COURSE INFORMATION FORM

DISCIPLINE          Computer Science Information Systems
COURSE TITLE        Network and Systems Security

CR.HR   3   LECT HR.   2   LAB HR.   2   CLIN/INTERN HR.   ||   CLOCK HR.   

CATALOG DESCRIPTION
This course will introduce to students to network and systems security by exploring vulnerabilities, threats, attacks, and countermeasures. Students will also learn fundamental security design principles and implementation techniques. This course helps students prepare for the current CompTIA Security+ certification exam.

PREREQUISITES
CSIS 112 or CSIS 161 with a grade of C or better and
CSIS 170 with a grade of C or better (or concurrent enrollment)

EXPECTED STUDENT OUTCOMES IN THE COURSE (ESO)

Upon completion of this course, the student will be able to:

1. Describe potential system attacks, characteristics, and the actors that might perform them.
2. Describe and apply cyber defense tools, methods and strategies to prepare systems to repel attacks.
3. Describe appropriate measures to be taken should a system compromise occur.
4. List the first principles of security and describe their impact on the development of security policies.
5. Describe how the fundamental concepts of cyber defense can be used to provide system security.
6. Examine a use case and identify significant vulnerabilities, risks, and points at which specific security technologies/methods should be utilized.
7. Analyze common security failures and identify specific design principles that have been violated.
8. Identify the needed design principle when given a specific scenario
9. Understand the interaction between security and system usability and the importance for minimizing the affects of security mechanisms
10. Identify the elements of a cryptographic system
11. Describe the differences between symmetric and asymmetric algorithms
12. Describe which cryptographic protocols, tools and techniques are appropriate for a given situation

GENERAL EDUCATION OUTCOMES (ESO)

Specify which general education outcomes, if any, are substantially addressed by the course. Numbers in parentheses identify the Expected Student Outcomes linked to the specific General Education Outcome.

<table>
<thead>
<tr>
<th>Outcomes</th>
<th>ESO</th>
</tr>
</thead>
</table>
PROGRAM-LEVEL OUTCOMES

CAREER AND TECHNICAL EDUCATION PROGRAM OUTCOMES
Specify which Career and Technical program outcomes, if any, are substantially addressed by the course by completing the “Career and Technical Education template” to show the relationship between course and program outcomes to assessment measures.

1. Use industry specific software and/or apply troubleshooting skills to solve problems
2. Create and defend solutions to real life business challenges
3. Demonstration professional oral and written communication skills
4. Recognize the need for continued professional development

CLASS-LEVEL ASSESSMENT MEASURES
Student accomplishment of expected student outcomes may be assessed using the following measures. (Identify which measures are used to assess which outcomes.)

1. Examination/Quizzes (1-12)
2. Class Discussion/Participation (1-12)
3. Exercises/Projects (1-12)
4. Written/Oral Reports (1-12)
Individual instructors may order this outline as fits the needs of their individual courses. In addition, they may place more emphasis on some areas than on others. What is assured is that this particular list is covered in the course. Other topics may be added to a course as the instructor sees fit, and as time and interest allow. An *asterisk can be used to mark an item as optional.

I. Network Security
   A. Network device security
   B. Secure network administration principles
   C. Secure network components and design principles
   D. Common protocols and services
   E. Secure wireless networking

II. Threats and Vulnerabilities
   A. Malware
   B. Types of attacks
   C. Social engineering
   D. Mitigation and deterrent techniques
   E. Penetration testing and vulnerability scanning

III. Application, Host, and Data Security
   A. Application security control
   B. Mobile device security
   C. Host security concepts
   D. Data security concepts

IV. Access Control
   A. Authentication and authorization
   B. Account management

V. Cryptography
A. Confidentiality
B. Integrity
C. Non-repudiation

VI. Technologies and Tools

A. Software tools to assess the security posture of an organization
B. Troubleshooting common security issues
C. Analyzing and interpreting output from security tools
D. Implementing secure protocols