San José State University
Science/Computer Science
CS 166, Information Security, Sections 3&5, Fall, 2018

Course and Contact Information

Instructor:	Ben Reed
Office Location:	MH 213
Telephone:	(408) 924-5174
Email:	ben.reed@sjsu.edu
Office Hours:	Monday & Wednesday 10:30-11:30, 3:00-4:00 Tuesday & Thursday 10:30-11:30, 1:00-2:00
Class Days/Time:	Tuesday & Thursday/ 3:00-4:15 (Section 5), 4:30-5:45 (Section 3)
Classroom:	DH 450
Prerequisites:	CS 146 (Data Structures & Algorithms) and either CS 47 or CMPE 102 or CMPE 120

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 (CLO)

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

1. Know the purposes of and the difference between symmetric and public key cryptosystems.
2. Know how cryptographic digests work and are used.
3. Know how PKI systems work.
4. Be familiar with various forms of cryptanalysis.
5. Understand the different types authentication and authorization systems and how they work together.
6. Know the phases of security protocols such as SSL, SSH, and Kerberos, and understand the different properties of those protocols.
7. Be familiar with various security vulnerabilities of modern software and hardware.

Required Texts/Readings

Textbook

We will use a manuscript that will eventually become the 3rd edition of the textbook **Information Security: Principles and Practice** by Mark Stamp. $35 will be collected in class from each student to do quick printing order.

Other technology requirements / equipment / material

Programming assignments will be a significant part of this course, so access to a computer with Java is required.

Course Requirements and Assignments

Homework will be given, but will not be graded. It is intended for self evaluation and will be the basis for future exams. I encourage students to work on homework in groups and discuss possible solutions together. We will take time at the beginning of each class to discuss any difficulties students have completing the homework.

It is anticipated that programming projects will be assigned each week on Tuesday during class, and will be due the following Monday at 5PM. Any assignments turned in late on the Monday it is due will have 10 points deducted from the final score. Any assignments turned in late after the Monday it is due will have 20 points deducted.

Programming assignments are not group projects. If students get help on assignments, even to resolve a stupid problem, it must be documented in the code with the name of the person rendering the help and a brief description of the help provided. Extensive help on a project will result in a reduced grade. Failure to document help, or any other forms of cheating will result in a failing grade on the assignment at a minimum and may result in failure of the course.

The University Policy S16-9, Course Syllabi (http://www.sjsu.edu/senate/docs/S16-9.pdf) requires the following language to be included in the syllabus:

“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

This course will have a cumulative final exam given during exam week.

Grading Information

Determination of Grades

Grades will be calculated by averaging the percentages of average of project grades, the two mid semester exams, and the final. Thus, the grade distribution is 25% project, 25% exam 1, 25% exam 2, 25% final exam.

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

Classroom Protocol

This is your class. Please ask questions. Please come prepared. Do not engage in activity that may distract other students.

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/" Make sure to review these policies and resources.

CS 166 / Information Security, Sections 3&5, Fall 2018 Course Schedule

Course Schedule

Week	Date	Topics, Readings, Assignments, Deadlines
1	8/21/2018	Chapter 1&2 Crypto Basics (Assignment 1)
1	8/23/2018	Chapter 1&2 Crypto Basics
2	8/28/2018	Chapter 3 Symmetric Key Crypto (Assignment 2)
2	8/30/2018	Chapter 3 Symmetric Key Crypto
3	9/4/2018	Chapter 4 Public Key Crypto (Assignment 3)

3	9/6/2018	Chapter 4 Public Key Crypto
4	9/11/2018	Chapter 5 Hash Functions & More (Assignment 4)
4	9/13/2018	Chapter 5 Hash Functions & More
5	9/18/2018	X.509 (Assignment 5)
5	9/20/2018	Document Signing
6	9/25/2018	Exam 1
6	9/27/2018	Collision Attacks
7	10/2/2018	Chapter 6 Cryptanalysis (Assignment 5)
7	10/4/2018	Chapter 6 Cryptanalysis
8	10/9/2018	Chapter 7 Authentication (Assignment 6)
8	10/11/2018	Chapter 7 Authentication
9	10/16/2018	Chapter 8 Authorization (Assignment 7)
9	10/18/2018	Chapter 8 Authorization
10	10/23/2018	Chapter 9 Simple Protocols (Assignment 8)
10	10/25/2018	Chapter 9 Simple Protocols
11	10/30/2018	Exam 2
11	11/1/2018	Digital Cash
12	11/6/2018	Chapter 10 Real World Protocols (Assignment 9)
12	11/8/2018	Chapter 10 Real World Protocols
13	11/13/2018	Chapter 10 Real World Protocols (Assignment 10)
13	11/15/2018	Chapter 10 Real World Protocols
14	11/20/2018	Chapter 11 Software Flaws
14	11/22/2018	Holiday
15	11/27/2018	Chapter 13 OS/App Security
15	11/29/2018	Chapter 13 OS/App Security
16	12/4/2018	Spectre/Meltdown/Row Hammer
16	12/6/2018	Review
Final Exam		Section 5: Monday, December 17 @ 2:45 Section 3: Friday, December 14 @ 2:45