CS 432/532 - Computer and Network Security

Spring 2021

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: Halit Alptekin (halitalptekin at sabanciuniv.edu, volunteer TA for CtF), M. Yuşa Ergüven (merguven at sabanciuniv.edu), F. Kerem Örs (fkerem at sabanciuniv.edu). Office hours are to be determined. Follow SUCourse for details.
Schedule: Lecture: T 16:40 – 17:30, W 8:40 – 10:30.
Zoom link: https://sabanciuniv.zoom.us/j/94205336921?pwd=T01wWXpISVZoRTJWdDRsM0YxcnovUT09
Lab/Recitation: Section A2: M 14:40 – 16:30, Section A1: F 10:40 – 12:30. 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 recitation/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)

Make-up Policy: No make-up! If you miss something, you miss it whatever the reason is! If the reason is really valid, you may take an oral examination instead of a written make-up.

See next page

Student responsibilities and loads (tentative)

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

- One midterm and one final exam. Both are online; details will be made clear later. At this point, we can say that the online exams can be re-evaluated via an extra oral exam depending on the issues raised during the online one and the exam grade can be changed after the oral exam.
- There will be 5 (+/- 1) labs. 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 4-5 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.

Tentative Grading and Timing

Midterm Exam	25%	week 9 - Tuesday April 20, 2021, 18:40 – 20:45.
Final Exam	35%	as scheduled by ÖK/SR
Homework, Lab, Project, CtF/Takehome	30%	deadlines will be determined separately
Top Hat	10%	top hat is daily small quizzes; half grade comes from attendance, half from correctness. Overall top hat grade will be multiplied by 1.25 and maximum of 100 and calculated grade will be taken as your final top hat grade. This is to cover any attendance issues; no other make-ups will be given.

PLAGIARISM WILL NOT BE TOLERATED