*testing note writing on Preview

*testing note writing on Preview

Introduction
CS 136
Computer Security

Peter Reiher

March 29, 2016

Text

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

A little bit of cryptography
NOT about building one
but all to use it

- Access control and security models
- Secure software design and programming
- Secure protocols —> security effects across the network
- Network security – threats and countermeasures
- Operating systems security

worms, DDoS

- Security analysis and forensics
- Malware, common attacks, and important defenses
- Privacy privacy & security: tradeoffs
- Practical computer security defenses

how to defend your own computers against these attacks

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
  - People have had serious problems with this unfamiliarity recently

Teaching Assistant

- Joshua Joy
  - jjoy@CS.UCLA.EDU
- Weekly recitation section Fridays
  - Section 1: 8-10, BH 5440
  - Won’t cover new material
  - May help with problems with lectures
- Will also handle all homework issues
- Office hours: TBA

Joshua Joy deal with all homework problems
NOT Professor Reiher

Grading

- Midterm – 25%
- Exercises – 35%
- Final – 40%

Class Format

- A lecture class
- Questions and discussions always welcomed

Reading Materials

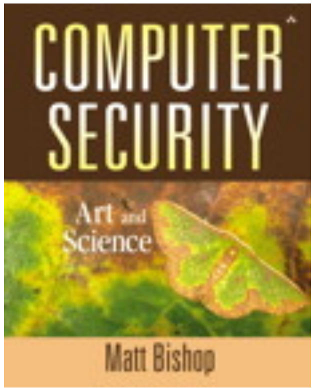
- Textbook
- Non-required supplemental text
- Optional papers and web pages

Textbook

more theoretical and analytical than Reiher:

- *Computer Security: Art and Science*
  - By Matt Bishop

highly respected in the Computer Security community



- Available in UCLA bookstore
- Bishop has a shorter version
  - That's not the one we're using
- First reading assignment: Chapter 1

Supplemental Text

computer security; broad range of computer security; philosophy of computer security

- *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

Exercises

- Five assignments
- Requiring practical work
- Performed on the Deter testbed
  – Accessible via the web from any connected location
- Individual, not group, assignments

Exercise Topics

1. Access control and permissions
   - Week 3
2. Exploits
   - Week 4
3. Analysis of attacks and forensics
   - Week 6 analyze a bunch of data
4. Man in the middle attacks
   - Week 7 perform a man in the middle attack
5. Botnets DDoS attack
   - Week 8

More on Exercises

usually due midnight of the due date

- Each exercise 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 exercises

The Deter Testbed

- A set of machines devoted to security research and education
- Located at ISI and SRI Palo Alto
  Marina Del Rey
- Accessible remotely
  Josh will help set up for account
- Special accounts set up for this class
- First discussion section will provide instructions on using Deter
  - With further assistance from TA
  - Key: CS136KEY

Tests

- Midterm – Tuesday, May 3 in class
- Final – Friday, June 10, 10:30 AM– 1:30 PM
- Closed book/notes tests

Office Hours

- TTh 2-3
- Held in 3532F Boelter Hall
- Other times possible by appointment

Class Web Page

http://www.lasr.cs.ucla.edu/classes/136_spring16

- Slides for classes will be posted there
  - By 5 PM the previous afternoon
  - In 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?

we are moving a lot of money around on the internet
a great deal of crime are going into breaking into computers

people who are on the network can send information
to the computer; they can do things that are bad
* attack power grids remotely in Ukraine; brought the power grid down

Why Is Security Necessary?

computer security insures that systems of computers behave properly

- Because people aren't always nice
- Because a lot of money is handled by computers

national security; private medical records; companies

- Because a lot of important information is handled by computers
- Because our society is increasingly dependent on correct operation of computers

they can control all sorts of processes
ex. our car is incresingly controlled by computers
our automobiles are 'computer networks'
*what about autonomous vehicles? How safe are they?

power grade: how to get electricity to everyone? Moving power around the world in an efficient way is complicated; ppl dealt with this using computers

computer security problem: PhD in 1979 for Professor Reiher wow!
A lot of people would not fund computer security because no one cared…

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

    masquarade as microsoft update
  - Stuxnet seriously damaged Iran's nuclear capability
  - Video showed cyberattack causing an electric transformer to fail
  - There's an underground business in cyber thievery
  - Increased industry spending on cybersecurity

Some Examples of Large Scale Security Problems

- Malicious code attacks
- Distributed denial of service attacks
- Vulnerabilities in commonly used systems

the malware are very successful are typically provided by big companies like Symantec
publish a report, telling you what they learned; Symantec has good report on these
they also have slight variance to create new virus + new malware

Malicious Code Attacks

- Multiple new viruses, worms, botnets, and Trojan horses appear every week
- Recent estimate of $10 billion annual damages from botnets
- Stuxnet worm targeted at nuclear facilities
  - Unspecified amounts of damage done to Iran's nuclear program
- IM and smartphone attacks are popular

botnet with 500 smartphones on it; rent it for DDoS attacks

more security in hardware instead of software - hard for anyone, including Apple, to break into the system

Distributed Denial of Service Attacks

- Use large number of compromised machines to attack one target generate a lot of traffic —> block users off the Internet
  - By exploiting vulnerabilities
  - Or just generating lots of traffic
- Very common today
- A favored tool for hacktivists
  - Recent large DDoS attacks on China and others
- In general form, an extremely hard problem

Vulnerabilities in Commonly Used Systems

- 802.11 WEP is fatally flawed use WPA, not WEP
- Recently, critical vulnerabilities in iOS, Windows, Linux kernel, glibc, Oracle Java implementation
- Many popular applications have vulnerabilities
  - Recent vulnerabilities in Adobe Acrobat, Android OS, Internet Explorer, Microsoft Office, VMWare vCenter Server, Adobe Flash, Oracle Database, etc. disappointing :(
- Many security systems have vulnerabilities
  - OpenSSL and Comodo Internet Security recently is it impossible to write perfect software?

Adobe: they had products a while back that have code base - they can’t redesign their code base from scratch; they have a serious problem here criminals are clever: they have specific methods to attack you

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: identity theft - date of birth, maiden name, SSN —> sitting online
  - 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 betting - legal in Britain —> maybe get hacked
- 2010's Sony data breach estimated to cost the company $170 million

laptop theft has a lot of private information; make sure to clean it before you sell it or turn it away *do not underestimate people on the other side

Ransomware: encrypt all data on your disk: then ask you for ransom to find out what the key is

a common victim here: hospitals

Some Recent Statistics

- 2015 Verizon report found over 2000 data breaches from just 70 organizations

attackers move a lot faster than the defenders

  - In 60% of cases, attackers broke in within minutes
  - And only 20% of the organizations found the breach within a few days
- FBI Cybercrime report for 2014 showed 260,000 reports
  - And losses of over $800,000,000
- Ponemon Institute 2014 survey showed 94% of healthcare organizations lost data in past two years

what attackers are after: espionage, get information, get control ex. US controls drones; what if someone intercepts the signal on the drones

Cyberwarfare

- Nation states have developed capabilities to use computer networks for such purposes
- DDoS attacks on Estonia and Georgia
  - Probably just hackers

maybe it is Russian hackers on these countries

- Some regard Stuxnet as real cyberwarfare
  - Pretty clear it was done by US
- Attacks on Ukrainian power grid

written to destroy stuff in Ukraine in one facility in one place in one country

- Continuous cyberspying by many nations
- Vulnerabilities of critical infrastructure
  - The smart grid will only increase the danger

ex. Google remembers what you searched for; how does Google make its money?
advertising (they know so much about you from your searches)

if at some pt, US government or Russian gov't ask Google for release of information
Facebook, Twitter, and a bunch of social media

Something Else to Worry About

NSA: found something interesting not related to terrorist; then talks to FBI about tackling people; someppl argue this is not legal

- Are some of the attempts to deal with cybersecurity damaging liberty?

Edward Snowden - NSA has been listening to many people and information

- Does data mining for terrorists and criminals pose a threat to ordinary people?
  - The NSA is looking at a lot of stuff . . .
  - And they aren't the only ones
- Can I trust Facebook/Google/MySpace/Twitter/whoever with my private information?
- Are we in danger of losing all privacy?

privacy might be disappearing

Why Aren't All Computer Systems Secure?

- Partly due to hard technical problems
- But also due to cost/benefit issues
- Security costs

increase security has a cost (monetary, or privacy)

- 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"
  - "I don't have any secrets and I don't care what the government/Google/my neighbor knows about me"
- Ignorance also plays a role

this is why I want to do an USIE seminar

  - Increasing numbers of users are unsophisticated
  - Important that computer security professionals don't regard this ignorance as a character flaw
  - It's a fact of life we must deal with

education is important for specified group of people; most people using computers probably don't even care

Legacy and Retrofitting

this is very concerning…

no one was thinking about security when these stuff are developed

- We are constrained by legacy issues
  - Core Internet design
  - Popular programming languages
  - Commercial operating systems

retro-fitting does not work well; why adobe continues to have these problems

- All developed before security was a concern
  - With little or no attention to security
- Retrofitting security works poorly
  - Consider the history of patching

Problems With Patching

working very fast means you want to find the fastest solution to the problem
this sometimes can introduce new problems

- 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

built into the system

- Since it's not organic security, patches sometimes introduce new security problems

IoT: people build tiny devices that are attached to your everyday objects —> these devices do not have any ability to upgrade their software; hard to patch, which means if they have a security flaw, they will always have security flaw

you always get attacked; BUT you don't have these vulnerabilities, so you are good
if you didn't patch windows machine, when you hooked it up into the Internet; your computer will be compromised within a couple of minutes

US Government usually has pretty bad cybersecurity

Speed Is Increasingly Killing Us

- Attacks are developed more quickly
  - Often easier to adapt attack than defense
- Malware spreads faster
  - Slammer got 75,000 nodes in 30 minutes

slammer is a computer worm

- More attackers generating more attacks
  - US DoD computers targeted at least 43,000 times in first half of 2009
  - US military doctrine says cyber attack could be an act of war

department of defense

If you are on the Internet you are being attacked all the time

gov't do get report cards, BUT even with a bad grade, they don't do anything about it

Some Important Definitions

- Security
- Protection
- Vulnerabilities
- Exploits
- Trust

Security and Protection

- *Security* is a policy

a rule or law governing something

  - E.g., "no unauthorized user may access this file"
- *Protection* is a mechanism

a way to implement security policies

  - E.g., "the system checks user identity against access permissions"
- Protection mechanisms implement security policies

Vulnerabilities and Exploits

- A *vulnerability* is a weakness that can allow an attacker to cause problems
  - Not all vulnerabilities can cause all problems
  - Most vulnerabilities are never exploited
- An *exploit* is an actual incident of taking advantage of a vulnerability

  someone found vulnerability, and tried to use that vulnerability to attack the user
  - Allowing attacker to do something bad on some particular machine
  - Term also refers to the code or methodology used to take advantage of a vulnerability

Trust

- An extremely important security concept
- You do certain things for those you trust
- You don’t do them for those you don’t
- Seems simple, but . . .

Problems With Trust

ultimately, we are writing software that are a set of detailed rules
for implementing security

- How do you express trust?
- Why do you trust something?
- How can you be sure who you're dealing with?
- What if trust is situational?

some days I trust you
some days I don't

- What if trust changes?

a very practical issue

certificates - to be discussed
it is a statement of trust; I trust him to do certain things
ex. go into web browser, check your certificates; every so often, one of those entities have certificates will be screwed up

Trust Is Not a Theoretical Issue

- Most vulnerabilities that are actually exploited are based on trust problems
- Attackers exploit overly trusting elements of the computer

phishing is a trust problem ; you trusted the email that came in, and you misplaced the trust

  - From the access control model to the actual human user
- Taking advantage of misplaced trust
- Such a ubiquitous problem that some aren't aware of its existence

transitive trust means you follow the chain of trust to trust ppl or entities you don't know

Transitive Trust

I trust Alice

Alice trusts Bob

Bob trusts David

David trusts Carol

So do I trust Carol?

Should I?

Examples of Transitive Trust

- Trust systems in peer applications
- Chains of certificates

Chain of trust - trust starts in the browser
ex. user with laptop has certificate signed off by CA
use

- But also less obvious things
  - Like a web server that calls a database
  - The database perhaps trusts the web server
  - But does the database necessarily trust the user who invoked the server?
  - Even if the web server trusts the user
- Programs that call programs that call programs are important cases of transitive trust

Because of transitive trust, when one node in this graph breaks, then we have a problem

What Are Our Security Goals?

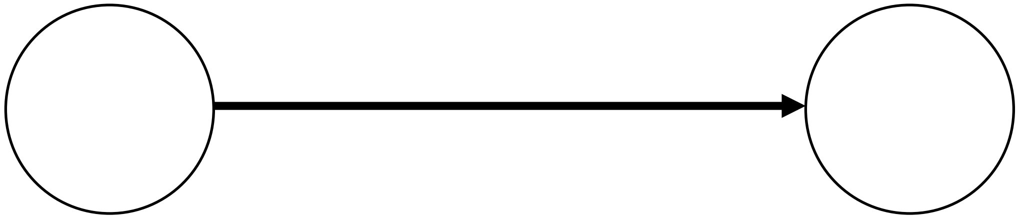
- CIA
- **Confidentiality**
  - If it's supposed to be a secret, be careful who hears it
- **Integrity** we want our data to NOT be changed
  - Don't let someone change something they shouldn't
- **Availability** we can use what we want
  - Don't let someone stop others from using services

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?

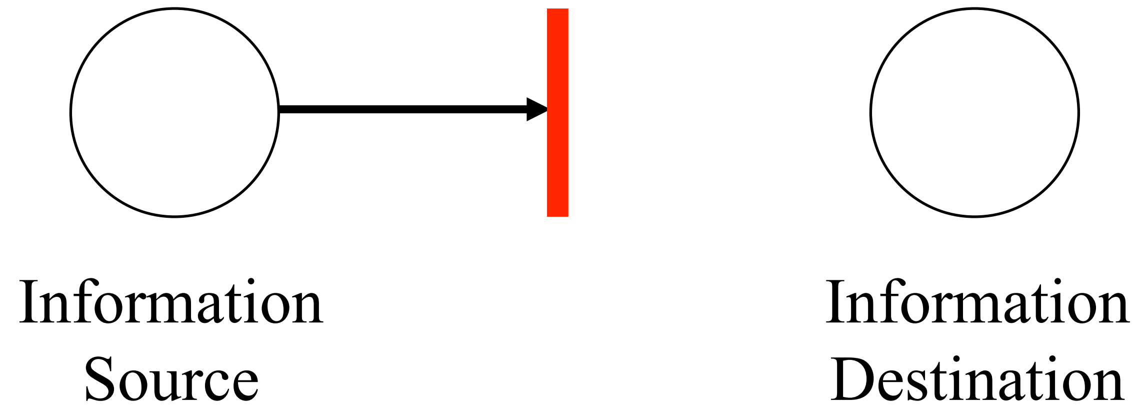


Information Source

Information Destination

Interruption

attacker prevents user from getting information from source to dest.
ex. a denial of service threat



The information never reaches the destination

Interruption Threats

could also be threat to confidentiality

- 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?

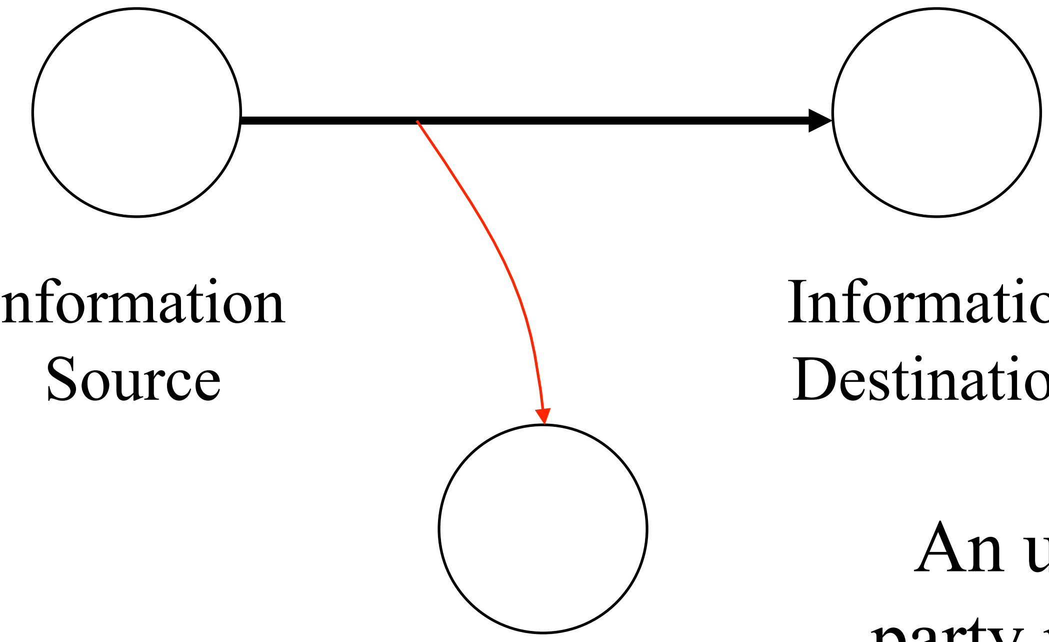
- Destruction of hardware, software, or data
- Interference with a communications channel

wireless channel interference

- Overloading a shared resource

Interception

unauthorized third party: also gets the information
he's not suppose to get it, he does



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 confidentiality

How Do Interception Threats Occur?

- Eavesdropping

communication channels: very general
don’t just mean the Internet; on-machine socket between two processes
bus is a comm channel
anything that allows information from one source to a dest.

- Masquerading

pretend to be someone who seems trusted

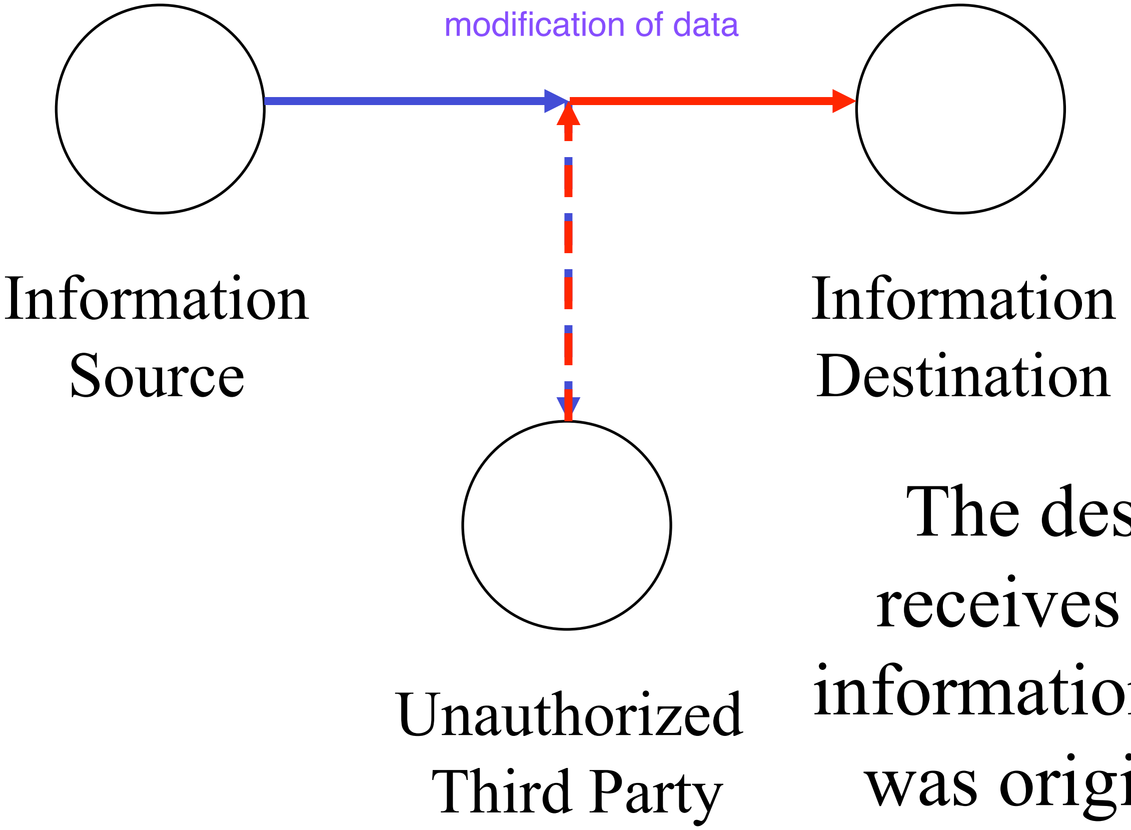
- Break-ins

break into a channel that you are not allowed in

- Illicit data copying

keeping data copy when you are not suppose to

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

physically changing the data request on the wire

- Masquerading
- Break-ins

both are similar to before

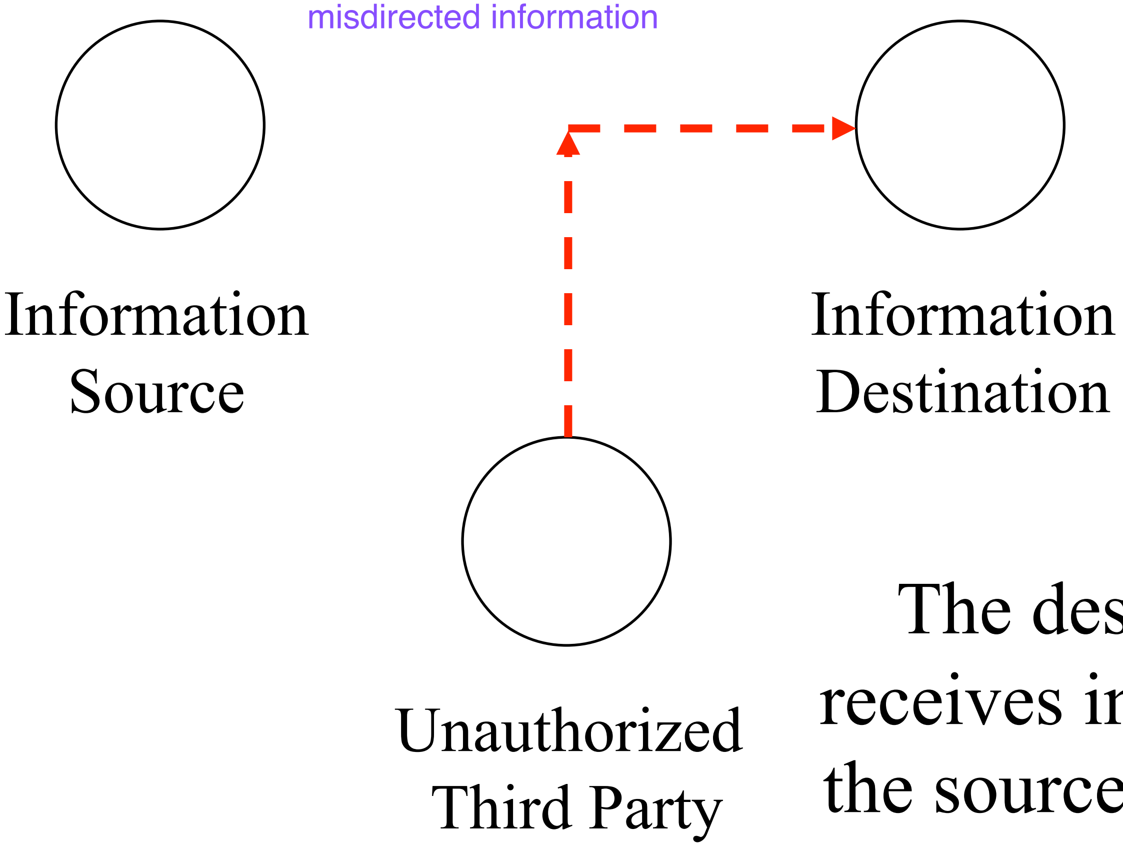
- Flaws in applications allowing unintended modifications

common vulnerabilities

- Other forms of illicit access to servers and their services

Fabrication

pretending information came from the source
improper behavior
misdirected information



The destination receives information the source never sent

Fabrication Threats

IP spoofing - faking your own IP address

- 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

threat to availability as well

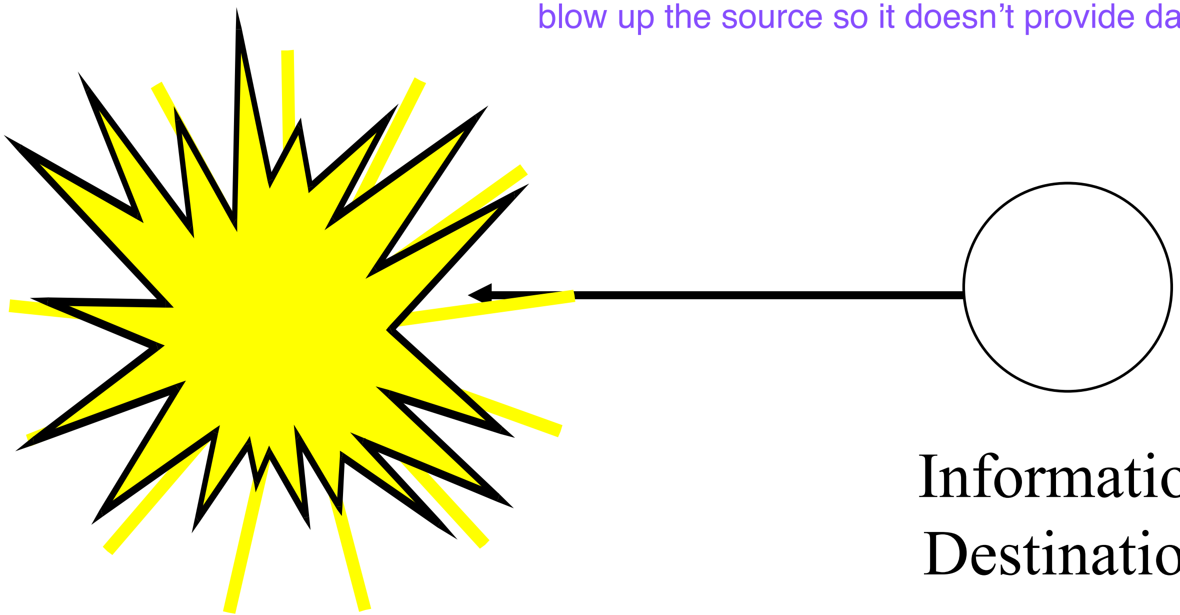
How Do Fabrication Threats Occur?

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

kept a good request, then used it again for bad request

Destruction Threats

blow up the source so it doesn't provide data to anybody



The information is no longer accessible to a legitimate user

Destruction Threats

- Destroy data, hardware, software, etc.
- Often easier to destroy something than usefully modify it
- Often (not always) requires physical access
  - As counterexample, consider demo of destroying power generator[1]
  - Stuxnet destroyed centrifuges
- Destruction threats primarily threaten availability

computer connected to power generator

[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
  more clandestine
  - 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 is very common today

Social Engineering Example

- Phishing suppose to visit a website to write password
- 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?

it is so prevalent….

- Anti-Phishing Work Group reported 65,000 unique phishing sites in December 2015[1]
  - 80,000 unique phishing attacks reported
  - Targeting 406 different brands
- 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 <u>everything</u> right
  - Any mistake is an opportunity for your opponent
- When was the last time you saw a computer system that did <u>everything</u> right?
- So, must we wait for bug-free software to achieve security?

How Common Are Software Security Flaws?

- SANS used to publish weekly compendium of newly discovered security flaws
- About 1500 security flaws found per year
  - Only counting popular software
  - Only flaws with real security implications
  - And only those that were publicized
- SANS stopped doing this because it's not reasonable to expect anyone to keep up

this was not a resonable way to finish up the patching

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

< — additional components of computer security if computer security is good

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.*

ex. enemy doesn't assck the front door, they smash the windows

- Put another way,

attackers ONLY attack you on weak points; they will only look into weakest spot

  - The smart opponent attacks you where you're weak, not where you're strong
  - And most opponents aren't stupid

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

work against another human opponent