Introduction'); DROP TABLE Syllabus; --

Secure Systems Engineering Spring 2024

🛡️ EE G7701

January 30, 2024

Tushar Jois

$ whoami

Tushar Jois (he/him)

Assistant professor

Electrical engineering

Computer security & privacy

Likes: computers, road trips, board games

Dislikes: mass surveillance, beets, computers

```
$ whoami
tushar

$ who
```

Survey time!

By show of hands, how many of you...

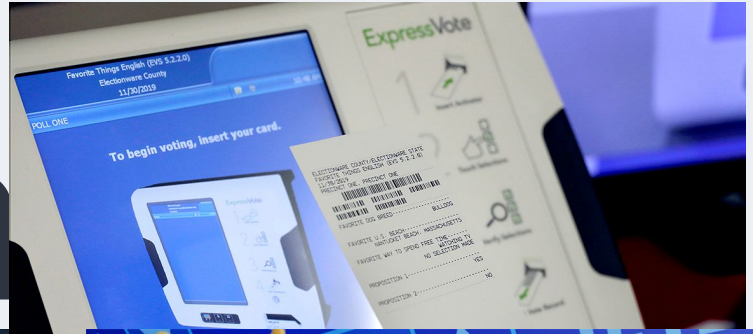
- Have configured a personal firewall
- Have used a virtual machine
- Have used Wireshark
- Know how to read `tcpdump` output manually
- Understand how a buffer overflow works
- Have written shellcode for a buffer overflow
- Have written Rust code
- Know what IKE stands for
- Understand how certificate chains work
- Have browsed the Internet using Tor
- Have written a virus or worm
- Have hacked into someone else's system

```
$ whoami
tushar

$ who
successful survey

$ why
```

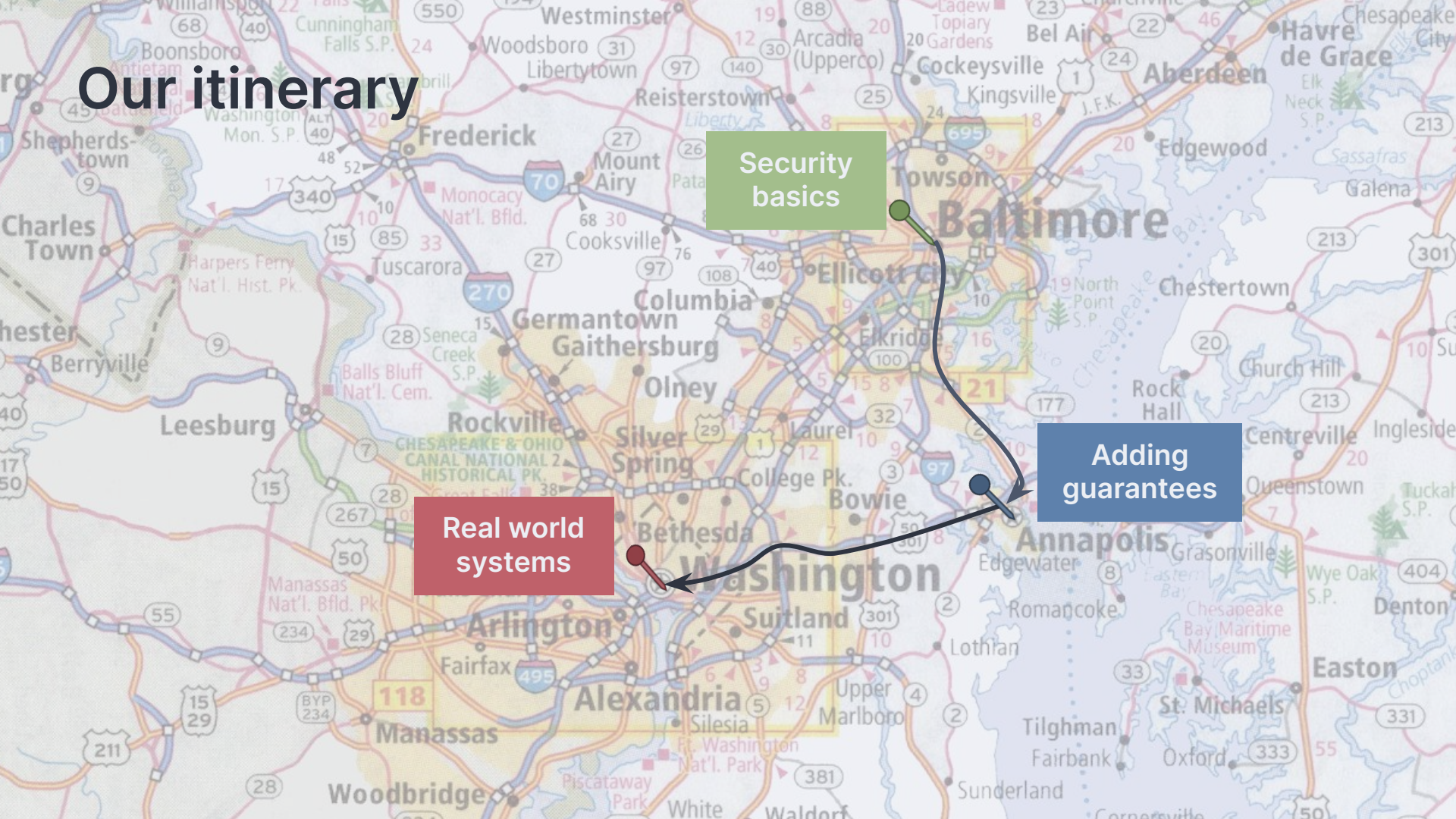

pjm


ExpressVote
To begin voting, insert your card.


stonks
made with dogetizer

wat do

Our itinerary



Course goals

- Know core security concepts, both in theory and practice
- Apply the proper defenses to common attacks on systems
- Understand the societal, cultural, and political implications of the field
- Be prepared for research, if you so choose

Course expectations

- Come to class on-time and ready to contribute
- Be prepared to collaborate with your peers on labs and projects
- Complete coursework honestly and with effort
- Respect your classmates, as well as the course staff

Course information

- Required text: None!
  - But, there will be posted readings
- Please do the readings
  - They're helpful especially for the in-class activities
- Course page: `https://tjo.is/teaching/sse-sp24/`
  - Has the course schedule, which has due dates and links to materials
  - Familiarize yourself with the content of the syllabus (below the schedule)
- Content submission: Blackboard
- Discussion board for assignment questions: Blackboard
- Late work not permitted without an excuse
  - If you have an excuse, please inform the staff in advance for consideration

In-class activity

- Second half of class each week
  - After lecture and a short break
  - Come prepared to contribute to discussion topics and work through hands-on lab problems
- Please bring your laptop to follow along
  - We have a course virtual machine (see course page for link)
  - Let the course staff know ASAP if this is not possible for you
- Submit lab deliverables on time to receive full credit for attendance
- Topics covered will be on the exam
  - Lectures are not the only source of content!

Course project: capture-the-flag

- Your team will develop a voting machine that is intentionally vulnerable to attack
- You'll use the vulnerabilities that you learn from the labs and hide it into the voting machine

The case study:

An electronic voting machine

- Another group takes your code and attempts to figure out what the vulnerabilities are
- Then, you'll try to exploit them!
- More details to come

Course schedule

Date	Lecture topic	In-class activity	Reading	Deliverables
Jan 30, 2024	Course intro & Unix security basics	Course virtual machine setup	Security Engineering book chapter	Assignment 1 out, due by **10p Feb 12**
Feb 6, 2024	Buffer overflows	Intro to GDB & Assignment 1 in-class work	Book chapter (see Blackboard)	
Feb 13, 2024	Rust programming	Lab 1: Hands-on with Rust	Rust Book, chapters 1, 3-6	Assignment 2 out, due by **10p Mar 4**
Feb 20, 2024	Practical cryptography	Lab 2: More fun with Rust	Rust Book, chapters 7-11	
Feb 27, 2024	Case study: Transport Layer Security (TLS)	Lab 3: Wireshark & TLS	The Illustrated TLS 1.2 Connection	
Mar 5, 2024	**Exam 1**	Project introduction & group assignment		Project description out (note due dates)

(as of 2024-01-26; subject to change; see latest version here)

Course schedule

Date	Lecture topic	In-class activity	Reading	Deliverables
Mar 12, 2024	Case study: electronic voting	Project check-in 1 & in-class work	Blaze law review paper	
Mar 19, 2024	Backdoors in secure systems	Lab 4: Build-a-backdoor	TBA	Assignment 3 out, due by **10p Apr 8**
Mar 26, 2024	Side channels (**online lecture**)	Project check-in 2 & in-class work	TBA	
Apr 2, 2024	Privacy & anonymity	Lab 5: Signal & Tor	Double Ratchet specification, sections 1, 2; optional: Tor paper	
Apr 9, 2024	Advanced topics	Lab 6: Trusted hardware	DOVE research paper	Submit Project code by **10p Apr 15**
Apr 16, 2024	**Exam 2**	Project check-in 3 & in-class work		

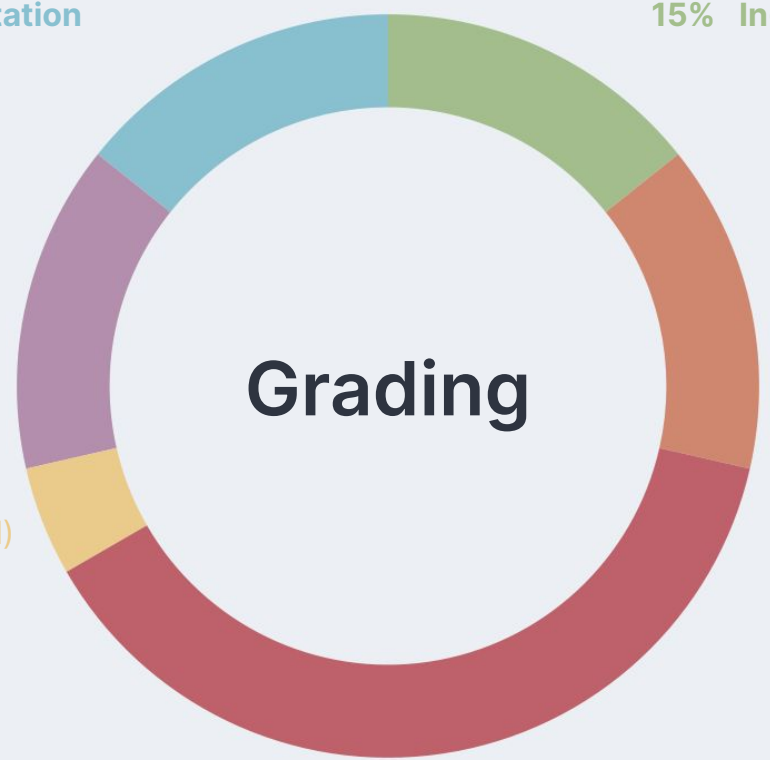
(as of 2024-01-26; subject to change; see latest version here)

Course schedule

Date	Lecture topic	In-class activity	Reading	Deliverables
Apr 23, 2024	*Spring recess (no class)*			
Apr 30, 2024	*Spring recess (no class)*			
May 7, 2024	**Project code demos**	Project check-in 4 & in-class work		Submit Project presentation slides by **10p May 13**
May 14, 2024	**Project presentations**			

(as of 2024-01-26; subject to change; see latest version here)

Grading



15% **Project presentation**

15% **In-class labs** (6 total)

15% **Project code & demo**

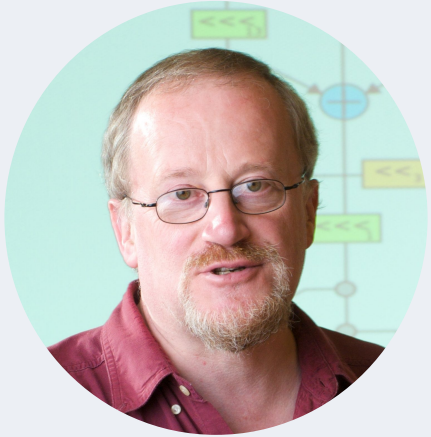
15% **Assignments** (3 total)

5% **Project check-ins** (4 total)

40% **Midterm exams** (2 total)


Let’s
jump
in!

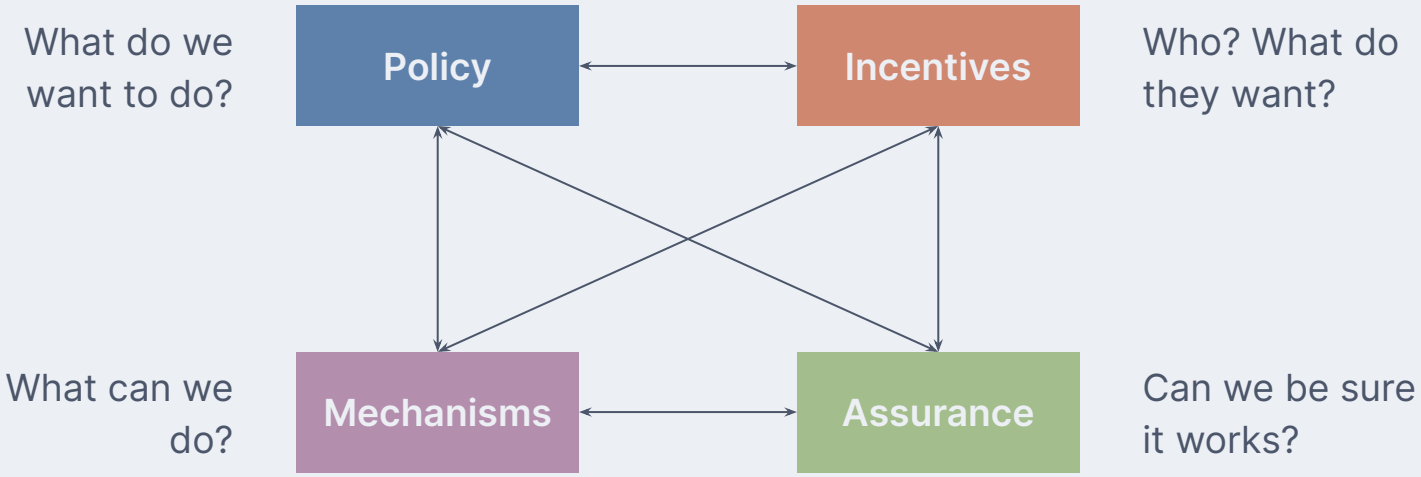
Security engineering



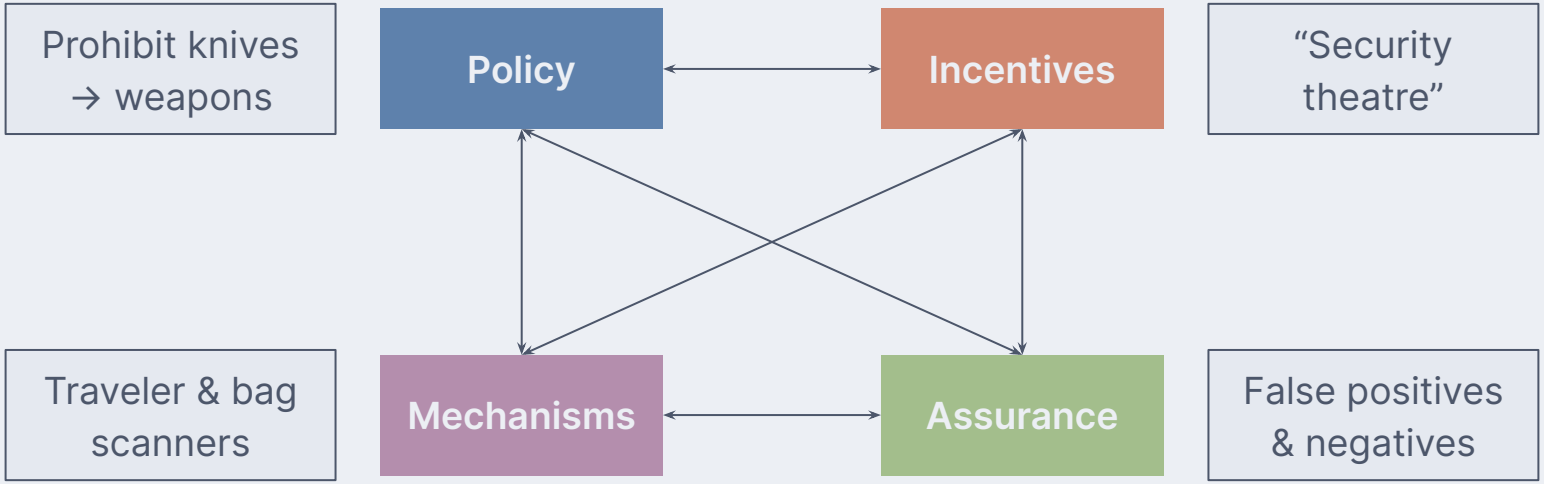
Ross Anderson

Professor, University of Cambridge

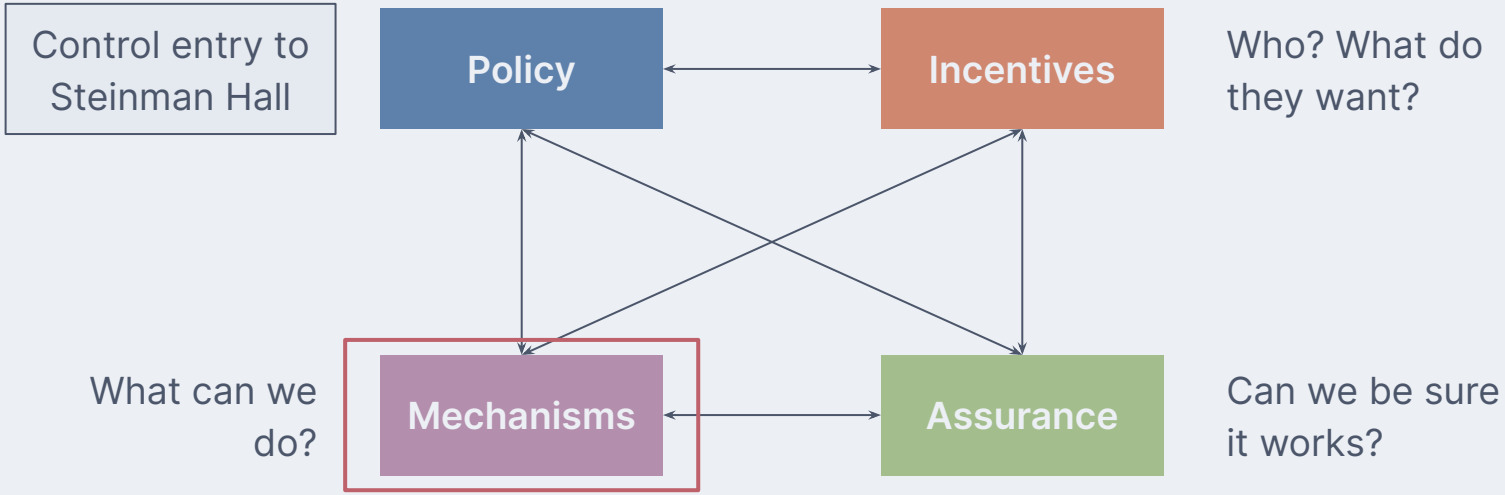
Security engineering



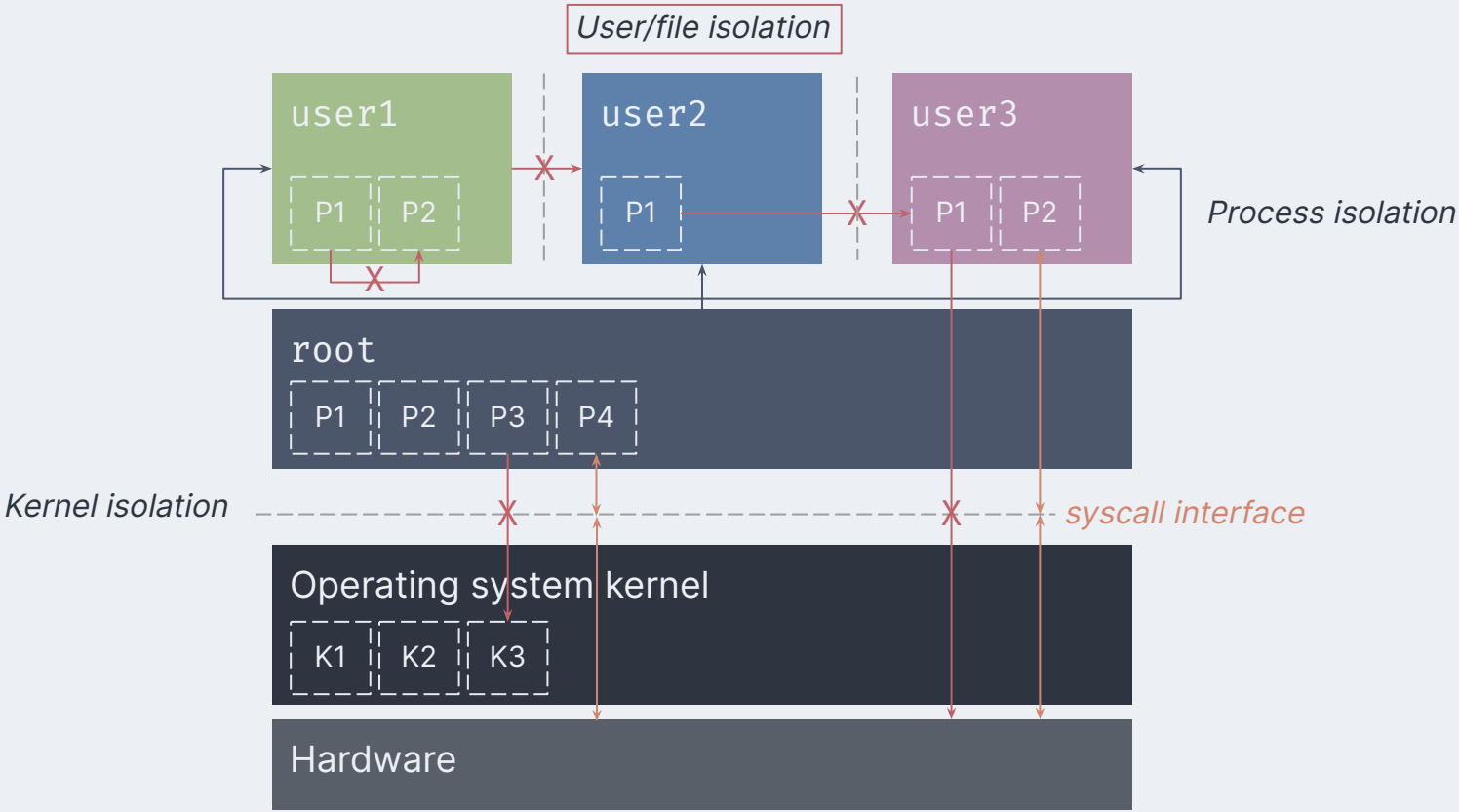
Airport security



Activity


Control entry to Steinman Hall
Policy
Incentives
Who? What do they want?
What can we do?
Mechanisms
Assurance
Can we be sure it works?

Unix isolation



Users

```
seed@VM:~$ cat /etc/passwd | grep seed
seed:x:1000:1000:seed,,,:/home/seed:/bin/bash

seed@VM:~$ id
uid=1000(seed) gid=1000(seed) groups=1000(seed)

seed@VM:~$ cat /etc/passwd | grep root
root:x:0:0:root:/root:/bin/bash

root@VM:~# id
uid=0(root) gid=0(root) groups=0(root)
```

Users and groups

- Groups represent a group of users
  - Assigning permissions based on group
  - A user can belong to multiple groups
  - A user's primary group is in `/etc/passwd`
- Commands for managing users and groups
  - Use `groups` or `id` to list your user's groups
  - Use `adduser` to add a user
  - Use `groupadd` to add a group
  - Use `usermod` to add a user to a group
  - Use `su` to switch to another user

```
seed@VM:~$ groups
seed adm cdrom sudo dip plugdev
lpadmin sambashare

seed@VM:~$ id
uid=1000(seed) gid=1000(seed)
groups=1000(seed),4(adm),24(cdrom)
,27(sudo),30(dip),46(plugdev),113(
lpadmin),128(sambashare)
```

File permissions

- Types of access on files
  - read (`r`): user can view the contents of the file
  - write (`w`): user can change the contents of the file
  - execute (`x`): user can execute or run the file if it is a program or script
- Types of access on directories
  - read (`r`): user can list the contents of the directory (*e.g.*, using `ls`)
  - write (`w`): user can create files and sub-directories inside the directory
  - execute (`x`): user can enter that directory (*e.g.*, using `cd`)
- More fine-grained access control with `getfacl/setfacl`

```
seed@VM:~$ ls -l xyz
-rw-rw-r-- 1 seed seed 0 Aug 26 15:32 xyz
```

owner
group
world
user name
group name
file information

Running commands as `root`

- Run commands as `root` with `sudo`: **s**uper**u**ser **do**
  - Just add `sudo` to the front of a command that requires privilege
  - By default runs commands as `root`, but can select the user with `-u`
  - User needs authorization to use `sudo`
- Get a full shell as `root` with `sudo -s`
  - Not recommended in general

```
seed@VM:~$ cat /etc/sudoers
cat: /etc/sudoers: Permission denied

seed@VM:~$ sudo cat /etc/sudoers
# (snip)
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) NOPASSWD:ALL
```

User authentication

- Authentication verifies a user identity, based on something...
  - A user knows (a password)
  - A user has (ID card, smartphone)
  - A user is (fingerprint)
- Multi-factor authentication combines these together
- In Unix, authentication is primarily done through a password
  - User metadata stored in `/etc/passwd`
  - The password itself is stored (hashed) in `/etc/shadow`

Why?

Purpose?

Looking ahead

- Review the course page for the class
  - QR code, on Blackboard, and at `https://tjo.is`
- Assignment 1 is out
  - We will go over the concepts required next class, but take a look anyway
- Do the reading for next time
  - Chapter is on Blackboard
  - Incredibly helpful for working on Assignment 1!
- Bring your laptop to work on the in-class activity
- Read stuff! Hacker News, Lobste.rs, Ars Technica
- **Today's activity**: setup the course virtual machine