What’s Wrong With This Picture?
What’s Wrong With This Picture?
Course Staff

• Instructor:
  – Franziska Roesner (Franzi)

• TAs:
  – John Abercrombie, Zelina Chen, Garrett Marconet, Jared Moore, Michael Yu

• How to reach us: cse484-tas@cs.washington.edu
Waitlist / Overload Instructions

• Overload instructions will be shared on Friday.
Quiz Sections and Office Hours

• Quiz sections:
  – Thursday, 1:30-2:20pm, EEB 003
  – Thursday, 2:30-3:20pm, LOW 205

• Office hours
  – Franzi: Mondays 11am-12pm, CSE 654
  – TAs:
    • Thursdays, 11:30am-1pm, CSE 220
    • Fridays, 11:30am-12:30pm, CSE 007
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)

- 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: 3:30-4:20pm
  Sections: Thurs: 1:30-2:20pm and 2:30-3:20pm
• 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:
  - 3 labs (timeline TBD, tentative date on website)
    - First lab out next week
  - Submit to Catalyst system (URL 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, ...

• Third lab: TBD
Homework

• 2 or 3 homeworks distributed across the quarter (tentative dates on website)
  – First homework out now (due Oct 6)

• Do now: 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:
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: harder in a large class, but worth it!
  – More opportunities in section!
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 4.
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%
  – See website for exceptions -- some assignments must be turned in on time
Course Materials

• **Textbook:**
  – 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
  – 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, government, legal
  - Some already scheduled, others TBD
Mailing List

multi_cse484a_au17@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/44137

• 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)
What Does “Security” Mean to You?

• See worksheet, Q1
• (Feel free to answer Q3 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
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.
To Do

• Ethics form (due Wed Oct 4 – do it now!)
• Homework #1 (due Fri Oct 6)
  – Now: Start forming groups (e.g., use discussion board) and thinking about events and technologies you’d like to review.

Questions?

franzi@cs.washington.edu
cse484-tas@cs.washington.edu