San Jose State University
Department of Computer Science
CS 266, Topics in Information Security, Sec 1, Spring 2019

Course Outline

Course and Contact Information

Instructor:	Melody Moh
Office Location:	MQH 411
Telephone:	(408) 9245088
Email:	MyFirstName <dot> MyLastName <at> SJSU <dot> EDU
Office Hours:	Mon and Wed 1120 to 1150 and Wed 1330 to 1400
Class Days/Time:	MW 1200 to 1315
Classroom:	MQH 422
Prerequisites:	CS 166, CS 265, or instructor consent

Course Format Lecture

Faculty Web Page and MYSJSU Messaging (Optional)

Course materials such as syllabus, handouts, notes, assignment instructions, etc. can be found on my faculty web page http://www.cs.sjsu.edu/~melody/index.html
You are responsible for regularly checking with the email system through MySJSU at http://my.sjsu.edu to learn of any updates.

Course Description

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. Prerequisite: CS 166 or instructor consent. Repeatable for credit when topic changes. This semester, the topics will center around the applications of machine learning and deep learning in information security.

Course Learning Outcomes (CLO)

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

1. **CLO 1 -** Understand the covered topics through completion of homework, quizzes, and examinations.
2. **CLO 2 -** Successfully complete programming projects on advanced information security.
3. **CLO 3 -** Complete a term project, including independent research, oral presentation, and programming on a latest advancement in information security.

Required Texts/Readings

Required Textbooks

- *Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security*, ACM, Oct 2017.
  - https://dl.acm.org/citation.cfm?id=3128572
- *Proceedings of the 11th ACM Workshop on Artificial Intelligence and Security*, ACM, Oct 2018.

- https://dl.acm.org/citation.cfm?id=3270101

Optional Textbooks and References

- P. Tan, M. Steinbach, a. Karpatne, and V. Kumar, *Introduction to Data Mining*, 2nd ed., Pearson, 2018.
- William Stallings, "Cryptography and Network Security: Principles and Practice," 7th Edition, Pearson, 2017.
- Mark Stamp, Information Security: Principles and Practice, 2nd Edition, Wiley, 2011.
- Other references for specific topics/projects will be provided along with those topic/project assignments.

Course Requirements and Assignments

Homework is due (hard copy) 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.

ASSIGNMENTS

Refer the course website for latest information of assignments.

- **HQP**: Homework assignments, in-class quizzes, and classroom participation.
- **PROJ:** Several research and programming projects will span the entire semester
- **Oral Presentation:** Included in projects (PROJ)

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.

EXAMS

One mid-term exam (**Mid)** scheduled approximately at the end of 8th week, and a final exam (**FIN**).

Schedule

For continual updates of course schedule, please check the course schedule webpage available at http://www.cs.sjsu.edu/faculty/melody/266_19S_GS.html

CS 266 final exam is scheduled on Friday May 17, 0945-1200. Refer to the Spring semester final exam schedule, posted at http://info.sjsu.edu/static/catalog/final-exam-schedule-spring.html

Grading Policy

- *I will determine letter grades for the course, including +/- grades 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*

- *Percentage weight [or point value] assigned to various class assignments*

    - HQP - 20%, PROJ- 40%, Mid - 20%, FIN - 20%.
- *No make-up exams will be given and no late assignment will be accepted.*

NOTE that University policy F69-24 at http://www.sjsu.edu/senate/docs/F69-24.pdf states the following:

- *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.*

Classroom Protocol and Other Notes

1. **Always start your email subject with "CS266" to get my attention.**
2. The pre-requisite to this course (CS 166 or CS 265) will be monitored. Instructor consent may be obtained by having completed a course in machine learning, artificial intelligence, or related topics.
3. **Cheating** will not be tolerable; a ZERO will be given to any cheated assignment/exam, and will be reported to the Department and the University.
4. **Wireless laptop** is required. Your laptop must remain closed (preferably in your backpack and not on your desk) until you are informed that it is needed.
5. To encourage participation from students, no recording is allowed.
6. Students must be respectful of the instructor and other students. For example: turn off/silence **cell phones and other mobile devices**.
7. Attendance is crucial to doing well on assignments and examinations.
8. Students are responsible for all materials distributed and discussed in the class.
9. The instructor may decide to replace the final exam by a term paper. This will be communicated in class at least 2 weeks before the end of the instruction.
10. Office hours are on a 90% basis; they may be rescheduled or canceled due to conflicting department/university or other professional meetings.

University Policies

Per University Policy S16-9, university-wide policy information relevant to all courses, such as academic integrity, accommodations, etc. will be available on Office of Graduate and Undergraduate Programs' Syllabus Information web page at http://www.sjsu.edu/gup/syllabusinfo/

CS 266, Spring 2019, Course Schedule

The schedule is subject to change with fair notice; the notice will be made available in class.

Course Schedule

Weeks	Topics
1	Introduction to advance information security
2	Botnet detection in IoT networks
3	Anomaly detection
4	Log analysis
5	AI for detecting attacks
6	CAPTCHA: attacks and countermeasures with AI
7	Deep learning
8	Adversarial attacks and defenses of deep learning models
9	Authentication
10	Intrusion detection

11	Poisoning
12	Defense against poisoning
13	Malware
14	Malware analysis
15	Case studies
16	Review
Final Exam	9:45am on Friday May 17.