CSE 484 / CSE M 584: Computer Security and Privacy

Autumn 2018

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

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

Course Staff

- Instructor:
  - Tadayoshi Kohno (**Yoshi**)
- TAs:
  - Ivan Evtimov, **Amanda Lam**, Yang Wang, Jack Xu, Kyle Yan, Jeff Zhao

- How to reach us: cse484-tas@cs.washington.edu

Quiz Sections and Office Hours

- Quiz sections:
  - Thursday, 1:30-2:20pm, BAG 260
  - Thursday, 2:30-3:20pm, WFS 201
  - Thursday, 3:30-4:20pm, WFS 201
- Office hours
  - Yoshi: Mondays 10:30-11:20, CSE 558
  - TAs:
    - Monday, 2:30-3:30pm, CSE 4th floor breakout
    - Wednesday, 1:30-2:30pm, CSE 2nd floor breakout
    - Friday, 12-1pm, CSE 4th floor breakout

Prerequisites (CSE 484)

- Required: Data Abstractions (CSE 332)
- Required: Hardware/Software Interface (CSE 351)
- Assume: Working knowledge of C and assembly
  - One of the labs will involve writing buffer overflow attacks in C
  - You must have detailed understanding of x86 architecture, stack layout, calling conventions, etc.
- Assume: Working knowledge of software engineering tools for Unix environments (gdb, etc)
- Assume: Working knowledge of Java and JavaScript
- Assume: Ability to learn new programming languages easily

Prerequisites (CSE 484)

- Recommended: Computer Networks; Operating Systems
  - Will help provide deeper understanding of security mechanisms and where they fit in the big picture
- Recommended: Complexity Theory; Discrete Math; Algorithms
  - Will help with the more theoretical aspects of this course.

Prerequisites (CSE 484)

- Most of all: Eagerness to learn!
  - This is a 400 level course.
  - We expect you to push yourself to learn as much as possible.
  - We expect you to be a strong, independent learner capable of learning new concepts from the lectures, the readings, and on your own.

Course Logistics (CSE 484)

- Lectures: MWF: 10:30-11:20pm
  Sections: Thurs: 1:30-2:20pm, 2:30-3:20pm, 3:30-4:20pm
- Security is a contact sport!
- Labs (45% of the grade)
  - Hands-on experience with security issues
  - Can generally be done in teams of 3 students
    (see specific lab descriptions for details)
- Homework (25% of grade)
- Participation and in-class activities (10% of the grade)
- Final project (20% of the grade)

Course Logistics (CSE M 584)

- Same as before, but…
- Labs (42% of the grade) [-3%]
- Homework (22% of grade) [-3%]
- Research readings (10%) [+10%]
- Participation and in-class activities (10%)
- Final (16% of the grade) [-4%]

Labs

- General plan:
  - 2 or 3 labs
    - First lab out soon, likely next week
  - Submit to Canvas system (URL will be on website)
  - Groups of up to three generally allowed (check each project page for details)

Labs

- First lab: Software security
  - Buffer overflow attacks, double-free exploits, format string exploits, …
- Second lab: Web security
  - XSS attacks, SQL injection, …
- Likely third lab: Smart homes, threat modeling, and other emerging issues in computer security

Homework

- 2 or 3 homeworks distributed across the quarter (tentative dates on website)
  - https://courses.cs.washington.edu/courses/%20cse484/18au/assignments.html
  - First homework out now (due Oct 5)

- Do soon: sign ethics form!

Final Project

- **No midterm or final exam!**
- Instead: **12-15 min video** about a security/privacy topic of your choice
  - Groups of up to 3 people
  - Security is a broad field, and this class can't remotely cover everything – this is your chance to explore a security or privacy topic in more detail!
  - Multiple checkpoint deadlines throughout quarter
- Details: http://courses.cs.washington.edu/courses/cse484/18au/project/final.html

Participation

- In-class activities (like the one from today ☺)
  - You'll have 5 free in-class days (for travel etc.)
- Contributions to class forums
  - Don't be silent for 9 weeks and then make 10 posts on the last day of the quarter

- In class: Class too large to make this fair, but you are still encouraged to speak up in class, ask questions, etc
- Discussion section: More opportunities for discussion

Ethics

- To learn to defend systems, you will learn to attack them. You must use this knowledge ethically.

- In order to get a non-zero grade in this course, **you must electronically sign the "Security and Privacy Code of Ethics"** form by 11:59pm on Wed, Oct 3.

Late Submission Policy

- 3 free late days, no questions asked
  - Cumulative, throughout the quarter
  - Use however you wish (all at once, 3x1, …)
- After that, late assignments will be dropped 20% per calendar day.
  - Late days will be rounded up
  - So an assignment turned in 26 hours late will be downgraded 40% if no late days are used
  - See website for exceptions -- some assignments must be turned in on time

Course Materials

- Textbook:
  - Daswani, Kern, Kesavan, "Foundations of Security"
  - Textbook is by now old, but still conveys a way to look at the world
  - Additional materials linked to from course website
- Attend lectures
  - Lectures will not follow the textbook and will cover a significant amount of material that is not in the textbook
  - Lectures will focus on "big-picture" principles and ideas
- Attend sections
  - Details not covered in lecture, especially about homeworks and labs
  - More opportunity for discussion

Other Helpful Books (Online)

- Ross Anderson, "Security Engineering"
  - Focuses on design principles for secure systems
  - Wide range of entertaining examples: banking, nuclear command and control, burglar alarms
- Menezes, van Oorschot, and Vanstone, "Handbook of Applied Cryptography"
- Many many other useful books exist, not all online

Other Books, Movies, …

- Pleasure books include:
  - Little Brother by Cory Doctorow
    - Available online here http://craphound.com/littlebrother/download/
  - Cryptonomicon and REAMDE by Neal Stephenson
  - The Art of Intrusion and The Art of Deception by Kevin Mitnick
  - Countdown to Zero Day by Kim Zetter
  - Many more -- please feel free to post your favorites on the Google Group!
- Movies include:
  - Hackers
  - Sneakers
  - War Games
  - Many more -- please feel free to post your favorites on the Google Group!
- Historical texts include:
  - The Codebreakers by David Kahn
  - The Code Book by Simon Singh

Guest Lectures

- We will have a few guest lectures throughout the quarter
  - Useful to give you a different perspective: research, industry, government, legal
  - Some already scheduled, others TBD

Mailing List for Announcements

multi_cse484a_au18@uw.edu

- Make sure you're on the mailing list
  - We'll send a test mail after class; everyone enrolled should receive it
- URL for mailing list on course website
- We will use the mailing list for announcements; please use the Google Group for discussions

Google Group

- We will set up a Google Group for this course, to discuss assignments
  - https://courses.cs.washington.edu/courses/cse484/18au/admin.html
- Please use it to discuss the homework assignments and labs and other general class materials
- You can also use it to exercise the "security mindset"
  - Discussions of how movies get security right or wrong
  - Discussions of news articles about security (or not about security, but that miss important security-related things)
  - Discussions about security flaws you observe in the real world
  - …

What Does "Security" Mean to You?

- See worksheet, Q1 + Q2
- (Feel free to answer Q4 + Q5 now too)

How Systems Fail

Systems may fail for many reasons, including:

- Reliability deals with accidental failures
- Usability deals with problems arising from operating mistakes made by users
- Security deals with intentional failures created by intelligent parties
  - Security is about computing in the presence of an adversary
  - But security, reliability, and usability are all related

Challenges: What is "Security"?

- What does security mean?
  - Often the hardest part of building a secure system is figuring out what security means
  - What are the **assets** to protect?
  - What are the **threats** to those assets?
  - Who are the **adversaries**, and what are their **resources**?
  - What is the **security policy or goals**?
- Perfect security does not exist!
  - Security is not a binary property
  - Security is about risk management

Current events, security reviews, and other discussions are designed to exercise our thinking about these issues.

Two Key Themes of this Course

1. How to **think** about security
   - The "Security Mindset" – a "new" way to think about systems
2. **Technical aspects of security**
   - Vulnerabilities and attack techniques
   - Defensive technologies
   - Topics including: software security, cryptography, malware, web security, web privacy, smartphone security, authentication, usable security, anonymity, physical security, security for emerging technologies

What This Course is Not About

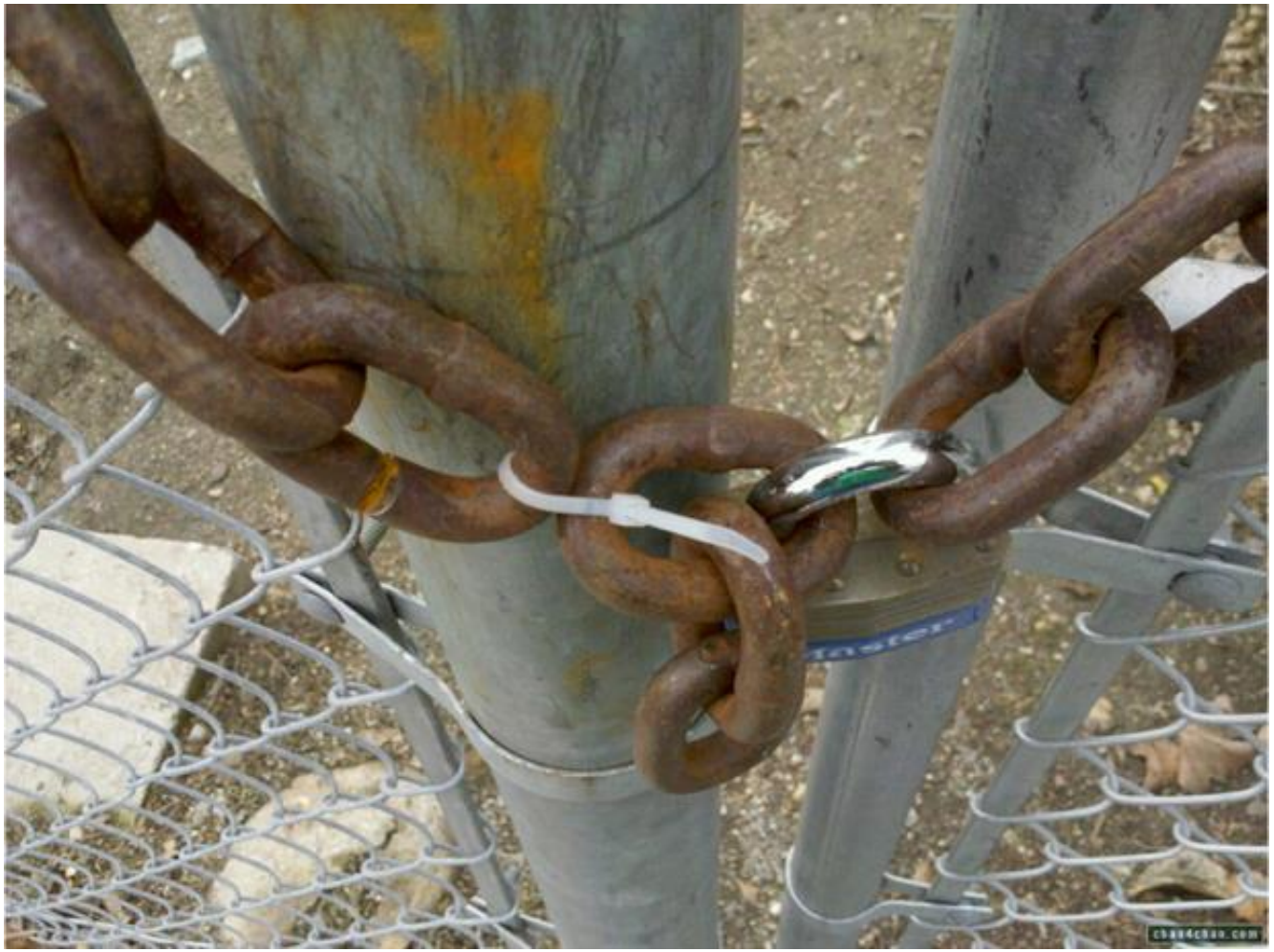
- Not a comprehensive course on computer security
  - Computer security is a broad discipline!
  - Impossible to cover everything in one quarter
  - So be careful in industry or wherever you go!
- Not about all of the latest and greatest attacks
  - Read news, discuss on Google Group
- Not a course on ethical, legal, or economic issues
  - We will touch on these issues, but the topic is huge
- Not a course on how to "hack" or "crack" systems
  - Yes, we will learn about attacks … but the ultimate goal is to develop an understanding of attacks so that you can build more secure systems

Theme 1: Security Mindset

- Thinking critically about designs, challenging assumptions
- Being curious, thinking like an attacker
- "That new product X sounds awesome, I can't wait to use it!" versus "That new product X sounds cool, but I wonder what would happen if someone did Y with it…"

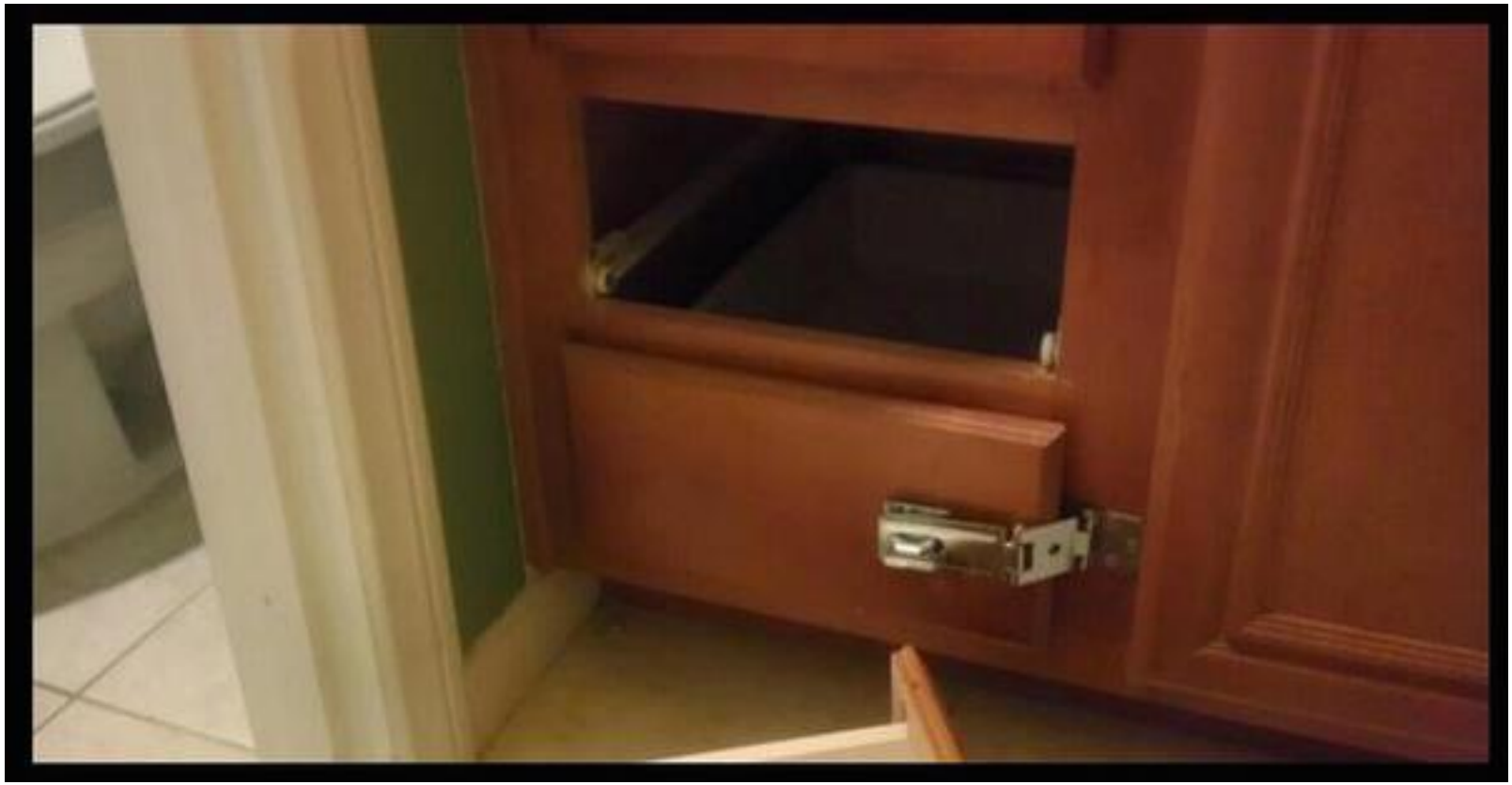
- Why it's important
  - Technology changes, so learning to think like a security person is more important than learning specifics of today
  - Will help you design better systems/solutions
  - Interactions with broader context: law, policy, ethics, etc.

Example



Example – What Do You See?

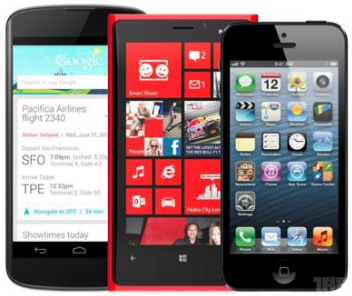
Example – What Do You See?



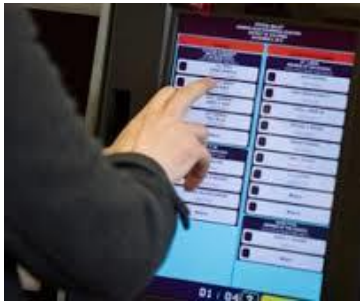
Learning the Security Mindset

- Several approaches for developing "The Security Mindset" and for exploring the broader contextual issues surrounding computer security
  - Homework #1
    - Current event reflections and security reviews
    - May work in groups of up to 3 people (groups are encouraged – **lots of value in discussing security with others!**)
  - In class discussions and activities
  - Participation in Google Group (e.g., critiquing movies)

Security: Not Just for PCs



smartphones



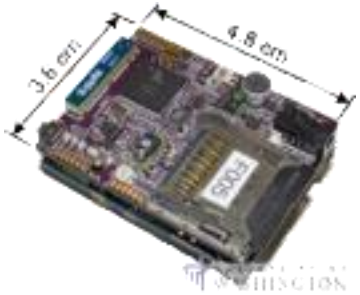
voting machines

EEG headsets

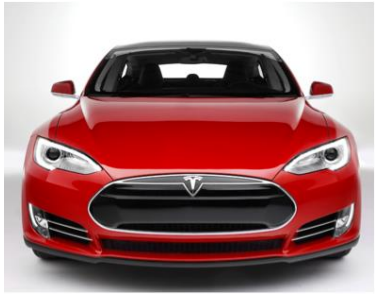
medical devices

wearables

RFID



mobile sensing platforms



cars

game platforms

airplanes