

**TCOM662 – Advanced Secure Networking**  
**Department of Electrical and Computer Engineering**  
**George Mason University**  
**Spring, 2008**

**Syllabus**      revised 11/19/07

**Administrative Information**

Instructor:

**Dr. Aleksandar Lazarevich**

Email: [alazarev@gmu.edu](mailto:alazarev@gmu.edu)    [subject=GMU-TCOM662-Sec/001\\_Your\\_name](mailto:alazarev@gmu.edu)

Phone:    703-393-2247

Office hours:      By appointment

Teaching Assistant

Mr. Anand Ashok <[amore1@gmu.edu](mailto:amore1@gmu.edu)>

**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**

Network Defense and Countermeasures – Principles and Practices

Chuck Easttom 2006; Pearson/Prentice Hall; ISBN: 0-13-171126-1

Publisher's Web page:

<http://vig.prehall.com/catalog/academic/product/0,1144,0131711261,00.html>

**Grading**

Raw scores may be adjusted to calculate final grades.

Grades will be assessed on the following components:

Homeworks (5@10% each)	50%
Mid-term exam	25%
Final exam	25%

These components are outlined in the following sections.

### Homework

**Homework 1** - Visit the Web sites listed on page 72 and compare the firewall products of each manufacturer. Which product would you choose to protect your personal PC? Be prepared to explain the reasoning behind your choice in a 3-4 page paper.

**Homework 2** - In a 3-4 page paper, discuss the potential costs of implementing a firewall solution for a large enterprise network. How do these costs compare to the potential costs of a security breach? When considering the expenses related to a security breach, list as many expenses as you can think of, including system downtime, lost data, lost work hours, the impact on customers and partners, and so on.

**Homework 3** – In a 3-4 page paper, explain what is the ideal password policy? Discuss the parameters that organizations can use in setting password standards. These include password length, types of characters, frequency of password resetting, and other requirements. Conclude with an example that the policy and the manner in which it will be enforced.

**Homework 4** - In a 3-4 page paper, suppose a worker in your organization frequently forgets his or her password, attempts to use obvious passwords, re-use old passwords, and sometimes gets locked out of the system for failed log-in attempts. How would you deal with such a user? What organizational policies should be in place for handling user behaviors of this kind?

**Homework 5** - In a 3-4 page paper, explain how is it that organizations can legally set and enforce usage policies, and use methods such as checking e-mail records, logging system use, or even searching a worker's desktop computer? Do you think such practices are legal and ethical? Why or why not? Discuss these issues with classmates, and explain your position.

Reports will due in Weeks 4, 6, 9, 12, and 15.

Late reports will be assessed a penalty of 25% of the assignment grade for each week or part there of it is late.

### 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 “closed book”– no reference materials other than those provided with the exam paper will be permitted.

**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 “closed book” – no reference materials other than those provided with the exam paper will be permitted.

**Schedule**

<b>Week</b>	<b>Date</b>	<b>Topic</b>	<b>Reading Assignments</b>	<b>Projects Due</b>
Week 1	1/22/2008	Introduction to Network Security	Chapter 1	
Week 2	1/29/2008	Types of attacks	Chapter 2	
Week 3	2/5/2008	Fundamentals of Firewalls	Chapter 3	
Week 4	2/12/2008	Firewall practical applications	Chapter 4	Report 1 due
Week 5	2/19/2008	Intrusion Detection Systems	Chapter 5	
Week 6	2/26/2008	Encryption	Chapter 6	
Week 7	3/4/2008	Mid-Term	Covers Chapt. 1-6	
Week 8	3/11/2008	Spring Break		Report 2 due
Week 9	3/18/2008	Virtual Private Networks	Chapter 7	
Week 10	3/25/2008	Operating System Hardening	Chapter 8	
Week 11	4/1/2008	Defending against Virus attacks, Trojans, Spyware, and Adware	Chapter 9 & 10	Report 3 due
Week 12	4/8/2008	Security Policies	Chapter 11	
Week 13	4/15/2008	Assessing a system	Chapter 12	Report 4 due
Week 14	4/22/2008	Security Standards	Chapter 13	
Week 15	4/29/2007	Computer based Espionage and Terrorism	Chapter 14	Report 5 due
Week 16	5/13/2007	Final exam	Covers Chapt. 7-14	

*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**

<b>Last day to add classes</b>	Tues. Feb. 5
<b>Last day to drop with no tuition liability</b>	Tues. Feb. 5
<b>Last day to drop</b>	Fri Feb 22

From

<http://registrar.gmu.edu/calendars/spring08acadmeiccalendar.pdf>

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<sup>\[1\]</sup>](#).

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.

---

<sup>[1]</sup> Available at [www.gmu.edu/catalog/apolicies/honor.html](http://www.gmu.edu/catalog/apolicies/honor.html) and related GMU Web pages.