SJSU SAN JOSÉ STATE UNIVERSITY

College of Sciences · Computer Science

CS-266
Topics in Information Security

2026 Spring Section 1 1/26/2026 to 05/11/2026 Modified 03/17/2026

Contact Information

Instructor(s): Melody Moh

Office Location: DH 214/214A. Office telephone (Zoom phone): 408 9245088

Email: melody.moh@sjsu.edu

Class Meeting Days/Time: Mon/Wed 1:30 - 2:45 PM

Office Hours: Mon 3-4PM (DH 214) and Fri 9:30-10:30AM (Zoom only)

TA: Alan Chuang. Email: alan.chuang@sjsu.edu

Course Catalog Description and Prerequisites

Advanced topics in the area of information security. Content differs with each offering. Possible topics include, but are not restricted to: Network Security, Software Reverse Engineering and Cryptanalysis.

Prerequisites

CS 166 and Graduate standing. Allowed Declared Major: Computer Science, Bioinformatics, Data Science. Or instructor consent.

Classroom Protocols

- **Attendance for the first two class meetings is required**. Important class information, including policies and class schedules. Students who do not attend the first class meeting and not contact the instructor by the second class meeting will be removed from the course.
- Students are expected to assist in **maintaining a classroom environment** that is conducive to learning. Inappropriate behavior in the classroom that leads to the distraction of others shall not be tolerated under any circumstances.
- Instruction will begin at or within several minutes of the official published start time for the course. Please make sure that **cell phones and texting devices are turned off** during the entire scheduled class time. Excessive audible discussions with fellow students are prohibited so that others are not disturbed.
- **If a student is caught cheating** on a homework/assignment/project, the student will receive a 0 on that assignment. The instructor must report any incidents of cheating or plagiarism to the University per University Policy F15-7.
- Class meetings and office hours may be moved online due to work/conference travels.

Dropping and Adding

Feb 17 is the last day to add and the last day to drop (without an entry to students' permanent record).

Course Learning Outcome (CLO)

The focus of this course will be on selected advanced topics of security and privacy issues in cloud/networked systems and AI/ML/LLM systems. After completing this course students should have a solid understanding and advanced knowledge of selected security/privacy issues in cloud/networked and AI/ML/LLM systems.

Course Materials

Required Readings

Selected peer-reviewed publications from journals and conference proceedings will be provided.

Course Requirements and Assignments

Class participation is essential in understanding the course concepts and relies on being prepared for class. 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 S16-9 at http://www.sjsu.edu/senate/docs/S16-9.pdf.

Homework and assignments *are due typewritten 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 typically be graded.*

Refer the course website for latest information of homework assignments.

NOTE that University policy F15-12 at http://www.sjsu.edu/senate/docs/F15-12.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.”

Tentative Grading Weights

- Classroom participation: 10%
- Homework: 20%
- Paper presentations (including survey/preliminary studies): 30% (10% each)
- Final Project (presentation/implementation/demonstration/written report): 40%
- ***NO*** *late assignments will be accepted.*

Final Examination/Evaluation

This is a project-based course, and the final examination/evaluation is done by the Final Project and the written report in LaTeX format, in-class presentation, and project demonstration (40%).

Grading Information

The letter grades for the course, including +/- grades are based on:

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-*
60 - 69	*D*
59 and below	*F*

Course Schedule

CS-266 Topics in Information Security

Detailed course schedule will be available soon.

Topics may include but not limited to:

- Cloud/edge/IoT/networked systems and security/privacy issues
  - Autoscaling, predictive autoscaling
  - Privacy, partial privacy, DDoS attacks in federated learning
  - Hardware security (most relevant to clouds and AI/ML systems)
  - Vulnerabilities and attack detections in IoT systems
  - Cyber risks of autonomous systems
  - Detection and analysis of cyber threats/attacks
- AI/ML systems and security/privacy issues
  - Data bias/poisoning
  - Deepfake detections
  - Adversary attacks, detection, and defense strategies
  - Explainable robustness
- LLM and security/privacy issues
  - Prompt engineering, chain of thoughts, prompt guidance
  - Gemini, Mermaid, ChatGPT, DeepSeek
  - Hallucination

University Policies and Procedures

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 https://www.sjsu.edu/curriculum/courses/syllabus-info.php". Make sure to visit this page, review and be familiar with these university policies and resources.

Academic Integrity

For this class, you should obviously not cheat on tests/quizzes/exams. For quizzes and exams, you should not discuss or share code or problem solutions between groups or friends! At a minimum a 0 on the quiz or exam will be given. A student caught using resources like Rent-a-coder will receive an F for the course. Faculty members are required to report all infractions to the Office of Student Conduct and Ethical Development. All quizzes and exams that a student submits will be checked by turn-it-in for plagiarism.

Accommodations

If you need a classroom accommodation for this class and have registered with the Accessible Education Center (https://www.sjsu.edu/aec/ (Links to an external site.)), please come see me earlier rather than later in the semester to give me a heads up on how to be of assistance. Your experience in this class is important to me. If you have already established accommodations with Student Accessibility Services, please communicate your approved accommodations to me at your earliest convenience so we can discuss your needs in this course.
Calendar: We will strictly follow the following SJSU calendar for add/drop/any other related deadlines; holidays; final exam schedule etc.

Follow the Calendar: https://www.sjsu.edu/registrar/calendar/spring-2026.php

Final Exam Schedule: https://www.sjsu.edu/classes/final-exam-schedule/spring-2026.php