Operating Systems!

Security:
Introduction to (OS) Security
(part 1)

Prof. Travis Peters

Montana State University

CS 460 - Operating Systems

Fall 2020

https://www.cs.montana.edu/cs460

Some diagrams and notes used in this slide deck have been adapted from Sean Smith's OS courses @ Dartmouth. Thanks, Sean!

Today

- Announcements
  - *Done* grading PA3! ☺
  - Exam 2 details coming soon (11/20? 11/23?)

- Upcoming Deadlines
  - **Project Submission (HARD DEADLINE)**
    Sunday [11/15/2020] @ 11:59 PM (MST)
  - **Project Evaluations (HARD DEADLINE)**
    Wednesday [11/18/2020] @ 11:59 PM (MST)
  - **Exam #2**
    TBD… Leaning towards Friday (11/20)
    -> current poll shows 81% (26 people) vs. 19% (6 people) favoring 11/20

Security

- What is it? identify weaknesses vulnerabilities → find defenses
- Why is it important? sensitive info: credentials, medical records, banking info, PII; safety → Availability; integrity (tamper) → CIAAR
- Why is this an OS issue? Your machine could be taken over / unusable / inaccurate view of the system

Today

- Agenda
  - ~~The Basics~~
  - Buffer Overflows (an illustrative example of [OS] vulns and countermeasures)
  - Access Control
  - (Authentication)
  - (The Future of Authentication?)
  - (SGX & Trusted I/O?)

-> Take CSCI 476/594 next semester! ☺
(Tu/Th @ 3:05-4:20pm) -> I already see almost 60 people signed up!

Take Computer Security Next Semester!

CSCI 476/594 (Computer Security / Advanced Security) – Spring 2021

- **Introduction & Security Overview/Basics**
  - basic concepts
  - linux security basics
- **Software Security**
  - classics attacks: : Set-UID attacks, env. variable attacks, buffer overflow attacks (, format string attacks)
  - recent issues in SW: return-oriented programming, Shellshock attack
- **Network & Web Security**
  - SQL injection attacks, XSS
  - sniffing, spoofing, and network attacks (e.g., TCP/IP)
- **Crypto**
  - symmetric & asymmetric cryptography
  - encryption & decryption
  - digital signatures
- **Recent Topics (as time permits, e.g., side-channel attacks)**

The Basics

Threats

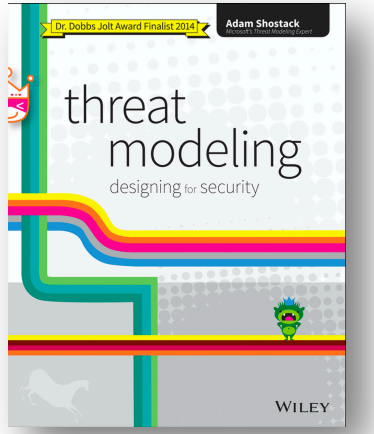
- Intruders
  - **Masquerader** Non-authorized actor that tries to impersonate a legitimate user / exploit a legit. user's access privileges (**outsider**)
  - **Misfeasor** A legit. user that abuses their inside access to carry out nefarious deeds (**insider**)
  - **Clandestine** Any entity that seizes **privileged control** of a system and **evades detection**

- Malicious Software ("Malware")
  - **Trojan Horse** Code that misuses its environment
    - classic examples: NetBus, Back Orifice (BO), Back Orifice 2000 (BO2K)
  - **Backdoor** A "feature" that enables an adversary to bypass normal security procedures (e.g., specific user identifier or password)
    - classic examples: LiteBot, Remote Connection (RedNeck)
  - **(Stack/Heap) Buffer Overflow** Exploits overflow bug to obtain ability to execute arbitrary code
    - classic examples: Internet worm (fingerd), Code Red (IIS), SQLSlammer (MS SQL Server)
  - **Spyware** SW that installs itself on a computer, reports personal info or activities
    - classic examples: adware, stealware

Security Goal

PREVENT attempts to gain unauthorized privileges
(or at least **DETECT** it…)

Basic Threat Modeling



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?

NEED: A Systematic Approach to "Threat Modeling"

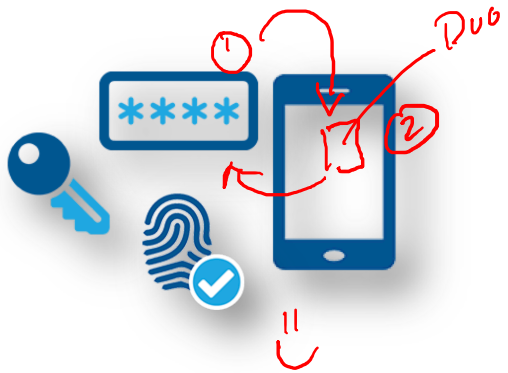
E.g., **STRIDE**
= Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege
https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN

-> help developers identify types of attacks that software tends to experience

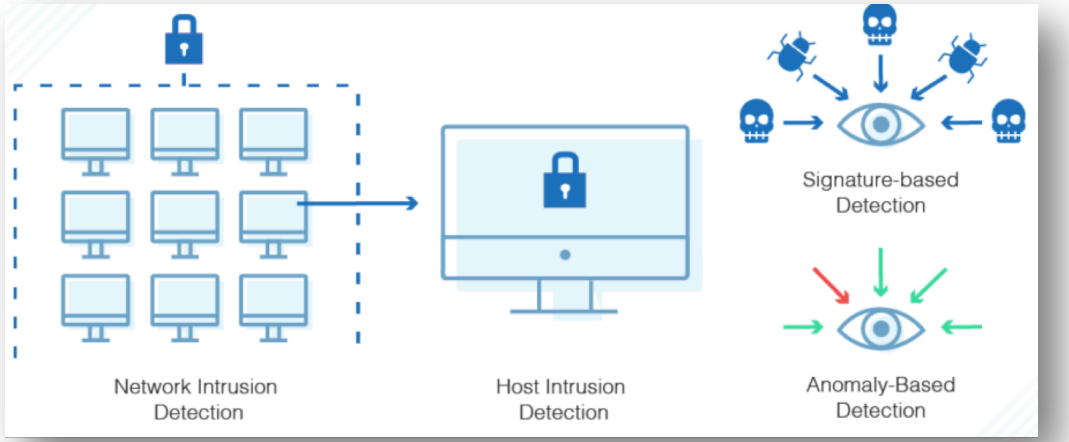
+ Attack Trees, OWASP Top 10, etc.

General Countermeasures / Defenses

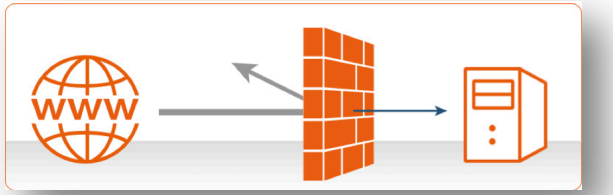
(Multi-Factor) Authentication & Access Control



Intrusion Detection Systems (IDS)



Firewalls



+ "Hardening" the OS/system

(updating/patching, removing unnecessary services, testing, etc.)

General Countermeasures / Defenses

K. Wang and S. Stolfo. Anomalous Payload-Based Network Intrusion Detection. Recent Advances in Intrusion Detection, 2004.

Intrusion Detection Systems (IDS)