security (PGP, S/MIME), PKI and certificate systems, Viruses, Firewalls, Intrusion Detection, E-commerce Security

Prerequisite: Students are expected to come with undergrad level computer networks and operating systems background. Moreover, computer-programming expertise is necessary. For CS532, there is no formal prerequisite since it is a graduate course. For CS432, 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: Sacit Emre Akça (sacitakca at sabanciuniv.edu), Simge Demir (simgedemir at sabanciuniv.edu), Barış Pakyürek (bpakyurek at sabanciuniv.edu). Office hours are to be determined. Follow SUCourse for details.

Schedule: Lecture: M 15:40 – 16:30 (FMAN 1099), Th 8:40 – 10:30 (FENS G077).
Zoom link: https://sabanciuniv.zoom.us/j/92217316690?pwd=Qk9pcFgvL2YydWpJUVoveDBGWE1Vdz09

Labs: W 17:40 – 19:30. Some of them will be online, some of them will be hybrid. Please do not take the classrooms specified in the schedule for your sections into account. Both sections will meet together in the link and/or classroom specified for each lab separately in the lab website/SUCourse. 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, 7th edition (5th or 6th editions OK), William Stallings
Homer link: https://www.homerbooks.com/urun/cryptography-and-network-security-1

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 (tentative)

Common responsibilities and loads (for both CS432 and CS532 students)

- 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. **Note:** CS532 students will be exempt of CtF (Capture the Flag) part of the course (CS432 students will take this part). However, if a CS532 student wants to take part in CtF, he/she may do so pending consent of instructor.
- 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. CS432 students will be able to work in groups of 3-5 people (not less, not more). However, CS532 students should make the project alone. However, CS532 students have an option to propose their own project instead of doing the common one (proposals, if any, are due before the deadline of the first stage of the common project).

Additional responsibilities and loads for only CS532 students

- **Takehome exam:** A small takehome exam will be given towards the end of the course. You may consider this takehome exam as a challenging homework as well.

Exam Details and Make-up Policy

There will be one midterm and one final exam. In line with the order of the university administration and higher education council, **all exams will be performed face-to-face**.

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.

Hybrid System for the Lectures, Attendance and Physical Attendance Encouragement

Hybrid means I will lecture in the auditorium with camera and microphone and the lecture will be streamed through zoom. You may prefer to attend physically or online. Since the auditoriums' reduced capacities are sufficient to cover the entire class, we will not apply rotation. Please wear your masks all the time in class and respect the physical distance. The seats that you are not allowed to seat are clearly marked with a cross.

Lecture videos will be shared through SUCourse+. The videos will not be removed until the end of the semester. Labs will not be recorded and shared.

Hybrid lectures are different than the online ones that you attended during remote education. The main difference is that my focus during the lecture cannot be the camera; I have to address to people in class. Moreover, the camera is not going to be the laptop camera that used to show my face, but the auditorium's camera that shows me from a distance. There could be some voice issues as well. Thus the online participants may experience some concentration issues during lectures and I strongly encourage physical participation.

We also have a grading related policy to encourage physical attendance to the lectures. 5% of the overall grade is reserved for this purpose. This is 100 for everyone at the beginning of the semester and provided that overall physical attendance will not drop below a certain threshold, I will give 100 to everyone at the end of semester. However, if physical attendance drops consistently below 37 people (calculated as 70% min. YÖK attendance rule * 60% YÖK's min physical lectures rule over 90 enrollments), the deal of 100 for everyone will be cancelled and I will switch to another method for this 5%, of which the details are currently unknown. Definitely, this method will be to encourage physical attendance.

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/IUyhdMIG0ofB2qXXUMVJmI

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

Midterm Exam	25%	week 9 - Lab Hour, Wednesday April 27, 2022, 17:40 – 19:30.
Final Exam	35%	as scheduled by ÖK/SR
Homework, Lab, Project, CtF/Takehome	35%	deadlines will be determined separately
Physical Attendance Encouragement	5%	please see above about how I will use this

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