CSE4243
Information and Computer Security

REQUIRED/ELECTIVE:

Computer Science – Elective
Software Engineering – Required
Computer Engineering – Elective

CATALOG DATA:
(Prerequisites: CSE4733/CSE6733 with a grade of C or better). Three hours lecture. Topics include encryption systems, operating system security, database security, network security, electronic commerce, system threats, and risk avoidance procedures.

PREREQUISITE BY TOPIC:
1. Computer Programming
2. Database Concepts
3. Software quality
4. Operating System Fundamentals

TEXTBOOKS AND OTHER REQUIRED MATERIAL:
Introduction to Computer Security, Matt Bishop, 2005, Addison Wesley
Handouts, lab exercises, and web site at http://www.cse.msstate.edu/~cs6243

COORDINATOR:
Dr. Rayford B. Vaughn, Jr.

COURSE OBJECTIVES:
1. Provide an introduction to the security engineering discipline
2. Expose students to contemporary risks and attack procedures.
3. To provide students with an appreciation of the historical perspective in information assurance research.
4. Describe security engineering processes – particularly those being used in industry.
5. Students will be able to apply generally accepted selection criteria to choose security products.
6. Students will be able to design a defense in depth architecture to defend a specific system from attack.
7. The student will be able to apply standard, accepted security engineering techniques to protect a system with respect to a specific organizational security policy.
8. The student will demonstrate an ability to document their work to an acceptable standard.

TOPICS COVERED: (Number of class hrs)
1. Security Engineering Perspectives 2 hours
2. Security Historical Perspectives 2 hours
3. Operating System Security 3 hours
4. Database Security 3 hours
5. Network Security 3 hours
6. Security Administration 3 hours
7. Encryption types and techniques 2 hours
8. Prevention, Detection, and Response 3 hours
9. Guest Speakers 3 hours
10. Legal and Ethical Issues 3 hours
11. Exams 3 hours

CONTRIBUTION TO PROFESSIONAL COMPONENT:
Engineering Topics of engineering science and design

ASSESSMENTS:
1. Quizzes
2. Tests
3. Lab exercises
4. Class Participation

RELATIONSHIP TO PROGRAM OUTCOMES:
Note: Parenthesized list indicates the ABET and Software Engineering outcomes addressed by each criteria.
1. The student will be able to describe, discuss, and apply the security engineering discipline. (e, SE7)
2. The student will be able to select the correct process for a given security requirement scenario. (c, SE9)
3. The student will be capable of discussing the historical perspectives of security engineering and apply
   lessons learned to contemporary problems. (j, g, i, SE3, SE4, SE9)
4. The student will be able to architect a defensive perimeter for an unprotected system. (c,e, SE7, SE8)
5. The student will demonstrate proficiency in selecting appropriate security products by using generally
   accepted security engineering practices. (a,b,e, SE7, SE9)
6. The student be able to discuss the broad implication of risk to their system in a global, interconnected
   network and recommend solutions to mitigate that risk. (h, j, k, SE8)
7. The student will demonstrate an ability to consider ethics and law in application of security
   engineering. (h,j,SE6)

PREPARED BY:
Rayford B. Vaughn, Jr., Professor, Department of Computer Science and Engineering, April 15, 2005

ESTIMATE CSAB CATEGORY CONTENT:

<table>
<thead>
<tr>
<th></th>
<th>CORE</th>
<th>ADVANCED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Structures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Algorithms</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Design</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Core</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Computer Organization and Architecture</th>
<th>Core</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concepts of Programming Languages</td>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>

ORAL AND WRITTEN COMMUNICATIONS:

Every student is required to submit at least ___12___ written reports (not including exams, tests, quizzes, or commented programs) of typically ___2___ pages and to make ___0___ oral presentations of typically ___n/a___ minutes duration. Include only material that is graded for
grammar, spelling, style, and so forth, as well as for technical content, completeness, and accuracy.

SOCIAL AND ETHICAL ISSUES:

Three hours of class time is devoted to the topic of ethics and the law with respect to security engineering and prosecution of illegal acts.

THEORETICAL CONTENT:

1. The role of formal specification in trusted software – (2 hours)
2. The theory behind trusted systems (2 hours)

PROBLEM ANALYSIS:

The students are given 12 computer security lab exercises that require them to exercise a security tool or technique, analyze the results of the lab, and report those results formally to the instructor once per week.

SOLUTION DESIGN:

The students are given problem scenarios in class involving systems in need of protection and are required to design and justify a defensive protection scheme as a class verbal exercise. To a certain extent – design related questions are asked on the exams which require a student response.