CSC/CPE 456 Introduction to Computer Security

1. CSC/CPE 456 Introduction to Computer Security

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

3. **Course Coordinator**: Phillip Nico


5. a. **Course Description**: Survey of topics in computer system and network security, including protection, access control, distributed access control, operating system security, applied cryptography, network security, firewalls, secure coding practices, and case studies from real-world systems. 3 lectures, 1 laboratory. Crosslisted as CPE/CSC 456.
   b. **Prerequisite**: CSC/CPE 453 and either CSC/CPE 300 or CPE 350.
   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></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 outcomes of this course are intended to be consistent with National Security Telecommunications and Information Systems Committee (NSTISSC) standard 4011, entitled “National Standard for Information Systems Security (INFOSEC) Professionals.”

   The student will be able to:
   
   - Demonstrate the ability to implement software that is robust against common security attacks,
   - Understand the capabilities of modern cryptographic systems and apply them appropriately,
• Decompose system security requirements into confidentiality, integrity, and availability components,
• Assess threats to and vulnerabilities of a computer system,
• Evaluate the level of risk associated with various types of threats,
• Justify appropriate countermeasures in response to identified threats,
• Identify legal and ethical ramifications of policy decisions and defend those decisions,
• Distinguish desired system features (policy) from their implementation (mechanism).
• Design a security plan for an instructor-supplied system description,
• Play the role of either system penetrator or protector when given an instructor-supplied system description, evaluate the system's security, identify points of exploitation, and apply appropriate countermeasures. Be able to function in a general networked computing environment
• Demonstrate basic elements of good programming style.

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>I</td>
<td>I</td>
<td>I</td>
<td></td>
<td></td>
<td>A</td>
<td>I</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>SE/CPE</td>
<td>A</td>
<td>A</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td></td>
<td></td>
<td>A</td>
<td>I</td>
<td>A</td>
<td></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 (3)
   • Authentication and Access Control (3)
   • Authentication attacks, Unix access control, Access Control Lists (1)
   • Malicious code and robust programming (1)
   • Capabilities, Mandatory Access Controls (1)
   • Malicious Logic, Sandboxing, and Integrity Checking (1)
   • Role of Trust, Denial of Service (Availability) (1)
   • Security Policy, Information Flow (Lattice model), Integrity (1)
   • Network-based attacks, Vulnerabilities and Threats (1)
   Intrusion Detection, Covert Channels (1)