CSC 321 – Introduction to Computer Security

1. CSC 321 – Introduction to Computer Security

2. **credit units**: 4  **contact hours**: 6

3. **Course Coordinator**: Zachary Peterson

4. **Textbook**: (and/or other required material)

5. a. **Course Description**: This course is a broad survey of the terminology, concepts, issues, policies and technologies associated with computer and network security. Students will explore how systems and networks are attacked and the common mechanisms to defend them. 3 lectures, 1 laboratory.

   b. **Prerequisite**: CSC/CPE357

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

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

6. a. **Course Goals/Outcomes**

   The student will be able to:

   - Decompose system security requirements into confidentiality, integrity, and availability components,
   - Be able to characterize the types, powers, and motivations of common adversaries.
   - Assess threats to, and common vulnerabilities in a computer system, and then justify appropriate countermeasures in response to the same.
   - Identify legal and ethical ramifications of security decisions.
   - Learn the common ways to attack a system, and then to defend against those attacks by analyzing the system for vulnerabilities and ameliorating those problems.
   - Understand the capabilities of modern cryptographic systems and apply them appropriately.
   - Demonstrate the ability to implement software that is robust against common security attacks.

   b. **How Student Outcomes addressed**

   (“B” = Basic level, “I” = Intermediate level, “A” = Advanced level)

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSC</td>
<td>A</td>
<td>I</td>
<td>B</td>
<td>B</td>
<td>B</td>
<td>A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
7. **Major Topics Covered: (number of lecture hours each)**

- Introduction to Computer Security, Trust, and Risk Analysis (3)
- Computer Communications, Classical and Modern Cryptography (6)
- Identity and Authentication (3)
- Authentication attacks, UNIX Access Control, Capabilities and Access Control Lists (1)
- Software Security, Malicious code and Robust Programming (3)
- Web and Web Application Security (3)
- Data Security and Forensics (3)
- Network-based attacks, Vulnerabilities and Threats (3)