TCOM662 – Advanced Secure Networking  
Department of Electrical and Computer Engineering  
George Mason University  
Spring, 2010

Syllabus revised 01/10/2010

Administrative Information

Instructor:
Mr. David E. Fowler, CISSP-ISSMP, CISM, CISA

Email: dfowler4@gmu.edu subject=GMU-TCOM662-Sec/001_Your name

Phone:
Office hours: By appointment

Teaching Assistant
TBD

Day/time of class: Tuesday 7:20-10:00 pm

Location: Engineering Building, Room 1110

Class section: 001

Course Description

662 Advanced Secure Networking (3:3:0)
Prerequisites: TCOM 509 and 562, and a working knowledge of network routing protocols.
Advanced technologies in network security that can be applied to enhance enterprise and ISP’s network security. Covers network perimeter defense concept and various components for complete layered defense system. Examines each component and its technologies, including TCP/IP protocol vulnerabilities, router access control list (ACL), dynamic ACL, firewall, network address translation (NAT), virtual private network (VPN), IPSec tunnels, intrusion detection system (IDS), routing protocol security, denial-of-service (DOS) attack, DOS detection and mitigation techniques.

From http://www.gmu.edu/catalog/courses/tcom.html

Textbook

Grading

Raw scores may be adjusted to calculate final grades.

Grades will be assessed on the following components:

<table>
<thead>
<tr>
<th>Component</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Homeworks (5 @ 10% each)</td>
<td>50%</td>
</tr>
<tr>
<td>Mid-term exam</td>
<td>25%</td>
</tr>
<tr>
<td>Final exam</td>
<td>25%</td>
</tr>
</tbody>
</table>

These components are outlined in the following sections.

Homework

Homework 1 - Although typically not as critical as a server, workstations also have an attack surface. Have you thought about the services that are running on your computer? How about your computer’s physical security? Elaborate your answer in a 3-4 page paper.

Homework 2 - In a 2-4 page paper, identify and describe four considerations you should take into account when designing a secure infrastructure.

Homework 3 – In a 2-4 page paper, define secure baseline and list and describe its components. Conclude with an example implementation.

Homework 4 - In a 3-4 page paper, list and discuss the types of information that can be reported by spyware and effective means to protect that information.

Homework 5 - In a 3-4 page paper, describe how a statistical anomaly IDS works, and discuss its advantages and disadvantages.

Reports will due in Weeks 4, 6, 10, 12, and 15. Late reports will be assessed a penalty of 25% of the assignment grade for each week or part there of if it is late. No report will be accepted after three weeks.

Mid-term exams

The mid-term exam will be conducted during class time in Week 7 and will cover material discussed in Weeks 1-6.
The mid-term exam will be “open book”.

**Final exam**

The final exam will be held the week after the final class in the same room used for classes and will cover material from the weeks 9-15. The final exam will be “open book”.

### Schedule

<table>
<thead>
<tr>
<th>Week</th>
<th>Date</th>
<th>Topic</th>
<th>Reading Assignments</th>
<th>Projects Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>Week 1</td>
<td>01/19/2010</td>
<td>Computer and Network Security Principles</td>
<td>Chapter 1</td>
<td></td>
</tr>
<tr>
<td>Week 2</td>
<td>1/26/2010</td>
<td>Network and Server Security</td>
<td>Chapter 2</td>
<td></td>
</tr>
<tr>
<td>Week 3</td>
<td>2/2/2010</td>
<td>Cryptography</td>
<td>Chapter 3</td>
<td></td>
</tr>
<tr>
<td>Week 4</td>
<td>2/9/2010</td>
<td>Authentication</td>
<td>Chapter 4</td>
<td>Report 1 due</td>
</tr>
<tr>
<td>Week 5</td>
<td>2/16/2010</td>
<td>Authorization and Access Control</td>
<td>Chapter 5</td>
<td></td>
</tr>
<tr>
<td>Week 7</td>
<td>3/2/2010</td>
<td>Mid-Term</td>
<td>Covers Chapt. 1-6</td>
<td></td>
</tr>
<tr>
<td>Week 8</td>
<td>3/9/2010</td>
<td>Spring Break</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Week 10</td>
<td>3/23/2010</td>
<td>Server Roles and Security</td>
<td>Chapter 8</td>
<td>Report 3 due</td>
</tr>
<tr>
<td>Week 11</td>
<td>3/30/2010</td>
<td>Protecting Against Malware</td>
<td>Chapter 9</td>
<td></td>
</tr>
<tr>
<td>Week 13</td>
<td>4/13/2010</td>
<td>Fault Tolerance and Disaster Recovery</td>
<td>Chapter 11</td>
<td></td>
</tr>
<tr>
<td>Week 14</td>
<td>4/20/2010</td>
<td>Intrusion Detection and Response</td>
<td>Chapter 12</td>
<td></td>
</tr>
<tr>
<td>Week 15</td>
<td>4/27/2010</td>
<td>Computer based Espionage and Terrorism</td>
<td></td>
<td>Report 5 due</td>
</tr>
<tr>
<td>Week 16</td>
<td>5/4/2010</td>
<td>Final exam</td>
<td>Covers Chapt. 7-12</td>
<td></td>
</tr>
</tbody>
</table>

*This schedule is subject to revision before and throughout the course.*

Call 703–993–1000 for recorded information on campus closings (*e.g.* due to weather).

**Important Dates**

- **Last day to add classes**: Tues. Feb 2
- **Last day to drop with no tuition liability**: Tues. Feb 2
- **Last day to drop**: Fri. Feb 19


See that Web page for more information.

**Attendance Policy**

Students are expected to attend each class, to complete any required preparatory work (including assigned reading) and to participate actively in lectures, discussions and exercises. As members of the academic community, all students are expected to contribute regardless of their proficiency with the subject matter.
Students are expected to make prior arrangements with Instructor if they know in advance that they will miss any class and to consult with the Instructor if they miss any class without prior notice.

Departmental policy requires students to take exams at the scheduled time and place, unless there are truly compelling circumstances supported by appropriate documentation. Except in such circumstances, failure to attend a scheduled exam may result in a grade of zero (0) for that exam.

Communications

Communication on issues relating to the individual student should be conducted using email or telephone. Email is the preferred method – for urgent messages, you should also attempt to contact the Instructor via telephone. Email messages from the Instructor to all class members will be sent to students' GMU email addresses – if you use another email account as your primary address, you should forward your GMU email to that account.

Lecture slides are complements to the lecture process, not substitutes for it - access to lecture slides will be provided as a courtesy to students provided acceptable attendance is maintained.

Honor Code

Students are required to be familiar and comply with the requirements of the GMU Honor Code[1]. The Honor Code will be strictly enforced in this course. All assessable work is to be completed by the individual student. Students must NOT collaborate on the project reports or presentation without explicit prior permission from the Instructor.


"You plagiarize when, intentionally or not, you use someone else's words or ideas but fail to credit that person. You plagiarize even when you do credit the author but use his exact words without so indicating with quotation marks or block indentation. You also plagiarize when you use words so close to those in your source, that if you placed your work next to the source, you would see that you could not have written what you did without the source at your elbow" (p. 167).