Computer Security and Privacy

Tadayoshi Kohno

Thanks to Dan Boneh, Dieter Gollmann, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...
High-level information

◆ Instructor: Tadayoshi Kohno (Yoshi)
  • Office: CSE 558
  • Office hours: Mondays, 3:30 to 4:20pm (right after class, may change)
  • Open door policy – don’t hesitate to stop by!

◆ TAs: Alexei Czeskis, Tamara Denning, Karl Koscher
  • Office/hours: See website (TBD)

◆ Course website
  • Assignments, reading materials, ...

◆ Course email list
  • Announcements

◆ Course forum
  • Discussion
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 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 (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.
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 (CSE 484)

- Lectures: Mon, Wed, Fri: 2:30-3:20pm; Recitations: Thurs: 1:30-2:20pm and 2:30-3:20pm
- Security is a contact sport!
- Labs (40% of the grade)
  - Labs involve a lot of programming
  - Can generally be done in teams of 3 students (see specific lab descriptions for details)
- Homeworks (25% of grade)
- Participation (10% of grade)
- Final (25% of the grade)

Exceptional work may be rewarded with extra credit

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 (35% of the grade)
- Homeworks (20% of grade)
- Participation (10% of grade)
- Final (25% of the grade)
- Research readings (10%)
  - Read research papers (1 per week for first 9 weeks)
  - Possibly present one of these papers to the class (depending on enrollment)
Late Submission Policy

Late assignments will (generally) be dropped 20% per day.

- Late days will be rounded up
- So an assignment turned in 26 hours late will be downgraded 40%.
- See website for exceptions

Many assignments due on Friday
Participation Grade

Two possibilities:

• #1: Regular contributions to class forums
  – (You can pick a pseudonym, though course staff will still know who owns each pseudonym)

• #2: Participation in class
  – We will have a seating chart ... at least until I learn everyone’s names.
  – On Wednesday, please pick a seat that you’d like to have for at least the first part of the quarter
Small class in a large class

- This class has ~60 enrolled students
- Hard to have 1-on-1 interactions; not very personal
- Coffee / tea?
  - Approximately once a week for the first half of the quarter, let’s go as a small group for coffee or tea (~8 or 9 students and me)
  - Not required.
  - But an opportunity for all of us to get to know each other better, to discuss security, the broader context, thoughts about the course, current movies, ...
  - Sign up form will be on the website soon
Course Materials

◆ Textbooks:
  • Daswani, Kern, Kesavan, “Foundations of Security”
  • Ferguson, Schneier, Kohno, “Cryptography Engineering”
  • Additional materials linked to from course website

◆ Attend lectures.
  • Lectures will not follow the textbooks
  • Lectures will focus on “big-picture” principles and ideas
  • Lectures will cover some material that is not in the textbook – and you will be tested on it!
  • (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.

- 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
    - Available online here http://craphound.com/littlebrother/download/
  - Cryptonomicon by Neal Stephenson

◆ Movies include:
  - Hackers
  - Sneakers
  - Diehard 4
  - Wargames
  - ...

◆ Historical texts include:
  - The Codebreakers by David Kahn
  - The Code Book by Simon Singh
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 and return the “Security and Privacy Code of Ethics” form by the end of class on Monday (Jan 10).
Mailing List

- Make sure to sign up for the mailing list
- URL for mailing list on course website:
- Used for announcements
Forum

- We’ve set up a forum for this course to discuss assignments
  - https://catalysttools.washington.edu/gopost/board/kohno/20059/
- Please use it to discuss the homeworks and labs and other general class materials
Labs

- Tentative schedule online (future dates subject to change based on progress, etc)

- General plan (tentative):
  - 3 labs
    - Jan 28, Feb 11, March 10
    - First one posted online by next Monday
  - Due Fridays at 5pm.
  - 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: Botnets (tentative)
  • Build a botnet, command and control, leasing, crypto, ...
  • Heavy emphasis on building a secure system (a botnet that can’t be attacked by others)
Homeworks

- Approximately 3 or 4 homework assignments distributed across the quarter (with deadlines compatible with the lab deadlines)
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 forum
    - [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

- Forum: Current event reflections
- Forum: Security reviews
- In class discussions
- Additional participation in forums
Forum: Current events and security reviews

- Two current events posted by (Feb 4, March 4)
- Two security reviews posted by (Feb 4, March 4)
- 12 points each
- 1 point extra credit for each week that you are early
- 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
- Please participate in follow-up discussions on forum
Forum: Current events and security reviews

Previous courses looked at

- Nike+iPod Sport Kit
- Wireless keyboards
- iPhone
- Zune
- SlingBox
- Nintendo Wii
- Dodgeball
- Netflix
- ...

Past blog URL: http://cubist.cs.washington.edu/Security/

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 bugtraq or other online sources instead
- **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
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, terror....
- Fake websites, identity theft, steal money
- 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
Security is a Big Problem

- Security very often on the front page of Slashdot and other media outlets
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.
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?**

Don’t forget the users! They are a critical component!
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