CSE 484 / CSE M 584: Physical Security

Fall 2022

Franziska (Franzi) Roesner
franzi@cs

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

• **Homework 3 due** Friday
  – OK to use late days

• **Last extra credit reading due** Thursday [tomorrow]
  – No late days

• **Final project due** next Monday (12/12)
  – No late days
  – Make sure you:
    • Include references
    • Include at least one legal/ethics discussion slide
    • Create original content
    • Go beyond class materials (if it’s a topic we also covered)

• **No section this week**

• **My office hours:** 11:30am on Thursday [tomorrow]
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 not 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
  - From “Social Engineering: The Art of Human Hacking” by Christopher Hadnagy
  - (See also: “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”
  – Tobias, “Opening Locks by Bumping in Five Seconds or Less”

• Careful: possessing lock picks is legal in Washington State, but not everywhere!
Course Evaluation

• Please fill out the course evaluation!
  – https://uw.iasystem.org/survey/264178
  – Or check email

• A good activity for when you are done lockpicking or while you are waiting for locks 😊