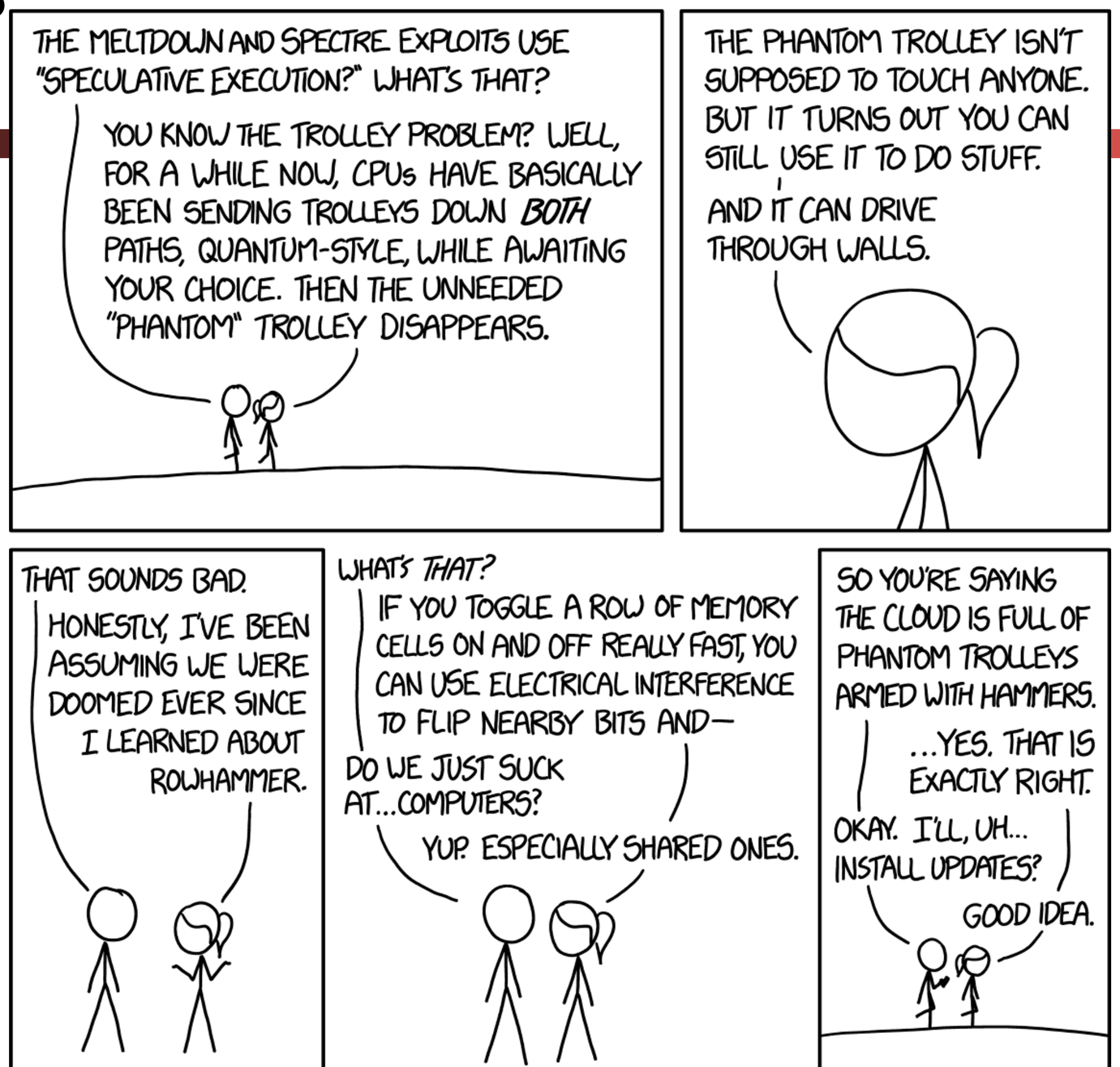
Hardware Attacks
+
Rafael's Personal Self-Defense Decisions...

Hardware Attacks

- Rowhammer
- Meltdown
- Spectre



Physical Security

- Hardware Keyloggers
- RFID Card Cloning
- Proximity attacks (Wi-Fi, Bluetooth, 4G, etc.)

Break
Random fact about... David Patterson

- Has taught various computer architecture classes
- Patterson & Henessy: classical computer architecture textbook
- Won the Turing Award in 2017 (RAID, RISC-V)
- UC Berkeley has the highest number of Turing Award winners if you count by where they did their Turing Award work
- In his Turing lecture, Dave tried to distinguish himself from other Turing award winners

Dave is the strongest of them (literally).

Won California powerlifting championship in 2013 for his age range.

Putting CS161 in Context: Rafael's Self Defense Strategies...

- ***How*** and ***why*** do I protect myself online and in person...

Threat Model

- *Your* threat model is not *my* threat model, but *your* threat model *is okay*
- We probably don’t even know who our real attackers are

My Personal Threats:

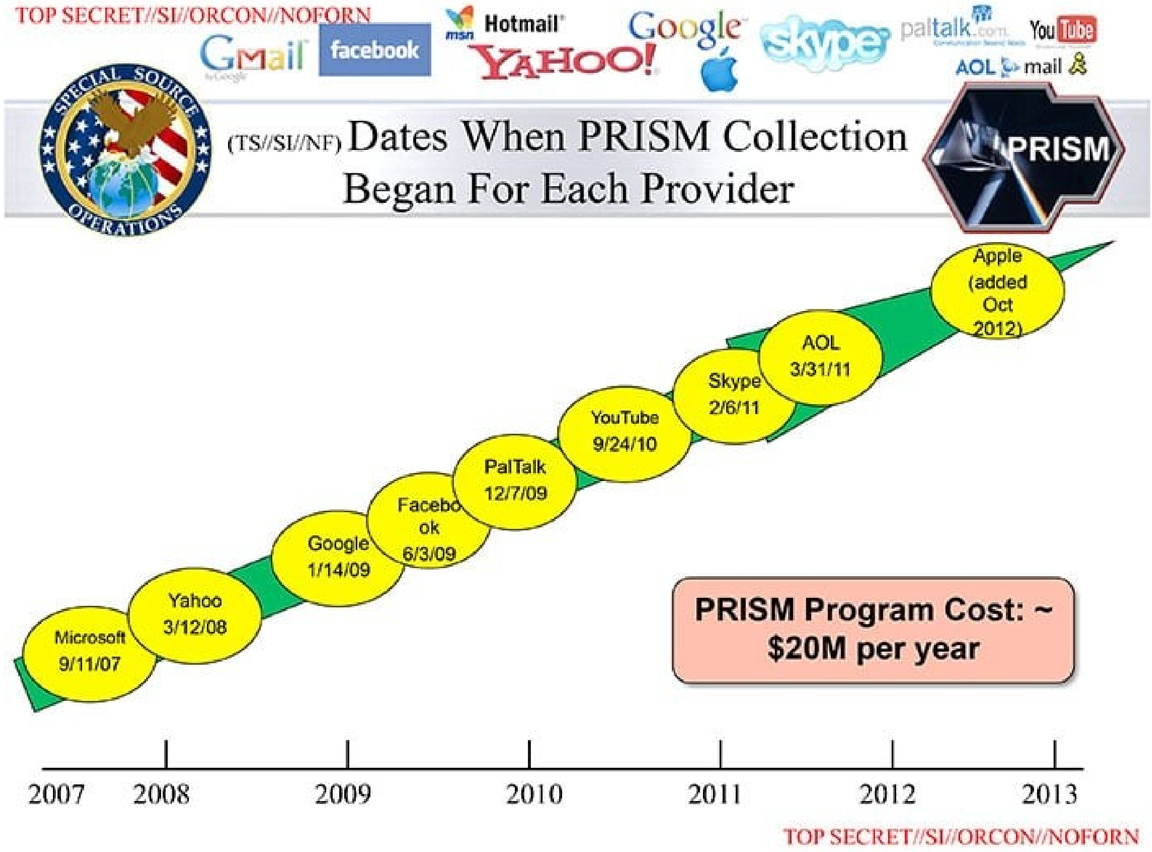
- The generic opportunist
- Intimate Partner Threats
- Corporations
- Nation States

My Personal Threats:
The generic opportunist

- No password reuse (use a password manager instead)
- Full disk encryption & strong passwords on devices:
  - LUKS for GNU/Linux computers
  - LUKS for encrypted USB drives too!
  - Enable device encryption in Android/LineageOS
- Mitigates the damage from theft

My Personal Threats: Corporations

- I only trust **Free and Open Source Software** (FOSS)
- Because really who can trust them to have your best interest in mind?



My Personal Threats: The Nation State

- The network is always assumed to be hostile
- Use Tor for everything
  - Also gives strong protection from corporation tracking
- Crossing borders
  - Every nation maintains the right to conduct searches of all electronic contents at a border checkpoint

My Border Crossing Policy

- I use full disk encryption with strong passwords on all devices
  - Primary use is to prevent theft from also losing data
- I have a backup strategy
  - Encrypted archived backups
- So, as the plane lands:
  - Power off my devices
    - Device encryption is only ***robust*** when you aren't logged in
    - Prevents Cold Boot attack
  - Go through the border
- If my devices get siezed...
  - Burn it with fire!
  - It can no longer be trusted

Passwords and 2-factor...

- 2-factor can really boost security
  - Instead of me having to interrogate the site to determine phishing...
  - The site has to prove to the key it is legitimate!
- For passwords I always use a password manager
  - Yes, if an attacker compromises my computer, they can steal all my passwords...
  - But the same attacker can get all the passwords I actually use when I type them in (a 'keylogger').
  - KeePassX

Credit Cards are Awful

- The mag stripe is all that is needed to duplicate a swipe-card
  - And you can still use swipe-only at gas pumps and other such locations
- The numbers front and back is all that is needed for card-not-present fraud
- No privacy
- I use cash as much as I can
  - Is still not anonymous – serial numbers
- Cryptocurrencies might be an option (Zcash?)

Signal
End-to-end Encrypted Communications

- End-to-end encryption for:
  - Chats
  - Group chats
  - Audio calls
  - Video calls

- Signal is open-source (including server code)
- Allows verification of public-key fingerprint
- Has forward secrecy + deniability

My Current Smartphone

- Pixel device with Open Source Android (LineageOS)
  - Updated every week
- microG: replacement for Google Play Services
  - Don’t reveal your Geolocation to Google
  - Still, carrier (T-Mobile) knows course location
- I don’t use fingerprint reader to unlock the phone
  - Governments already have your fingerprint
  - Even if they hadn’t, they can legally demand it (unlike passphrase)
- Network traffic for apps routed through Tor (Orbot)

Future: Purism Librem 5 Smartphone

- Might become the first truly free and open source smartphone
- Operating system is basically a desktop GNU/Linux
- Baseband modem sandboxed
  - Because it’s untrusted
- Hardware kill switches

Purism Librem Computers

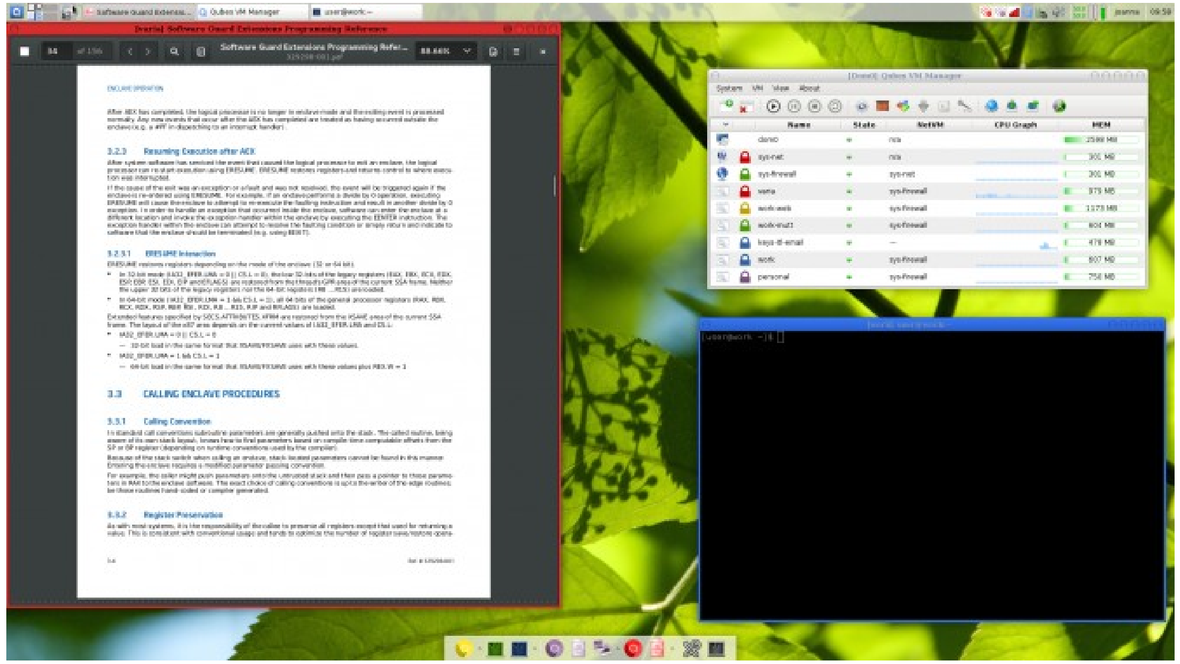
- The ***Trusted Platform Module (TPM)*** can be used for verified boot
  - With Heads firmware
  - Detects “Evil Maid” Attack
- Intel Management Engine disabled
- Full disk encryption enabled by default
- Hardware kill switches

Secure Operating Systems
Tails

- Runs from Live USB system
  - Leaves no trace on disk
- Routes all traffic through Tor
- Applications sandboxed

Secure Operating Systems
Qubes

- Takes sandboxing to a whole new level
- Every untrusted application can be run on a separate Virtual Machine!
- Also allows routing all traffic through Tor using a Whonix Gateway VM.
- Compartmentalize!



Relevant classes

- CS 194: Undergrad cryptography
  - Nick may also have a 194 in a year if he gets drone funding...
- CS 276: Graduate crypto
- CS 261: Graduate security
- CS 261N: Graduate network security
- CS 294: Miscellaneous
  - In the Fall: decentralized security

email instructor for permission to enroll as undergraduate

Please fill in course evaluations

https://course-evaluations.berkeley.edu

- Very helpful to the department and to us, the staff
- Department-wide effort to increase responsiveness
- +1% points on the final exam
  - After filling it in, submit a screenshot of the confirmation
  - Instructions are posted on Piazza

Thanks to our staff... the TAs and the readers!

Rafael Tupynambá Dutra

Ruta Jawale

Spencer McCall

Ryan Lehmkuhl

Peyrin Kao

Thanks to our random facts “victims”

Most importantly,