San José State University
School/Department
CS 166 Section 02, Information Security, Spring, 2021

Course and Contact Information

Instructor:	Sanjoy Paul
Office Location:	[TBD]
Telephone:	(832) 805-4877
Email:	paul.sanjoy@sjsu.edu
Office Hours:	[TBD]
Class Days/Time:	TuTh: 18:00-19:15 PST
Classroom:	Zoom

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

Prerequisites: 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); or instructor consent.

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

- Approximate schedule (3 hours equals 1 week of class time):
    - Introduction
        - Chapter 1 (1 hour)
    - Crypto
        - Chapter 2: Crypto Basics (3 hours)
        - Chapter 3: Symmetric Key Crypto (4 hours)
        - Chapter 4: Public Key Crypto (4 hours)
        - Chapter 5: Hash Functions and Other Topics (4 hours)
    - Access Control
        - Chapter 7: Authentication (4 hours)

        - Chapter 8: Authorization (2 hour)
    - Protocols
        - Chapter 9: Simple Authentication Protocols (4 hours)
        - Chapter 10: Real-World Security Protocols (5 hours)
    - Software
        - Chapter 11: Software Flaws and Malware (4 hours)
        - Chapter 12: Insecurity in Software (4 hours)
        - Chapter 13: Operating Systems and Security (4 hours)
- Note: Due to time constraints, we omit Chapter 6 and various parts of the last three chapters.

- Some useful resources are given below and many more will be provided on an ongoing basis:
    - ***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. 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 Format

Technology Intensive, Hybrid, and Online Courses

This course will be taught online. You need Internet connectivity and zoom installed on your a computer to participate in the classroom activities and/or submit assignments. You need to have a Python software development environment installed on your computer to do the projects.

Course Description

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

Course Learning Outcomes

Upon successful completion of this course, you should be knowledgeable of the major technical security challenges in each of the following areas: cryptography, access control, protocols, and software.

Other technology requirements / equipment / material

We will use Zoom for our online sessions

Installing Zoom

https://www.youtube.com/watch?v=fVu9BILRkww

Course Requirements and Assignments

Homework Assignments:

Homework assignments will be posted and submitted on Canvas. For full credit, they must be submitted by the posted due date.

Weekly Quizzes:

We will have a weekly quiz aimed at checking your understanding of the previous week's material. I will count the 10 best scores out of the 12 total quizzes in the semester. You must be in the online classroom to take the quiz. Missed quizzes cannot be made up.

Midterm Exam:

The midterm exam will take place in the classroom during class time on Tuesday March 16 during regular class hours.

Final Exam:

The final exam will take place on Tuesday May 25 – 19:45-22:00

Grading Information

The final grade in the course will be calculated based on the following percentages:

Homework Assignments: 30%

Weekly Quizzes: 20%

Midterm: 20%

Final Exam: 30%

Late Work:

Late assignments will not be accepted.

Grade Scale:

The letter grade will be determined based on the following scale:

A+ = 96% - 100%	A = 91% - 95%	A- = 86% - 90%
B+ = 81% - 85%	B = 76% - 80%	B- = 71% - 75%
C+ = 66% - 70%	C = 61% - 65%	C- = 56% - 60%
D = 51% - 55%		
F = below 50		

Classroom Protocol

Regular attendance is an integral part of the learning process. Please arrive on time for the classes.

University Policies

Per University Policy S16-9 *(http://www.sjsu.edu/senate/docs/S16-9.pdf)*, relevant information to all courses, such as academic integrity, accommodations, dropping and adding, consent for recording of class, etc. is available on Office of Graduate and Undergraduate Programs' Syllabus Information web page at http://www.sjsu.edu/gup/syllabusinfo/". Make sure to visit this page, review and be familiar with these university policies and resources.

CS166 Information Security, Spring, 2021, Course Schedule

Please note that this schedule is subject to change with fair notice. Any changes will be announced in class and posted on the Canvas course site.

Course Schedule

Week	Date	Topics	Readings (Textbook)	HW Due date
1	Jan 28	Introduction + Overview of the Course	Chapter 1	
2	Feb 2	Overview of the Course continued + Crypto Basics I	Chapter 2	HW1 Feb 10
2	Feb 4	Crypto Basics II	Chapter 2	
3	Feb 9	Symmetric Key Crypto I	Chapter 3	Quiz#1
3	Feb 11	Symmetric Key Crypto II	Chapter 3	HW2 Feb 24
4	Feb 16	Symmetric Key Crypto III	Chapter 3	Quiz#2
4	Feb 18	Public Key Crypto I	Chapter 4	HW3 Mar 3
5	Feb 23	Public Key Crypto II	Chapter 4	Quiz#3
5	Feb 25	Public Key Crypto III	Chapter 4	HW4 Mar 10
6	Mar 2	Hash Function & Other topics I	Chapter 5	Quiz#4
6	Mar 4	Hash Function & Other topics II	Chapter 5	HW5 Mar 17
7	Mar 9	Authentication I	Chapter 7	Quiz#5
7	Mar 11	Authentication II	Chapter 7	HW6 Mar 24
8	Mar 16	Authentication III	Chapter 7	Quiz#6
8	Mar 18	Midterm		
9	Mar 23	Authorization I	Chapter 8	HW7 Apr 5
9	Mar 25	Authorization II	Chapter 8	
10	Mar 30	Simple Authentication Protocols I	Chapter 9	Quiz#7
10	Apr 1	Simple Authentication Protocols II	Chapter 9	HW8 Apr 14
11	Apr 6	Simple Authentication Protocols III	Chapter 9	Quiz#8
11	Apr 8	Real-world Security Protocols I	Chapter 10	HW9 Apr 21
12	Apr 13	Real-world Security Protocols II	Chapter 10	Quiz#9
12	Apr 15	Real-world Security Protocols III	Chapter 10	HW10 Apr 28
13	Apr 20	Software Flaws and Malware I	Chapter 11	Quiz#10
13	Apr 22	Software Flaws and Malware II	Chapters 11	
14	Apr 27	Software Flaws and Malware III	Chapters 11	Quiz#11
14	Apr 29	Insecurity in Software I	Chapters 12	HW11 May 13
15	May 4	Insecurity in Software II	Chapter 12	Quiz#12
15	May 6	Operating Systems and Security I	Chapter 13	

16	May 11	Operating Systems and Security II	Chapter 13	
16	May 13	Operating Systems and Security III	Chapter 13	
Final	May 25	FINAL EXAM	19:45-22:00	