High-level information

- Instructor: Tadayoshi Kohno (Yoshi)
  - Office: CSE 558
  - Office hours: Wednesdays, 10:30 to 11:20am (right after class, may change)
  - Open door policy – don’t hesitate to stop by!
- TAs: Alexei Czeskis and Karl Koscher
  - Office/hours: See website (TBD)
- Course website
  - Assignments, reading materials, lecture notes
- Course email list (and blog)
  - Student discussions, announcements

Prerequisites

- Required: Data Structures (CSE 326)
- Required: Machine Org and Assembly (CSE 378)
- Assume: Working knowledge of C and assembly
  - One of the projects involves 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

- 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

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

Course Logistics

† Lectures: Mon, Wed, Fri: 9:30 to 10:20am
† Recitations: Thurs: 8:30 to 9:20am
† Security is a contact sport!
† Projects (40% of the grade)
  • Projects involve a lot of programming
  • Can be done in teams of 2-3 students
† Homeworks (20% of grade)
  • Textbook-style questions (10%)
  • Blog entries (10%)
† Midterm (15% of the grade)
† Final (25% of the grade)

Late Submission Policy

† Homeworks should be turned in at the start of class on the due date
† Blog posts and projects should also be turned in on time
† Late assignments will be dropped 20% per day.
  • Late days will be rounded up
  • So an assignment turned in 1.25 days late will be downgraded 40%.
† Homeworks generally due on Fridays, some exceptions.

Course Materials

† Textbooks:
  Pfleeger and Pfleeger, “Security in Computing” (Main textbook)
  Kaufman, Perlman, and Speciner, “Network Security” (Secondary textbook)
† Lectures will not follow the textbooks
  • Lectures will focus on "big-picture" principles and ideas
  • Attend lectures. Lectures will cover some material that is not in the textbook – and you will be tested on it!
  (Also make sure to read the blog)
† Plus assigned readings from other sources
Other Helpful Books (all online)

- Ross Anderson, "Security Engineering"
  - 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.
- Kaashoek and Saltzer, "Principles of Computer System Design"
- Menezes, van Oorschot, and Vanstone, "Handbook of Applied Cryptography"

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 blog
    - [http://slashdot.org/](http://slashdot.org/)
- Technical aspects of security
  - Attack techniques
  - Defenses

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
  - "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
    - Not much language-based security
    - Moderate discussion of crypto (crypto could take a whole year of courses)
  - So be careful in industry or wherever you go!
- Not about all of the latest and greatest attacks
  - Read bugtraq or other online sources instead
- Not a course on ethical, legal or economic issues
  - We will touch on ethical issues, but not focus on them
- Not a course on how to “hack” or “crack” systems

What is Computer Security?
- Systems may fail for many reasons
- 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, curiosity, politics....
  - Fake websites, identity theft, steal money and more
  - Control victim's machine, send spam, capture passwords
  - Industrial espionage and international politics
  - Access copy-protected movies and videos
  - Attack on website, extort money
  - Wreak havoc, achieve fame and glory

Growing Problem

<table>
<thead>
<tr>
<th>Year</th>
<th>Vulnerabilities reported</th>
</tr>
</thead>
<tbody>
<tr>
<td>1995</td>
<td>4,000</td>
</tr>
<tr>
<td>1996</td>
<td>4,000</td>
</tr>
<tr>
<td>1997</td>
<td>4,000</td>
</tr>
<tr>
<td>1998</td>
<td>4,000</td>
</tr>
<tr>
<td>1999</td>
<td>4,000</td>
</tr>
<tr>
<td>2000</td>
<td>4,000</td>
</tr>
<tr>
<td>2001</td>
<td>4,000</td>
</tr>
<tr>
<td>2002</td>
<td>4,000</td>
</tr>
<tr>
<td>2003</td>
<td>4,000</td>
</tr>
<tr>
<td>2004</td>
<td>4,000</td>
</tr>
<tr>
<td>2005</td>
<td>4,000</td>
</tr>
</tbody>
</table>
**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?
- **Perfect security does not exist!**
  - Security is not a binary property
  - Security is about risk management

**From Policy to Implementation**
- After you’ve figured out what security means to your application, there are still challenges
  - How is the security policy enforced?
  - Design bugs
    - Poor use of cryptography
    - Poor sources of randomness
  - Implementation bugs
    - Buffer overflow attacks
  - Is the system usable?

**Many Participants**
- Many parties involved
  - System developers
  - Companies deploying the system
  - The end users
  - The adversaries (possibly one of the above)
- Different parties have different goals
  - System developers and companies may wish to optimize cost
  - End users may desire security, privacy, and usability
  - But the relationship between these goals is quite complex (will customers choose not to buy the product if it is not secure?)

**Other (Mutually-Related) Issues**
- Do consumers actually care about security?
- Security is expensive to implement
- Plenty of legacy software
- Easier to write “insecure” code
- Some languages (like C) are unsafe
Approaches to Security

- Prevention
  - Stop an attack
- Detection
  - Detect an ongoing or past attack
- Response
  - Respond to attacks
- The threat of a response may be enough to deter some attackers

Blog and Security Reviews

- Previous courses looked at
  - Nike+iPod Sport Kit
  - Wireless keyboards
  - iPhone
  - Zune
  - SingBox
  - Nintendo Wii
  - Dodgeball
  - Netflix
  - ...

Homework 1


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 sign the "Security and Privacy Code of Ethics" form by the start of class on Jan 14 (next Monday).