San José State University
School/Department
Computer Science 265: Cryptography and Computer Security, Fall 2019

Course and Contact Information

Instructor:	Auston Davis
Office Location:	MacQuarrie Hall 217
Telephone:	408-832-5448
Email:	auston.davis@sjsu.edu (preferred)
Office Hours:	Tue 6pm – 7pm (online only)
Class Days/Time:	Mon/Wed 6:00 – 7:15pm
Classroom:	MacQuarrie Hall 222
Prerequisites:	**CS149 or instructor consent**

Course Format

This a traditional classroom lecture type format. Students will be required to bring a functional laptop to all quizzes, the midterm and final

Canvas

Course materials such as syllabus, handouts, notes, assignment instructions, etc. can be found on the 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

This course focuses on security mechanisms for protecting information in computer systems and networks. This includes cryptography and its applications to security services in distributed systems, mathematics of cryptography, access control, protection models, security policies, design of secure systems, firewalls, and intrusion detection.

Course Learning Outcomes

Upon successful completion of this course, students will be knowledgeable of the major technical security challenges in each of the following four areas: cryptography, access control, protocols, and software. In addition, students will have advanced knowledge in cryptanalysis, endpoint defense and software reverse engineering, as evidenced by work on the major projects.

Required Texts/Readings

Textbook

Information Security: Principles and Practice, 3rd Edition, Mark Stamp (Only available via classroom purchase)

Other Readings

- ***A Bug Hunter's Diary: A Guided Tour Through the Wilds of Software Security***, Tobias Klein, No Starch Press, 2011. Lots of interesting real-world examples of vulnerable code.
- ***Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software***, Michael Sikorski and Andrew Honig, No Starch Press, 2012. An excellent book for information on reverse engineering (whether for malware analysis or other purposes). Includes many hands-on exercises.
- ***Software Reverse Engineering (SRE) website (http://reversingproject.info/)***. This website, which was created by a former masters student, includes lots of good information and detailed exercises with solutions.
- ***Network Security: Private Communication in a Public World***, second edition, Charlie Kaufman, Radia Perlman, and Mike Speciner, Prentice Hall, 2002, ISBN: 0-13-046019-2. This book provides good coverage of cryptography and excellent coverage of several security protocols.
- ***Security in Computing***, third edition, Charles P. Pfleeger and Shari Lawrence Pfleeger, Prentice Hall, 2003, ISBN: 0-13-035548-8. The strength of this book is its coverage of the security issues related to software. In particular, operating systems and some aspects of secure software engineering are covered well. This book also has some good, basic information on viruses.
- ***Applied Cryptography: Protocols, Algorithms and Source Code in C***, second edition, Bruce Schneier, John Wiley & Sons, Inc., 1995, ISBN: 0-471-11709-9. For better or for worse, in industry, this is the standard reference for all things cryptographic.
- ***Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses***, Ed Skoudis with Tom Liston, Prentice Hall, 2006, ISBN: 0-13-148104-5. There are many books that claim to provide information on how to foil hackers, but this is by far the best that I have seen. This is an updated version of the original Counter Hack, published in 2001.
- ***Computer Viruses and Malware***, John Aycock, Springer, 2006, ISBN: 0387302360. This book gives a good introduction to research topics related to malware. The book is well-written and surprisingly easy reading, given the technical nature of the material.

Course Requirements and Assignments

- Lectures: Students are strongly encouraged to attend all lectures. Any material presented in any lecture may be tested in any subsequent quiz, midterm or final exam. Quite a bit of material that is covered in class only will be necessary to successfully complete the projects, quizzes, mid-term and final.

- Homework: There will be a total of 7 homework assignments due. Assignments are due no later than midnight the day they are due. **No late homework will be accepted for any reason**. Assigned problems typically require a solution and an explanation (or work) detailing how you arrived at your solution. Cite any outside sources used to solve a problem.

  Save your homework to a Zip file named cs265hmk<assignment#><last name><last 4 of student number>.zip. Upload this file to the corresponding assignment in Canvas.

- Quizzes: Students will have 3 quizzes. Quizzes will be closed-book and administered in class. The student is responsible for ensuring their browser is functional. Makeup quizzes will only be given in

cases of a verifiable emergency and at the discretion of the professor. Be aware, makeup quizzes tend to be significantly more difficult.

- Projects: Students are expected to complete two projects over the course of the semester. The Cryptology Project (Project #1) and Reverse Engineering Project (Project #2) information is provided in separate documents and posted to Canvas

- Midterm Exam: The midterm exam will be held on Oct 14th. The midterm will be in-class, closed-book, and comprehensive. Makeup midterm exams will only be given in cases of a verifiable emergency and at the discretion of the professor.

- Final Exam: The final exam will be held on Dec 11th from 5:15 PM – 7:30 PM. Makeup final exams will only be given in cases of a verifiable emergency and at the discretion of the professor.

Grading Information

In addition to the stipulations provided above, grading will be based on the following:

Assignments: 100 pts
Quizzes: 100 pts
Project 1: 100 pts
Project 2: 100 pts
Midterm: 100 pts
Final: 100 pts

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

- No extra credit is anticipated

- Wireless laptop is required. Your laptop must remain **closed** and not on your desk. You will be informed when it is needed for a particular activity
- Cheating will not be tolerated
- Student must be respectful of the teacher and other students
- No disruptive or annoying talking
- Turn off cell phones
- Class begins on time
- Class is not over until I say it's over
- A valid picture ID is required at all times

University Policies

Per University Policy S17-9, 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/"

Course Schedule

This schedule is subject to change with fair notice. Notifications will be made via Canvas

Week	Date	Topics, Readings, Assignments, Deadlines
1	Aug 21	Introduction to the Course, Introduction to Cryptography and Data Security
2	Aug 26	Cryptology - Crypto Basics (READING: Chapter 1 - 2 - Stamp)
2	Aug 28	Cryptology – Symmetric Key Crypto. (READING: Chapter 3.3 - Stamp)
3	Sep 2	**NO CLASS –** Labor Day - Campus Closed - Campus Closed
3	Sep 4	Cryptology - Advanced Encryption Standard (AES) *Cryptography Project Topic Due.* (READING: Chapter 3.3 – 3.5 - Stamp)
4	Sep 9	Cryptology - Introduction to Public-Key Cryptography, RSA, Diffe-Heilman (READING: Chapter 4.1 – 4.4 - Stamp)
4	Sep 11	Cryptology – Uses for Public-Key Cryptography. Public-Key Infrastructure (PKI) (READING: Chapter 4.6 – 4.9 - Stamp)

San José State University
School/Department
Computer Science 265: Cryptography and Computer Security, Fall 2019

Week	Date	Topics, Readings, Assignments, Deadlines
5	Sep 16	Cryptology – Hash Functions. Birthday Attack. Non-Crypto Hashing. Tiger Hash. (READING: Chapter 5.1 – 5.8 - Stamp)
5	Sep 18	Cryptology – Visual Cryptography. Information Hiding. Steganography. (Section Review) (READING: Chapter 5.9.1.2 – 5.10 - Stamp)
6	Sep 23	Cryptology – Elliptical Curve Crypto (Video) (READING: Up through Chapter 6 - Stamp)
6	Sep 25	**[Cryptology Quiz],** Access Control - Passwords. (READING: Chapter 7.1 – 7.4 - Stamp)
7	Sep 30	Access Control – Authorization, Orange Book, EAL, Authentication vs Authorization, ACLs (READING: Chapter 8.1 – 8.6 - Stamp)
7	Oct 2	Access Control - Biometrics. Cookies. Single Sign On (SSO). Federated Access. (READING: Chapter 7.4 – 7.8 - Stamp)
8	Oct 7	Access Control – Multilevel Security Models, Bell-LaPadula. Compartments. Covert Channel (READING: Chapter 8.7 – 8.8 - Stamp)
8	Oct 9	Access Control - Inference Control, CAPTCHA. 2-Factor Authentication, Access Control Section Review. (READING: Chapter 9.1 – 9.2 - Stamp)
9	Oct 14	**MIDTERM – Cryptology – Access Control** (READING: Up through Chapter 9.2 - Stamp)
9	Oct 16	Protocols – Network Basics, Simple Protocols. Firewalls. Application Proxy. Intrusion Detection Systems, Anti-Virus v. Whitelisting. Anomaly Detection. Defense-in-Depth (READING: Chapter 8.9 – 8.11 - Stamp) (READING: Chapter 9.3 – 9.4 - Stamp)
10	Oct 21	Protocols - Authentication Protocols. Authentication and TCP (READING: Chapter 9.3 – 9.4 - Stamp)
10	Oct 23	Protocols – Real World Security Protocols: SSH. SSL. IPSEC (READING: Chapter 10.1 – 10.4 - Stamp)
11	Oct 28	Protocols – Real World Security Protocols: Kerberos. WEP, (Section Review) (READING: Chapter 10.5 - 10.6 - Stamp)
11	Oct 30	**[Protocols Quiz]** Software Security - Software Flaws (READING: Chapter 11.1 - Stamp)
12	Nov 4	Software Security - Reverse Engineering. Buffer Overflow. Stack Smashing Defense. Input Validation. Incomplete Mediation. Race Conditions (READING: Chapter 11.2 - Stamp)
12	Nov 6	Software Security – Malware. Trojans. Botnets. Ransomware, Real-World Attack Anatomy (READING: Chapter 11.3 – 11.5 - Stamp)
13	Nov 11	**NO CLASS –** Veteran's Day (Observed) - Campus Closed

San José State University
School/Department
Computer Science 265: Cryptography and Computer Security, Fall 2019

Week	Date	Topics, Readings, Assignments, Deadlines
13	Nov 13	Software Security – Software Security – Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Interactive Application Security Testing (IAST), Run-time Application Security Protection (RASP), Vulnerability Scanning, Penetration Testing
14	Nov 18	Program Security – Security Incident and Event Management (SIEM) Correlation, Big Data Analytics, SOAR, Threat Response and Cyber-Forensic Investigations, Self-Healing Enterprises
15	Nov 20	Program Security – Security Reviews, Policies, Standards and Guidelines, Exceptions Management, Regulatory Certification, Cybersecurity Frameworks
15	Nov 25	Software and Program Security (Section Review)
16	Nov 27	**NO CLASS –** Non-Instructional Day – (NI)
16	Dec 2	***Reverse Engineering Project Presentations***
17	Dec 4	***Reverse Engineering Project Presentations***
17	Dec 9	Finals Review (Section Review)
Final Exam	Dec 11	5:15pm