What Are Our Security Goals?

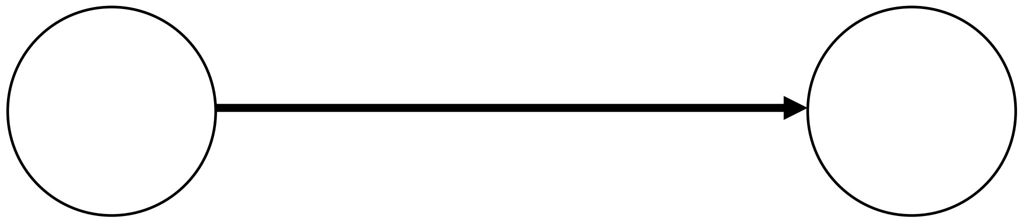
- CIA
- **C**onfidentiality
  - If it's supposed to be a secret, be careful who hears it
- **I**ntegrity
  - Don't let someone change something they shouldn't
- **A**vailability
  - Don't let someone stop others from using services

What Are the Threats?

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

Thinking About Threats

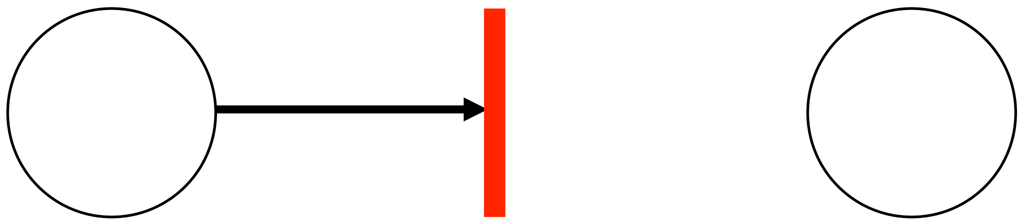
- Threats are viewed as types of attacks on normal services
- So, what is normal service?



Information Source

Information Destination

Interruption



Information Source

Information Destination

The information never reaches the destination

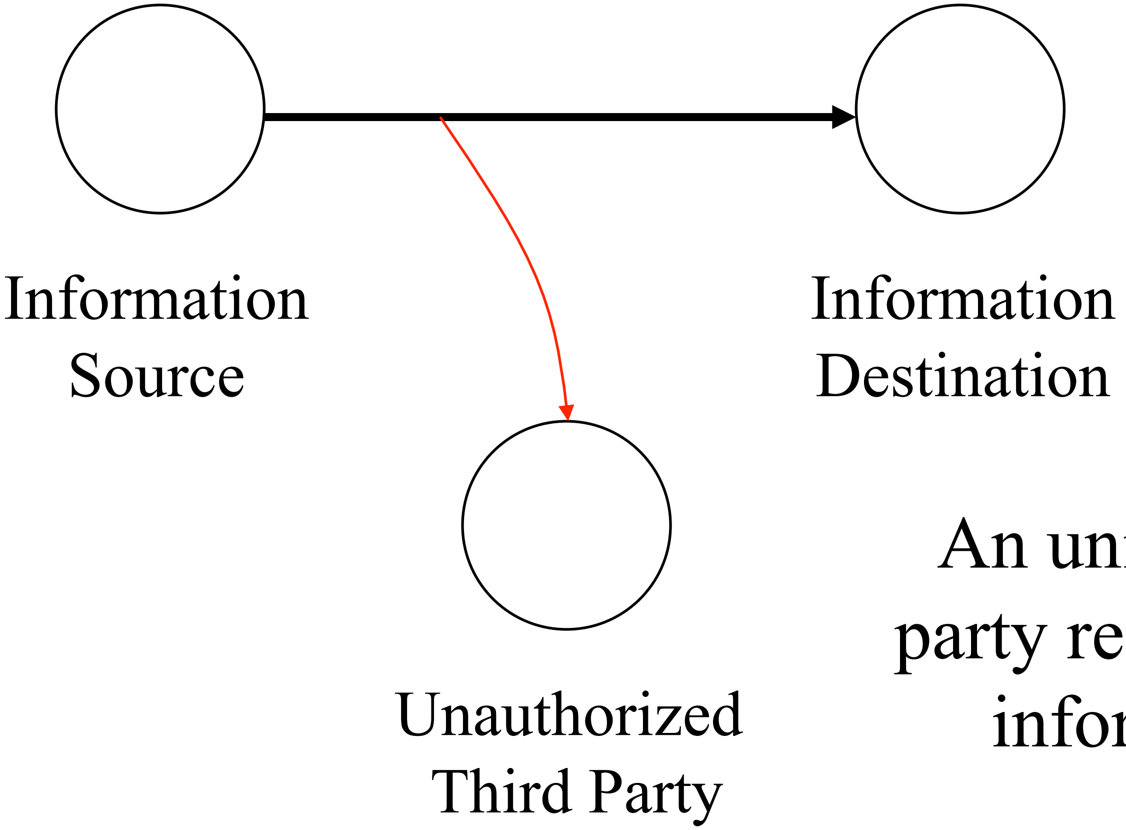
Interruption Threats

- 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

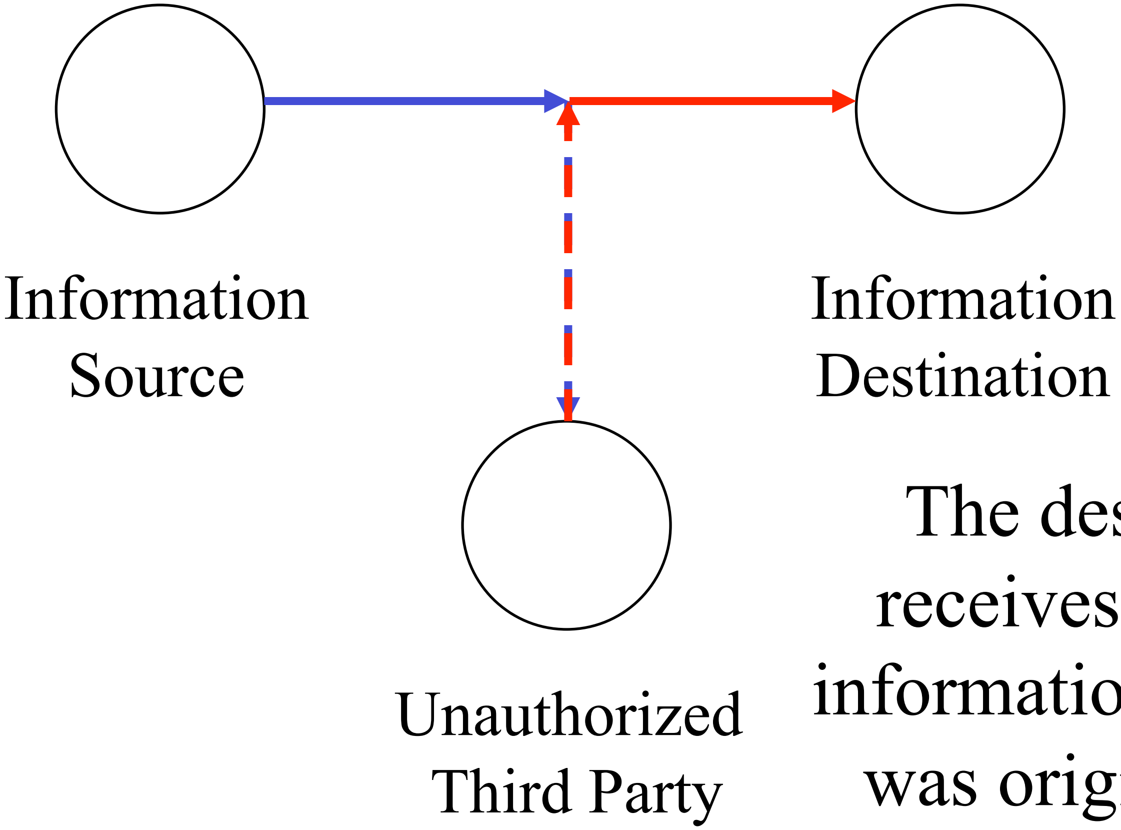
Interception Threats

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

How Do Interception Threats Occur?

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

Modification



Information Source

Information Destination

Unauthorized Third Party

The destination receives different information than what was originally sent

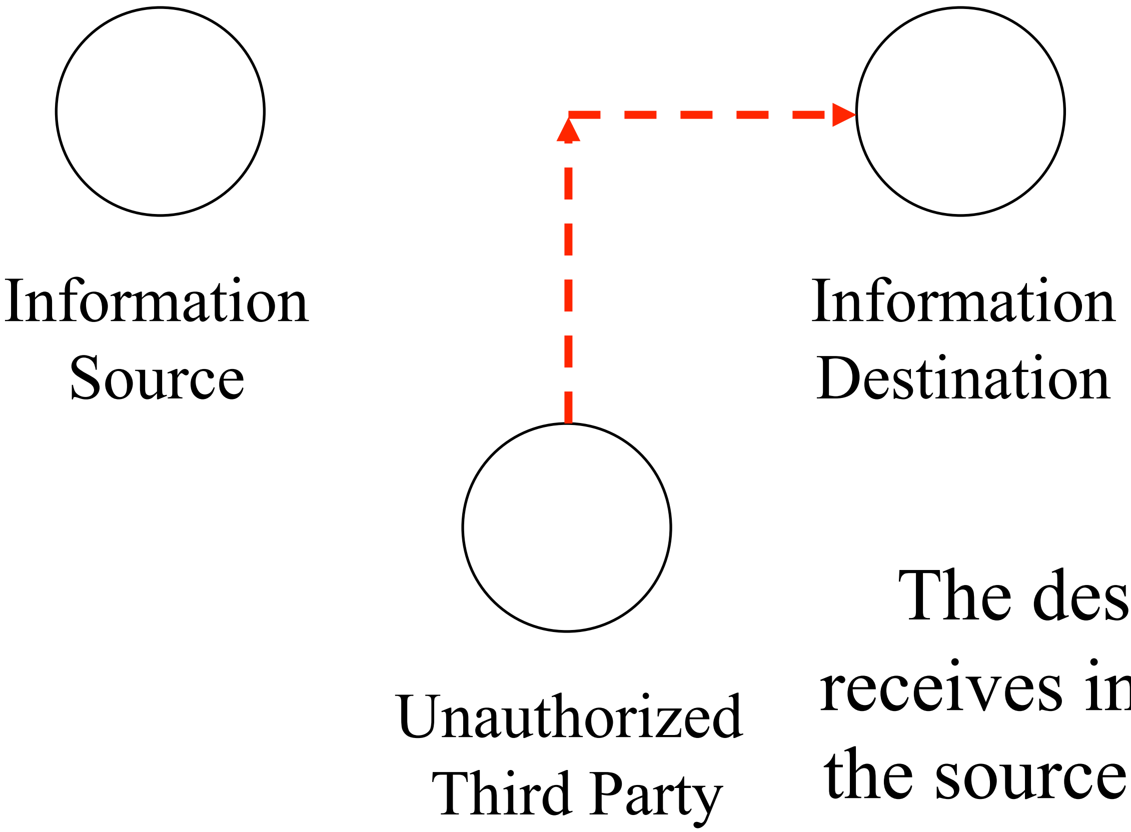
Modification Threats

- 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

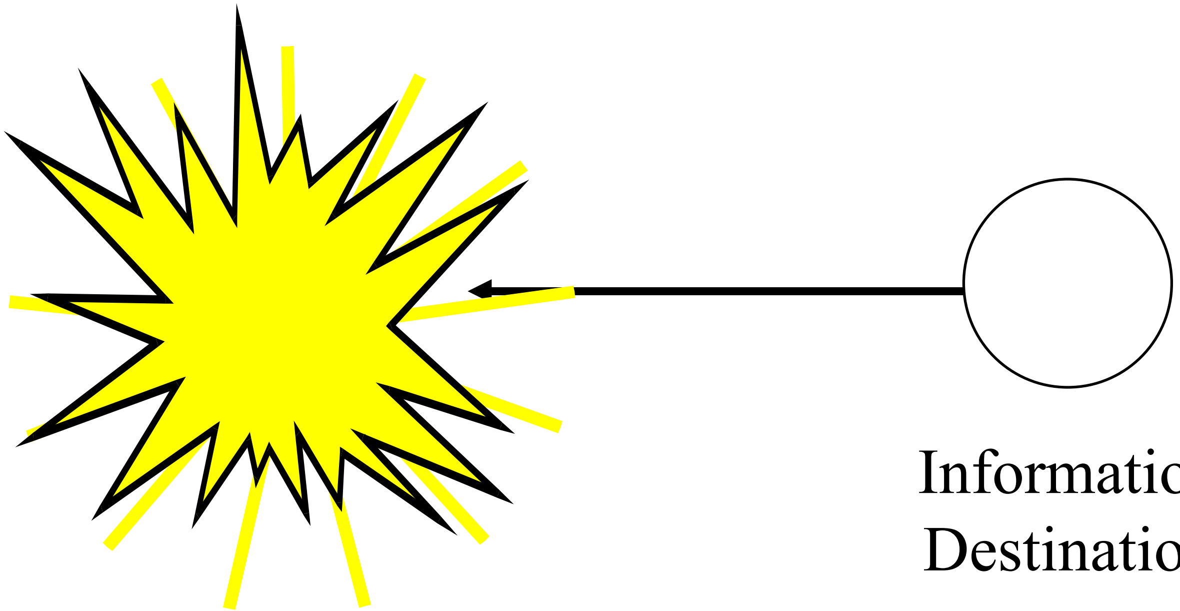
Fabrication Threats

- 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

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
  - 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 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 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 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

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