SENG 5199-4: Cyber Security

MSSE: Spring 2015

Course Description

This course introduces the major topics of cyber security. Class time will include some lectures, but the focus is on demonstrations, exercises, mini-projects, and discussions. Topics include authentication, access control, file system forensics, symmetric and asymmetric cryptography, network monitoring and controls, dynamic web site attacks, and network cryptography. During the class we will be using open-source software for access control, file and email encryption, network monitoring, and attack simulation. While there will be a textbook ("Elementary Information Security") we will also be reading the latest security incident reports, surveys, and analyses.

The course title listed above does not match the catalog or transcript name, but I see no point in using the official, long, jaw-cracker phrase used previously. But to prevent confusion, be assured that this course is indeed **Data and Network Security: Theory and Practice.**

Prerequisites

The course assumes that the student has paid some attention to previous MSSE courses. Students should also have sufficient time to do the reading, work on homework assignments, and collaborate with team-mates on group projects.

All students need access to a laptop or other computer that runs Linux, Mac OS X, or Windows. All students should have administrative access to that computer.

Instructor

I, the instructor, am Dr. Rick Smith, a veteran software developer and security engineer, email: rick@cryptosmith.com, phone 651-437-5772. I mostly write and teach these days, and do a little consulting as well.

Readings

The course will use a combination of recent reports on security incidents, descriptions of security technologies, and textbook materials. We also look at Internet engineering documents, especially RFCs. The textbook is Smith, *Elementary Information Security*, first edition. Don't let the title fool you. There is a short on-line quiz on the readings each week. You need to finish the quiz before class.

Grading

Course work includes on-line quizzes, in-class work, and homework. Quizzes and many assignments will be graded, while some are simply "pass/fail" - you do it or you don't. All handed-in homework and many in-class activities will count towards the course

grade. There is no “final project.” Students who complete all work on time and with respectable content will earn an A.

Class Schedule

Week	Topic	Tools	Homework
1	Authentication	Google Authenticator, hashing	
2	Software integrity	User admin	Quiz 1+
3	Access control and volume forensics	Hexedit	Quiz 2+
4	File encryption	7zip	Quiz 3, use 7zip, threat profile
5	Volume encryption	TrueCrypt	Quiz 4, TrueCrypt, FAT lab
6	Network addressability	ARP, ping, WireShark	Quiz 5
7	Internet architecture	Wireshark, nmap	Quiz 6, Clark paper review
8	Email security, POP, DNS	GPGmail	Quiz 7, install GPGmail
9	NO CLASS - Spring Break		
10	Public-key certificates	GPG Keychain	Quiz 8, PGP paper review
11	Network Crypto	gateways	Quiz 9, Cert paper review
12	Web site tech	Intercepting proxy, Wireshark	Quiz 10+
13	Debate	TBD	Debate preparation
14	Web attacks, network scanning	WebGoat, SQL, Nessus	Identify network to assess
15	Commencement Weekend		
16	Lab time	Webgoat	Finish labs