Threats and Attacks

Modifications by Prof. Dong Xuan
and Adam C. Champion

Learning Objectives

Upon completion of this material, you should be able to:

- Identify and understand the threats posed to information security
- Identify and understand the more common attacks associated with those threats

Terminology (1)

- ***Vulnerability:*** Weakness or fault that can lead to an exposure
- ***Threat:*** Generic term for objects, people who pose a potential danger to an asset (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

- 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 (continued)

- The 2004 Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI) survey found:
  - 79 percent of organizations reported cyber security breaches within the last 12 months
  - 54 percent of those organizations reported financial losses totaling 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 Information Security[4]

Categories of threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Forces of nature	Fire, flood, earthquake, lightning
9. Deviations in quality of service from service providers	Power and WAN service issues
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies

Acts of Human Error or Failure (1)

- Includes acts performed without malicious intent
- Causes include:
  - Inexperience
  - Improper training
  - Incorrect assumptions
- Employees are among the greatest threats to an 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***...

FIGURE 2-1 Acts of Human Error or Failure

Deliberate Acts of Espionage or Trespass

- Access of protected information by unauthorized individuals
- 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

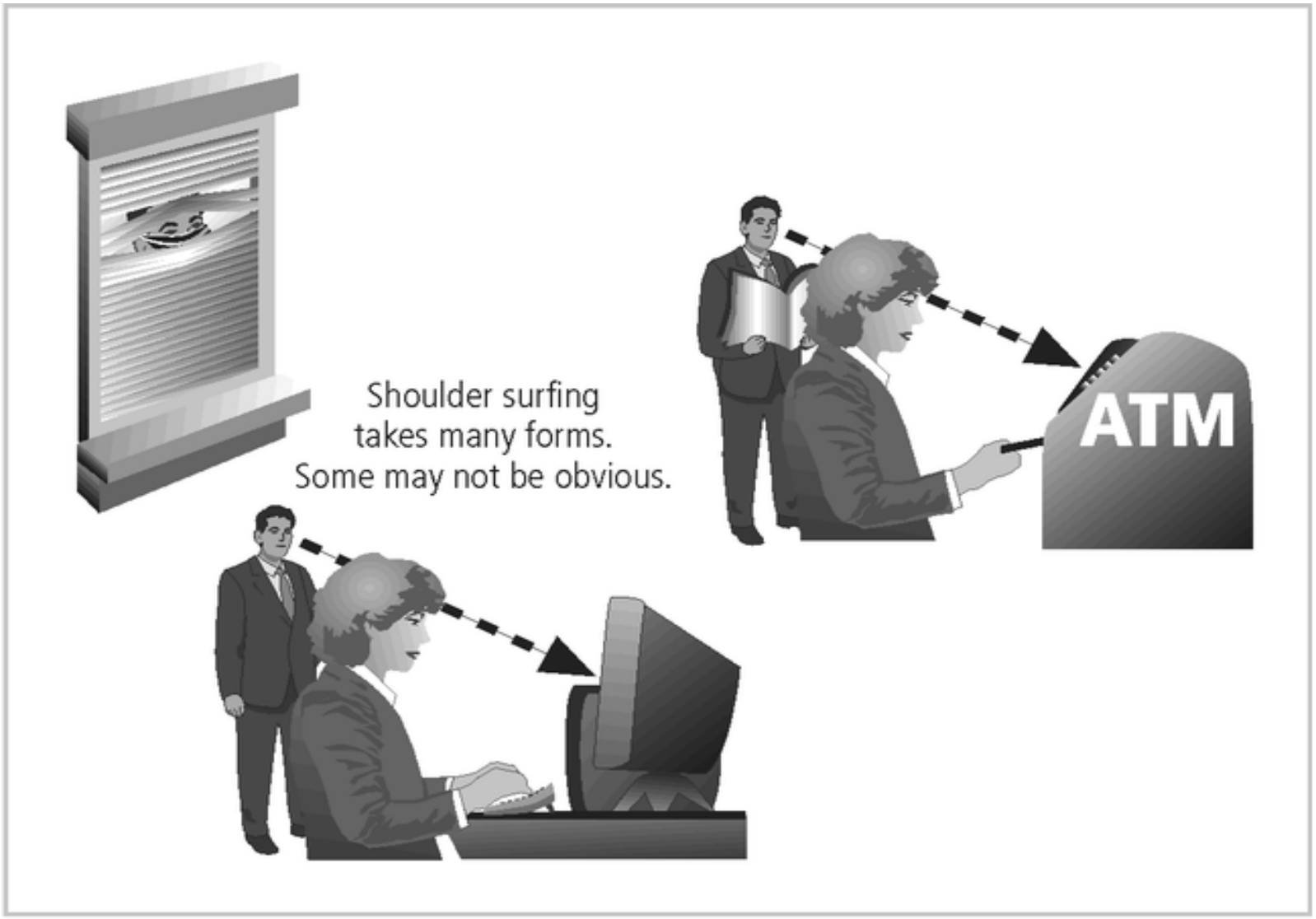

FIGURE 2-2 Shoulder Surfing

Deliberate Acts of Theft

- Illegal taking of another's physical, electronic, or intellectual property
- Physical theft is controlled relatively easily
- Electronic theft is more complex problem; evidence of crime not readily apparent

Deliberate Software Attacks

- Malicious software (malware) designed to damage, destroy, or deny service to target systems
- Includes viruses, worms, Trojan horses, logic bombs, back doors, and denial-of-service attacks

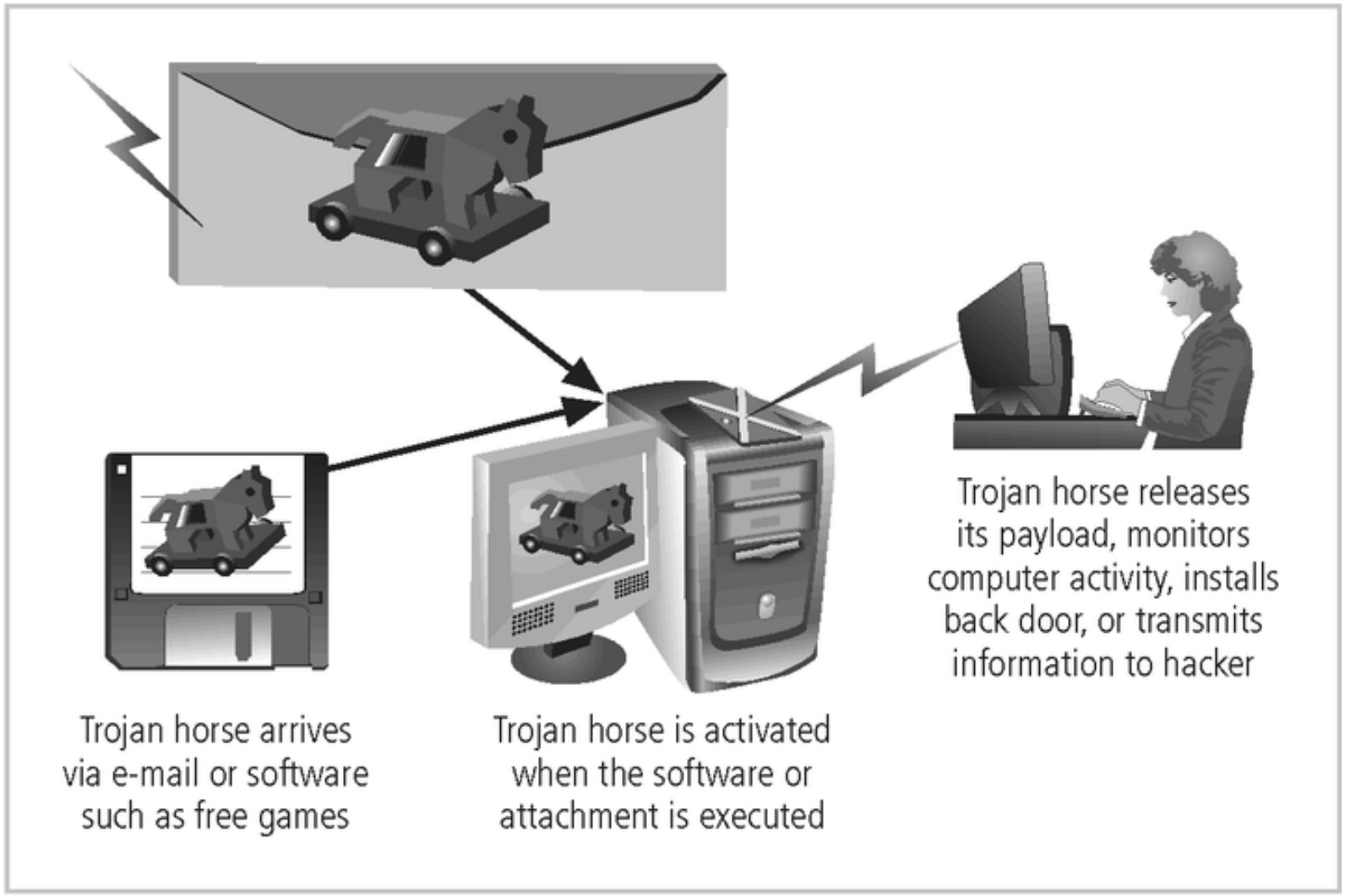

FIGURE 2-8 Trojan Horse Attack

Forces of Nature

- Forces of nature are among the most dangerous threats
- Disrupt not only individual lives, but also storage, transmission, and use of information
- Organizations must implement controls to limit damage and prepare contingency plans for continued operations

Deviations in Quality of Service

- Includes situations where products or services not delivered as expected
- Information system depends on many interdependent support systems
- Internet service, communications, and power irregularities dramatically affect availability of information and systems

Internet Service Issues

- Internet service provider (ISP) failures can considerably undermine availability of information
- Outsourced Web hosting provider assumes responsibility for all Internet services as well as hardware and Web site operating system software

Attacks

- 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

Table 2-2 Attack Replication Vectors

Vector	Description
IP scan and attack	The infected system scans a random or local range of IP addresses and targets any of several vulnerabilities known to hackers or left over from previous exploits such as Code Red, Back Orifice, or PoizonBox.
Web browsing	If the infected system has write access to any Web pages, it makes all Web content files (.html, .asp, .cgi, and others) infectious, so that users who browse to those pages become infected.
Virus	Each infected machine infects certain common executable or script files on all computers to which it can write with virus code that can cause infection.
Unprotected shares	Using vulnerabilities in file systems and the way many organizations configure them, the infected machine copies the viral component to all locations it can reach.
Mass mail	By sending e-mail infections to addresses found in the address book, the infected machine infects many users, whose mail-reading programs also automatically run the program and infect other systems.
Simple Network Management Protocol (SNMP)	By using the widely known and common passwords that were employed in early versions of this protocol (which is used for remote management of network and computer devices), the attacking program can gain control of the device. Most vendors have closed these vulnerabilities with software upgrades.

Attacks (continued)

- Malicious code: includes execution of viruses, worms, Trojan horses, and active Web scripts with intent to destroy or steal information
- Backdoor: gaining access to system or network using known or previously unknown/newly discovered access mechanism

Attacks (continued)

- 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 (continued)

- 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

In a denial-of-service attack, a hacker compromises a system and uses that system to attack the target computer, flooding it with more requests for services than the target can handle.

In a distributed denial-of-service attack, dozens or even hundreds of computers (known as zombies) are compromised, loaded with DoS attack software and then remotely activated by the hacker to conduct a coordinated attack.

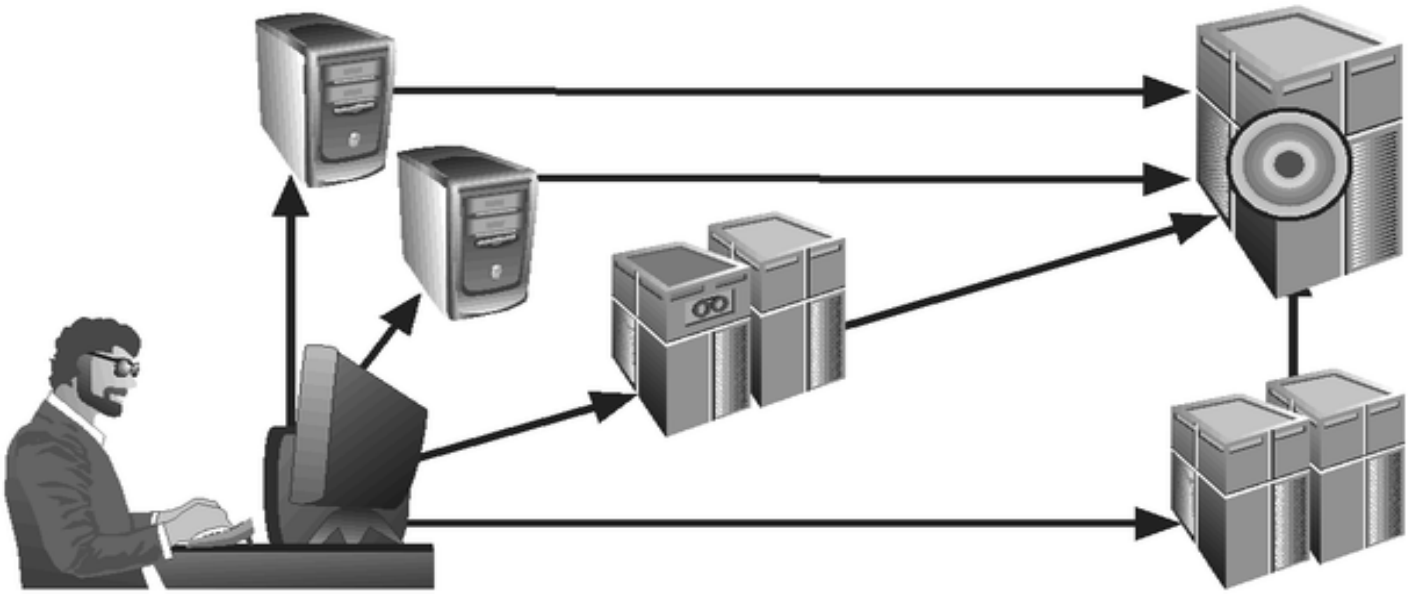

FIGURE 2-9 Denial-of-Service Attacks

Attacks (continued)

- 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

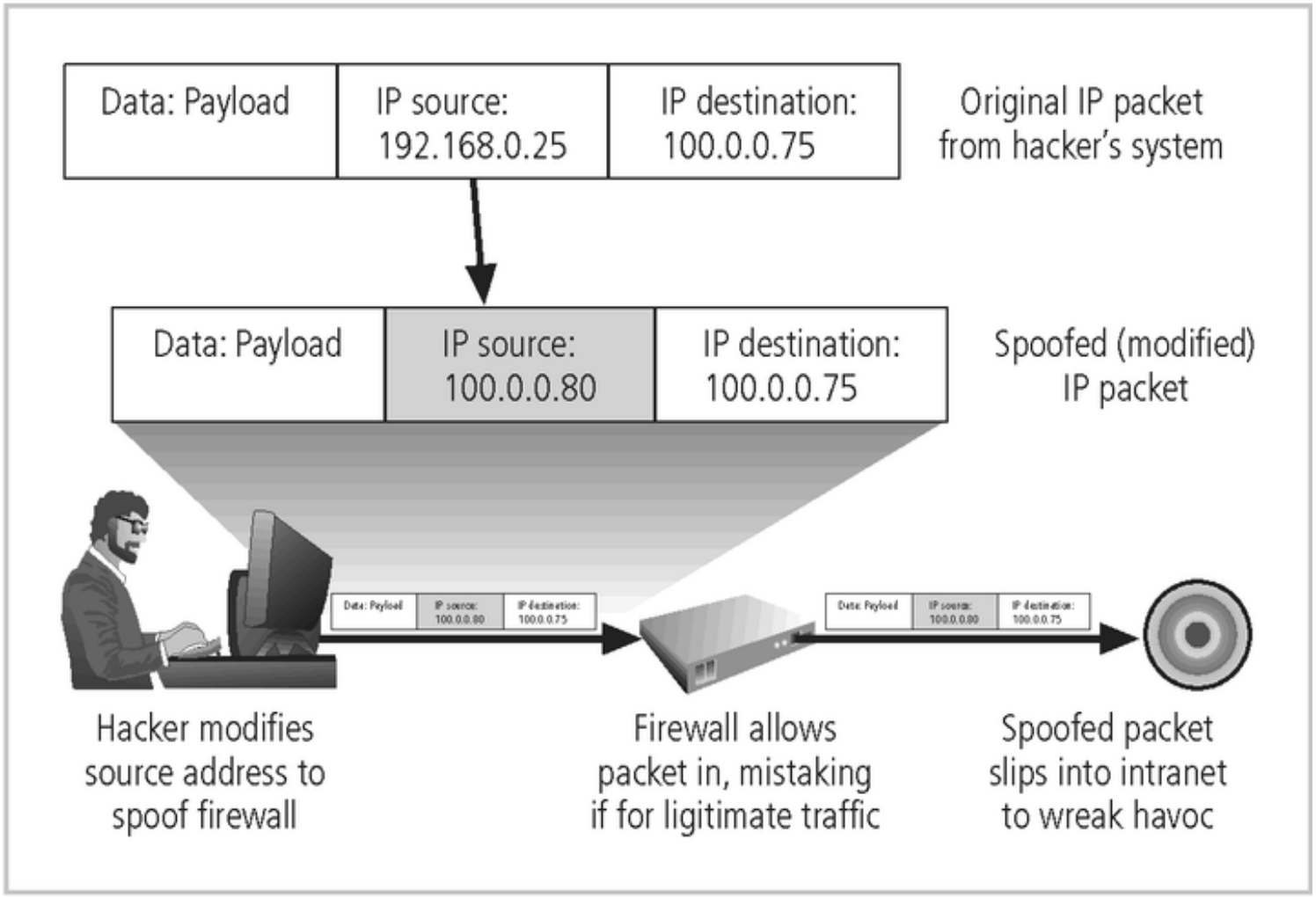

FIGURE 2-10 IP Spoofing

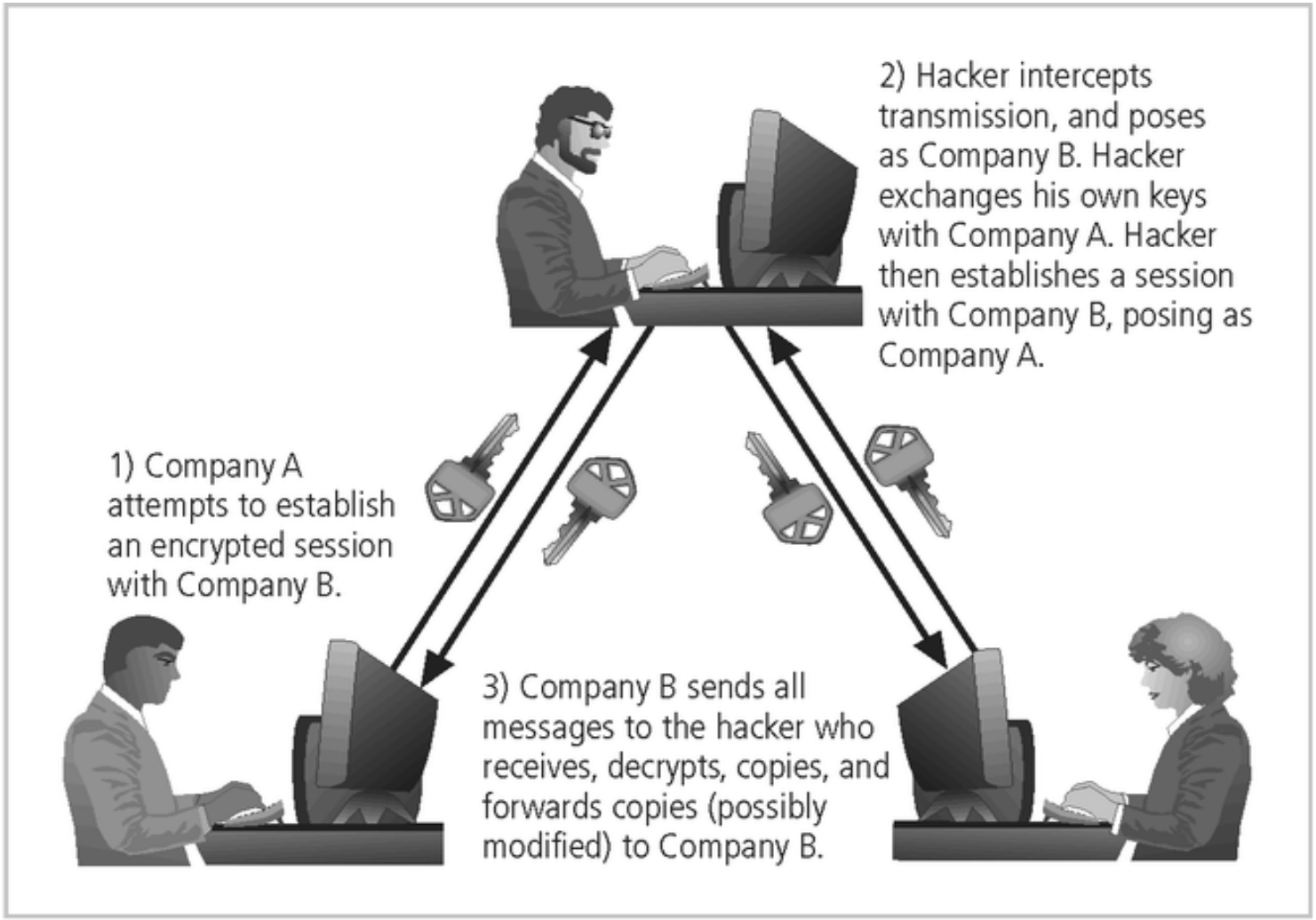

FIGURE 2-11 Man-in-the-Middle Attack

Attacks (continued)

- 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 (continued)

- Buffer overflow: application error occurring when more data is 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.

Summary

- Threat: object, person, or other entity representing a constant danger to an asset
- Attack: a deliberate act that exploits vulnerability