San José State University
School/Department
CS 166 Section 02, Information Security, Spring, 2021

Course and Contact Information

Instructor: Sanjoy Paul

Office Location: [TBD]

Telephone: (832) 805-4877

Email: paul.sanjoy@sjtu.edu

Office Hours: [TBD]

Class Days/Time: TuTh: 18:00-19:15 PST

Classroom: Zoom

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

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.


Approximate schedule (3 hours equals 1 week of class time):
  - Introduction
    - Chapter 1 (1 hour)
  - Crypto
    - Chapter 2: Crypto Basics (3 hours)
    - Chapter 3: Symmetric Key Crypto (4 hours)
    - Chapter 4: Public Key Crypto (4 hours)
    - Chapter 5: Hash Functions and Other Topics (4 hours)
  - Access Control
    - Chapter 7: Authentication (4 hours)
- Chapter 8: Authorization (2 hour)
  - Protocols
  - Chapter 9: Simple Authentication Protocols (4 hours)
  - Chapter 10: Real-World Security Protocols (5 hours)

- Software
  - Chapter 11: Software Flaws and Malware (4 hours)
  - Chapter 12: Insecurity in Software (4 hours)
  - Chapter 13: Operating Systems and Security (4 hours)

- Note: Due to time constraints, we omit Chapter 6 and various parts of the last three chapters.

- Some useful resources are given below and many more will be provided on an ongoing basis:
  - 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.
  - 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.
Course Format

Technology Intensive, Hybrid, and Online Courses

This course will be taught online. You need Internet connectivity and zoom installed on your computer to participate in the classroom activities and/or submit assignments. You need to have a Python software development environment installed on your computer to do the projects.

Course Description

This course will cover selected security topics in each of the following areas: cryptography, access control, protocols, and software.

Course Learning Outcomes

Upon successful completion of this course, you should be knowledgeable of the major technical security challenges in each of the following areas: cryptography, access control, protocols, and software.

Other technology requirements / equipment / material

We will use Zoom for our online sessions

Installing Zoom

https://www.youtube.com/watch?v=fVu9BIIRkww
Course Requirements and Assignments

Homework Assignments:
Homework assignments will be posted and submitted on Canvas. For full credit, they must be submitted by the posted due date.

Weekly Quizzes:
We will have a weekly quiz aimed at checking your understanding of the previous week's material. I will count the 10 best scores out of the 12 total quizzes in the semester. You must be in the online classroom to take the quiz. Missed quizzes cannot be made up.

Midterm Exam:
The midterm exam will take place in the classroom during class time on Tuesday March 16 during regular class hours.

Final Exam:
The final exam will take place on Tuesday May 25 – 19:45-22:00

Grading Information
The final grade in the course will be calculated based on the following percentages:
Homework Assignments: 30%
Weekly Quizzes: 20%
Midterm: 20%
Final Exam: 30%

Late Work:
Late assignments will not be accepted.
Grade Scale:

The letter grade will be determined based on the following scale:

- A+ = 96% - 100%
- A  = 91% - 95%
- A- = 86% - 90%
- B+ = 81% - 85%
- B  = 76% - 80%
- B- = 71% - 75%
- C+ = 66% - 70%
- C  = 61% - 65%
- C- = 56% - 60%
- D  = 51% - 55%
- F  = below 50

Classroom Protocol

Regular attendance is an integral part of the learning process. Please arrive on time for the classes.

University Policies

Per University Policy S16-9 (http://www.sjsu.edu/senate/docs/S16-9.pdf), relevant information to all courses, such as academic integrity, accommodations, dropping and adding, consent for recording of class, etc. is available on Office of Graduate and Undergraduate Programs’ Syllabus Information web page at http://www.sjsu.edu/gup/syllabusinfo/”. Make sure to visit this page, review and be familiar with these university policies and resources.
### CS166 Information Security, Spring, 2021, Course Schedule

Please note that this schedule is subject to change with fair notice. Any changes will be announced in class and posted on the Canvas course site.

#### Course Schedule

<table>
<thead>
<tr>
<th>Week</th>
<th>Date</th>
<th>Topics</th>
<th>Readings (Textbook)</th>
<th>HW Due date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jan 28</td>
<td>Introduction + Overview of the Course</td>
<td>Chapter 1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Feb 2</td>
<td>Overview of the Course continued + Crypto Basics I</td>
<td>Chapter 2</td>
<td>HW1 Feb 10</td>
</tr>
<tr>
<td>2</td>
<td>Feb 4</td>
<td>Crypto Basics II</td>
<td>Chapter 2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Feb 9</td>
<td>Symmetric Key Crypto I</td>
<td>Chapter 3</td>
<td>Quiz#1</td>
</tr>
<tr>
<td>3</td>
<td>Feb 11</td>
<td>Symmetric Key Crypto II</td>
<td>Chapter 3</td>
<td>HW2 Feb 24</td>
</tr>
<tr>
<td>4</td>
<td>Feb 16</td>
<td>Symmetric Key Crypto III</td>
<td>Chapter 3</td>
<td>Quiz#2</td>
</tr>
<tr>
<td>4</td>
<td>Feb 18</td>
<td>Public Key Crypto I</td>
<td>Chapter 4</td>
<td>HW3 Mar 3</td>
</tr>
<tr>
<td>5</td>
<td>Feb 23</td>
<td>Public Key Crypto II</td>
<td>Chapter 4</td>
<td>Quiz#3</td>
</tr>
<tr>
<td>5</td>
<td>Feb 25</td>
<td>Public Key Crypto III</td>
<td>Chapter 4</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Mar 2</td>
<td>Hash Function &amp; Other topics I</td>
<td>Chapter 5</td>
<td>Quiz#4</td>
</tr>
<tr>
<td>6</td>
<td>Mar 4</td>
<td>Hash Function &amp; Other topics II</td>
<td>Chapter 5</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Mar 9</td>
<td>Authentication I</td>
<td>Chapter 7</td>
<td>Quiz#5</td>
</tr>
<tr>
<td>7</td>
<td>Mar 11</td>
<td>Authentication II</td>
<td>Chapter 7</td>
<td>HW6 Mar 24</td>
</tr>
<tr>
<td>8</td>
<td>Mar 16</td>
<td>Authentication III</td>
<td>Chapter 7</td>
<td>Quiz#6</td>
</tr>
<tr>
<td>8</td>
<td>Mar 18</td>
<td>Midterm</td>
<td>Chapter 8</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Mar 23</td>
<td>Authorization I</td>
<td>Chapter 8</td>
<td>HW7 Apr 5</td>
</tr>
<tr>
<td>9</td>
<td>Mar 25</td>
<td>Authorization II</td>
<td>Chapter 8</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Mar 30</td>
<td>Simple Authentication Protocols I</td>
<td>Chapter 9</td>
<td>Quiz#7</td>
</tr>
<tr>
<td>10</td>
<td>Apr 1</td>
<td>Simple Authentication Protocols II</td>
<td>Chapter 9</td>
<td>HW8 Apr 14</td>
</tr>
<tr>
<td>11</td>
<td>Apr 6</td>
<td>Simple Authentication Protocols III</td>
<td>Chapter 9</td>
<td>Quiz#8</td>
</tr>
<tr>
<td>11</td>
<td>Apr 8</td>
<td>Real-world Security Protocols I</td>
<td>Chapter 10</td>
<td>HW9 Apr 21</td>
</tr>
<tr>
<td>12</td>
<td>Apr 13</td>
<td>Real-world Security Protocols II</td>
<td>Chapter 10</td>
<td>Quiz#9</td>
</tr>
<tr>
<td>12</td>
<td>Apr 15</td>
<td>Real-world Security Protocols III</td>
<td>Chapter 10</td>
<td>HW10 Apr 28</td>
</tr>
<tr>
<td>13</td>
<td>Apr 20</td>
<td>Software Flaws and Malware I</td>
<td>Chapter 11</td>
<td>Quiz#10</td>
</tr>
<tr>
<td>13</td>
<td>Apr 22</td>
<td>Software Flaws and Malware II</td>
<td>Chapters 11</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Apr 27</td>
<td>Software Flaws and Malware III</td>
<td>Chapters 11</td>
<td>Quiz#11</td>
</tr>
<tr>
<td>14</td>
<td>Apr 29</td>
<td>Insecurity in Software I</td>
<td>Chapters 12</td>
<td>HW11 May 13</td>
</tr>
<tr>
<td>15</td>
<td>May 4</td>
<td>Insecurity in Software II</td>
<td>Chapter 12</td>
<td>Quiz#12</td>
</tr>
<tr>
<td>15</td>
<td>May 6</td>
<td>Operating Systems and Security I</td>
<td>Chapter 13</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Date</td>
<td>Course</td>
<td>Chapter</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>-----------</td>
<td>---------------------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>May 11</td>
<td>Operating Systems and Security II</td>
<td>Chapter 13</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>May 13</td>
<td>Operating Systems and Security III</td>
<td>Chapter 13</td>
<td></td>
</tr>
<tr>
<td>Final</td>
<td>May 25</td>
<td>FINAL EXAM</td>
<td>19:45-22:00</td>
<td></td>
</tr>
</tbody>
</table>