

San Jose State University
Department of Computer Science
CS 166, Information Security, Section 5

Spring Semester, 2016

Course and Contact Information

Instructor:	Fabio Di Troia
Office Location:	DH282
Telephone:	
Email:	fabio.ditroia@sjsu.edu
Office Hours:	Monday 12:00-1:00pm and Friday 12:30-1:30pm
Class Days/Time:	Tuesday and Thursday, 12:00-1:15pm
Classroom:	MH 225
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.

- **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.

- **Required Texts/Readings**

- Textbook: *Information Security: Principles and Practice*, Mark Stamp
- Other useful resources:
 - *A Bug Hunter's Diary: A Guided Tour Through the Wilds of Software*

Security, Tobias Klein, No Starch Press, 2011.

- *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*, Michael Sikorski and Andrew Honig, No Starch Press, 2012.
- [Software Reverse Engineering \(SRE\)](http://reversingproject.info/) at <http://reversingproject.info/>.
- *Network Security: Private Communication in a Public World*, second edition, Charlie Kaufman, Radia Perlman, and Mike Speciner, Prentice Hall, 2002, ISBN: 0-13-046019-2.
- *Security Engineering: A Guide to Building Dependable Distributed Systems*, Ross Anderson, John Wiley & Sons, Inc., 2001, ISBN: 0-471-38922-6;
- *Security in Computing*, third edition, Charles P. Pfleeger and Shari Lawrence Pfleeger, Prentice Hall, 2003, ISBN: 0-13-035548-8.
- *Applied Cryptography: Protocols, Algorithms and Source Code in C*, second edition, Bruce Schneier, John Wiley & Sons, Inc., 1995, ISBN: 0-471-11709-9.
- *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses*, Ed Skoudis with Tom Liston, Prentice Hall, 2006, ISBN: 0-13-148104-5.
- *Computer Viruses and Malware*, John Aycock, Springer, 2006, ISBN: 0387302360.

- **Course Requirements and Assignments**

- 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 S12-3](http://www.sjsu.edu/senate/docs/S12-3.pdf) at <http://www.sjsu.edu/senate/docs/S12-3.pdf>.
- 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 typically be graded.

Assignment 1: Due **TBD**

Assignment 2: Due **TBD**

Assignment 3: Due **TBD**

Assignment 4: Due **TBD**

Assignment 5: Due **TBD**

Assignment 6: Due **TBD**

Assignment 7: Due **TBD**

Assignment 8: Due **TBD**

Assignment 9: Due **TBD**

Assignment 10: Due **TBD**

Assignment 11: Due **TBD**

Assignment 12: Due **TBD**

Assignment 13: Due **TBD**

- NOTE that [University policy F69-24](http://www.sjsu.edu/senate/docs/F69-24.pdf) 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."
- **Grading Policy**
 - Test 1, 100 points
 - Test 2, 100 points
 - Homework, quizzes, class participation, and other work as assigned, 100 points.
 - Final, 100 points

 - Semester grade will be computed as a weighted average of the 4 major scores listed above.
 - **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.

 - 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

- Note that "All students have the right, within a reasonable time, to know their academic scores, to review their grade-dependent work, and to be provided with explanations for the determination of their course grades." See [University Policy F13-1](http://www.sjsu.edu/senate/docs/F13-1.pdf) at <http://www.sjsu.edu/senate/docs/F13-1.pdf> for more details.
- **Classroom Protocol**
 - **Cheating** will not be tolerated, but working together is encouraged.
 - Student must be respectful of the instructor and other students. For example, No disruptive or annoying talking
 - Turn off cell phones Class begins on time
 - Valid picture ID required at all times
- **University Policies**
 - General Expectations, Rights and Responsibilities of the Student: As members of the academic community, students accept both the rights and responsibilities incumbent upon all members of the institution. Students are encouraged to familiarize themselves with SJSU's policies and practices pertaining to the procedures to follow if and when questions or concerns about a class arises. See [University Policy S90-5](http://www.sjsu.edu/senate/docs/S90-5.pdf) at <http://www.sjsu.edu/senate/docs/S90-5.pdf>. More detailed information on a variety of related topics is available in the SJSU catalog, at <http://info.sjsu.edu/web-dbgen/narr/catalog/rec-12234.12506.html>. In general, it is recommended that students begin by seeking clarification or discussing concerns with their instructor. If such conversation is not possible, or if it does not serve to address the issue, it is recommended that the student contact the Department Chair as a next step.
- Dropping and Adding:
 - Students are responsible for understanding the policies and procedures about add/drop, grade forgiveness, etc. Refer to the current semester's [Catalog Policies section](http://info.sjsu.edu/static/catalog/policies.html) at <http://info.sjsu.edu/static/catalog/policies.html>. Add/drop deadlines can be found on the current academic year calendars document on the [Academic Calendars webpage](http://www.sjsu.edu/provost/services/academic_calendars/) at http://www.sjsu.edu/provost/services/academic_calendars/. The [Late Drop Policy](http://www.sjsu.edu/aars/policies/latedrops/policy/) is available at <http://www.sjsu.edu/aars/policies/latedrops/policy/>. Students should be aware of the current deadlines and penalties for dropping classes. Information about the latest changes and news is available at the [Advising Hub](http://www.sjsu.edu/advising/) at <http://www.sjsu.edu/advising/>.
- Consent for Recording of Class and Public Sharing of Instructor Material: [University Policy S12-7](http://www.sjsu.edu/senate/docs/S12-7.pdf), <http://www.sjsu.edu/senate/docs/S12-7.pdf>, requires students to obtain instructor's permission to record the course and the following items to be included in the syllabus:

"Common courtesy and professional behavior dictate that you notify someone when you are recording him/her. You must obtain the instructor's permission to make audio or video recordings in this class. Such permission allows the recordings to be used for your private, study purposes only. The recordings are the intellectual property of the instructor; you have not been given any rights to reproduce or distribute the

material."

It is suggested that the greensheet include the instructor's process for granting permission, whether in writing or orally and whether for the whole semester or on a class by class basis.

In classes where active participation of students or guests may be on the recording, permission of those students or guests should be obtained as well.

"Course material developed by the instructor is the intellectual property of the instructor and cannot be shared publicly without his/her approval. You may not publicly share or upload instructor generated material for this course such as exam questions, lecture notes, or homework solutions without instructor consent."

- Academic integrity: Your commitment, as a student, to learning is evidenced by your enrollment at San Jose State University. The University [Academic Integrity Policy S07-2](http://www.sjsu.edu/senate/docs/S07-2.pdf) at <http://www.sjsu.edu/senate/docs/S07-2.pdf> requires you to be honest in all your academic course work. Faculty members are required to report all infractions to the office of Student Conduct and Ethical Development. The [Student Conduct and Ethical Development](http://www.sjsu.edu/studentconduct/) website is available at <http://www.sjsu.edu/studentconduct/>.
- Campus Policy in Compliance with the American Disabilities Act: If you need course adaptations or accommodations because of a disability, or if you need to make special arrangements in case the building must be evacuated, please make an appointment with me as soon as possible, or see me during office hours. [Presidential Directive 97-03](http://www.sjsu.edu/president/docs/directives/PD_1997-03.pdf) at http://www.sjsu.edu/president/docs/directives/PD_1997-03.pdf requires that students with disabilities requesting accommodations must register with the [Accessible Education Center](http://www.sjsu.edu/aec) (AEC) at <http://www.sjsu.edu/aec> to establish a record of their disability.

CS166 Information Security, Spring 2016, Course Schedule

This schedule is subject to change. Any change will be communicate via Canvas with fair notice.

Course Schedule

Week	Date	Topics, Readings, Assignments, Deadlines
1	1/28	Introduction and Crypto Basic
1	2/2	Crypto Basic
2	2/4	Symmetric Key Crypto
2	2/9	Symmetric Key Crypto
3	2/11	Public Key Crypto
3	2/16	Public Key Crypto
4	2/18	Hash Functions and Other Topics
4	2/23	Hash Functions and Other Topics
5	2/25	Hash Functions and Other Topics
5	3/1	Authentication
6	3/3	Authentication
6	3/8	Authorization
7	3/10	Authorization
7	3/15	MIDTERM
8	3/17	Simple Authentication Protocols
8	3/22	Simple Authentication Protocols
9	3/24	Simple Authentication Protocols
9	4/5	Real-World Security Protocols
10	4/7	Real-World Security Protocols
10	4/12	Real-World Security Protocols
11	4/14	Software Flaws and Malware
11	4/19	Software Flaws and Malware
12	4/21	Software Flaws and Malware
12	4/26	Insecurity in Software
13	4/28	Insecurity in Software
13	5/3	Insecurity in Software
14	5/5	Operating Systems and Security
14	5/10	Operating Systems and Security

Week	Date	Topics, Readings, Assignments, Deadlines
15	5/12	Operating Systems and Security
Final Exam	5/19	FINAL EXAM