Introduction
CS 239
Security for System Software
Peter Reiher
April 1, 2002

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
- Encapsulated environments
- 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

- Non-required supplemental texts
- Papers and web pages

Recommended Text 1

- *Security in Computing*
  - By Charles Pfleeger
- Kind of a pre-Internet approach to security
- But covers lots of material that's basic and still relevant
- Not a beloved textbook the last time I taught this class

Supplemental Text

- *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

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 beginning of 4th week of classes
  - 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

Possible Project Topics

- Security for sensor networks
- Security for ad hoc wireless networks
- Security for Internet infrastructure
- Active network security
- Intrusion and insider threat detection
- Security evaluations of local labs
- DDoS defense mechanisms

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 the first day of finals week

Project Deadlines

- Submit project proposal – April 24
- Demonstration of project to instructor and project reports – first day of finals week

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.spring02

- Slides for classes will be posted there
  - By 5PM the previous afternoon
  - In 6-up Postscript 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

Some Examples of Large Scale Security Problems

- The Internet Worm
- Newer virus and worm 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

Virus Attacks

- Multiple new viruses and worms appear every week
- A recent worm is the MyLife worm
  - And its variants
- Most recent version carries a caricature of Bill Clinton
  - And a claim that it is “viruse free”
- It actually deletes system files and sends itself to everyone in your address book

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

Vulnerabilities in Commonly Used Systems

- 802.11 WEP is fatally flawed
- Bugs pop up regularly in Linux
- And then there’s Windows . . .
  - Latest problem is that the integrated Media Player will run any arbitrary code provided to it with the proper extension

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
- Credit card number theft, extortion for stolen on-line information, many other problems have become common

Some Recent Statistics

- From Computer Security Institute/FBI Computer Crime and Security Survey, 2001[1]
- 85% of respondents reported breaches
  - 64% reported financial losses
- Total estimated losses by respondents: $377 million
  - Primarily loss of proprietary info and financial fraud

[1] Survey available at http://www.gocsi.com/prelea/000321.html

Results of a Recent Experiment

- 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
- And 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

What Are Our Security Goals?

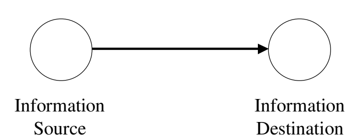
- Confidentiality
  – If it's supposed to be a secret, be careful who hears it
- Integrity
  – Don't let someone change something they shouldn't
- Availability
  – Don't let someone stop others from using services
- Exclusivity
  – Don't let someone use something he shouldn't

What Are the Threats?

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

Thinking About Threats

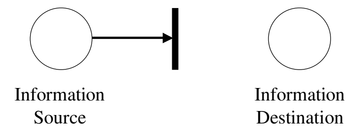
- Threats are viewed as types of attacks on normal services
- So, what is normal service?



Classification of Threats

- Secrecy
- Integrity
- Availability
- Exclusivity

Interruption



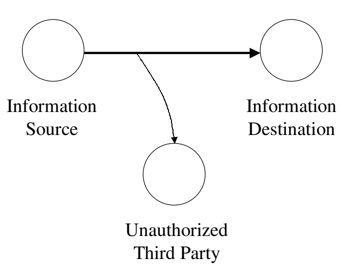
Interruption Threats

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

How Do Interruption Threats Occur?

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

Interception



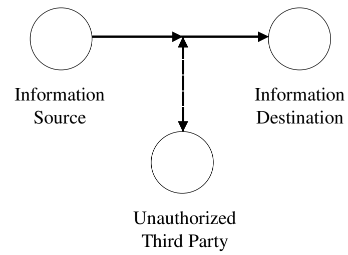
Interception Threats

- 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



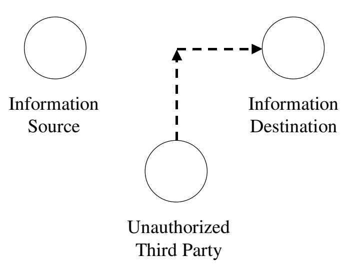
Modification Threats

- 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
- Other forms of illicit access to servers and their services

Fabrication



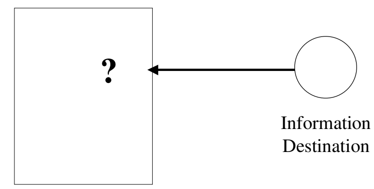
Fabrication Threats

- 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

Destruction Threats



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

- Recently, attackers on IRC/IM services have tried this kind of attack[1]:
  - Convince users to manually download dangerous code
    - “You are infected with a virus that lets hackers get into your machine and read ur files, etc. I suggest you to download <*malicious URL*> and clean ur infected machine. Otherwise you will be banned from <*IRC network*>.”
  - If you download it, your machine is taken over

[1] More details at http://www.cert.org/incident_notes/IN-2002-03.html

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