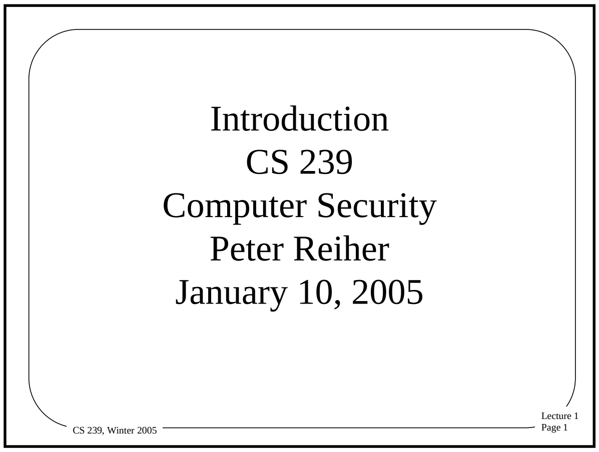
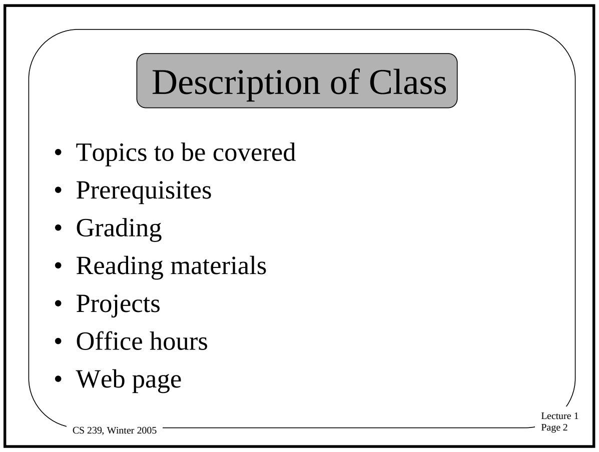
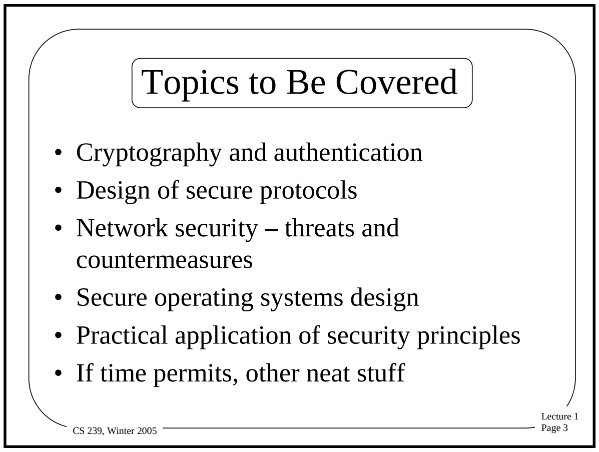


Introduction
CS 239
Computer Security
Peter Reiher
January 10, 2005



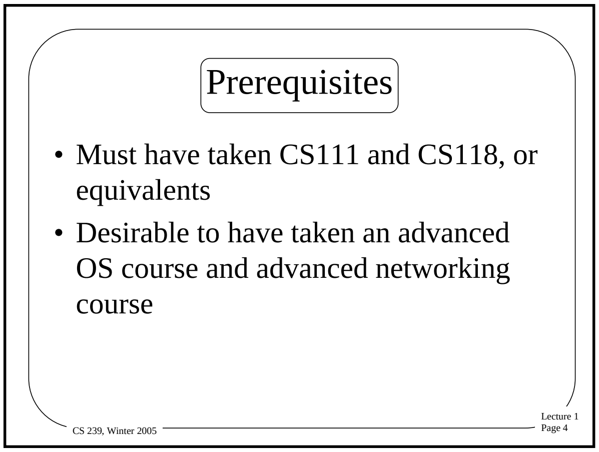
Description of Class

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



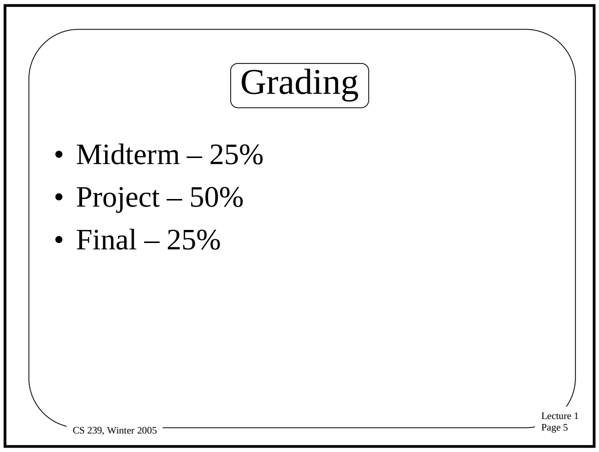
Topics to Be Covered

- Cryptography and authentication
- Design of secure protocols
- Network security – threats and countermeasures
- Secure operating systems design
- Practical application of security principles
- If time permits, other neat stuff



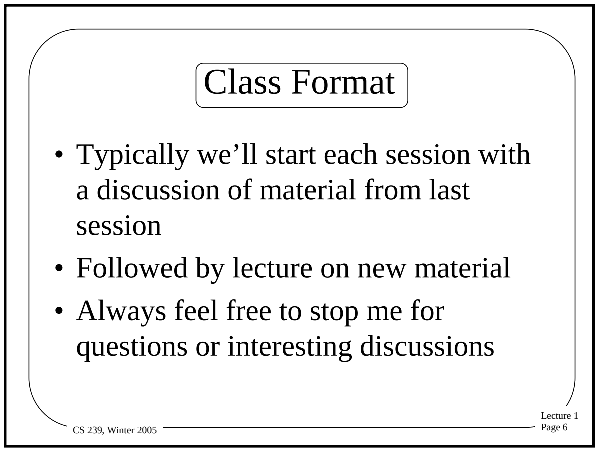
Prerequisites

- Must have taken CS111 and CS118, or equivalents
- Desirable to have taken an advanced OS course and advanced networking course



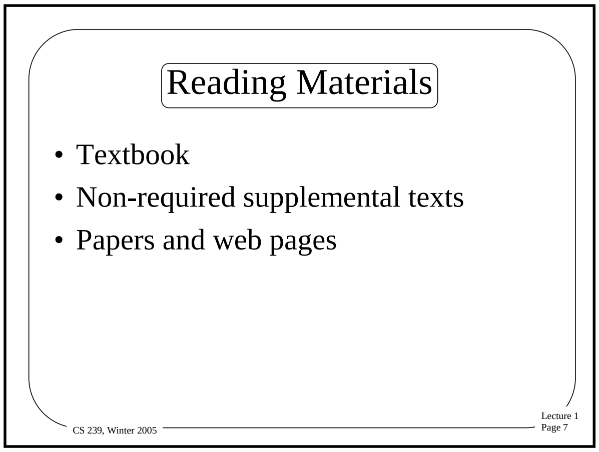
Grading

- Midterm – 25%
- Project – 50%
- Final – 25%



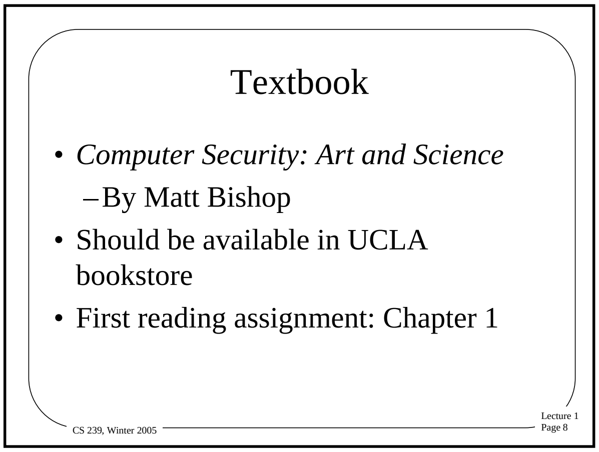
Class Format

- Typically we’ll start each session with a discussion of material from last session
- Followed by lecture on new material
- Always feel free to stop me for questions or interesting discussions



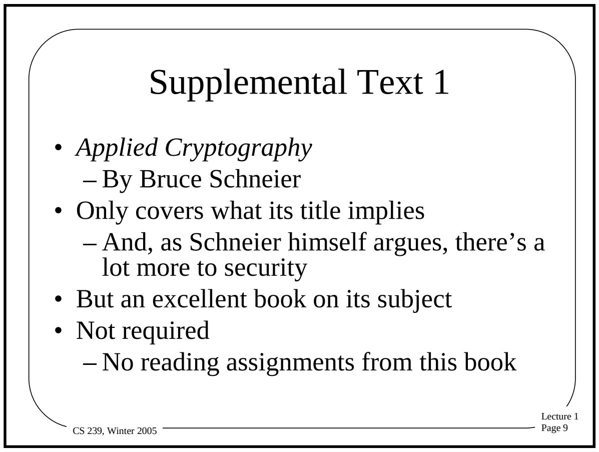
Reading Materials

- Textbook
- Non-required supplemental texts
- Papers and web pages



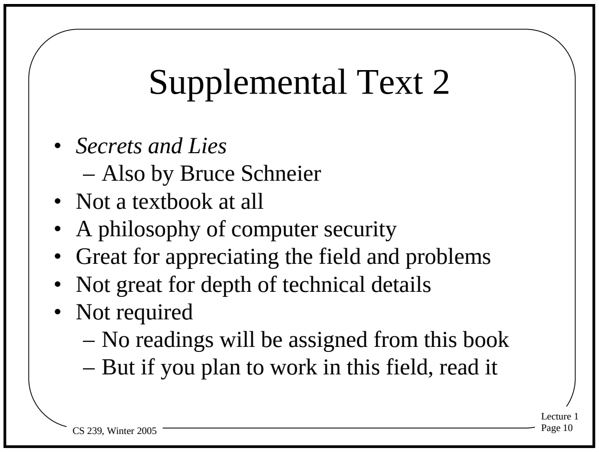
Textbook

- *Computer Security: Art and Science*
  - By Matt Bishop
- Should be available in UCLA bookstore
- First reading assignment: Chapter 1



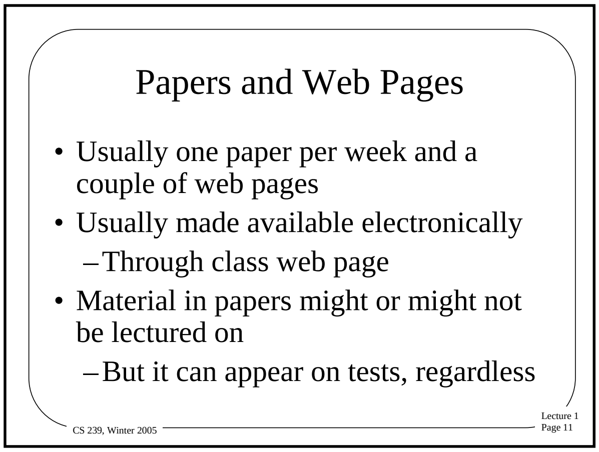
Supplemental Text 1

- *Applied Cryptography*
  - By Bruce Schneier
- Only covers what its title implies
  - And, as Schneier himself argues, there's a lot more to security
- But an excellent book on its subject
- Not required
  - No reading assignments from this book



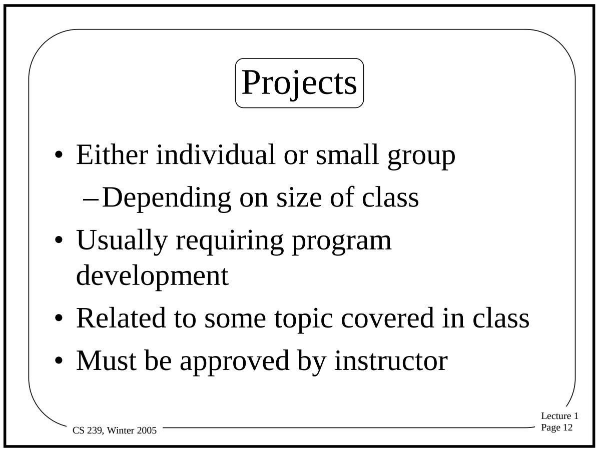
Supplemental Text 2

- *Secrets and Lies*
  - Also 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

- Usually one paper per week and a couple of web pages
- Usually made available electronically
  - Through class web page
- Material in papers might or might not be lectured on
  - But it can appear on tests, regardless



Projects

- Either individual or small group
  - Depending on size of class
- Usually requiring program development
- Related to some topic covered in class
- Must be approved by instructor

Choosing a Project Topic

- Submit a 1 page proposal
  - By end of 3d week of classes (January 28)
  - Email submissions OK
- I will approve them and offer suggestions
- Must be submitted, but not part of grade

What Makes a Good Project?

- Something new
- Something you're interested in
- Maybe it can turn into a paper for you
- Feasible to demonstrate something interesting within the quarter
  - Running code or other practical demonstration, not just a paper

Possible Project Topics

- Security for Internet infrastructure
- Security for ad hoc wireless networks
- Security for peer systems
- Intrusion and insider threat detection
- DDoS and worm defense mechanisms
- Handling botnets
- Defenses against spam and phishing
- Security for sensor networks
- Security evaluations of local labs

Project Updates

- Due at the end of the 7th week of class
  - February 25th
- 1 page report on your group's progress on its project
  - Email submission OK
- Not graded, but required
  - And should describe actual progress

Project Reports

- Written report on the project
- Should:
  - Describe project
  - Discuss how project was performed
  - Cover difficulties and interesting points
  - Describe the implementation
- Expected to be around 15 pages

Project Demos

- Must show working version of project to instructor
- Schedule time individually for this
- Must be done by middle of finals week

Project Deadlines

- Submit project proposal – January 28th
- Submit project update – February 25th
- Demonstration of project to instructor and project reports – March 24th

Tests

- Midterm – February 9
- Final – March 22 (8-11 PM)
- Both tests will be open book
  - Essay questions concentrating on applying knowledge

Office Hours

- MW 2-3
- Held in 3732J Boelter Hall
- Other times available by prior arrangement

Class Web Page

www.lasr.cs.ucla.edu/classes/239_1.winter05

- Slides for classes will be posted there
  - By 5 PM the previous afternoon
  - In 6-up PDF form
- Readings will be posted there
  - With links to papers
- Also links to other interesting info

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
  - A company recently went out of business due to a DDoS attack
  - Many individuals have been harmed by phishing and identity theft

Some Examples of Large Scale Security Problems

- The Internet Worm
- New 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 and worms appear every week
- The Skulls.B Trojan horse contains the Cabir.B worm
  - Spreads to cellphones via Bluetooth
- Skulls wipes out your application files
- Cabir burns your battery trying to spread

Another Recent Example

- The Santy worm
- Exploits a vulnerability in phpBB
  - A bulletin board system
- Interesting feature is how it finds its victims:
  - It searches for them using Google

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 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

Vulnerabilities in Commonly Used Systems

- 802.11 WEP is fatally flawed
- Vulnerabilities pop up regularly in Windows and Linux
- Many popular applications have vulnerabilities
- Many security systems have vulnerabilities

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 will follow
- Common problems:
  - Credit card number theft (often via phishing)
  - Extortion for stolen on-line information
  - Identity theft (phishing, again, is a common method)
  - Manipulation of e-commerce sites
  - Extortion via DDoS attacks

Some Recent Statistics

- From Computer Security Institute/FBI Computer Crime and Security Survey, 2004[1]
- 53% of respondents reported unauthorized use of their systems
- Total estimated losses by respondents: $141 million
  - Primarily costs of handling viruses and denial of service attacks

[1] Survey available at http://www.gocsi.com/press/20020407.html

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.

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
- And, relatively speaking, the computer/network environment is still fairly benevolent
- Ignorance also plays a role
  - Increasing numbers of users are unsophisticated

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?

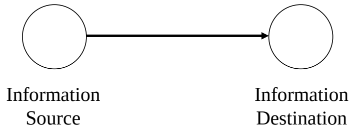
- Confidentiality
  - If it’s supposed to be a secret, be careful who hears it
- Integrity
  - Don’t let someone change something they shouldn’t
- Availability
  - Don’t let someone stop others from using services
- Exclusivity
  - Don’t let someone use something he shouldn’t

What Are the Threats?

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

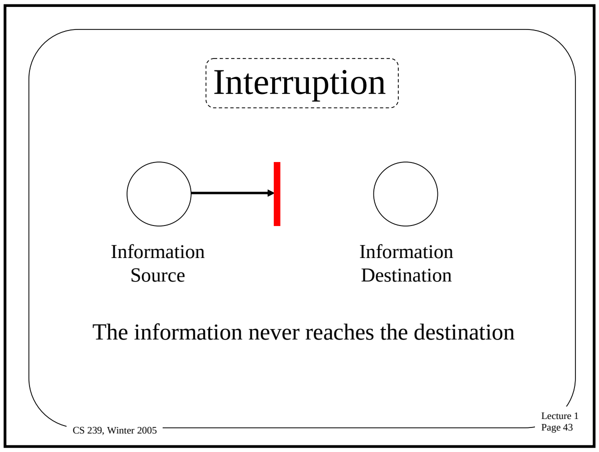
Thinking About Threats

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



Classification of Threats

- Secrecy
- Integrity
- Availability
- Exclusivity

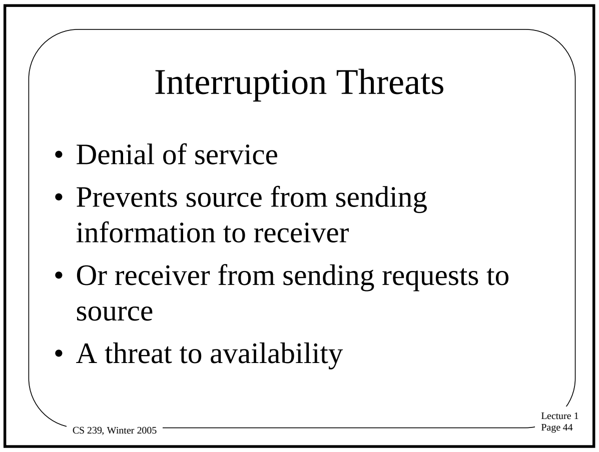


Interruption

Information Source

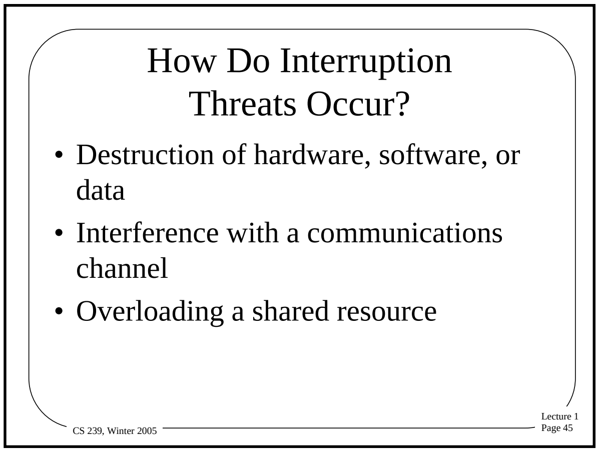
Information Destination

The information never reaches the destination



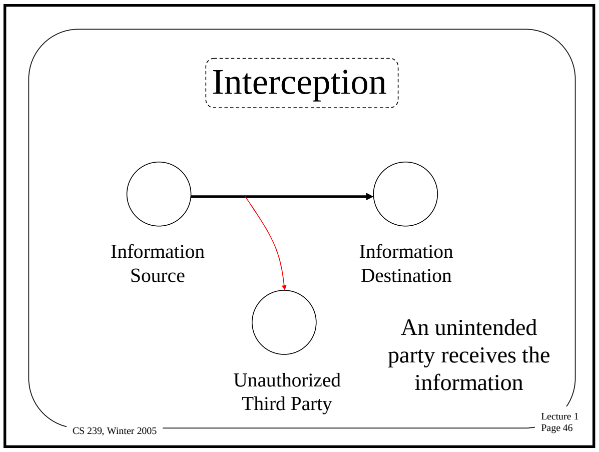
Interruption Threats

- 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



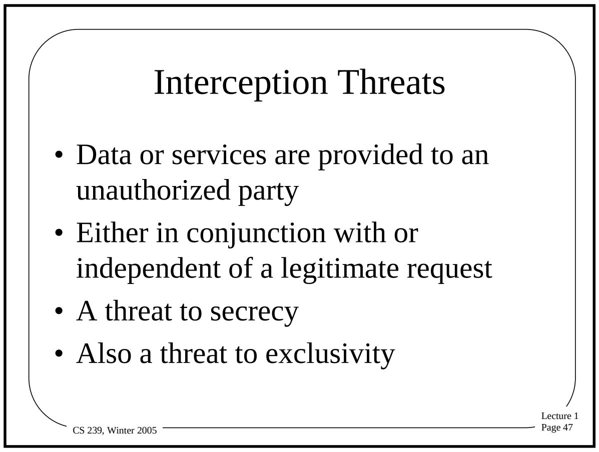
Interception

Information Source

Information Destination

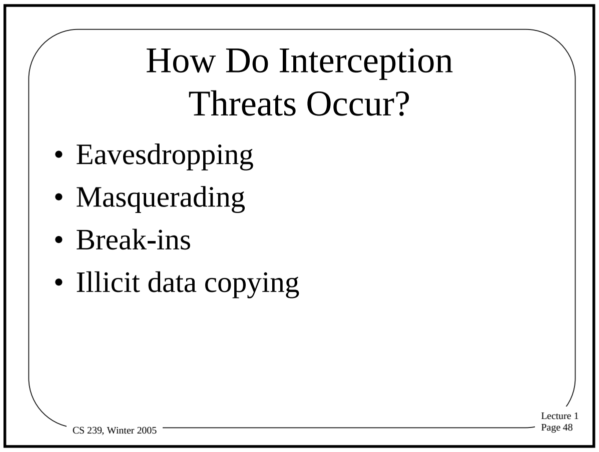
Unauthorized Third Party

An unintended party receives the information



Interception Threats

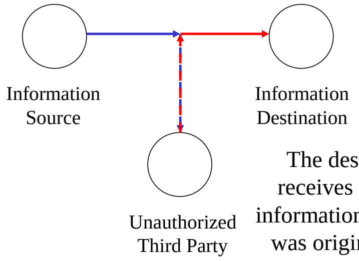
- Data or services are provided to an unauthorized party
- Either in conjunction with or independent of a legitimate request
- A threat to secrecy
- Also a threat to exclusivity



How Do Interception Threats Occur?

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

Modification



The destination receives different information than what was originally sent

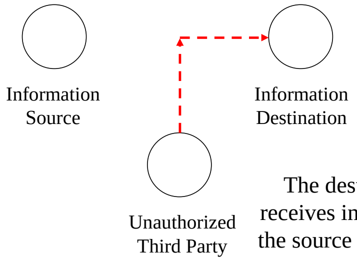
Modification Threats

- 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

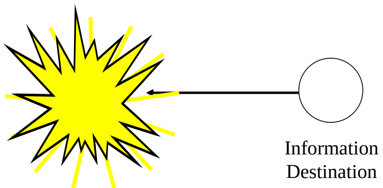
Fabrication Threats

- 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



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

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

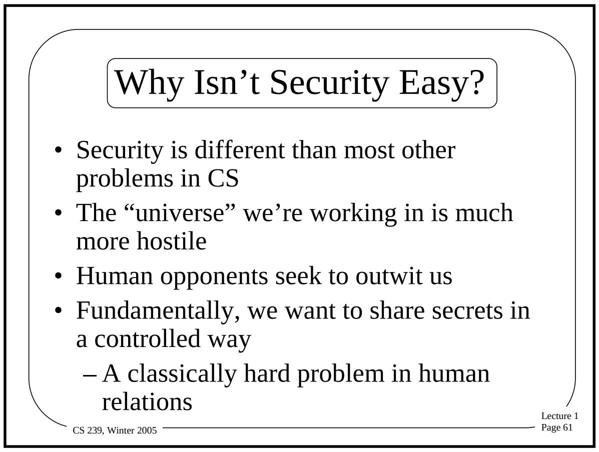
- The best computer security practices are easily subverted by bad human practices
  - E.g., giving passwords out over the phone to anyone who asks
- Social engineering attacks tend to be cheap, easy, effective
- So all our work may be for naught

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

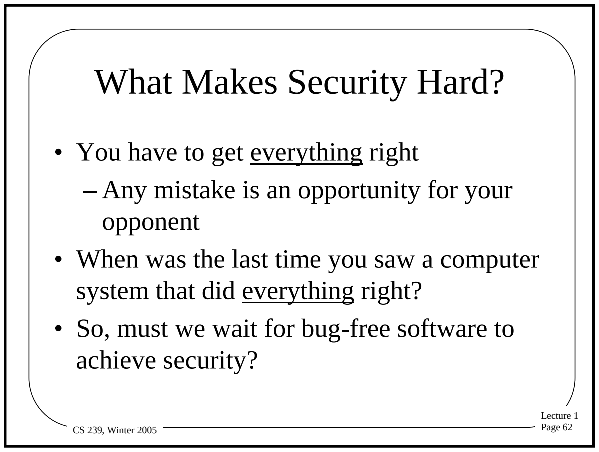
How Popular is Phishing?

- Anti-Phishing Work Group reported 6597 new phishing schemes in October 2004 alone
- Up from 2158 in August 2004
- Based on gullibility of humans more than computer vulnerability
- But can computer scientists do something to help?



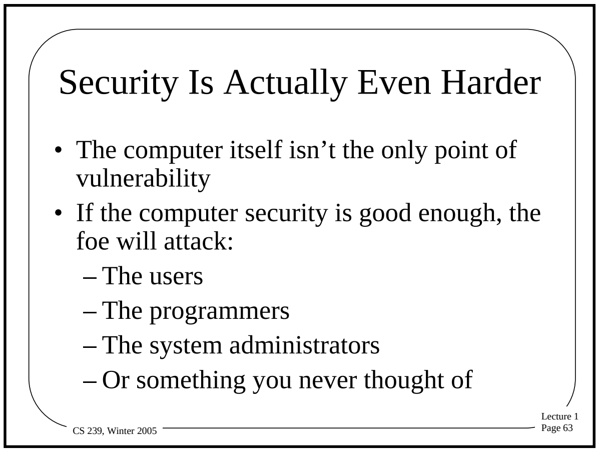
Why Isn't Security Easy?

- 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



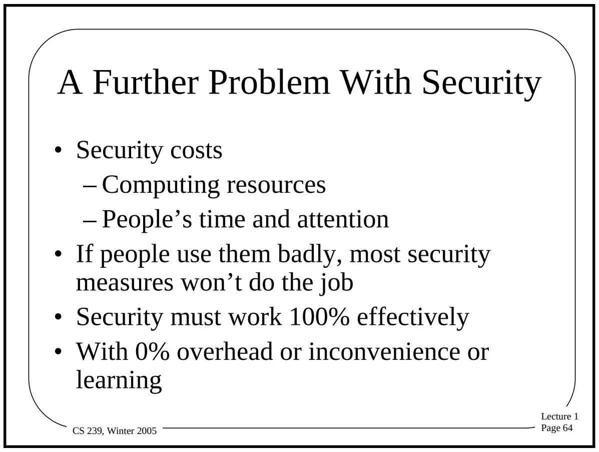
What Makes Security Hard?

- 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?



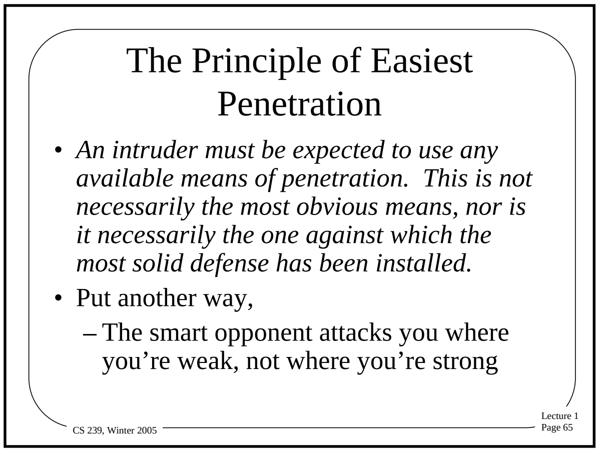
Security Is Actually Even Harder

- 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



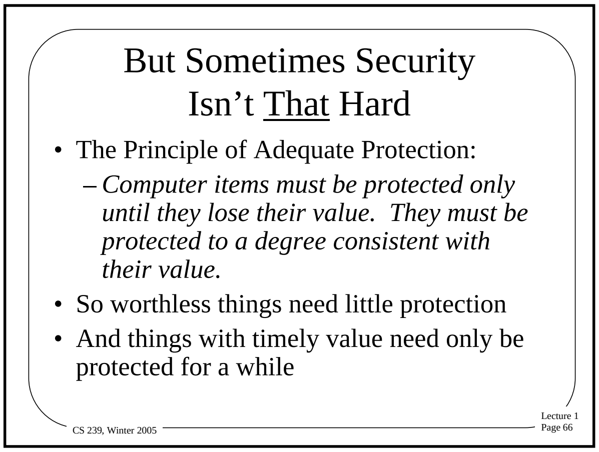
A Further Problem With Security

- 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



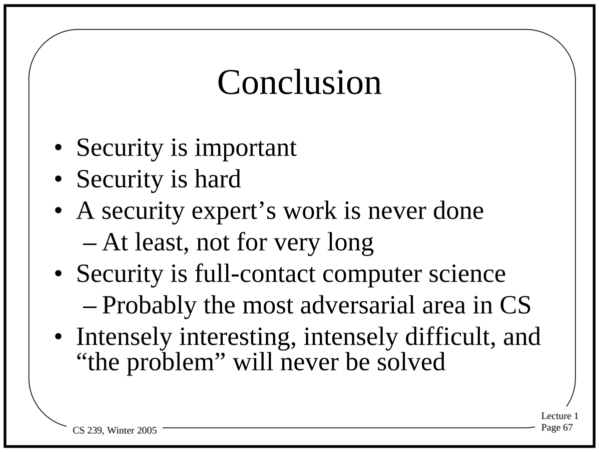
The Principle of Easiest Penetration

- *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

CS 239, Winter 2005

Lecture 1
Page 67