San José State University
School of Science/Computer Science
CS 166, Information Security, Section 3, Fall, 2017

Course and Contact Information

Instructor:	Tom Austin
Office Location:	MH 216
Telephone:	408-924-7227
Email:	thomas.austin@sjsu.edu
Office Hours:	Monday/Thursday noon-1 pm
Class Days/Time:	Monday/Wednesday 1:30-2:45 pm
Classroom:	MH 223
Prerequisites:	CS 146 & (CS 47 or CMPE 102 or CMPE 120), "C-" or better.

Course Format

Courese Web Page

Course materials such as syllabus, handouts, notes, assignment instructions, etc. can be found on my faculty web page at https://www.cs.sjsu.edu/~austin/cs166-spring17/ or on Canvas Leaning Management System course login website at http://sjsu.instructure.com. You are responsible for regularly checking with the messaging system through Canvas to learn of any updates.

Course Description

Fundamental security topics including cryptography, protocols, passwords, access control, software security, and network security. Additional topics selected from multilevel security, biometrics, tamper-resistant hardware, information warfare, e-commerce, system evaluation and assurance, and intrusion detection. Prerequisite: CS 146 (with a grade of "C-" or better) and either CS 47 or CMPE 102 or CMPE 120 (with a grade of "C-" or better). **Due to ABET accreditation, I need to see proof of your prerequisites or I must drop you from the course.**

Course Learning Outcomes (CLO) (Required)

Upon successful completion of this course, students will be able to understand the major technical security challenges in each of the following four areas: cryptography, access control, protocols, and software. More specific outcomes are listed here:

- Given an iteration of the Fiat-Shamir zero knowledge protocol, find Alice's secret S, and verify that v = S2 mod N (assessed with an exam question)

- Suppose that Alice's RSA public key is (N,e). Determine Alice's private key d. (assessed with an exam question)

Required Texts/Readings

Textbook

Information Security: Principles and Practice, 2nd edition, Mark Stamp,
(Wiley, May 2011, ISBN-10: 0470626399, ISBN-13: 978-0470626399).

Other Readings

Other readings will be listed on the class schedule.

Course Requirements and Assignments

Final grades will be determined by a weighted average of the following:

1. 30%: Homework
2. 20%: Test 1
3. 20%: Test 2
4. 20%: Final exam (http://info.sjsu.edu/static/catalog/final-exam-schedule-spring.html):
5. 10%: Participation (lab assignments)

Extra credit assignments may be offered sporadically throughout the semester.

Grading Information

Nominal grading scale:

Percentage	Grade
92 and above	A
90 - 91	A-
88 - 89	B+
82 - 87	B
80 - 81	B-
78 - 79	C+
72 - 77	C
70 - 71	C-
68 - 69	D+
62 - 67	D
60 - 61	D-
59 and below	F

Classroom Protocol

Attendance is strongly recommended, but not mandatory. Should you show up late to class, quietly sit down, and do not expect me to go over material that you missed just for your benefit.

You will be expected to bring your laptop to class in order to work on the labs. You may work with a partner for labs, but NOT for homework assignments unless otherwise indicated.

Cell phone use is prohibited.

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/.

CS 166 / Information Security, Spring 2017, Course Schedule

Please note that the schedule is subject to change with fair notice, which will be posted through Canvas at https://sjsu.instructure.com.

Course Schedule

Week	Date	Topics and Readings
1	8/23	Introduction – chapter 1
2	8/28	Classic crypto – chapter 2
2	8/30	Stream ciphers / block ciphers – chapter 3
3	9/4	**LABOR DAY – NO CLASS**
3	9/6	More block ciphers
4	9/11	Public key crypto – chapter 4 **(GUEST LECTURE)**
4	9/13	More public key crypto
5	9/18	Hash functions – chapter 5
5	9/20	More hash functions
6	9/25	Password cracking
6	9/27	Authentication using passwords – chapter 7
7	10/2	Alternate authentication methods
7	10/4	**TEST REVIEW**
8	10/9	**MIDTERM 1**
8	10/11	Authorization: classifications and CAPTCHAs – chapter 8
9	10/16	Authorization: firewalls
9	10/23	Authorization: intrusion detection
10	10/25	Cross-site request forgery lab
10	10/30	Simple protocols – chapter 9

Week	Date	Topics and Readings
11	11/1	Timestamps, zero-knowledge proofs, SSH, SSL – chapter 10
11	11/6	IPSec
12	11/8	Kerberos, WEP, GSM
12	11/13	Cryptocurrencies – Bitcoin paper https://bitcoin.org/bitcoin.pdf
13	11/15	Software flaws – chapter 11
13	11/20	**TEST REVIEW**
14	11/22	**MIDTERM 2**
14	11/27	Cross-site scripting (XSS), SQL injection
15	11/29	Malware – chapter 12
15	12/4	Insecurity in software
16	12/6	TBD
16	12/11	**TEST REVIEW**
Final Exam	12/18	12:15 pm in MH 223