Information Security

Lecture 5

The Need for Security

Dr. Tehsin Kanwal
Assistant Professor

Introduction

- Primary mission of information security is to ensure systems and contents stay the same
- If no threats existed, resources could be focused on improving systems, resulting in vast improvements in ease of use and usefulness
- Attacks on information systems are a daily occurrence

Safeguarding Technology Assets in Organizations

- Organizations must have secure infrastructure services based on size and scope of enterprise
- Additional security services may be needed as organization grows
- More robust solutions may be needed to replace security programs the organization has outgrown

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
- Overall security is improving
- The 2009 CSI/FBI survey found
  - 64 percent of organizations had malware infections
  - 14 percent indicated system penetration by an outsider

	Category of Threat	Examples
1.	Compromises to intellectual property	Piracy, copyright infringement
2.	Software attacks	Viruses, worms, macros, denial of service
3.	Deviations in quality of service	ISP, power, or WAN service issues from service providers
4.	Espionage or trespass	Unauthorized access and/or data collection
5.	Forces of nature	Fire, flood, earthquake, lightning
6.	Human error or failure	Accidents, employee mistakes
7.	Information extortion	Blackmail, information disclosure
8.	Missing, inadequate, or incomplete	Loss of access to information systems due to disk in place drive failure without proper backup and recovery plan organizational policy or planning
9.	Missing, inadequate, or incomplete controls	Network compromised because no firewall security controls
10.	Sabotage or vandalism	Destruction of systems or information
11.	Theft	Illegal confiscation of equipment or information
12.	Technical hardware failures or errors	Equipment failure
13.	Technical software failures or errors	Bugs, code problems, unknown loopholes
14.	Technological obsolescence	Antiquated or outdated technologies

Software attacks- Malware, software attacks will be discussed in detail in next lecture.

Table 2-1 Threats to Information Security[4]

Compromises to Intellectual Property

- Intellectual property (IP): “ownership of ideas and control over the tangible or virtual representation of those ideas”
- The most common IP breaches involve software piracy
- Two watchdog organizations investigate software abuse:
  - Software & Information Industry Association (SIIA)
  - Business Software Alliance (BSA)
- Enforcement of copyright law has been attempted with technical security mechanisms

Deliberate Software Attacks

- Malicious software (malware) designed to damage, destroy, or deny service to target systems
- Includes:
  - Viruses
  - Worms
  - Trojan horses
  - Logic bombs
  - Back door or trap door
  - Polymorphic threats
  - Virus and worm hoaxes

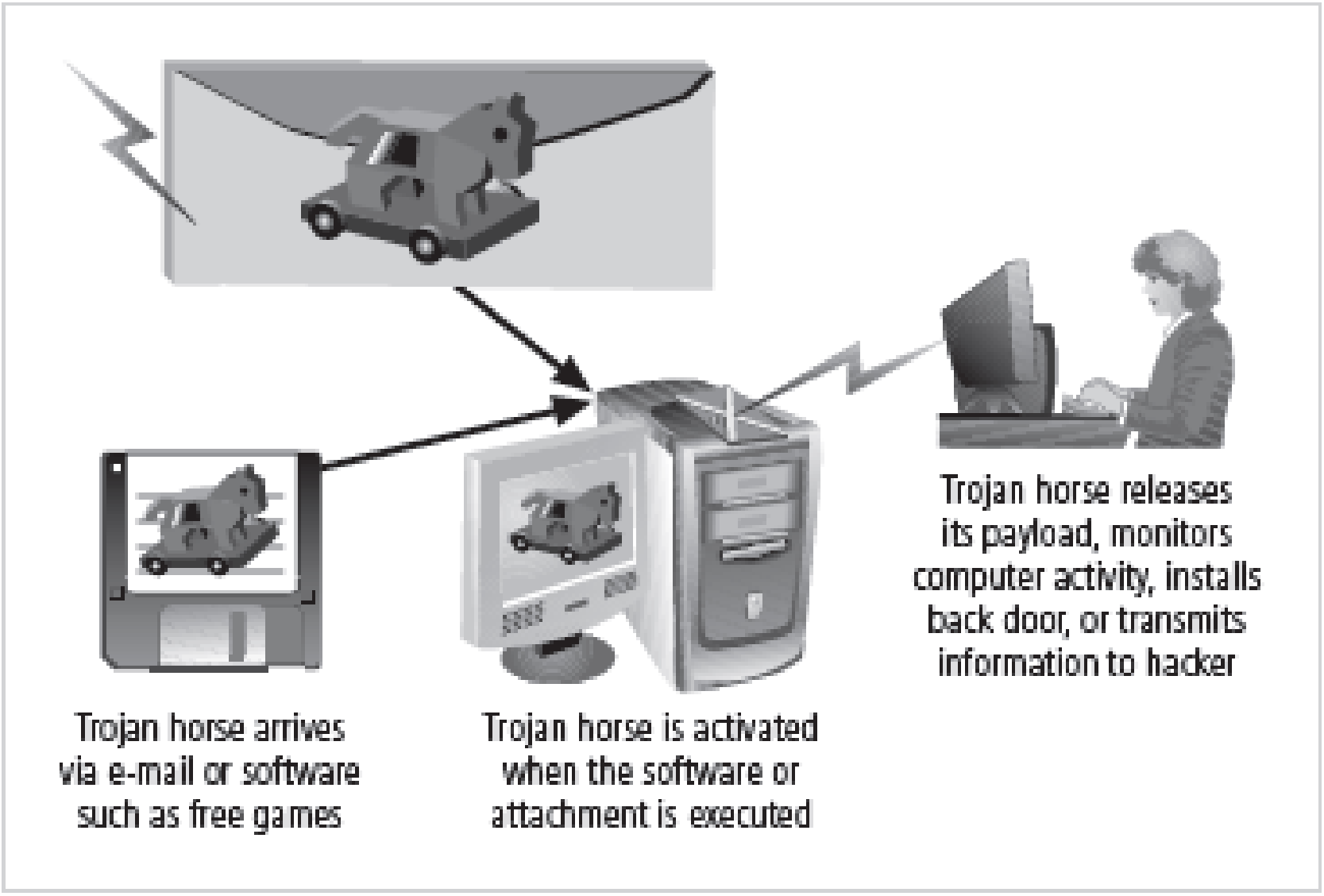

Figure 2-4 Trojan Horse Attack

Deviations in Quality of Service

- Includes situations where products or services are 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

Deviations in Quality of Service (cont'd.)

- 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
- Communications and other service provider issues
  - Other utility services affect organizations: telephone, water, wastewater, trash pickup, etc.
  - Loss of these services can affect organization's ability to function

Deviations in Quality of Service (cont'd.)

- Power irregularities
  - Commonplace
  - Organizations with inadequately conditioned power are susceptible
  - Controls can be applied to manage power quality
  - Fluctuations (short or prolonged)
    - Excesses (spikes or surges) – voltage increase
    - Shortages (sags or brownouts) – low voltage
    - Losses (faults or blackouts) – loss of power

Espionage or Trespass

- Access of protected information by unauthorized individuals
- Competitive intelligence (legal) vs. industrial espionage (illegal)
- Shoulder surfing can occur anywhere a person accesses confidential information
- Controls let trespassers know they are encroaching on organization's cyberspace
- Hackers use skill, guile, or fraud to bypass controls protecting others' information

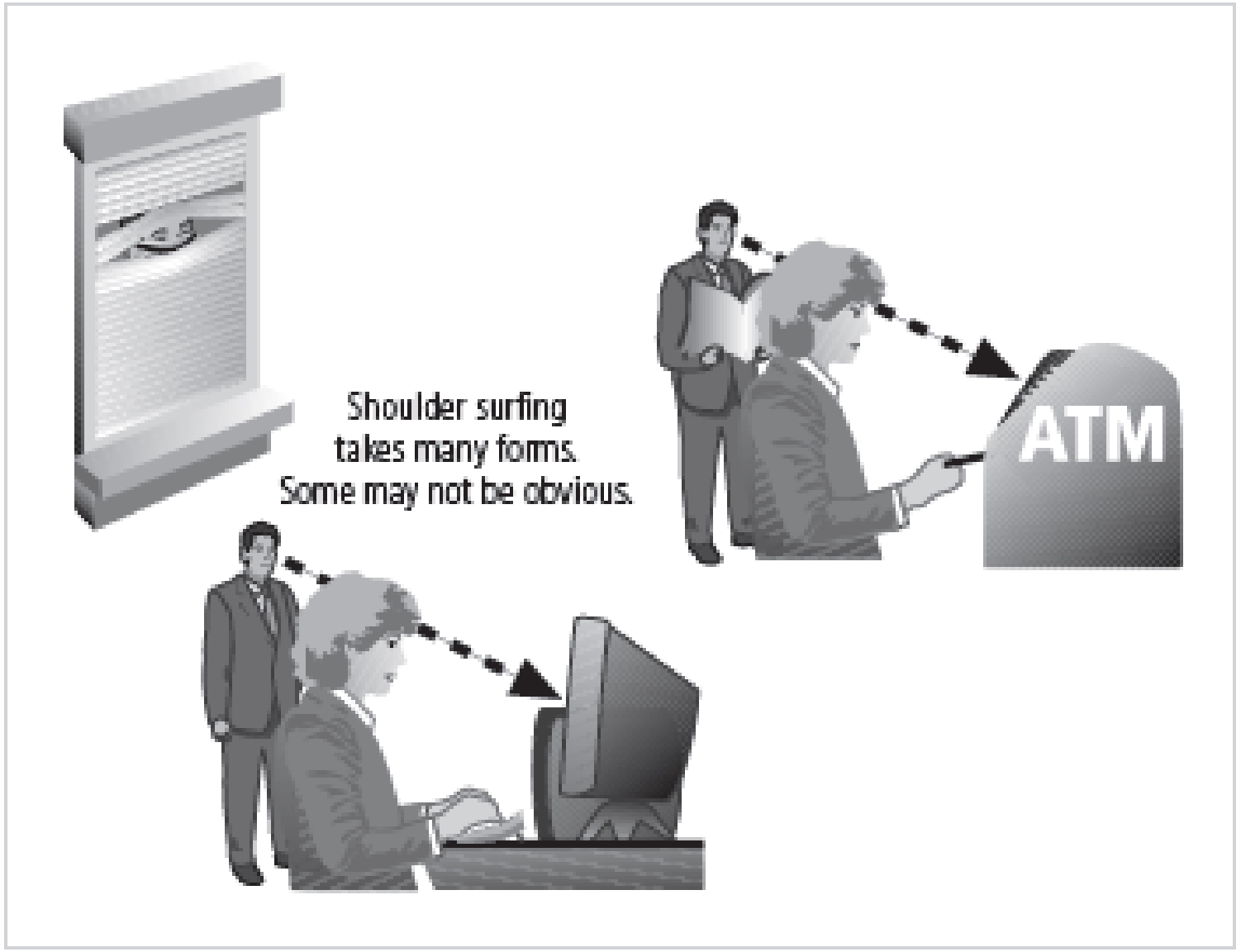

Figure 2-5 Shoulder Surfing

Traditional hacker profile:
Age 13-18, male with limited parental supervision; spends all his free time at the computer

Modern hacker profile:
Age 12-60, male or female, unknown background, with varying technological skill levels; may be internal or external to the organization

Figure 2-6 Hacker Profiles

Espionage or Trespass (cont'd.)

- Expert hacker
  - Develops software scripts and program exploits
  - Usually a master of many skills
  - Will often create attack software and share with others
- Unskilled hacker
  - Many more unskilled hackers than expert hackers
  - Use expertly written software to exploit a system
  - Do not usually fully understand the systems they hack

Espionage or Trespass (cont'd.)

- Other terms for system rule breakers:
  - Cracker: "cracks" or removes software protection designed to prevent unauthorized duplication
  - Phreaker: hacks the public telephone network

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

Human Error or Failure

- Includes acts performed without malicious intent
- Causes include:
  - Inexperience
  - Improper training
  - Incorrect assumptions
- Employees are among the greatest threats to an organization's data

Human Error or Failure (cont'd.)

- 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

Figure 2-8 Acts of Human Error or Failure

Information Extortion

- Attacker steals information from computer system and demands compensation for its return or nondisclosure
- Commonly done in credit card number theft

Missing, Inadequate, or Incomplete

- In policy or planning, can make organizations vulnerable to loss, damage, or disclosure of information assets
- With controls, can make an organization more likely to suffer losses when other threats lead to attacks

Sabotage or Vandalism

- Threats can range from petty vandalism to organized sabotage
- Web site defacing can erode consumer confidence, dropping sales and organization's net worth
- Threat of hacktivist or cyberactivist operations rising
- Cyberterrorism: much more sinister form of hacking

Figure 2-9 Cyber Activists Wanted

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

Technical Hardware Failures or Errors

- Occur when manufacturer distributes equipment containing flaws to users
- Can cause system to perform outside of expected parameters, resulting in unreliable or poor service
- Some errors are terminal; some are intermittent

Technical Software Failures or Errors

- Purchased software that contains unrevealed faults
- Combinations of certain software and hardware can reveal new software bugs
- Entire Web sites dedicated to documenting bugs

Technological Obsolescence

- Antiquated/outdated infrastructure can lead to unreliable, untrustworthy systems
- Proper managerial planning should prevent technology obsolescence
- IT plays large role

Attacks

- Attacks
  - Acts or actions that exploits vulnerability (i.e., an identified weakness) in controlled system
  - Accomplished by threat agent that damages or steals organization's information
- Types of attacks
  - Malicious code: includes execution of viruses, worms, Trojan horses, and active Web scripts with intent to destroy or steal information
  - Hoaxes: transmission of a virus hoax with a real virus attached; more devious form of attack

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.

Table 2-2 Attack Replication Vectors

Attacks (cont'd.)

- Types of attacks (cont'd.)
  - Back door: gaining access to system or network using known or previously unknown/newly discovered access 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 (cont'd.)

- Types of attacks (cont'd.)
  - 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.

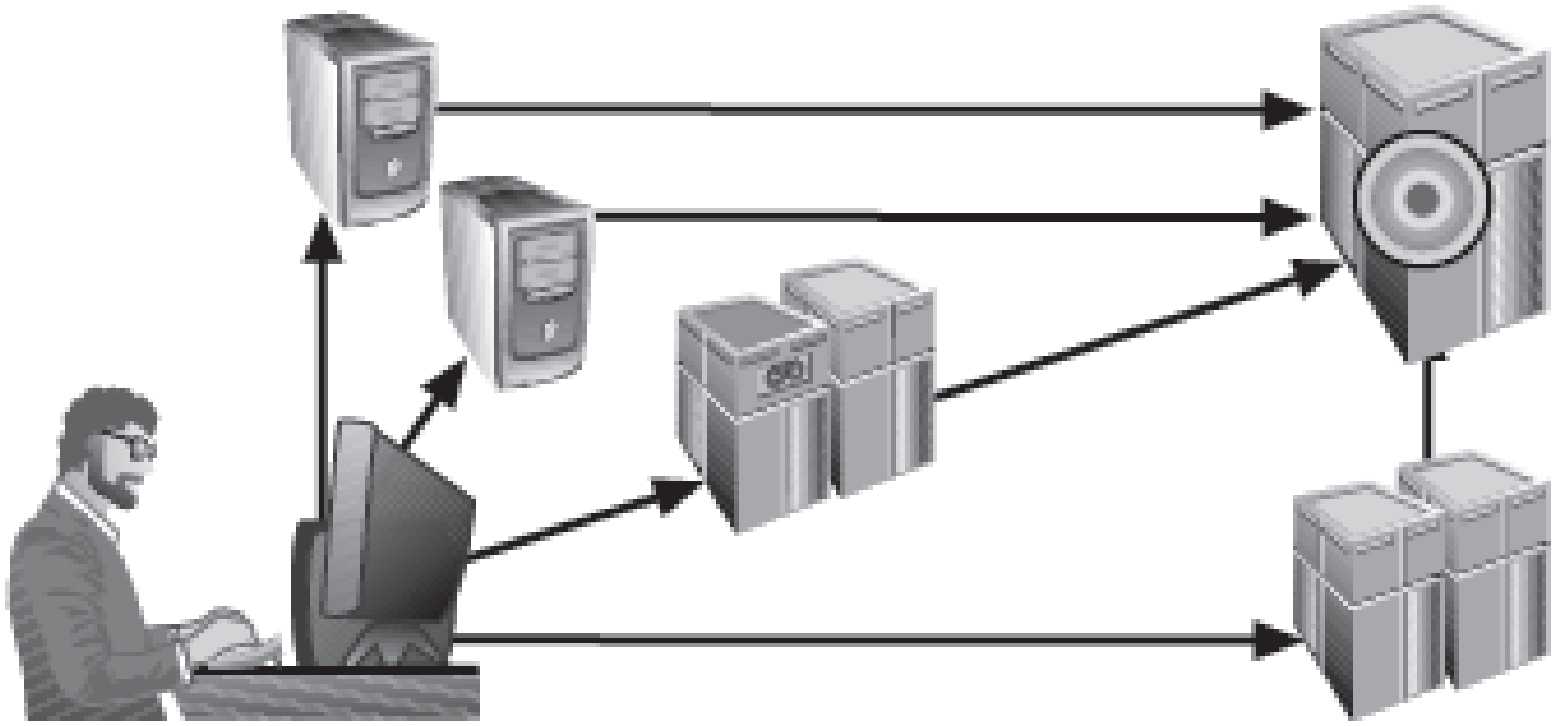

Figure 2-11 Denial-of-Service Attacks

Attacks (cont'd.)

- Types of attacks (cont'd.)
  - 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
  - Mail bombing: also a DoS; attacker routes large quantities of e-mail to target

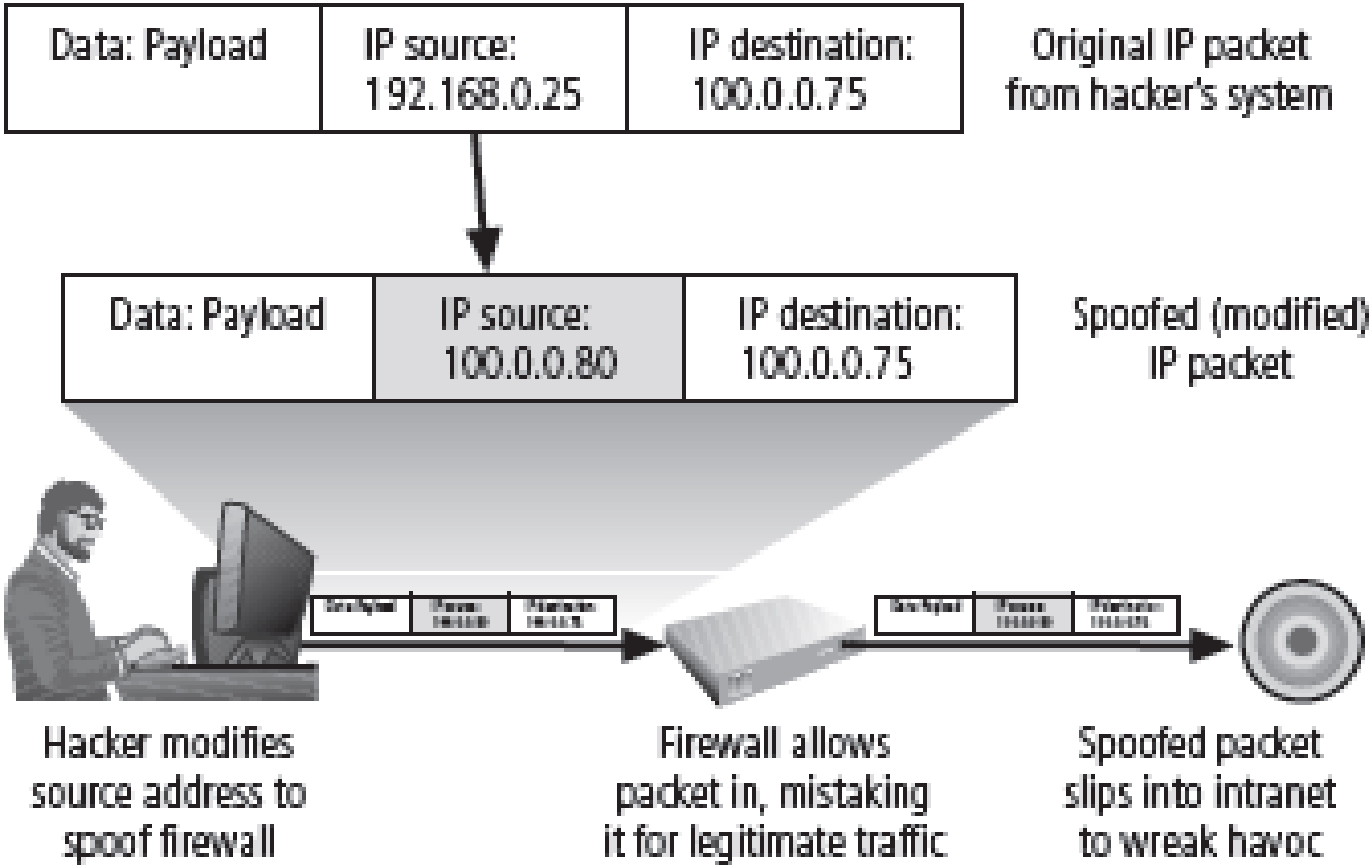

Figure 2-12 IP Spoofing

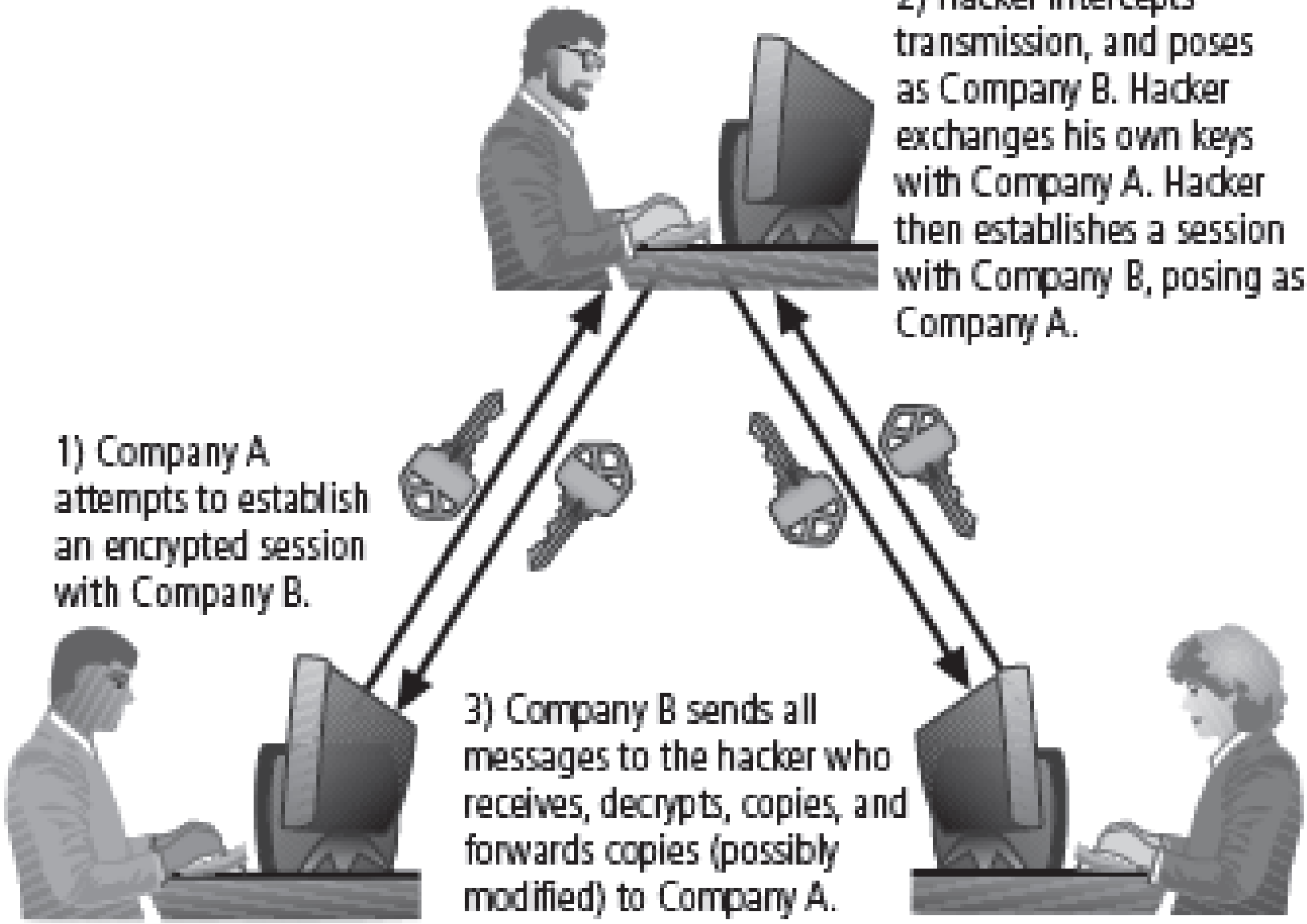

Figure 2-13 Man-in-the-Middle Attack

Attacks (cont'd.)

- Types of attacks (cont'd.)
  - Sniffers: program or device that monitors data traveling over network; can be used both for legitimate purposes and for stealing information from a network
  - Phishing: an attempt to gain personal/financial information from individual, usually by posing as legitimate entity
  - Pharming: redirection of legitimate Web traffic (e.g., browser requests) to illegitimate site for the purpose of obtaining private information

Attacks (cont'd.)

- Types of attacks (cont'd.)
  - Social engineering: using social skills to convince people to reveal access credentials or other valuable information to attacker
  - "People are the weakest link. You can have the best technology; firewalls, intrusion-detection systems, biometric devices ... and somebody can call an unsuspecting employee. That's all she wrote, baby. They got everything." — Kevin Mitnick
  - Timing attack: relatively new; works by exploring contents of a Web browser's cache to create malicious cookie

Software Design Principles

- Good software development results in secure products that meet all design specifications
- Some commonplace security principles:
  - Keep design simple and small
  - Access decisions by permission not exclusion
  - Every access to every object checked for authority
  - Design depends on possession of keys/passwords
  - Protection mechanisms require two keys to unlock
  - Programs/users utilize only necessary privileges

Software Design Principles (cont'd.)

- Some commonplace security principles (cont'd.):
  - Minimize mechanisms common to multiple users
  - Human interface must be easy to use so users routinely/automatically use protection mechanisms

Software Development Security Problems

- Problem areas in software development:
  - Buffer overruns
  - Command injection
  - Cross-site scripting
  - Failure to handle errors
  - Failure to protect network traffic
  - Failure to store and protect data securely
  - Failure to use cryptographically strong random numbers

Software Development Security Problems (cont'd.)

- Problem areas in software development (cont'd.):
  - Format string problems
  - Neglecting change control
  - Improper file access
  - Improper use of SSL
  - Information leakage
  - Integer bugs (overflows/underflows)
  - Race conditions
  - SQL injection

Software Development Security Problems (cont'd.)

- Problem areas in software development (cont'd.):
  - Trusting network address resolution
  - Unauthenticated key exchange
  - Use of magic URLs and hidden forms
  - Use of weak password-based systems
  - Poor usability

Summary

- Unlike any other aspect of IT, information security's primary mission to ensure things stay the way they are
- Information security performs four important functions:
  - Protects organization's ability to function
  - Enables safe operation of applications implemented on organization's IT systems
  - Protects data the organization collects and uses
  - Safeguards the technology assets in use at the organization

Summary (cont'd.)

- Threat: object, person, or other entity representing a constant danger to an asset
- Management effectively protects its information through policy, education, training, and technology controls
- Attack: a deliberate act that exploits vulnerability
- Secure systems require secure software