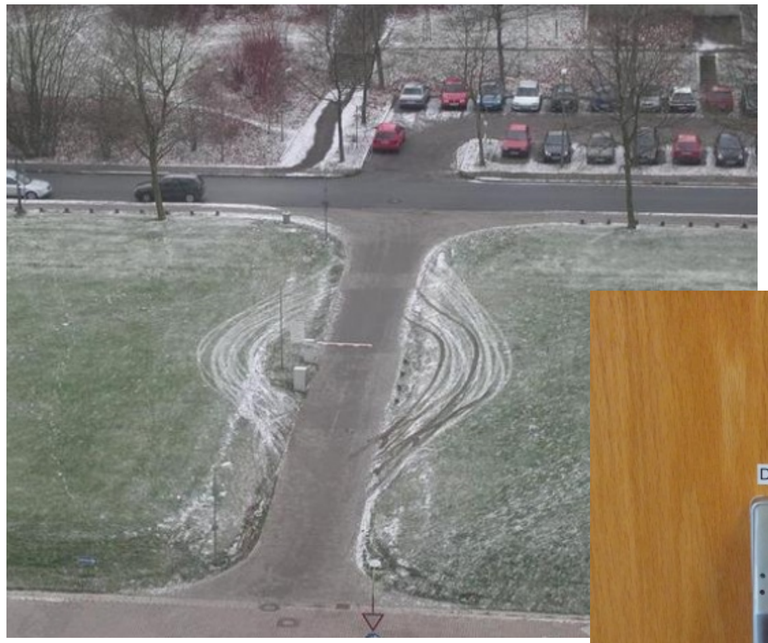
Introduction to Computer Security (Part I)

Professor Travis Peters
CSCI 476 Computer Security
Spring 2020

So what are we doing here?

- Learning to think about security!



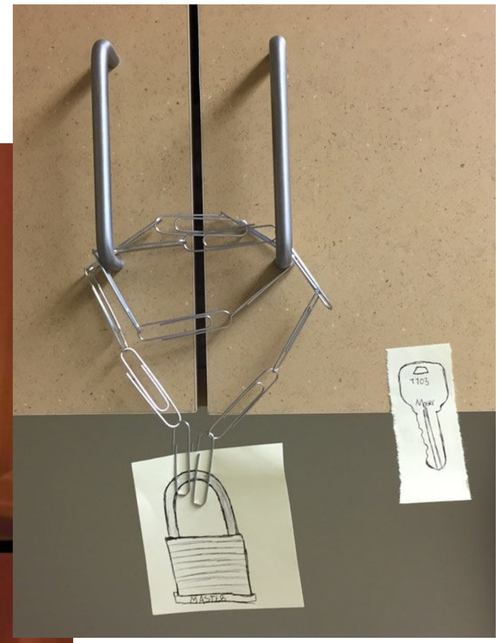


Photo credits: https://brightside.me/wonder-curiosities/20-ridiculous-security-fails-that-are-too-good-to-be-true-426810/

OK, OK, HA HA. So what *is* security?

Think-Pair-Share Activity:

You Tell Me!

What is security?

What is security ***not***?

Popular examples?

Examples you've encountered (recent or past)?

The Standard Rubric: C.I.A. *a.k.a The CIA Triad*

Confidentiality *> the system does not reveal data to the wrong parties*

Integrity *> data the system stores does not get changed in inappropriate/illicit ways*

Availability *> the right parties can always use the system when they need it*

- Is this definition sufficient?
  - Is each property equally important? (Examples?!)
  - Authenticity / Non-repudiation (CIAA) *> inability to deny a commitment to do something/having done something*
  - *There are many others…*

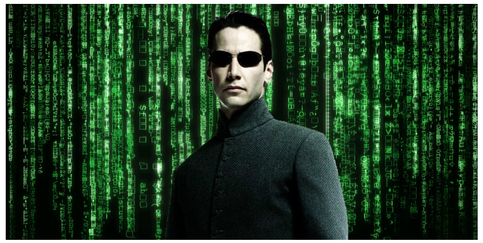
- Oft used to describe requirements for ***information security*** *(InfoSec) /* ***data security***

- What about other types of security?
  - Physical security?
  - Critical infrastructure security?

The Craft of System Security - 1st Edition. Sean Smith (2007).

The Matrix

- No, no… not *that* Matrix



- The Access Control Matrix

  The idea: *prevent the wrong people from doing the wrong things within a system*

  - specify what are the objects,

  - who are the subjects, and

  - what subjects can do to which objects

SYSTEM

SUBJECTS	OBJECTS: File 1	File 2	File 3	File 4
User A	Own Read Write		Own Read Write	
User B	Read	Own Read Write	Write	Read
User C	Read Write	Read		Own Read Write

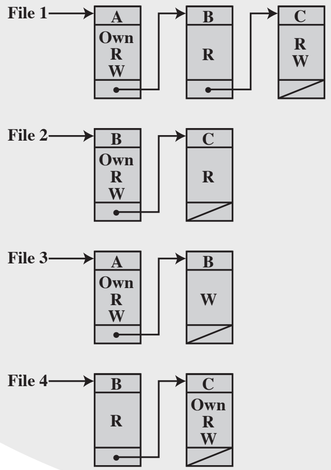
For each subject → easy to look up their capabilities

For each object → easy to look up authorized users

Simpler:

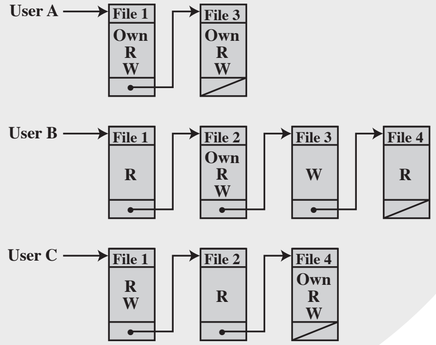
"Access Control List (ACL)"

objects → subjects



"Capabilities" List

subjects → objects



SYSTEM

So…

- Is our system secure?
  - CIA?
  - Access Control Matrix / Access Control Lists / Capabilities Lists?

- Maybe better questions are:

*Given a **model** of the threats to our system,*
how much of our resources should we expend
to mitigate the risk and impact of an attack?

*Who is the **adversary**? What **resources** do they have? What **capabilities** do they have?*

***Detect** or **Prevent**?*

*What's the **cost**?*

In general, define the adversary and see whether the system can remain in a good state despite the adversary

The Take-Home Message

*Learning to **think** about security!*

At the end of the day, security is hard to define!

The security & privacy field is always evolving:

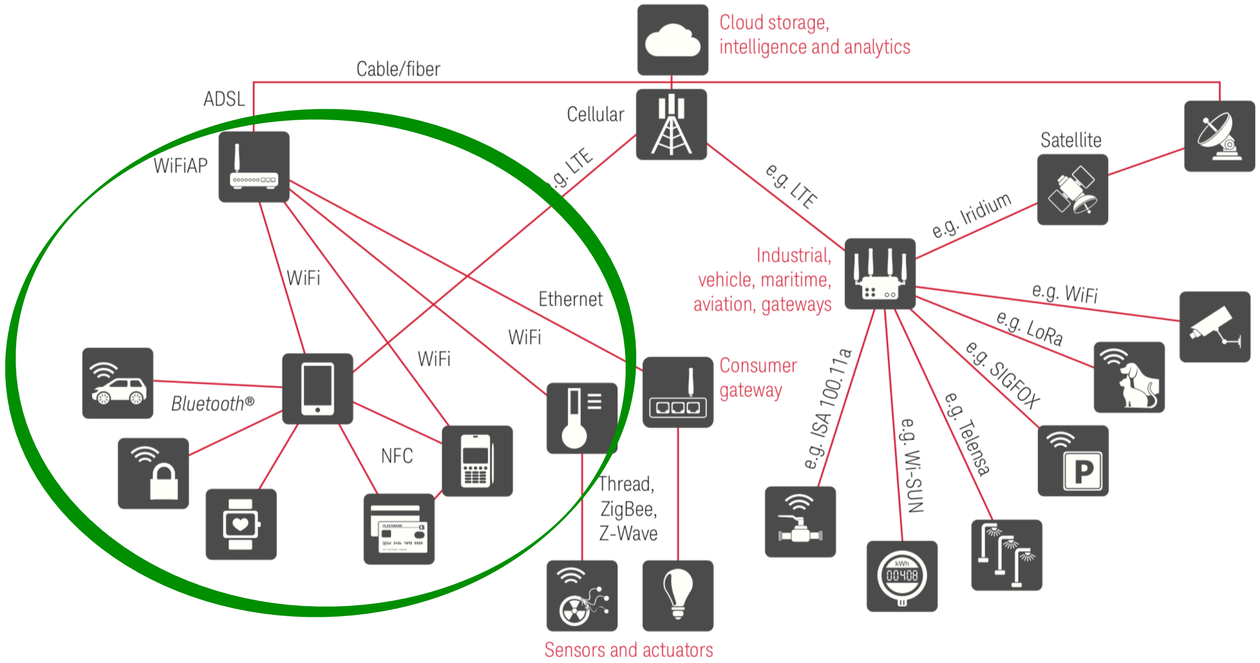
- new **assets**
- new **threats**
- new **capabilities**
- new **technologies**

You need to be ready to think through new situations that arise, leveraging what you've already learned (here, past experiences, case studies, reports, etc.) to find S&P solutions for those new situations.

Sounds intriguing! But uh… who *is* this guy?

- **Travis Peters (me)**
  - New prof @ MSU as of Fall 2019
  - Enthusiastic about helping other people learn about security!

- In my work, I mostly wear the hat of the "defender"
  - **wireless security** solutions for IoT, Wi-Fi, Bluetooth/BLE
  - **system security** solutions for mobile health devices, popular PCs
  - **data security** for sensitive user data



Key Insight Technologies, IoT Infogram - https://www.keysight.com/us/en/home.html

Also: The Age of Devastating Vulnerabilities

LILY HAY NEWMAN SECURITY 07.29.19 11:04 AM

AN OPERATING SYSTEM BUG EXPOSES 200 MILLION CRITICAL DEVICES

Think of how the WannaCry ransomware used the Eternal Blue Windows vulnerability to spread across networks and around the world. It's like that, but with firewalls, industrial equipment, and medical devices instead of Windows machines. The result could be anything from device malfunctions to full system takedowns.

MOTHERBOARD TECH BY VICE | By Kim Zetter | Mar 25 2019, 9:00am

Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers

The "solutions"…

TC

*"How do you stay safe? **Keep all of your devices updated** regularly and **be wary of older IoT devices**."*

THE VERGE

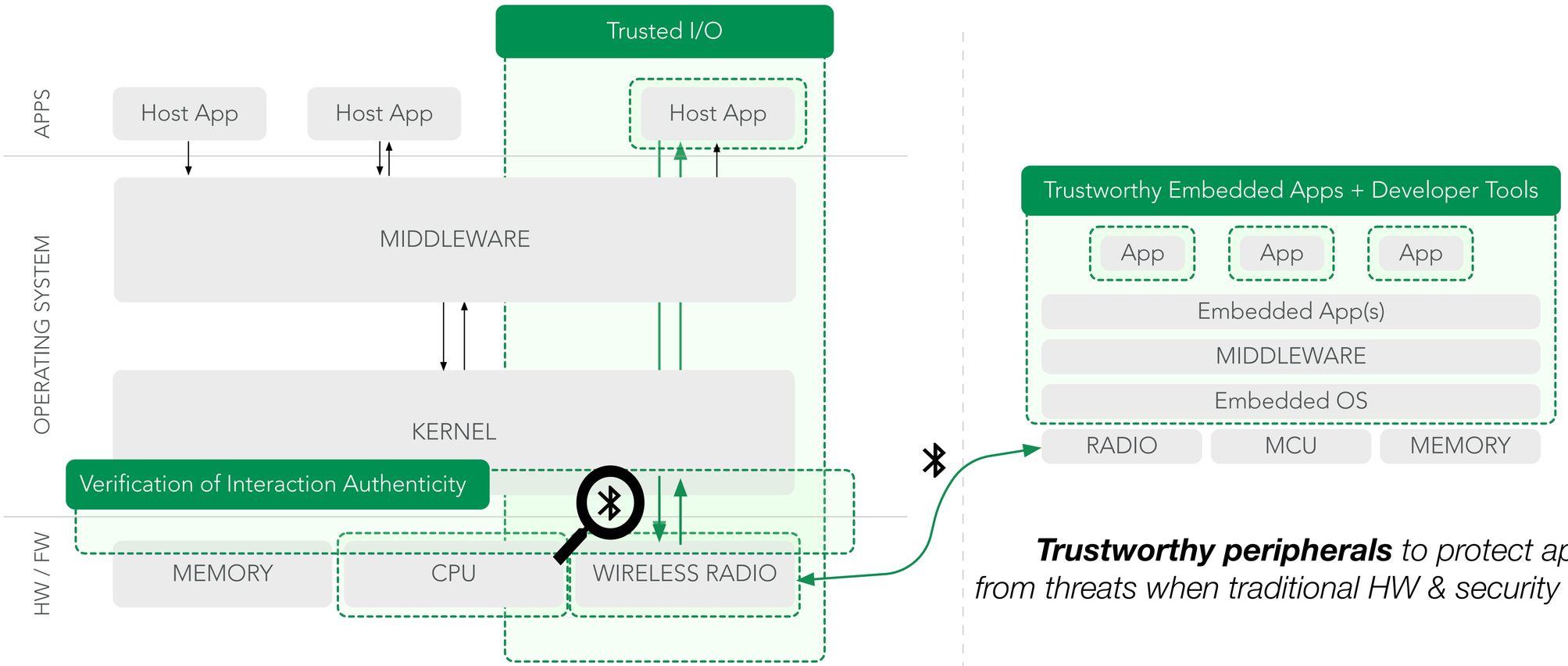
*"The simplest protection is to **leave Bluetooth off**, but since phones are still vulnerable when they're connected to a Bluetooth device, **the only recommendation is not to use Bluetooth at all**."*

There must be a better way….

My Research

Towards more trustworthy WPANs

Trustworthy I/O *to protect user data from privileged threats*



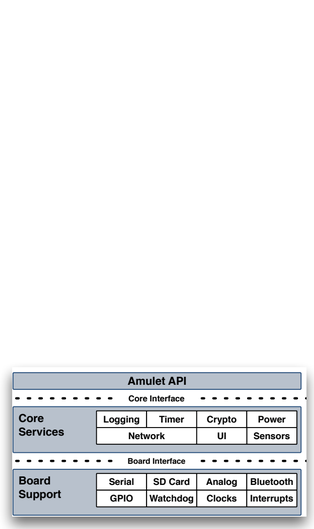
Trustworthy peripherals *to protect apps & data from threats when traditional HW & security is not available*

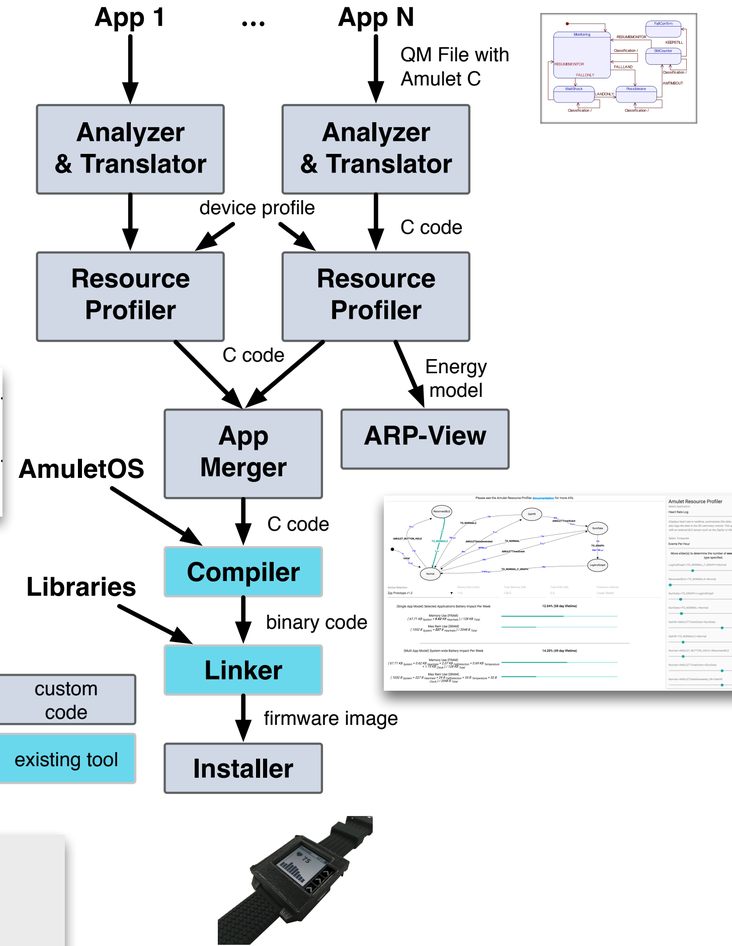
Verification of Trustworthy Interactions *to protect apps & devices over time*

Amulet

Better security for resource-constrained devices — "Security on a Budget"

- A secure & efficient mHealth platforms that
  - ***isolates apps*** through compile-time and run-time isolation mechanisms;
  - ***controls access*** to system resources through authorization policies;
  - ***profiles resource usage*** of apps through static analysis of code;
  - generates dynamic ***tool to aid applications developers***; *and*
  - merges applications & Amulet OS into a ***smaller, faster, more secure firmware image suitable for peripheral devices***.





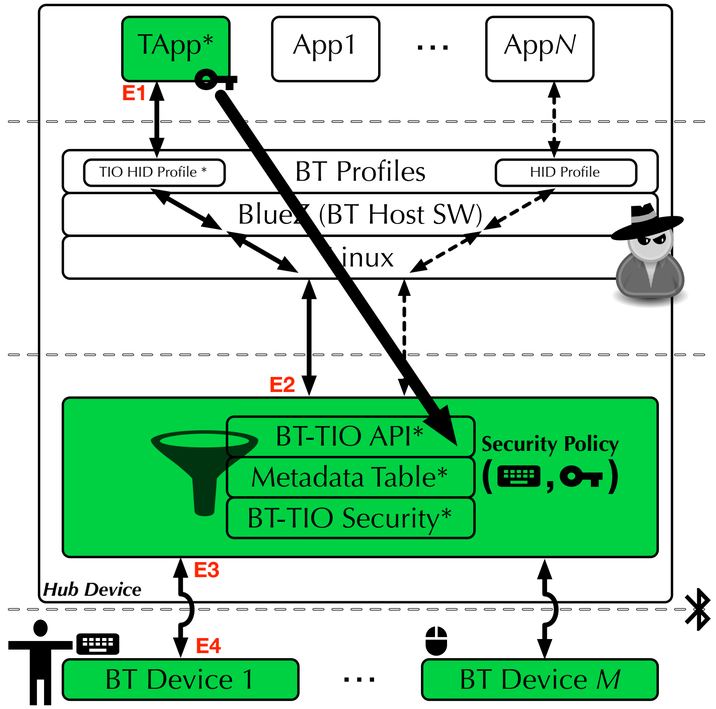
1. Josiah Hester, *Travis Peters*, Tianlong Yun, Ronald Peterson, Joseph Skinner, Bhargav Golla, Kevin Storer, Steven Hearndon, Kevin Freeman, Sarah Lord, Ryan Halter, David Kotz, Jacob Sorber. **Amulet: An Energy-Efficient, Multi-Application Wearable Platform**. Proceedings of the ACM Conference on Embedded Networked Sensor Systems (SenSys'16). November, 2016.

2. Andres Molina-Markham, Ronald Peterson, Joseph Skinner, Tianlong Yun, Bhargav Golla, Kevin Freeman, *Travis Peters*, Jacob Sorber, Ryan Halter, David Kotz. **Amulet: A secure architecture for mHealth applications for low-power wearable devices**. Proceedings of the Workshop on Mobile Medical Applications - Design and Development (WMMADD'14). November, 2014.

BASTION-SGX

Bluetooth and Architectural Support for Trusted I/O on SGX

- Achieved ***trustworthy app-device I/O*** through platform extensions rooted in Bluetooth Controller firmware that
  - unobtrusively collects per-channel metadata;
  - uses metadata to secure I/O data between app and Bluetooth Controller *without*…
    - relying on untrusted host software, or
    - requiring changes to SGX, Bluetooth device, or Bluetooth standard.
- Prototype and case study demonstrates effective mitigation of ***privileged keylogger,*** which cannot access user input data from connected Bluetooth device (keyboard).
- Analytical evaluation demonstrates acceptable impact to memory, latency, and throughput.



1. *Travis Peters*, Reshma Lal, Srikanth Varadarajan, Pradeep Pappachan, David Kotz. **BASTION-SGX: Bluetooth and Architectural Support for Trusted I/O on SGX**. Proceedings of the Workshop on Hardware and Architectural Support for Security and Privacy (HASP'18). June, 2018.

2. Srikanth Varadarajan, Reshma Lal, Steven B. McGowan, Hakan Magnus Eriksson, *Travis W. Peters*. **System, apparatus and method for providing trusted input/output communications**. U.S. Patent 10,372,656, August 2019.

3. *Travis Peters*. **A Survey of Trustworthy Computing on Mobile & Wearable Systems**. Dartmouth College Technical Report TR2017-823. May, 2017.

A few slides skipped here (unpublished work :-)

Sounds intriguing! But uh… who *is* this guy?

- **Travis Peters (me)**
  - New prof @ MSU as of Fall 2019
  - Enthusiastic about helping other people learn about security!

- In my work, I mostly wear the hat of the "defender"
  - **wireless security** solutions for IoT, Wi-Fi, Bluetooth/BLE
  - **system security** solutions for mobile health devices, popular PCs
  - **data security** for sensitive user data

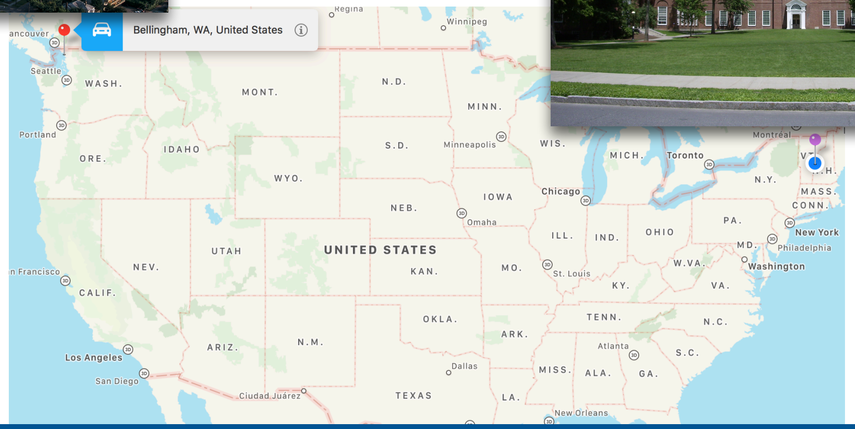
Check out my website for links to papers, etc. if you are interested :-)

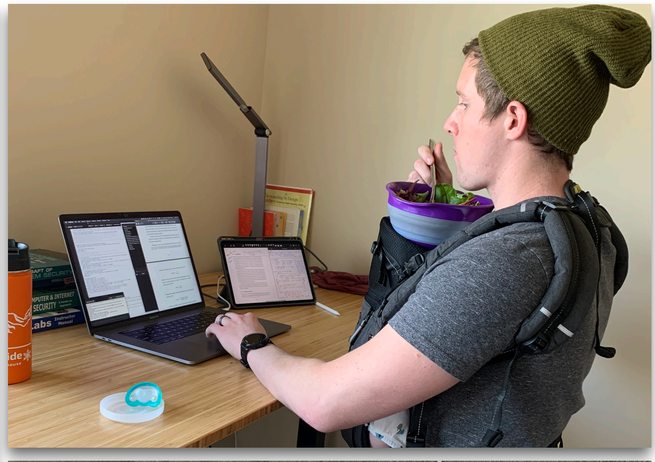
https://www.traviswpeters.com

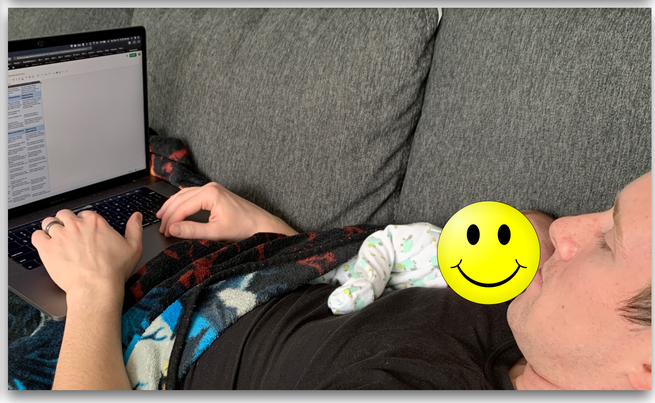
Key Insight Technologies, IoT Infogram - https://www.keysight.com/us/en/home.html

Sounds intriguing! But uh… who *is* this guy?

- Beyond the prof/researcher/security enthusiast…
  - A new dad! *(note: FMD this term…)*
  - I do other stuff too…
    - reading, running, biking, (amateur) woodworker, netflix, …
  - ugrad @ Western Washington University
  - grad @ Dartmouth







So what are we doing this semester? *The 30,000' View*

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
- sniffing & spoofing
- network attacks (e.g., TCP/IP)

Crypto

- symmetric & asymmetric cryptography
- Encryption & decryption
- digital signatures

System Security / Recent Topics

- Side-channel attacks

Admin Stuff

Course website:

https://www.traviswpeters.com/cs476/

Let's take a minute now to walk over a few important things…

- Office Hours
- Textbook
- Course Tools……..
- Grading
  - Labs (tentatively,
  - Final Exam
- Please bring laptops to class (at least on Thursdays). Please no using cellphones in class…
- Accommodations—talk to me and/or the appropriate office (notes, tests, etc.)
  - Note taking, anyone?!

Looking ahead…

Pro Tips

- Do the labs! AND START EARLY!
- Go to office hours — we aren't scary, and we are here to help! :-)
- Ask questions
- Try stuff!

For next time, think about…

- Note taking, anyone?
- Please be sure to fill out the **Questionnaire** (link on the website)
- Keep an eye out for **Lab 00** (setting up the work environment) — "due" next week
  https://www.traviswpeters.com/cs476/labs

Introduction to Computer Security (Part II)

Professor Travis Peters
CSCI 476 Computer Security
Spring 2020

Today

Announcements

- We need a note taker for the class! ➡ ***Contact ODS if interested***
- Lab 00 ➡ ***It's up!***
- Bring your laptops (especially on Thursdays—in general, these will be more hands-on days!)

Goals & Learning Objectives

- Review some basics
  - Models/layout of a computer & a program
  - Basic C programming
  - Basic command line usage
  - Linux & Basic Linux Security

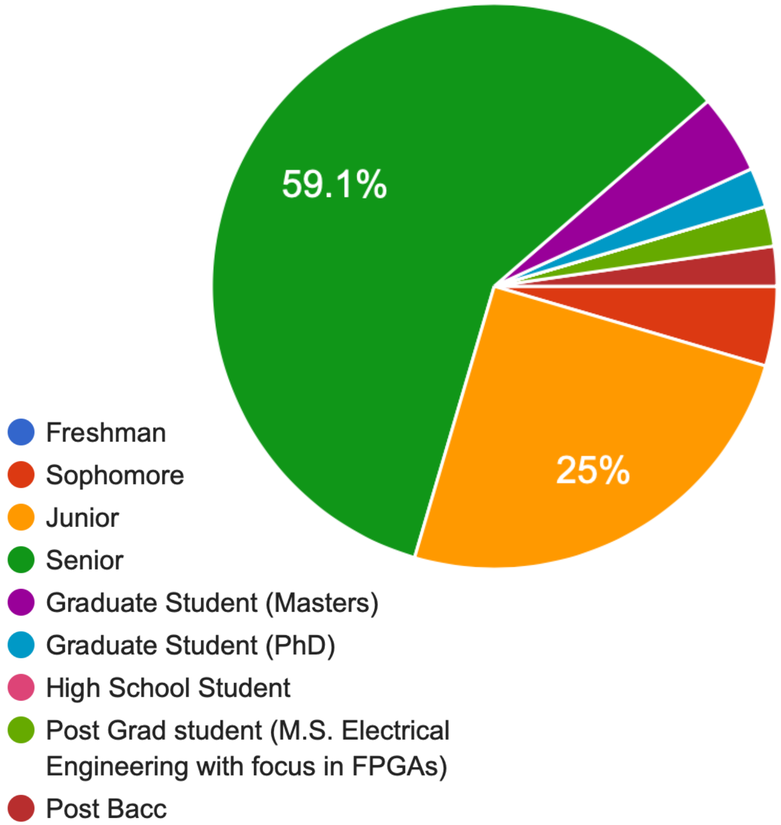
BUT FIRST, Some Insights From the Questionnaire!

The results are in! (mostly…)

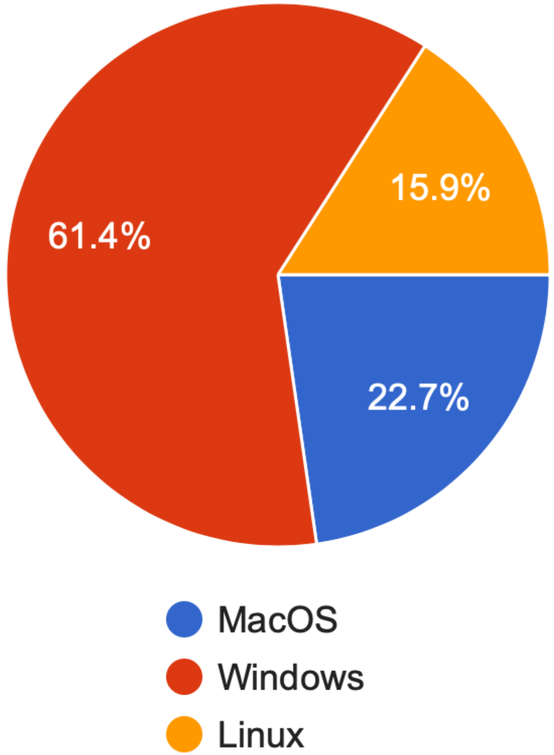
First, Some Insights From the Questionnaire!

Some insights into who we are, our coursework backgrounds, and what types of OS/machines we use

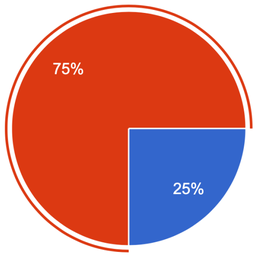
Who do we have in the class?



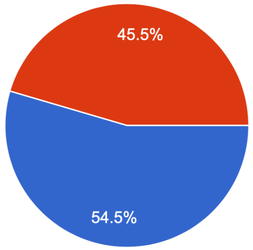
What OS/machine are people using?



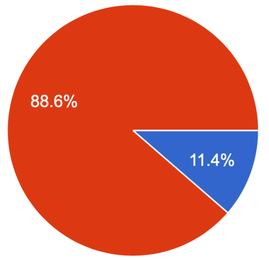
Have you taken OS?



Have you taken Networks?

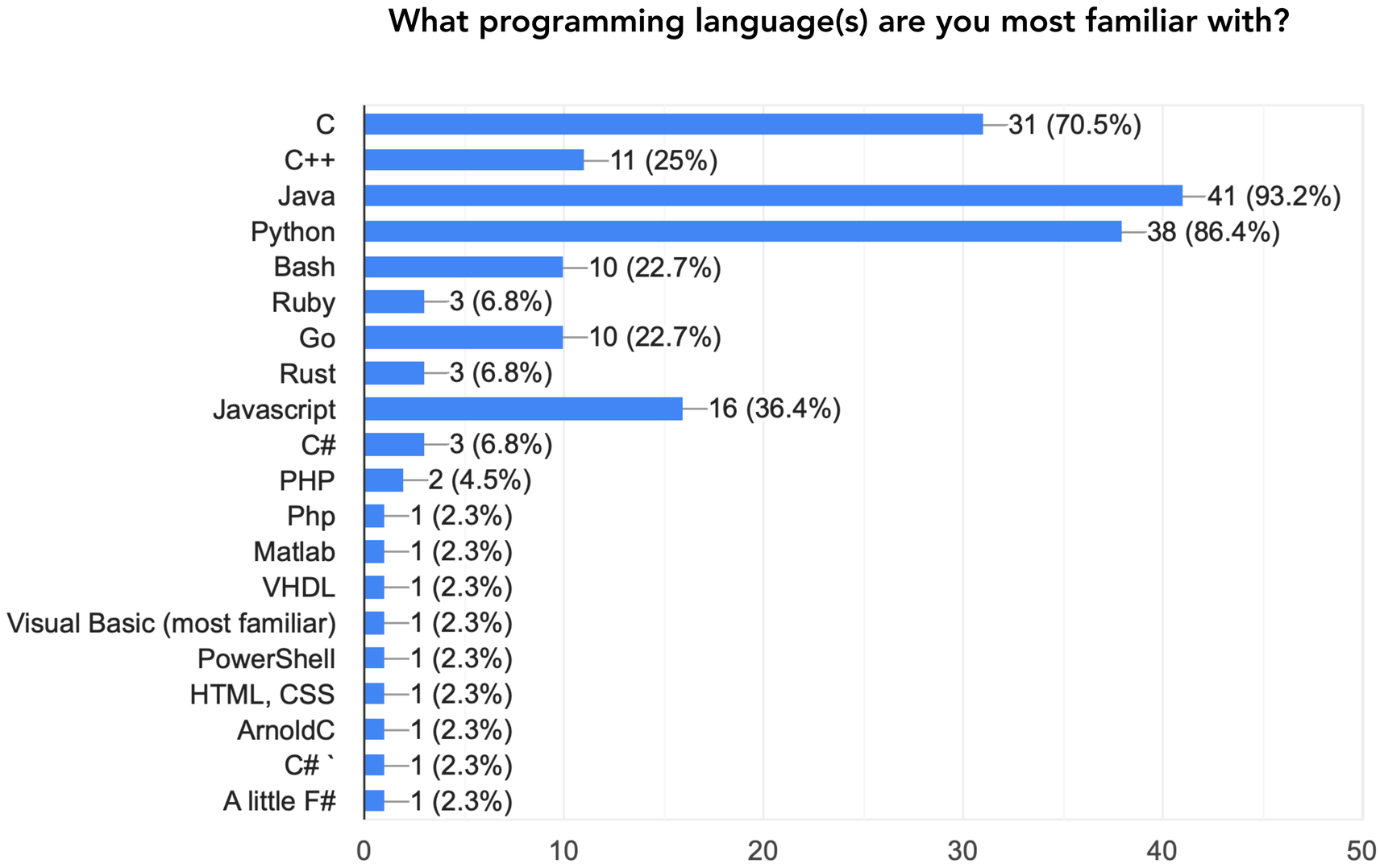


Have you taken Security?



First, Some Insights From the Questionnaire!

Some insights into what programming languages we use



First, Some Insights From the Questionnaire!

Some comments from the class

So I can understand what threats actually exist in the real world to reduce the exposure of the attacks within the systems I build.

I want to do Infosec as a career

I'd like to explore options for a career involving computer security but I don't yet have a security background.

I want to learn how to protect information.

Why are you taking CSCI 476?
What do you really hope to learn?

it's a 400 level class

need the credit, sounded really interesting

Some people also said nice things about me…

People also seemed to be interested in…

Web Security (e.g., JWT), Crypto, Internet Security, VPNs, Cybercrime, ML in Security, DNS Vulns, CPU Vulns, Best Practices, …
How to be the best hacker ever
How to break all the things

…we won't cover all of these topics, but it should be a good starting point for you!

First, Some Insights From the Questionnaire!

Some comments from the class (cont.)

I generally like the option to work alone on projects and assignments.

I work full-time/ on the weekends/ part-time as an intern

I really like to read textbooks. I prefer an introduction to the topic in class so that I can further read about it in my own time. I wouldn't mind occasional lab periods, but I prefer going to your office hours for specific questions.

I love programming projects that let me apply what I'm learning.

Anything else I should know about you?

Who's honestly good on exams?

I hate and love computers.

I would love to do research in this area, if you have any ideas or advice please let me know!

C > Python, Linux > Windows, Ford > Chevy

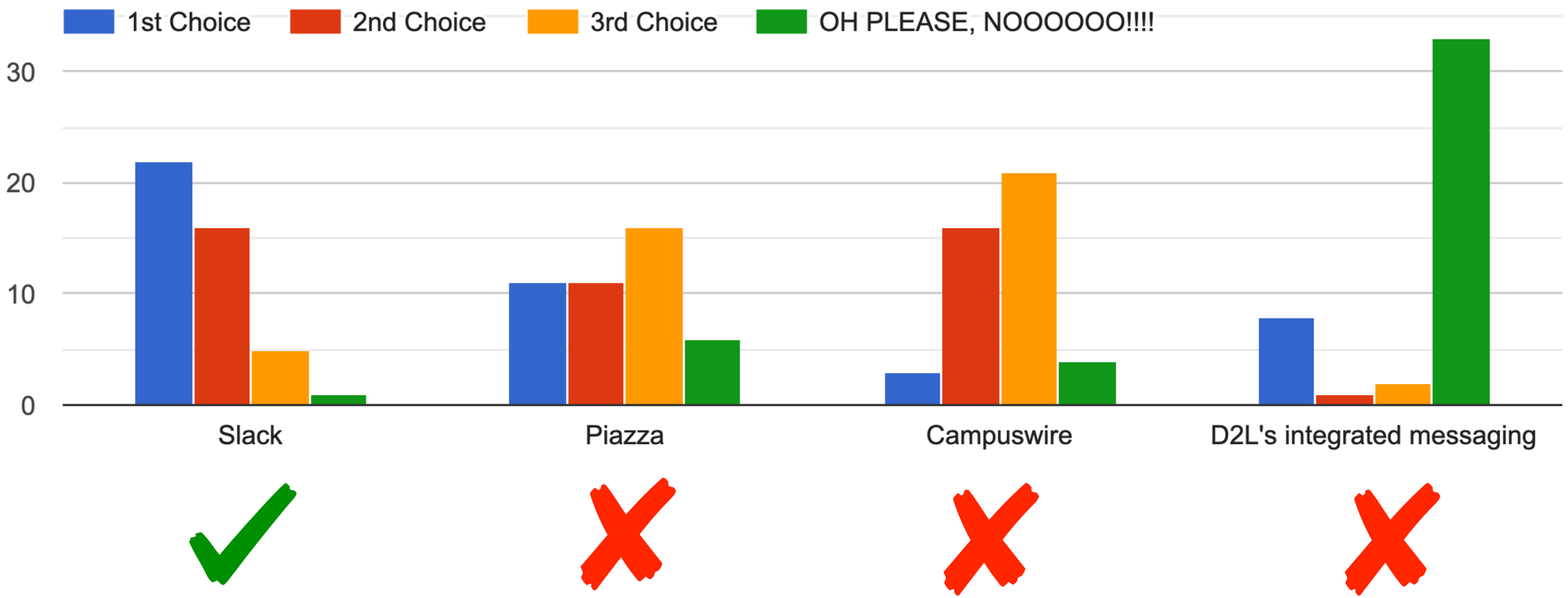
Office hours definitely scare me because I never feel like I know what to ask

This class intimidates the heck out of me. Answering your questions about OS and networks is concerning me even more because I don't know really anything about either of those.

First, Some Insights From the Questionnaire!

Some insights into our communication preferences

If we were to use ONE TOOL for COURSE COMMUNICATIONS, what is your preference?



First, Some Insights From the Questionnaire!

Some insights into our communication preferences

*Some in class exploration — let's take a quick peek at **Slack***

— https://media.tenor.co

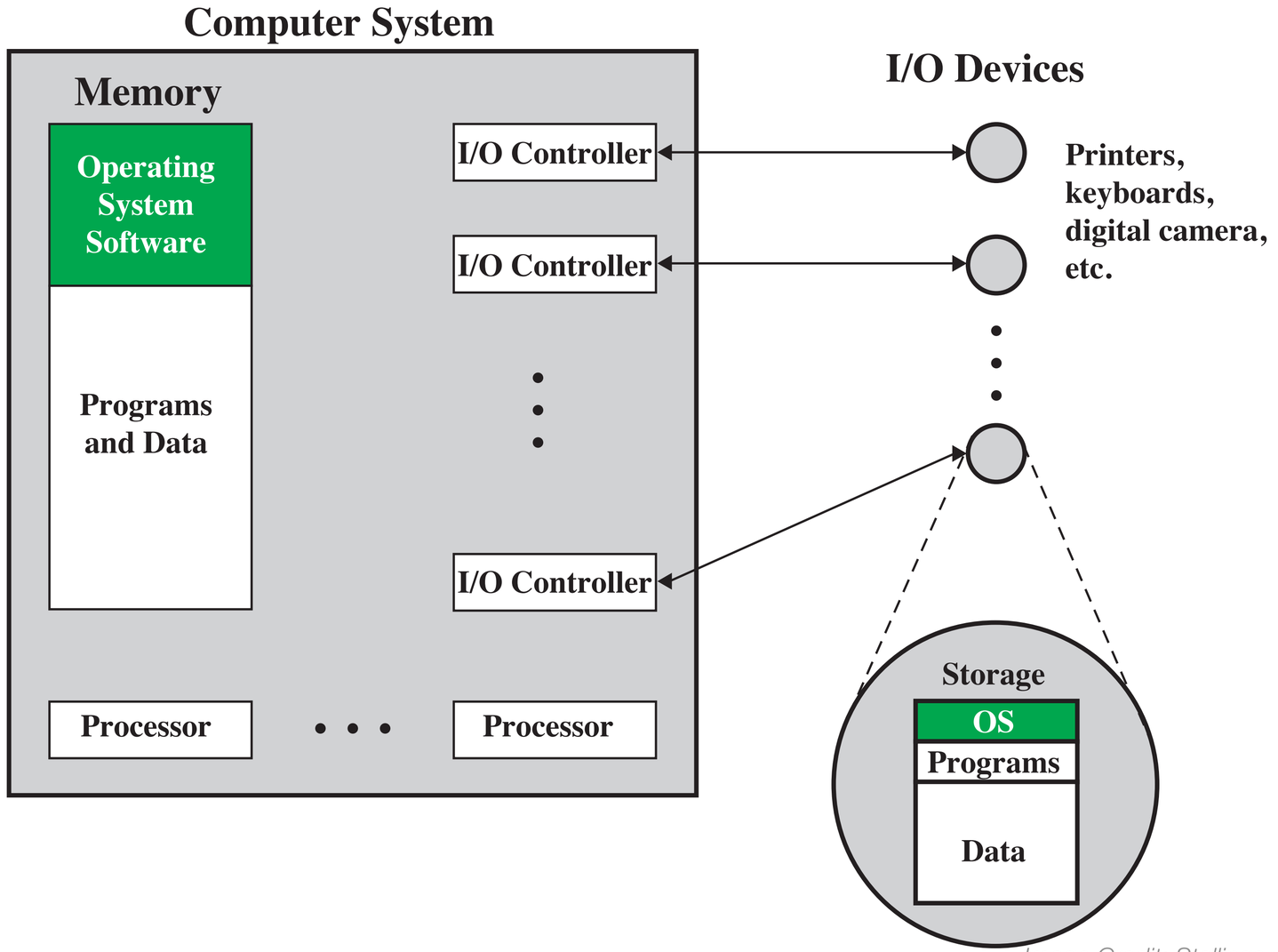
Some Review

Many of the following concepts are specific to the UNIX family (specially Linux), which is most relevant for this course.

A lot of the ideas, however, are universally relevant.

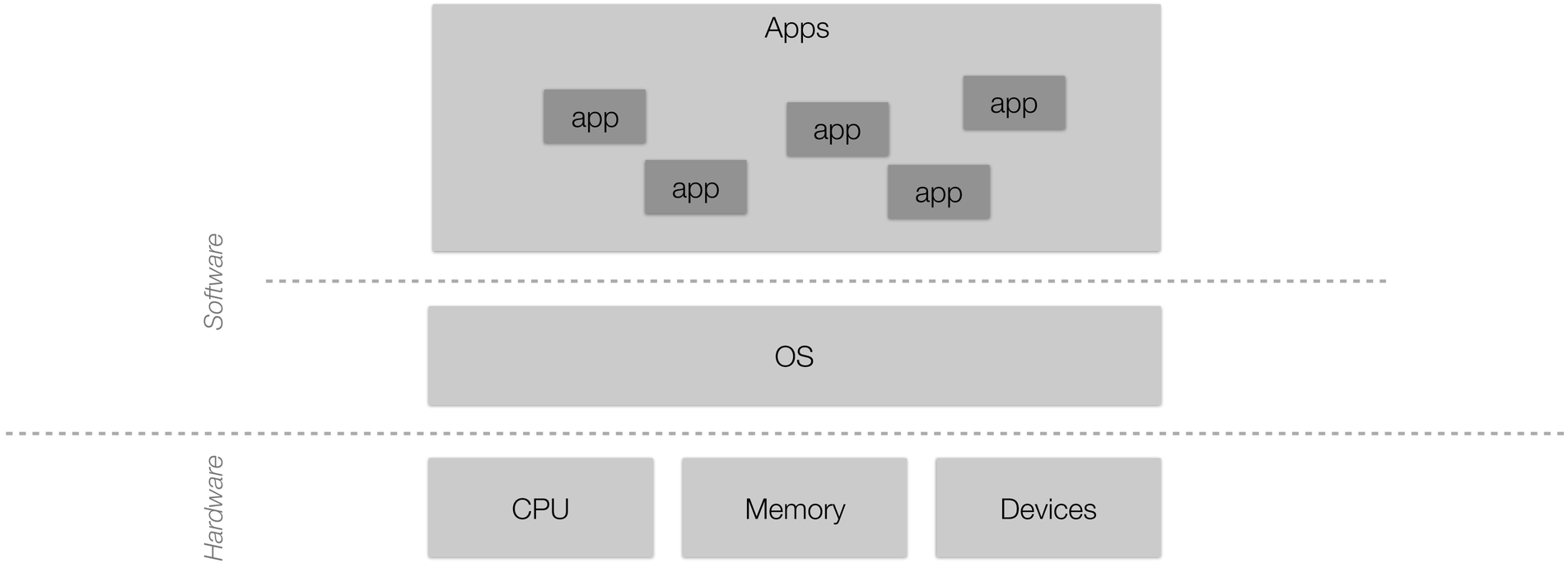
Background: A Computer in a Nutshell

A computer, is a computer, is a computer, …

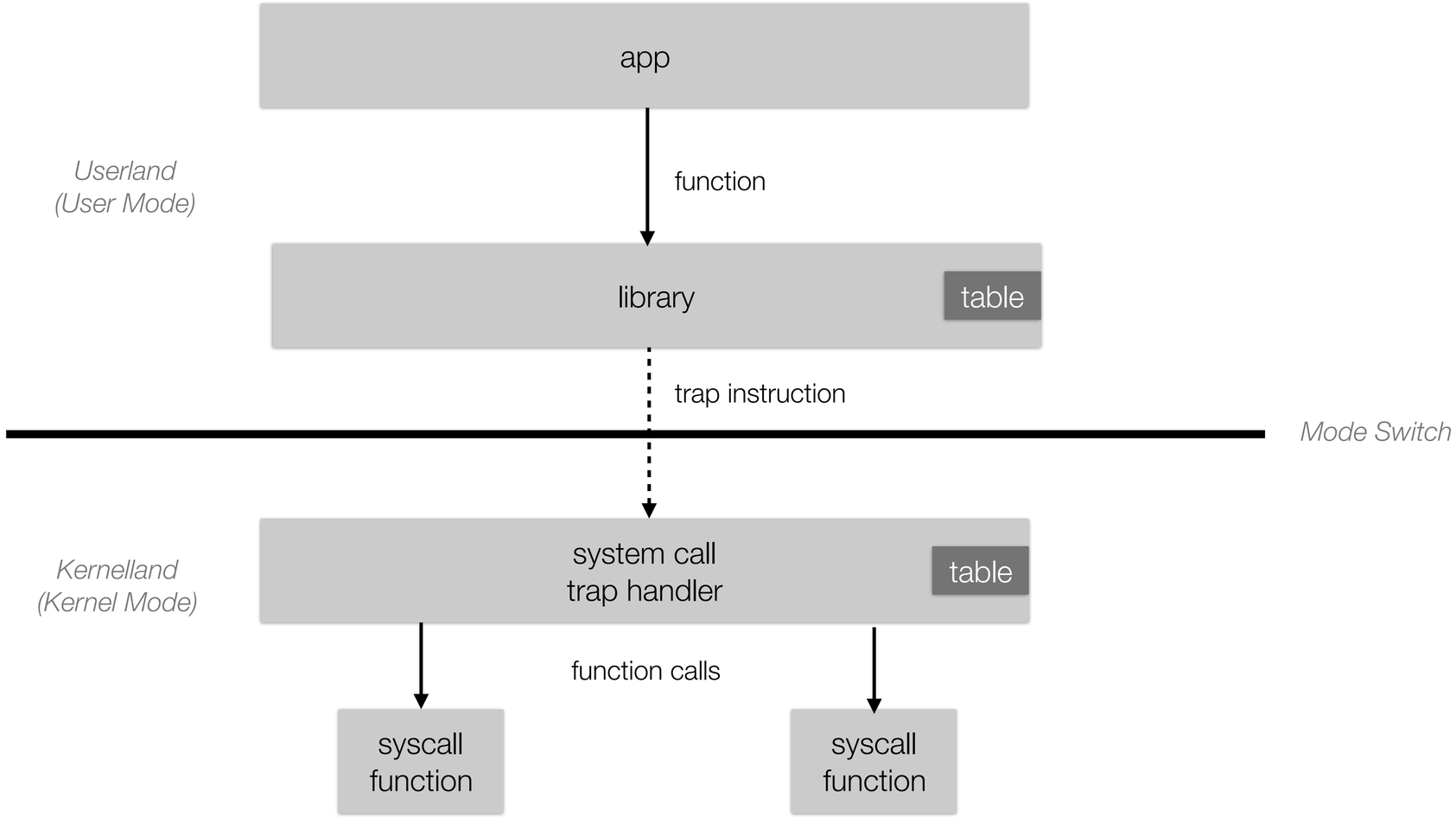


—*Image Credit: Stallings*

Background: Typical Layers of a Computer



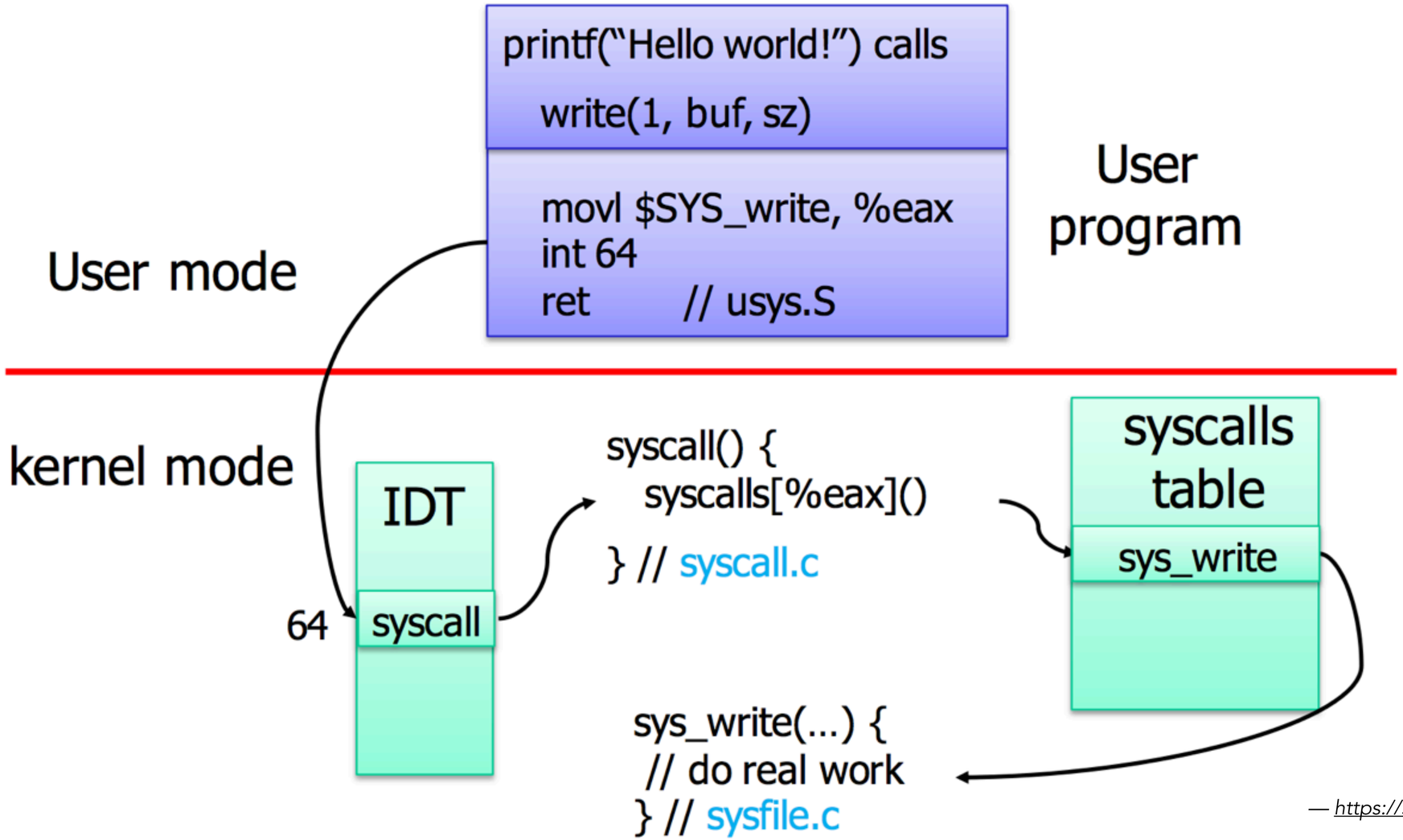
Background: How Apps Use System Resources



Inspired by Figure 4.4 from The Craft of System Security - 1st Edition. Sean Smith (2007).

Background: How Apps Use System Resources

An example



— *https://stackoverflow.com/a/29658740*

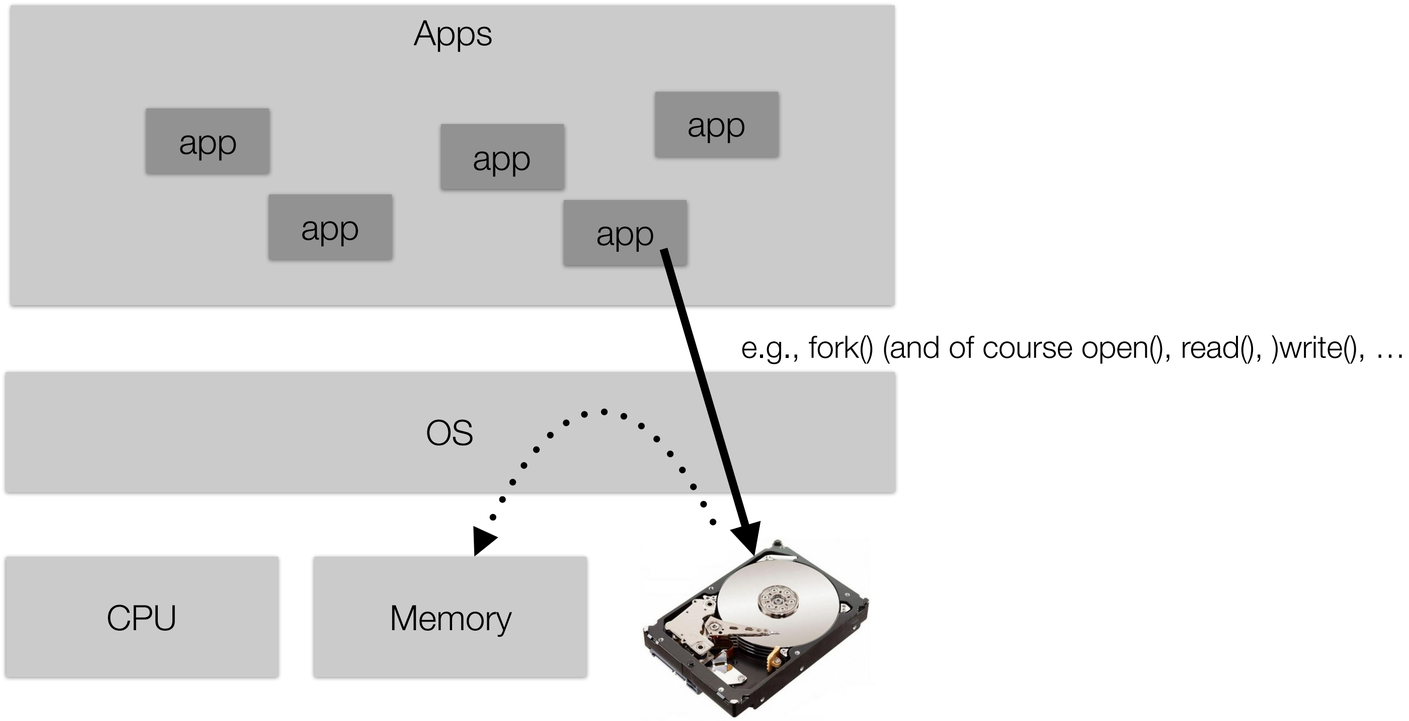
Inspired by Figure 4.4 from The Craft of System Security - 1st Edition. Sean Smith (2007).

Background: An App's Layout in Memory

- How does a program (file) get loaded?

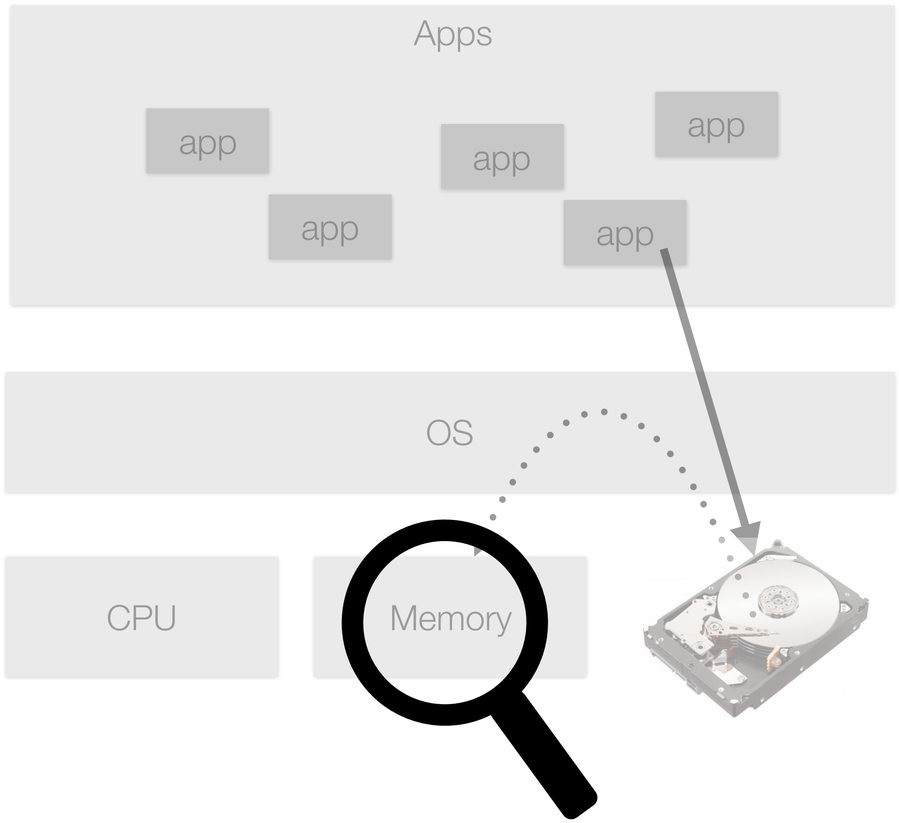
Background: An App's Layout in Memory

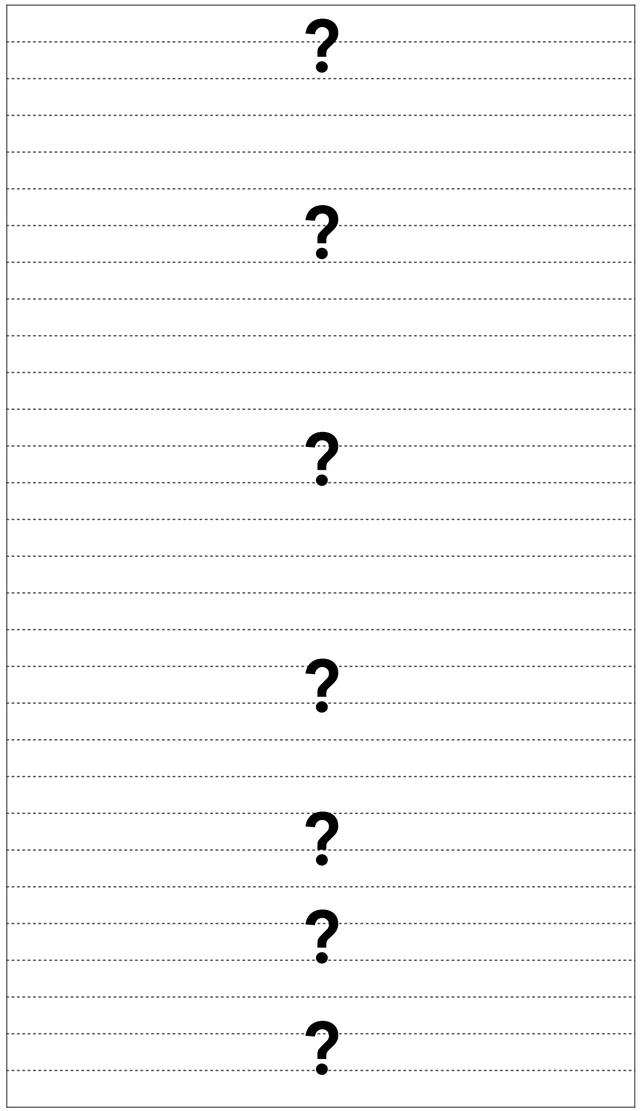
- How does a ***program*** (file) get loaded?



Background: An App's Layout in Memory

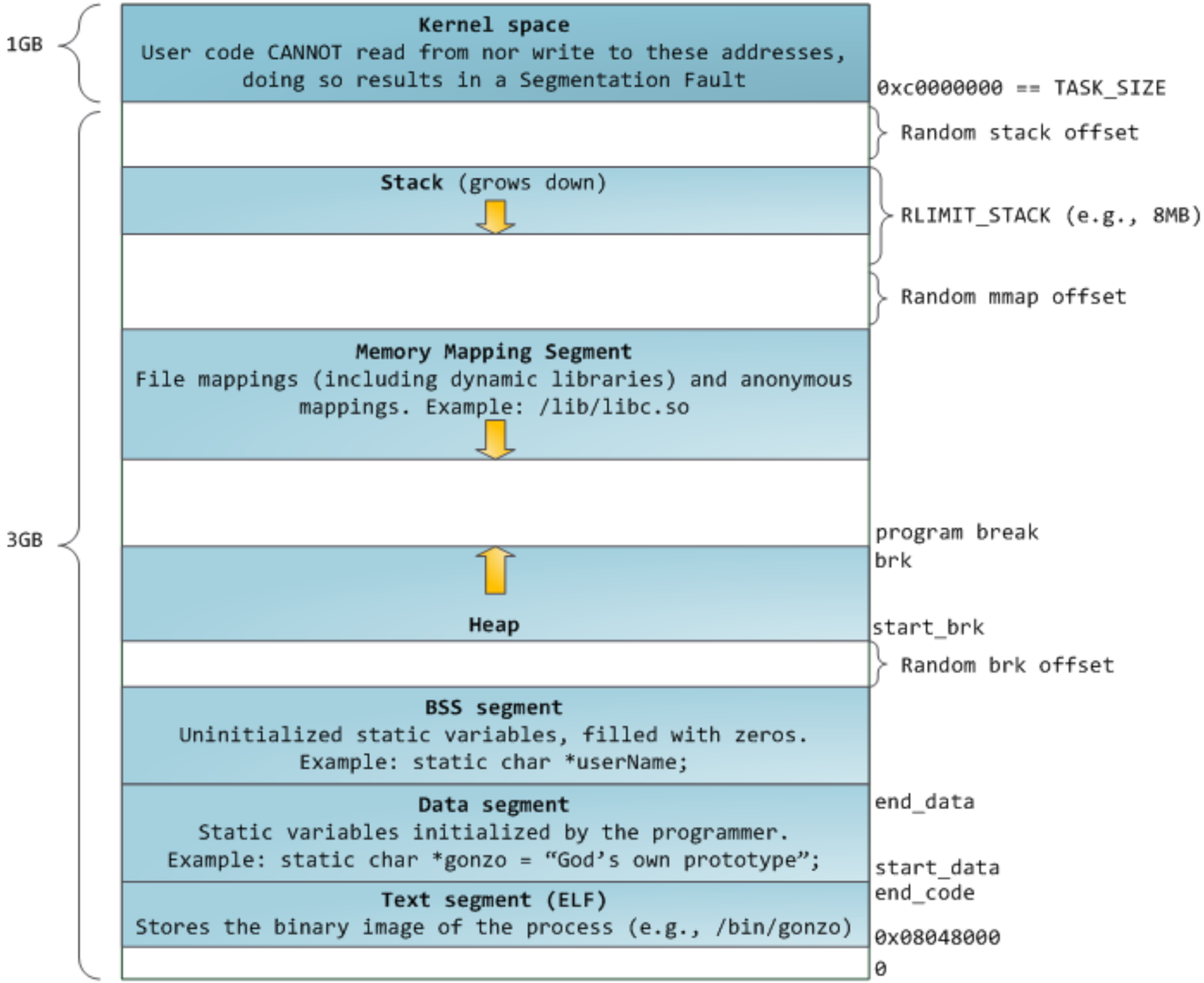
- When a ***program*** is loaded into memory, what does it look like?





Background: An App's Layout in Memory

- When a ***program*** is loaded into memory, what does it look like?



Background: A C Program to Verify Our Thoughts…

Some in class exploration — see ***probe.c***

Some Linux Basics: Users, Groups, Files—*oh my!*

How would you protect your computer & its resources?

How would you protect your computer & its resources?

Ideas?!

How would you protect your computer & its resources?

Modeling and managing system security the UNIX-y way: access control

who can do **what** to **whom**

users/groups

Need notions of "identity"

A human?

Groups of humans?

A service?

An administrator? (e.g., "root")

objects

Usually *things* on a *filesystem*

(e.g., programs, data)

permissions (read/write/execute)

*OK, I know the who/whom—what are **you** permitted to do?*

Read the file?

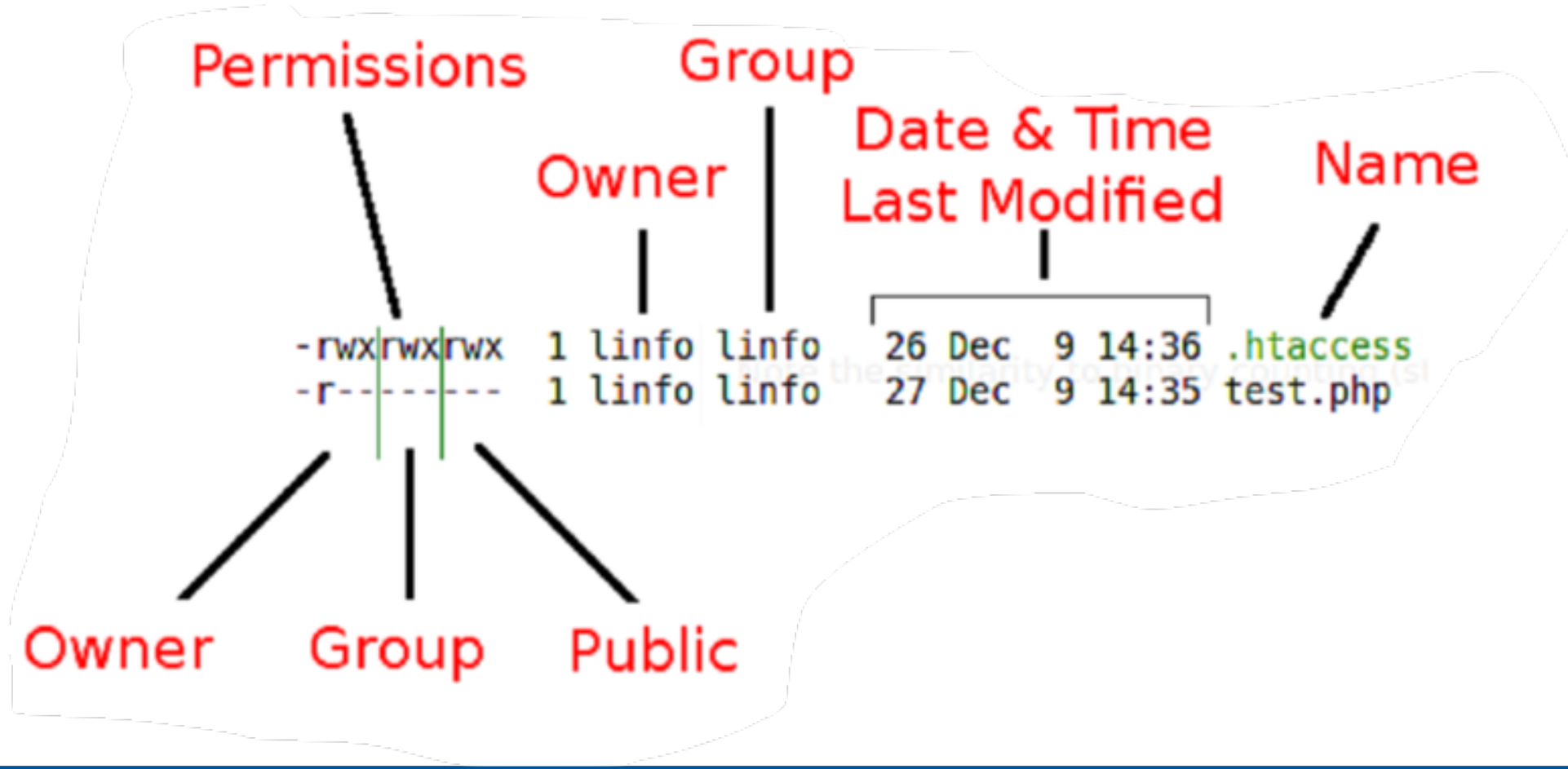
Write to it/modify it?

Run it?

How would you protect your computer & its resources?

Modeling and managing system security the UNIX-y way: access control

Every file has…



A Typical **who** can do **what** to **whom** Flow

If **user A** asks to perform **operation O** on a **file object F**, the OS checks:

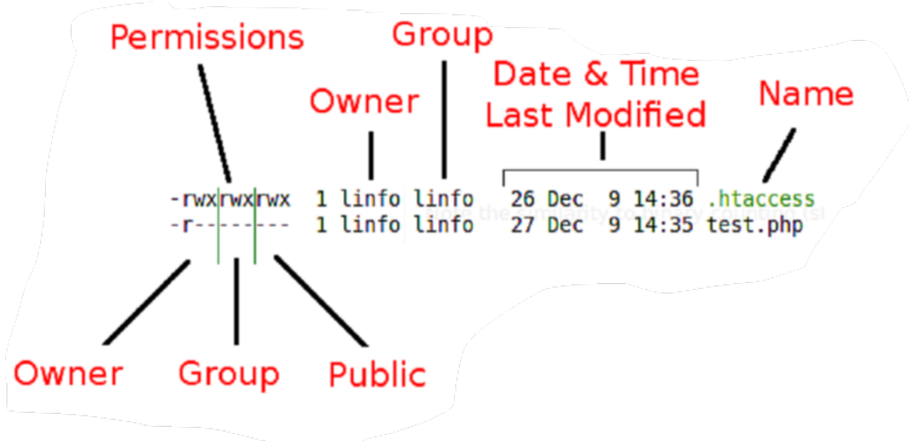
1. Is **A** the owner of **F**? >>> use **owner permissions** to decide whether A can do operation O.

   A is not F's owner

2. Is **A** a member of **F's** group? >>> use **group permissions** to decide…

   A is not F's owner or a member of F's group

3. >>> use the **"everyone else" / "others" permissions** to decide…



First, Some Insights From the Questionnaire!

Some insights into our communication preferences

Some in class exploration — let's take a quick look at these ideas in a VM.

Except….

*…for this interesting thing known as **Set-UID** and **Set-GID***

- UNIX mechanisms for changing user/group identity
  - **setuid** = set user ID
  - **setgid** = set group ID
  - Enables users to run an executable with the permissions of the executable's owner or group, respectively
- Created to deal with inflexibilities of UNIX access control
  - *Why might this be useful?*
- Also the source of endless security problems…
  - *Why might this be a bad idea?*