San José State University
Computer Science Department
CS 265 Cryptography and Computer Security, Sec 01, Fall 2015

Course and Contact Information

Instructor: Auston Davis

Office Location: MH 216

Telephone: 408.924.5094

Email: Auston.davis@sjsu.edu

Office Hours: Thursdays 7:15 – 7:45 BBC 122 (Email is the best way to contact)

Class Days/Time:

Classroom:

Prerequisites: CS 149 or instructor consent

Course Description

We will cover selected security topics in each of the following areas: cryptography, access control, protocols, and software.

Course Learning Outcomes (CLO)

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

Required Texts/Readings

Textbook

We will use a manuscript that will eventually become the 3rd edition of the textbook Information Security: Principles and Practice, Mark Stamp

Required Reading: National Institute of Standards and Technology NIST) 800-86 – Guide to Integrating Forensic Techniques into Incident Response
http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

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 Engineering: A Guide to Building Dependable Distributed Systems***, Ross Anderson, John Wiley & Sons, Inc., 2001, ISBN: 0-471-38922-6; see Ross Anderson's Security Engineering website http://www.cl.cam.ac.uk/~rja14/book.html, where you can obtain a free (and legal) copy of the 1st edition of the book. This is an excellent book for an overview of security in general, but it is not too focused or technically detailed.
- ***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

SJSU classes are designed such that in order to be successful, it is expected that students will spend a minimum of forty-five hours for each unit of credit (normally three hours per unit per week), including preparing for class, participating in course activities, completing assignments, and so on. More details about student workload can be found in University Policy S12-3 at http://www.sjsu.edu/senate/docs/S12-3.pdf.

Task	Points	Date
Test	100	Tuesday, October 6th
Reverse Engineering Project	100	Thursday, October 8th (Topic) Friday, December 1st (Project)
Quiz #1 – Basic Crypto Quiz	20	Thursday, September 3rd
Quiz #2 – Access Control Quiz	20	Thursday, September 24th
Quiz #3 – Protocols Quiz	20	Tuesday, October 20th
Quiz #4 – Malware Quiz	20	Tuesday, November 3rd
Quiz #5 – Software/Security Quiz	20	Tuesday, December 8th
Homework, Class Participation (In Class)	100	
Final	100	Tuesday, December 15th
TOTAL	500	

- Reverse Engineering Project: Information is provided in a separate document and posted to Canvas
- Final Schedule: The official finals schedule is here: http://info.sjsu.edu/static/catalog/final-exam-schedule-spring.html
- Semester grade will be computed as a weighted average of the major scores listed above.
- No make-up tests or quizzes will be given and no late homework or project (or other work) will be accepted. Also, in-class work must be completed in the section that you are enrolled in.

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."

Grading Policy

Note that "All students have the right, within a reasonable time, to know their academic scores, to review their grade-dependent work, and to be provided with explanations for the determination of their course grades." See University Policy F13-1 at http://www.sjsu.edu/senate/docs/F13-1.pdf for more details.

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

Homework: Homework is due typewritten (including source code) by class starting time on the due date. Each assigned problem requires a solution and an explanation (or work) detailing how you arrived at your solution. Cite any outside sources used to solve a problem. When grading an assignment, I may ask for additional information. A subset of the assigned problems will be graded.
Zip your homework into a file named cs265hmk<assignment><last name><last 4 of student number>.zip. Upload this file to the corresponding assignment in Canvas.
Example:

Cs265hmk2davis5191.zip

Other Important Stuff:

- The last day to drop is Tuesday, September 1, and the last day to add is Wednesday, September 9
- No extra credit is anticipated
- Wireless laptop is required. Your laptop must remain closed (preferably in your backpack and, in any case, not on your desk) until I inform you that 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
- Valid picture ID required at all times

Keys to success: Do high quality work on the projects, do the homework, and attend class

University Policies

General Expectations, Rights and Responsibilities of the Student

As members of the academic community, students accept both the rights and responsibilities incumbent upon all members of the institution. Students are encouraged to familiarize themselves with SJSU's policies and practices pertaining to the procedures to follow if and when questions or concerns about a class arises. See University Policy S90–5 at http://www.sjsu.edu/senate/docs/S90-5.pdf. More detailed information on a variety of related topics is available in the SJSU catalog, at http://info.sjsu.edu/web-dbgen/narr/catalog/rec-12234.12506.html. In general, it is recommended that students begin by seeking clarification or discussing concerns with their instructor. If such conversation is not possible, or if it does not serve to address the issue, it is recommended that the student contact the Department Chair as a next step.

Dropping and Adding

Students are responsible for understanding the policies and procedures about add/drop, grade forgiveness, etc. Refer to the current semester's Catalog Policies section at http://info.sjsu.edu/static/catalog/policies.html. Add/drop deadlines can be found on the current academic year calendars document on the Academic Calendars webpage at http://www.sjsu.edu/provost/services/academic_calendars/. The Late Drop Policy is available at http://www.sjsu.edu/aars/policies/latedrops/policy/**.** Students should be aware of the current deadlines and penalties for dropping classes.

Information about the latest changes and news is available at the Advising Hub at http://www.sjsu.edu/advising/.

Consent for Recording of Class and Public Sharing of Instructor Material

University Policy S12-7, http://www.sjsu.edu/senate/docs/S12-7.pdf, requires students to obtain instructor's permission to record the course and the following items to be included in the syllabus:

- "Common courtesy and professional behavior dictate that you notify someone when you are recording him/her. You must obtain the instructor's permission to make audio or video recordings in this class. Such permission allows the recordings to be used for your private, study purposes only. The recordings are the intellectual property of the instructor; you have not been given any rights to reproduce or distribute the material."
    - It is suggested that the greensheet include the instructor's process for granting permission, whether in writing or orally and whether for the whole semester or on a class by class basis.
    - In classes where active participation of students or guests may be on the recording, permission of those students or guests should be obtained as well.
- "Course material developed by the instructor is the intellectual property of the instructor and cannot be shared publicly without his/her approval. You may not publicly share or upload instructor generated material for this course such as exam questions, lecture notes, or homework solutions without instructor consent."

Academic integrity

Your commitment, as a student, to learning is evidenced by your enrollment at San Jose State University. The University Academic Integrity Policy S07-2 at http://www.sjsu.edu/senate/docs/S07-2.pdf requires you to be honest in all your academic course work. Faculty members are required to report all infractions to the office of Student Conduct and Ethical Development. The Student Conduct and Ethical Development website is available at http://www.sjsu.edu/studentconduct/.

Campus Policy in Compliance with the American Disabilities Act

If you need course adaptations or accommodations because of a disability, or if you need to make special arrangements in case the building must be evacuated, please make an appointment with me as soon as possible, or see me during office hours. Presidential Directive 97-03 at http://www.sjsu.edu/president/docs/directives/PD_1997-03.pdf requires that students with disabilities requesting accommodations must register with the Accessible Education Center (AEC) at http://www.sjsu.edu/aec to establish a record of their disability.