

## CS 432/532 - Computer and Network Security

Spring 2008

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 share course with both graduate and undergraduate codes. Graduate students will have more loads as compared to undergraduate students. Projects of graduate and undergraduate students will be different. Graduate students will make a presentation and will have an extra (but small) takehome exam. The exams and homework assignments will mostly be common, 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 TE404 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:** İsmail Fatih Yıldırım, Ömer Zekvan Yılmaz

**Schedule:** Lecture: M 13:40 – 15:30 and T 10:40 – 11:30, FENS G035  
Lab/Recitation: F 15:40 – 17:30, FENS G035

**Text book:** Cryptography and Network Security, 4<sup>th</sup> edition, William Stallings

**Reference:** 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 week)
- ❑ 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) (2 weeks)
- ❑ PKI and certificate systems, (1 week)
- ❑ Access Control (1 week)
- ❑ Firewalls and Intrusion Detection Systems (1-2 week)

**Make-up Policy:** No make-up! If you miss something, you miss it whatever the reason is!

### Student responsibilities and loads (tentative)

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

- ❑ One in-class midterm and one in-class final exam.
- ❑ There will be 3-4 labs. The labs will be dedicated to some practical aspects of the course. Labs will be graded either as a lab performance or as a separate homework. Aside the lab homeworks, there will 1-2 lecture related homework assignments. Some homework assignments may require programming.

#### Additional responsibilities and loads for only CS432 students

- ❑ A programming project on a secure networking application. This project will be done in groups.

#### Additional responsibilities and loads for only CS532 students

- ❑ **Research projects:** Students are expected to make research on a specific area and give a 20 minutes presentation.
- ❑ **Development projects:** Development projects are (i) either big programming projects on secure networking applications (ii) or research-driven projects on a particular area about computer and network security. Depending on the scope, development projects may be done in groups.
- ❑ **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 for CS432

Midterm Exam	25-30%
Final Exam	35-40%
Homeworks and Development Project	30-40%

#### Tentative Grading for CS532

Midterm Exam	20-25%
Final Exam	25-30%
Takehome Exam	10%
Research project and presentation	5-10%
Homeworks and Development Project	30-40%

#### Timing (tentative)

Development project proposal (CS532)	April 7, 2008	week 8
Research project proposal(CS532)	April 21, 2008	week 9
Midterm Exam (CS432 and CS532)	April 28, 2008 (class hour)	week 10
Research proj. presentations (CS532)	week of May 19, 2008 (recitation and if needed extra hours)	
Dev. proj. progress report&demo (CS532)	May 16, 2008	week 12
Take-home exam (CS532)	sometime around 13 <sup>th</sup> -14 <sup>th</sup> week (exact dates TBD)	
Development proj. demo and report (CS532)	June 13, 2008	end of finals
Final Exam (CS432 and CS532)	as scheduled by ÖK	

Class Website: [http://people.sabanciuniv.edu/levi/cs432\\_532](http://people.sabanciuniv.edu/levi/cs432_532)

**PLAGIARISM WILL NOT BE TOLERATED**