San José State University
Department of Computer Science
CS 166, Information Security, Section 02, Spring 2018

Course and Contact Information

Instructor:	Thomas Austin
Office Location:	MacQuarrie Hall 216
Email:	thomas.austin@sjsu.edu
Office Hours:	Mondays, 3-4pm (4-5pm Feb. 5 and Feb19 only), Tuesdays, 10-11am
Class Days/Time:	Monday/Wednesday 1:30 – 2:45 pm.
Classroom:	Duncan Hall 450
Prerequisites:	CS 146 & (CS 47 or CMPE 102 or CMPE 120), "C-" or better.

Course Format

Faculty Web Page and MYSJSU Messaging (Optional)

Course materials such as syllabus, handouts, notes, assignment instructions, etc. can be found on my faculty web page at http://www.cs.sjsu.edu/~austin/cs166-spring18/ and 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)

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

Assignments are due by 11:59 PM Pacific Time on the specified day. **Late homework assignments will not be accepted.**

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.

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, Readings, Assignments, Deadlines
1	January 24	Introduction – chapter 1
2	January 29	Classic crypto – chapter 2
2	January 31	Stream ciphers / block ciphers – chapter 3
3	February 5	More block ciphers
3	February 7	Public key crypto – chapter 4
4	February 12	More public key crypto
4	February 14	Hash functions – chapter 5
5	February 19	More hash functions
5	February 21	Password cracking
6	February 26	Authentication using passwords – chapter 7
6	February 28	Alternate authentication methods
7	March 5	**TEST REVIEW**
7	March 7	**MIDTERM 1**
8	March 12	Authorization: classifications and CAPTCHAs – chapter 8
8	March 14	Authorization: firewalls
9	March 19	Authorization: intrusion detection
9	March 21	Cross-site request forgery lab
10	March 26	**SPRING BREAK – NO CLASS**
10	March 30	**SPRING BREAK – NO CLASS**
11	April 2	Simple protocols – chapter 9

Week	Date	Topics, Readings, Assignments, Deadlines
11	April 4	Timestamps, zero-knowledge proofs, SSH, SSL – chapter 10
12	April 9	IPSec
12	April 11	Kerberos, WEP, GSM
13	April 16	Cryptocurrencies – Bitcoin paper https://bitcoin.org/bitcoin.pdf
13	April 18	Software flaws – chapter 11
14	April 23	**TEST REVIEW**
14	April 25	**MIDTERM 2**
15	April 30	Cross-site scripting (XSS), SQL injection
15	May 2	Malware – chapter 12
16	May 7	Insecurity in software
16	May 9	TBD
17	May 14	**TEST REVIEW**
Final Exam	May 22	Duncan Hall 450, 12:15 – 2:30