Principles of Information Security

Chapter 2

The Need for Security

Our bad neighbor makes us early stirrers,

Which is both healthful and good husbandry.

WILLIAM SHAKESPEARE (1564–1616),
KING HENRY, IN HENRY V, ACT 4, SC. 1, L. 6-7.

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

- Information security performs four important functions for an organization
  - Protects ability to function
  - Enables safe operation of applications implemented on its IT systems
  - Protects data the organization collects and uses
  - Safeguards technology assets in use

Protecting the Functionality of an Organization

- Management (general and IT) responsible for implementation
- Information security is both management issue and people issue
- Organization should address information security in terms of business impact and cost

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

Protecting Data that Organizations Collect and Use

- Organization, without data, **loses** its record of transactions and/or ability to deliver value to customers
- Protecting data in motion and data at rest are both critical aspects of information security

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
- 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

Table 2-1 Threats to Information Security[4]

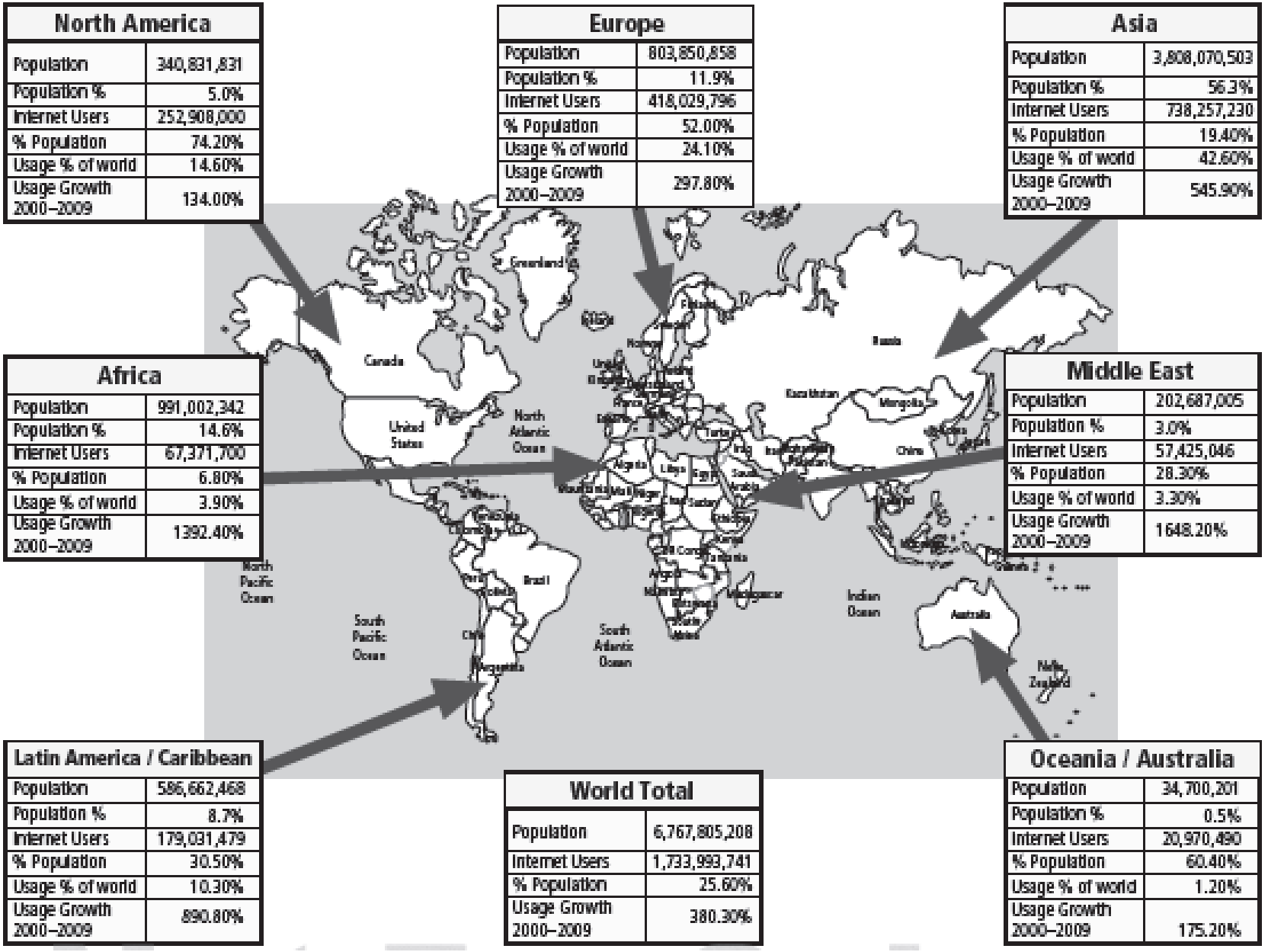

Figure 2-1 World Internet usage[3]

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 (such as digital watermarks, embedded codes)

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

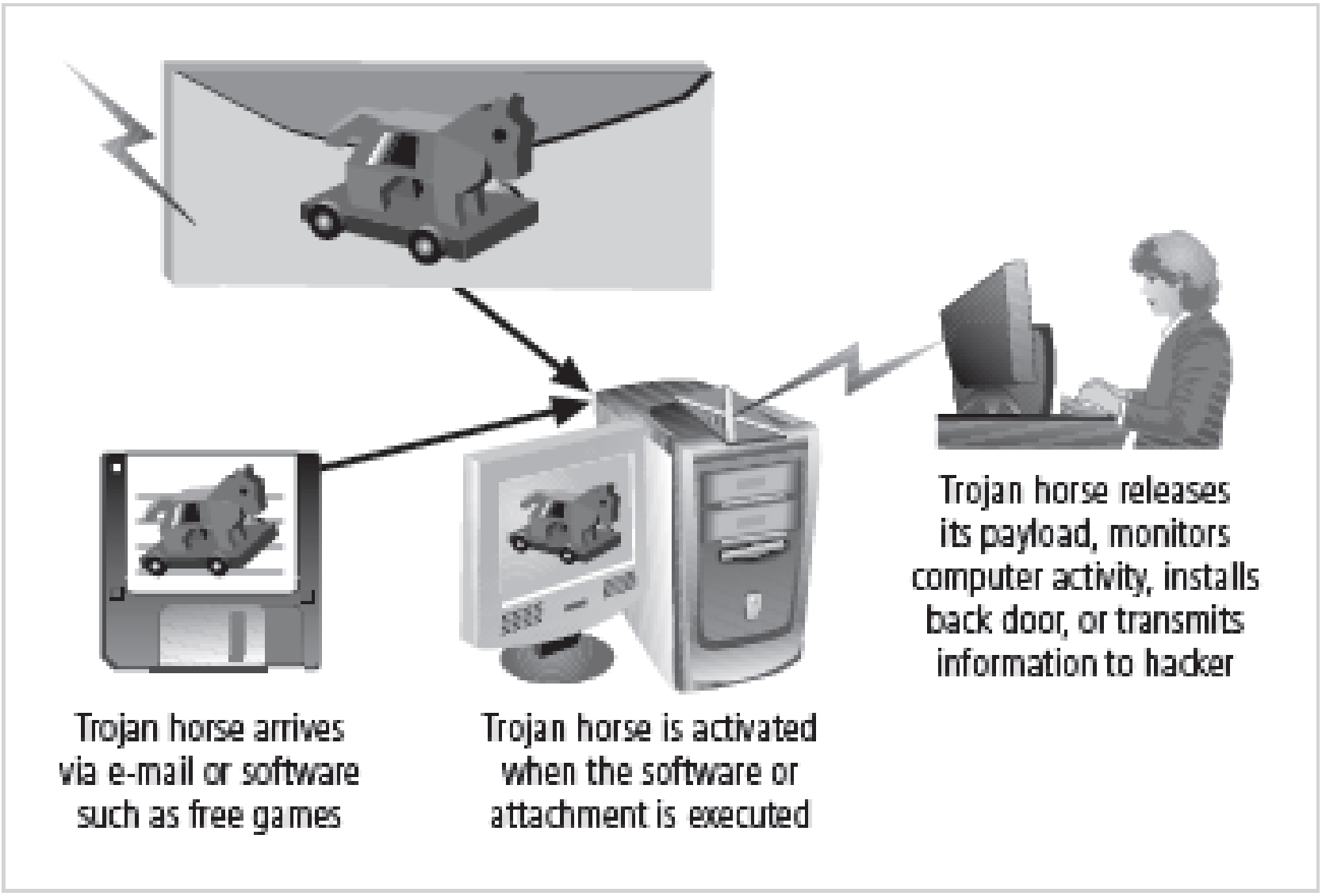

Figure 2-4 Trojan Horse Attack

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 loss 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 (happening frequently)
  - 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
- 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

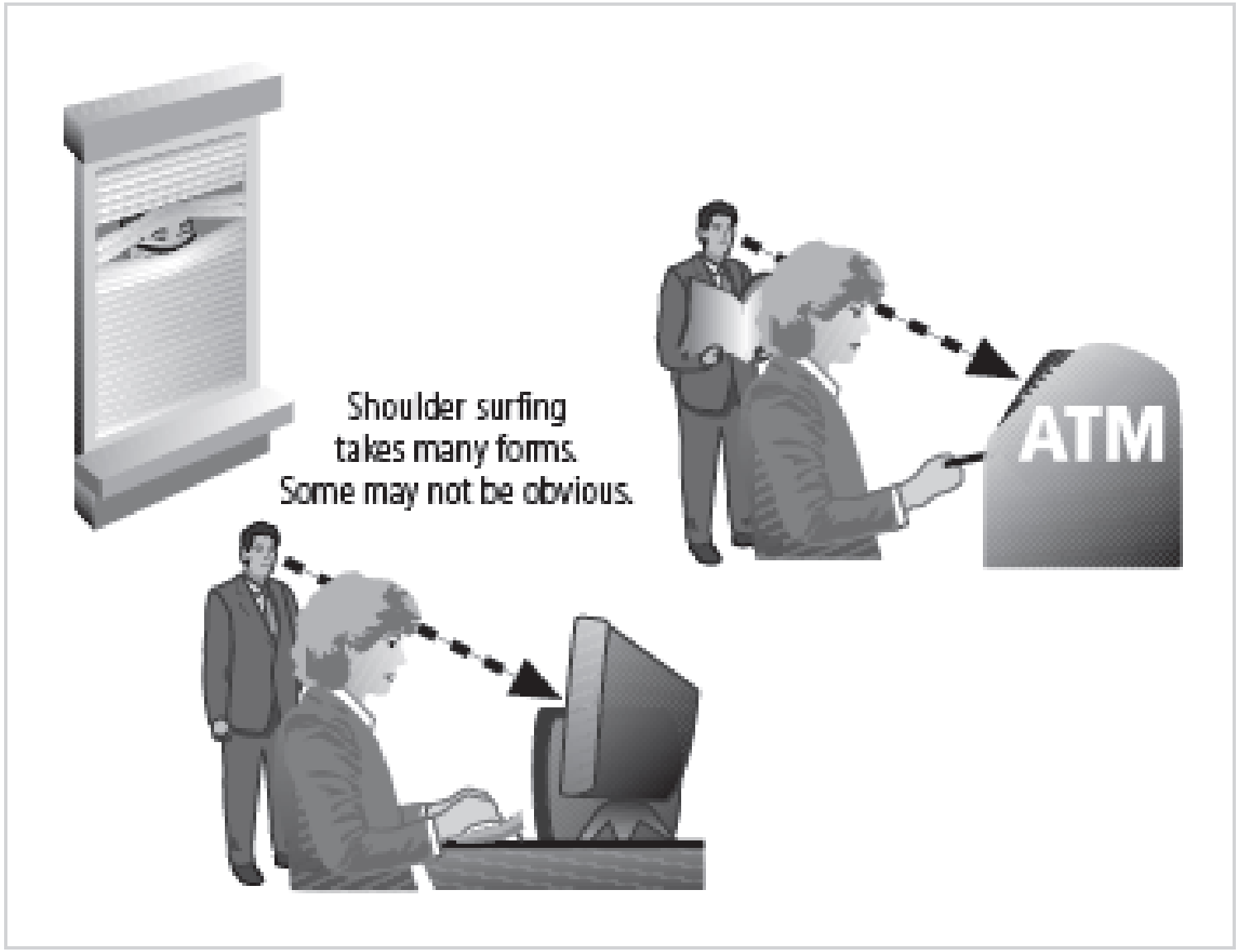

Figure 2-5 Shoulder Surfing

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

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/loss consumer confidence, dropping sales and organization's net worth
- Threat of hacktivist or cyberactivist operations rising
- Cyberterrorism: much more sinister/evil 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

Technical Software Failures or Errors

- Purchased software that contains unrevealed /hidden faults
- Combinations of certain software and hardware can reveal new software 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/legal 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.

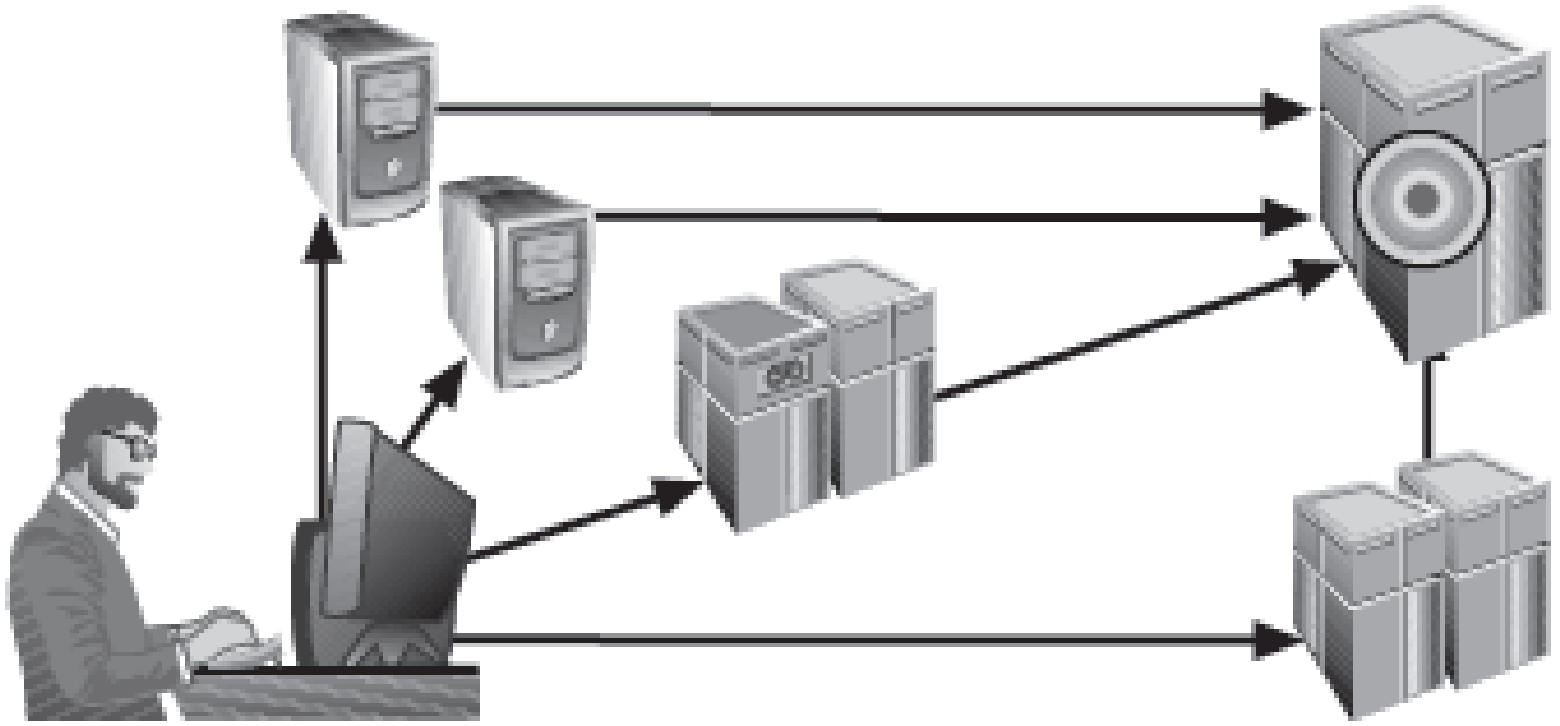

Figure 2-11 Denial-of-Service Attacks

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/unrequested commercial e-mail; more a nuisance/bother 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

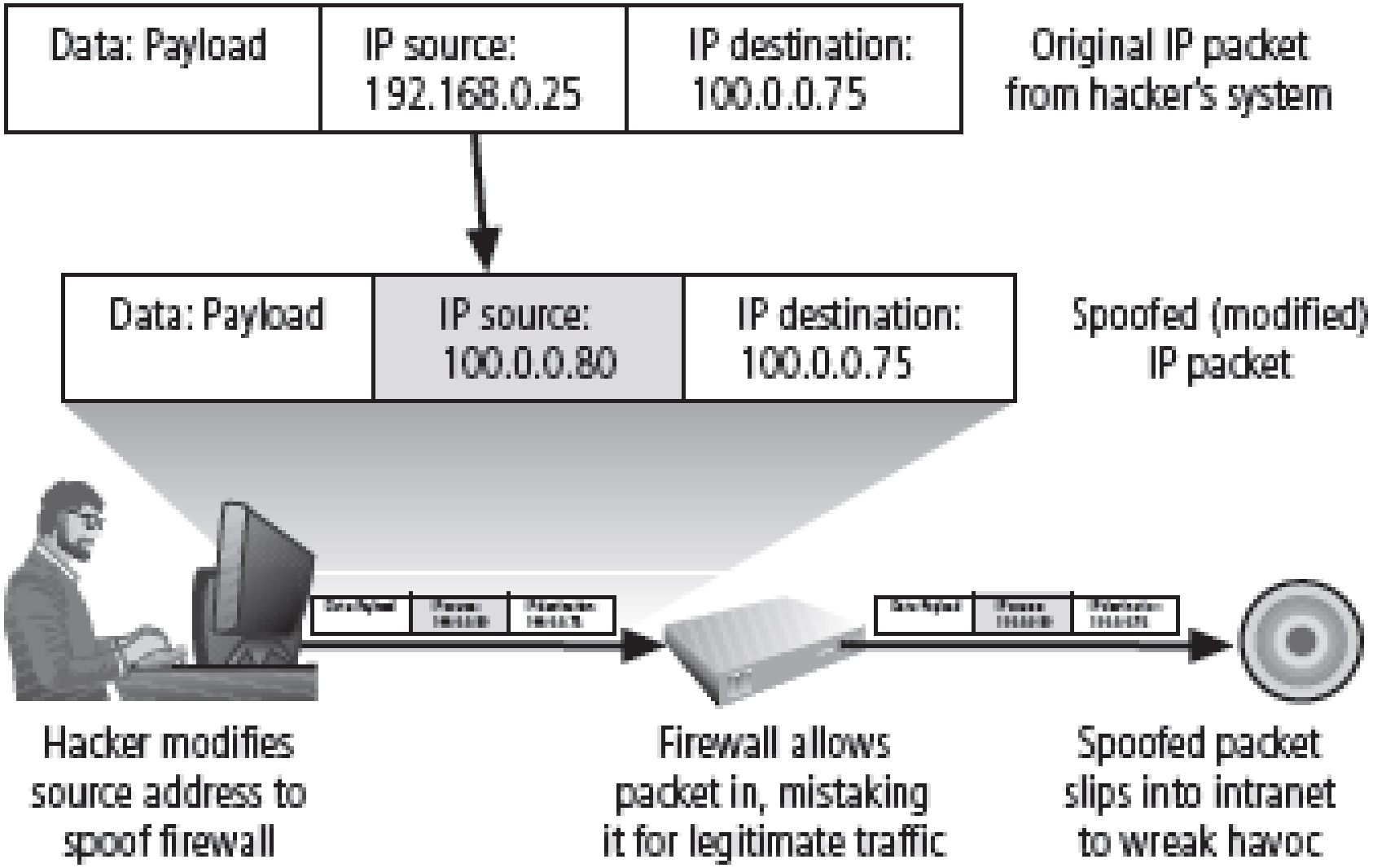

Figure 2-12 IP Spoofing

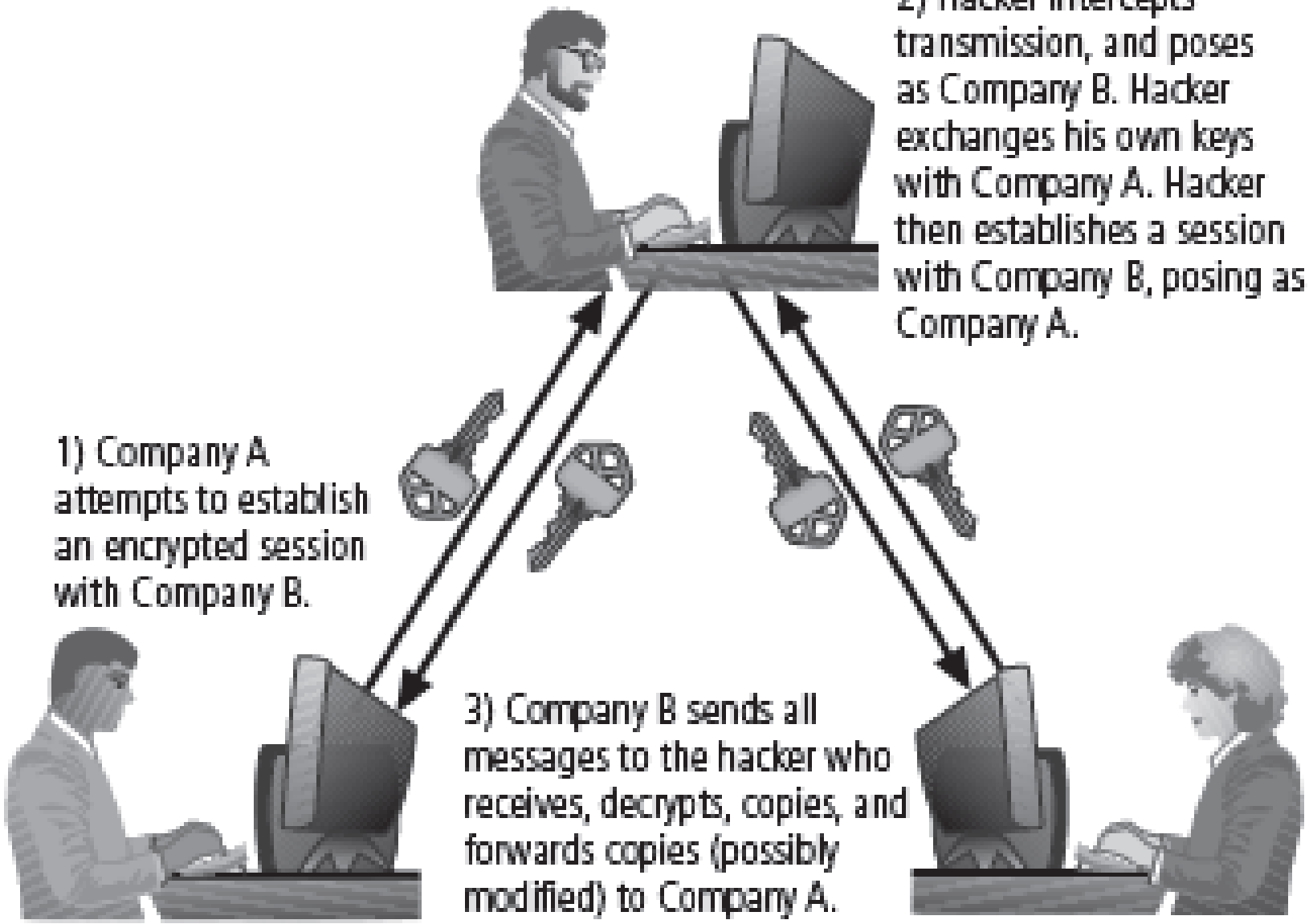

Figure 2-13 Man-in-the-Middle Attack

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

Dr Michael E. Whitman
Kennesaw State University
Department of Computer Science
& Information Systems 1000
Chastain Road Kennesaw, GA
30144-5591 U.S.A
30144/5591

NIGERIA NATIONAL PETROLEUM CORPORATION
PETROLEUM AND PROJECT DIVISION
TEL: +234-80-33004657, 234-1-4805653, FAX: +234-1-2692153,234-1-7591061
P.M.B 2071, LAGOS -- NIGERIA.

29TH JANUARY, 2002

DEAR SIR

This letter is not intended to cause any embarrassment in whatever form, rather is compelled to contact your esteemed self, following the knowledge of your high repute and trustworthiness. Firstly, I must solicit your confidentiality, this is by the virtue of its' nature as being utterly confidential and top secret though I know that a transaction of this magnitude will make anyone apprehensive and worried, but I am assuring you that all will be well at the end of the day. A bold step taken shall not be regretted I assure you.

I am Mr. Tony Okeke and I head a seven man tender board in charge of contract awards and payment approvals. I came to know of you in search of a reliable and reputable person to handle a very confidential business transaction which involves the transfer of a huge sum of money to foreign account requiring maximum confidence. My colleagues and I are top officials of the NIGERIA NATIONAL PETROLEUM CORPORATION (NNPC). OUR DUTIES INCLUDE VETTING, EVALUATION AND FORESEEING THE MAINTENANCE OF THE REFINERIES IN ALL THE DESIGNATED OIL PIPELINES. We are therefore soliciting for your assistance to enable us transfer into your account the said funds. Our country loses a lot of money everyday that is why the international community is very careful and warning their citizens to be careful but I tell you "A TRIAL WILL CONVINCE YOU".

The source of the fund is as follows; during the last military regime here in Nigeria this committee awarded a contract of US$400million to a group of five construction companies on behalf of the NIGERIA NATIONAL PETROLEUM CORPORATION for the construction of the oil pipelines in Kaduna, Port-Harcourt, Warri refineries. During this process my colleagues and I deliberately inflated the total contract sum to the tune US$428million with the intention of sharing the inflated sum of US$28. The government has since approved the sum of US$428 for us as the contract sum, but since the contract is only worth US$400million, the remaining US$28million is what we intend to transfer to reliable and safe offshore account, we are prohibited to operate foreign account in our names since we are still in government. Thus, making it impossible for us to acquire the money in our name right now, I have therefore been delegated as a matter of trust by my colleagues to look for an oversea partner into whose account we can transfer the sum of US$28million.

My colleagues and I have decided that if you/your company can be the beneficiary of this funds on our behalf, you or your company will retain 20% of the total sum US$28million while 75% will be for us the officials and remaining 5% will be used for offsetting all debts/expenses incurred during this transaction.

We have decided that this transaction can only proceed under the following conditions:

1. That you treat this transaction with utmost secrecy and confidentiality and conviction of your transparent honesty.
2. That upon the receipt of the funds you will release the funds as instructed by us after you have removed your share of 20%. Please acknowledge the receipt of this letter using the above telephone and fax numbers. I will bring you into the nomenclature of this transaction when I have heard from you.

Your urgent response will be highly appreciated as we catching on the next payment schedule for the financial quarter. Please be assured that this transaction is 100% legalistic free, only trust can make the reality of this transaction.

Best Regards,

Tony Okeke

MR. TONY OKEKE

Figure 2-14 Example of a Nigerian 4-1-9 Fraud

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 Assurance and the SA Common Body of Knowledge

- National effort underway to create common body of knowledge focused on secure software development
- US Department of Defense and Department of Homeland Security supported Software Assurance Initiative, which resulted in publication of Secure Software Assurance (SwA) Common Body of Knowledge (CBK)
- SwA CBK serves as a strongly recommended guide to developing more secure applications

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/exception
  - Every access to every object checked for authority
  - Design depends on possession/ownership 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

Software Development Security Problems (cont'd)

- Problem areas in software development:
  - 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

Software Development Security Problems (cont'd.)

- Problem areas in software development (cont'd.):
  - 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