Course Syllabus

Course Information

CS 4393.001 – Computer and Network Security

Term:	**Spring 2019**
Days & Time and Location:	TTh 2:30PM- 3:45PM @ ECSS 2.415

Instructor Contact Information

Nhut Nguyen, *Ph.D.*
Phone: *972-883-4521*
Email: *nhutnn@utdallas.edu*
Office hours: TTh 4:00PM – 5:00PM, *also by appointment*
Office: *ECSS 3.607*

Course Pre-requisites, Co-requisites, and/or Other Restrictions

CS/SE 3340 – Computer Architecture
CS/SE 3376/3377 – C/C++ Programming in a UNIX Environment
CS 4348 – Operating Systems Concepts

Course Description

This course is a comprehensive study of the security principles and practices for computer systems and networks. Topics to be covered include basic security concepts, common attacking techniques, common security policies, basic cryptographic tools and secure protocols. Defense techniques such as authentication, access control and network intrusion detection will also be discussed. Software security, operating system security, network security as well as legal and ethical issues will also be covered (3 semester hours).

Student Learning Objectives/Outcomes

After successful completion of this course, a student is expected to gain:

- Ability to understand and explain fundamental security concepts .
- Ability to understand common threats and vulnerabilities of computer systems and networks
- Ability to understand algorithms and practices of symmetric key cryptography
- Ability to understand algorithms and practices of public key cryptography
- Ability to understand principles and practices of authentication methods
- Ability to understand principles of secured protocols and their practices
- Ability to understand principles and practices of networks defense
- Ability to understand techniques, principles and practices of computer systems defense

Recommended Textbooks:

[Bis] *Matt Bishop*, Introduction to Computer Security, Addison-Wesley, 2004. ISBN 0-321-24744-2.

[KPS] *Charlie Kaufman, Radia Perlman, and Mike Speciner*, Network Security—Private Communication in a Public World, 2nd Edition. Prentice Hall, 2002. ISBN 978-0-13-046019-6.

[SB] *William Stallings and Lawrie Brown*, Computer Security - Principles and Practice 3rd Ed., Pearson 2016, ISBN 0-13-377392-2.

Suggested Reference Materials:

Charles P. Pfleeger and Shari Lawrence Pfleeger, Security in Computing, Fifth Edition. Prentice Hall, 2015. ISBN 978-0-13-408504-3.

Michael Goodrich and Roberto Tamassia, Introduction to Computer Security, Addison-Wesley, 2010. ISBN 0321557867

Required Course Materials:

Assignments will include hands on labs that require a virtual machine image that can be downloaded from the SEED lab project at the University of Syracuse (http://www.cis.syr.edu/~wedu/seed/)

Assignments & Academic Calendar

Exams: There will be three exams during the semester, and the last exam is comprehensive. Test material will be taken mainly from classroom lectures. Details will be announced in the class.

Assignments: Assignments will include hands-on labs using a SEED virtual machine image and typical question-answer/exercise homework.

For the hands-on labs the first one can be done with a partner but the remaining ones are individual.

There will be regularly assigned in-class exercises that will be used to assess class attendance and participation of each student.

Tentative Schedule

Week	Topic	Reading	Assignment
01	Introduction		
	Security – an overview I	[Bish] Ch 1	
02	Security – an overview II		
	Software security I	[Bish] Ch 2-3	
03	Software security II	[SB] Ch 10, [Bish] Ch 26	#1
	Malware I	[SB] Ch 11, [Bish] Ch 26	
04	Malware II	[SB] Ch 6, [Bish] Ch 19	
	Network security threats	[Bish] Ch 19	
05	Cryptography – an overview	[SB] Ch7	#2
	Private key cryptography I	[KPS] Ch 2	
06	Private key cryptography II	[KPS] Ch 3, [SB] Ch20	
	Exam I review	[KPS] Ch 4	
07	***Exam I (Feb 26)***		
	Hashes and message digests		#3
08	Public key cryptography I	[KPS] Ch 5	
	Public key cryptography II	[KPS] Ch 6	
09	Authentication	[KPS] Ch 6	
	Kerberos & X.509 Auth.	[SB] Ch 3	#4
10	*Spring Break*		
11	Access control	[KPS] Ch 13-14	
	Exam II review	[SB] Ch 4	
12	***Exam II (Apr 2)***		
	Secured protocols		
13	IPSec – an overview		#5
	SSL/TLS	[KPS] Ch 17-18	
14	Intrusion detection systems (IDS)	[KPS] Ch 19	
	Firewalls	[SB] Ch 8	
15	Wireless LANs Security	[SB] Ch 9	#6
	Exam III review		
16	***Exam III (Apr 30)***		
	Extra credits report (optional) working time		Extra credits report (optional)

Grading Policy

The grade each student earns from this class will be based the weighted score that is calculated from the following table:

Exam I	10%
Exam II	20%
Exam III	30%
Assignments	40%
Total	100%

Grades are assigned according to the scale on the right:

A	93.0 - 100
A-	90.0 - 92.9
B+	87.0 - 89.9
B	83.0 - 86.9
B-	80.0 - 82.9
C+	77.0 - 79.9
C	73.0 - 76.9
C-	70.0 - 72.9
D+	67.0 - 69.9
D	60.0 - 66.9
F	Below 60.0

Course & Instructor Policies

- **Attendance policy:** *missing **four** in-class exercises leads to **one letter grade drop**, missing **five** in-class exercises leads to **an F grade**.*
- *There will be no makeup exams under normal circumstances.*
- *No late homework or assignment will be accepted!*
- *I do not read e-Learning e-mails. Please use my UTD e-mail account above for any communications.*

UT Dallas Syllabus Policies and Procedures

The information contained in the following link constitutes the University's policies and procedures segment of the course syllabus.

Please go to *http://go.utdallas.edu/syllabus-policies* for these policies.

These descriptions and timelines are subject to change at the discretion of the Instructor.