Overview

Background

Goals for the course

Goals for computer security

Background

What's your background?

- academic program
- security background/interest/practices

My background

- education
- privacy and security research

I did my undergraduate degree here at Memorial; I know (and care about!) the program deeply. Then I went off to the University of Cambridge for my PhD, where I looked into some of the privacy problems with online social networking (TL;DR: there are a lot) and approaches by which we could build something better.

My graduate students and I work in privacy and security for real systems, very broadly defined. Specifically, we've done work in:

- security protocols
- operating systems
    - application sandboxing
    - cryptographic filesystems
    - security-enhanced hardware
- privacy and social networks (PhD, IEEE Security & Privacy summary)
- applications:
    - full-motion video integrity
    - health privacy
    - marine systems

Course goals

To pass! 😀

What are you looking for in this course?

My goal: give an introduction to fundamental ideas.

- "what every computer engineer should know about security"
- **not** a rigorous treatment of all aspects of computer security: foundation for further study with **some** in-depth exploration

To learn how to pass, please consult the course outline!

You won't come out of this course being an expert in computer security. Specificially, you should _____ call yourself a:

- cryptographer
- network defender
- penetration tester
- protocol designer
- secure "coder"

After completing this course, you should at least have the _____ with which to discuss security issues that come up in computer engineering.

Course content

Introduction

Software security

Host security

Network security

Web security

The four content modules of the course will be approximately similar in length, although they may not be exactly the same in breadth or depth. We will be able to go deeper in some areas than in others.

Course resources

Tools and Jewels (van Oorschot)

- Hardcover from Springer
- Free PDFs from PVO's website

Security Engineering (Anderson)

- Third edition is current
- Second edition still available as free PDFs

Everything that I'll expect you to know will be discussed in the lectures. Thus, I suggest that you _____ in these lectures of what we discuss and _____ immediately afterwards. Make sure that you _____ these ideas and, where possible, can _____ them.

In addition to the lecture materials, further reading is definitely encouraged! Rather than scouring YouTube, however, where you can find anybody to say anything, I'll point you at a couple of excellent (but still free) resources.

I am recommending a "textbook" for this course, but we won't be following it very strictly. It's a good book, though, so I'd definitely recommend checking it out. You can buy a hardcover version (which looks great on a shelf!) from Springer, but Prof. Van Oorschot publishes PDFs of the book's chapters for free on his website.

Security Engineering by Ross Anderson (no relation, apart from our academic family tree) is the most fun you'll ever have reading 1,000 pages. We'll use it as a reference, and it's another one to keep handy on your shelf.

Course evaluation

Assignments: *individual* work ("I did this")

Labs: done in pairs

(ENGI 9823) Project: *self-directed* investigation

Midterm and exam

From the course outline:

> *Academic integrity means taking full responsibility for the academic work you submit in this course, so that I can evaluate you on the basis of your own knowledge and effort. When you submit work, you must acknowledge sources of both facts (references) and their presentation (authorship). It is an academic offence to claim work as original when it has been substantially derived from another source without attribution, whether that source is another person or a generative artificial intelligence tool. If GAI is permitted in a deliverable, you must reference any GAI tools you use and provide the sequence of prompts in an appendix.*

The project (for graduate students) should be a self-directed investigation of a security topic: an attack, a vulnerability, a defensive technique, etc. Undergraduate case studies should be _____ in nature. Graduate projects need to include an element of _____ and/or _____.

We will also have traditional written exams: a midterm and a final exam.

Overview

~~Background~~

~~Goals for the course~~

Goals for computer security

Security goals

Big question:

Is my system/network/data "secure"?

Big answer:

No!

Question asked by the ignorant: "bottom line, is it secure?"

If we want a more meaningful _____, we must ask a more meaningful _____.

Security questions

Typical SE question:

Can the system do X for me?

Typical security question:

Can the system do X *against* me?

We'll do some negative thinking... but not always!

Negative thinking in two senses:

1. thinking about negative things,
2. thinking *in the negative* about what is *not* possible.

We won't *always* be thinking negatively: proper privacy and security practices can _____ amazing and even beautiful things! A secure system is one that can be extended in new and originally-unintended ways.

Thinking about security

Security properties: CIA[AAA]

Security policies

Security mechanisms

Security violations

Security activities

CIA[AAA] properties

- Confidentiality
- Integrity
- Availability
- Authentication
- Authorization
- Accountability

Confidentiality is often the first goal that people think of, but it's not always the most important. For example: believe it or not, I don't care all that much about the confidentiality of my bank account (maybe if I had more money than student debt, but that's not the case!). However, I care very much about the _____ of my bank balance and about the _____ of the banking system.

Authentication is about whether or not someone is who they claim to be (or, in some cases, whether a thing is what someone claims it to be). We will mostly use the word "authentication" in the context of _____: if the person typing at the keyboard claims to be Jonathan Anderson from Memorial University, how can we *know* whether or not that claim is true? If the person on the other end of the phone claims to be from your bank's fraud department, how can you *know* if that's true?

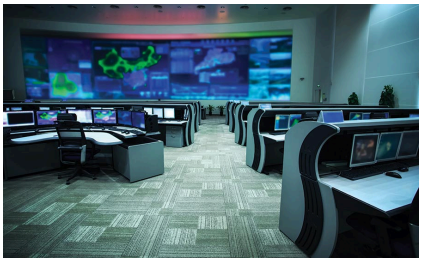
Authorization is about _____ is allowed to _____ to _____. Can user `alice` write to this file? Can `bob` serve TCP connections from port 80?

Accountability is a more abstract concept, but it's also important. We can never prevent all bad behaviours, but some can be discouraged if people know that that bad behaviour will result in negative consequences for them. This is true of `sudo` misuse, corporate embezzlement and global thermonuclear war: many people are dissuaded not by a technical measure but by the fear of consequences.

Understanding the security _____ we might want to have enables us to think clearly about...

Security mechanisms

- Techniques, systems, products, SOCs*... whee!
- Do your mechanisms give the **right properties**?
- Don't be vendor-led.
- Don't be mechanism-led.
- Start with the **policy**!



* See: https://taosecurity.blogspot.com/2018/06/why-do-socs-look-like-this.html

We'll be introduced to lots of techniques in this course: stack smashing, memory safety, fuzzing, ASLR, ROP gadgets, DAC, MAC, ciphers, hashes, John the Ripper, biometrics, compartmentalization, digital signatures, protocols, double-ratcheting private messaging, VPNs, cross-site scripting, SQL injection, Onion sites...

Big screens make for exciting television.

Being vendor-led is OK if your goal is, "we want things that look shiny that are at least as expensive as what our competitors have." Speaking cynically, that's actually what some people's goal is: to show that they've put enough money or work into their system that they can't be fired if things go South. However, that's not a security goal: it's a job security goal!

Policy talks about what we _____... how do we talk about what we _____?

Security policy

Separable from mechanism

What should happen

What should not happen

e.g., "no lone access" vs cryptography, two-factor authentication...

Mechanism is "cool" (everyone loves words like _____ and _____), but mechanism is not our first priority!

e.g., an integrity policy: video evidence is what was taken, wasn't altered

Security violations

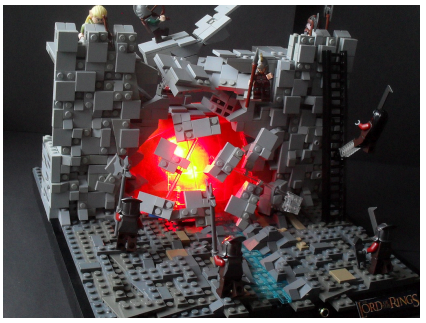
What's the worst that could happen?

Threat

Vulnerability

Adversary

Attack



_____ "combination of circumstances and entitites inclined to harm assets, i.e., cause security violations" (Oorschot)

_____ weakness that could allow a threat to be realized by an...

_____ a _____ or _____ (not a _____!) that wants to violate your policy via an...

_____ an adversary *exploits* one or more vulnerabilities (the *attack vector*) in order to bring the threatened harm about

Security activities

Proactive:

- Threat modeling and risk assessment
- Prevention and mitigation

Reactive:

- Incident response and post-attack mitigation
- Attribution... and response

This course will focus on the _____ elements of this problem. How have attackers exploited vulnerabilities, and how can we use that knowledge to _____ that are _____ to attack?

Reactive elements of computer security are also important, but they aren't the focus of this course. Somebody absolutely needs to do _____, to identify _____ and _____. However, those things are mostly of interest to engineers insofar as they help us _____.

Next time...

Threat modeling

Adversarial thinking