

San José State University
Department of Computer Science
CS 166 / SE 166, Information Security, Section 3, Spring, 2018

Course and Contact Information

Instructor:	Prakash Atawale
Office Location:	DH 282
Telephone:	
Email:	prakash.atawale@sjsu.edu
Office Hours:	Mondays 3.45pm-4.30pm, Wednesdays: 4:00pm-4.30pm
Class Days/Time:	Mondays and Wednesdays 4.30pm to 5.45pm
Classroom:	MH 223
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.

Course Description:

Fundamental security topics including cryptography, protocols, passwords, access control, software security, and network security. Additional topics selected from multilevel security, biometrics, tamper-resistant hardware, information warfare, e-commerce, system evaluation and assurance, and intrusion detection. Prerequisite: 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, or Software Engineering Majors only; or instructor consent.

Course Learning Outcomes:

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

Course Resources:

Textbook:

Manuscript, Information Security: Principles and Practice. Author: Mark Stamp. To be ordered in class on 1/24/2018 and to be picked up by the student from Maple press on Jan 31st.

Online:

We will be using **Canvas** for everything. Course materials such as slides, notes, homework etc. will be posted to Canvas. This is also the preferred way to communicate.

Computer and software:

Wireless laptop with fully charged battery. Student should have administrator access to the laptop.

Fully functioning Java Development Kit must be installed on the laptop. A cloud virtual machine instance hosted by Amazon Web Services is required to complete the course project.

Other Readings

- Java Cryptography Architecture reference guide. This is the official documentation from Oracle. Information provided here will be useful to complete the coding assignments.
<https://docs.oracle.com/javase/7/docs/technotes/guides/security/crypto/CryptoSpec.html>
- Java tutorial, security trail: <https://docs.oracle.com/javase/tutorial/security/index.html>
- *A Bug Hunter's Diary: A Guided Tour through the Wilds of Software Security*, Tobias Klein, No Starch Press, 2011. Lots of interesting real-world examples of vulnerable code.
- [Software Reverse Engineering \(SRE\)](#) website. This website, which was created by a former master's student, includes lots of good information and detailed exercises with solutions.
- *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.
- OWASP Top 10: powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are.
https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- *Computer Viruses and Malware*, John Ayccock, 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 Requirements and Assignments

This course requires you to complete tests, coding projects, weekly homework assignments, classroom assignments, quizzes and a final examination.

Grading Policy

1. Midterm test, 100 points
2. Homework: 100 points
3. Quizzes, class participation, and other work as assigned, 50 points.
4. Project: 50 points.
5. Final, 100 points.
6. Semester grade will be computed based on the percentage of the points earned.
7. **No** make-up tests or quizzes will be given and **no** late homework (or other work) will be accepted. Also, in-class work must be completed in the section that you are enrolled in.
8. Nominal Grading Scale:

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-
68 - 69	D+
62 - 67	D
60 - 61	D-
59 and below	F

- **Homework:** Homework is due *typewritten* (include source code, but not executable files) 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 be graded. Exact mechanism for submitting digital content will be communicated at the time homework is assigned.
- **Project:** Your project will dive deep into one of the topics you learn in this class. You are required to create original work related to your chosen information security topic. Coding, preferably using Java, is expected as a component of the project. Points will be based on the completed features, and achieved milestones, design documents, test cases created and other artifacts produced.

Classroom Protocol

I expect every student to be exemplary. Learn, and let others learn. Constructive participation and discussions are allowed.

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](http://www.sjsu.edu/gup/syllabusinfo/) at <http://www.sjsu.edu/gup/syllabusinfo/>

CS 166 / Information Security, Section 3, spring 2018, Course Schedule

Schedule is subject to change with fair notice. Notice will be made available in class and via Canvas.

Course Schedule

Week	Topics, Readings, Assignments, Deadlines
1 – 1/24	Introduction to cryptography
2 – 1/29, 1/31	Classic Crypto
3 – 2/5, 2/7	Symmetric Crypto
4 – 2/12, 14	Public Crypto
5 – 2/19, 2/21	Public Crypto

Week	Topics, Readings, Assignments, Deadlines
6 – 2/26, 2/28	Hash functions
7 – 3/5, 3/7	Authentication
8 – 3/12, 3/14	Access control
9 – 3/19, 3/21	Review, midterm
10 - Break	Spring Break
11 - 4/2, 4/4	Basic security protocols
12 – 4/9, 4/11	Real security protocols
13 – 4/16, 4/18	Malware
14 – 4/23, 4/25	Web application security
15 – 4/30, 5/2	Software reverse engineering
16 – 5/7, 5/9	Privacy in software, Secure software development
17 – 5/14	Review. Final project due.
5/16 Finals	2:45pm -5:00pm. Wed May 16, 2018. Room: MH 223. The official finals schedule is here: http://info.sjsu.edu/static/policies/final-exam-schedule-spring.html