San José State University
College of Engineering/Computer Engineering Department
CMPE/EE 209, Network Security, Spring 2019

Course and Contact Information

Instructor: Gokay Saldamli

Office Location: ENG 185

Telephone: 408 924 4150

Email: gokay.saldamli@sjsu.edu

Office Hours: Tue 5:00-6:00

Class Days/Time: Tue 6:00-8:45

Classroom: ENGR-325

Prerequisites: CMPE 206 or EE 281

Faculty Web Page and MYSJSU Messaging

Course materials such as syllabus, handouts, notes, assignment instructions, etc. can be found on Canvas Leaning Management System course login website at http://sjsu.instructure.com. You are responsible for regularly checking with the messaging system through MySJSU at http://my.sjsu.edu (or other communication system as indicated by the instructor) to learn of any updates.

Course Description

The course examines basic cryptography and network security protocols and technology. We cover the basics of cryptography, including conventional and public-key cryptography, authentication, and digital signatures. We further go through the important network security tools and applications such as IP Security, Kerberos, SSL/TLS, and HTTPS. Moreover, methods for countering hackers and viruses are also explored.

Course Learning Outcomes (CLO)

CMPE 209 is an introductory level graduate class to network security. The course emphasizes the important cryptographic methods and network security protocols that are used in practice.

Upon successful completion of this course, students will be able to:

1. Understand Symmetric Cipher Model
2. Understand Block Cipher Design Principles and AES
3. Understand Public Key Cryptosystems RSA and ECC Algorithms
4. Understand SHA family of Hashes and MACs
5. Understand Key Management and Distribution

6. Understand User Authentication Protocols
7. Be able to apply SSL, TLS, HTTPS and SSH
8. Understand Wireless Network Security.

Required Texts/Readings

Textbook

[S17] William Stallings , Cryptography and Network Security: Principles and Practice, 7th Edition

Other Readings

https://engineering.purdue.edu/kak/compsec/Lectures.html
http://www.cis.syr.edu/~wedu/Teaching/CompSec/lecturenotes.html

[BS15] Dan Boneh and Victor Shoup, A Graduate Course in Applied Cryptography, draft, Agust, 2015. https://crypto.stanford.edu/~dabo/cryptobook/draft_0_2.pdf

[FSK10] Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno, Cryptography Engineering, Design Principles and Practical Applications, John Wiley & Sons, 2010.

Course Requirements and Assignments

The class assignments that are assessed and that contribute to your final grade include quizzes, homework, midterm exam and one final exam. Major exams in this class may be video recorded to ensure academic integrity. The recordings will only be viewed if there is an issue to be addressed. Under no circumstances will the recordings be publicly released.

NOTE that University policy F69-24 at http://www.sjsu.edu/senate/docs/F69-24.pdf states that "Students should attend all meetings of their classes, not only because they are responsible for material discussed therein, but because active participation is frequently essential to insure maximum benefit for all members of the class. Attendance per se shall not be used as a criterion for grading."

Students cannot take this class without fulfilling its prerequisite or obtaining instructor approval. Please note that, according to department policy, "*students who do not provide documentation of having satisfied the class prerequisite and co-requisite requirements (if any) by the second class meeting will be dropped from the class.*"

"*Success in this course is based on the expectation that students will spend, for each unit of credit, a minimum of 45 hours over the length of the course (normally three hours per unit per week) for instruction, preparation/studying, or course related activities, including but not limited to internships, labs, and clinical practice. Other course structures will have equivalent workload expectations as described in the syllabus.*"

Final Examination or Evaluation

This course has a comprehensive final examination at a firm schedule.

Grading Information

The final grade will be calculated based on the following table:

Grade	*Points*
A plus	890 to 1000
A	860 to 889
A minus	830 to 859
B plus	800 to 829
B	770 to 799
B minus	740 to 769
C plus	710 to 739
C	680 to 709
C minus	650 to 679
D plus	620 to 649
D	590 to 619
D minus	560 to 589
F	0 to 559

Late assignments

Assignments submitted after the deadline earns no credit. However, many exam questions are derived from assignments. It is never too late to do the assignments.

Determination of Grades

The percentage weight assigned to class assignments is listed below. Detailed grading rubrics for homework assignment and team projects, and exact due dates for each assignment will be posted on Canvas.

Quizzes	12%
Homework assignments	10%
Midterm Exam	24%
Project	20%
Final exam	34%
Bonus grade (in-class and group discussions)	4%

Classroom Protocol

Students are expected to arrive in time for class. Laptop/tablet/smart phone use is allowed only for activities related to the class.

University Policies

Per University Policy S16-9, university-wide policy information relevant to all courses, such as academic integrity, accommodations, etc. will be available on Office of Graduate and Undergraduate Programs' Syllabus Information web page at http://www.sjsu.edu/gup/syllabusinfo/".

CMPE/EE 209, Network Security,
Spring 2019 Course Schedule

The schedule (and related dates/readings/assignments) is tentative and subject to change with fair notice. In case of guest lectures, the syllabus will be updated accordingly. Any changes will be announced in due time in class and on the course's web site (Canvas). The students are obliged to consult the most updated and detailed version of the reading material and syllabus, which will be posted on Canvas.

Course Schedule

WK	Tue	Topic	Chapter
2	1/29	Basic of Network security and review of classical encryption techniques	1, 3
3	2/5	Block ciphers and AES	3
4	2/12	Public Key Encryption	6
5	2/19	RSA and ECC	9
6	2/26	Hash Functions and MACs	10
7	3/5	Digital Signatures	11,12
8	3/12	Key Distribution, PKI, Kerberos	13
9	3/19	Midterm 1	
10	3/26	User Authentication	
11	4/2	Spring Recess	14
12	4/9	TLS, SSL and SSH	15
13	4/16	Attacks on TLS	17
14	4/23	WiFi and IP Security	17
15	4/30	Intrusion Detection and Firewalls	18, 20
16	5/7	Project Presentations	22, 23
	Final Exam	Tuesday, May 21, 17:15-19:30	