San Jose State University
Department of Computer Science
CS 166, Information Security, Spring 2024

- **Course and Contact information**
  - **Instructor:** Mark Stamp
  - **Office Location:** MH 216
  - **Telephone:** 408-924-5094
  - **Email:** mark.stamp@sjsu.edu
  - **Text:** for oh ate fore owe to 10-five-too
  - **Office hours:**
    - Tuesday & Thursday, 2:00-2:30pm, Zoom: https://sjsu.zoom.us/j/81394314643?pwd=cGhCeis1U3E3NzloUG5nbTgxRkhzZz09
    - Friday, 10:00 - 11:00am, in-person
    - or by appointment
  - **Class Days/Times:** Tuesday and Thursday, Noon-1:15pm
  - **Classroom:** BBC 202
  - **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 the textbook *Information Security: Principles and Practice*, 3rd edition, Mark Stamp, Wiley, 2021. Be sure to get the 3rd edition, and do *not* attempt to use the e-book version.

  - Other useful resources:
    - *Introduction to Machine Learning with Applications in Information Security*, 2nd edition, Mark Stamp, Chapman and Hall/CRC, 2022. A timely book by one of my favorite authors.
    - *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.
    - 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.
    - *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 some cryptography basics and excellent coverage of several security protocols.
    - *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3rd edition, Ross Anderson, John Wiley & Sons, Inc., 2020. This is an excellent book for an overview of security in general, but it is generally not too focused or technically detailed.

- **_Computer Viruses and Malware_**, John Aycock, Springer, 2006. 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, and other resources at http://www.cs.sjsu.edu/~stamp/infosec/
  - Current semester lecture videos are available at http://www.cs.sjsu.edu/~stamp/infosec/lectures/CS166_Spr24/. 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 Campuswire at https://campuswire.com/c/G440BA989/feed. 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 additional 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 --- Review for final

  - 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 _all_ 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.

    Your written solutions must be submitted in a pdf file. Submit any source code or other attachments in separate files (i.e., no code within the solution itself). You must provide enough explanation of your solution so that the grader can understand what you did and why, and so that the grader can be sure that you understand your solution. Put your written solution and any relevant source code in a folder named "yourlastname". Then zip your homework folder and submit the file yourlastname.zip via email to CS166.spring24@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 Tuesday, January 30
  Chapter 1, problems 2, 5, 6, 7, 9, 12, 13.
  Chapter 1 is available at http://www.cs.sjsu.edu/~stamp/CS166/files/Chapter1.pdf

- Assignment 2: Due Tuesday, February 6
  Chapter 2, problems 1, 5, 7, 11, 18, 19, 21, 23. Extra credit: 13

- Assignment 3: Due Thursday, February 15
  Chapter 3, problems 3, 7, 10, 12, 16, 20, 21, 24, 31, 32. Your code for problem 7 must be written in some version of the C programming language (C, C++, C#, etc.).

- 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 11, problems TBD

- Assignment 12: Due TBD
  Chapter 12, problems TBD

- Assignment 13: Due Varies
  Attend at least one of the Master's student defenses listed at
  http://www.cs.sjsu.edu/faculty/stamp/defenses/spr24.html. You can attend a second defense for extra credit.

- 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, 100 points.
    - Final, 100 points
        - Date & time: Monday, May 20 from 9:45am - noon.
        - The [official finals schedule](#) is at https://www.sjsu.edu/classes/final-exam-schedule/spring-2024.php
    - 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](#) 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 your instructor informs 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 your instructor says it's over

    - Valid picture ID required at all times

    - The last day to drop is Monday, February 19, and the last day to add is Monday, February 19

- **College and 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](http://www.sjsu.edu/gup/syllabusinfo/) at http://www.sjsu.edu/gup/syllabusinfo/