CSC/CPE 556 Computer Security

1. CSC/CPE 556 Computer Security

2. credit units 4 contact hours 6

3. Course Coordinator: Phillip Nico


5. a. Course Description: CSC 556 Computer Security (4) (Also listed as CPE 556) Exploration of advanced topics in computer security with an emphasis on research topics. 3 lectures, 1 laboratory.

b. Prerequisite: CSC/CPE 456 and graduate standing, or consent of instructor.

c. Required/Elective/Selective Elective for CPE, CSC, EE, SE

<table>
<thead>
<tr>
<th>Required</th>
<th>CPE</th>
<th>CSC</th>
<th>SE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elective</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Selective Elective</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

6. a. Course Goals/Outcomes
The student will be able to:

- Become familiar with several areas of current Computer Security research and methods.
- Become familiar with the professional literature relating to Computer Security.
- Gain an in-depth understanding of one of the fundamental topics of Computer Security by participating in a small group charged with presenting that topic to the class and leading a discussion.
- Develop their skills as researchers by pursuing an (instructor-guided) independent research project in a current research area of Computer Security.
- Improve oral and written communication skills by preparing a report on the results of the project and presenting those results to the class in a mock conference talk.

b. How Student Outcomes addressed
(“B” = Basic level, “I” = Intermediate level, “A” = Advanced level)

<table>
<thead>
<tr>
<th></th>
<th>3a</th>
<th>3b</th>
<th>3c</th>
<th>3d</th>
<th>3e</th>
<th>3f</th>
<th>3g</th>
<th>3h</th>
<th>3i</th>
<th>3j</th>
<th>3k</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSC</td>
<td>A</td>
<td>A</td>
<td></td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>SE/</td>
<td>A</td>
<td>A</td>
<td></td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td></td>
<td></td>
<td>A</td>
</tr>
<tr>
<td>CPE</td>
<td>A</td>
<td>A</td>
<td></td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td>A</td>
</tr>
</tbody>
</table>
7. Major Topics Covered: (number of lecture hours each)

- Provide a detailed week-by-week outline (you may include readings, discussion topics, lab experiments, activities, assignments, etc.) For courses with multiple sections, faculty and/or courses with different subtitles, describe the consistent principles or key elements that will be common to all sections. For a course with different subtitles, please provide a representative sample of a syllabus.

If course is proposed for General Education, refer to GE criteria and identify GE objectives and criteria here.
If course is proposed for U. S. Cultural Pluralism, refer to USCP criteria and identify USCP content here.

This course will provide an overview of both historical and current Computer Security research and practice in a student-driven manner. After an introductory period of two weeks, the students will be divided into groups and each group will be assigned one of the topic areas below. The groups will be responsible for investigating that area (with instructor guidance) and presenting it to the class in the form of a 50 minute class presentation.

Although the readings below are taken from Matt Bishop's textbook (Bishop, M., Computer Security: Art and Science. Addison-Wesley, 2002), they are intended as guides to topics. Student presentations will be expected to rely on primary sources in the computer security literature, including some recent ones.

The lab for the course will consist of a quarter-long project where student groups will be asked to take some work from a current conference proceedings or journal article and either reproduce or extend it, ultimately presenting the results in a mock conference talk at the end of the quarter. The in-class portion of the lab will be guidance for and presentation of these projects.

Lecture Topics:

Week 1) Introduction to Computer Security, Trust, and Risk Analysis (Bishop 1, 13, 29.5)
Week 2) Discussion of research and presentation methods, assignment of group topics and demonstration presentation of a topic area. A likely example will be the seminal paper: J. H. Saltzer and M. D. Schroeder, The Protection of Information in Computer Systems. 63(9):1278--1308, September 1975.
Week 3) Authentication and Access Control (Bishop 2, 12, 14, 15.1, 28.2)
Week 4) Authentication attacks, Unix access control, Access Control Lists  (Bishop 2, 15.1)
Week 5) Capabilities and Mandatory Access Controls  (Bishop 5, 15.2-15.5)
Week 6) Malicious Logic, Sandboxing, and Integrity Checking (Bishop 6, 17.1-2, 22)
Week 7) Role of Trust, Denial of Service (Availability) (Bishop 4.3)
Week 8) Security Policy, Information Flow (Lattice model), Integrity (Bishop 4, 6, 7, 16)
Week 9) Network-based attacks, Vulnerabilities and Threats (Bishop 23)
Week 10) Intrusion Detection, Covert Channels (Bishop 17.3, 25)