CSE 484 / CSE M 584:
Computer Security and Privacy

Autumn 2019

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

Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, John Manferdelli, John Mitchell, Franzi Roesner, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Announcements

- My office hours
  - 12/4 (Wed), 11:30am, CSE1 Attrium?
- Final Project checkpoint 2 looked great!
- HW3 + Lab3: both "light", but please don't wait until Friday to start
- Friday: *Optional* opportunity to learn about Space + Security

Next

- Physical Security + Connections to Computer Security
- Usability
- Social Engineering

PHYSICAL SECURITY

Physical Security and Computer Security

- Relate physical security to computer security
  - Locks, safes, etc
- Why?
  - More similar than you might think!!
  - The more places one sees "the Security Mindset" and security issues manifest, the more opportunities "the Security Mindset Muscle" can grow
  - After CSE 484, please do try to keep thinking about security everywhere – computers, locks, windows, …
    - Of course, take a balanced perspective, consider risk management, and note that "the sky is not falling" ☺

Switching Slide Decks

- We will switch to a slide deck that will not be online
- But if you’re interested in the subject of lockpicking, 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”

Returning now from the other slide deck…

Adversarial Goals

- **Confidentiality** … adversary should not be able to enter and steal information (e.g., see the spy movies, or think about bank computer screens facing windows)
- **Integrity** … adversary should not be able to enter property and remove items, or 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)

Threat Modeling (Security Reviews)

- Assets: What are we trying to protect? How valuable are those assets?
- Adversaries: Who might try to attack, and why?
- Vulnerabilities: How might the system be weak?
- Threats: What actions might an adversary take to exploit vulnerabilities?
- Risk: How important are assets? How likely is exploit?
- Possible Defenses

- E.g., Different defenses and considerations might be appropriate in different situations (e.g., gym locker, bank, nuclear weapons silos)
- E.g., Different adversaries (insiders, like former tenants or ex-employees, or outsiders)

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

Whole System is Critical

- 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.

Overlapping Defensive Ideas

- Defense in Depth
  - Layers, e.g., cardkey access then physical keys
- Deterrents (which can also be layers)
  - Home alarm systems
  - Cameras
- Least Privilege
  - At UW:
    - Grad keys can open certain doors
    - Faculty keys can open all those doors and more doors
    - Custodial keys can open even more doors
    - (see previously cited document from Matt Blaze to understand how this works)

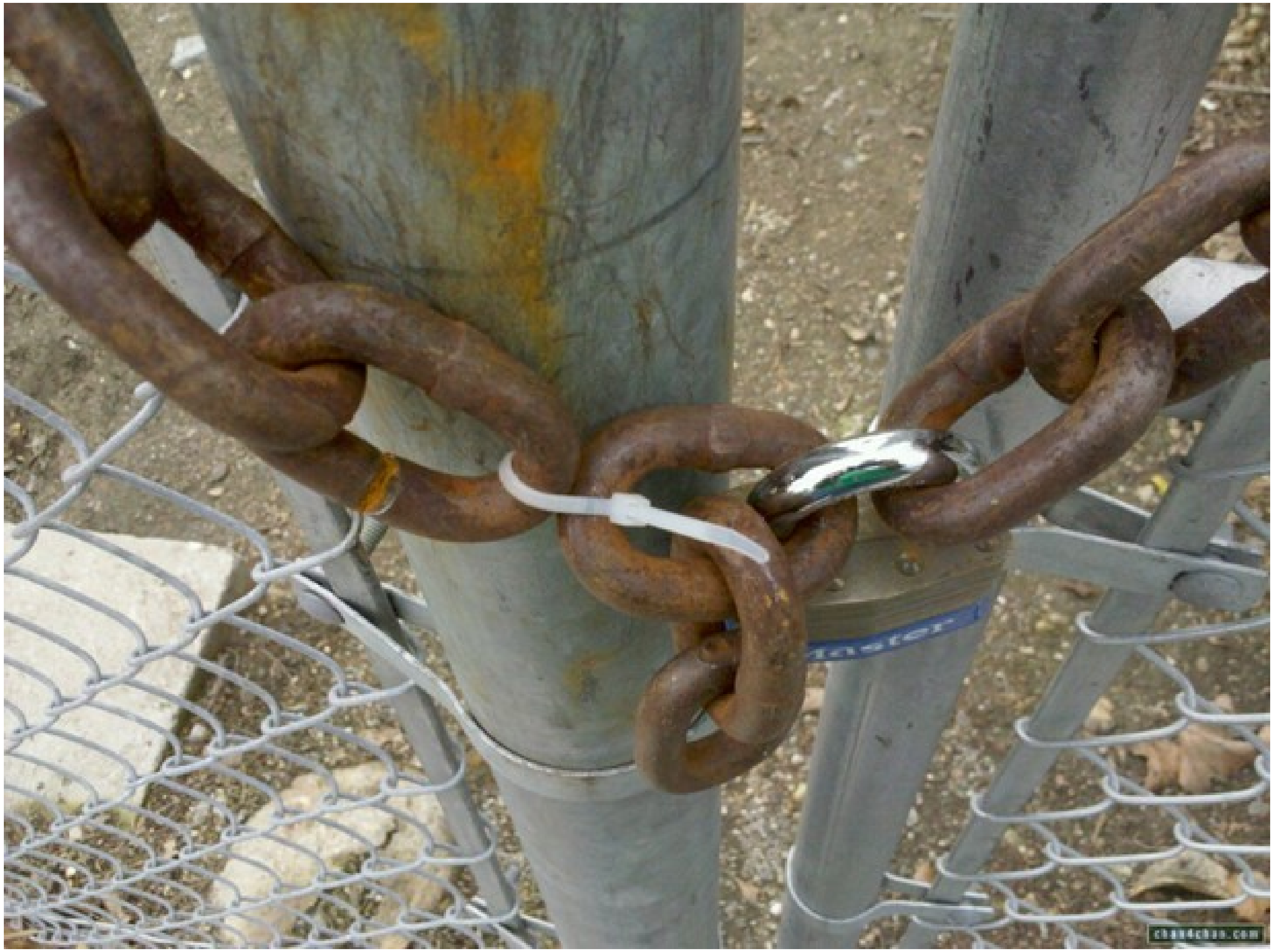
Saltzer and Schroeder (1975 paper)

- See the paper: http://web.mit.edu/Saltzer/www/publications/protection/
- Wikipedia's summary of principles on next slide (since Wikipedia summary is shorter): https://en.wikipedia.org/wiki/Saltzer_and_Schroeder%27s_design_principles
  - Connections and insights can be made by thinking about these principles in the context of physical security

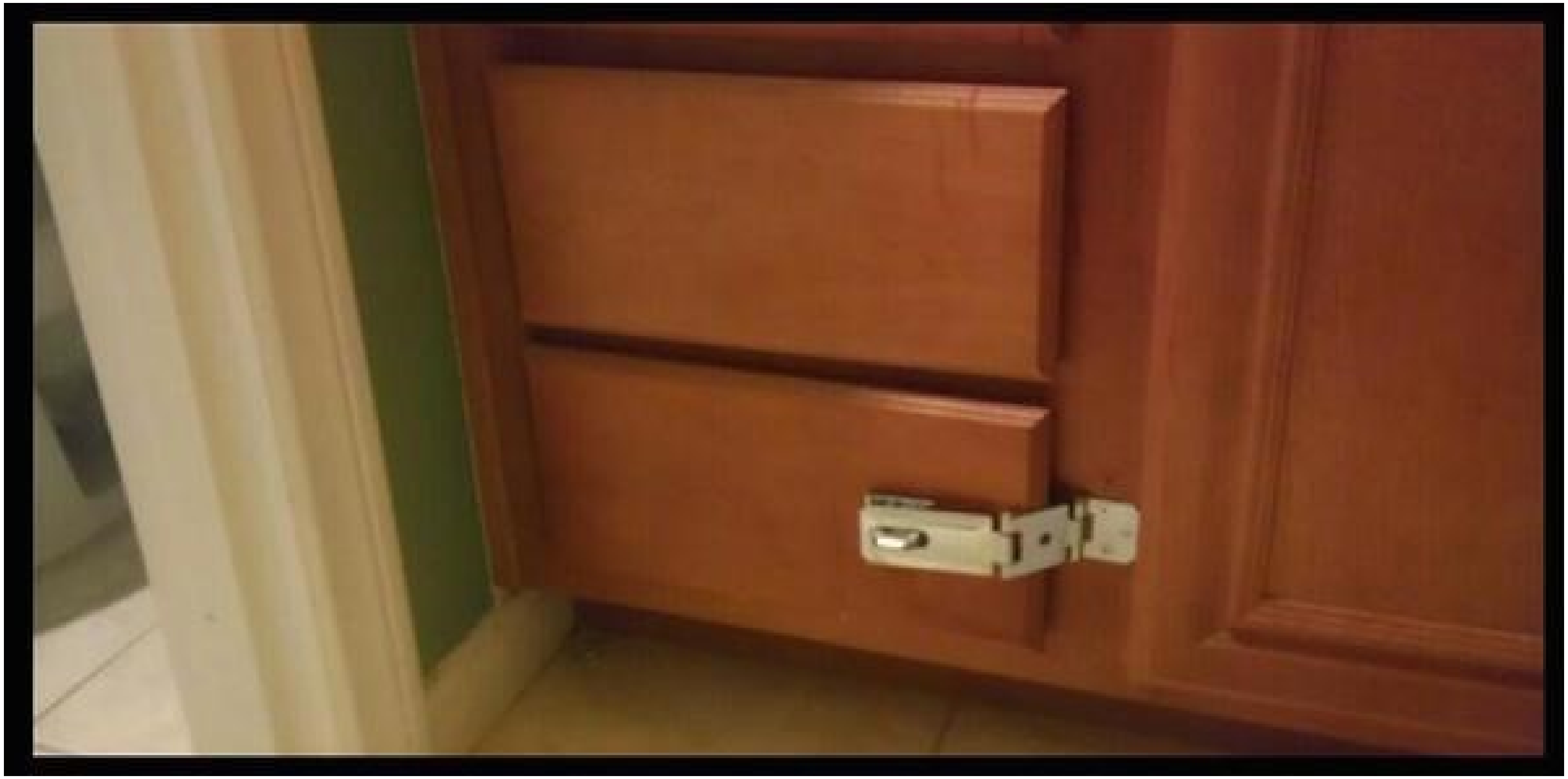
Saltzer and Schroeder (1975 paper)

- **Economy of mechanism:** Keep the design as simple and small as possible.
- **Fail-safe defaults:** Base access decisions on permission rather than exclusion.
- **Complete mediation:** Every access to every object must be checked for authority.
- **Open design:** The design should not be secret.
- **Separation of privilege:** Where feasible, a protection mechanism that requires two keys to unlock it is more robust and flexible than one that allows access to the presenter of only a single key.
- **Least privilege:** Every program and every user of the system should operate using the least set of privileges necessary to complete the job.
- **Least common mechanism:** Minimize the amount of mechanism common to more than one user and depended on by all users.
- **Psychological acceptability:** It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.
- **Work factor:** Compare the cost of circumventing the mechanism with the resources of a potential attacker.
- **Compromise recording:** It is sometimes suggested that mechanisms that reliably record that a compromise of information has occurred can be used in place of more elaborate mechanisms that completely prevent loss.

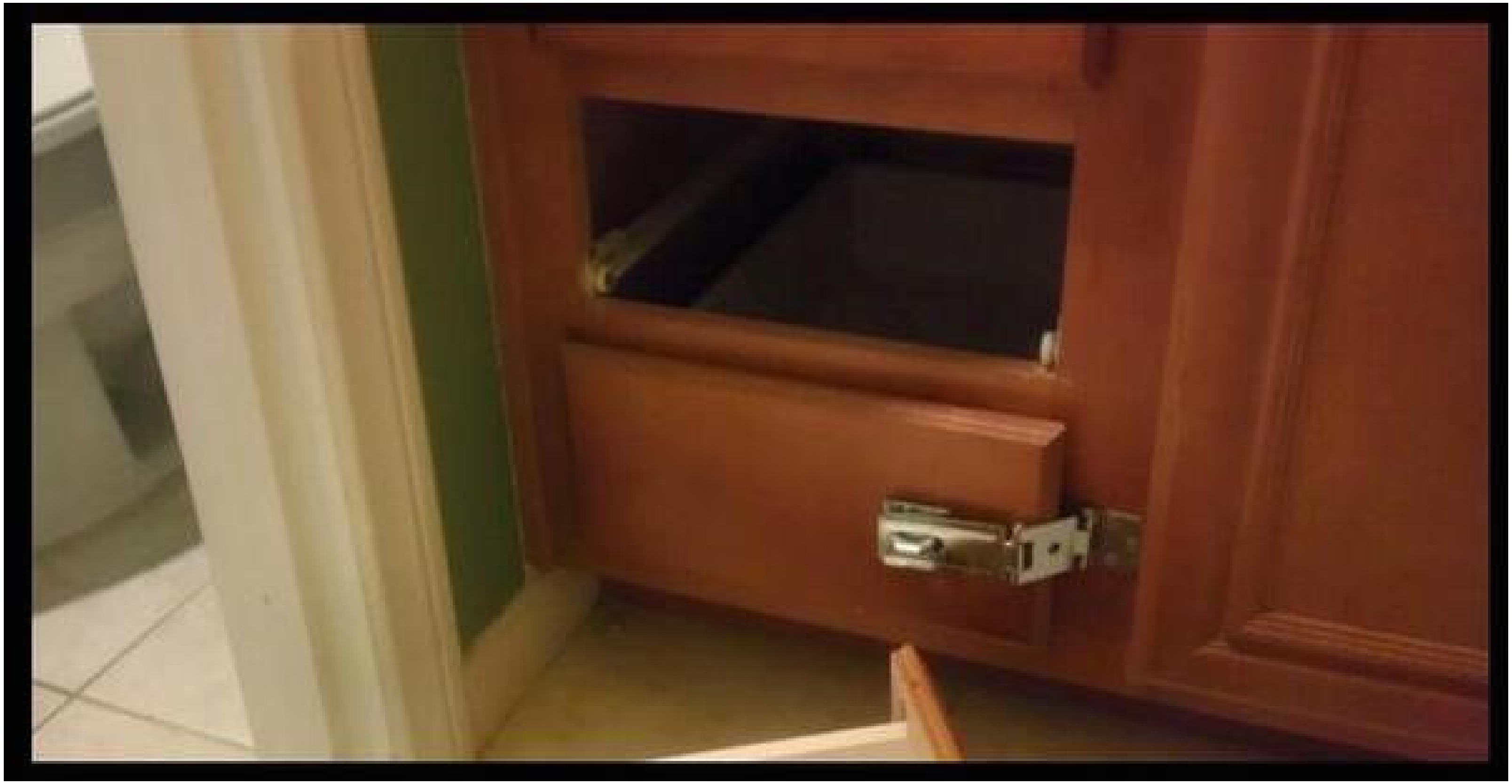
What’s Wrong With This Picture?



What’s Wrong With This Picture?



Think About the Whole System



Usability

- Usability is so important, that the importance of usability has permeated much of this course
- But let's now take a few moments to consider usability specifically

- And I encourage everyone to consider taking an HCI course!
- And to always think about *all* the stakeholders that might be impacted by a system
  - Direct stakeholders
  - Indirect stakeholders
- Developers are users too ☺ (i.e., consider making it easy/usable to develop secure solutions)

On Usability

- Why is usability important?
  - People are the critical element of any computer system
    - People are the real reason computers exist in the first place
  - Even if it is **possible** for a system to protect against an adversary, people may use the system in other, **less secure** ways
  - Usability errors can lead people to think that they are using a secure setting when in fact they are not (e.g., certain password managers)

Question

- What does usable security mean?
- What does it mean for a system to have usable security?

How to Improve?

- These are all **concepts** that people have discussed (not that everyone agrees):
  - Security education and training
  - Help users build accurate mental models
  - Find ways to make systems better match people's natural mental models
  - Make security invisible
  - Make security the least-resistance path
- **On your own:** Think about usability challenges that you have encoutered, with respect to security, and what would have made those systems more usable
- **Big recommendation:** Think proactively about all stakeholders (not just people similar to the system designers)

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
  - (Also see: 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
  - Executive recruiters
  - Salespeople
  - Governments

Example

- Hello?
- Hello?
- Hello?
- You called me?
- You called me?
- There’s something wrong with this phone – what kind of phone do you have?
- (From DEFCON social engineering competition winner)

Example

- Take this survey, win and iPhone
- Call “victims”, to explain that they were victims of a phishing training, which they failed, and now need to clear up their computer
- Have them download and install clean up software
- Yes, okay to bypass “unknown source” warning for the software install
- Okay, great, now next, I need you to now change your password on this main system…
- Good, good, you are clearly a responsible employee. Thank you for taking this so seriously. Now I need you to download a new certificate for your directory server, let me tell you how…
- (Inspired by a talk by Chris Hadnagy, though I might have exact words wrong)

Example from Mark Seiden

- Every time he pen tests a company, he carries with him a printed document that says
  - "This person is doing a pen test of security, authorized by the CEO"
  - "If you have any questions, call this number <number>"
  - Signed by the CEO
- 50% of times that he is stopped by a security guard, he shows them the paper and they say "oh, okay, that makes sense", and then lets him proceed
- 50% of the remaining 50% of the times: the security guard calls the phone number *on the paper…*

Information Gathering

- “No information is irrelevant”

- Example:
  - Know that target collects bumper stickers (see forum post related to bumper sticker collecting)
  - Call target, mention recently inherited a bumper sticker collection
  - Send follow-up email, with a link (behind which is malware)
  - Information used: email address, phone number, information about interest in bumper stickers

Information to Collect

- About a company
  - The company itself
  - Procedures within the company (e.g., procedures for breaks)
- About individuals

Elicitation

- To bring or draw out. Alternately, it is defined as a stimulation that calls up a particular class of behaviors
  - Being able to use elicitation means you can fashion questions that draw people out and stimulate them to take a path of behavior you want.
  - (From Social Engineering: The Art of Human Hacking by Christopher Hadnagy)
- NSA definition: "the subtle extraction of information during an apparently normal and innocent conversation."

Why Elicitation Works

- Most people have the desire to be polite, especially to strangers
- Professionals want to appear well informed and intelligent
- If people are praised, they will often talk more and divulge more
- Most people would not lie for the sake of lying
- Most people respond kindly to people who appear concerned about them

Strategies Social Engineering Experts Mention

- Appeal to Someone’s Ego
- Express a Mutual Interest
- Make a Deliberately False Statement
- Volunteer Information
- Assume Knowledge
- Use the Effect of Alcohol

Pretexting

- The background story, dress, grooming, personality, and attitude that make up the character you will be. Everything you would imagine that person to be.
  - Another definition: creating an invented scenario to persuade a targeted victim to release information or perform some action.
  - (From Social Engineering: The Art of Human Hacking by Christopher Hadnagy)

Principles and Planning

- The more research you do, the better chance of success
- Involving your own personal interests will increase success
- Practice dialects or expressions
- Phone can be easier than in person
- The simpler the pretext, the better the chance of success
- The pretext should appear spontaneous
- Provide a logical conclusion or follow-through for the target

CSE 484 / CSE M 584: Computer Security and Privacy

Autumn 2019

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

Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, John Manferdelli, John Mitchell, Franzi Roesner, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...