Threats and Attacks

CSE 4471: Information Security.

Terminology (1)

- ***Vulnerability:*** Weakness or fault that can lead to an exposure
- ***Threat:*** Generic term for objects, people who pose potential danger to assets (via attacks)
- ***Threat agent:*** Specific object, person who poses such a danger (by carrying out an attack)
  - DDoS attacks are a **threat**
  - If a hacker carries out a DDoS attack, he's a **threat agent**
- **Risk*:*** Probability that "something bad" happens times expected damage to the organization
  - Unlike vulnerabilities/exploits; *e.g.*, a web service running on a server may have a vulnerability, but if it's not connected to the network, risk is 0.0
- **Exposure:** a successful attack
- **Vector:** how the attack was carried out, *e.g.*, malicious email attachment

Terminology (2)

- ***Malware:*** malicious code such as viruses, worms, Trojan horses, bots, backdoors, spyware, adware, etc.
- ***Disclosure:*** responsible, full, partial, none, delayed, etc.
- ***Authentication:*** determining the identity of a person, computer, or service on a computer
- ***Authorization:*** determining whether an entity (person, program, computer) has access to object
  - Can be *implicit* (email account access) or *explicit* (attributes specifying users/groups who can read/write/execute file)
- ***Incident:*** definitions vary
  - Any attack, all attacks using vulnerability X, etc.
  - Anything resulting in service degradation other than problem mgmt., service request fulfillment

Threats (1)

- Threat: an object, person, or other entity that represents a constant danger to an asset

- Management must be informed of the different threats facing the organization

- By examining each threat category, management effectively protects information through policy, education, training, and technology controls

Threats (2)

- 2004 Computer Security Institute (CSI) / Federal Bureau of Investigation (FBI) survey found:
  - 79% of organizations reported cyber security breaches within the last 12 months
  - 54% of those orgs. reported financial losses over $141 million
- Take the survey with a grain of salt
  - Underreporting, fear of bad publicity
  - Cybercrime: easy $$ at *perceived* low risk to attacker

Table 2.1: Threats to Info. Security

Threat Category	**Examples**
Acts of human error or failure	***Accidents, employee mistakes***
Intellectual property compromise	Piracy, copyright infringement
Deliberate espionage or trespass	Unauthorized access, data collection
Deliberate information extortion	Blackmail of info. disclosure
Deliberate sabotage or vandalism	Destruction of systems or info.
Deliberate theft	Illegally taking equipment or info.
Deliberate software attacks	***Viruses, worms, denial of service***
Forces of nature	Fires, floods, earthquakes
Deviations in service from providers	Power and Internet provider issues
Technological hardware failures	Equipment failure
Technological software failures	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

Acts of Human Error or Failure (1)

- Includes actions without malicious intent
- Causes include:
  - Inexperience
  - Improper training
  - Incorrect assumptions
- Employees: among the greatest threats to organization’s data

Acts of Human Error or Failure (2)

- Employee mistakes can easily lead to:
  - Revelation of classified data
  - Entry of erroneous data
  - Accidental data deletion or modification
  - Data storage in unprotected areas
  - Failure to protect information
- Many of these threats can be prevented with controls
- Then there's the ***insider threat***…

Questions

- Who poses the biggest threat to your company?
  - “Script kiddie” software hacker?
  - Convicted burglar in area?
  - Employee who accidentally deletes sole copy of project source code?
- How can we guard against these threats?

Deliberate Acts of Espionage/Trespass

- Unauthorized people access protected information
- Competitive intelligence (legal) vs. industrial espionage (illegal)
- ***Shoulder surfing occurs anywhere a person accesses confidential information***
- Controls let trespassers know they are encroaching on organization's cyberspace
- Hackers uses skill, guile, or fraud to bypass controls protecting others' information
- European Network and Info. Sec. Agency video

Deliberate Acts of Theft

- Illegal taking of another’s physical, electronic, or intellectual property
- Physical theft can be easily controlled
- Electronic theft is more complex: evidence of crime not obvious

Source: Pixabay/OpenClipArt

Deliberate Software Attacks

- Malicious software (malware) damages, destroys, or denies service to target systems
- Includes:
  - ***Viruses:*** Malware propagating with human help
  - ***Worms:*** Self-propagating malware over networks
  - ***Trojan horses:*** Malware claiming benign purpose
  - ***Logic bombs:*** Malicious code placed in software, triggered by attacker
  - ***Backdoors:*** Hidden bypass of system authentication
  - ***Denial-of-service (DoS) attacks:*** Attackers' traffic floods take down Internet services (one type)

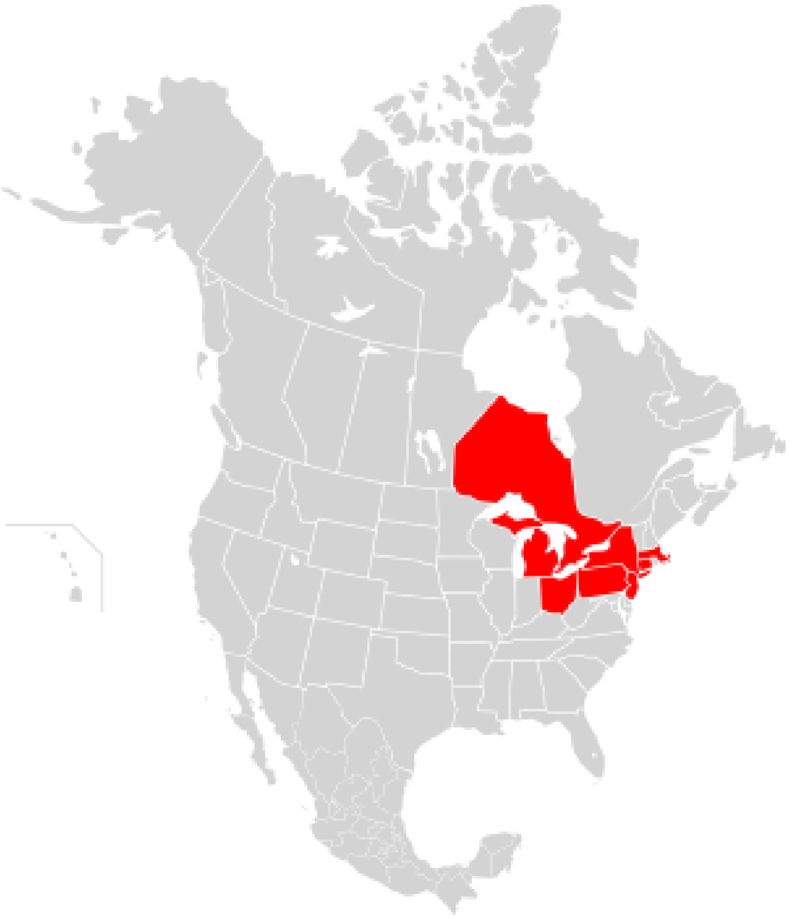
Forces of Nature

- Forces of nature: among most dangerous threats
- Disrupt individual lives plus information storage, transfer, use
- Organizations must implement controls to limit damage, prepare for worst-case scenarios

Sources: U.S. Dept. of Agriculture, NASA

Deviations in Quality of Service

- Situations where products, services not delivered as expected
- Info. system depends on many support systems
- Internet service, communications, and power outages affect systems availability



U.S. states and provinces affected (2003 Northeast blackout)
Source: Wikipedia

Internet Service Issues

- Internet service provider (ISP) failures can undermine information availability …

- Company’s outsourced Web hosting provider responsible for all company Internet services plus hardware, OS, and software

Attacks (1)

- Act or action that exploits vulnerability (i.e., an identified weakness) in controlled system
- Accomplished by threat agent which damages or steals organization’s information

Attacks (2)

- Malicious code: launching viruses, worms, Trojan horses, and active Web scripts aiming to steal or destroy info.
- Backdoor: accessing system or network using known or previously unknown mechanism
- Password crack: attempting to reverse calculate a password
- Brute force: trying every possible combination of options of a password
- Dictionary: selects specific accounts to attack and uses commonly used passwords (i.e., the dictionary) to guide guesses

Attacks (3)

- Denial-of-service (DoS): attacker sends large number of connection or information requests to a target
  - Target system cannot handle successfully along with other, legitimate service requests
  - May result in system crash or inability to perform ordinary functions
- Distributed denial-of-service (DDoS): coordinated stream of requests is launched against target from many locations simultaneously

Attacks (4)

- Spoofing: technique used to gain unauthorized access; intruder assumes a trusted IP address
- Man-in-the-middle: attacker monitors network packets, modifies them, and inserts them back into network
- Spam: unsolicited commercial e-mail; more a nuisance than an attack, though is emerging as a vector for some attacks

Attacks (5)

- Mail bombing: also a DoS; attacker routes large quantities of e-mail to target
- Sniffers: program or device that monitors data traveling over network; can be used both for legitimate purposes and for stealing information from a network
- Social engineering: using social skills to convince people to reveal access credentials or other valuable information to attacker

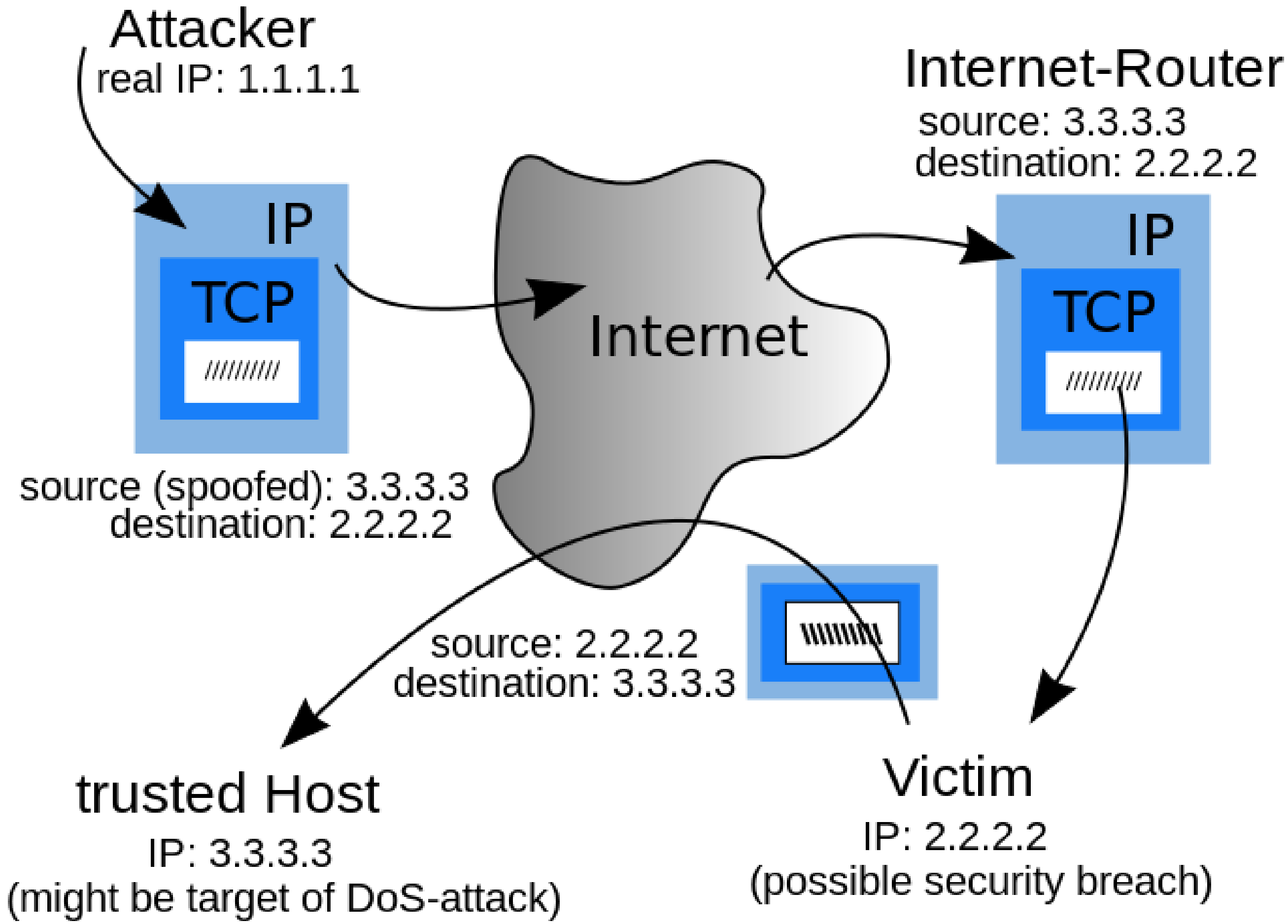
Attacks (6)

- Buffer overflow: application error where more data sent to a buffer than can be handled
- Timing attack: explores contents of a Web browser’s cache to create malicious cookie
- Side-channel attacks: secretly observes computer screen contents/electromagnetic radiation, keystroke sounds, etc.

Table 2.2: Attack Replication Vectors

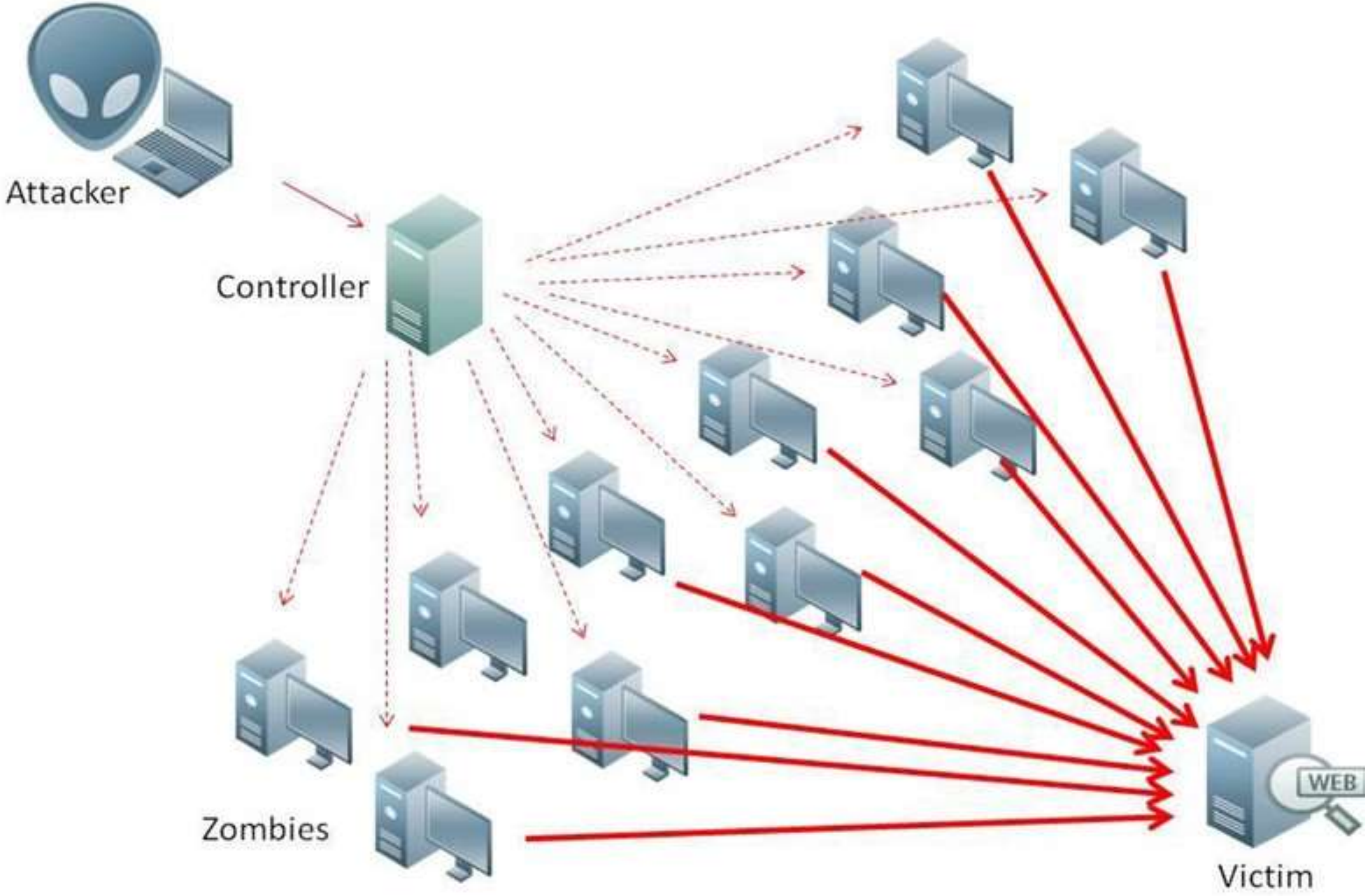
Attack Vector	Description
IP Scan and Attack	Malware-infected system scans for target IP addresses, then probes for vulnerable system components (e.g., Conficker).
Web Browsing	Malware-infected systems with webpage write privileges infects Web content (e.g., HTML files).
Viruses	Malware-infected system infects other systems to which it has access via executable scripts (human activity required).
Unprotected Shares	Malware-infected system uses file system vulnerabilities to spread malware to all writable locations.
Mass Email	Malware-infected system spams all contacts found in users' address books.
Simple Network Management Protocol (SNMP)	Malware-infected systems use SNMP to guess common or weak passwords on other network-connected systems, then spread. (Vendors have fixed many of these bugs.)

IP Spoofing Attack



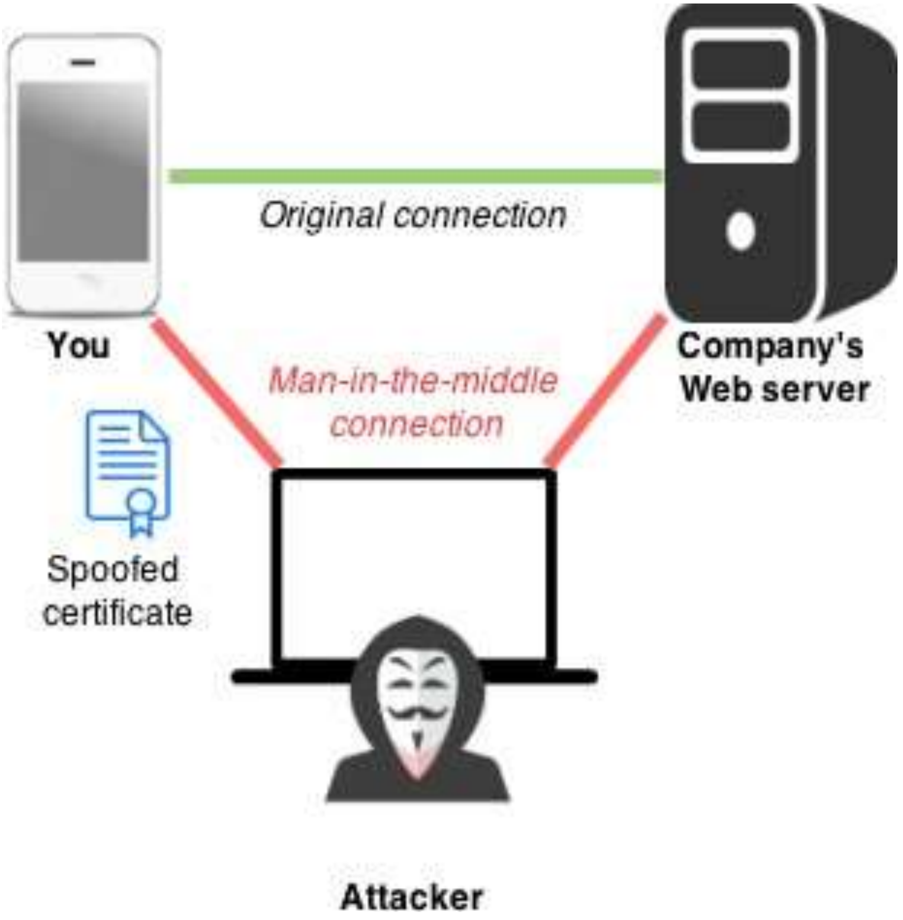
Source: Wikipedia

Denial-of-Service Attack



Source: Wikipedia

Man-in-the-Middle Attack



Source: Neil Smithline, Stack Overflow, https://security.stackexchange.com/questions/183723/i-started-to-learn-about-mitm-attacks-and-i-cant-figure-out-few-things

Summary

- Threat: object, person, or other entity representing constant danger to an asset

- Attack: deliberate action exploiting a vulnerability