I. Course Title: Web Programming and Security

II. Course Prefix/Number: CSCI 245

III. Credit Hours: 4.0

IV. Prerequisite(s):

Passing the ASC Technology Proficiency Examination OR Bus 120 minimum grade C- OR CSCI 100 minimum grade C- OR CSCI 208 minimum grade C-

V. Catalog Description:

Covers basic aspects of the internet, focusing on web programming and application layer computer security. No programming background is required. Students will learn how to write a web application using both client- and server-side scripting languages. Students will also participate in activities involving hacking and defending web applications.

VI. Curricular Relationships:

This course is required of students majoring in Mathematics with a Computer Science Emphasis, students obtaining an associate degree with an emphasis in Internet Computing and Security, and of students obtaining the Communications Technology minor. It will also be of interest to students (both majors and non-majors) wishing to acquire web programming skills and to in-depth understanding of web application hacking and security techniques.
VII. Student Learning Outcomes:

- Students will demonstrate a basic understanding of the Internet including application layer standards and protocols.

- Students will be able to program a web application using HTML, CSS, and both a client-side and server-side scripting language. Students will be familiar with and be able to write programs that comply with standards for web accessibility.

- Students will understand web programming security issues including major web application hacking techniques and how to program defensively.

- Students will be able to describe and implement the major features of web security. In particular, they will be able to
  - Implement SSL/TLS and the associated HTTPS protocol.
  - Use PKI certificates to secure authentication and the transmission of data.

- Students will be familiar with legal issues surrounding the World Wide Web including hacking, privacy, and copyright protection.

VIII. Content Outline:

1. History of the internet with an emphasis on how its history relates to computer security issues.

2. Application layer protocols

3. Web security
   a. Web application attacks and defenses including authentication, access control, session management, code injection, cross-site scripting, flaws in application logic, and path traversal vulnerabilities
   b. Web attack and security tools
   c. Trade-offs between security and usability
   d. Implementing SSL/TLS and the HTTPS protocol
   e. PKI certificates
   f. Application auditing and logging

4. The web as an example of client-server computing

5. Client- and server-side web application development skills
a. HTML and CSS
   i. Web accessibility standards and programming
b. Client-side Scripting and AJAX
c. Server-side Scripting
d. Introduction to database design and implementation

6. Web user-interface design
7. Software tools and environments
8. Legal and privacy issues
   a. Cookies and other web-based threats to privacy
   b. Legal and ethical aspects of hacking
   c. Copyright protection

9. Elective topics

IX. Course Procedures/Policies/Grading Scale:

- Regular homework assignments may be a component of the course grade.
- At least three examinations are given each semester.
- A comprehensive final examination is given during finals week.
- Computer projects are a component in determining the course grade.

X. Required/Recommended Readings:

Whether a textbook is used with the course will depend on the instructor and the specific client-side and server-side programming languages used in the course. Because web programming languages and security are rapidly evolving subjects, the instructor may find internet sources to be more up-to-date and relevant than a textbook. Example text books include:


XI. Issues Unique to Course:

Students are expected to spend additional time in the computer lab.

XII. Additional Departmental Issues:

This course addresses the topics listed in the CS body of knowledge core as described in the ACM/IEEE document *Computer Science Curriculum 2008: An Interim Revision of CS 2001, Report from the Interim Review Task Force*. The course includes topics from the following core areas: NC (Net-Centric Computing), NC (Human-Computer Interaction), and SE (Software Engineering), SP (Social and Professional Issues), IM (Information Management), PF (Programming Fundamentals), and PL (Programming Languages).

<table>
<thead>
<tr>
<th>Knowledge Area</th>
<th>Topic</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>NC</td>
<td>Introduction</td>
<td>2 core hours</td>
</tr>
<tr>
<td>NC</td>
<td>Network security</td>
<td>5 core hours (of 6)</td>
</tr>
<tr>
<td>NC</td>
<td>Networked Applications</td>
<td>24 elective hours</td>
</tr>
<tr>
<td>NC</td>
<td>Network management</td>
<td>2 elective hours</td>
</tr>
<tr>
<td>HC</td>
<td>Building-GUI Interfaces</td>
<td>2 core hours</td>
</tr>
<tr>
<td>HC</td>
<td>GUI Design</td>
<td>2 elective hours</td>
</tr>
<tr>
<td>SE</td>
<td>Software tools and environments</td>
<td>2 core hours (of 3)</td>
</tr>
<tr>
<td>SP</td>
<td>Privacy and civil liberties</td>
<td>1 core hour (of 2)</td>
</tr>
<tr>
<td>SP</td>
<td>Computer Crime</td>
<td>5 elective hours</td>
</tr>
<tr>
<td>IM</td>
<td>Database Systems</td>
<td>1 core hour (of 3)</td>
</tr>
<tr>
<td>IM</td>
<td>Data Modeling</td>
<td>1 core hour (of 4)</td>
</tr>
<tr>
<td>IM</td>
<td>Relational Databases</td>
<td>1 elective hour</td>
</tr>
<tr>
<td>PF</td>
<td>Event Driven Programming</td>
<td>2 core hours (of 4)</td>
</tr>
<tr>
<td>PF</td>
<td>Object Oriented</td>
<td>2 core hours (of 8)</td>
</tr>
<tr>
<td>PF</td>
<td>Foundations Information Security</td>
<td>2 core hours (of 4)</td>
</tr>
<tr>
<td>PF</td>
<td>Secure Programming</td>
<td>4 core hour (of 2)</td>
</tr>
<tr>
<td>PL</td>
<td>Declarations And Types</td>
<td>2 core hour</td>
</tr>
<tr>
<td>PL</td>
<td>Object Oriented Programming</td>
<td>2 core hours (of 10)</td>
</tr>
</tbody>
</table>