SENG 5199-4: Cybersecurity

MSSE: Spring 2018

Course Description

This course introduces the major topics of cyber security. Class time will focus 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. Most readings will be from the textbook ***Elementary Information Security***. The publisher assures me that new copies of the textbook include access to an on-line copy.

The official course title is **Data and Network Security: Theory and Practice**. I use the shorter title **Cybersecurity** because we really don't do theory in this class. It is hard to change a course name.

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 should bring to class a wireless-capable laptop or other computer that runs Linux, Mac OS X, or Windows. All students need administrative access to that computer, and permission to install security software on it.

Instructor

I am Dr. Rick Smith, a veteran software developer and security engineer, email: me@cys.me, phone 651-307-0542. I've written three books on cybersecurity, including the textbook we use. I am now semi-retired: I write, teach, and do a little consulting. For more, see my website at cryptosmith.com.

Submitted Work

Students need to complete an on-line quiz before most class sessions. The quiz is based on the readings and may be taken up to 4 times.

Labs and in-class exercises are mostly graded ok/zero. You either finish it or you don't. Late work and missed classes are handled on a case-by-case basis.

There is no final project.

Class Schedule

Week	Topic	Finish Before Class	
		Reading	Writing
1	Endpoint security basics		
2	Software integrity	Ch 2, 3.1, 3.2, 4.1	Quiz 1
3	Access control	Ch 3, 4, 5	Quiz 2
4	Volume forensics, Authentication	Ch. 5, 6	Quiz 3
5	File encryption	Ch 7, 8.x	Quiz 4, FAT lab
6	Volume encryption	Ch 9	Quiz 5, install 7Zip
7	Network addressability	Ch 10, 11	Quiz 6, install ViaCrypt
8	Network monitoring	Ch 11	Quiz 7, nmap
9	POP, DNS	Ch 12, Clark	Quiz 8, Wireshark
10	NO CLASS -- Spring Break		
11	Email security	Ch 8.x, 14.x, 15	Quiz 9, GPGmail
12	Network Crypto, Certificates	Ch 13.x, 14.x	Quiz 10
13	Web site tech	Ch 13.x, 16	Quiz 11
14	Web attacks, network scanning	Nessus docs, Webgoat	Install scanner, emulator
15	NO CLASS -- Commencement		
16	Government secrecy	Chapter 17	