Title (Units): COMP 3140 Computer And Network Security (3,3,0)

Course Aims: To introduce the fundamental concepts and techniques in computer and network security, including basic encryption techniques, cryptographic algorithms, authentication and digital signature, public key infrastructure, access control, security models, as well as their applications to IP security, Web security, trusted operating systems. To discuss other system and programming related security issues, including non-malicious errors, computer virus and intrusion detection, etc.

Prerequisite: COMP 1180 Structured Programming
COMP 2330 Data Communications and Networking and Year III Standing

Learning Outcomes (LOs):
Upon successful completion of this course, students should be able to:

<table>
<thead>
<tr>
<th>No.</th>
<th>Learning Outcomes (LOs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Describe fundamental concepts of computer security</td>
</tr>
<tr>
<td>2</td>
<td>Explain the basic concepts of symmetric &amp; asymmetric cryptography</td>
</tr>
<tr>
<td>3</td>
<td>Explain the fundamental concepts of different digital signature schemes</td>
</tr>
<tr>
<td>4</td>
<td>Identify security weaknesses in different networking environment</td>
</tr>
<tr>
<td>5</td>
<td>Identify the appropriate cryptography scheme &amp; security mechanism for different computing environment and information systems</td>
</tr>
<tr>
<td>6</td>
<td>Analyze the security of different computer systems &amp; networks</td>
</tr>
<tr>
<td>7</td>
<td>Develop a critical mind for evaluating the security of computer systems</td>
</tr>
</tbody>
</table>

Calendar Description: This course introduces the fundamental concepts and techniques in computer and network security. Topics include basic encryption techniques, cryptographic algorithms, authentication and digital signature, public key infrastructure, access control, security models, as well as their applications to, for example, IP security, Web security, trusted operating systems. In addition, it discusses other system and programming related security issues, including non-malicious errors, computer virus, and intrusion detection.

Assessment:

<table>
<thead>
<tr>
<th>No.</th>
<th>Assessment Methods</th>
<th>Weighting</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Continuous Assessment</td>
<td>30%</td>
<td>Continuous assessments are designed to measure how well the students have learned the material. A project is designed to give students hands-on experience in the subject matter.</td>
</tr>
<tr>
<td>2</td>
<td>Examination</td>
<td>70%</td>
<td>Final examination questions are designed to evaluate students’ understanding of the course material, and how far students have achieved the intended learning outcomes. Questions will primarily be analysis and skills based to assess the students’ ability to analyze the security of different computer systems.</td>
</tr>
</tbody>
</table>

Rubrics:

Excellent (A) • Achieve the first six CILOs, demonstrating a good mastery of both the theoretical and practical aspects of computer security
• Have a solid understanding of computer security fundamental concepts, and be able to explain and highlight the key points of these concepts
• Able to conduct security analysis on computer systems, and possibly highlighting security vulnerabilities with detailed explanation and proper reasoning
• Able to recommend suitable cryptographic technologies and security mechanisms to different situations and computing environments, and be able to design and develop, with competence,
high quality computer security systems using these technologies

| Good (B)                  | Achieve the first six CILOs, demonstrating a good understanding of both the theoretical and practical aspects of computer security  
|                          | Have a good understanding of computer security fundamental concepts  
|                          | Able to conduct security analysis on computer systems with sound reasoning  
|                          | Able to apply cryptographic technologies and security mechanisms to different situations and computing environments, and be able to design and develop computer security systems using these technologies  

| Satisfactory (C)         | Achieve most of the first six CILOs, demonstrating a basic level of understanding of the theoretical and practical aspects of computer security  
|                          | Have a basic understanding of computer security fundamental concepts  
|                          | Able to conduct a basic security analysis on most computer systems  
|                          | Demonstrate an adequate level of ability of applying cryptographic technologies and security mechanisms to different situations and computing environments  

| Marginal Pass (D)        | Achieve most of the first six CILOs, with a minimal level of understanding of the theoretical and practical aspects of computer security  
|                          | Have a minimal level of understanding of computer security fundamental concepts  
|                          | Ability to conduct security analysis on computer systems under a limited number of typical situations  
|                          | Ability to apply some of the cryptographic technologies and security mechanisms to a limited number of computing environments  

| Fail (F)                | Achieve less than three of the CILOs, and have little understanding of the theoretical and practical aspects of computer security  
|                          | Unable to provide solutions to simple problems which require basic understanding of computer security fundamental concepts  
|                          | Unable to conduct security analysis on computer systems  
|                          | Have little understanding of cryptographic technologies and security mechanisms and have difficulty in applying these technologies to computing environments  

**Learning Outcomes and Weighting:**

<table>
<thead>
<tr>
<th>Content</th>
<th>LO No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. Overview</td>
<td>1, 4, 7</td>
</tr>
<tr>
<td>II. Basic Encryption Techniques</td>
<td>1, 2, 4, 7</td>
</tr>
<tr>
<td>III. Secret-Key Cryptography</td>
<td>1, 2, 4, 5, 7</td>
</tr>
<tr>
<td>IV. Public-Key (Asymmetric) Cryptography</td>
<td>1, 2, 4, 5, 7</td>
</tr>
<tr>
<td>V. Message Authentication and Digital Signature</td>
<td>1, 2, 3, 4, 5, 7</td>
</tr>
<tr>
<td>VI. Network Security Practice</td>
<td>1, 4, 6, 7</td>
</tr>
</tbody>
</table>

**References:**

**Course Content in Outline:**

Page 2 of 3
I. Overview

II. Basic Encryption Techniques
   A. Substitution
   B. Transposition
   C. Steganography

III. Secret-Key Cryptography
   A. Block cipher
   B. Stream cipher
   C. Different encryption standards
   D. Key distribution

IV. Public-Key (Asymmetric) Cryptography
   A. Principles of public-key cryptosystems
   B. The RSA algorithm
   C. Key management
   D. Other public-key cryptosystems

V. Message Authentication and Digital Signature
   A. Message authentication code (MAC)
   B. Hash functions and algorithms
   C. Digital signature
   D. Authentication protocols

VI. Network Security Practice
   A. Threats in networks
   B. E-mail security
   C. IP security
   D. Web security