(Advanced) Computer Security!

Introduction to Software Security

Prof. Travis Peters

Montana State University

CS 476/594 – Computer Security

Spring 2021

https://www.traviswpeters.com/cs476

Reminders

- Please update your **Slack profile**
  - first name, last name, nice photo
- Please update your **GitHub profile**
  - first name, last name, nice photo
- Please update your **Zoom profile**
  - first name, last name, nice photo

  -> Let's take a minute now to do this for Zoom...

Today

- Announcements
  - Lab 0 was due earlier today – how'd it go?!
  - Are folks getting updates on **#announcements**?

- Learning Objectives
  - Basic ideas from security
    - CIA Triad (plus…)
    - Common threats & defenses
    - Threat Modeling 101
  - Review some basics
    - Models/layout of a computer & a program
    - Basic C programming and command line usage
    - Linux & Basic Linux Security

Are These "Systems" Secure?

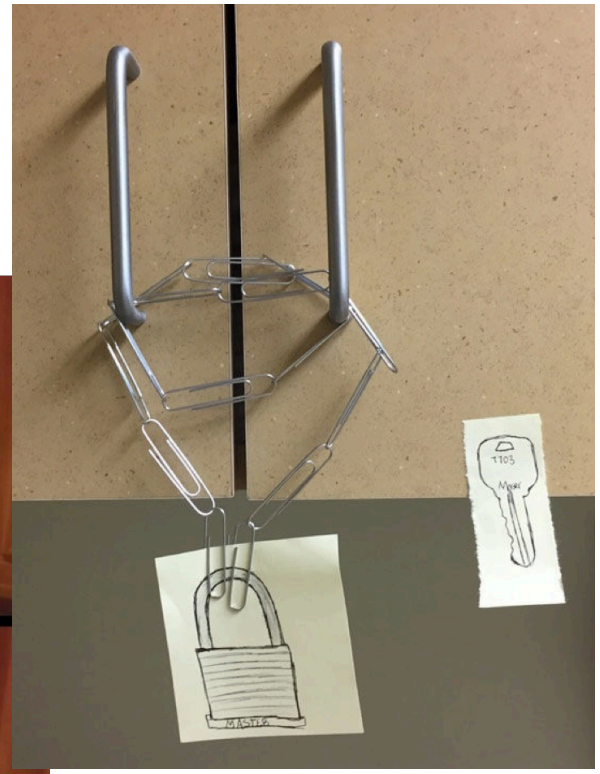


Photo credits: https://brightside.me/wonder-curiosities/20-ridiculous-security-fails-that-are-too-good-to-be-true-426810/

Security

Think. Pair (Break Out Rooms). Share.

What is security? (What is security **not**?)

Protection of assets
Controlling access
Threat mitigation
protective measures (mechanisms)

↔

data integrity
intention

Policies

Why is it important?

protection of privacy, property, etc.
prevent negative things from happening
safety

Popular examples? Examples you've encountered?

Equifax
Parler / data breach
Cambridge A.
Election integrity

destruction of COVID vaccines
scammers / ransomware
SolarWinds
Myrai
Stuxnet

What can we do about security issues?

Learning from past issues/attacks } post-mortem
Have a plan/strategy
Test it! (Red/Blue team)
Passwords / authentication (2F, MF)
↳ password managers
physical isolation

patch/update software
antivirus
firewalls
deterents (legal?)

Security: The Basics

Information Security

- CIA
  - Confidentiality – protection from **unauthorized access** (e.g., snooping)
  - Integrity – protection from **unauthorized modification** (e.g., tampering)
  - Availability – protection from **interruption** (e.g., denial of service)

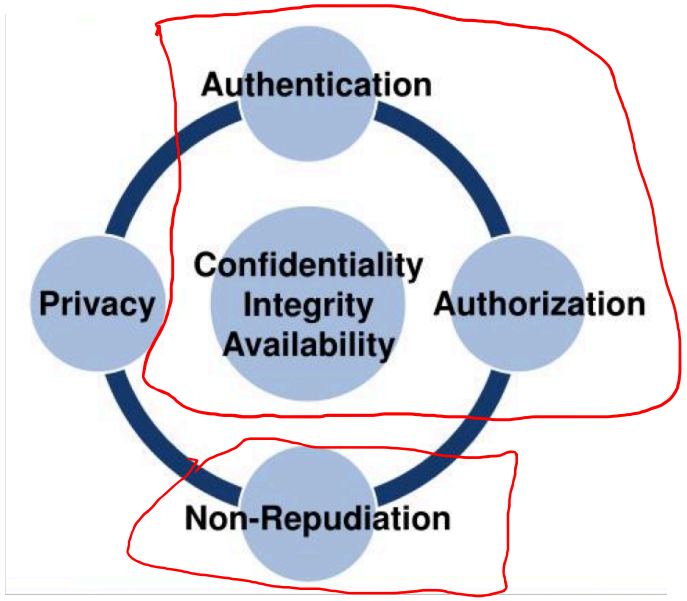
encryption

traditional infosec model
(a bit dated... but widely accepted)

Information Security

- CIA
  - Confidentiality – protection from **unauthorized access** (e.g., snooping)
  - Integrity – protection from **unauthorized modification** (e.g., tampering)
  - Availability – protection from **interruption** (e.g., denial of service)
- Also…

traditional infosec model
(a bit dated… but widely accepted)



…increasingly common to
include other goals

Common Threats & Attack Vectors

A.K.A. Goals of an Attacker

- Denial of Service (DoS)
  - violates the **availability** property (re: CIA)
- Information Leakage / Data Corruption
  - violates the **confidentiality** property (re: CIA)
  - violates the **integrity** property (re: CIA)
- Privilege Escalation ("Confused Deputy")
  - control flow hijacking
  - code/command injection
  - code reuse

NOTE:
An attacker may have other goals,
but we will mostly look at examples related to these goals in this class.

Defending Against Software Vulns.

In This class we will primarily focus on software security

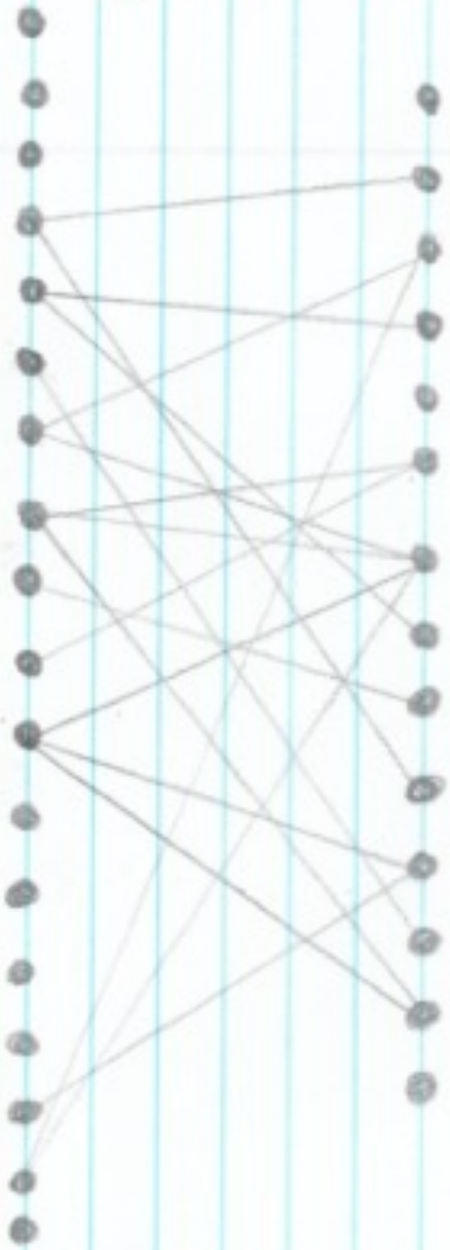
- Formal verification (not covered in this class)
- (Re)writing software in safe programming languages
- Software testing
- Built-in mitigations

How do we come up with all of this?

What's the "right" approach?

Security Controls

Sc1 Account Timeouts
Sc2 Account lockouts
Sc3 Two-factor authentication
Sc4 Password complexity guidelines
Sc5 Configure Device Ports
Sc6 Patch management
Sc7 Intrusion Detection/Prevention
Sc8 Data encryption
Sc9 Air-Gap from network
Sc10 Physical security
Sc11 DOS Protection
Sc12 Event Reporting
Sc13 offsite Data Backups
Sc14 Antivirus protection
Sc15 Penetration Testing
Sc16 Input sanitation
Sc17 Code Signing
Sc18 Runtime Application Self-protect

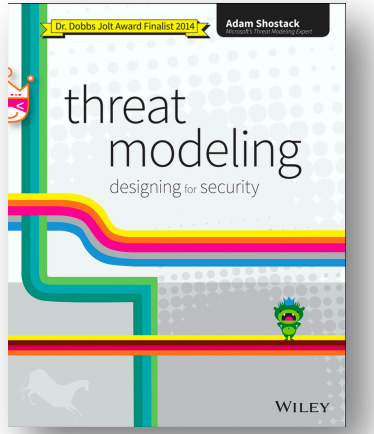


V1 Hardcoded PWDs
V2 Weak PWDs
V3 Command Injected flaw
V4 Open Ports
V5 No account lockout
V6 Unencrypted services
V7 insecure web applications
V8 insecure network services
V9 insecure cloud interface
V10 Account enumeration
V11 Cross-site scripting
V12 Buffer overflow
V13 removal of physical security
V14 missing authorization

Vulnerabilities

Former CSCI 476 Student
(Thanks, Maddi Tandberg!)

Basic Threat Modeling



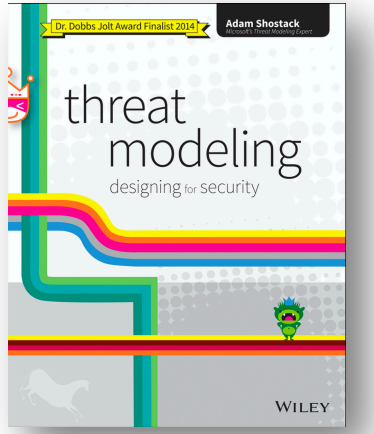
NEED: A consistent and structured approach to defense.

You begin threat modeling by focusing on four key questions:

1. What are you building?
2. What can go wrong?
3. What should you do about those things that can go wrong?
4. Did you do a decent job of analysis?

Basic Threat Modeling

"What's Your Threat Model?"

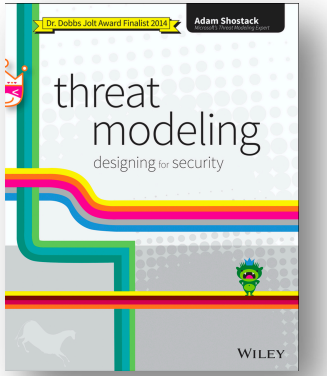


- A simple question to reveal **who**/**what** you're worried about!

- Common answers:
  - *"An attacker with the laptop"*
  - *"insiders"*
  - *"A thief could steal your money"*
  - *"Employees have access to sensitive documents and are not trusted"*
  - *"An untrusted network"*
  - *"An attacker can steal my cookie (web or otherwise)"*
  - *"huh?"*

Basic Threat Modeling

"What's Your Threat Model?"



Brainstorming Variants…

- Free-form brainstorming – Gather around a whiteboard; enumerate threats/possible defenses
- Scenario Analysis - Propose a scenario and ask "what might go wrong?"
- Pre-Mortem - Given a project/deadline, assume failure. What do you do next?
- Movie Plotting – Pick outrageous ideas; what happens next? (Think: Ocean's Eleven, The Italian Job, etc.)
- Literature review – study systems that are similar to yours

Try it! (Scenario Analysis)

Threat Model handing your phone to a cute person in a bar…