Lecture 1: Course Overview and Security Concepts

Summary

After reviewing the course schedule, syllabus, and policies, we will cover some basic security concepts and terminology. First we introduce terms that describe the phases of the attack-countermeasure cycle: *vulnerability, threat, attack,* and *control*. Next we classify attacks into as *interception, interruption, modification,* or *fabrication* and introduce the corresponding security goals of *confidentiality, integrity,* and *availability* (CIA). We'll end by relating these terms to two real-life examples. All of the material for today's lecture *except* the two examples is also covered in Chapter 1 of Pfleeger & Pfleeger.

Course Overview

Schedule and Topics
(see website — http://www.csee.umbc.edu/~cmarron/cmsc426-626)

Textbook — Pfleeger & Pfleeger, *Security in Computing*, 4th Edition

Projects

Undergrads (426) — one project
Grads (626) — two projects

Labs

Undergrads (426) — three labs
Grads (626) — two labs

Exams

There will be a mid-term exam and a comprehensive final exam. Grad students will receive more difficult exams. **You must show a picture ID to receive and turn-in an exam.**

Project and Lab Environments

Use of Virtual Machines — I am using VirtualBox.

Projects require Minix 3 OS. Minix was developed as an educational OS; now targeted at embedded systems.

Lab 1 requires a specific Ubuntu VM (to be provided).

Lab 2 requires you to write code; I suggest Python.

Lab 3 requires Linux or Mac with OpenSSL installed.

Exercises

Homework exercises will not be graded, but I may call on you in class to provide an answer to one! The purpose of the exercises is to give you practice with the concepts. Additionally, you should consider questions of the type given in the exercises as "fair game" for an exam.

Grading

Undergrads

Labs — 30%
Project — 25%
Mid-term Exam — 20%
Final Exam — 25%

Grads

Labs — 20%
Projects — 35%
Mid-term Exam — 20%
Final Exam — 25%

Academic Integrity

You are to complete projects and labs on your own unless help is specifically authorized by me.

For projects, you may work in pairs. This does *not* mean you can get help from whoever you want so long as there are only two of you present. It means that you and a partner may agree to work together on the project; any additional assistance must be authorized by me.

The following is a non-exhaustive list of specific AI violations:

- Copying code from another student
- Being in possession of another student's code
- Providing your code to another student
- Failing to secure hardcopies of your code
- Typing code read from another student's screen
- Submitting code found on the Internet as your own work

An AI violation will result in a score of zero for the assignment and a reduction of your course score by 10 points (one letter grade).

Email

I will try to answer all emails in a *reasonable time*, which I consider to be within 48 hours. If you ask me a question by email late in the evening, it is likely that I will not see it or have time to answer it until the next day. Like you, I have a life outside of classes — emails received on the weekend may not be answered until Monday.

Security Concepts

Reference: P&P, Chapter 1

How are assets protected: the bank analogy

Why do criminals rob banks?

Why are there fewer bank robberies now than in the past?

Assets of a computer system — hardware, software, and data

How does the current computer security situation compare with banking security?

Vulnerabilities, Threats, Attacks, and Controls

Principle of Easiest Penetration

Vulnerability

Threat

Within threat, we also consider *Method*, *Opportunity*, and *Motive.*

Attack

Control

Types of Attacks

Interception

Interruption

Modification

Fabrication

How do these four types of attack apply to hardware, software, and data?

Security Goals — CIA

Confidentiality

Integrity

Availability

Some add *Non-repudiation* and *Assurance*

Case Study: Heartbleed

References:

Good starting point with links: http://heartbleed.com

XKCD Cartoon: http://xkcd.com/1354/

Describe the vulnerability, threat, attack, and control.

What security goals were violated?

Case Study: The Debian Fiasco

References:

Summary and links from Bruce Schneier
https://www.schneier.com/blog/archives/2008/05/random_number_b.html

XKCD Comic
http://xkcd.com/424/

Describe the vulnerability, threat, attack, and control.

What security goals were violated?

Exercises

P&P, Chapter 1, Exercises 2, 3, 4, 7, 10, 11, 12.

A chemical company uses a proprietary process to produce certain chemicals on an industrial scale. Some of the chemicals used in the process are potentially hazardous to humans. A Supervisory Control and Data Acquisition (SCADA) system controls the manufacturing process, carrying real-time sensor data and commands to control the process, as well as routine audit and administrative data. What are the Confidentiality, Integrity, and Availability requirements for the SCADA system?

Consider the following code snippet. Assume that the function DidUserWinLottery() is a complex function that is intended to return one of two inter constants: WINNER or NOT_A_WINNER. What is the security flaw in the code and how would you re-write it to remove the flaw?

```
int won_lottery;

won_lottery = DidUserWinLottery();

if (won_lottery == NOT_A_WINNER) {
    printf("Better luck next time!\n");
} else {
    printf("You're a winner!\n");
    DispenseCash();
}
```