I. Course Title: Networking and Security

II. Course Prefix/Number: CSCI 215

III. Credit Hours: 3.0

IV. Prerequisite(s): CSCI 170 minimum grade of C-

V. Catalog Description:

Introduces the structure, implementation, and theoretical underpinnings of computer networking and the applications that have been enabled by that technology. Topics include the fundamentals of communications, network management, and wireless computing. An emphasis is placed on network security issues.

VI. Curricular Relationships:

CSCI 215 is required of students working toward the Associate of Science Degree with an emphasis in Internet Computing and Security. CSCI 215 can be used together with CSCI 216 to satisfy the networking requirement for the Bachelor of Science Degree in Mathematics with a Computer Science emphasis.

VII. Student Learning Outcomes:

- Students will demonstrate an understanding of fundamental networking and communications concepts. In particular, students will understand
  1. The hierarchical, layered structure of a typical network architecture
  2. Network protocols
  3. Network standards and bodies
  4. Physical and data link layer concepts (framing, error control, flow control, protocols and access control)
  5. Internetworking (routing algorithms and congestion control)
  6. The use of network infrastructure devices such as firewalls, hubs, modems, remote access services, routers, switches, telecom/PBX systems, wireless access points, and cabling.
• Students will describe in technical terms the following types of attacks: DoS, ping-of-death, spoofing, sniffing and traffic redirection, message integrity attacks, man-in-the-middle, replay attacks, route blackholing, and TCP session hijacking.

• Students will demonstrate an understanding of intrusion and intrusion detection.

• Students will demonstrate an understanding of the fundamental ideas of public-key cryptography and how it works.

• Students will demonstrate an understanding of how digital signatures are used and give examples of their use.

• Students will distinguish between the uses of private- and public-key algorithms.

• Students will discuss the fundamentals of network management.

• Students will describe the benefits of secure email, PGP, and S/MIME.

• Students will demonstrate an understanding of the fundamental concepts of wireless and mobile computing.

• Students will explain the theory and usage of basic network defense tools and strategies such as firewalls, IPSec, Virtual Private Networks, Virtual Local Area Networks, and Network Address Translation.

• Students will describe the implementation steps for secure wireless data transfer using WAP, WTLS, and WEP.

• Students will describe instant messaging and the security risks and vulnerabilities of such a service.

VIII. Content Outline:

• Communication and networking: Network standards and standardization bodies; the ISO 7-layer reference model in general and its instantiation in TCP/IP; circuit switching and packet switching; streams and datagrams; physical layer networking concepts; data link layer concepts; internetworking and routing; transport layer services

• Network attacks: DoS, ping-of-death, spoofing, sniffing and traffic redirection, message integrity attacks, man-in-the-middle, replay attacks, route blackholing, and TCP session hijacking.

• Hardening network applications: DNS Servers, DHCP services, email servers, LDAP servers, etc.

• Network defense tools: Network monitors, intrusion detection systems, IPSec, VPNs, NAT, VLANs, configuring routers and firewalls.
• Wireless and mobile computing: Overview of the history, evolution, and compatibility of wireless standards; the special problems of wireless and mobile computing; wireless local area networks and satellite-based networks; wireless local loops; mobile Internet protocol; mobile aware adaptation; extending the client-server model to accommodate mobility; mobile data access; the software packages to support mobile and wireless computing; the role of middleware and support tools; performance issues; emerging technologies.

• Cryptography basics, methods, and standards: hashing, symmetric and asymmetric algorithms, confidentiality, integrity, digital signatures, authentication, non-repudiation, access control, public key infrastructure, cryptographic attacks, cryptography standards and protocols, and key management.

IX. Course Procedures/Policies/Grading Scale:

1. Homework assignments will be given during the semester.

2. At least two examinations will be given during each semester.

3. A final examination will be given at the end of each semester.

X. Required/Recommended Readings:

A text book will be required. Example textbooks include:


XI. Issues Unique to Course: Course may be offered concurrently with CSCI 345, Net-centric Computing.

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. It targets the NC (net-centric computing) area as well adhering to the committee recommendation for an increased emphasis on security in the computer science curriculum.
<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 (of 2)</td>
</tr>
<tr>
<td>NC</td>
<td>Network Communication</td>
<td>10 core hours (of 7)</td>
</tr>
<tr>
<td>NC</td>
<td>Network Security</td>
<td>10 core hours (of 6)</td>
</tr>
<tr>
<td>NC</td>
<td>Network Management</td>
<td>4 elective hours</td>
</tr>
<tr>
<td>NC</td>
<td>Mobile Computing</td>
<td>6 elective hours</td>
</tr>
<tr>
<td></td>
<td>Other</td>
<td>10 hours</td>
</tr>
</tbody>
</table>