Information Security,

The Need for Security

Learning Objectives

- Upon completion of this material, you should be able to:
  - Demonstrate that organizations have a business need for information security
  - Explain why a successful information security program is the responsibility of both an organization’s general management and IT management

Learning Objectives (cont'd.)

- Identify the threats posed to information security and the more common attacks associated with those threats, and differentiate threats to the information within systems from attacks against the information within systems
- Describe the issues facing software developers, as well as the most common errors made by developers, and explain how software development programs can create software that is more secure and reliable

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

Business Needs First, Technology Needs Last

Information security performs four important functions for an organization:

1. Protects the organization’s ability to function
2. Enables the safe operation of applications implemented on the organization’s IT systems
3. Protects the data the organization collects and uses
4. Safeguards the technology assets in use at the organization

Protecting the Functionality of an Organization

- The three communities of interest—general management, IT management, and information security management—are each responsible for facilitating the information security program that protects the organization's ability to function.
- Information security is both management issue and people issue
- Organization should address information security in terms of business impact and cost

Protecting the Ability of the Organization to Function

- Both general management and IR management are responsible for implementing information security to protect the ability of the organization to function.
- “Information security is a management issue in addition to a technical issue, it is a people issue in addition to the technical issue.”
- To assist management in addressing the needs for information security, communities of interest must communicate in terms of business impact and the cost of business interruption and avoid arguments expressed only in technical terms.

- Without data, an organization loses its record of transactions and its ability to deliver value to customers.
- Any business, educational institution, or government agency that operates within the modern context of connected and responsive services relies on information systems.
- Even when transactions are not online, information systems and the data they process enable the creation and movement of goods and services.

- Therefore, data security—protecting data in transmission, in processing, and at rest (storage)—is a critical aspect of information security.
- The value of data motivates attackers to steal, sabotage, or corrupt it.
- An effective information security program implemented by management protects the integrity and value of the organization’s data.

- Managerial controls include policy, procedure, and governance.
- Technical controls used to secure databases rely on knowledge of access control, authentication, auditing, application security, backup and recovery, encryption, and integrity controls.
- Physical controls include the use of data centers with locking doors, fire suppression systems, video monitoring, and physical security guards.

- The fundamental practices of information security have broad applicability in the area of database security.
- One indicator of this strong degree of overlap is that the International Information Systems Security Certification Consortium (ISC)2, the organization that evaluates candidates for many prestigious information security certification programs, allows experience as a database administrator to count toward the experience requirement for the Certified Information Systems Security Professional (CISSP).

Enabling the Safe Operation of Applications

- Organization needs environments that safeguard applications using IT systems
- Management must continue to oversee infrastructure once in place—not relegate to IT department

Enabling the Safe Operation of Applications

- Today's organizations are under immense pressure to create and operate integrated, efficient, and capable applications.
- The modern organization needs to create an environment that safeguards applications using the organization's IT systems, particularly the environment of the organization's infrastructure.
- Once the infrastructure is in place, management must understand it has not abdicated to the IT department its responsibility to make choices and enforce decisions, but must continue to oversee the infrastructure.

Protecting Data that Organizations Collect and Use

- Many organizations realize that one of their most valuable assets is their data, because without data, an organization loses its record of transactions and/or its ability to deliver value to its customers.
- Protecting data in motion and data at rest are both critical aspects of information security.
- An effective information security program is essential to the protection of the integrity and value of the organization’s data.

Safeguarding the Technology Assets in Organizations

- To perform effectively, organizations must add secure infrastructure services based on the size and scope of the enterprise.
- When an organization grows and more capabilities are needed, additional security services may have to be provided locally.
- Likewise, as the organization's network grows to accommodate changing needs, more robust technology solutions may be needed to replace security programs the organization has outgrown.

Threats

- To make sound decisions about information security, create policies, and enforce them, management must be informed of the various kinds of threats facing the organization, its applications, data and information systems.
- 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

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

Common Attack Pattern Enumeration and Classification (CAPEC)

- A tool that security professionals can use to understand attacks is the Common Attack Pattern Enumeration and Classification (CAPEC) Web site hosted by Mitre—a non-profit research and development organization sponsored by the U.S. government.
- This online repository can be searched for characteristics of a particular attack or simply browsed by professionals who want additional knowledge of how attacks occur procedurally.
- For more information on CAPEC, visit http://capec.mitre.org, where the contents can be downloaded or viewed online.

Assignment

Explain the following:

a. Spoofing identities:
b. **T**ampering with data:
c. **R**epudiation:
d. **I**nformation disclosure:
e. **D**enial of service (DoS):
f. **E**levation of privilege:
g. Malware
h. A Logic Bomb
i. BackDoor
j. Trojan Horse

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

Compromises to Intellectual Property

- Many organizations create or support the development of intellectual property as part of their business operations.
- Intellectual property is defined as “the ownership of ideas and control over the tangible or virtual representation of those ideas.”
- Intellectual property for an organization includes trade secrets, copyrights, trademarks, and patents.

Compromises to Intellectual Property – Cont'd

- Once intellectual property (IP) has been defined and properly identified, breaches to IP constitute a threat to the security of this information.
- Most common IP breaches involve the unlawful use or duplication of software-based intellectual property, known as software piracy.

Compromises to Intellectual Property – Cont'd

- In addition to the laws surrounding software piracy, two watchdog organizations investigate allegations of software abuse: Software & Information Industry Association (SIIA), formerly the Software Publishers Association, and the Business Software Alliance (BSA).
- Enforcement of copyright violations, piracy, and the like has been attempted through a number of technical security mechanisms, including digital watermarks, embedded codes.

Copyright Protection and User Registration

- A number of technical mechanisms—digital watermarks, embedded code, copyright codes, and even the intentional placement of bad sectors on software media—have been used to enforce copyright laws.
- The most common tool is a unique software registration code in combination with an end-user license agreement (EULA) that usually pops up during the installation of new software, requiring users to indicate that they have read and agree to conditions of the software's use.

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

Deliberate Software Attacks – cont'd

- Deliberate software attacks occur when an individual or group designs software to attack an unsuspecting system. Most of this software is referred to as malicious code or malicious software, or sometimes malware.
- These software components or programs are designed to damage, destroy, or deny service to the target systems.
- Some of the more common instances of malicious code are viruses and worms, Trojan horses, logic bombs, back doors, and denial-of-services attacks.

Deliberate Software Attacks – Cont'd

- Computer viruses are segments of code that perform malicious actions.
- This code behaves very much like a virus pathogen attacking animals and plants, using the cell's own replication machinery to propagate and attack.
- The code attaches itself to the existing program and takes control of that program's access to the targeted computer.
- The virus-controlled target program then carries out the virus's plan by replicating itself into additional targeted systems.

Deliberate Software Attacks – Cont'd

- The macro virus is embedded in the automatically executing macro code, common in office productivity software like word processors, spread sheets, and database applications.
- The boot virus infects the key operating systems files located in a computer's boot sector.
- Worms - Malicious programs that replicate themselves constantly without requiring another program to provide a safe environment for replication. Worms can continue replicating themselves until they completely fill available resources, such as memory, hard drive space, and network bandwidth.

Deliberate Software Attacks – Cont'd

- Trojan horses - Software programs that hide their true nature and reveal their designed behavior only when activated. Trojan horses are frequently disguised as helpful, interesting, or necessary pieces of software, such as readme.exe files often included with shareware or freeware packages.
- Back door or Trap door - A virus or worm can have a payload that installs a back door or trap door component in a system. This allows the attacker to access the system at will with special privileges.

Deliberate Software Attacks – Cont'd

- Polymorphism - A threat that changes its apparent shape over time, representing a new threat not detectable by techniques that are looking for a preconfigured signature. These threats actually evolve, changing their size and appearance to elude detection by antivirus software programs, making detection more of a challenge.
- Virus and Worm Hoaxes - As frustrating as viruses and worms are, perhaps more time and money is spent on resolving virus hoaxes. Well-meaning people spread the viruses and worms when they send e-mails warning of fictitious or virus laden threats.

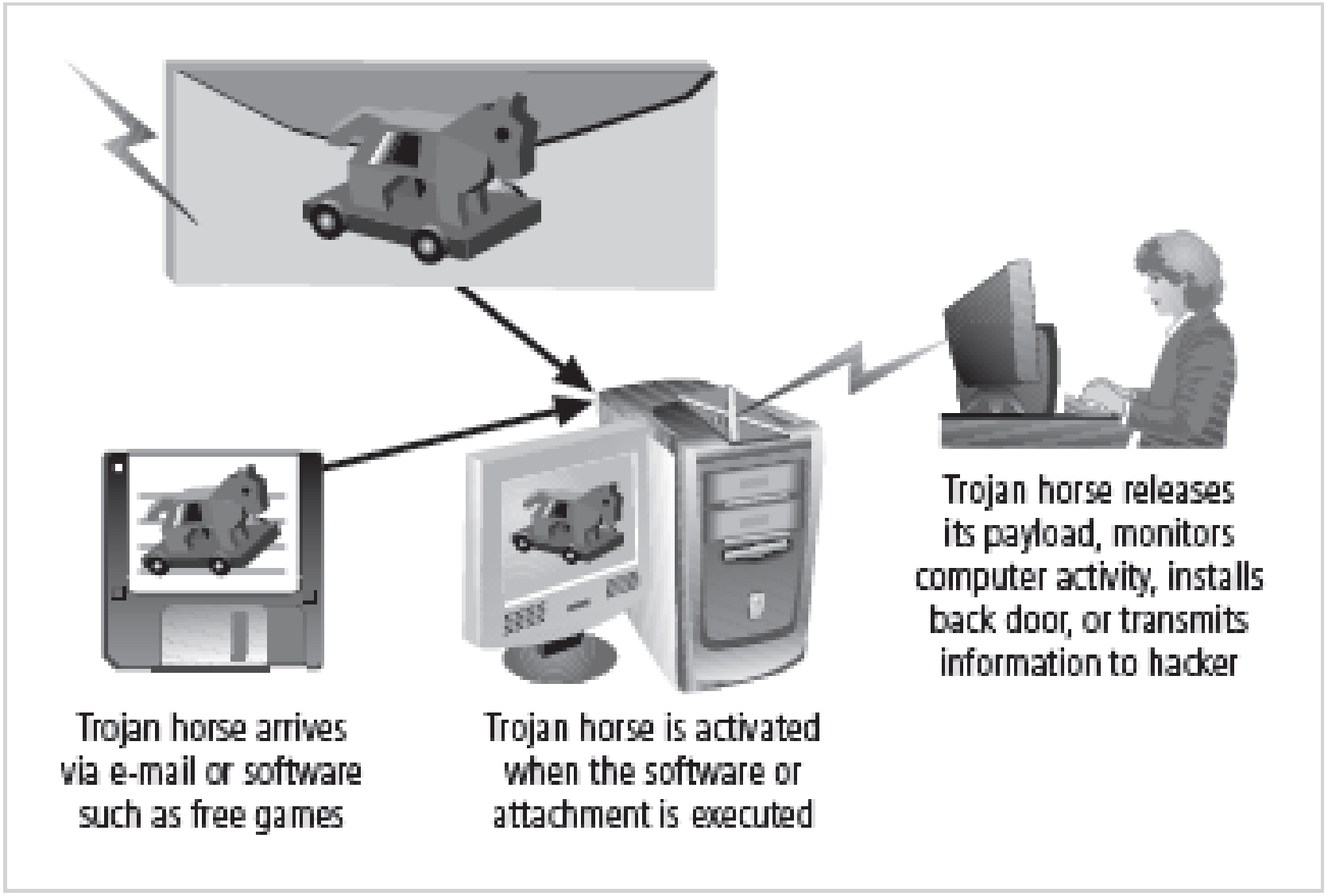

Figure 2-2 Trojan Horse Attack

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**

- The threat of irregularities from power utilities is common and can lead to fluctuations such as power excesses, power shortages, and power losses.
- Voltage levels can:
- spike – momentary increase or surge – prolonged increase
- sag – momentary low voltage, or brownout – prolonged drop
- fault – momentary loss of power, or blackout – prolonged loss

Deviations in Quality of Service - Power irregularities (cont'd.)

- 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

- Since sensitive electronic equipment, especially networking equipment, computers, and computer-based systems are susceptible to fluctuations, controls can be applied to manage power quality.

Deliberate Acts of Espionage or Trespass

- This threat represents a well-known and broad category of electronic and human activities that breach the confidentiality of information.
- When an unauthorized individual gains access to the information an organization is trying to protect, that act is categorized as a deliberate act of espionage or trespass.
- When information gatherers employ techniques that cross the threshold of what is legal and/or ethical, they enter the world of industrial espionage.

Deliberate Acts of Espionage or Trespass

- Instances of shoulder surfing occur at computer terminals, desks, ATM machines, public phones, or other places where a person is accessing confidential information.
- The threat of trespass can lead to unauthorized real or virtual actions that enable information gatherers to enter premises or systems they have not been authorized to enter.
- Controls are sometimes implemented to mark the boundaries of an organization’s virtual territory.

Deliberate Acts of Espionage or Trespass

- These boundaries give notice to trespassers that they are encroaching on the organization's cyberspace.
- The classic perpetrator of deliberate acts of espionage or trespass is the hacker.
- In the gritty world of reality, a hacker uses skill, guile, or fraud to attempt to bypass the controls placed around information that is the property of someone else. The hacker frequently spends long hours examining the types and structures of the targeted systems.

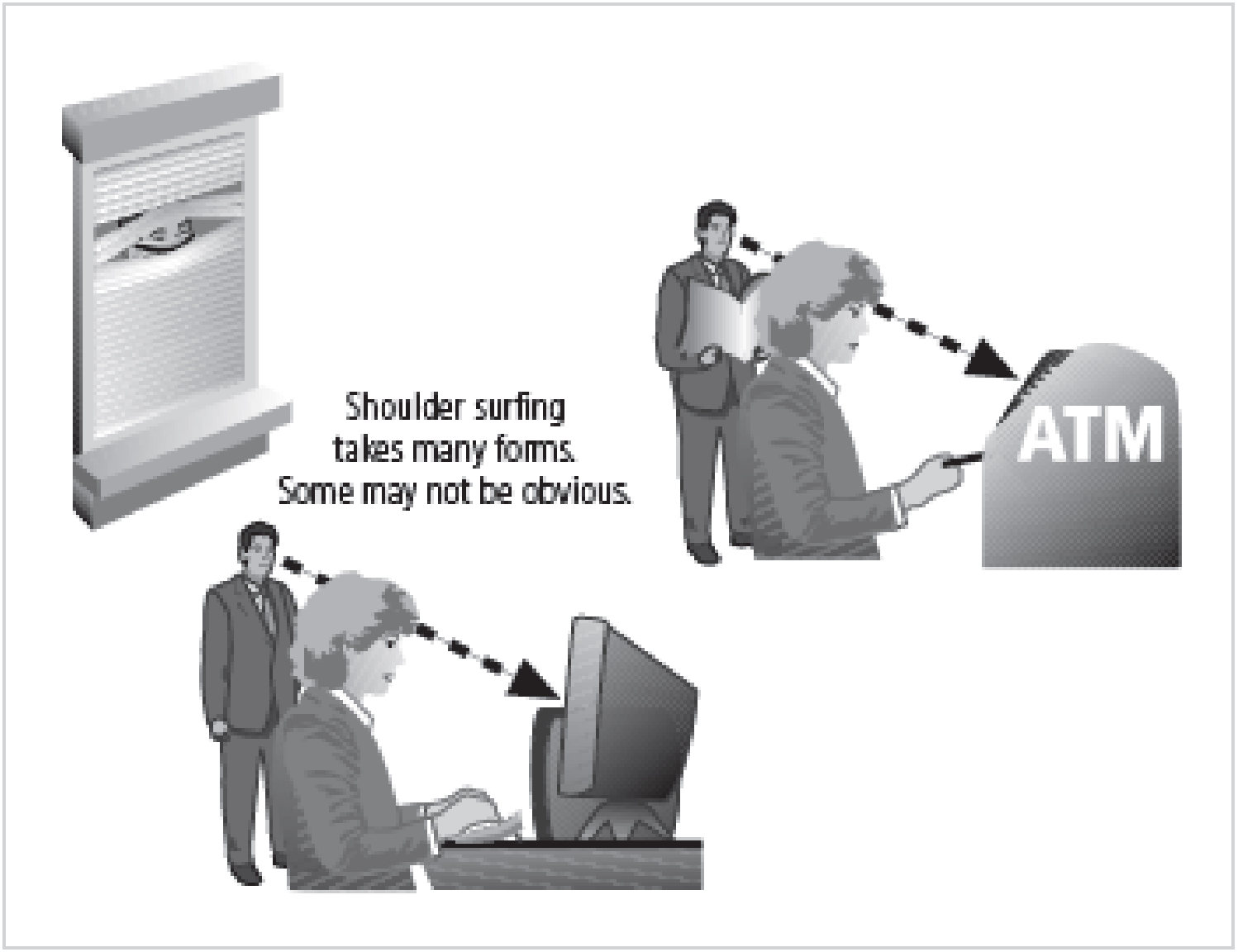

Figure 2-3 Shoulder Surfing

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 2-4 Hacker Profiles

Deliberate Acts of Espionage or Trespass (continued)

There are generally two skill levels among hackers.

- The first is the expert hacker, who develops software scripts and codes exploits used by the second category, the novice, or unskilled hacker.
- The expert hacker is usually a master of several programming languages, networking protocols, and operating systems and also exhibits a mastery of the technical environment of the chosen targeted system.
- However, expert hackers have now become bored with directly attacking systems and have turned to writing software.

Deliberate Acts of Espionage or Trespass (continued)

- The software they are writing are automated exploits that allow novice hackers to become script kiddies, hackers of limited skill who use expert-written software to exploit a system but do not fully understand or appreciate the systems they hack.
- As a result of preparation and continued vigilance, attacks conducted by scripts are usually predictable and can be adequately defended against.

Espionage or Trespass (cont’d.)

There are other terms for system rule breakers:

- The term cracker is now commonly associated with an individual who “cracks” or removes the software protection from an application designed to prevent unauthorized duplication.
- A phreaker hacks the public telephone network to make free calls, disrupt services, and generally wreak havoc.

Social Engineering Password Attacks

- While social engineering is discussed in detail later in the section called “Human Error or Failure,” it is worth mentioning here as a mechanism to gain password information.
- Attackers posing as an organization’s IT professionals may attempt to gain access to systems information by contacting low-level employees and offering to help with their computer issues.
- By posing as a friendly helpdesk or repair technician, the attacker asks employees for their usernames and passwords, then uses the information to gain access to organizational systems. Some even go so far as to actually resolve the user’s issues.

Forces of Nature

- Forces of nature, force majeure, or acts of God pose the most dangerous threats, because they are unexpected and can occur with very little warning.
- These threats can disrupt not only the lives of individuals, but also the storage, transmission, and use of information.
- These include fire, flood, earthquake, lightning, landslide or mudslide, tornado or severe windstorm, hurricane or typhoon, tsunami, electrostatic discharge, and dust contamination.

Forces of Nature

- Because it is not possible to avoid threats from forces of nature, organizations must implement controls to limit damage and prepare contingency plans for continued operations, such as disaster recovery plans, business continuity plans, and incident response plans.
- Knowing a region’s susceptibility to certain natural disasters is a critical planning component when selecting new facilities for an organization or considering the location of off-site data backup.

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.
- Controls, ranging from simple procedures, such as requiring the user to type a critical command twice, to more complex procedures, such as the verification of commands by a second party.

Figure 2-5 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

- Attacks on the face of an organization—its Web site
- 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- 6 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

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 (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.

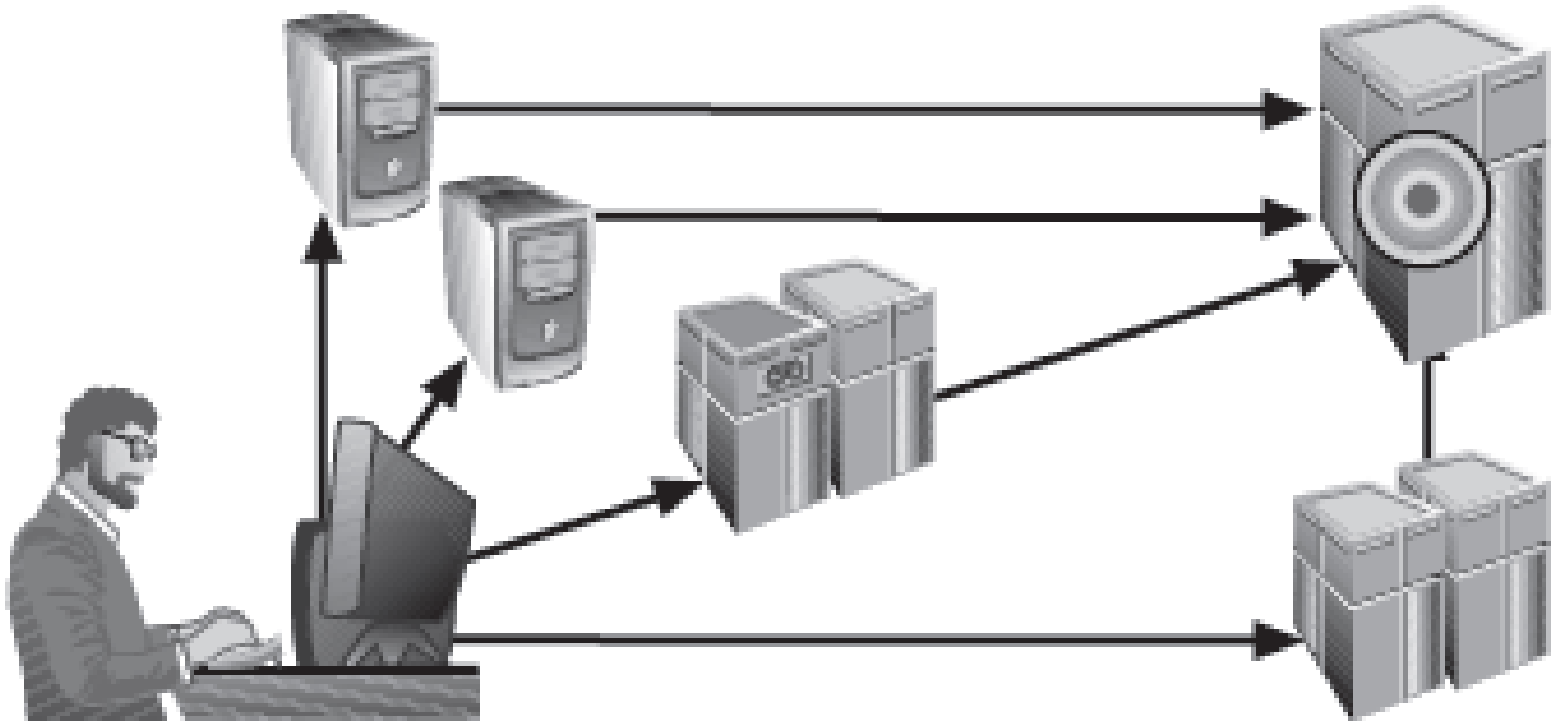

Figure 2-6 Denial-of-Service Attacks

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

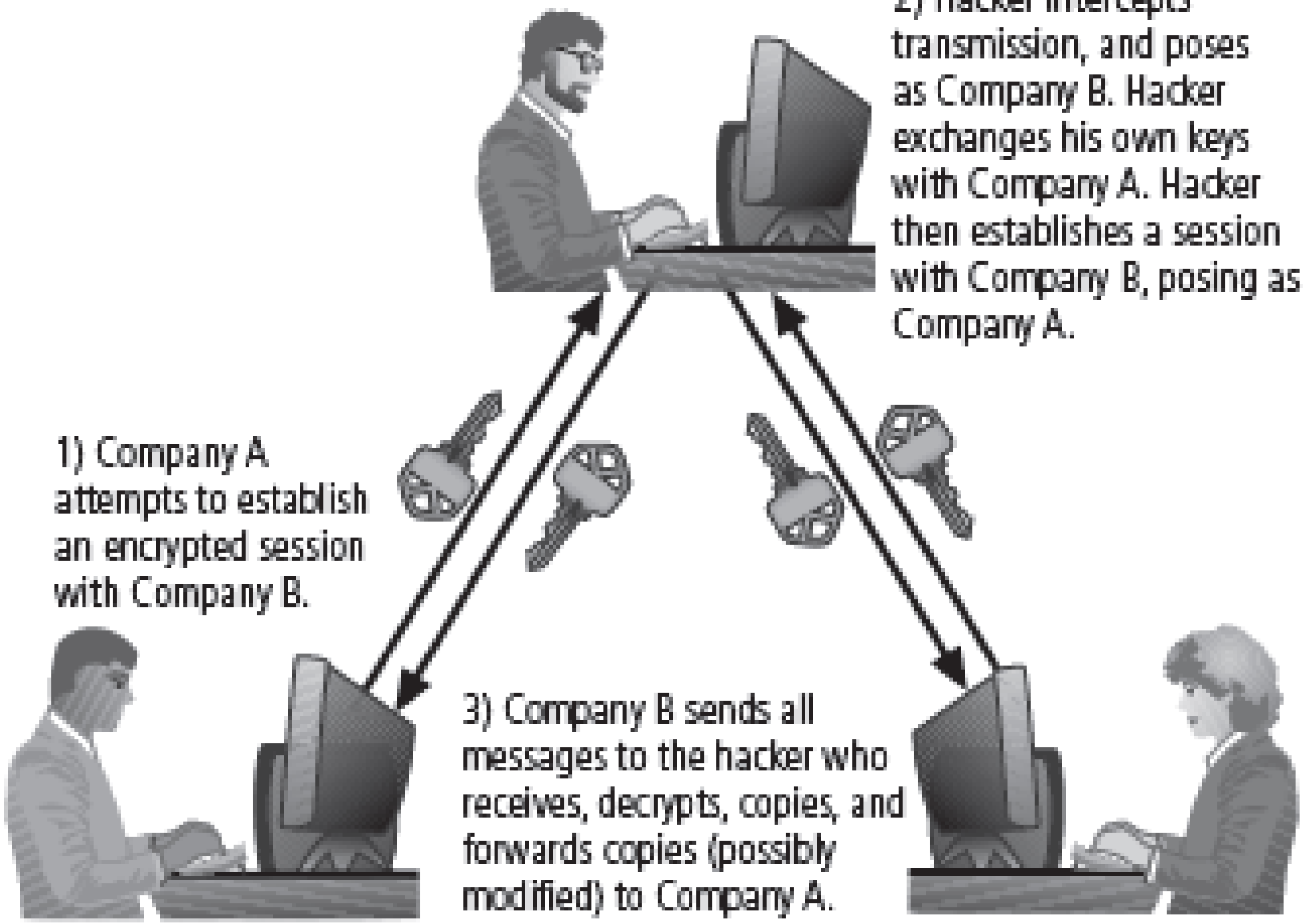

Figure 2-13 Man-in-the-Middle Attack

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

Secure Software Development

- Many information security issues discussed here are caused by software elements of system
- Development of software and systems is often accomplished using methodology such as Systems Development Life Cycle (SDLC)
- Many organizations recognize need for security objectives in SDLC and have included procedures to create more secure software
- This software development approach known as Software Assurance (SA)

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