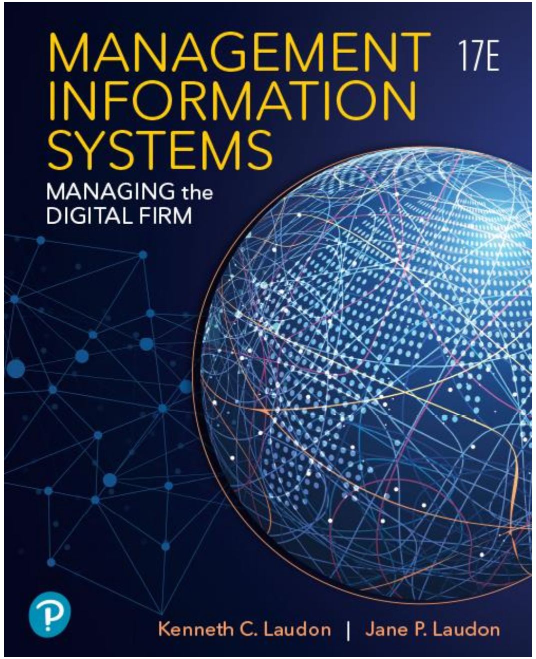
Management Information Systems: Managing the Digital Firm

Seventeenth Edition



Chapter 8

Securing Information Systems

Learning Objectives

8.1 Why are information systems vulnerable to destruction, error, and abuse?

8.2 What is the business value of security and control?

8.3 What are the components of an organizational framework for security and control?

8.4 What are the most important tools and technologies for safeguarding information resources?

8.5 How will MIS help my career?

Video Cases

- Case 1: Stuxnet and Cyberwarfare
- Case 2: Cyberespionage: The Chinese Threat
- Instructional Video 1: Sony PlayStation Hacked; Data Stolen from 77 Million Users
- Instructional Video 2: Meet the Hackers: Anonymous Statement on Hacking Sony

The Electric Power Grid Becomes a Cyberwarfare Battleground (1 of 2)

- Problem
  - Large complex infrastructure
  - Numerous access points
  - Uneven security
- Solutions
  - Issue security standards and guidelines
  - Monitor grid for attacks
  - U.S. government countermeasures
  - Education about malware and social engineering tactics

The Electric Power Grid Becomes a Cyberwarfare Battleground (2 of 2)

- Hackers took advantage of uneven security and controls to attack U.S. power grid
- Demonstrates vulnerabilities in information technology systems
- Illustrates some of the reasons organizations need to pay special attention to information system security

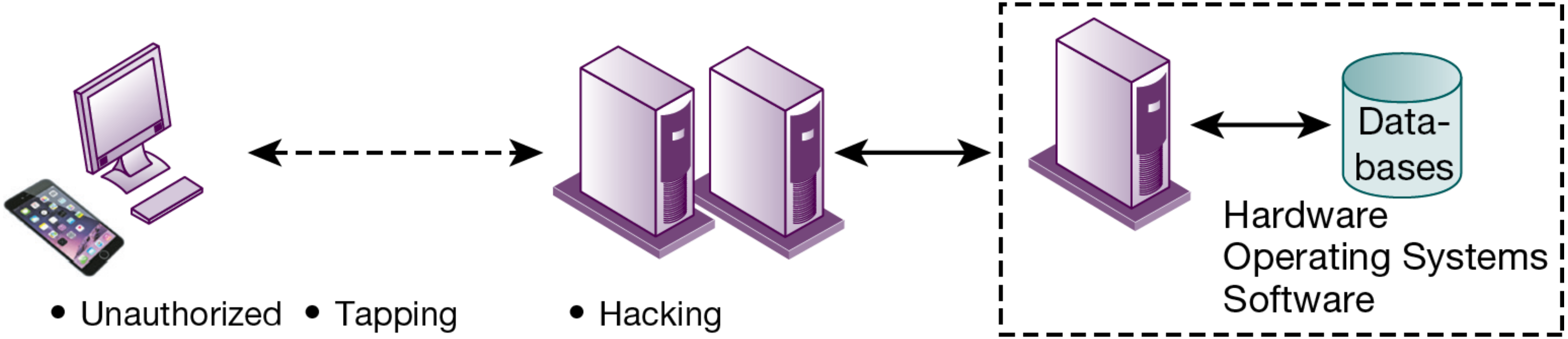
Why Systems are Vulnerable (1 of 2)

- 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

Why Systems are Vulnerable (2 of 2)

- 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

Figure 8.1 Contemporary Security Challenges and Vulnerabilities



Client (User)

- Unauthorized access
- Errors

Communications Lines

- Tapping
- Sniffing
- Message alteration
- Theft and fraud
- Radiation

Corporate Servers

- Hacking
- Malware
- Theft and fraud
- Vandalism
- Denial-of-service attacks

Corporate Systems

Data-bases

Hardware
Operating Systems
Software

- Theft of data
- Copying data
- Alteration of data
- Hardware failure
- Software failure

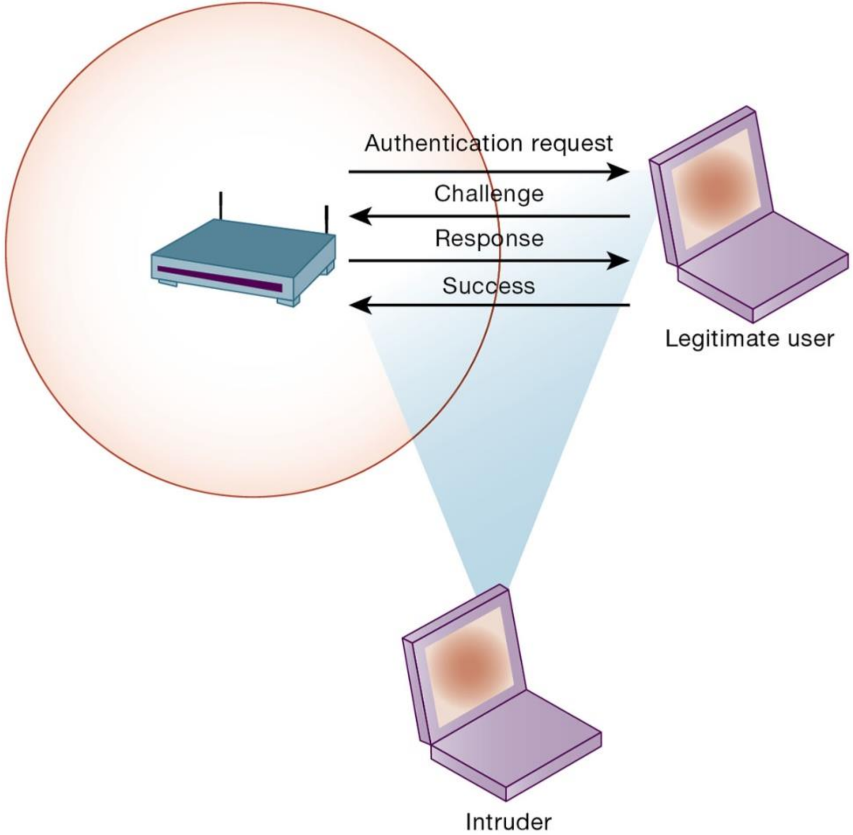
Internet Vulnerabilities

- Network open to anyone; size means abuses can have wide impact
- Corporate networks linked to Internet more vulnerable
- E-mail, IM, and P2P increase vulnerability
  - Email: attachments with malicious software; can be used to transmit trade secrets, confidential data
  - IM: back door into a secure network
  - P2P: can transmit malicious software, expose corporate data

Wireless Security Challenges

- Bluetooth and Wi-Fi networks susceptible to hacking
  - Radio frequency bands easy to scan
  - SSIDs (service set identifiers)
    - Identify access points, broadcast multiple times, can be identified by sniffer programs
- War driving
  - Eavesdroppers drive by buildings and try to detect SSID and gain access to network and resources
  - Once access point is breached, intruder can gain access to networked drives and files
- Rogue access points

Figure 8.2 Wi-Fi Security Challenges



Malicious Software: Viruses, Worms, Trojan Horses, and Spyware (1 of 2)

- Malware (malicious software)
- Viruses
- Worms
- Worms and viruses spread by
  - Downloads and drive-by downloads
  - E-mail, IM attachments
- Mobile device malware
- Social network malware

Malicious Software: Viruses, Worms, Trojan Horses, and Spyware (2 of 2)

- Trojan horse
- SQL injection attacks
- Ransomware
- Spyware
  - Key loggers
  - Other types
    - Reset browser home page
    - Redirect search requests
    - Slow computer performance by taking up memory

Hackers and Computer Crime (1 of 4)

- Hackers vs. crackers
- Activities include:
  - System intrusion
  - System damage
  - Cybervandalism
    - Intentional disruption, defacement, destruction of website or corporate information system
- Spoofing and sniffing

Hackers and Computer Crime (2 of 4)

- Denial-of-service attacks (DoS)
- Distributed denial-of-service attacks (DDoS)
- Botnets
- Spam

Hackers and Computer Crime (3 of 4)

- Computer crime defined by U.S. Department of Justice 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
- Computer may be instrument of crime

Hackers and Computer Crime (4 of 4)

- Identity theft
  - Phishing
  - Evil twins
  - Pharming
- Click fraud
- Cyberterrorism
- Cyberwarfare

Internal Threats: Employees

- Security threats often originate inside an organization
- Inside knowledge
- Sloppy security procedures
  - User lack of knowledge
- Social engineering
- Both end users and information systems specialists are sources of risk

Interactive Session: Technology: Capital One: A Big Bank Heist from the Cloud

- Class discussion
  - What management, organization, and technology factors were responsible for the Capitol One hack?
  - Was this an insider hack? Explain your answer.
  - What steps could have been taken to prevent the Capital One hack?
  - Should companies handling sensitive data use cloud computing services? Explain your answer.

Software Vulnerability

- Commercial software contains flaws that create security vulnerabilities
  - Bugs (program code defects)
  - Zero defects cannot be achieved
  - Flaws can open networks to intruders
- Zero-day vulnerabilities
- Patches and patch management: repair software flaws
- Vulnerabilities in microprocessor design: Spectre, Meltdown

What is the Business Value of Security and Control?

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

Legal and Regulatory Requirements for Electronic Records Management

- 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

Electronic Evidence and Computer Forensics

- Electronic evidence
  - Evidence for white collar crimes often in digital form
  - 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
  - Recovery of ambient data

Information Systems Controls

- May be automated or manual
- General controls
  - Govern design, security, and use of computer programs and security of data files in general throughout organization
  - Software controls, hardware controls, computer operations controls, data security controls, system development controls, administrative controls,
- Application controls
  - Controls unique to each computerized application
  - Input controls, processing controls, output controls

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

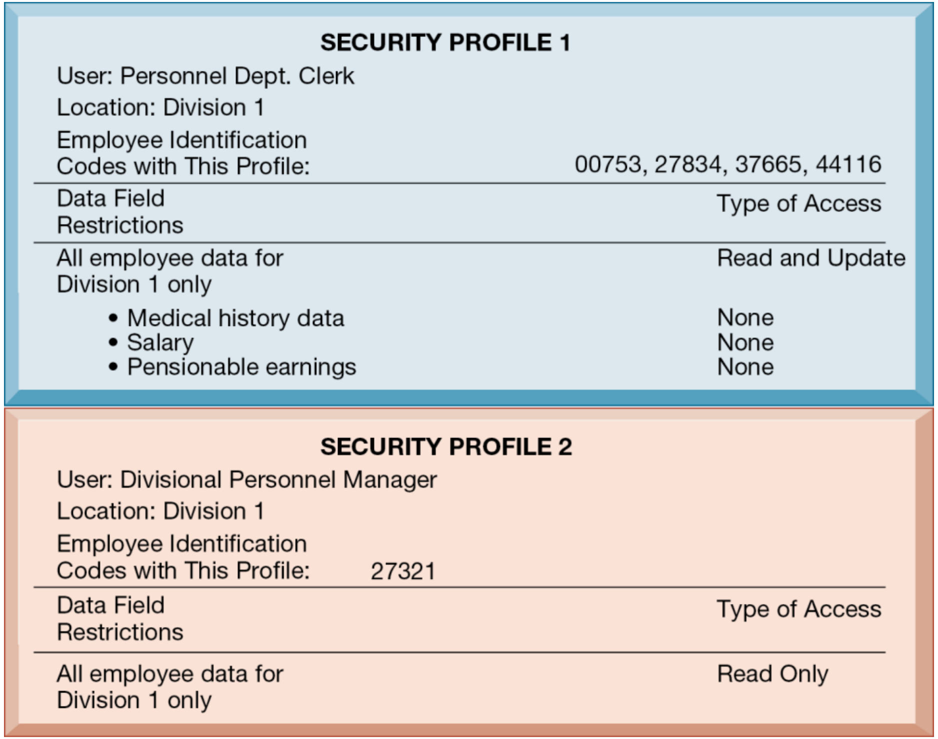
Table 8.5 Online Order Processing Risk Assessment

Exposure	Probability of Occurrence	Loss Range (Average) ($)	Expected Annual Loss ($)
Power failure	30%	$5,000 − $200,000 ($102,500)	$30,750
Embezzlement	5%	$1,000 − $50,000 ($25,500)	$1,275
User error	98%	$200 − $40,000 ($20,100)	$19,698

Security Policy

- Ranks information risks, identifies security goals and mechanisms for achieving these goals
- Drives other policies
- Acceptable use policy (AUP)
  - Defines acceptable uses of firm’s information resources and computing equipment
- Identity management
  - Identifying valid users
  - Controlling access

Figure 8.3 Access Rules for a Personnel System



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

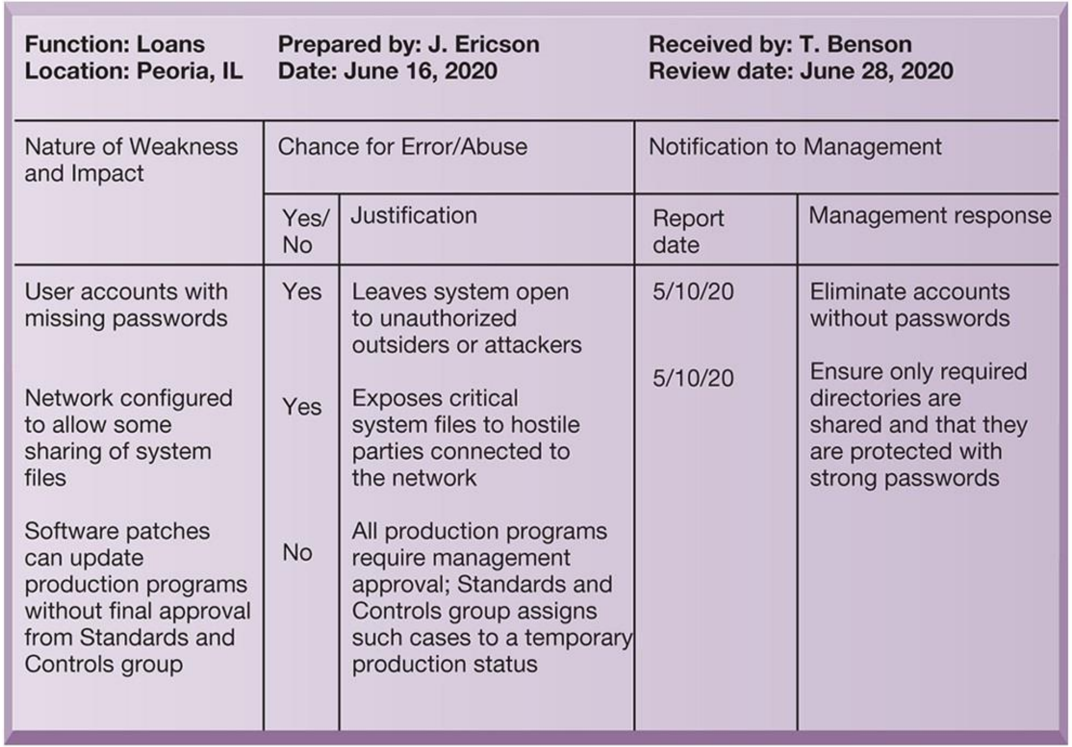
Disaster Recovery Planning and Business Continuity Planning

- 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

The Role of Auditing

- Information systems audit
  - Examines firm’s overall security environment as well as controls governing individual information systems
- Security audits
  - Review technologies, procedures, documentation, training, and personnel
  - May even simulate disaster to test responses
- List and rank control weaknesses and the probability of occurrence
- Assess financial and organizational impact of each threat

Figure 8.4 Sample Auditor’s List of Control Weaknesses



Function: Loans
Location: Peoria, IL

Prepared by: J. Ericson
Date: June 16, 2020

Received by: T. Benson
Review date: June 28, 2020

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	5/10/20	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	5/10/20	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		

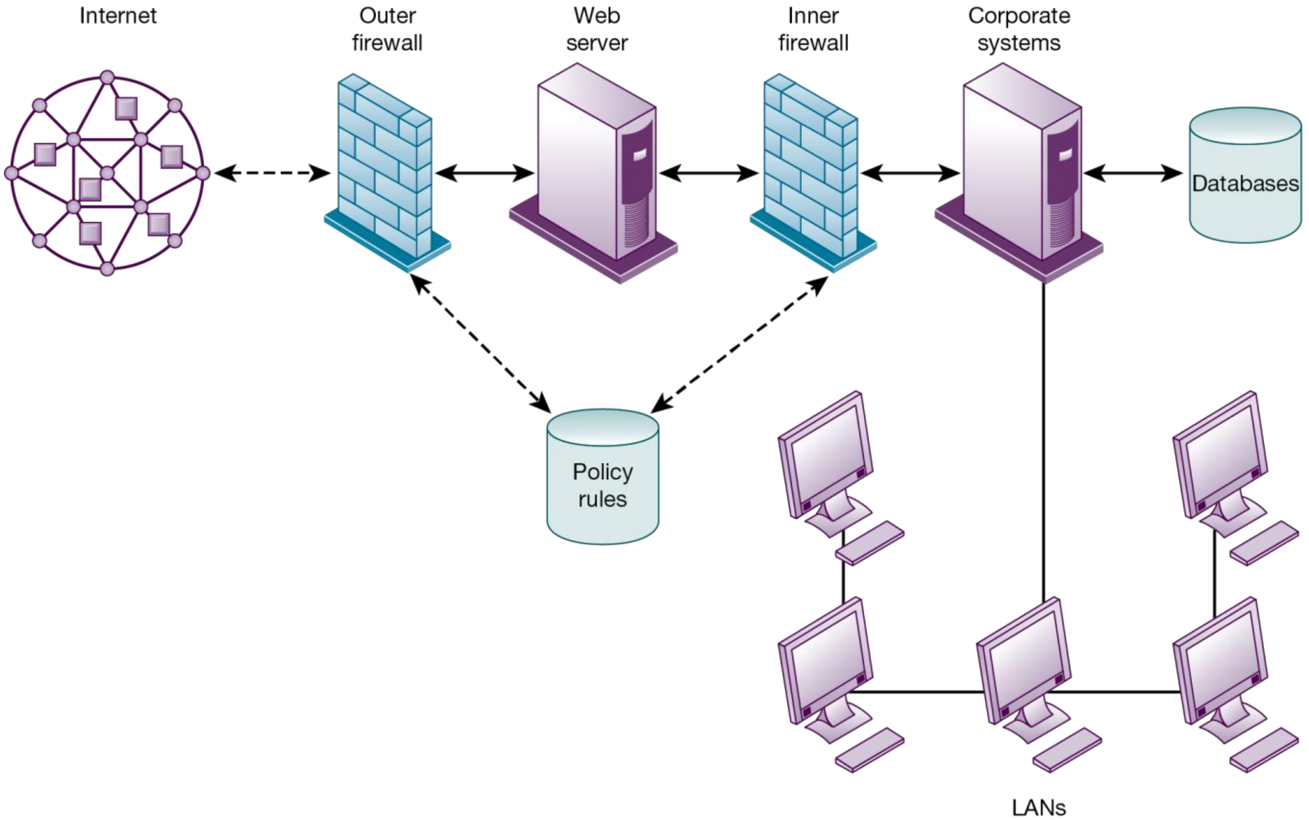
Tools and Technologies for Safeguarding Information Systems (1 of 3)

- 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
  - Two-factor authentication

Tools and Technologies for Safeguarding Information Systems (2 of 3)

- Firewall
  - Combination of hardware and software that prevents unauthorized users from accessing private networks
  - Packet filtering
  - Stateful inspection
  - Network address translation (NAT)
  - Application proxy filtering

Figure 8.5 A Corporate Firewall



Pearson

Tools and Technologies for Safeguarding Information Systems (3 of 3)

- Intrusion detection system
  - Monitors hot spots on corporate networks to detect and deter intruders
- Antimalware and antispyware software
  - Checks computers for presence of malware and can often eliminate it as well
  - Requires continual updating
- Unified threat management (UTM) systems

Securing Wireless Networks

- WEP security
  - Static encryption keys are relatively easy to crack
  - Improved if used in conjunction with VPN
- WPA2 specification
  - Replaces WEP with stronger standards
  - Continually changing, longer encryption keys
- WPA3 is most recent specification, with even stronger encryption

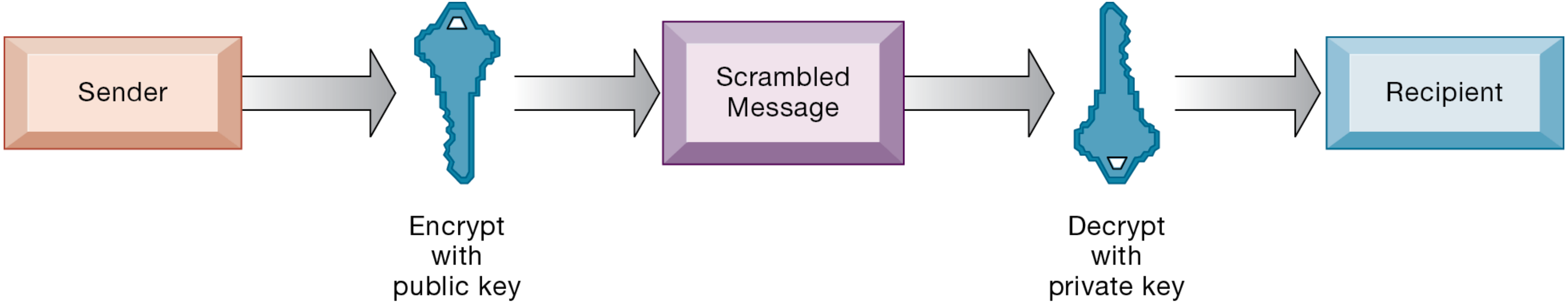
Encryption and Public Key Infrastructure (1 of 3)

- 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)

Encryption and Public Key Infrastructure (2 of 3)

- Two methods of encryption of messages
  - 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

Figure 8.6 Public Key Encryption



Pearson

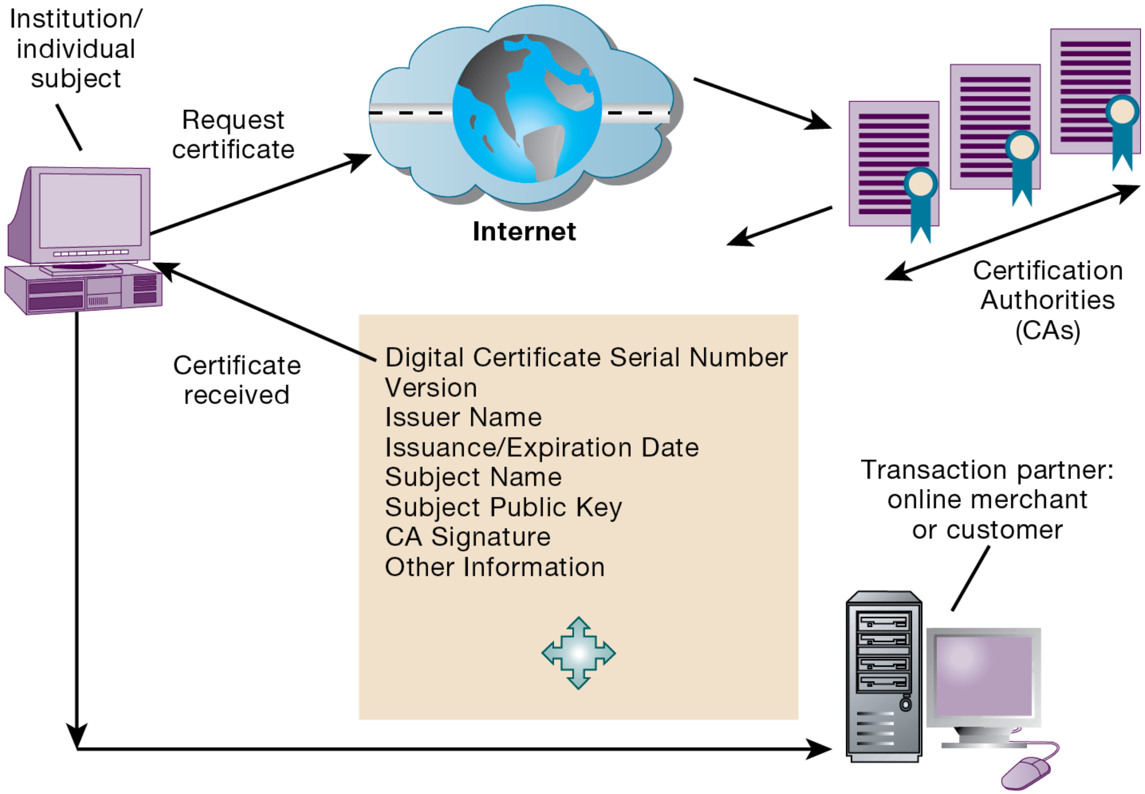
Encryption and Public Key Infrastructure (3 of 3)

- 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

Securing Transactions with Blockchain

- Secure transaction database
- Encryption used to verify users and transactions
- Decentralized
- Records cannot be changed
- Blockchain has some vulnerabilities requiring attention to security and controls

Figure 8.7 Digital Certificates



Institution/ individual subject

Request certificate

Internet

Certification Authorities (CAs)

Certificate received

Digital Certificate Serial Number
Version
Issuer Name
Issuance/Expiration Date
Subject Name
Subject Public Key
CA Signature
Other Information

Transaction partner: online merchant or customer

Ensuring System Availability

- Online transaction processing requires 100% availability
- Fault-tolerant computer systems
  - Contain redundant hardware, software, and power supply components that create an environment that provides continuous, uninterrupted service
- Security outsourcing
  - Managed security service providers (MSSPs)

Achieving Digital Resiliency

- Deals with how to maintain and increase resilience of organization and its business processes
- Calls attention to managerial and organizational issues in addition to IT infrastructure
- Single weak link can cause an outage if resiliency has not been explicitly designed in, measured, and tested

Interactive Session: Management: PayPal Ups Its Digital Resiliency

- Class discussion
  - Why is digital resiliency so important for a company such as PayPal?
  - How did PayPal benefit from measuring its digital resiliency? What issues did it address?
  - What is the role of management and organizational issues in making an organization’s IT infrastructure more resilient?

Security Issues for Cloud Computing and the Mobile Digital Platform (1 of 2)

- Security in the cloud
  - Responsibility for security resides with company owning the data
  - Firms must ensure providers provide adequate protection:
    - Where data are stored
    - Meeting corporate requirements, legal privacy laws
    - Segregation of data from other clients
    - Audits and security certifications
  - Service level agreements (SLAs)

Security Issues for Cloud Computing and the Mobile Digital Platform (2 of 2)

- Securing mobile platforms
  - Security policies should include and cover any special requirements for mobile devices
    - Guidelines for use of platforms and applications
  - Mobile device management tools
    - Authorization
    - Inventory records
    - Control updates
    - Lock down/erase lost devices
    - Encryption
  - Software for segregating corporate data on devices

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

How Will MIS Help My Career?

- The Company: No. 1 Value Supermarkets
- Position Description: Identity access and management support specialist, entry-level
- Job Requirements
- Interview Questions
- Author Tips

Copyright