



Chapter 8

SECURING INFORMATION SYSTEMS

VIDEO CASES

Case 1: IBM Zone Trusted Information Channel (ZTIC)

Case 2: Open ID and Web Security

Instructional Video 1: The Quest for Identity 2.0

Instructional Video 2: Identity 2.0



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

Learning Objectives

- **Why are information systems vulnerable to destruction, error, and abuse?**
- **What is the business value of security and control?**
- **What are the components of an organizational framework for security and control?**
- **What are the most important tools and technologies for safeguarding information resources?**



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

You're on Facebook? Watch Out!

- Facebook – world's largest social network
- **Problem** – Identity theft and malicious software
 - **Examples:**
 - 2009 18-month hacker scam for passwords, resulted in Trojan horse download that stole financial data
 - Dec 2008 Koobface worm
 - May 2010 Spam campaign aimed at stealing logins
- **Illustrates:** Types of security attacks facing consumers
- **Demonstrates:** Ubiquity of hacking, malicious software



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

System Vulnerability and Abuse

- **Security:**
 - Policies, procedures and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems
- **Controls:**
 - Methods, policies, and organizational procedures that ensure safety of organization's assets; accuracy and reliability of its accounting records; and operational adherence to management standards



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

System Vulnerability and Abuse

- **Why systems are vulnerable**
 - Accessibility of networks
 - Hardware problems (breakdowns, configuration errors, damage from improper use or crime)
 - Software problems (programming errors, installation errors, unauthorized changes)
 - Disasters
 - Use of networks/computers outside of firm's control
 - Loss and theft of portable devices



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

System Vulnerability and Abuse

CONTEMPORARY SECURITY CHALLENGES AND VULNERABILITIES

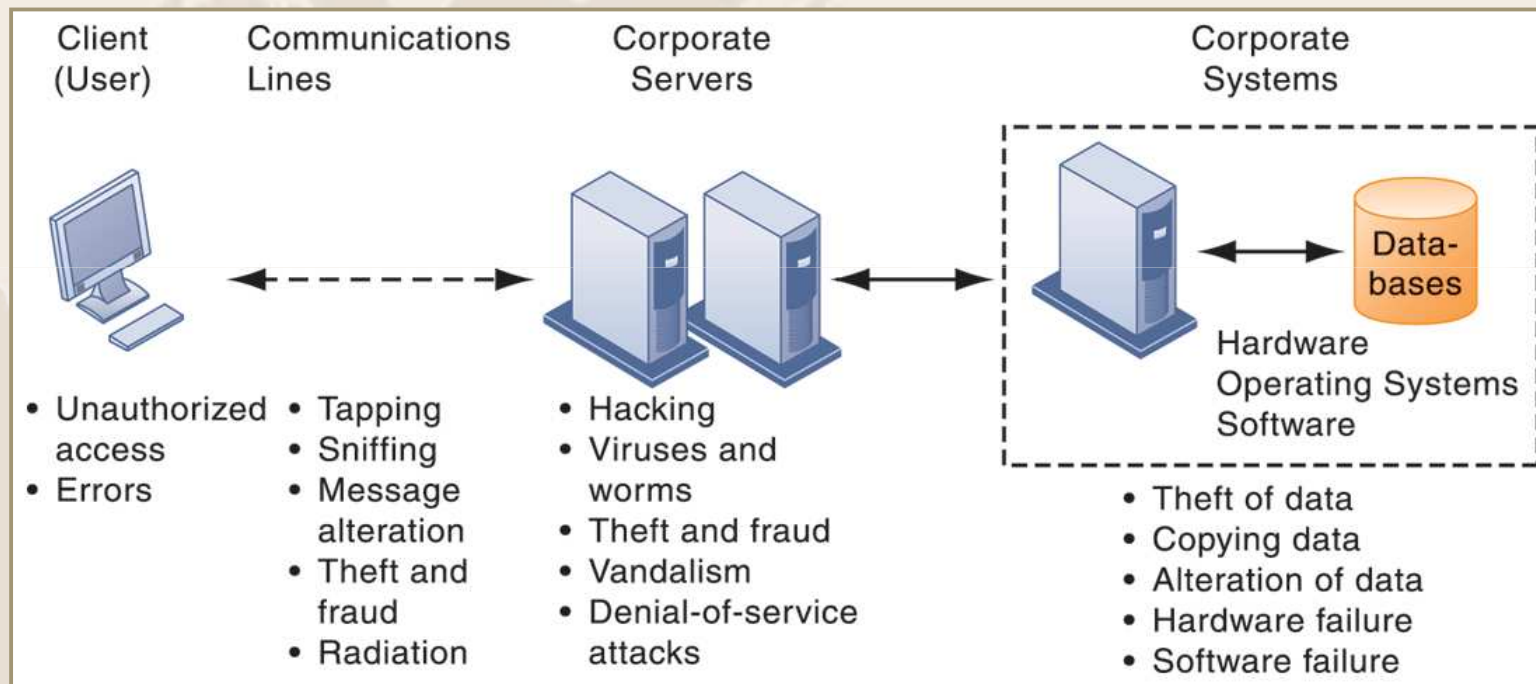


FIGURE 8-1

The architecture of a Web-based application typically includes a Web client, a server, and corporate information systems linked to databases. Each of these components presents security challenges and vulnerabilities. Floods, fires, power failures, and other electrical problems can cause disruptions at any point in the network.



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

System Vulnerability and Abuse

- **Internet vulnerabilities**
 - Network open to anyone
 - Size of Internet means abuses can have wide impact
 - Use of fixed Internet addresses with cable or DSL modems creates fixed targets hackers
 - Unencrypted VOIP
 - E-mail, P2P, IM
 - Interception
 - Attachments with malicious software
 - Transmitting trade secrets



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

System Vulnerability and Abuse

- **Wireless security challenges**
 - Radio frequency bands easy to scan
 - **SSIDs (service set identifiers)**
 - Identify access points
 - Broadcast multiple times
 - **War driving**
 - Eavesdroppers drive by buildings and try to detect SSID and gain access to network and resources
 - **WEP (Wired Equivalent Privacy)**
 - Security standard for 802.11; use is optional
 - Uses shared password for both users and access point
 - Users often fail to implement WEP or stronger systems



Management Information Systems

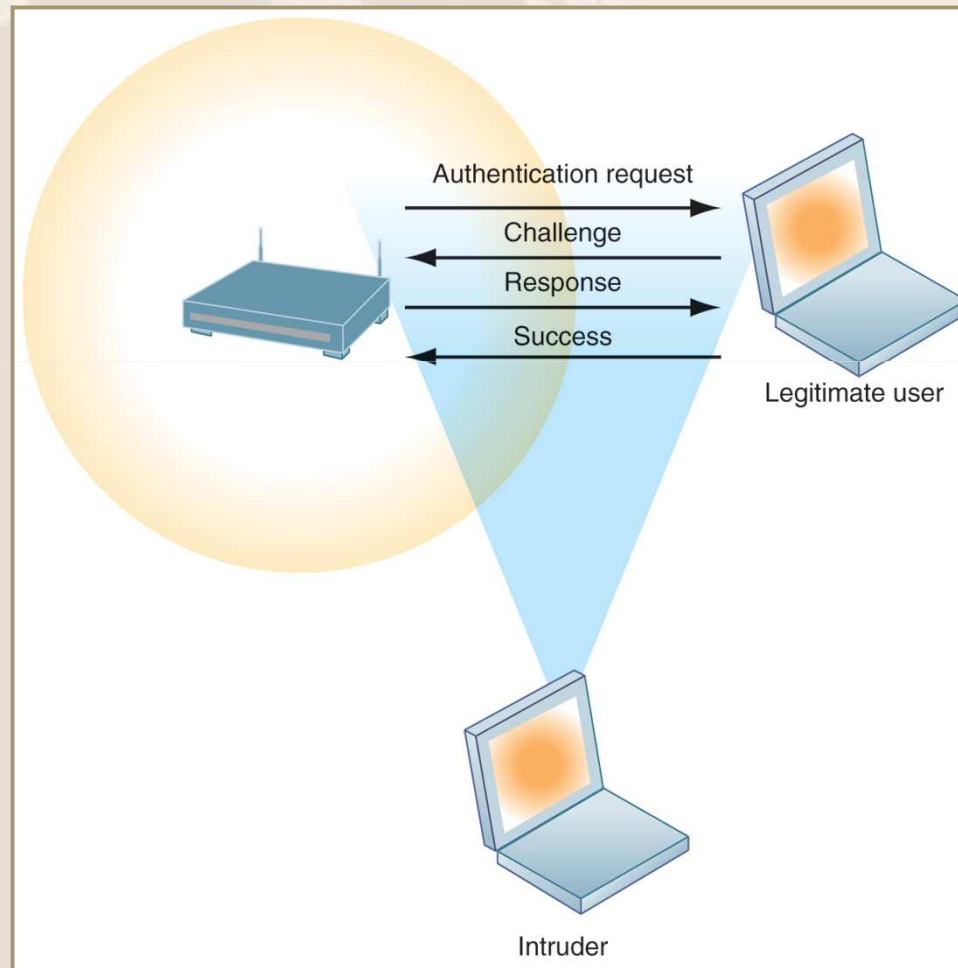
CHAPTER 8: SECURING INFORMATION SYSTEMS

System Vulnerability and Abuse

WI-FI SECURITY CHALLENGES

Many Wi-Fi networks can be penetrated easily by intruders using sniffer programs to obtain an address to access the resources of a network without authorization.

FIGURE 8-2





Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

System Vulnerability and Abuse

- **Malware (malicious software)**
 - **Viruses**
 - Rogue software program that attaches itself to other software programs or data files in order to be executed
 - **Worms**
 - Independent computer programs that copy themselves from one computer to other computers over a network.
 - **Trojan horses**
 - Software program that appears to be benign but then does something other than expected.



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

System Vulnerability and Abuse

- **Malware (cont.)**
 - **SQL injection attacks**
 - Hackers submit data to Web forms that exploits site's unprotected software and sends rogue SQL query to database
 - **Spyware**
 - Small programs install themselves surreptitiously on computers to monitor user Web surfing activity and serve up advertising
 - **Key loggers**
 - Record every keystroke on computer to steal serial numbers, passwords, launch Internet attacks



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

System Vulnerability and Abuse

- **Hackers and computer crime**
 - Hackers vs. crackers
 - Activities include
 - System intrusion
 - System damage
 - Cybervandalism
 - Intentional disruption, defacement, destruction of Web site or corporate information system



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

System Vulnerability and Abuse

- **Spoofing**
 - Misrepresenting oneself by using fake e-mail addresses or masquerading as someone else
 - Redirecting Web link to address different from intended one, with site masquerading as intended destination
- **Sniffer**
 - Eavesdropping program that monitors information traveling over network
 - Enables hackers to steal proprietary information such as e-mail, company files, etc.



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

System Vulnerability and Abuse

- **Denial-of-service attacks (DoS)**
 - Flooding server with thousands of false requests to crash the network.
- **Distributed denial-of-service attacks (DDoS)**
 - Use of numerous computers to launch a DoS
 - Botnets
 - Networks of “zombie” PCs infiltrated by bot malware
 - Worldwide, 6 - 24 million computers serve as zombie PCs in thousands of botnets



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

System Vulnerability and Abuse

- **Computer crime**
 - Defined as “any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution”
 - **Computer may be target of crime, e.g.:**
 - Breaching confidentiality of protected computerized data
 - Accessing a computer system without authority
 - **Computer may be instrument of crime, e.g.:**
 - Theft of trade secrets
 - Using e-mail for threats or harassment



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

System Vulnerability and Abuse

- **Identity theft**
 - Theft of personal Information (social security id, driver's license or credit card numbers) to impersonate someone else
- **Phishing**
 - Setting up fake Web sites or sending e-mail messages that look like legitimate businesses to ask users for confidential personal data.
- **Evil twins**
 - Wireless networks that pretend to offer trustworthy Wi-Fi connections to the Internet



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

System Vulnerability and Abuse

- **Pharming**
 - Redirects users to a bogus Web page, even when individual types correct Web page address into his or her browser
- **Click fraud**
 - Occurs when individual or computer program fraudulently clicks on online ad without any intention of learning more about the advertiser or making a purchase
- **Cyberterrorism and Cyberwarfare**



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

System Vulnerability and Abuse

- **Internal threats: employees**
 - Security threats often originate inside an organization
 - Inside knowledge
 - Sloppy security procedures
 - User lack of knowledge
 - **Social engineering:**
 - Tricking employees into revealing their passwords by pretending to be legitimate members of the company in need of information



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

System Vulnerability and Abuse

- **Software vulnerability**
 - **Commercial software contains flaws that create security vulnerabilities**
 - Hidden bugs (program code defects)
 - Zero defects cannot be achieved because complete testing is not possible with large programs
 - Flaws can open networks to intruders
 - **Patches**
 - Vendors release small pieces of software to repair flaws
 - However exploits often created faster than patches be released and implemented



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

System Vulnerability and Abuse

WHEN ANTIVIRUS SOFTWARE CRIPPLES YOUR COMPUTERS

Read the Interactive Session and discuss the following questions

- What management, organization, and technology factors were responsible for McAfee's software problem?
- What was the business impact of this software problem, both for McAfee and for its customers?
- If you were a McAfee enterprise customer, would you consider McAfee's response to the problem be acceptable? Why or why not?
- What should McAfee do in the future to avoid similar problems?



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

Business Value of Security and Control

- **Failed computer systems can lead to significant or total loss of business function**
- **Firms now more vulnerable than ever**
 - **Confidential personal and financial data**
 - **Trade secrets, new products, strategies**
- **A security breach may cut into firm's market value almost immediately**
- **Inadequate security and controls also bring forth issues of liability**



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

Business Value of Security and Control

- **Legal and regulatory requirements for electronic records management and privacy protection**
 - **HIPAA:** Medical security and privacy rules and procedures
 - **Gramm-Leach-Bliley Act:** Requires financial institutions to ensure the security and confidentiality of customer data
 - **Sarbanes-Oxley Act:** Imposes responsibility on companies and their management to safeguard the accuracy and integrity of financial information that is used internally and released externally



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

Business Value of Security and Control

- **Electronic evidence**
 - **Evidence for white collar crimes often in digital form**
 - Data on computers, e-mail, instant messages, e-commerce transactions
 - **Proper control of data can save time and money when responding to legal discovery request**
- **Computer forensics:**
 - **Scientific collection, examination, authentication, preservation, and analysis of data from computer storage media for use as evidence in court of law**
 - **Includes recovery of ambient and hidden data**



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

Establishing a Framework for Security and Control

- **Information systems controls**
 - Manual and automated controls
 - General and application controls
- **General controls**
 - Govern design, security, and use of computer programs and security of data files in general throughout organization's information technology infrastructure.
 - Apply to all computerized applications
 - Combination of hardware, software, and manual procedures to create overall control environment



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

Establishing a Framework for Security and Control

- **Types of general controls**
 - Software controls
 - Hardware controls
 - Computer operations controls
 - Data security controls
 - Implementation controls
 - Administrative controls



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

Establishing a Framework for Security and Control

- **Application controls**
 - Specific controls unique to each computerized application, such as payroll or order processing
 - Include both automated and manual procedures
 - Ensure that only authorized data are completely and accurately processed by that application
 - Include:
 - Input controls
 - Processing controls
 - Output controls



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

Establishing a Framework for Security and Control

- **Risk assessment:** Determines level of risk to firm if specific activity or process is not properly controlled
 - Types of threat
 - Probability of occurrence during year
 - Potential losses, value of threat
 - Expected annual loss

EXPOSURE	PROBABILITY	LOSS RANGE (AVG)	EXPECTED ANNUAL LOSS
Power failure	30%	\$5K - \$200K (\$102,500)	\$30,750
Embezzlement	5%	\$1K - \$50K (\$25,500)	\$1,275
User error	98%	\$200 - \$40K (\$20,100)	\$19,698



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

Establishing a Framework for Security and Control

- **Security policy**
 - Ranks information risks, identifies acceptable security goals, and identifies mechanisms for achieving these goals
 - **Drives other policies**
 - Acceptable use policy (AUP)
 - Defines acceptable uses of firm's information resources and computing equipment
 - Authorization policies
 - Determine differing levels of user access to information assets



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

Establishing a Framework for Security and Control

- **Identity management**
 - **Business processes and tools to identify valid users of system and control access**
 - Identifies and authorizes different categories of users
 - Specifies which portion of system users can access
 - Authenticating users and protects identities
 - **Identity management systems**
 - Captures access rules for different levels of users



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

System Vulnerability and Abuse

SECURITY PROFILES FOR A PERSONNEL SYSTEM

These two examples represent two security profiles or data security patterns that might be found in a personnel system. Depending on the security profile, a user would have certain restrictions on access to various systems, locations, or data in an organization.

FIGURE 8-3

SECURITY PROFILE 1	
User: Personnel Dept. Clerk	
Location: Division 1	
Employee Identification Codes with This Profile: 00753, 27834, 37665, 44116	
Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read and Update
• Medical history data	None
• Salary	None
• Pensionable earnings	None

SECURITY PROFILE 2	
User: Divisional Personnel Manager	
Location: Division 1	
Employee Identification Codes with This Profile: 27321	
Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read Only



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

Establishing a Framework for Security and Control

- **Disaster recovery planning:** Devises plans for restoration of disrupted services
- **Business continuity planning:** Focuses on restoring business operations after disaster
 - **Both types of plans needed to identify firm's most critical systems**
 - **Business impact analysis to determine impact of an outage**
 - **Management must determine which systems restored first**



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

Establishing a Framework for Security and Control

- **MIS audit**
 - Examines firm's overall security environment as well as controls governing individual information systems
 - Reviews technologies, procedures, documentation, training, and personnel.
 - May even simulate disaster to test response of technology, IS staff, other employees.
 - Lists and ranks all control weaknesses and estimates probability of their occurrence.
 - Assesses financial and organizational impact of each threat



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

System Vulnerability and Abuse

SAMPLE AUDITOR'S LIST OF CONTROL WEAKNESSES

This chart is a sample page from a list of control weaknesses that an auditor might find in a loan system in a local commercial bank. This form helps auditors record and evaluate control weaknesses and shows the results of discussing those weaknesses with management, as well as any corrective actions taken by management.

FIGURE 8-4

Function: Loans Location: Peoria, IL		Prepared by: J. Ericson Date: June 16, 2011		Received by: T. Benson Review date: June 28, 2011	
Nature of Weakness and Impact	Chance for Error/Abuse		Notification to Management		
	Yes/ No	Justification	Report date	Management response	
User accounts with missing passwords	Yes	Leaves system open to unauthorized outsiders or attackers	5/10/11	Eliminate accounts without passwords	
Network configured to allow some sharing of system files	Yes	Exposes critical system files to hostile parties connected to the network	5/10/11	Ensure only required directories are shared and that they are protected with strong passwords	
Software patches can update production programs without final approval from Standards and Controls group	No	All production programs require management approval; Standards and Controls group assigns such cases to a temporary production status			



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

Technologies and Tools for Protecting Information Resources

- **Identity management software**
 - Automates keeping track of all users and privileges
 - Authenticates users, protecting identities, controlling access
- **Authentication**
 - Password systems
 - Tokens
 - Smart cards
 - Biometric authentication



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

Technologies and Tools for Protecting Information Resources

- **Firewall:**
 - **Combination of hardware and software that prevents unauthorized users from accessing private networks**
 - **Technologies include:**
 - Static packet filtering
 - Network address translation (NAT)
 - Application proxy filtering



Management Information Systems

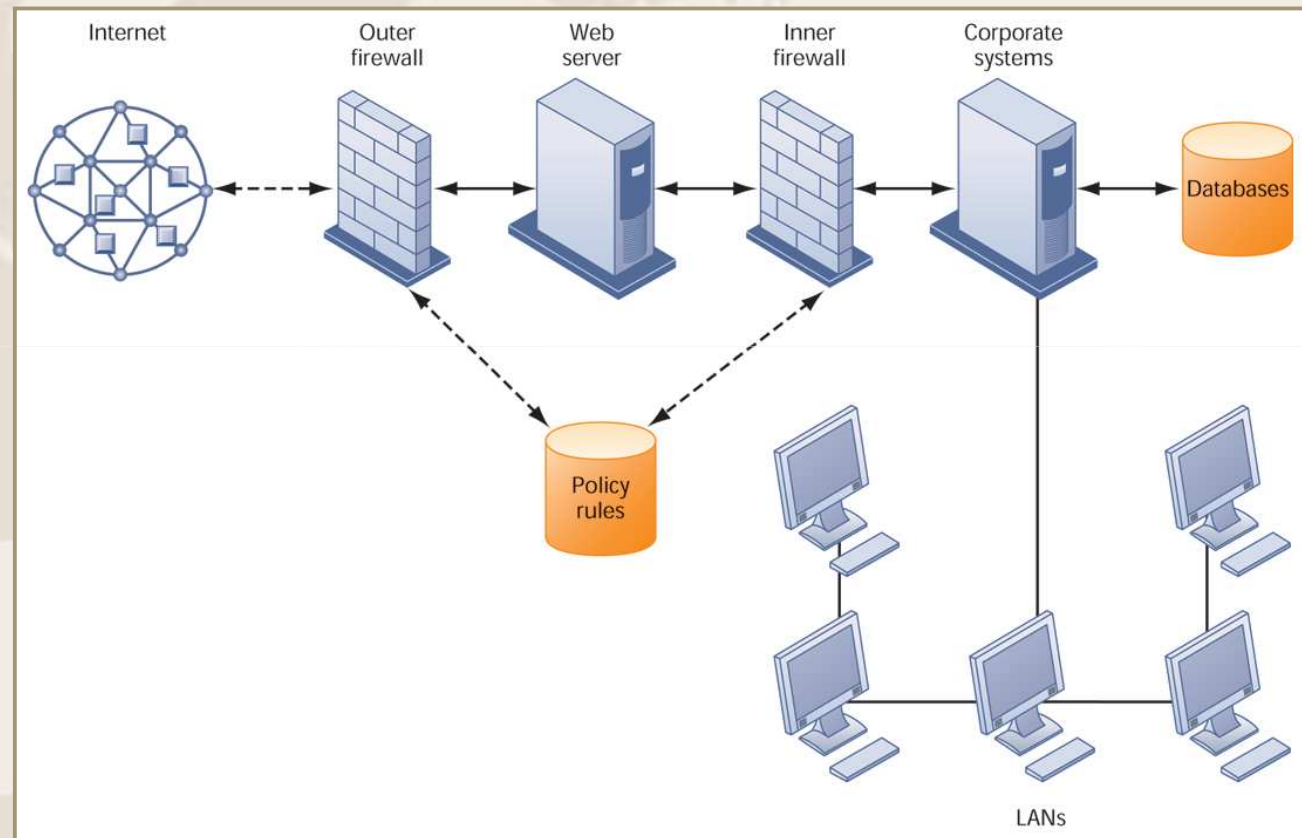
CHAPTER 8: SECURING INFORMATION SYSTEMS

Technologies and Tools for Protecting Information Resources

A CORPORATE FIREWALL

The firewall is placed between the firm's private network and the public Internet or another distrusted network to protect against unauthorized traffic.

FIGURE 8-5





Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

Technologies and Tools for Protecting Information Resources

- **Intrusion detection systems:**
 - Monitor hot spots on corporate networks to detect and deter intruders
 - Examines events as they are happening to discover attacks in progress
- **Antivirus and antispyware software:**
 - Checks computers for presence of malware and can often eliminate it as well
 - Require continual updating
- **Unified threat management (UTM) systems**



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

Technologies and Tools for Protecting Information Resources

- **Securing wireless networks**
 - **WEP security can provide some security by**
 - Assigning unique name to network's SSID and not broadcasting SSID
 - Using it with VPN technology
 - **Wi-Fi Alliance finalized WAP2 specification, replacing WEP with stronger standards**
 - Continually changing keys
 - Encrypted authentication system with central server



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

Technologies and Tools for Protecting Information Resources

- **Encryption:**
 - Transforming text or data into cipher text that cannot be read by unintended recipients
 - Two methods for encryption on networks
 - Secure Sockets Layer (SSL) and successor Transport Layer Security (TLS)
 - Secure Hypertext Transfer Protocol (S-HTTP)



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

Technologies and Tools for Protecting Information Resources

- **Two methods of encryption**
 - **Symmetric key encryption**
 - Sender and receiver use single, shared key
 - **Public key encryption**
 - Uses two, mathematically related keys: Public key and private key
 - Sender encrypts message with recipient's public key
 - Recipient decrypts with private key



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

Technologies and Tools for Protecting Information Resources

PUBLIC KEY ENCRYPTION

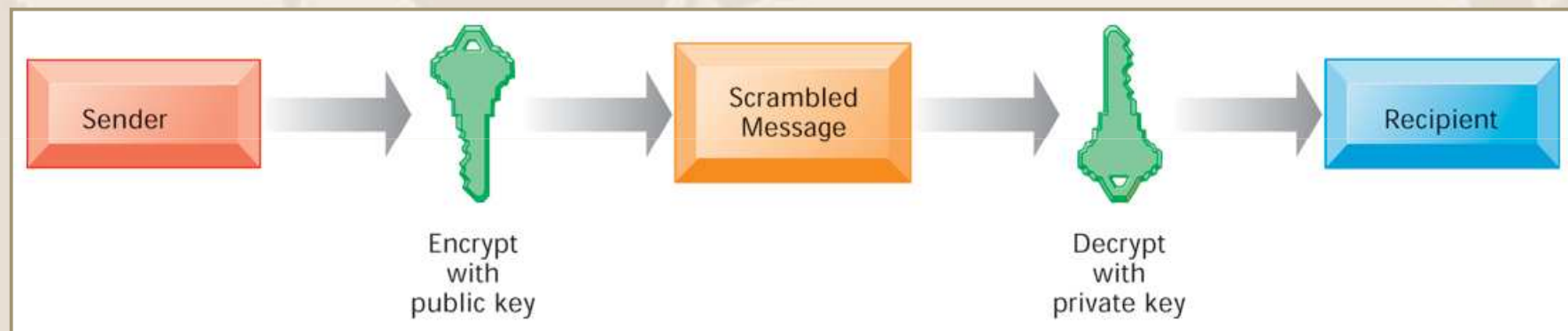


FIGURE 8-6

A public key encryption system can be viewed as a series of public and private keys that lock data when they are transmitted and unlock the data when they are received. The sender locates the recipient's public key in a directory and uses it to encrypt a message. The message is sent in encrypted form over the Internet or a private network. When the encrypted message arrives, the recipient uses his or her private key to decrypt the data and read the message.



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

Technologies and Tools for Protecting Information Resources

- **Digital certificate:**
 - Data file used to establish the identity of users and electronic assets for protection of online transactions
 - Uses a trusted third party, certification authority (CA), to validate a user's identity
 - CA verifies user's identity, stores information in CA server, which generates encrypted digital certificate containing owner ID information and copy of owner's public key
- **Public key infrastructure (PKI)**
 - Use of public key cryptography working with certificate authority
 - Widely used in e-commerce



Management Information Systems

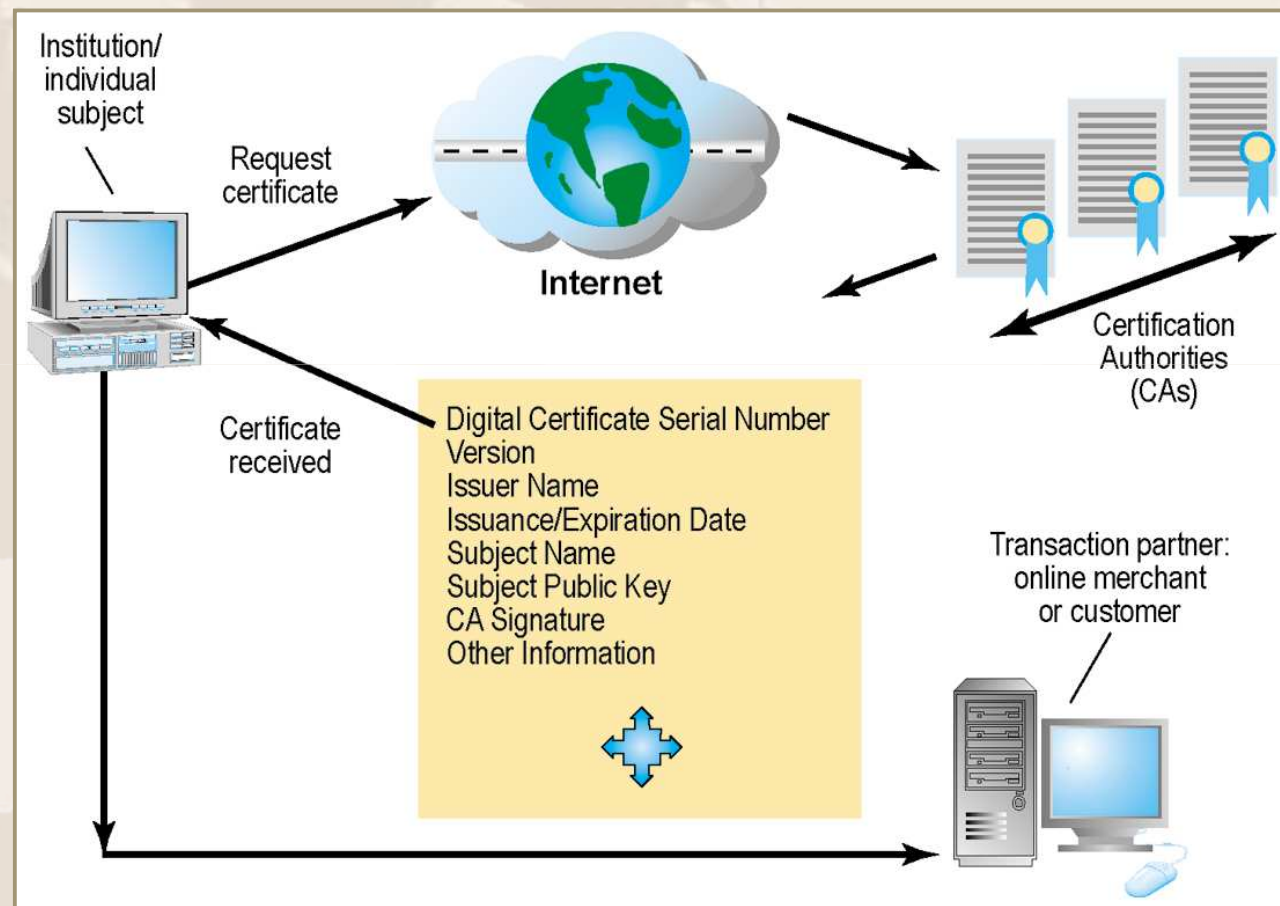
CHAPTER 8: SECURING INFORMATION SYSTEMS

Technologies and Tools for Protecting Information Resources

DIGITAL CERTIFICATES

Digital certificates help establish the identity of people or electronic assets. They protect online transactions by providing secure, encrypted, online communication.

FIGURE 8-7





Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

Technologies and Tools for Protecting Information Resources

- **Ensuring system availability**
 - Online transaction processing requires 100% availability, no downtime
- **Fault-tolerant computer systems**
 - For continuous availability, e.g. stock markets
 - Contain redundant hardware, software, and power supply components that create an environment that provides continuous, uninterrupted service
- **High-availability computing**
 - Helps recover quickly from crash
 - Minimizes, does not eliminate downtime



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

Technologies and Tools for Protecting Information Resources

- **Recovery-oriented computing**
 - Designing systems that recover quickly with capabilities to help operators pinpoint and correct of faults in multi-component systems
- **Controlling network traffic**
 - Deep packet inspection (DPI)
 - Video and music blocking
- **Security outsourcing**
 - Managed security service providers (MSSPs)



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

Technologies and Tools for Protecting Information Resources

- **Security in the cloud**
 - Responsibility for security resides with company owning the data
 - Firms must ensure providers provides adequate protection
 - Service level agreements (SLAs)
- **Securing mobile platforms**
 - Security policies should include and cover any special requirements for mobile devices
 - E.g. updating smart phones with latest security patches, etc.



Management Information Systems

CHAPTER 8: SECURING INFORMATION SYSTEMS

Technologies and Tools for Protecting Information Resources

HOW SECURE IS THE CLOUD?

Read the Interactive Session and discuss the following questions

- What security and control problems are described in this case?
- What people, organization, and technology factors contribute to these problems?
- How secure is cloud computing? Explain your answer.
- If you were in charge of your company's information systems department, what issues would you want to clarify with prospective vendors?
- Would you entrust your corporate systems to a cloud computing provider? Why or why not?



Management Information Systems

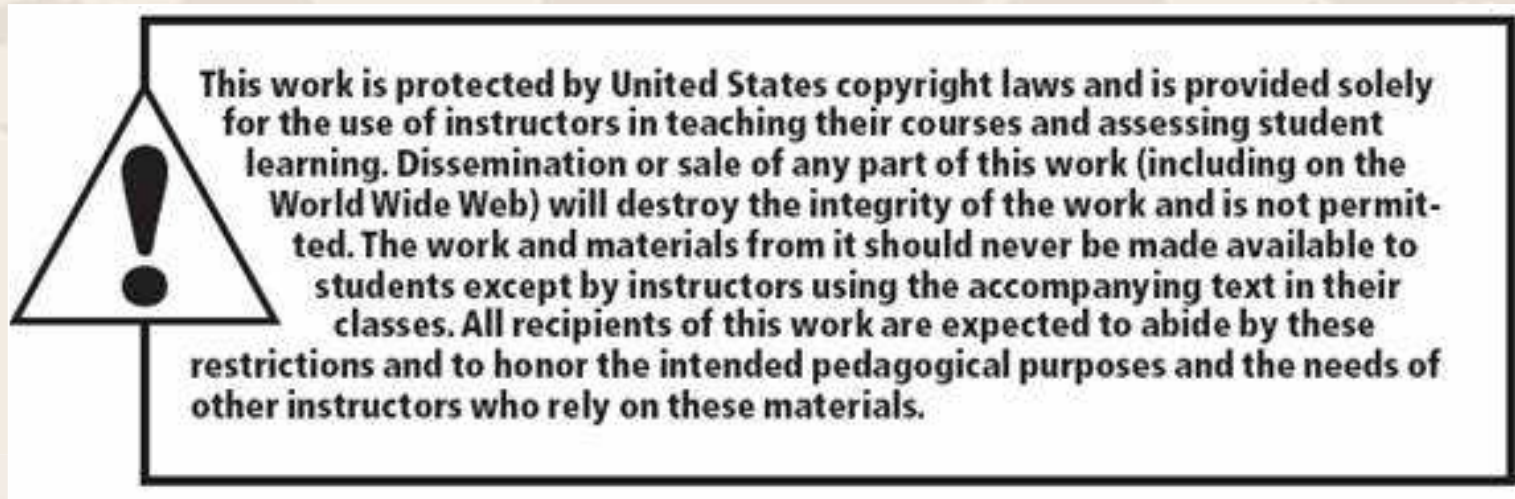
CHAPTER 8: SECURING INFORMATION SYSTEMS

Technologies and Tools for Protecting Information Resources

- **Ensuring software quality**
 - **Software metrics: Objective assessments of system in form of quantified measurements**
 - Number of transactions
 - Online response time
 - Payroll checks printed per hour
 - Known bugs per hundred lines of code
 - **Early and regular testing**
 - **Walkthrough: Review of specification or design document by small group of qualified people**
 - **Debugging: Process by which errors are eliminated**



Management Information Systems



All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher. Printed in the United States of America.

Copyright © 2011 Pearson Education, Inc.
Publishing as Prentice Hall