CSE 484 / CSE M 584: Computer Security and Privacy

Spring 2015

Franziska (Franzi) Roesner
franzi@cs.washington.edu

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

What's Wrong With This Picture?

What's Wrong With This Picture?

High-Level Information

- Instructor:
  - Franziska Roesner (Franzi)
- TAs:
  - Peter Ney, Adrian Sham, Michael Mallory, Yueqi Sheng
- Course website
  - Assignments, reading materials, …
- Course email list
  - Announcements
- Course forum
  - Discussion

High-Level Information

- Quiz sections:
  - Thursday, 1:30-2:20pm, EEB 125
  - Thursday, 2:30-3:20pm, EEB 025
- Office hours
  - Franzi: Mondays 9:30-10:30am, CSE 654
  - Others: TBD

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

Prerequisites (CSE 484)

- Required: Data Structures (CSE 326) or Data Abstractions (CSE 332)
- Required: Hardware/Software Interface (CSE 351) or Machine Org and Assembly Language (CSE 378)
- 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

Prerequisites (CSE 484)

- Strongly 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: 8:30-9:20am ;
  Sections: Thurs: 1:30-2:20pm and 2:30-3:20pm
- Security is a contact sport!
- Labs (45% of the grade)
  - Labs involve a lot of programming
  - Can generally be done in teams of 3 students (see specific lab descriptions for details)
- Homework (20% of grade)
- Participation and in-class activities (10% of the grade)
- Final (25% of the grade)
  - Tuesday, June 9, 8:30-10:20am

No make-up or substitute exams! If you are not sure you will be able to take the exam on the assigned date and time, **do not take this course!**

Course Logistics (CSE M 584)

- Same as before, but…
- Labs (40% of the grade) [-5%]
- Homework (15% of grade) [-5%]
- Research readings (10%) [+10%]
- Participation and in-class activities (10% of the grade)
- Final (25% of the grade)

Late Submission Policy

- Late assignments will (generally) be dropped 20% per calendar day.
  - Late days will be rounded up
  - So an assignment turned in 26 hours late will be downgraded 40%
  - See website for exceptions -- some assignments must be turned in on time
- Many assignments due on Friday

Participation Grade

- In-class activities (we'll do one next time)
  - You'll have (at least) 3 free in-class days (for travel etc.)
- Regular contributions to class forums
  - You can pick a pseudonym, though course staff will still know who owns each pseudonym
  - Don't be silent for 9 weeks and then make 10 posts on the last day of the quarter
- In class: harder in a large class, but worth it!

Course Materials

- Textbook:
  - Daswani, Kern, Kesavan, "Foundations of Security"
  - Additional materials linked to from course website
- Attend lectures
  - Lectures will not follow the textbook and will cover some material that is not in the textbook – and you will be tested on it!
  - Lectures will focus on "big-picture" principles and ideas
  - Much of the crypto work will come from "Cryptography Engineering" (Ferguson et al), but you shouldn't need to buy the book (come to lectures)
- Attend sections
  - Details not covered in lecture, especially about homeworks and labs

Other Helpful Books (Online)

- Ross Anderson, "Security Engineering" (1st edition)
  - Focuses on design principles for secure systems
  - Wide range of entertaining examples: banking, nuclear command and control, burglar alarms
  - You should all at least look at the Table of Contents for this book.
  - (2nd edition available for purchase)
- 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
  - Many more -- please feel free to post your favorites on the forum!
- Movies include:
  - Hackers
  - Sneakers
  - Die Hard 4
  - WarGames
  - Many more -- please feel free to post your favorites on the forum!
- 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, law enforcement, government, legal
  - Some already scheduled, others TBD

Ethics

- In this class you will learn about how to attack the security and privacy of (computer) systems.
- Knowing how to attack systems is a critical step toward knowing how to protect systems.
- But one must use this knowledge in an ethical manner.
- In order to get a non-zero grade in this course, you must electronically sign the "Security and Privacy Code of Ethics" form by 5pm Wednesday, April 8.

Mailing List

multi_cse484a_sp15@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
- Used for announcements

Forum

- We've set up a forum for this course to discuss assignments
  - https://catalyst.uw.edu/gopost/board/franzi/39530/
- 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"
  - (Including discussions of movies, books, and security in the real world)

Labs

- General plan (tentative):
  - 3 labs (timeline TBD, tentative date on website)
    - First lab out approximately next Wednesday
  - Submit to Catalyst system (URL on website)
  - Groups of three generally allowed (check each project page for details)
- http://courses.cs.washington.edu/courses/cse484/15sp/assignments.html

Labs (tentative plan)

- First lab: Software security
  - Buffer overflow attacks, double-free exploits, format string exploits, ...
- Second lab: Web security
  - XSS attacks, ...
- Third lab: TBD

Homework

- Three homeworks distributed across the quarter (tentative dates on website)
  - http://courses.cs.washington.edu/courses/cse484/15sp/assignments.html

- Do now: sign ethics form!

Waitlist

- If you are not yet enrolled, please come see me after class today.

What Does "Security" Mean to You?

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?
- 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

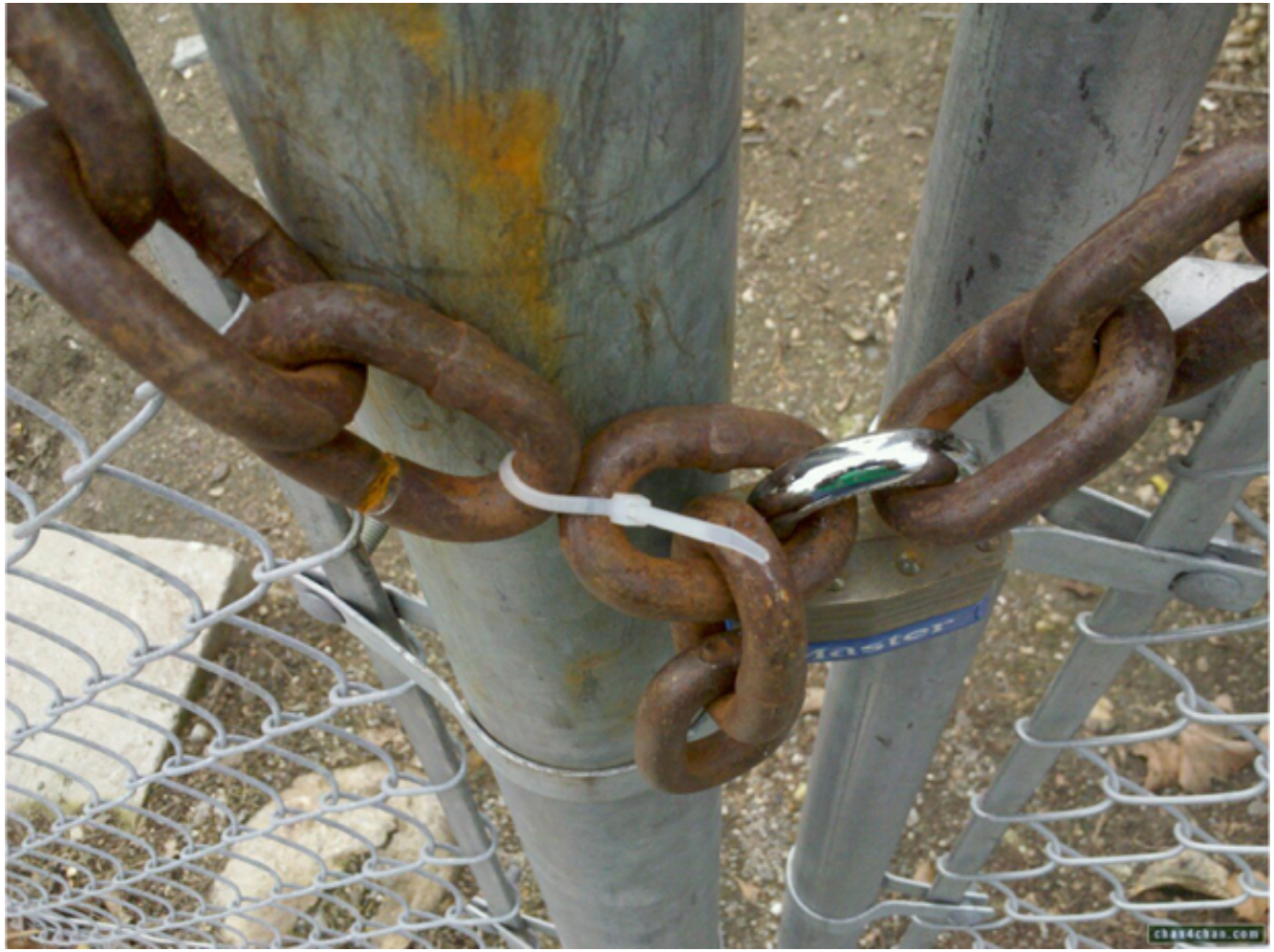
- Not a comprehensive course on computer security
  - Computer security is a broad discipline!
  - Impossible to cover everything in one quarter
  - So be careful in industry or wherever you go!
- Not about all of the latest and greatest attacks
  - Read news
- Not a course on ethical, legal, or economic 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



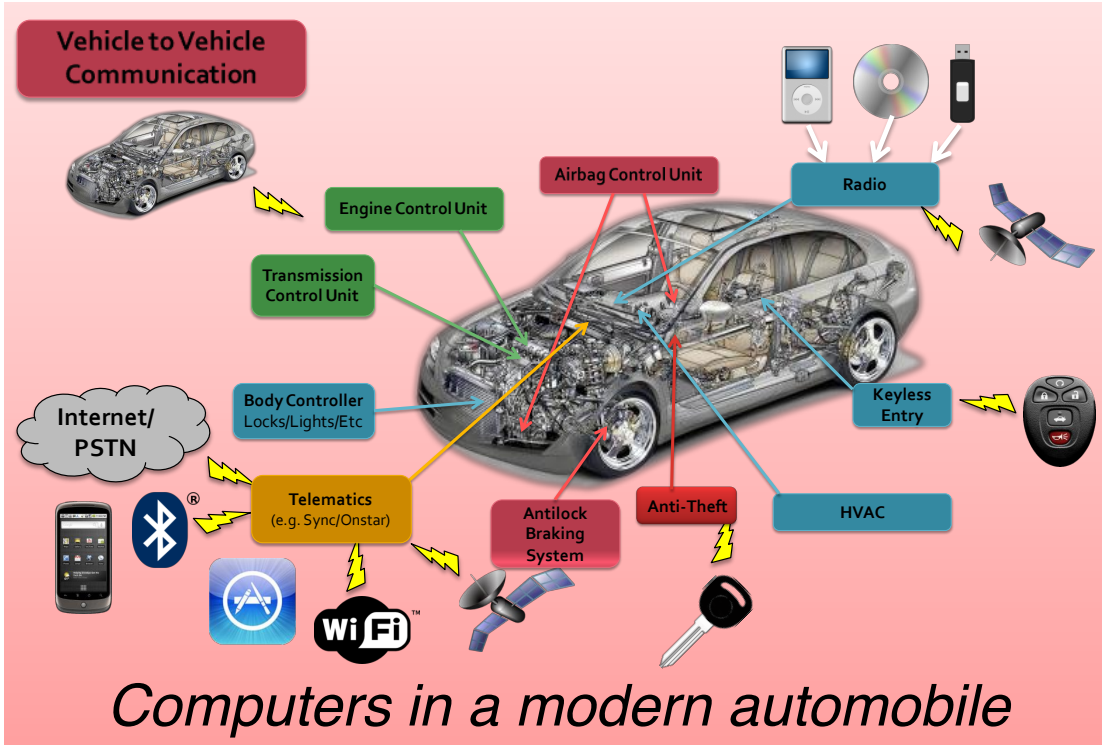
Learning the Security Mindset

- 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 forums (e.g., critiquing movies)

Example: Modern Automobiles

Modern automobiles contain dozens of computers.

Those computers control nearly everything in the car, including locks, lights, brakes, the engine, the airbags, etc.



Computers in a modern automobile

Who might want to attack? Why, and how?