High-level information

- **Instructor:**
  - Tadayoshi Kohno (Yoshi)

- **TAs:**
  - Gabriel Cadamuro, Kiron Lebeck, Adrian Sham, Bo Wang

- **Course website**
  - Assignments, reading materials, ...

- **Course email list**
  - Announcements

- **Course forums**
  - Discussion
High-level information

Quiz sections (but no quizzes):
- Thursday, 1:30-2:20 and 2:30-3:20 (EEB 003 and ARC G070)

Office hours:
- Yoshi’s: After class on Wednesdays
- TAs: TBD
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: Mon, Wed, Fri: 10:30-11:20am;
  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 (25% of grade)

- Final project (20% of grade)

- In class activities (10% of grade)

Exceptional work may be rewarded with extra credit
Course Logistics (CSE M 584)

- Same as before, but...
- Labs (42% of the grade)  [-3%]
- Homework (22% of grade)  [-3%]
- Final project (16% of the grade)  [-4%]
- Research readings (10%)  [+10%]
  - Read research papers (~1 paper per week)
  - CSE 484 students can read papers for extra credit
- In class activities (10% of 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
Extra Credit

● Forums
  – *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)

● Sometimes options on assignments

● Research readings
Course Materials

Textbook:
- Daswani, Kern, Kesavan, “Foundations of Security”
- Additional materials linked to from course website

Attend lectures.
- Lectures will not follow the textbook
- Lectures will focus on “big-picture” principles and ideas
- Lectures will cover some material that is not in the textbook
- 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)
- (Also make sure to read the forum)
Other Helpful Books (online)

  - 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)
Others books, movies, ...

- **Pleasure books include:**
  - *Little Brother* by Cory Doctorow
  - *Cryptonomicon* by Neal Stephenson
  - *REAMDE* by Neal Stephenson
  - Many more -- please feel free to post your favorites on the forum!

- **Movies include:**
  - *Hackers*
  - *Sneakers*
  - *Ironman*
  - *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
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 on Friday, October 9.

– URL on course web page
Mailing List

- 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 class-related materials
  - https://catalyst.uw.edu/gopost/board/kohno/40925/

- Please use it to discuss the homework assignments and labs and other general class materials

- Please also use it to discuss “security-mindset-related” things, like movies, books, security in the real world
Labs

General plan:

- ~3 labs (timeline TBD, most likely due on Fridays)
  - First lab out soon
- Submit to Catalyst system (URL on course page)
- Groups of three generally allowed (check each project page for details)
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

- Approximately 4 homework assignments distributed across the quarter

- Do now: sign ethics form
What does “security” mean to you?
Two key themes of this course

- **How to think about security**
  - The Security Mindset - “new” way to think about systems
  - Threat models, security goals, assets, risks, adversaries
  - Connection between security, technology, politics, ethics, ...
  - The first few lectures, and the “security mindset”
    - [http://slashdot.org/](http://slashdot.org/)

- **Technical aspects** of security
  - Attack techniques
  - Defenses
How to *think about security*

Several approaches for developing “The Security Mindset” and for exploring the broader contextual issues surrounding computer security

- Homework 1: Current event reflections
- Homework 1: Security reviews
- In class discussions
- Additional participation in forums (e.g., critiquing movies)
Homework 1: Current events and security reviews

- One current event article
- One security review
- 12 points each
- May work in groups of up to 3 people.
  - Working in groups is actually encouraged.
  - Recall: security is a contact sport -- lots of value in discussing security with other people
  - You can also post on forum, and discuss with more than just your group (but please remember the Gilligan Island rule)
  - And posting in the forum gets you extra credit 😊
Example current events and security reviews

- Past blog URL:  

- Past Security Reviews:  
Technical Themes

- Vulnerabilities of computer systems
  - Software problems (buffer overflows); crypto problems; network problems (DoS, worms); people problems (usability, phishing)

- Defensive technologies
  - Protection of information in transit: cryptography, security protocols
  - Protection of networked applications: firewalls and intrusion detection
  - Least privilege, “Defense in depth”
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 ethical 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
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
What Drives the Attackers?

- Adversarial motivations:
  - Money, fame, malice, revenge, curiosity, politics, terror....
- Fake websites: identity theft, steal money
- Control victim’s machine: send spam, capture passwords
- Industrial espionage and international politics
- Attack on website, extort money
- Wreak havoc, achieve fame
What Drives the Attackers?
(More)

- Access copy-protected movies and videos
- Monitor kids’ Internet activity
- Bypass parents’ monitoring of kids’ Internet activity
What Drives the Attackers? (More)

- Access copy-protected movies and videos
- Monitor kids’ Internet activity
- Bypass parents’ monitoring of kids’ Internet activity
- Monitor kids’ bypassing of parents’ monitoring of kids’ Internet activity
- Bypass parents’ monitoring of kids’ bypassing of parents’ monitoring of kids’ Internet activity
- ...


In-class Activity

- Security and crowdsourcing