Introduction
CS 136
Computer Security
Peter Reiher
January 8, 2008

Purpose of Class

- To introduce students to computer security issues
- To familiarize students with secure software development
- To learn to handle security in today's installations and systems

Description of Class

- Topics to be covered
- Prerequisites
- Grading
- Reading materials
- Homework
- Office hours
- Web page

Topics to Be Covered

- Cryptography and authentication
  - Use, not design and analysis
  - Crypto classes cover more deeply
- Access control and security models
- Secure software design and programming
- Secure protocols
- Network security – threats and countermeasures
- Operating systems security
- Security analysis and forensics
- Malware, common attacks, and important defenses

Prerequisites

- CS111 (Operating Systems)
- CS118 (Computer Networks)
- Or equivalent classes elsewhere
- If you aren't familiar with this material, you'll be at a disadvantage
  - Talk to me if you want to take this class, anyway

Teaching Assistant

- Peter Petersen
  - pahp@cs.ucla.edu
- Weekly recitation sections on Fridays at 2-4
  - Rolfe 3126
  - Won't cover new material
  - But likely to be helpful with problems with lectures
- Will also handle all homework issues
- Office hours: TBA

Grading

- Midterm – 25%
- Homeworks – 25%
- Final – 50%

Class Format

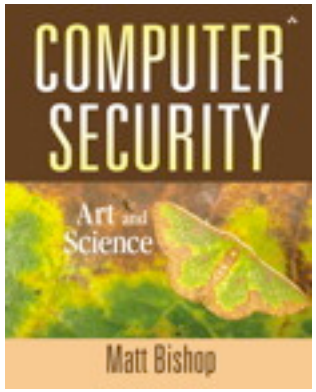
- A lecture class
- Usually discussion of recently covered material at start of the class
- Then lecture on new material
- Questions and discussions always welcomed

Reading Materials

- Textbook
- Non-required supplemental text
- Optional papers and web pages

Textbook

- *Computer Security: Art and Science*
  - By Matt Bishop
- Available in UCLA bookstore
- Bishop has a shorter version
  - That's not the one we're using
- First reading assignment: Chapter 1



Supplemental Text

- *Secrets and Lies*
  - By Bruce Schneier
- Not a textbook at all
- A philosophy of computer security
- Great for appreciating the field and problems
- Not great for depth of technical details
- Not required
  - No readings will be assigned from this book
  - But if you plan to work in this field, read it

Papers and Web Pages

- Non-required reading material
- Might or might not be assigned each week
- Usually made available electronically
  - Through class web page
- Generally relevant news stories or discussion of security topics

Homeworks

- Five assignments
- Requiring practical work
- Performed on the Deter testbed
  - Can be done from any connected location
- Individual, not group, assignments

Homework Topics

1. Access control and permissions
   - Week 3
2. Exploits
   - Week 4
3. Analysis of attacks and forensics
   - Week 6
4. Man in the middle attacks
   - Week 7
5. Intrusion detection
   - Week 8

More on Homeworks

- Each homework has an associated web page
  - With full instructions and pointers to necessary tools
- Due by midnight on Thursday of indicated week
- Class TA will provide advise and assistance on homeworks

The Deter Testbed

- A set of machines devoted to security research and education
- Located at ISI and SRI
- Accessible remotely
- Special accounts set up for this class
- Second lecture will provide instructions on using Deter
  - With further assistance from TA

Tests

- Midterm – February 12 in class
- Final – Friday, March 21, 3:00-6:00 PM
- Closed book/notes tests

Office Hours

- MW 2-3
- Held in 3532F Boelter Hall
- Other times available by prior arrangement

Class Web Page

http://www.lasr.cs.ucla.edu/classes/136_winter08

- Slides for classes will be posted there
  - By 5 PM the previous afternoon
  - In 6-up PDF form or Powerpoint
- Readings will be posted there
  - With links to web pages

Introduction to Computer Security

- Why do we need computer security?
- What are our goals and what threatens them?

Why Is Security Necessary?

- Because people aren't always nice
- Because a lot of money is handled by computers
- Because a lot of important information is handled by computers
- Because our society is increasingly dependent on correct operation of computers

History of the Security Problem

- In the beginning, there was no computer security problem
- Later, there was a problem, but nobody cared
- Now, there's a big problem and people care
  - Only a matter of time before a real disaster
  - At least one company went out of business due to a DDoS attack
  - Identity theft and phishing claim vast number of victims
  - A cyberattack released a large quantity of sewage in Australia
  - Recent video showed cyberattack causing an electric transformer to fail
  - Increased industry spending on cybersecurity

Some Examples of Large Scale Security Problems

- The Internet Worm
- Modern malicious code attacks
- Distributed denial of service attacks
- Vulnerabilities in commonly used systems

The Internet Worm

- Launched in 1988
- A program that spread over the Internet to many sites
- Around 6,000 sites were shut down to get rid of it
- And (apparently) its damage was largely unintentional
- The holes it used have been closed
  - But the basic idea still works

Malicious Code Attacks

- Multiple new viruses, worms, and Trojan horses appear every week
- Storm worm continues to compromise large numbers of computers
- IM attacks becoming increasingly popular
  - And cell phone attacks appearing

Distributed Denial of Service Attacks

- Use large number of compromised machines to attack one target
  - By exploiting vulnerabilities
  - Or just generating lots of traffic
- Very common today
- Attacks are increasing in sophistication
- In general form, an extremely hard problem

The (first) DNS DDoS Attack

- Attack on the 13 root servers of the DNS system
- Ping flood on all servers
- Interrupted service from 9 of the 13
- But did not interrupt DNS service in any noticeable way
- A smaller attack on DNS more recently
  - Even less successful

Vulnerabilities in Commonly Used Systems

- 802.11 WEP is fatally flawed
- Vulnerabilities pop up regularly in Windows, Linux, and Apple systems
  - Today, Microsoft will release patches for two Windows vulnerabilities, one critical
- Many popular applications have vulnerabilities
  - Recent vulnerabilities in Adobe Flash and RealPlayer
- Many security systems have vulnerabilities
  - Recent buffer overflow in Cisco Security Agent

Electronic Commerce Attacks

- As Willie Sutton said when asked why he robbed banks,
  - "Because that's where the money is"
- Increasingly, the money is on the Internet
- Criminals have followed
- Common problems:
  - Credit card number theft (often via phishing)
  - Identity theft (phishing, again, is a common method)
  - Loss of valuable data from laptop theft
  - Manipulation of e-commerce sites
  - Extortion via DDoS attacks or threatened release of confidential data

Another New Form of Cyberattack

- Click fraud
- Based on popular pay-per-click model of Internet advertising
- Two common forms:
  - Rivals make you pay for "false clicks"
  - Profit sharers "steal" or generator bogus clicks to drive up profits

Some Recent Statistics

- From Computer Security Institute Computer Crime and Security Survey, 2007[1]
- 46% of respondents reported a security incident in last year
- Total estimated losses by respondents: $66 million
  - 1/3 from financial fraud
  - Also big losses from worms, spyware, outsider penetration

[1] http://www.gocsi.com/forms/csi_survey.jhtml

How Much Attack Activity Is There?

- Blackhole monitoring on a small (8 node) network[1]
- Detected 640 **billion** attack attempts over four month period
- At peak of Nimda worm's attack, 2000 worm probes per **second**

[1] Unpublished research numbers from Farnham Jahanian, U. of Michigan, DARPA FTN PI meeting, January 2002.

Cyberwarfare

- Nation states already developing capabilities to use computer networks for such purposes
- DDoS attack on Estonia
- Continuous cyberspying by many nations
- Concerns about national vulnerabilities of critical infrastructure
  - Many utilities are now connected to the Internet

Something Else to Worry About

- Are some of the attempts to deal with cybersecurity damaging liberty?
- Does data mining for terrorists and criminals pose a threat to ordinary people?
- Are we in danger of losing all privacy?

But Do We Really Need Computer Security?

- The preceding examples suggest we must have it
- Yet many computers are highly insecure
- Why?
- Ultimately, because many people don't think they need security
  - Or don't understand what they need to do to get it

Why Aren't All Computer Systems Secure?

- Partly due to hard technical problems
- But also due to cost/benefit issues
- Security costs
- Security usually only pays off when there's trouble
- Many users perceive no personal threat to themselves
  - "I don't have anything valuable on my computer"
- Ignorance also plays a role
  - Increasing numbers of users are unsophisticated

Computer Security and History

- Much of our computer infrastructure is constrained by legacy issues
  - Core Internet design
  - Popular programming languages
  - Commercial operating systems
- All developed before security was a concern
  - Generally with little or no attention to security

Retrofitting Security

- Since security not built into these systems, we try to add it later
- Retrofitting security is known to be a bad idea
- Much easier to design in from beginning
- Patching security problems has a pretty dismal history

Problems With Patching

- Usually done under pressure
  - So generally quick and dirty
- Tends to deal with obvious and immediate problem
  - Not with underlying cause
- Hard (sometimes impossible) to get patch to everyone
- Since it's not organic security, patches sometimes introduce new security problems

Speed Is Increasingly Killing Us

- Attacks are developed more quickly
  - Often easier to adapt attack than defense to counter it
- Malware spreads faster
  - Slammer infected 75,000 nodes in 30 minutes
- More attackers generating more attacks
  - Over 38,000 new phishing scams last September

Well, What About Tomorrow?

- Will security become more important?
- Yes!
- Why?
  - More money on the network
  - More sophisticated criminals
  - More leverage from computer attacks
  - More complex systems

What Are Our Security Goals?

- Confidentiality
  - If it's supposed to be a secret, be careful who hears it
- Integrity
  - Don't let someone change something they shouldn't
- Availability
  - Don't let someone stop others from using services
- Exclusivity
  - Don't let someone use something he shouldn't

What Are the Threats?

- Theft
- Privacy
- Destruction
- Interruption or interference with computer-controlled services

Thinking About Threats

- Threats are viewed as types of attacks on normal services
- So, what is normal service?

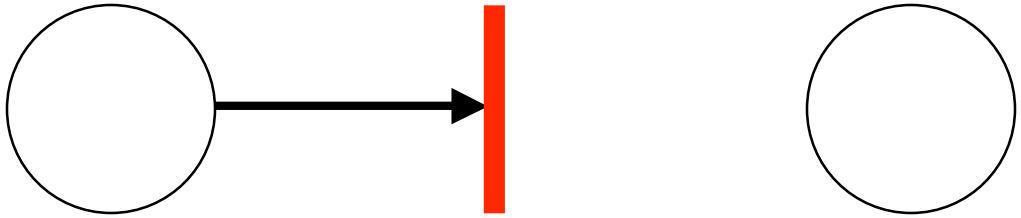
Information Source

Information Destination

Classification of Threats

- Secrecy
- Integrity
- Availability
- Exclusivity

Interruption



Information Source

Information Destination

The information never reaches the destination

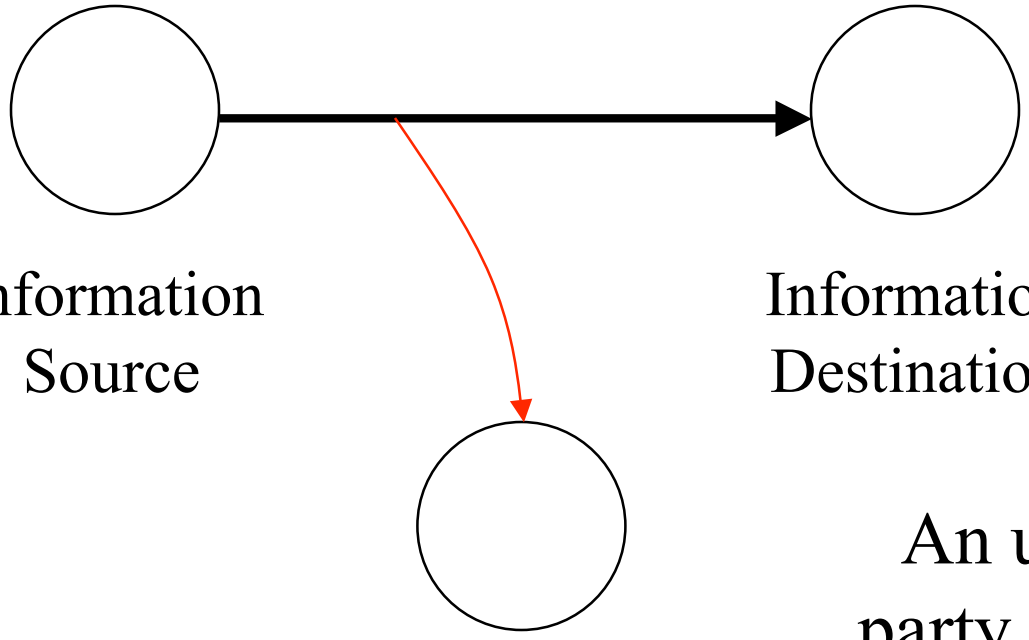
Interruption Threats

- Denial of service
- Prevents source from sending information to receiver
- Or receiver from sending requests to source
- A threat to availability

How Do Interruption Threats Occur?

- Destruction of hardware, software, or data
- Interference with a communications channel
- Overloading a shared resource

Interception



An unintended party receives the information

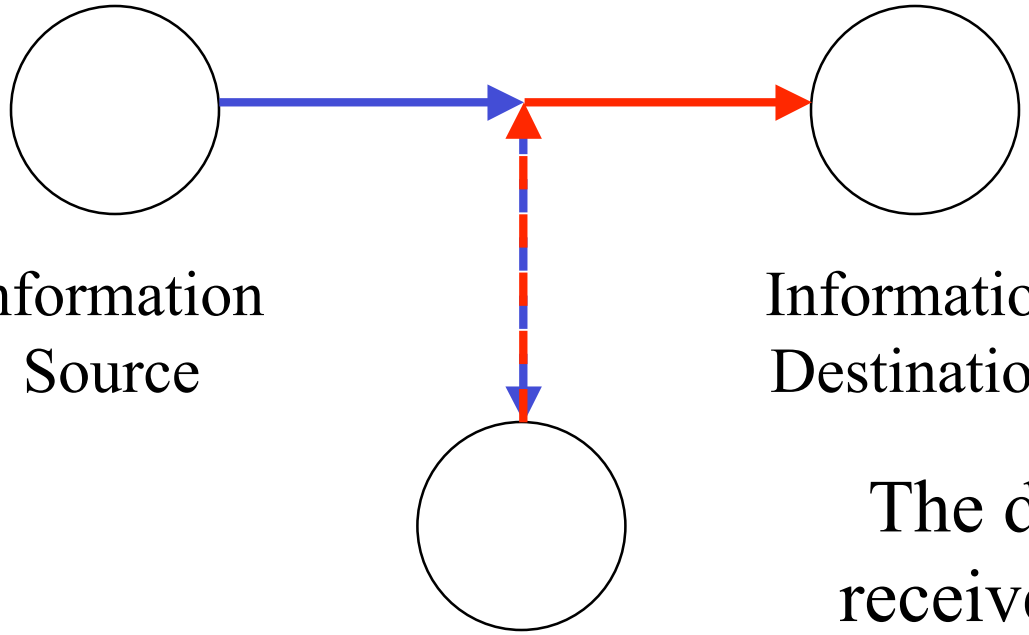
Interception Threats

- Data or services are provided to an unauthorized party
- Either in conjunction with or independent of a legitimate request
- A threat to secrecy
- Also a threat to exclusivity

How Do Interception Threats Occur?

- Eavesdropping
- Masquerading
- Break-ins
- Illicit data copying

Modification



The destination receives different information than what was originally sent

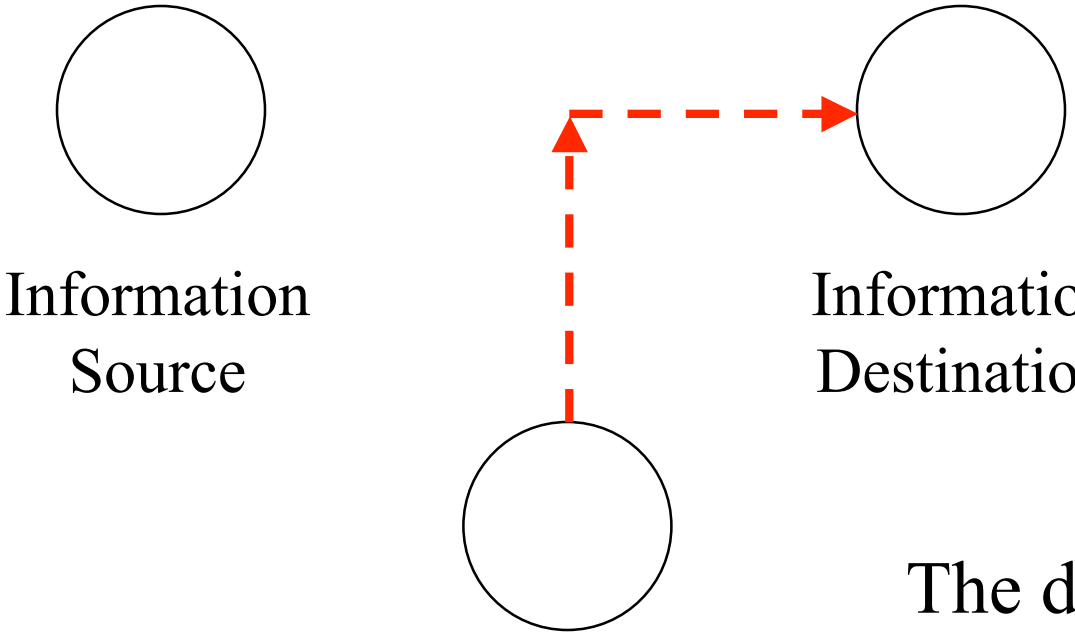
Modification Threats

- Unauthorized parties modify the data
- Either on the way to the users
- Or permanently at the servers
- A threat to integrity

How Do Modification Threats Occur?

- Interception of data requests/replies
- Masquerading
- Break-ins
- Flaws in applications allowing unintended modifications
- Other forms of illicit access to servers and their services

Fabrication



The destination receives information the source never sent

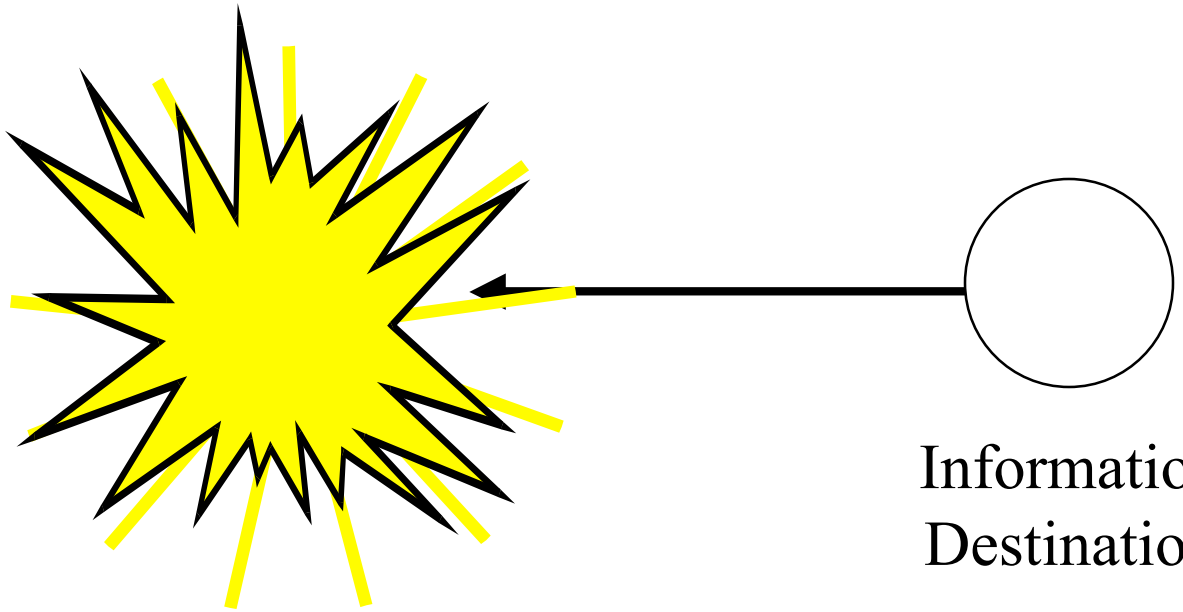
Fabrication Threats

- Unauthorized parties insert counterfeit objects into the system
- Causing improper changes in data
- Or improper use of system resources
- Or other bad behavior
- A threat to integrity
  - And possibly exclusivity

How Do Fabrication Threats Occur?

- Masquerading
- Bypassing protection mechanisms
- Duplication of legitimate requests/responses

Destruction Threats



Information
Destination

The information is no longer accessible to a legitimate user

Destruction Threats

- Destroy data, hardware, messages, or software
- Often easier to destroy something than usefully modify it
- Often (but not always) requires physical access
  - As counterexample, consider demo of destroying power generator remotely[1]

[1]http://www.cnn.com/2007/US/09/26/power.at.risk/index.html?iref=newssearch#cnnSTCVideo

Active Threats Vs. Passive Threats

- *Passive threats* are forms of eavesdropping
  - No modification, injections of requests, etc.
- *Active threats* are more aggressive
- Passive threats are mostly to secrecy
- Active threats are to all properties

Social Engineering and Security

- The best computer security practices are easily subverted by bad human practices
  - E.g., giving passwords out over the phone to anyone who asks
  - Or responding to bogus email with your credit card number
- Social engineering attacks tend to be cheap, easy, effective
- So all our work may be for naught

Social Engineering Example

- Phishing
- Attackers send plausible email requesting you to visit a web site
- To "update" your information
- Typically a bank, popular web site, etc.
- The attacker controls the site and uses it to obtain your credit card, SSN, etc.
- Likelihood of success based on attacker's ability to convince the victim that he's real
  - And that the victim had better go to the site or suffer dire consequences

How Popular is Phishing?

- Anti-Phishing Work Group reported 38,514 new phishing schemes in September 2007 alone[1]
- Up from 13,000 in August 2007
- Based on gullibility of humans more than computer vulnerability
- But can computer scientists do something to help?

[1] http://www.antiphishing.org/

Why Isn't Security Easy?

- Security is different than most other problems in CS
- The "universe" we're working in is much more hostile
- Human opponents seek to outwit us
- Fundamentally, we want to share secrets in a controlled way
  - A classically hard problem in human relations

What Makes Security Hard?

- You have to get everything right
  - Any mistake is an opportunity for your opponent
- When was the last time you saw a computer system that did everything right?
- So, must we wait for bug-free software to achieve security?

How Common Are Software Security Flaws?

- SANS publishes weekly compendium of newly discovered security flaws
- Nearly 100 flaws listed in recent SANS Risks digest
  - Pretty typical number for a week
- So ~5000 security flaws found per year
  - Only counting popular software
  - Only flaws with real security implications
  - And only those that were publicized

Security Is Actually Even Harder

- The computer itself isn't the only point of vulnerability
- If the computer security is good enough, the foe will attack:
  - The users
  - The programmers
  - The system administrators
  - Or something you never thought of

A Further Problem With Security

- Security costs
  - Computing resources
  - People's time and attention
- If people use them badly, most security measures won't do the job
- Security must work 100% effectively
- With 0% overhead or inconvenience or learning

Another Problem

- Most computer practitioners know little or nothing about security
- Few programmers understand secure programming practices
- Few sysadmins know much about secure system configuration
- Typical users know even less

The Principle of Easiest Penetration

- *An intruder must be expected to use any available means of penetration. This is not necessarily the most obvious means, nor is it necessarily the one against which the most solid defense has been installed.*
- Put another way,
  - The smart opponent attacks you where you're weak, not where you're strong

But Sometimes Security Isn't That Hard

- The Principle of Adequate Protection:
  - *Computer items must be protected only until they lose their value. They must be protected to a degree consistent with their value.*
- So worthless things need little protection
- And things with timely value need only be protected for a while

Conclusion

- Security is important
- Security is hard
- A security expert's work is never done
  - At least, not for very long
- Security is full-contact computer science
  - Probably the most adversarial area in CS
- Intensely interesting, intensely difficult, and "the problem" will never be solved