



# E-commerce

business. technology. society.

*Second Edition*

**Kenneth C. Laudon**  
**Carol Guercio Traver**



# Chapter 5

## Security and Encryption



## **The Merchant Pays Class Discussion**

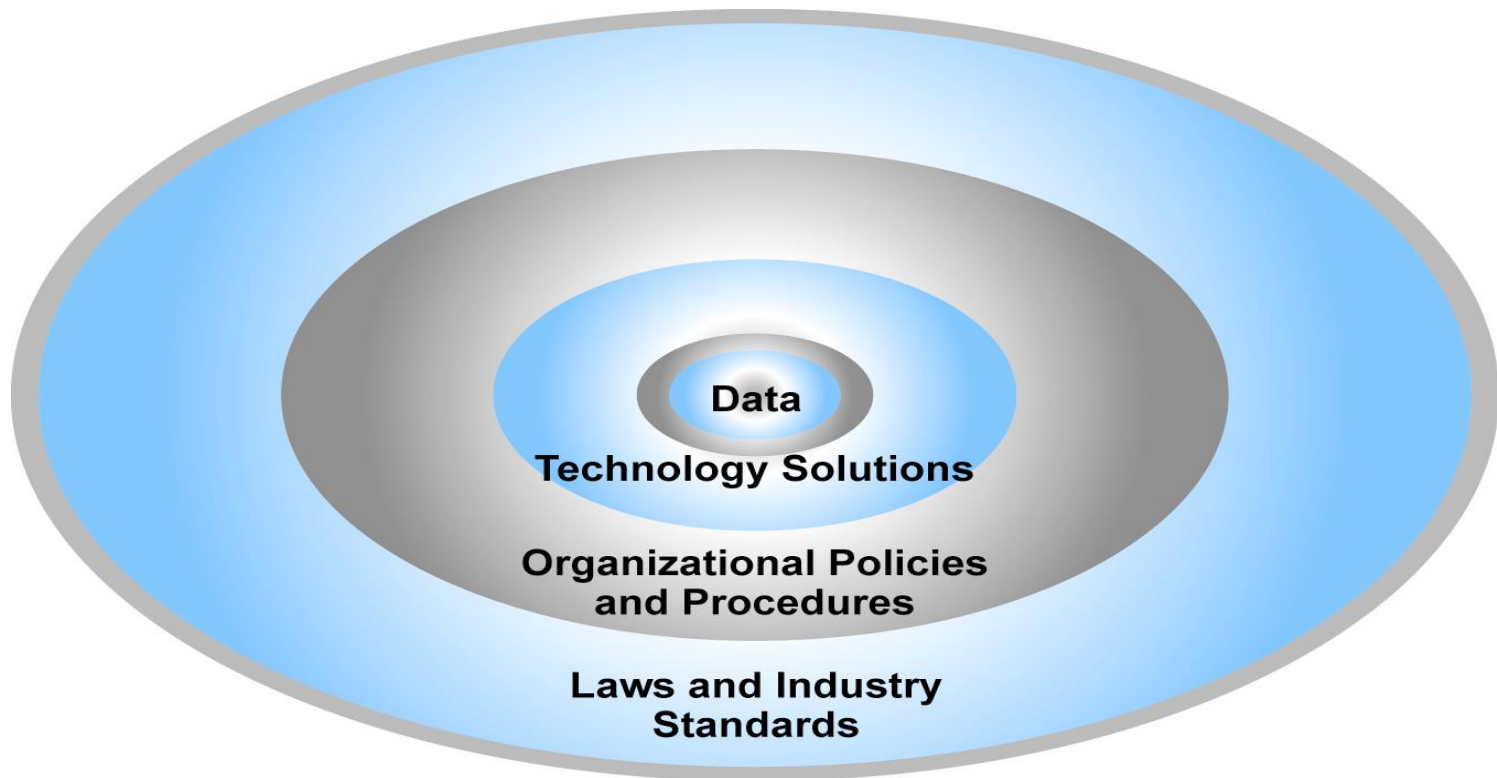
- Why are offline credit card security procedures not applicable in online environment?
- What new techniques are available to merchants that would reduce credit card fraud?
- Why should the merchant bear the risk of online credit purchases? Why not the issuing banks?
- What other steps can merchants take to reduce credit card fraud at their sites?
- Why are merchants reluctant to add additional security measures?

# The E-commerce Security Environment: The Scope of the Problem

- Overall size of cybercrime unclear; amount of losses significant but stable; individuals face new risks of fraud that may involve substantial uninsured losses
  - Symantec: Over 50 overall attacks a day against business firms between July 2004–June 2005
  - 2005 Computer Security Institute survey
    - 56% of respondents had detected breaches of computer security within last 12 months and 91% of these suffered financial loss as a result
    - Over 35% experienced denial of service attacks
    - Over 75% detected virus attacks

# The E-commerce Security Environment

Figure 5.4, Page 253



# Dimensions of E-commerce Security

- Integrity: ability to ensure that information being displayed on a Web site or transmitted/received over the Internet has not been altered in any way by an unauthorized party
- Nonrepudiation: ability to ensure that e-commerce participants do not deny (repudiate) online actions
- Authenticity: ability to identify the identity of a person or entity with whom you are dealing on the Internet
- Confidentiality: ability to ensure that messages and data are available only to those authorized to view them
- Privacy: ability to control use of information a customer provides about himself or herself to merchant
- Availability: ability to ensure that an e-commerce site continues to function as intended

# Customer and Merchant Perspectives on the Different Dimensions of E-commerce Security

Table 5.1, Page 254

TABLE 5.1		CUSTOMER AND MERCHANT PERSPECTIVES ON THE DIFFERENT DIMENSIONS OF E-COMMERCE SECURITY	
DIMENSIONS	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE	
Integrity	Has information I transmit or receive been altered?	Has data on the site been altered without authorization? Is data being received from customers valid?	
Nonrepudiation	Can a party to an action with me later deny taking the action?	Can a customer deny ordering products?	
Authenticity	Who am I dealing with? How can I be assured that the person or entity is who they claim to be?	What is the real identity of the customer?	
Confidentiality	Can someone other than the intended recipient read my messages?	Are messages or confidential data accessible to anyone other than those authorized to view them?	
Privacy	Can I control the use of information about myself transmitted to an e-commerce merchant?	What use, if any, can be made of personal data collected as part of an e-commerce transaction? Is the personal information of customers being used in an unauthorized manner?	
Availability	Can I get access to the site?	Is the site operational?	



# The Tension Between Security and Other Values

- Security vs. ease of use: the more security measures that are added, the more difficult a site is to use, and the slower it becomes
- Security vs. desire of individuals to act anonymously



# Security Threats in the E-commerce Environment

- Three key points of vulnerability:
  - Client
  - Server
  - Communications channel

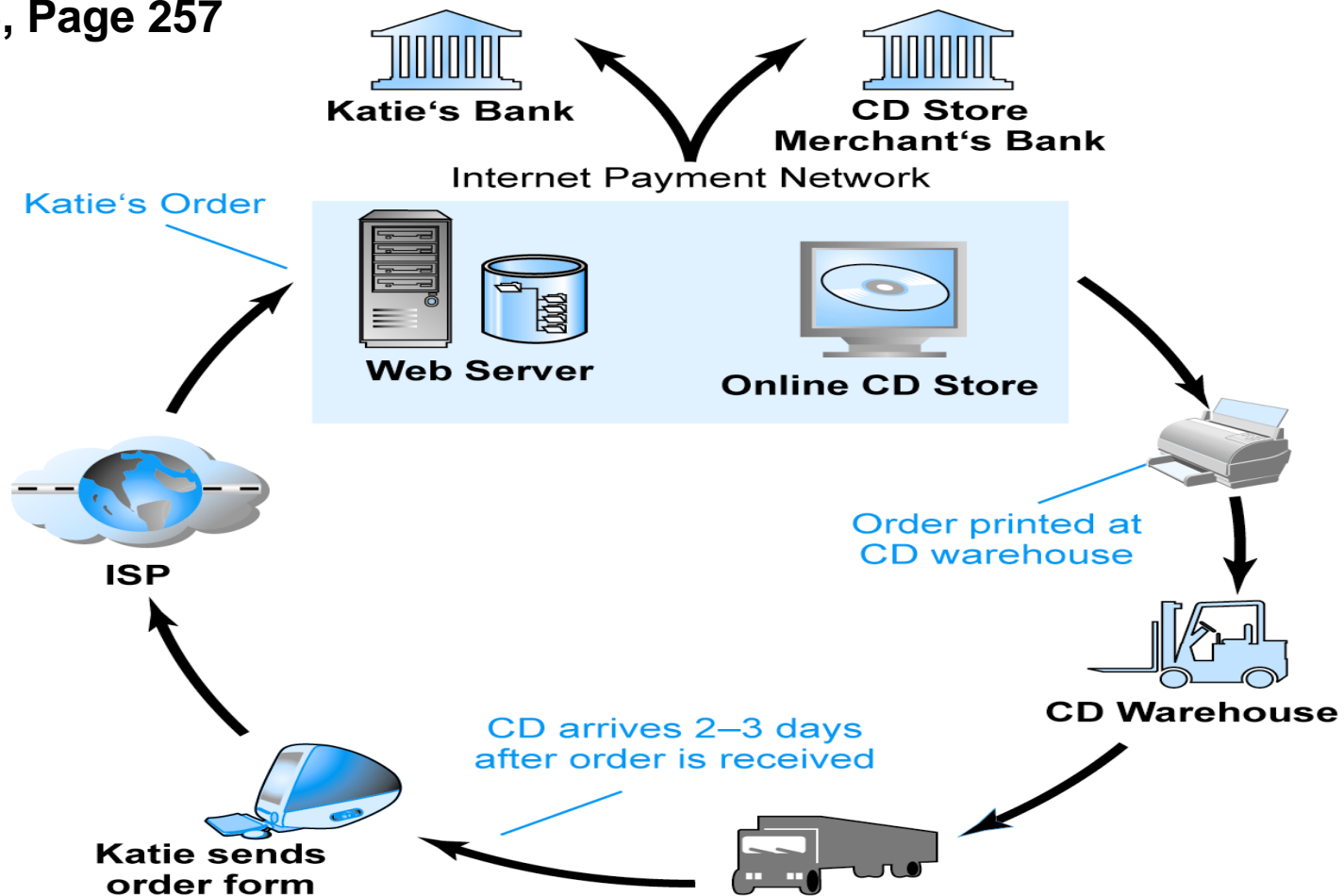


# Security Threats in the E-commerce Environment (cont'd)

- Most common threats:
  - Malicious code
  - Phishing
  - Hacking and cybervandalism
  - Credit card fraud/theft
  - Spoofing (pharming)
  - Denial of service attacks
  - Sniffing
  - Insider jobs
  - Poorly designed server and client software

# A Typical E-commerce Transaction

Figure 5.5, Page 257



SOURCE: Boncella, 2000.

# Vulnerable Points in an E-commerce Environment

Figure 5.6, Page 258

## Security Risks

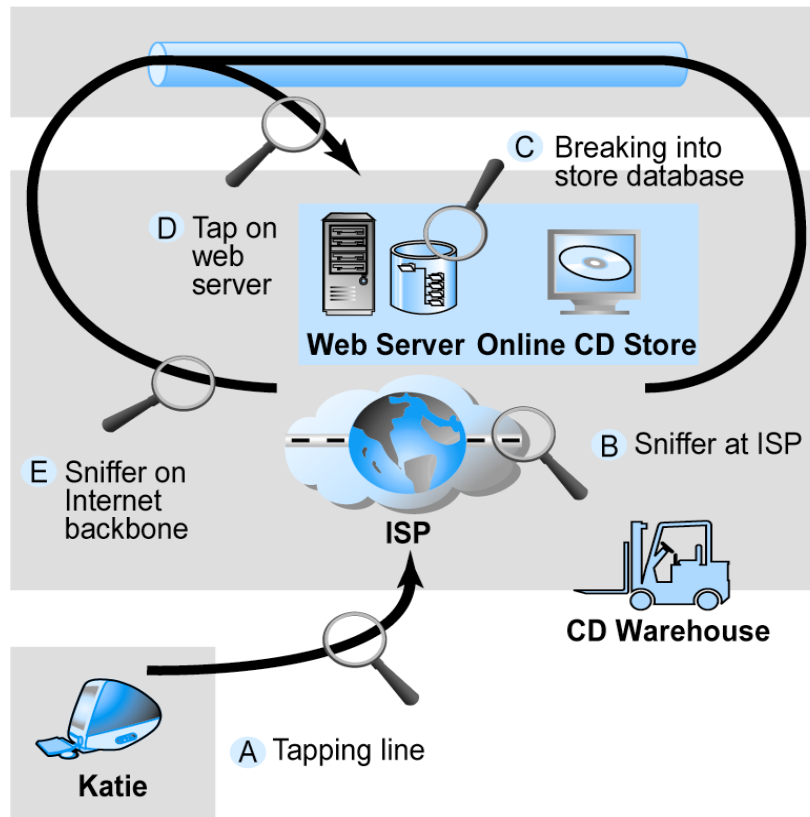
### Internet communications

### Servers

ISP  
Merchant  
Banks

### Clients

Business  
Home



SOURCE: Boncella, 2000.

# Malicious Code

- Viruses: computer program that has ability to replicate and spread to other files; most also deliver a “payload” of some sort (may be destructive or benign); include macro viruses, file-infecting viruses, and script viruses
- Worms: designed to spread from computer to computer
- Trojan horse: appears to be benign, but then does something other than expected
- Bots: can be covertly installed on computer; responds to external commands sent by the attacker



# Phishing

- Any deceptive, online attempt by a third party to obtain confidential information for financial gain
  - Most popular type: e-mail scam letter
  - One of fastest growing forms of e-commerce crime



# Hacking and Cybervandalism

- Hacker: Individual who intends to gain unauthorized access to computer systems
- Cracker: Used to denote hacker with criminal intent (two terms often used interchangeably)
- Cybervandalism: Intentionally disrupting, defacing or destroying a Web site
- Types of hackers include:
  - White hats
  - Black hats
  - Grey hats



# Credit Card Fraud

- Fear that credit card information will be stolen deters online purchases
- Hackers target credit card files and other customer information files on merchant servers; use stolen data to establish credit under false identity
- One solution: New identity verification mechanisms



# **Insight on Society: “Evil Twins” and “Pharming”: Keeping Up with the Hackers? Class Discussion**

- What are “evil twins” and “pharming”
- What is meant by “social engineering techniques?”
- What is the security weakness in the domain name system that permits pharming?
- What steps can users take to verify they are communicating with authentic sites and networks?



# Spooftng (Pharming)

- Misrepresenting oneself by using fake e-mail addresses or masquerading as someone else
- Threatens integrity of site; authenticity



# DoS and dDoS Attacks

- Denial of service (DoS) attack: Hackers flood Web site with useless traffic to inundate and overwhelm network
- Distributed denial of service (dDoS) attack: hackers use numerous computers to attack target network from numerous launch points



## Other Security Threats

- Sniffing: Type of eavesdropping program that monitors information traveling over a network; enables hackers to steal proprietary information from anywhere on a network
- Insider jobs: Single largest financial threat
- Poorly designed server and client software: Increase in complexity of software programs has contributed to an increase in vulnerabilities that hackers can exploit



# Technology Solutions

- Protecting Internet communications (encryption)
- Securing channels of communication (SSL, S-HTTP, VPNs)
- Protecting networks (firewalls)
- Protecting servers and clients

# Tools Available to Achieve Site Security

Figure 5.7, Page 269





# Protecting Internet Communications: Encryption

- Encryption: The process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and receiver
- Purpose: Secure stored information and information transmission
- Provides:
  - Message integrity
  - Nonrepudiation
  - Authentication
  - Confidentiality

# Symmetric Key Encryption

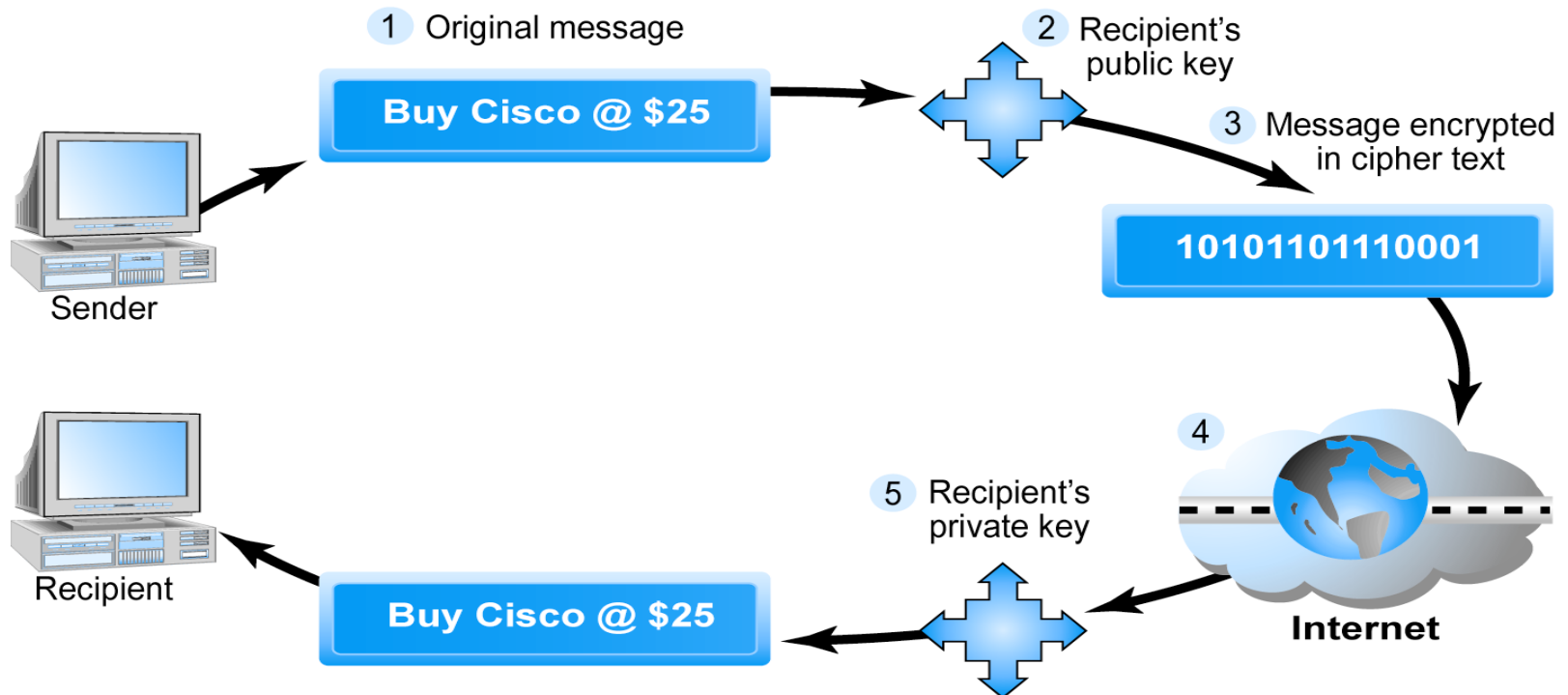
- Also known as secret key encryption
- Both the sender and receiver use the same digital key to encrypt and decrypt message
- Requires a different set of keys for each transaction
- Data Encryption Standard (DES): Most widely used symmetric key encryption today; uses 56-bit encryption key; other types use 128-bit keys up through 2048 bits

# Public Key Encryption

- Public key cryptography solves symmetric key encryption problem of having to exchange secret key
- Uses two mathematically related digital keys – public key (widely disseminated) and private key (kept secret by owner)
- Both keys are used to encrypt and decrypt message
- Once key is used to encrypt message, same key cannot be used to decrypt message
- For example, sender uses recipient's public key to encrypt message; recipient uses his/her private key to decrypt it

# Public Key Cryptography – A Simple Case

Figure 5.8, Page 272



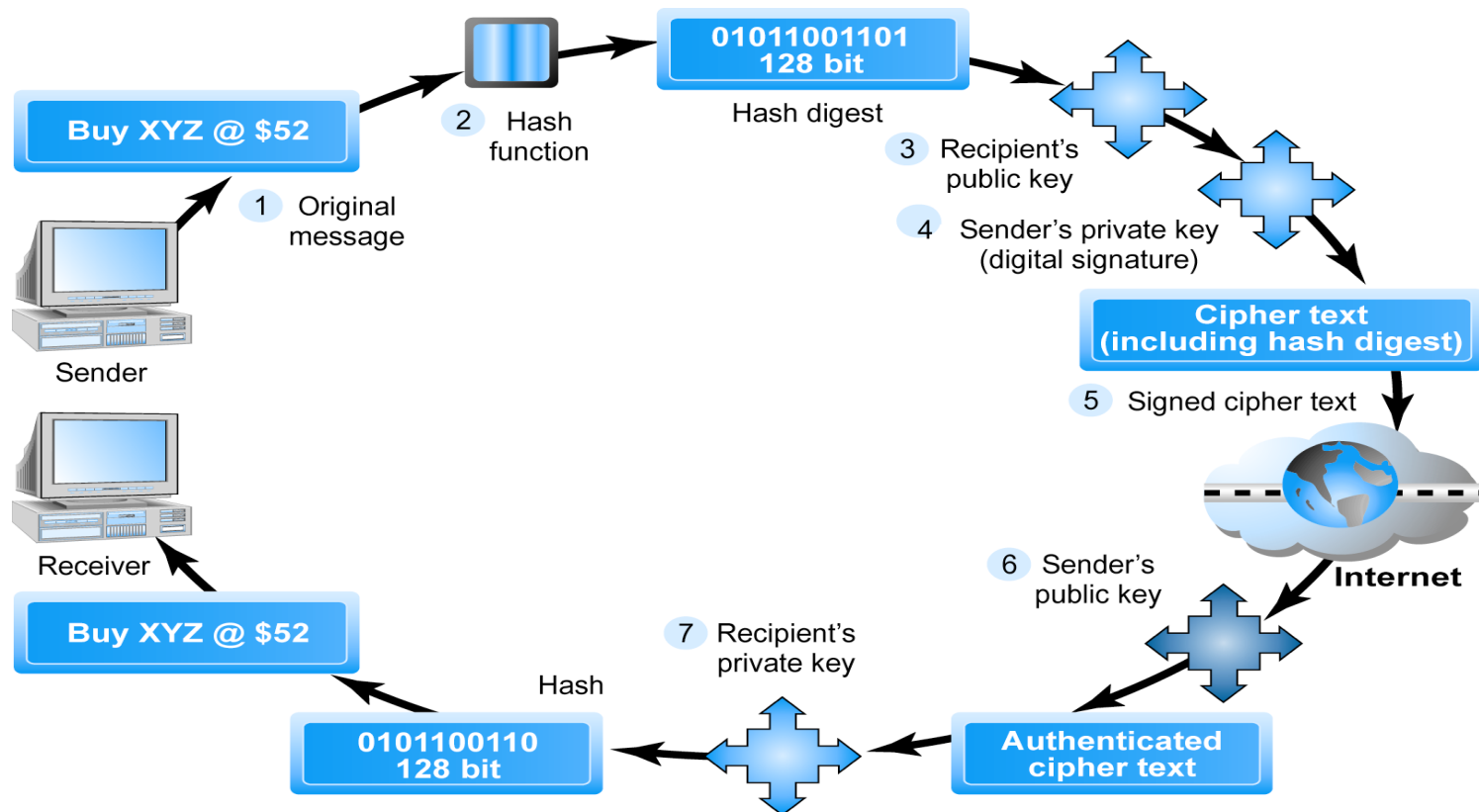


# Public Key Encryption using Digital Signatures and Hash Digests

- Application of hash function (mathematical algorithm) by sender prior to encryption produces hash digest that recipient can use to verify integrity of data
- Double encryption with sender's private key (digital signature) helps ensure authenticity and nonrepudiation

# Public Key Cryptography with Digital Signatures

Figure 5.9, Page 274



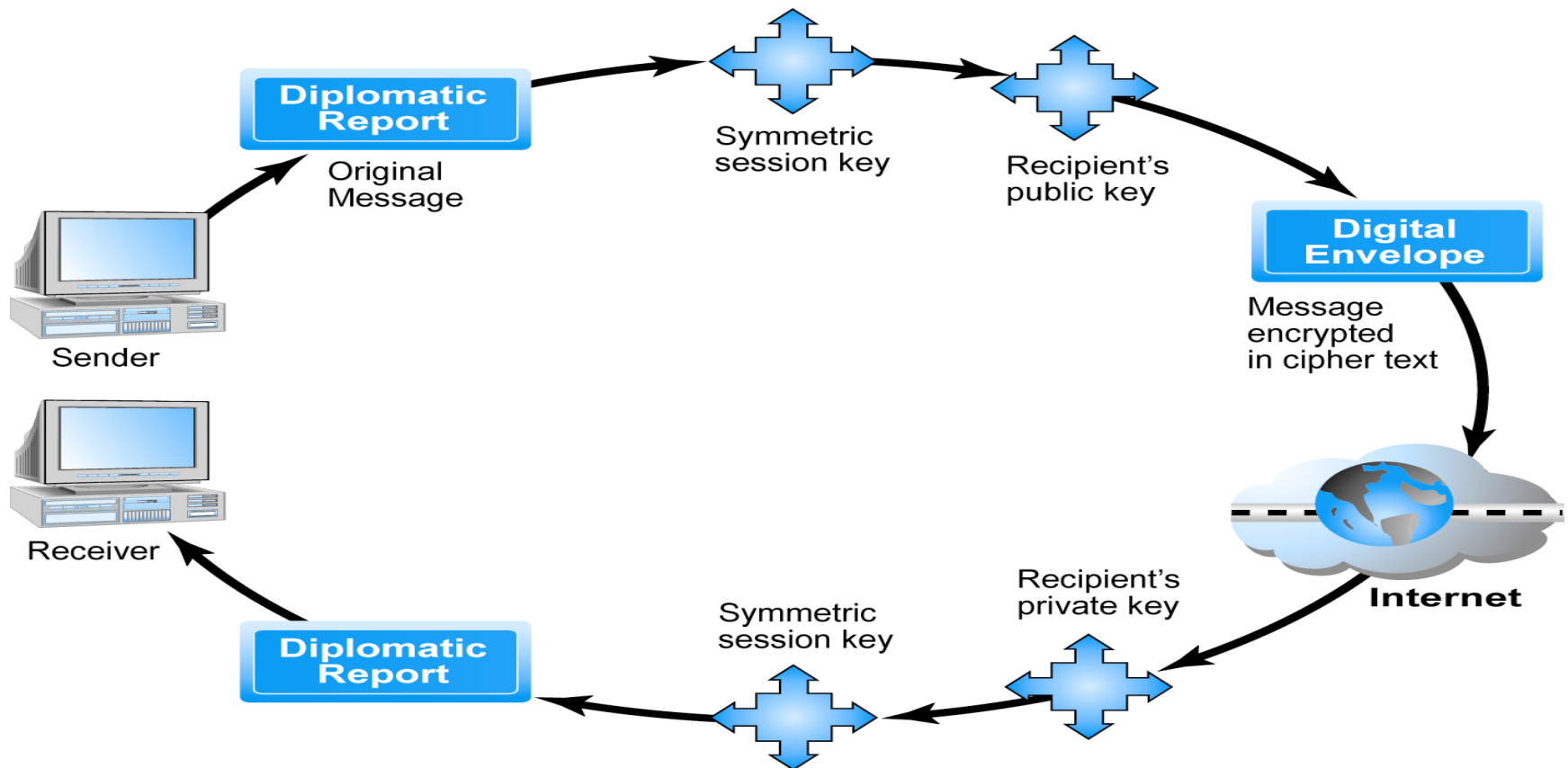


# Digital Envelopes

- Addresses weaknesses of public key encryption (computationally slow, decreases transmission speed, increases processing time) and symmetric key encryption (faster, but more secure)
- Uses symmetric key encryption to encrypt document but public key encryption to encrypt and send symmetric key

# Public Key Cryptography: Creating a Digital Envelope

Figure 5.10, Page 275

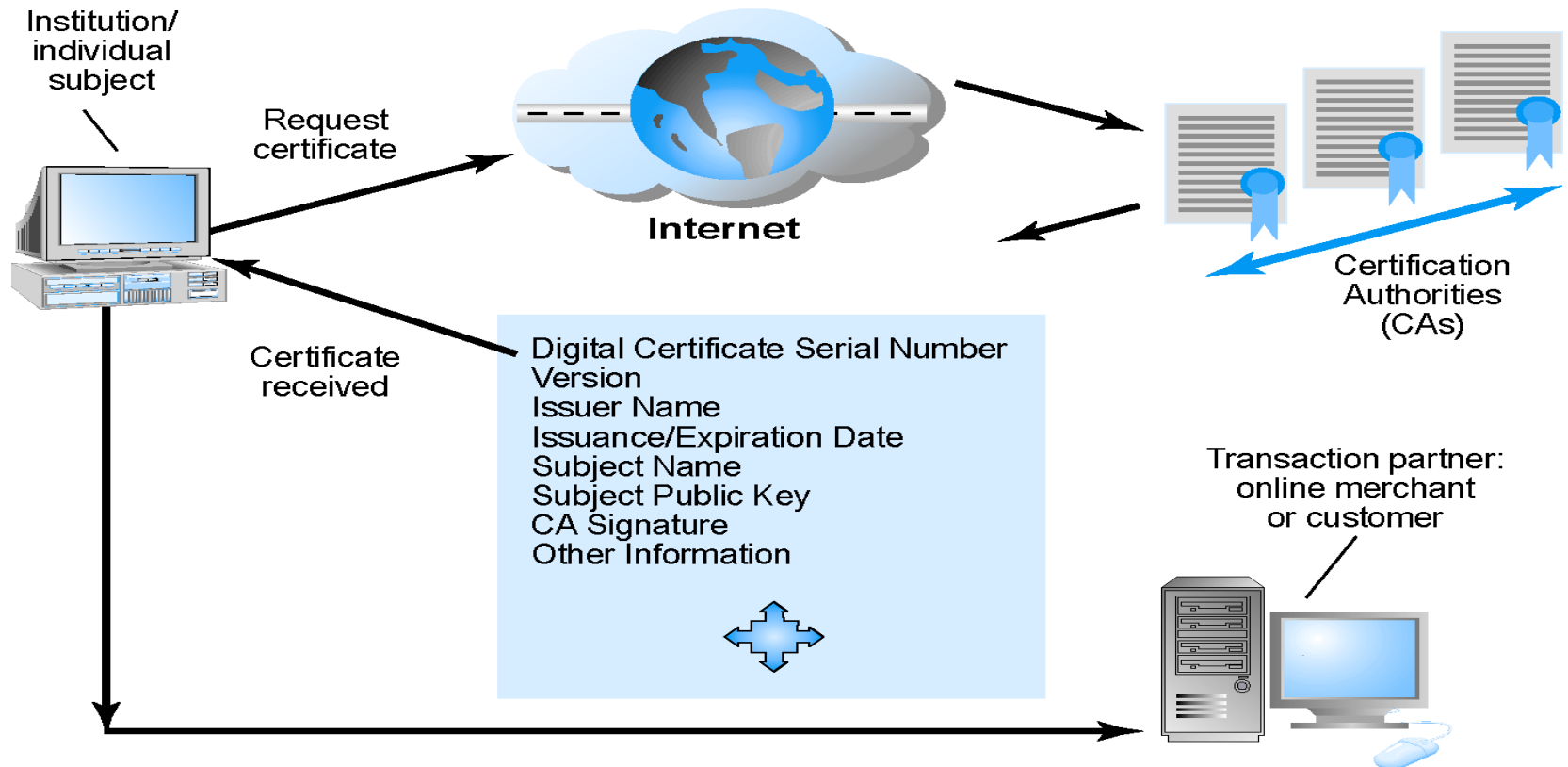


# Digital Certificates and Public Key Infrastructure (PKI)

- Digital certificate: Digital document that includes:
  - Name of subject or company
  - Subject's public key
  - Digital certificate serial number
  - Expiration date
  - Issuance date
  - Digital signature of certification authority (trusted third party institution) that issues certificate
  - Other identifying information
- Public Key Infrastructure (PKI): refers to the CAs and digital certificate procedures that are accepted by all parties

# Digital Certificates and Certification Authorities

Figure 5.11, Page 277





# Limits to Encryption Solutions

- PKI applies mainly to protecting messages in transit
- PKI is not effective against insiders
- Protection of private keys by individuals may be haphazard
- No guarantee that verifying computer of merchant is secure
- CAs are unregulated, self-selecting organizations



# **Insight on Technology: Advances in Quantum Cryptography May Lead to the Unbreakable Key**

## **Class Discussion**

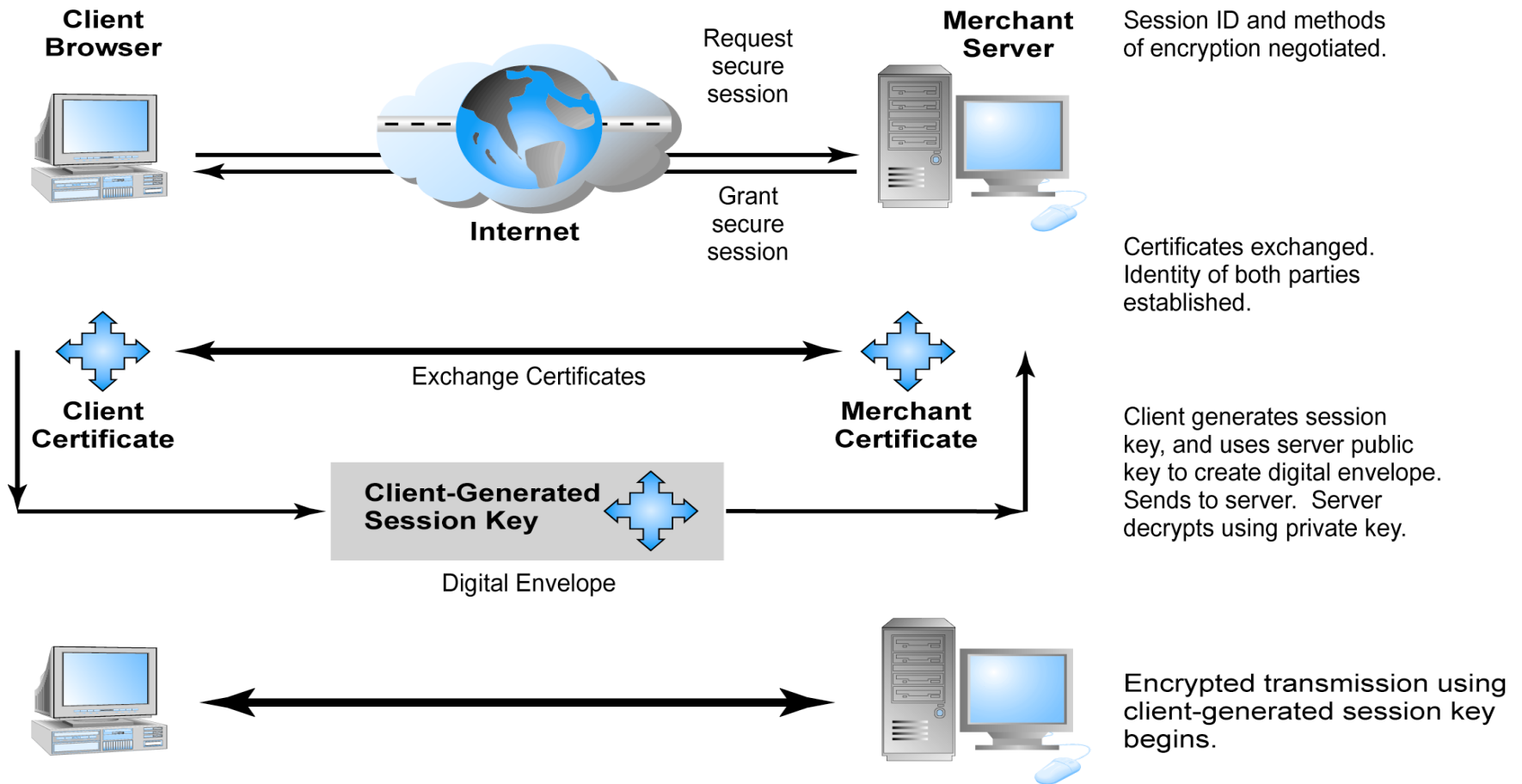
- Why are existing encryption systems over time more vulnerable?
- What is quantum encryption?
- What is the weakness of a symmetric key system (even one based on quantum techniques)?
- Would quantum-encrypted messages be immune to the growth in computing power?

# Securing Channels of Communication

- Secure Sockets Layer (SSL): Most common form of securing channels of communication; used to establish a secure negotiated session (client-server session in which URL of requested document, along with contents, is encrypted)
- S-HTTP: Alternative method; provides a secure message-oriented communications protocol designed for use in conjunction with HTTP
- Virtual Private Networks (VPNs): Allow remote users to securely access internal networks via the Internet, using Point-to-Point Tunneling Protocol (PPTP)

# Secure Negotiated Sessions Using SSL

Figure 5.12, Page 281



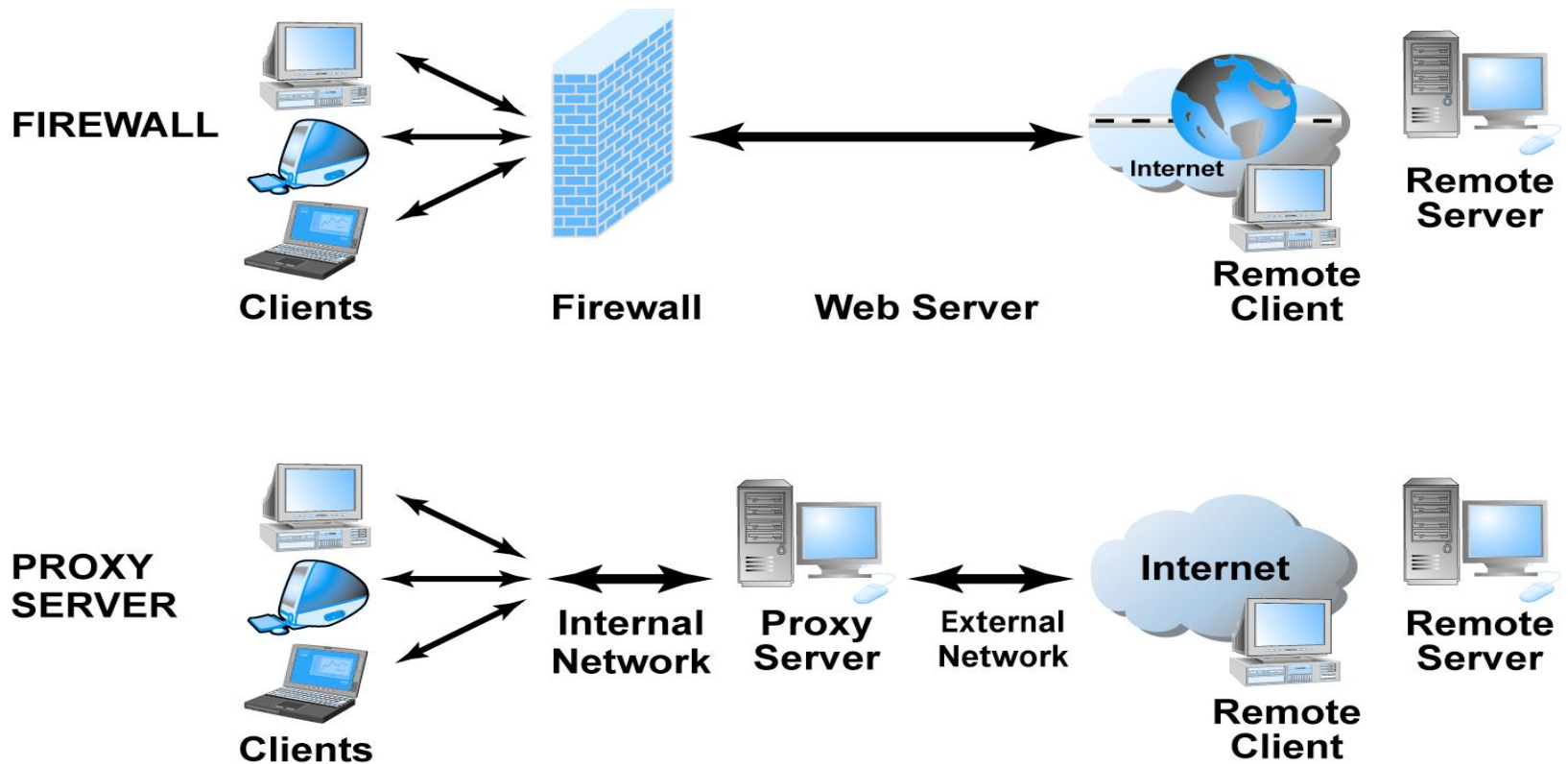


# Protecting Networks: Firewalls and Proxy Servers

- Firewall: Hardware or software filters communications packets and prevents some packets from entering the network based on a security policy
- Firewall methods include:
  - Packet filters
  - Application gateways
- Proxy servers: Software servers that handle all communications originating from or being sent to the Internet

# Firewalls and Proxy Servers

Figure 5.13, Page 283





# Protecting Servers and Clients

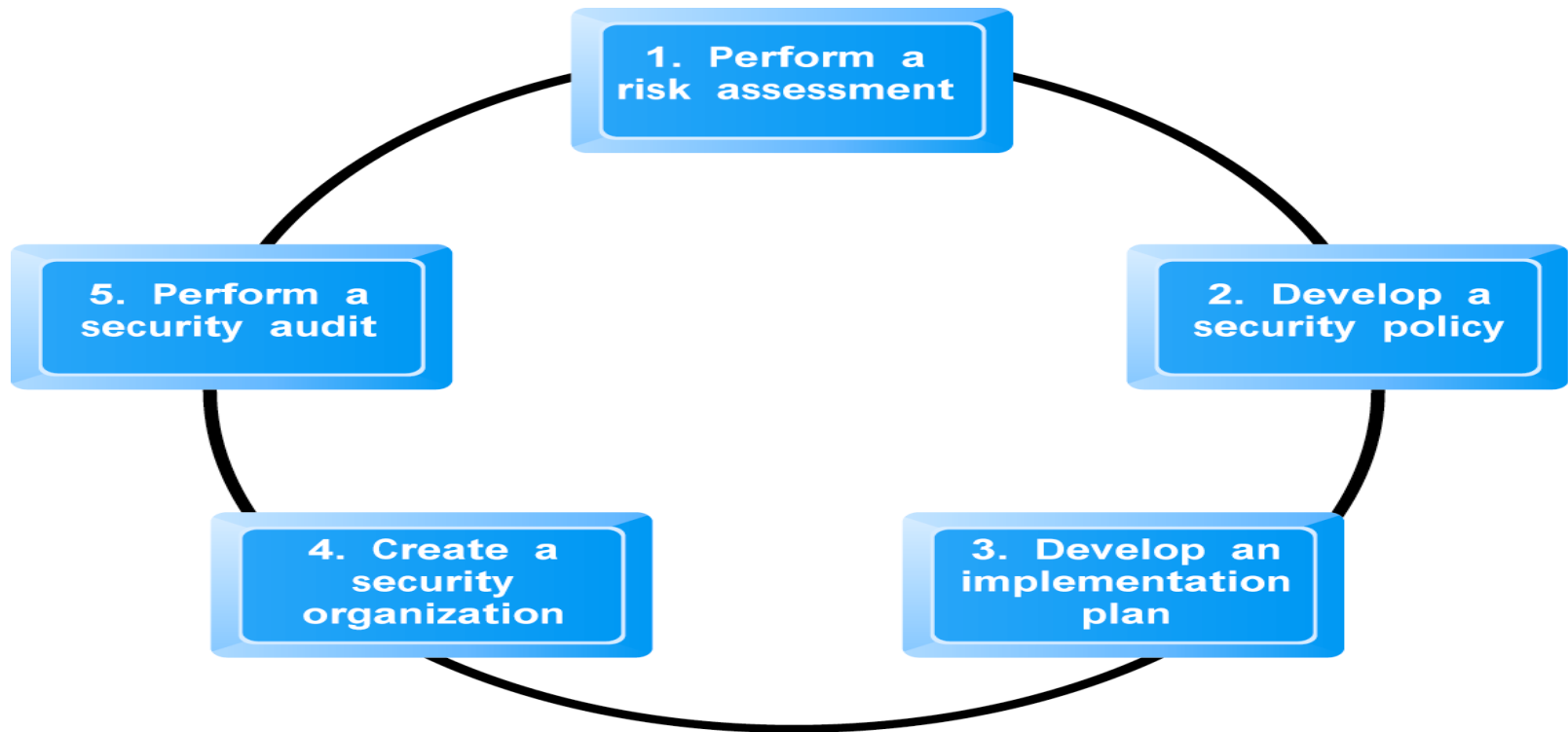
- Operating system controls: Authentication and access control mechanisms
- Anti-virus software: Easiest and least expensive way to prevent threats to system integrity


# A Security Plan: Management Policies

- Steps in developing a security plan
  - Perform risk assessment: assessment of risks and points of vulnerability
  - Develop security policy: set of statements prioritizing information risks, identifying acceptable risk targets, and identifying mechanisms for achieving targets
  - Develop implementation plan: action steps needed to achieve security plan goals
  - Create security organization: in charge of security; educates and trains users, keeps management aware of security issues; administers access controls, authentication procedures and authorization policies
  - Perform security audit: review of security practices and procedures

# Developing an E-commerce Security Plan

Figure 5.14, Page 286





# **Insight on Business: Hiring Hackers to Locate Threats: Penetration Testing**

## **Class Discussion**

- Why would firms hire outsiders to crash its systems?
- What are “grey” and “black” hats and why do firms avoid them as security testers?
- Are penetration specialists like Johnny Long performing a public service or just making the situation worse?



# The Role of Laws and Public Policy

- New laws have granted local and national authorities new tools and mechanisms for identifying, tracing and prosecuting cybercriminals
  - National Infrastructure Protection Center – unit within National Cyber Security Division of Department of Homeland Security whose mission is to identify and combat threats against U.S. technology and telecommunications infrastructure
  - USA Patriot Act
  - Homeland Security Act
- Government policies and controls on encryption software

# OECD Guidelines

- 2002 Organization for Economic Cooperation and Development (OECD) Guidelines for the Security of Information Systems and Networks has nine principles:
  - Awareness
  - Responsibility
  - Response
  - Ethics
  - Democracy
  - Risk assessment
  - Security design and implementation
  - Security management
  - Reassessment