San Jose State University
Department of Computer Science
CS 265, Section 1, Cryptography and Computer Security, Spring 2017

- **Course and Contact information**
  - **Instructor:** Mark Stamp
  - **Office Location:** MH 216
  - **Telephone:** 408-924-5094
  - **Email:** mark.stamp@sjsu.edu
  - **Office hours:** Tuesday and Thursday, noon-1:00pm
  - **Class Days/Times:** Tuesday and Thursday, 10:30-11:45am
  - **Classroom:** MH 225
  - **Prerequisites:** CS 149 or instructor consent.

- **Course Description**
  - We will cover selected security topics in each of the following areas: cryptography, access control, protocols, and software.

- **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:**
    - ***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.
    - ***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. This website, which was created by a former masters student, includes lots of good information and detailed exercises with solutions.
    - ***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. This book provides good coverage of cryptography and excellent coverage of several security protocols.
    - ***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.

- ***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.
- ***Applied Cryptography: Protocols, Algorithms and Source Code in C***, second edition, Bruce Schneier, John Wiley & Sons, Inc., 1995, ISBN: 0-471-11709-9. For better or for worse, in industry, this is *the* standard reference for all things cryptographic.
- ***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.
- ***Computer Viruses and Malware***, John Aycock, 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.

- 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 You Tube at http://www.youtube.com/playlist?list=PLQEAKfSI2JLOzrgaQOgF6S3PqXs2zR614
  - Current semester lecture videos are available at http://www.cs.sjsu.edu/~stamp/infosec/lectures/CS265_Spr17/. 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 http://piazza.com/sjsu/spring2017/cs265/home. 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.

  - Schedule
    - Week 1 --- Introduction and overview

- Week 2 --- Crypto basics
- Week 3 --- Symmetric key cryptography
- Week 4 --- Public key cryptography
- Week 5 --- Cryptographic hash function and related topics
- Week 6 --- Review and first midterm
- Week 7 --- Authentication
- Week 8 --- Authorization
- Week 9 --- Network security basics
- Week 10 --- Simple authentication protocols
- Week 11 --- Review and second midterm
- Week 12 --- Real-world security protocols
- Week 13 --- Software flaws and malware
- Week 14 --- Additional software security topics
- Week 15 --- Project presentations

- 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 cs265.sjsu.spr17@gmail.com. The subject line of your email ***must*** be of the form:

  ```
  CS265HMK 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, February 2
    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.
    Read the first 10 pages of PoS RAM Scraper Malware at http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-pos-ram-scraper-malware.pdf. Then read a section on one of the "PoS RAM Scraper Families" and write a one-paragraph description. Finally, do the same for one of the "Next-Generation PoS RAM Scrapers".

  - Assignment 2: Due TBD
    Chapter 2, problems TBD

  - Assignment 3: Due TBD
    Chapter 3, problems TBD

  - Assignment 4: Due TBD
    Chapter 4, problems TBD

  - Assignment 5: Due TBD
    Chapter 5, problems TBD

        - Assignment 6: Due TBD
          Chapter 6, problems TBD
        - Assignment 7: Due TBD
          Chapter 7, problems TBD
        - Assignment 8: Due TBD
          Chapter 8, problems TBD
        - Assignment 9: Due TBD
          Chapter 9, problems TBD
        - Assignment 10: Due TBD
          Chapter 10, problems TBD
        - Assignment 11: Due TBD
          Chapter 10, problems TBD
        - Assignment 12: Due TBD
          Chapter 11, problems TBD
          Chapter 12, problems TBD
        - Assignment 13: Due Varies
          Attend one (or more) of the master's defenses listed at http://cs.sjsu.edu/~stamp/defenses/spring17.html
    - 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
    - Test 2, 100 points Date: TBD
    - Homework, quizzes, class participation and other work as assigned, 50 points.
    - Cryptanalysis Project, 100 points. Your project topic is due Friday, February 5 and the completed project is due Friday, March 18. Note that a written report is required, but no oral report.
    - SRE Project, 50 points. Your project topic is due Friday, March 31 and the completed project is due Tuesday, May 2. Presentations will be given beginning on the due date. Note that an oral report is required, but no written report.
    - Final, 100 points
        - Date & time: Monday, May 22 from 9:45am-noon
        - The official finals schedule is here: http://info.sjsu.edu/static/catalog/final-exam-schedule-spring.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 and ***no*** late homework or project (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 at http://www.sjsu.edu/senate/docs/F13-1.pdf for more details.

- **Classroom Protocol**
  - Keys to success: 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, February 7, and the last day to add is Tuesday, February 14

- **University Policies**
  - Office of Graduate and Undergraduate Programs maintains university-wide policy information relevant to all courses, such as academic integrity, accommodations, etc. You may find all syllabus related university policies and resources information listed on GUP's Syllabus Information web page at http://www.sjsu.edu/gup/syllabusinfo/