I. Course Title: Computer Security

II. Course Prefix/Number: CSCI 170

III. Credit Hours: 2.0

IV. Prerequisite(s): None

V. Catalog Description:
Covers the fundamentals of computer security. Students will conduct hands-on activities for securing both Windows and UNIX operating systems using virtual machines.

VI. Curricular Relationships:
This course is required of students obtaining an Associate of Science Degree in Internet Computing and Security. It will also be of interest to students wishing to obtain in-depth understanding of computer security issues.

VII. Student Learning Outcomes:
- Students will explain the objectives and tradeoffs inherent in information security.
- Students will explain the importance and application of confidentiality, integrity, and availability.
- Students will recognize the basic risks, vulnerabilities and threats to computer operations and communications.
- Students will list at least three types of social-engineering attacks and explain how they work, why they can be damaging, and how to hinder them.
- Students will list and describe the major types of malicious software and identify a counter measure for each one.
- Students will understand authentication and biometric techniques for securing equipment and data.
- Students will explain the mechanisms available in an operating system to control access to resources.
- Students will list and demonstrate basic computer forensic techniques.
- Students will explain the purpose and application of virtualization technology as well as how to set-up and configure virtual machines.
- Students will have an in-depth understanding of how to defend both Windows and UNIX operating systems including:
  - Students will be able to manage user accounts, create strong password policies, and implement login scripts.
  - Students will be able to assign appropriate rights to files, applications, and resources.
  - Students will be able to demonstrate how to maintain, backup, and restore data.
  - Students will be able to implement a security baseline by using OS hardening.
  - Students will be able to identify running processes.
  - Students will be able to configure and use anti-virus and anti-spam software.

VIII. Content Outline:
1. Security Fundamentals
   a. Confidentiality, Integrity, and Availability
   b. Physical, Operational, and Management Security
   c. Trade-offs inherent in security
d. Risk management

2. Identification and Authentication
   a. Managing and protecting usernames and passwords
   b. Logon procedures
      i. One, two, and three-factor authentication
      ii. Single sign-on
      iii. Biometric techniques for securing equipment and data

3. Access Control

4. Human Security Threats
   a. Identity Theft
   b. Phishing
   c. Social Engineering

5. Virtual Machines
   a. Purpose and applications
   b. Set-up and configuration

6. System security threats
   a. Privilege escalation
   b. Viruses
   c. Worms
   d. Trojans
   e. Spyware
   f. Spam
   g. Adware
   h. Rootkits
   i. Botnets
   j. Logic bombs

7. Security Risks pertaining to system hardware and peripherals
   a. BIOS
   b. USB devices
   c. Cell phones

8. Protecting Computers (UNIX and Windows)
   a. Physical Security and Access Controls
   b. Maintenance, backup, and restoration of data
   c. Operating System Security
      i. User accounts
      ii. File and directory security
      iii. Password security
      iv. Hot fixes, service packs, and patches
      v. OS hardening to implement a security baseline
      vi. Anti-virus software
      vii. Anti-scam
      viii. Disk cleanup, scheduled tasks, and disk defragmentation
      ix. Intrusion detection
      x. System logging

9. Introduction to Computer Forensics
   a. Methodology of a forensic investigation, enforcing the chain of custody, preserving and collecting evidence
   b. Privacy and Security Regulation including Patriot Act, Gramm-Leach-Bililey Act, Computer Fraud and Abuse Act, and Cyberspace Electronic Security Act
   c. Cyberforensics-related aspects of Internet-based investigations
i. Use of domain search tools such as DNSstuff.com, SamSpade, and whois.
ii. Use of tools to examine e-mail headers, browser histories, chat and messaging logs, and social networks.
d. Example computer forensic activities such as
   i. Examination of the file-system of a CDMA cell phone to find information such as phone numbers, voice mail codes, and call history.
   ii. Imaging RAM using tools such as dd and Helix to analyze the contest of a disk

IX. Course Procedures/Policies/Grading Scale:
   • Regular homework assignments may be a component of the course grade.
   • At least one examination is given each semester.
   • A comprehensive final examination is given during finals week.
   • Many of the computer security concepts will be taught through hands-on activities that will be a component in determining the course grade.

X. Required/Recommended Readings:
A textbook is required. Example text and reference 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.* In particular, it targets the committee recommendation for an increased emphasis on security in the computer science curriculum at a lower division level. The course includes topics from the following core areas: PF (Programming Fundamentals), OS (Operating System), HC (Human-Computer Interaction), PL (Programming Languages), and SP (Social and Professional Issues)

<table>
<thead>
<tr>
<th>Knowledge Area</th>
<th>Topic</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>PF</td>
<td>Foundations of Information Security</td>
<td>4 core hours (of 4)</td>
</tr>
<tr>
<td>OS</td>
<td>Security and Protection</td>
<td>2 core hour (of 2)</td>
</tr>
<tr>
<td>HC</td>
<td>Human Factors and Security</td>
<td>4 elective hours</td>
</tr>
<tr>
<td>PL</td>
<td>Virtual Machines</td>
<td>2 core hours (of 1)</td>
</tr>
<tr>
<td>SP</td>
<td>Security Operations</td>
<td>4 elective hours</td>
</tr>
<tr>
<td>SP</td>
<td>Computer Crime</td>
<td>4 elective hours</td>
</tr>
<tr>
<td></td>
<td>12 hours</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>----------</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>