CSCE 201 - Introduction to Computer Security
Credit Hours: 3 hours
Contact Hours: 3 lecture hours
Instructor: Dr. N. Stiffler


Bulletin Description: Introduction to the theory and practice of computer security, including security policies, authentication, digital certificates, firewalls, malicious code, legal and ethical issues, and incident handling.

Prerequisites: Prereq or coreq: CSCE 101 or CSCE 102 or CSCE 145

Required Course in CE, CIS, and CS programs

Learning Outcomes: Students will be able to:
1. Understand basic concepts and practices of information security
2. Understand tools and techniques used by attackers to penetrate computer systems
3. Understand tools and techniques used by defense to protect computer systems
4. Be able to check for security updates, apply and use patches and other defense mechanisms
5. Be able to understand and follow security and privacy policies
6. Understand the ethical implications of using attack tools on computer systems

Student (Program) Outcomes addressed by course (Detailed mappings available.)

<table>
<thead>
<tr>
<th>Student Program Outcomes</th>
<th>SOs supported</th>
<th>SOs Moderately supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Engineering</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer Information Systems</td>
<td>e, g, i</td>
<td>h</td>
</tr>
<tr>
<td>Computer Science</td>
<td>e, g, i</td>
<td>h</td>
</tr>
</tbody>
</table>

Topics covered and approximate weight:
1. Weeks 1—5: Basic Security Concepts
2. Week 1: Overview of computer security, …, risks and threats.
3. Week 2: Operating Systems. Security capabilities of different platforms
5. Week 4: Access Control and Firewalls, ownership. Basic cryptography
6. Week 5: Assessing and Securing a system
8. Week 6: Software security. Malware: Viruses, worms, freeware and spyware
9. Week 7: Network security, TCP/IP primer. Firewall and Router security, PKI.
10. Week 8: Web security. Web application security
12. Weeks 11—15: Popular applications, ethics, security and privacy