San Jose State University
Department of Computer Science
CS 266, Topics in 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, noon-1:15pm
  - **Classroom:** MH 422
  - **Prerequisites:** CS 166 or instructor consent

- **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.

- **Learning Outcomes**
  - After completing this course you should be knowledgeable concerning the major technical security challenges related to malware. In addition, you should be knowledgeable of various machine learning techniques, and have a deep understanding of the application of such techniques to select challenges in information security.

- **Required Texts/Readings**
  - Computer Viruses and Malware, John Aycock, Springer 2006,

  - We will also use a manuscript written by your instructor. This manuscript, titled ***Machine Learning with Applications in Information Security***, covers many machine learning concepts, mostly in the context of malware.

  - Other useful resources:
    - Open Malware at http://www.offensivecomputing.net/ has a large collection of samples of live malware.
    - VX Heavens (i.e., Virus eXchange) at http://vx.netlux.org/ is a source for "hacker" information on viruses and malware samples.
    - Journal of Computer Virology and Hacking Techniques at http://www.springer.com/computer/journal/11416 is a journal for malware-specific research papers. There are several good conferences too, including Malcon 2015 at http://isiom.wssrl.org/.
    - ***Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software***, Michael Sikorski and Andrew Honig, No Starch Press, 2012. An excellent book for information on reverse engineering (whether for malware

analysis or other purposes). Includes many hands-on exercises.
    - Software Reverse Engineering (SRE) website at http://reversingproject.info/. This website, which was created by a former masters student, includes lots of good information and detailed exercises with solutions.
    - ***Security in Computing***, third edition, Charles P. Pfleeger and Shari Lawrence Pfleeger, Prentice Hall, 2003, ISBN: 0-13-035548-8. The strength of this book is its coverage of the security issues related to software. In particular, operating systems and some aspects of secure software engineering are covered well. This book also has some good basic information on viruses.
    - Recent masters project reports are at http://www.cs.sjsu.edu/~stamp /cv/mss.html#masters. Many of which deal with malware-related topics.

- Additional relevant material:
    - PowerPoint slides and other resources are available at http://www.cs.sjsu.edu /faculty/stamp/CS266/ppt.
    - Lecture videos are available at http://www.cs.sjsu.edu/~stamp/infosec/lectures /CS266_Fall15/. **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 /idjeiu4sdnb5pr. 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 cs266.at.sjsu@gmail.com. The subject line of your email ***must*** be of the form:

      ```
      CS266HMK 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 TBD
  Create two examples of "parasitic code". Your code must satisfy the following requirements.
  - The code must be written in C/C++ and/or assembly.
  - The code must infect exe files on Windows. However, your code need not be capable of infecting all Windows executables. (With the instructor's permission, you may work on Mac OS or a specific flavor of Linux instead.)
  - Your parasitic code can infect an exe only through a "dropper" program. That is, the parasitic code itself does not infect additional files. Also, the dropper program can only infect one specified file at a time.
  - When the exe containing your parasitic code is executed, it must append the line "You're infected" to a file called "infections.txt" which resides in the same directory as the infected file. Your parasitic code cannot perform any other meaningful function. Furthermore, the infected exe must still execute normally.
  - Your dropper program must be able to detect whether an exe is infected or not, so that it does not try to re-infect files that are already infected.
  - You need to create 2 version of your parasitic code. The 2 versions must be identical in function---the only difference is that one is encrypted and/or highly obfuscated, and one is not.
  - All of your code must be written by you, and you must understand every line of your code. You can look at other examples of parasitic code for ideas, but you cannot copy such code.
  - You may work with a partner on this assignment. If you do, both partners must contribute to the assignment, and both must completely understand the code and all other material that is submitted.
  - For the next assignment, you will give another team a set of exe files, some of which are infected, along with an exe corresponding to your parasitic code. That team will try to detect and remove the infections. Your score on this project will depend, in part, on how difficult it is for the other team to detect your parasitic code and disinfect the infected exe files.

- Assignment 2: Due Thursday September 17
  Chapter 1, problems 1, 2, 3, 9, 10. For problem 9, you need to write the HMM program entirely on your own, based on the pseudo-code given in Section 2.7, and to test your program, use the English text found in the Brown Corpus. For problem 10, use this ciphertext and you can use this A matrix.

- Assignment 3: Due Thursday September 24
  Chapter 2, problems 3, 4, 6b. Extra credit for problem 5a. If you solve 5a, use uniform probabilities for the "random model", i.e., the q_{xi} that appear in the forward algorithm recursive relations on p. 47.

- Assignment 4: Due Thursday October 1

Chapter 8, Problems 1, 2, 4, 5, 6, 7.

- Assignment 5: Due Thursday October 15
  Chapter 4, Problems 1, 2, 3, 4.
- Assignment 6: Due Thursday October 22
  Chapter 5, Problems 1, 3, 4, 5, 8.
- Assignment 7: Due Thursday ~~November 5~~ November 12
  Chapter 6, Problems 2, 4, 5, 7, 8, 10, 14.
- Assignment 8: Due TBD
- Assignment 9: Due TBD
- Assignment 10: Due TBD

  - NOTE that University policy F69-24 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. Date: TBD.
  - Homework, quizzes, class participation and other work as assigned, 100 points. A subset of the assigned problems will be graded.
  - Malware Project, 100 points. You must obtain approval for your project (via email) by October 9. A written project report is due December 1. Note that a written report is required, and oral presentations will begin on (or shortly after) the report due date.
  - Final, 100 points. Date: Friday, December 11 from 9:45am-noon. The official finals schedule is here: http://info.sjsu.edu/static/schedules/final-exam-schedule-fall.html
  - Semester grade will be computed as a weighted average of the major scores listed above.
  - ***No*** make-up tests or quizzes will be given, ***no*** late homework or project (or other work) will be accepted.
  - 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 at http://www.sjsu.edu/senate/docs/F13-1.pdf for more details.

- **Classroom Protocol**
  - Keys to success at 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. 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 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 at http://www.sjsu.edu/provost/services/academic_calendars/. The Late Drop 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 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, 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.