SJSU SAN JOSÉ STATE UNIVERSITY

**College of Science · Computer Science**

# Information Security Section 01

## CS 166

Spring 2024 3 Unit(s) 01/24/2024 to 05/13/2024 Modified 01/24/2024

## Contact Information

### Instructor: Dr. Chao-Li Tarng

**Email:** chaoli.tarng@sjsu.edu
**Office:** ENG 187

#### Office Hours

Wednesday, 2:30 PM to 3:30 PM, ENG 187

The office hour is either in-person (walk-in) at ENG 187 or on Zoom: https://sjsu.zoom.us/j/87239048374 (https://sjsu.zoom.us/j/87239048374). No appointment is needed during the office hour. If you want to meet me any time other than the office hour, an appointment is required.

## Course Description and Requisites

Fundamental security topics including cryptography, authentication, access control, network security, security protocols, and software security. Networking basics are covered. Additional security topics selected from multilevel security, biometrics, blockchain, machine learning, information warfare, e-commerce, intrusion detection, system evaluation and assurance.

Prerequisite(s): 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); Computer Science, Applied and Computational Math, Forensic Science: Digital Evidence, or Software Engineering Majors only; or instructor consent.

Letter Graded

## Classroom Protocols

- 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.

# Program Information

Diversity Statement - At SJSU, it is important to create a safe learning environment where we can explore, learn, and grow together. We strive to build a diverse, equitable, inclusive culture that values, encourages, and supports students from all backgrounds and experiences.

# Course Goals

## Course Format

TheCS-166 Information Security course combines both theoretical study as well as hands-on exercises of the information security technology. Therefore, it requires each 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 capable of running multiple instances of virtual machines, such as VirtualBox. Students using Mac OSX must be aware of that M1/M2-based Macbook Pros are not compatible with the virtual machines provided. Therefore, students using M1/M2 Macbook Pros need to have access to an Intel x86-based computer (Windows/Linux/Mac OSX) in order to perform the exercises and homework.

This course provides hands-on experiences about various attack cases in a Linux operation system running in a virtual machine environment. In addition, this course provides an example to create a network topology to launch possible attacks in a virtual lab environment, such as the SEED Lab. This course has quizzes, 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.

The quizzes, midterms, and final exam are in class and online using students' personal computers.

# Course Learning Outcomes (CLOs)

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.

# Course Materials

## 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

2017. 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 VirtualBox. M1/M2-based Macbook Pro unfortunately is not suitable for the virtual machine environment.

# 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 (closed books) during the semester. The final exam, closed books and comprehensive, will be worth 25% 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."

# ✔ Grading Information

## 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*
- 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%* |

| *Grade* | *Points* | *Percentage* |
|---|---|---|
| *F* | *000 to 449* | *0%-44%* |

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

# University Policies

Per University Policy S16-9 (PDF) (http://www.sjsu.edu/senate/docs/S16-9.pdf), relevant university policy concerning all courses, such as student responsibilities, academic integrity, accommodations, dropping and adding, consent for recording of class, etc. and available student services (e.g. learning assistance, counseling, and other resources) are listed on the Syllabus Information (https://www.sjsu.edu/curriculum/courses/syllabus-info.php) web page. Make sure to visit this page to review and be aware of these university policies and resources.

# Course Schedule

The schedule is subject to changes with a one-week notice.

| Week | Date | Topics | Readings/Assignments |
|---|---|---|---|
| 1 | 1/24 | Course Overview, Linux tutorial | Slides |
| 2 | 1/29 | Information Security Introduction | Ch. 1 |
| | 1/31 | Classic Encryption Technology | Notes |
| 3 | 2/5 | Cryptographic Tools | Ch. 2 |
| | 2/7 | Symmetric Encryption | Ch. 20, HW#1 |
| 4 | 2/12 | Symmetric Encryption | |
| | 2/14 | Asymmetric Encryption | Ch. 21 |
| 5 | 2/19 | Asymmetric Encryption | HW#2 |
| | 2/21 | User Authentication | Ch. 3 |
| 6 | 2/26 | User Authentication | Quiz1 |
| | 2/28 | Midterm I Exam | |

| | | | |
|---|---|---|---|
| 7 | 3/4 | Web Security | Notes |
| | 3/6 | Web Security | HW#3 |
| 8 | 3/11 | Access Control | Ch. 4 |
| | 3/13 | Access Control | |
| 9 | 3/18 | Key Distribution | Notes |
| | 3/20 | Key Distribution | |
| 10 | 3/25 | Fundamental of Networking (TCP/IP Tutorial) | Quiz2 |
| | 3/27 | Midterm II Exam | |
| 11 | 4/1 | Spring Break - No Class | |
| | 4/3 | Spring Break - No Class | |
| 12 | 4/8 | Fundamental of Networking (TCP/IP Tutorial) | HW#4 |
| | 4/10 | Network Attacks (DoS, etc.) | Ch. 7 |
| 13 | 4/15 | Network Attacks (DoS, etc.) | |
| | 4/17 | Network Attacks (DoS, etc.) | |
| 14 | 4/22 | Buffer Overflow | Ch. 10 |
| | 4/24 | Buffer Overflow | HW#5 |
| 15 | 4/29 | Malicious Software | Ch. 11 |
| | 5/1 | Malicious Software | |
| 16 | 5/6 | Project presentation | |
| | 5/8 | Project presentation | |
| | 5/20 | Final Exam: Monday 5/20, 12:15pm - 2:30pm | Final Exam |