TCOM 562 – Network Security Fundamentals
Department of Electrical and Computer Engineering
George Mason University
Fall, 2019

Syllabus

revised July 1, 2019

Administrative Information

Instructor:

Mr. David E. Fowler, CISSP-ISSMP, CISM

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

Phone:

Teaching Assistant
TBD

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

Location: DL

Class sections: DL

Course Description

TCOM 562 Network Security Fundamentals

Introduces full spectrum of network security. Topics include taxonomy such as language commonality in incident handling, national strategy to secure cyberspace, and cybersecurity organizations; organizational structure for network defense; best practices, security policy, and threats; actors and tools, countermeasures, vulnerability identification/correction, intrusion detection, and impact assessment; firewalls and intrusion detection systems; antivirus software; active defense; disaster recovery; and law enforcement and privacy issues. Reviews threats and vulnerabilities in network systems based on reports, case studies available in the literature, and actual experience.

Credits:
3.0

Prerequisites:
TCOM 500.

From http://telecom.gmu.edu/courses/network-security-fundamentals

Textbook

Michael E. Whitman, *Principles of Information Security, 6th Edition*. Cengage, 2019, ISBN-13 9781337102063.

Grading

Raw scores may be adjusted to calculate final grades.

Grades will be assessed on the following components:

Homework (4@10% each)	40%
Class Participation	10%
Mid-term exam	25%
Final exam	25%

Class Participation – Students must participate in at least two BB discussion forums for full credit.

These components are outlined in the following sections. Homework assignments are subject to change.

Homework

Homework Assignments are TBD

Homework 1 –

Homework 2 –

Homework 3 –

.

Homework 4 –

Assignments will due in Weeks 3, 5, 7, 11, and 13bvcx.
Late assignments will be assessed a penalty of 5% of the assignment grade for each week or part there of it is late. No assignment will be accepted after three weeks.

Mid-term exams

The mid-term exam will be virtual. It will cover materials discussed in Lectures 1-7.

The mid-term exam will be "open book".

Final exam

The Final Exam will be virtual. It will cover material from the lecture 8-13.
The Final will be "open book".

Schedule

Week	Date	Topic	Reading Assignments	Homework Due
Week 1	8/27/2019	Introduction to Information Security	Chapter 1	
Week 2	9/3/2019	The Need for Security	Chapter 2	
Week 3	9/10/2019	Legal, Ethical, and Professional Issues in Information Security	Chapter 3	Homework 1 due
Week 4	9/17/2019	Planning for Security	Chapter 4	
Week 5	9/24/2019	Risk Management	Chapter 5	Homework 2 due
Week 6	10/1/2019	Security Technology: Access Controls, Firewalls, and VPNs	Chapter 6	1st Discussion input due
Week 7	10/8/2019	Mid-Term (virtual)	Covers Lectures 1-6	
Week 8	10/15/2019	Columbus Day No Tuesday Class		
Week 9	10/22/2019	Security Technology: Intrusion Detection and Prevention Systems and Other Security Tools	Chapter 7	
Week 10	10/29/2019	Cryptography	Chapter 8	
Week 11	11/5/2019	Physical Security	Chapter 9	Homework 3 due
Week 12	11/12/2019	Implementing Information Security	Chapter 10	
Week 13	11/19/2019	Security and Personnel	Chapter 11	Homework 4 due
Week 14	11/26/2019	Cloud Computing Security Issues		2st Discussion input due
Week 15	12/3/2019	Information Security Maintenance	Chapter 12	
Week 16	12/15/2019	Final exam (virtual)	Covers Lectures.7-13	

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

See Web Page for Important Dates

https://registrar.gmu.edu/calendars/fall-2019/

Attendance Policy

Students are expected 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.

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.

Booth, Colomb, and Williams state in their book, The Craft of Research (University of Chicago Press, 1995):

> "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).

[1] Available at www.gmu.edu/catalog/apolicies/honor.html and related GMU Web pages.