CSE 484 / CSE M 584: Physical Security

Winter 2023

Tadayoshi (Yoshi) Kohno
yoshi@cs.Washington.edu

UW Instruction Team: David Kohlbrenner, Yoshi Kohno, Franziska Roesner. Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Announcements

- Monday, 3/6: Last day of lecture (side channels)
- Wednesday, 3/8: Informal conversation about security, research, industry, etc (meeting in CSE2, smaller room)
- Friday, 3/10: Charlie Reis (Google, Chrome, Site Isolation)

Announcements

- Extra Credit Homework 3 online
  - Part 1: Read (short!) fiction and do security analyses
  - Part 2: Use the "fiction writing process" to explore security + society + people
- Final Project Deadline
  - Was told official final time was Monday, 3/13, 8:30-10:20
  - But I think a Monday morning deadline is difficult
  - Deadline: Wednesday, 3/15, 10:20am

Physical Security

- Relate physical security to computer security
  - Locks, safes, etc.
- Why?
  - More similar than you might think!
  - Lots to learn:
    - Computer security issues are often abstract; hard to relate to
    - But physical security issues are often easier to understand
  - Hypothesis:
    - Thinking about the "physical world" in new (security) ways will help you further develop the "security mindset"
    - You can then apply this mindset to computer systems, …

Remember This Example?

Remember This Example?

Physical Security: Adversarial Goals

- **Confidentiality:** adversary should not be able to enter and steal information (e.g., see spy movies, or think about bank computer screens facing windows)
- **Integrity:** adversary should not be able to enter property and remove items, damage items, or place new items (e.g., installing spy device)
- **Availability:** adversary should no be able to deny legitimate entry (denial of service) into an environment (e.g., put superglue in a lock, or gum, or break a wrong key in lock)

Physical Security: Approaches to Security

- Prevention
  - Stop an attack
  - E.g., door locks and fences and bars on windows in physical world environment
- Detection
  - Detect an ongoing or past attack
  - E.g., video camera in physical world environment
- Response
  - Respond to attacks
  - E.g.., home alarm system that calls police when entry is detected

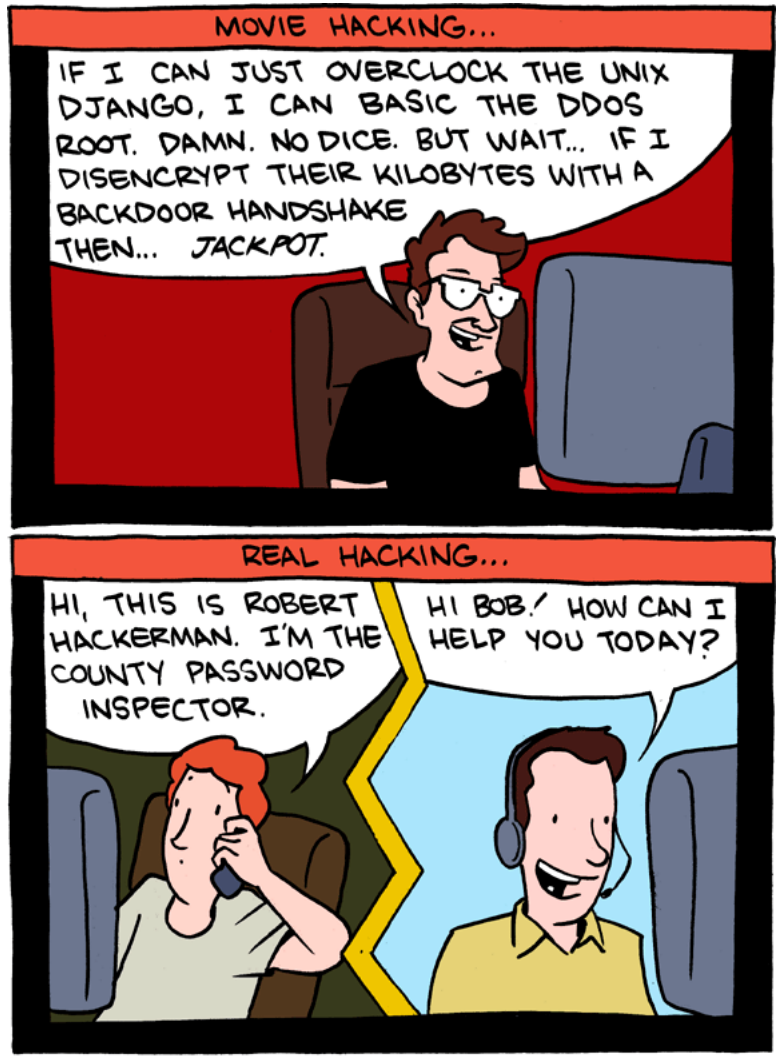
Physical Security is Part of Digital Security

- Securing a system involves a whole-system view
  - Cryptography
  - Implementation
  - People
  - **Physical security**
  - Everything in between

- This is because "security is only as strong as the weakest link," and security can fail in many places
  - No reason to attack the strongest part of a system if you can walk right around it.

Brief (Related) Tangent: Social Engineering

- Art or science of skillfully maneuvering human beings to take action in some aspect of their lives
  - See, e.g.: "The Art of Deception: Controlling the Human Element of Security" by Kevin Mitnick and William Simon
- Used by:
  - Hackers. Penetration testers. Spies. Identity thieves, Disgruntled employees. Scam artists, Recruiters, Salespeople, Governments. …



https://www.smbc-comics.com/?id=2526

Lockpicking

- The following slides will not be online.
- But if you're interested in the subject, we recommend:
  - Blaze, "Cryptology and Physical Security: Rights Amplification in Master-Keyed Mechanical Locks"
  - Blaze, "Safecracking for the Computer Scientist"
  - Tool, "Guide to Lock Picking"
  - Tobias, "Opening Locks by Bumping in Five Seconds or Less"
- Careful: our understanding is that, under current law, possessing lock picks is legal in Washington State, but not everywhere!