Syllabus

CS 4235/6035: Introduction to Information Security

Overview

This is an introductory course in information security. It teaches the basic concepts, principles, and fundamental approaches to secure computers and networks. Its main topics include: security basics, security management and risk assessment, software security, operating systems security, database security, cryptography algorithms and protocols, network authentication and secure network applications, malware, network threats and defenses, web security, mobile security, legal and ethical issues, and privacy.

Prerequisites

You should have taken an undergraduate level course on, or be otherwise familiar with, operating systems and networks. Prior programming experience with C or Java is recommended. Knowledge of algebra and discrete mathematics is also recommended.

Textbook

Computer Security: Principle and Practice, 3/E, by William Stallings and Lawrie Brown.

A recommended supplementary textbook is: Applied Information Security: A Hands-on Approach, by David Basin, Patrick Schaller, and Michael Schlapfer.

Grading

Grading will be based on:

- 80% Homework assignments (no late submissions unless special circumstances subject to GT rules,e.g., medical/family emergencies, and instructor approvals)
    - 20% per-and-pencil: T/F and multiple-choice on T-Square Quizzes
        - You are expected to complete two lessons each week. On Friday each week, we will release one quiz that covers the two lessons of the week, and the quiz is due on the following Friday. There will be 10 quizzes that each counts 2% (the very last two lessons are counted as one).
    - 60% projects (15% each, see schedules below):
        - Project #1: software security: buffer overflow - implement a stack overflow attack and a return-to-libc buffer overflow attack (C programing required)
        - Project #2: malware analysis: learn how to use Cuckoo to analyze malware, analyze 10 malware samples provided and report findings of various malware behaviors (some scripting may be required)
        - Project #3: crypto: build a killer app of public key cryptography
        - Project #4: web security: implement SQL Injection, XSS, and XSRF attacks (scripting)
- 20% Exams: 10% the first-half exam and 10% the second-half exam (T/F and multiple-choice)
- 10% optional project: (i.e., the maximum grade for the course is 110 points) You can choose only one of these optional projects to submit. The choices are as follows:
    - Project 1.5 (Optional Project 1): A host-based system capable of detecting buffer overflow attacks
    - Project 2.5 (Optional Project 2): An analysis of an advanced form of trigger malware
    - Project 4.5 (Optional Project 4): A testing system that can analyze a web site to detect vulnerabilities such as SQL Injection, XSS and XSRF.

Instructor

Professor Wenke Lee
Klaus 3222A
wenke.lee@gmail.com
Office hours: TTH 3-4

TAs

Schedule (slides are posted in Resources)

Lecture	Topics	Notes	Preparation/Reading
1 (8/23)	Security Mindset		Chapter 1
2 (8/30)	Software Security		Chapters 10 and 11

		Project #1	
3 (9/1)	Operating Systems Security		Chapter 12
4 (9/6)	Authentication		Chapter 3
5 (9/13)	Access Control		Chapter 4
6 (9/15)	Mandatory Access Control		Chapter 13
7 (9/20)	Database Security		Chapter 5
8 (9/22)	Malicious Code	Project #2	Chapter 6
9 (9/27)	Modern Malware		Chapters 6 and 7
	One-Hour Close-Everying Exam I on Sept 29.		
10 (10/4)	Firewalls		Chapter 9
11 (10/6)	Intrusion Detection		Chapter 8
12 (10/13)	Introduction to Cryptography		Chapter 2
13 (10/18)	Symmetric Encryption	Project #3	Chapter 20
14 (10/25)	Public-Key Cryptography		Chapter 21
15 (10/27)	Hashes		Chapter 21
16 (11/1)	Security Protocols		Chapter 23
17 (11/8)	IPSec and TLS		Chapter 22
18 (11/10)	Wireless and Mobile Security		Chapter 24
19 (11/15)	Web Security	Project #4	
20 (11/17)	Security Management and Cyber Risk Assessment		Chapters 14 and 15
21 (11/22)	Law, Ethics, and Privacy		Chapter 19
	One-Hour Close-Everyting Exam II on Dec 6		