Introduction'); DROP TABLE Syllabus; --

Secure Systems Engineering Fall 2024

🛡️ EE G7701

August 28, 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...

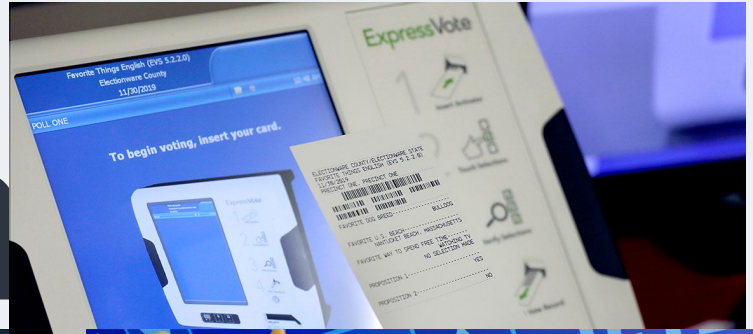
- Have configured a personal firewall
- Have used a virtual machine
- Have used Wireshark
- Know how to read `tcpdump` output manually
- Understand how a buffer overflow works
- Have written shellcode for a buffer overflow
- Have written Rust code
- Know what IKE stands for
- Understand how certificate 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
```

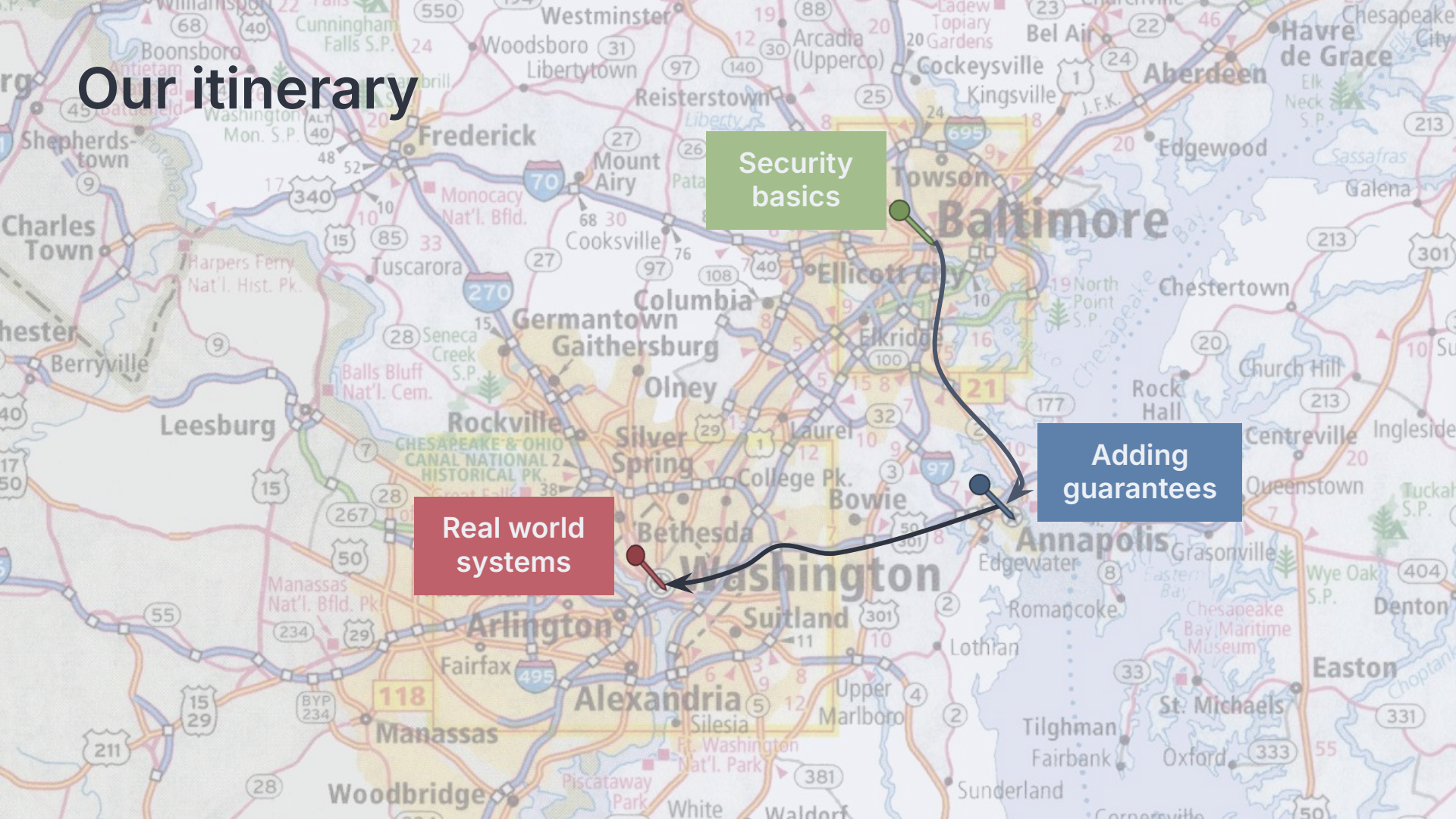

pjm


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
  - To make sure you do them, there will be reading quizzes!
- Course page: `https://tjo.is/teaching/sse-fa24/`
  - 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!
  - 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
- Bring your laptop to follow along, or you can use the lab's (Linux) PCs
  - We have a course virtual machine for some labs (see course page for link)
  - Let the course staff know ASAP if this is not possible for you
- Some assignments can be completed in-class, others will require take-home effort
- Topics covered will be on the exam
  - Lectures are not the only source of content!
- Generative AI use is not allowed for this class

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

(as of 2024-08-28; subject to change; see latest version here)

Date	Lecture topic	In-class activity	Reading	Deliverables
Aug 28	Course intro & Unix security basics	Lab 1: Introduction	Security Engineering book chapter	Labs are due **10p Tue** after they are out
Sep 4	Rust programming (**guest lecture**)	Lab 2: Hands-on with Rust	Rust Book, chapters 1, 3-6	
Sep 11	Buffer overflows	Lab 3: Buffer overflows	Book chapter (see Blackboard)	
Sep 18	Practical cryptography	Lab 4: Cryptography in Rust	Rust Book, chapters 7-11	
Sep 25	Transport Layer Security (TLS)	Lab 5: Wireshark & TLS	The Illustrated TLS 1.2 Connection	
Oct 2	*Fall break (no class)*			
Oct 9	**Exam 1**	Project introduction & group assignment		Project description out (note due dates

Course schedule

(as of 2024-08-28; subject to change; see latest version here)

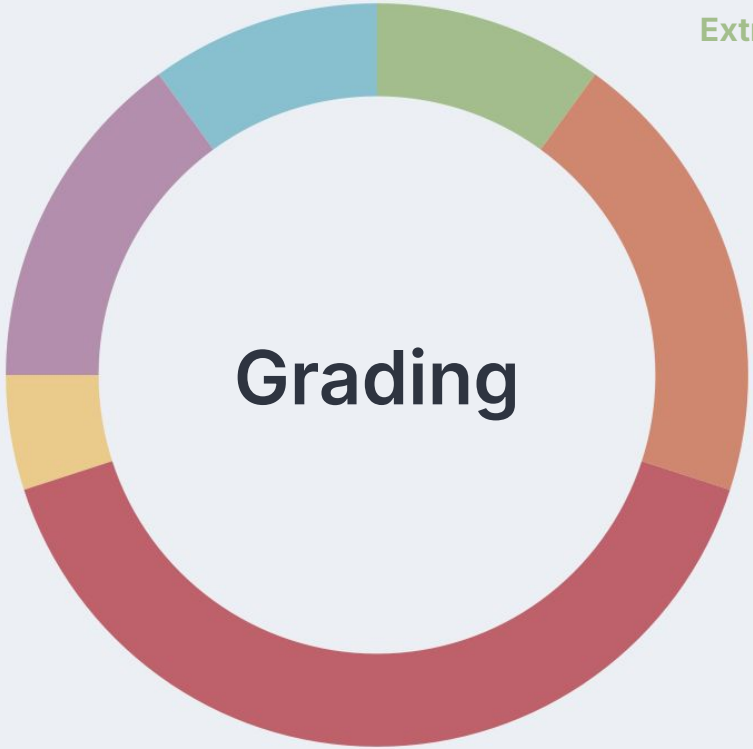
Date	Lecture topic	In-class activity	Reading	Deliverables
Oct 16	Backdoors in secure systems (**online lecture**)	Lab 6: Trusting Trust	Reflections on Trusting Trust	
Oct 23	Case study: electronic voting	Project check-in 1 & in-class work	Blaze law review paper	Project check-ins are due **10p the same day** they are out
Oct 30	Privacy & anonymity	Lab 7: Privacy	Double Ratchet specification, sections 1, 2; optional: Tor paper	
Nov 6	Advanced topics	Project check-in 2 & in-class work	DOVE research paper	
Nov 13	**Exam 2**	Project check-in 3 & in-class work		Submit Project code by **10p Nov 19**

Course schedule

(as of 2024-08-28; subject to change; see latest version here)

Date	Lecture topic	In-class activity	Reading	Deliverables
Nov 20	Demo practice & red team analysis (**self-guided**)	Project check-in 4 & in-class work		
Nov 27	*Thanksgiving (no class)*			
Dec 4	**Project code demos**			Submit Project presentation slides by **10p Dec 10**
Dec 11	**Project presentations**			

Grading



10% **Project presentation**

10% **Reading quizzes** (8 total)

Extra credit seminars

15% **Project code & demo**

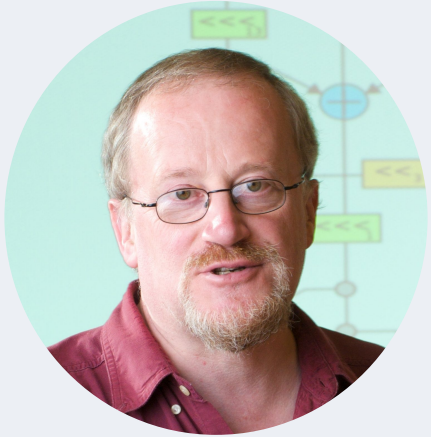
20% **Assignments** (7 total)

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

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


Let’s
jump
in!

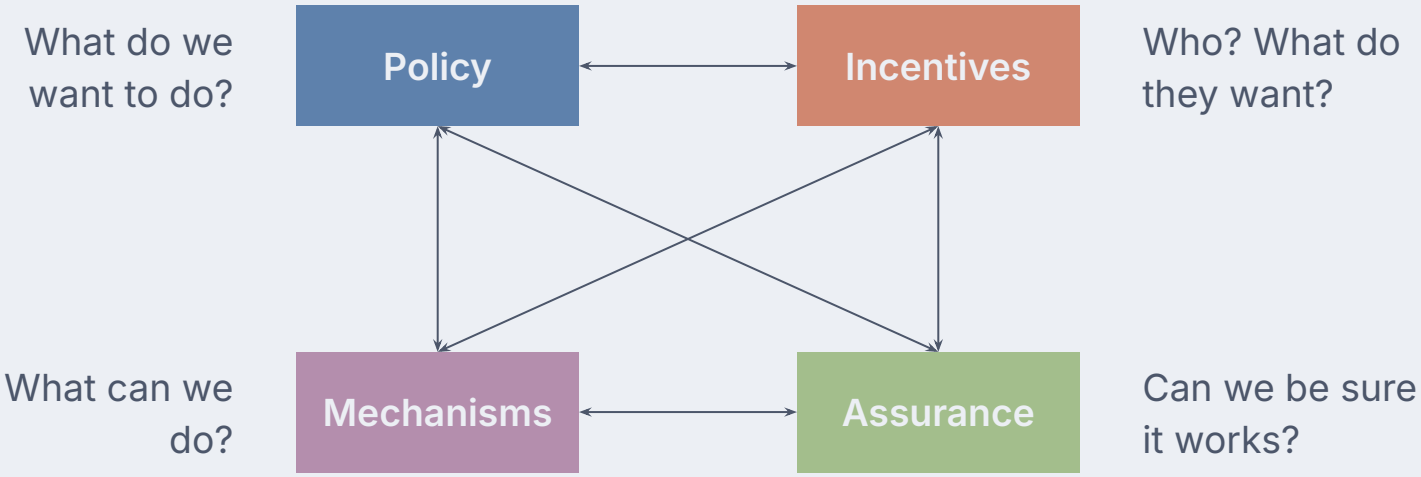
Security engineering



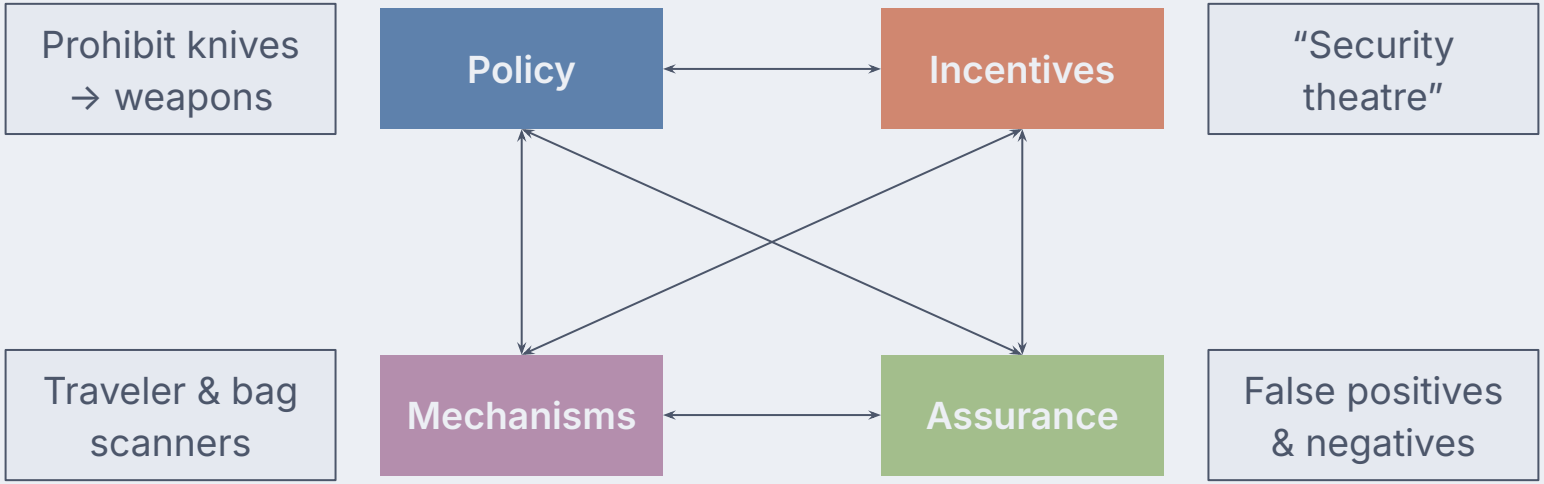
Ross Anderson

Professor, University of Cambridge

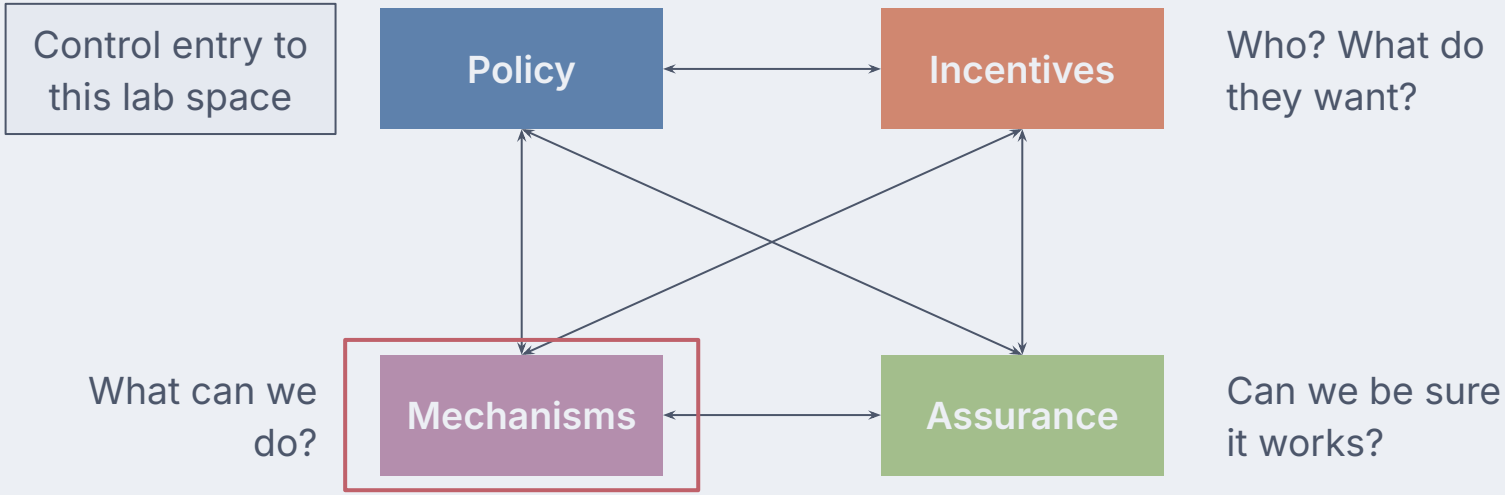
Threat modeling



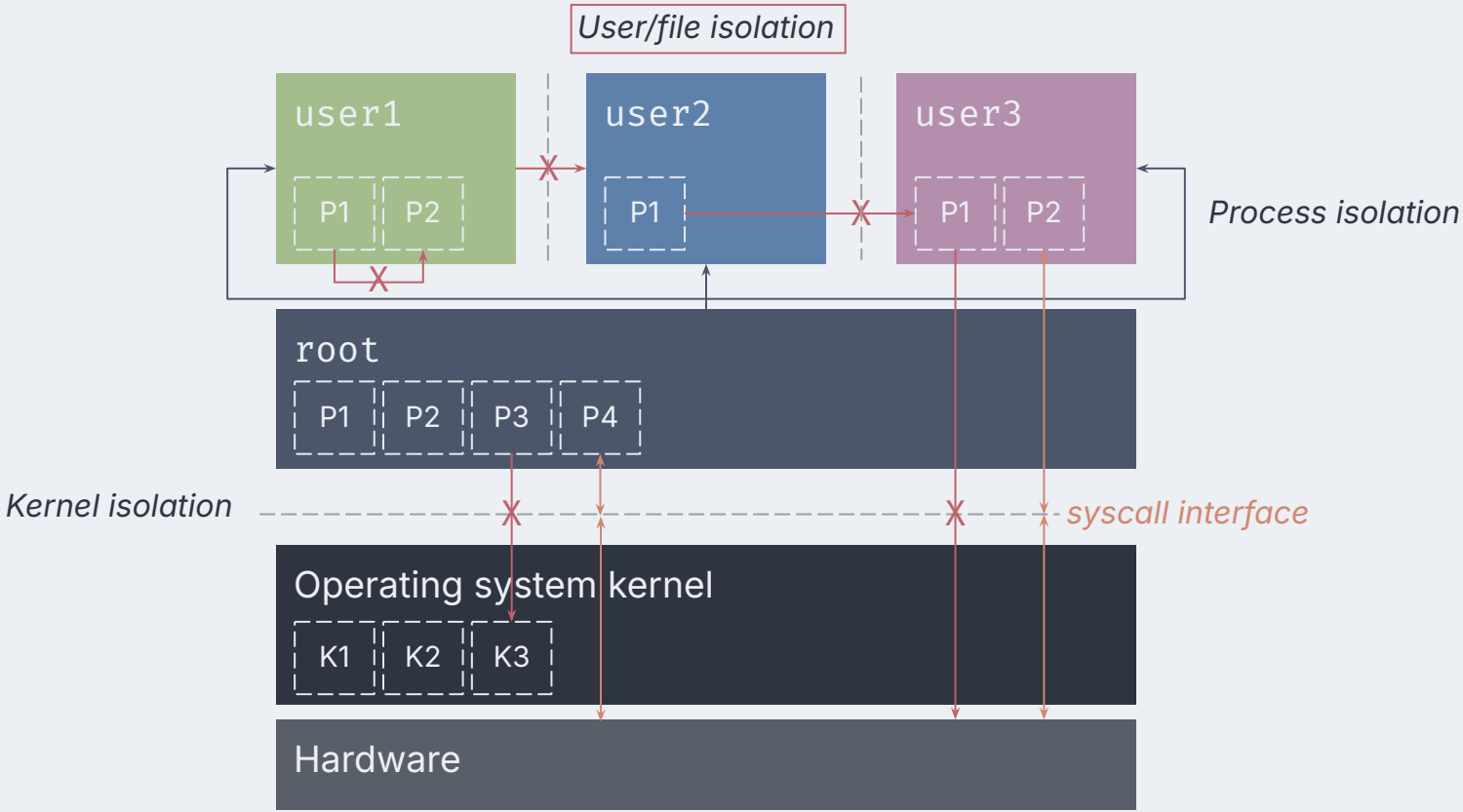
Airport security



Activity


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

Unix isolation



Looking ahead

- Review the course page for the class
  - QR code, on Blackboard, and at `https://tjo.is`
  - Read through the whole syllabus!
- Next class will be an **online guest lecture** by David Inyangson
  - Being on camera will be required
  - Details will be available on Blackboard, so keep an eye out
- Do the reading for next time
  - There will be a reading quiz!
- If you can, bring your laptop to work on the in-class activity
- Read stuff! Hacker News, Lobste.rs, Ars Technica
- **Today's assignment:** fun with GDB!