San Jose State University
Department of Computer Science
CS 166, Information Security, Fall 2015

- **Course and Contact information**
  - **Instructor:** Mark Stamp
  - **Office Location:** MH 216
  - **Telephone:** 408-924-5094
  - **Email:** mark.stamp@sjsu.edu
  - **Office hours:** Tuesday 10:15-11:30am and 1:15-2:00pm
  - **Class Days/Times:** Tuesday and Thursday, 9:00-10:15am
  - **Classroom:** MH 422
  - **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: We will use a manuscript that will eventually become the 3rd edition of the textbook *Information Security: Principles and Practice*, Mark Stamp
  - Other useful resources:
    - *Software Reverse Engineering (SRE)* at http://reversingproject.info/. This website, which was created by a former masters student, includes lots of good information and detailed exercises with solutions.
0-13-046019-2. This book provides good coverage of cryptography and excellent coverage of several security protocols.


- **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. There are many books that claim to provide information on how to foil hackers, but this is by far the best that I have seen. This is an updated version of the original *Counter Hack*, published in 2001.


- Additional relevant material:
  - PowerPoint slides, errata, lecture videos, and other resources at http://www.cs.sjsu.edu/~stamp/infosec/
  - Previous semester lecture videos are available on YouTube at http://www.youtube.com/playlist?list=PLQEAkIf12JLOzrgaQOgF6S3PqXs2zR614
  - Current semester lecture videos are available at http://www.cs.sjsu.edu/~stamp/infosec/lectures/CS166_Fall15/. If you are asked to login to access the videos, both the username and password are "infosec". **Note:** The instructor hereby gives students permission to record his lectures (audio and/or video). At least with respect to this class, your instructor has nothing to hide.
  - Class-related discussion will be posted on Piazza at https://piazza.com/class/idjegsisou2vy. You are strongly encouraged to participate by asking questions, as well as by responding to questions that other students ask. At the start of the semester, you should receive an email asking you to join this discussion group—if not, contact your instructor via email.

- **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 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.

Zip your homework into a file named hmk.zip. Email your work to cs166.sjsu@gmail.com. The subject line of your email must be of the form:

CS166HMK assignmentnumber yourlastname last4digitofyourstudentnumber

That is, the subject line must consist of four identifiers. There is no space within an identifier and each identifier is separated by a space.

- Assignment 1: Due Thursday, August 27
  Chapter 1, problems 1, 9, 11, 13, 15, 17. The problems for Chapter 1 are available at http://www.cs.sjsu.edu/~stamp/other/chap1/probs1.pdf. Also, read each of the following and write a one-paragraph summary:
  - EBay asks 145 million users to change passwords after cyber attack at http://www.reuters.com/article/2014/05/21/us-ebay-password-idUSBREA4K0B420140521.

- Assignment 2: Due Thursday, September 3
  Chapter 2, problems 2, 5, 8, 9, 12, 15, 19, 22, 26, 28. Solve problem 12 before attempting problem 9, and use your program from problem 12 to help you solve 9.

- Assignment 3: Due Thursday, September 10
  Chapter 3, problems 3, 5, 6, 9, 11, 14, 19, 25, 27, 30, 31, 39a.

- Assignment 4: Due Thursday, September 17
  Chapter 4, problems 1, 2, 6, 8, 10, 15, 19a, 22, 25, 29, 30, 42a.

- Assignment 5: Due Thursday, September 24
  Chapter 5, problems 5, 12, 17, 21, 22, 25, 26, 27, 35, 42, 48.
■ Assignment 6: Due Thursday, October 15
Chapter 7, problems 10, 11, 13, 18, 26, 28, 29, 31, 32, 37, 38.

■ Assignment 7: Due Thursday, October 22
Chapter 8, problems 3, 7, 10, 11, 13, 15, 21, 24, 25.

■ Assignment 8: Due Tuesday, November 3
Chapter 9, Problems 4, 6, 16, 17, 18, 19, 20, 27, 36, and
1) Send a spoofed email to mark.stamp@sjsu.edu. Do not identify yourself in the
spoofed email. In your submitted solution include the contents of the spoofed email
and explain how you sent the email.
2) What are the inherent security strengths and weaknesses of stateless protocols,
as compared to stateful protocols (and vice versa)?
3) Provide a brief description of the IP "overlapping fragment attack" as discussed,
for example, in RFC 1858 at https://tools.ietf.org/html/rfc1858. How can such an
attack be prevented?
4) Recall the ARP cache poisoning attack discussed in class. How can you prevent
such an attack? Does your suggested prevention measure create any potential
vulnerability? Why or why not?
5) Read about a 2007 attack on the DNS root servers at https://www.icann.org
of the report. In your summary, be sure to mention how the attack packets were
successfully filtered.
6) Outline a DoS attack that exploits the TCP 3-way handshake. Discuss possible
defenses against such an attack and discuss possible countermeasures that Trudy
could use to circumvent your suggested defenses.

■ Assignment 9: Due Tuesday, November 24
Chapter 10, Problems 1, 10, 12, 14, 15, 16, 21, 22, 24, 26, 27a-d, 28a-d, 32, 35,
37a-c, 38, 41, 42.

■ Assignment 10: Due TBD

■ Assignment 11: Due TBD

■ Assignment 12: Due TBD

■ Assignment 13: Due TBD

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 Date: **Tuesday, September 29** Thursday, October 1
  - Test 2, 100 points Date: **Thursday, November 5**
  - Homework, quizzes, class participation, and other work as assigned, 100 points.
  - Final, 100 points
    - Date & time: **Thursday, December 10** from 7:15am-9:30am.
    - The is here: [official finals schedule](http://info.sjsu.edu/static/schedules/final-exam-schedule-fall.html)
  - 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:

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>92 and above</td>
<td>A</td>
</tr>
<tr>
<td>90 - 91</td>
<td>A-</td>
</tr>
<tr>
<td>88 - 89</td>
<td>B+</td>
</tr>
<tr>
<td>82 - 87</td>
<td>B</td>
</tr>
<tr>
<td>80 - 81</td>
<td>B-</td>
</tr>
<tr>
<td>78 - 79</td>
<td>C+</td>
</tr>
<tr>
<td>72 - 77</td>
<td>C</td>
</tr>
<tr>
<td>70 - 71</td>
<td>C-</td>
</tr>
<tr>
<td>68 - 69</td>
<td>D+</td>
</tr>
<tr>
<td>62 - 67</td>
<td>D</td>
</tr>
<tr>
<td>60 - 61</td>
<td>D-</td>
</tr>
<tr>
<td>59 and below</td>
<td>F</td>
</tr>
</tbody>
</table>

- 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) for more details.

- **Classroom Protocol**
  - [Keys to success](http://cs.sjsu.edu/~stamp/CS166/syllabus/success.html): Do the homework and attend class

  - **Wireless laptop is required.** Your laptop must remain closed (preferably in your
backpack and, in any case, not on your desk) until I inform you that it is needed for a particular activity.

- **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
  - Class is not over until I say it's over

- Valid picture ID required at all times.

- The last day to drop is **Tuesday, September 1**, and the last day to add is **Wednesday, September 9**

### 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 at [http://www.sjsu.edu/senate/docs/S90-5.pdf](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](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 at [http://info.sjsu.edu/static/catalog/policies.html](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 at [http://www.sjsu.edu/provost/servicesacademic_calendars/.](http://www.sjsu.edu/provost/servicesacademic_calendars/) The Late Drop Policy is available at [http://www.sjsu.edu/aars/policieslatedrops/policy/](http://www.sjsu.edu/aars/policieslatedrops/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 at [http://www.sjsu.edu/advising/](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 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 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 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 (AEC) at http://www.sjsu.edu/aec to establish a record of their disability.