**CMPSC 443**

**Introduction to Computer and Network Security**

**Catalog Data:**
Introduction to the theory and practice of computer and network security with an emphasis on Internet and operating systems applications. Prerequisites: CMPSC 473, CMPEN 362.

**Typical Textbook:**

**Course Objectives:**
This course provides an introduction to the theory and application of security in computer and network environments. Students will develop the skills necessary to formulate and address the security needs of enterprise and personal environments. The course will begin by describing the goals and mechanisms of security as motivated by recent incidents and seminal works in the area. Latter topics will cover cryptography, authentication, secure programming, security in operating systems, network security, secure storage, access control, denial-of-service, and file systems, and conclude with emerging trends in secure systems design. Course projects will focus on the application of security tools to real world problems.

**Primary Course Outcomes:**
For the areas of network and operating systems, students will learn the basic concepts of network and computer security, including cryptography, secure communication, authentication, access control, and secure programming. Security appears in a variety of contexts, and we will examine several of these contexts and provide students with the terminology to communicate security issues and solution.

In general, we have the following pedagogical objectives for this course. Students will develop the following skills.

- Security Analysis – Students will be able to evaluate the security of commercial security products, organizational policies, and software designs.
- Security Development – Students will be able to construct and realize a security strategy within a software design or software deployment.
- Security Terminology – Students will be able to speak cogently about security using the terms of art.

**Relationship to Undergraduate Program Outcomes:**
CMPSC 443 introduces students to the issues in designing computers to implement security requirements, which directly related to Program Outcome 5: Design the architecture and organization of the basic components of a computer system.

CMPSC 443 requires that students learn techniques for software assurance to enable verification of program correctness for security, which is related to Program Outcome 7: Analyze algorithms or computer code for correctness and efficiency.

Students in CMPSC 443 develop program modules that implement security mechanisms. Although these modules are typically less than 1000 lines of code, the modules require careful consideration of data structures and algorithms. Thus, these assignments support Program Outcome 8: Develop a modest software application using appropriate data structures and algorithms.

CMPSC 443 requires students to configure their own Linux virtual machine, including
the development of system code, to protect it from security compromises. This work supports Program Outcomes 10 and 14: Design and implement computer operating system components for managing various system resources and Demonstrate independent learning by using unfamiliar computer systems, test equipment, and software tools to solve technical problems.

As computer security consists of many concepts and terms, CMPSC 443 exams consist of many short essay questions, requiring the students to satisfy Program Outcome 12: Write clear and effective technical prose.

Security is a topic of immediate concern in the computing industry, particularly with respect to computer ethics. Further, the exploration of security requires that the students adhere to ethical requirements. These support Program Outcomes 15 and 17: Be able to discuss major trends in industry and current research activities within the discipline and Be able to state a code of professional ethics and identify ethical issues in engineering case studies.

**Required Topics:**

- Introduction to security problems in networks and operating systems (1.5 hrs).
- Definition of security concepts, security goals, and security models (1.5 hrs).
- Basic Cryptography – Ciphers, Hash Functions (3 hrs).
- Applied Cryptography – Constructions using cryptographic operations (3 hrs).
- Authentication – basic problem of authenticating users, password limitations, cryptographic authentication mechanisms (3 hrs).
- Web Security – Differences between the web and network security in general, SSL, web cookies, web scripting and vulnerabilities, web server configuration (3 hrs).
- Programming Security – Common programming flaws, buffer overflow details, type safety, secure programming goals, programming tools to improve security (3 hrs).
- Access Control Basics – Access control concepts, problems with access control, protection vs. security, fundamental security problems (3 hrs).
- UNIX Security – UNIX security model, applications of the model, UNIX vulnerabilities and causes (1.5 hrs).
- Windows Security – Windows security model, applications of the model, Windows vulnerabilities and causes (1.5 hrs).
- Trustworthy Computing – Overview of trusted computing approach, trusted computing hardware, important protocols, applications (1.5 hrs).
- Access Control Policies – Secrecy goals, Multilevel security policy, Chinese Wall policy, program-level secrecy, integrity goals, integrity policies, alternative techniques to ensure integrity (3 hrs).
- Mandatory Access Control – Definition of mandatory access control, implementation of true reference monitors, early MAC systems, current MAC systems (1.5 hrs).
- Intrusion Detection – Anomaly and misuse detection, example techniques, difference from access control, Bayesian fallacy (1.5 hrs).
- Special Topics in Systems Security – One of virtual machine systems, security assurance, achieving integrity in practice, language security, privacy, etc. (1.5 hrs).
- Special Topics in Network Security – One of wireless security, Email security, advanced network protocol security, advanced cryptography, emerging network architectures (1.5 hrs).

**Class Format:** Two lectures per week. Each lecture is 75 minutes.
Professional Component: CMPSC 443 is designed to aid the professional development of engineers and scientists by developing skills in problem solving, critical thinking, the design of security solutions, and the implementation of solutions in a variety of security areas. The use a virtual machine environment for development enables students to configure their own system against attacks as a real administrator would.

Evaluation: 40-65% proctored assessments (exams)
35-60% unproctored assessments (programming projects, homeworks, etc.)

Suggested breakdown based on 1000 points
200 Exam 1
300 Final
350 Programming Projects
150 Homeworks and/or Quizzes

Programming Assignments: Tentative Schedule

<table>
<thead>
<tr>
<th>Goals</th>
<th>Assigned</th>
<th>Due</th>
<th>Worth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptographic Operations</td>
<td>L4</td>
<td>L7</td>
<td>75</td>
</tr>
<tr>
<td>Cryptographic Protocols</td>
<td>L9</td>
<td>L13</td>
<td>75</td>
</tr>
<tr>
<td>Network Security</td>
<td>L16</td>
<td>L19</td>
<td>75</td>
</tr>
<tr>
<td>Code Security</td>
<td>L20</td>
<td>L23</td>
<td>50</td>
</tr>
<tr>
<td>Access Control</td>
<td>L25</td>
<td>L29</td>
<td>75</td>
</tr>
</tbody>
</table>

Author: Trent Jaeger, Patrick McDaniel
Last Revised: May 31, 2007