San José State University
Charles W. Davidson College of Engineering/Computer Engineering Department
CS-166, Information Security, Section 03, Spring 2021

Course and Contact Information

Instructor:	Chao-Li Tarng, Ph.D.
Office Location:	ENG 259
Telephone:	TBD
Email:	chaoli.tarng@sjsu.edu
Office Hours:	Wed 3:00 – 4:00 pm
Class Days/Time:	Monday and Wednesday 4:30pm – 5:45pm
Classroom:	Online
Prerequisites:	CS-146 (with a grade of C- or above) and either CS-47 or CMPE-102 or CMPE-120 (with a grade of C- or above)

Course Format

Technology Intensive, Hybrid, and Online Courses

Due to the COVID-19 coronavirus pandemic, there are no required in person meetings. The lectures are offered online using the Zoom meetings. The course is offered in a synchronous and asynchronous hybrid mode. The lectures will be recorded via Zoom. Therefore, students can attend the class in an asynchronous fashion by watching the lectures after they are recorded. **However, in certain classes, such as quizzes, project demo and presentation, and exams, students must attend the class synchronously.** The synchronous class dates are marked on the Course Schedule at the end of this syllabus.

This course requires each student to have a personal computer installed with a modern operating system, such as MS Windows ™, Mac OS X ™, or Linux. The personal computer must be able to connect to Internet and capable of running multiple instances of virtual machines, such as VMware ™. A VMware education license will be provided. In addition, necessary software such as Respondus Lockdown Browser needs to be installed so that students can take online quizzes and exams. The personal computer must be equipped with a webcam so that students can be proctored during the exams using the webcam.

This course provides hands-on experiences about various attack cases in Linux operation system. In addition, this course provides an example to create a network topology to launch possible attacks in a virtual lab environment, such as DeterLab. This course has two midterm exams, a final exam, homework including lab assignments, and a group-based course project. All assignments must be submitted through our eLearning platform Canvas at http://sjsu.instructure.com.

Due to the online nature of the class, the lectures (i.e., Zoom meetings) will be recorded. The recording will be posted for students to review once available. Students must obtain permission in advance to record any course materials. Such permission allows the recordings to be used for a student's private, study purposes only.

Students will not be permitted to share any class recordings with someone who isn't enrolled in the class or without permission. The recordings are protected by instructor's copyright.

Faculty Web Page and MYSJSU Messaging

Copies of the course materials such as the syllabus, major assignment handouts, etc. may be found on the course shell available from the eLearning platform Canvas at: *http://sjsu.instructure.com*. Submission of any assignment (homework, report, etc.) should be made at Canvas as well. You are responsible for regularly (i.e. every couple of days) checking with the messaging system (email, discussions, announcements, news) through Canvas and through MySJSU.

Course Description

A study of computer and network security from centralized systems to distributed networks. Cryptology, vulnerabilities and controls. Firewalls, privacy enhanced e-mail, viruses and worms. Case studies will be featured. Prerequisite: CMPE 126. Computer Engineering or Software Engineering Majors Only.

https://catalog.sjsu.edu/preview_course_nopop.php?catoid=2&coid=7023

Course Learning Outcomes (CLO)

Upon successful completion of this course, students will be able to:

1. Demonstrate in-depth understanding of tools and common techniques in different network attacking phases and effective defenses against these attacks.
2. Demonstrate in-depth understanding of cryptography algorithms and standards, authentication protocols.
3. Understanding various network security defense methods against system and network security problems.
4. Demonstrate the capability of discovering security problems in networked systems and developing a defense technique.
5. Conduct a set of hands-on labs which are available at SEED Labs supported by NSF.
6. Demonstrate the capability of working collaboratively and productively in a team environment.

Required Texts/Readings

Textbook

William Stallings, Lawrie Brown, *Computer Security: Principles and Practice* (4th Edition), Prentice Hall, 2018, ISBN-13: 978-0134794105 (eText ISBN: 9780134794181)

Students can obtain the eText for $34.99: http://www.informit.com/store/computer-security-principles-and-practice-subscription-9780134794181

Other Readings

Wenliang Du, *Computer Security: A Hands-on Approach*
https://www.handsonsecurity.net

W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th Ed., Pearson 2017. ISBN 10: 0-13-335469-5, ISBN 13: 978-0-13-335469-0

Other technology requirements / equipment / material

This course requires the student to have a personal computer that is installed with a modern operating system, such as MS Windows ™, Mac OS X ™, or Linux. The personal computer must be able to connect to Internet and is capable of running multiple instances of virtual machines, such as VMware. A VMware education license will be provided.

Course Requirements and Assignments

The class assignments that are assessed and that contribute to your final grade include homework assignments, project presentation and report, one midterm exam, and one final exam.

- **Homework/Lab assignments**: Labs with exercises will be assigned after learning several topics. The labs and the homework are tools for you to learn the material and prepare you for the exams. **I will NOT accept late ones.**
  - **Labs and Class Demos:** This class provides different hands-on techniques to understand various attacks.
  - **Target techniques:** Brute Force Authentication Attack with Burp Suite, SQL Injection Attacks, Man-in-the-middle attacks, DoS attacks, DNS Hijacking, XSS attacks, Buffer overflow attacks, and so on.
  - **Testbed and Tools:** DeterLab, SEED Labs, Mininet, Kali Linux, Linux, Wireshark, and so on.
- **Reading assignments:** You should read some chapters in the textbook before the next class.
- **Programming/Project assignments:** A term project will be assigned. You can choose one hot topic from a literature survey in security areas. Programming assignments are based on a group, unless otherwise specified. Each team is required to submit a project report for each phase to the course Canvas site. The due date of each report is to be announced later.
- **Exams**: There are three exams (close books) during the semester. The final exam, closed books and comprehensive, will be worth 30% of your grade. The exams will contain multiple choices questions with several short answer questions and descriptive questions.

No late assignments will be accepted. Email submission of assignments will NOT be accepted. Please turn in all assignment on CANVAS, the eLearning platform Canvas at: http://sjsu.instructure.com. An extension or an exception will be granted only if a student has serious and compelling reasons that can be proven by an independent authority (e.g. doctor's note if the student has been sick).

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."

"Success in this course is based on the expectation that students will spend, for each unit of credit, a minimum of 45 hours over the length of the course (normally three hours per unit per week) for instruction, preparation/studying, or course related activities, including but not limited to internships, labs, and clinical practica. Other course structures will have equivalent workload expectations as described in the syllabus."

Final Examination or Evaluation

"Faculty members are required to have a culminating activity for their courses, which can include a final examination, a final research paper or project, a final creative work or performance, a final portfolio of work, or other appropriate assignment."

Grading Information (Required)

Homework & Quizzes	20%
Term Course Project	15%
Two Midterm Exams	40%
Final Exam (comprehensive)	25%
Total	100%

- The final grade of this class is *solely* based on *your* performance in *this* class.
- Course Project Report will be submitted through Canvas. Plagiarism will result in a grade of F for the class as well being referred to the department chair.
- No extra credit is available.
- Major exams in this class may be video recorded to ensure academic integrity. The recordings will only be viewed if there is an issue to be addressed. Under no circumstances will the recordings be publicly released.

Determination of Grades

Grade	*Points*	*Percentage*
A plus	*960 to 1000*	*96 to 100%*
A	*910 to 959*	*91 to 95%*
A minus	*870 to 909*	*87 to 90%*
B plus	*840 to 869*	*84 to 86 %*
B	*800 to 839*	*80 to 83%*
B minus	*750 to 799*	*75 to 79%*
C plus	*700 to 749*	*70 to 74%*
C	*650 to 699*	*65 to 69%*
C minus	*600 to 649*	*60 to 64%*
D plus	*550 to 599*	*55 to 59%*
D	*500 to 549*	*50 to 54%*
D minus	*450 to 499*	*45 to 49%*
F	*000 to 449*	*0%-44%*

- Refer to Spring 2021 Special University Grading Policy for grade changes.

Classroom Protocol

- Each student is required to engage in classroom activities, participate in labs, submit assignments and reports on time, *and* take exams and tests on time.
- Web browsing in class is strictly not allowed. Cell Phones are to be turned off during lectures and tests. During exams if you receive a cell phone call or page it will be assumed that you have completed your exam and no further work will be allowed.
- No make-up exams will be held.

- Exams will be closed book. One cheat sheet (letter size and both sides) is allowed in each exam.
- Student causing disruption in the class will be asked to leave the class.

Zoom Classroom Etiquette

- **Mute Your Microphone:** To help keep background noise to a minimum, make sure you mute your microphone when you are not speaking.
- **Be Mindful of Background Noise and Distractions:** Find a quiet place to "attend" class, to the greatest extent possible.
    - Avoid video setups where people may be walking behind you, people talking/making noise, etc.
    - Avoid activities that could create additional noise, such as shuffling papers, listening to music in the background, etc.
- **Position Your Camera Properly:** Be sure your webcam is in a stable position and focused at eye level.
- **Limit Your Distractions/Avoid Multitasking:** You can make it easier to focus on the meeting by turning off notifications, closing or minimizing running apps, and putting your smartphone away (unless you are using it to access Zoom).
- **Use Appropriate Virtual Backgrounds:** If using a virtual background, it should be appropriate and professional and should NOT suggest or include content that is objectively offensive or demeaning.

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.

CS 166, Information Security, Spring 2021
Course Schedule

The schedule is subject to change with fair notice through Canvas

Course Schedule

Note: The synchronous class dates are highlighted in blue and bold.

Week	Date	Topics	Readings/Assignments
1	1/27	Course Overview, Linux tutorial	Slides
2	2/1	Information Security Introduction	Ch. 1
	2/3	Classic Encryption Technology	Notes
3	2/8	Cryptographic Tools	Ch. 2
	2/10	Symmetric Encryption	Ch. 20, HW#1
4	2/15	Symmetric Encryption	
	2/17	Asymmetric Encryption	Ch. 21
5	2/22	Asymmetric Encryption	HW#2
	2/24	User Authentication	Ch. 3
6	***3/1***	User Authentication	**Quiz1**
	3/3	**Midterm I Exam**	
7	3/8	Web Security	Notes
	3/10	Web Security	HW#3
8	3/15	Access Control	Ch. 4
	3/17	Access Control	
9	3/22	Key Distribution	Notes
	3/24	Key Distribution	
10	3/29	***Spring Break - No Class***	
	3/31	***Spring Break - No Class***	
11	***4/5***	Fundamental of Networking (TCP/IP Tutorial)	**Quiz2**
	4/7	**Midterm II Exam**	
12	4/12	Fundamental of Networking (TCP/IP Tutorial)	HW#4
	4/14	Network Attacks (DoS, etc.)	Ch. 7
13	4/19	Network Attacks (DoS, etc.)	
	4/21	Network Attacks (DoS, etc.)	
14	4/26	Malicious Software	Ch. 11
	4/28	Malicious Software	HW#5
15	5/3	Buffer Overflow	Ch. 10
	5/5	Buffer Overflow	

16	***5/10***	Project presentation	
	5/12	Project presentation	
17	5/17	No class - self review	
17	***5/20***	***Final Exam: Thursday 5/20/2021, 2:45pm - 5:00pm***	**Final Exam**