E-commerce Security and Payment Systems

The E-commerce Security Environment

- **Overall size and losses of cybercrime unclear**
  - Reporting issues
- **2012 survey: Average annualized cost of cybercrime was $8.9 million/year**
- **Underground economy marketplace:**
  - Stolen information stored on underground economy servers

What Is Good E-commerce Security?

- **To achieve highest degree of security**
  - New technologies
  - Organizational policies and procedures
  - Industry standards and government laws
- **Other factors**
  - Time value of money
  - Cost of security vs. potential loss
  - Security often breaks at weakest link

The E-commerce Security Environment

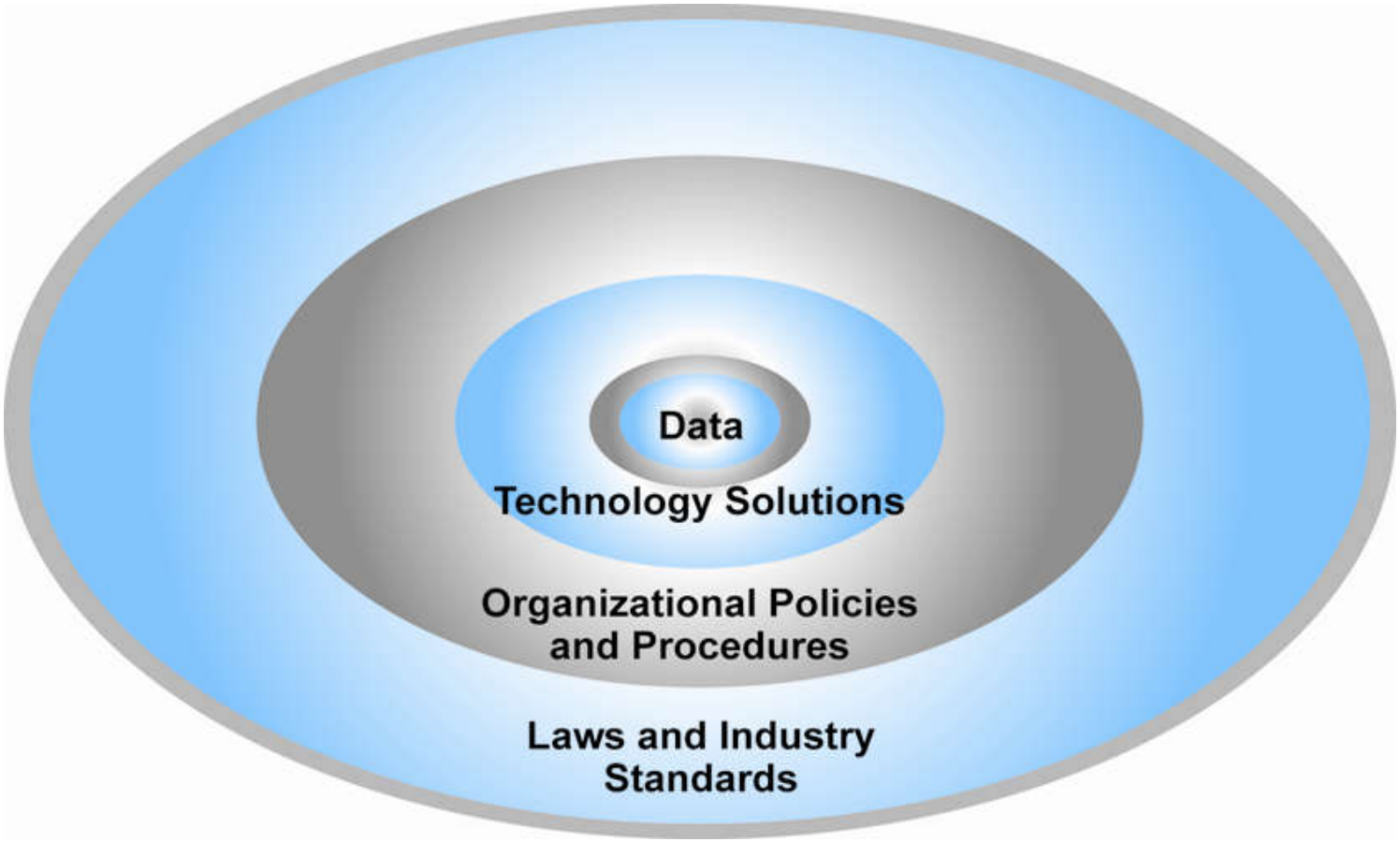

Figure 5.1, Page 252

TABLE 5.3	CUSTOMER AND MERCHANT PERSPECTIVES ON THE DIFFERENT DIMENSIONS OF E-COMMERCE SECURITY	
DIMENSION	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE
Integrity	Has information I transmitted or received 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?

Table 5.3, Page 254

The Tension Between Security and Other Values

- **Ease of use**
  - The more security measures added, the more difficult a site is to use, and the slower it becomes
- **Public safety and criminal uses of the Internet**
  - Use of technology by criminals to plan crimes or threaten nation-state

Security Threats in the E-commerce Environment

- **Three key points of vulnerability in e-commerce environment:**
  1. Client
  2. Server
  3. Communications pipeline (Internet communications channels)

A Typical E-commerce Transaction

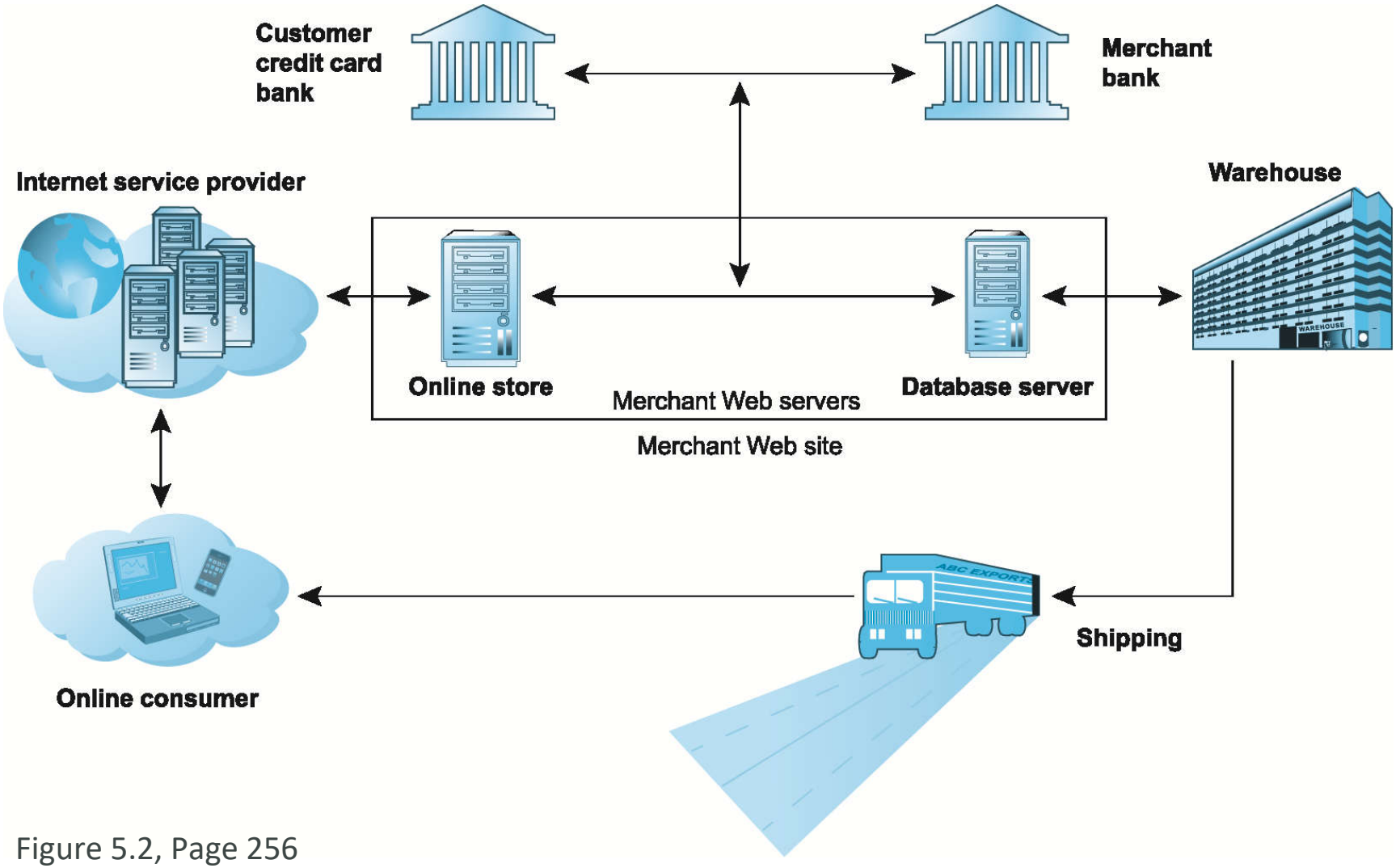

Figure 5.2, Page 256

Vulnerable Points in an E-commerce Transaction

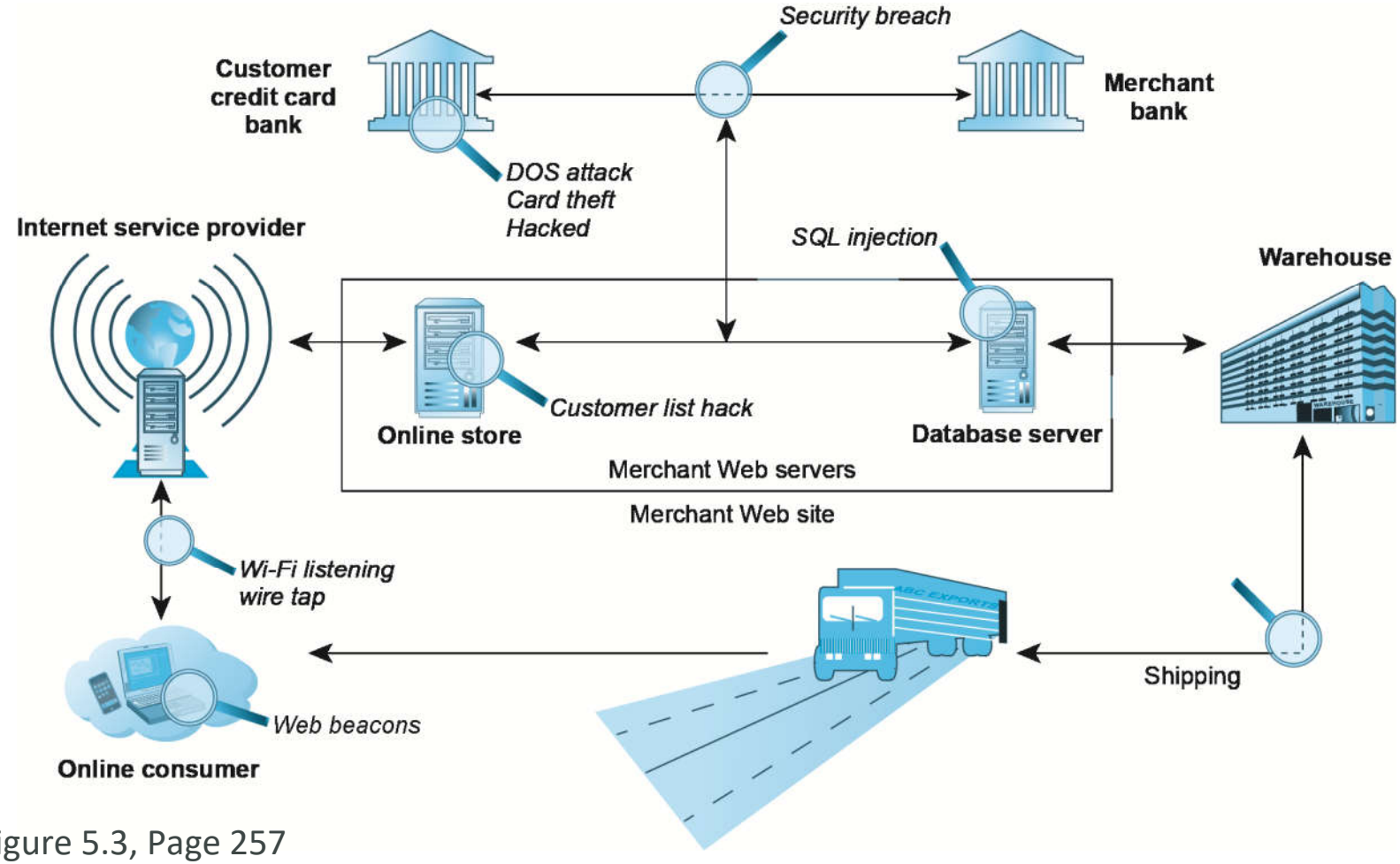

Figure 5.3, Page 257

Most Common Security Threats in the E-commerce Environment

- **Malicious code (malware, exploits)**
  - Drive-by downloads
  - Viruses
  - Worms
  - Ransomware
  - Trojan horses
  - Backdoors
  - Bots, botnets
  - Threats at both client and server levels

Most Common Security Threats (cont.)

- **Potentially unwanted programs (PUPs)**
  - Browser parasites
  - Adware
  - Spyware
- **Phishing**
  - Social engineering
  - E-mail scams
  - Spear-phishing
  - Identity fraud/theft

Most Common Security Threats (cont.)

- **Hacking**
  - Hackers vs. crackers
  - Types of hackers: White, black, grey hats
  - Hacktivism
- **Cybervandalism:**
  - Disrupting, defacing, destroying Web site
- **Data breach**
  - Losing control over corporate information to outsiders

We Are Legion

- **What organization and technical failures led to the data breach on the PlayStation Network?**
- **Are there any positive social benefits of hacktivism?**
- **Have you or anyone you know experienced data breaches or cybervandalism?**

Most Common Security Threats (cont.)

- Credit card fraud/theft
- Spoofing and pharming
- Spam (junk) Web sites (link farms)
- Identity fraud/theft
- Denial of service (DoS) attack
  - Hackers flood site with useless traffic to overwhelm network
- Distributed denial of service (DDoS) attack

Most Common Security Threats (cont.)

- **Sniffing**
  - Eavesdropping program that monitors information traveling over a network
- **Insider attacks**
- **Poorly designed server and client software**
- **Social network security issues**
- **Mobile platform security issues**
  - Vishing, smishing, madware
- **Cloud security issues**

Think Your Smartphone Is Secure?

- What types of threats do smartphones face?
- Are there any particular vulnerabilities to this type of device?
- What did Nicolas Seriot's "Spyphone" prove?
- Are apps more or less likely to be subject to threats than traditional PC software programs?

Technology Solutions

- **Protecting Internet communications**
  - Encryption
- **Securing channels of communication**
  - SSL, VPNs
- **Protecting networks**
  - Firewalls
- **Protecting servers and clients**

Tools Available to Achieve Site Security

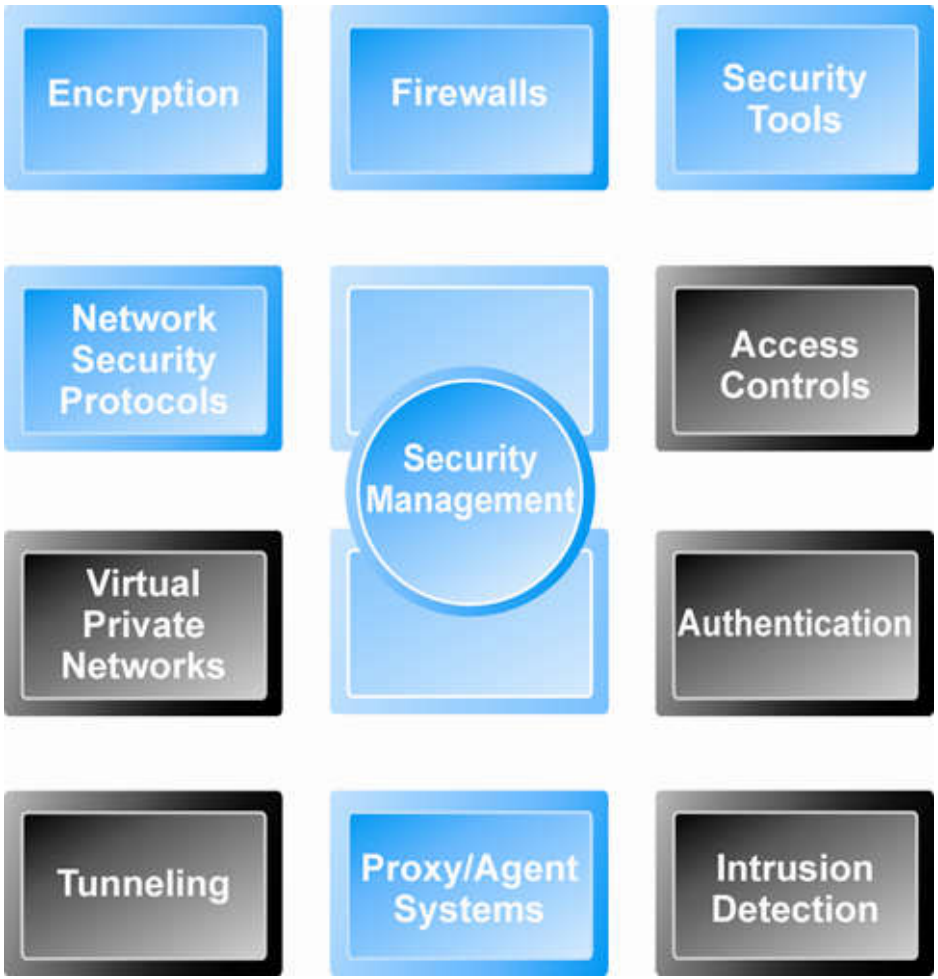

Figure 5.5, Page 276

Encryption

Encryption

- Transforms data into cipher text readable only by sender and receiver
- Secures stored information and information transmission
- Provides 4 of 6 key dimensions of e-commerce security:
  - Message integrity
  - Nonrepudiation
  - Authentication
  - Confidentiality

Symmetric Key Encryption

- **Sender and receiver use same digital key to encrypt and decrypt message**
- **Requires different set of keys for each transaction**
- **Strength of encryption**
  - Length of binary key used to encrypt data
- **Data Encryption Standard (DES)**
- **Advanced Encryption Standard (AES)**
  - Most widely used symmetric key encryption
  - Uses 128-, 192-, and 256-bit encryption keys
- **Other standards use keys with up to 2,048 bits**

Public Key Encryption

- **Uses two mathematically related digital keys**
  - Public key (widely disseminated)
  - Private key (kept secret by owner)
- **Both keys used to encrypt and decrypt message**
- **Once key used to encrypt message, same key cannot be used to decrypt message**
- **Sender uses recipient's public key to encrypt message; recipient uses private key to decrypt it**

Public Key Cryptography: A Simple Case

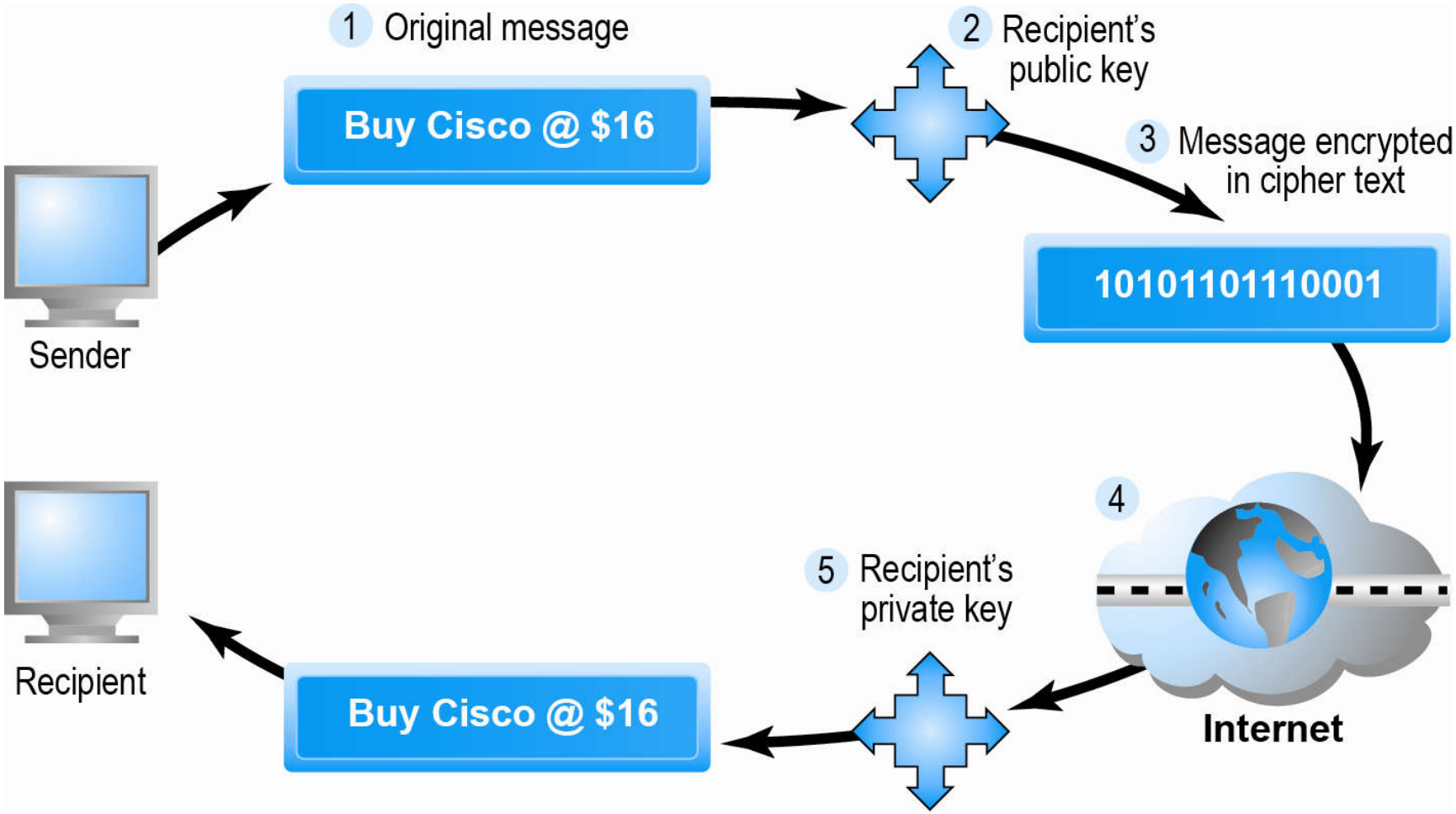

Figure 5.6, Page 279

Public Key Encryption using Digital Signatures and Hash Digests

- **Hash function:**
  - Mathematical algorithm that produces fixed-length number called message or hash digest
- **Hash digest of message sent to recipient along with message to verify integrity**
- **Hash digest and message encrypted with recipient's public key**
- **Entire cipher text then encrypted with recipient's private key—creating digital signature—for authenticity, nonrepudiation**

Public Key Cryptography with Digital Signatures

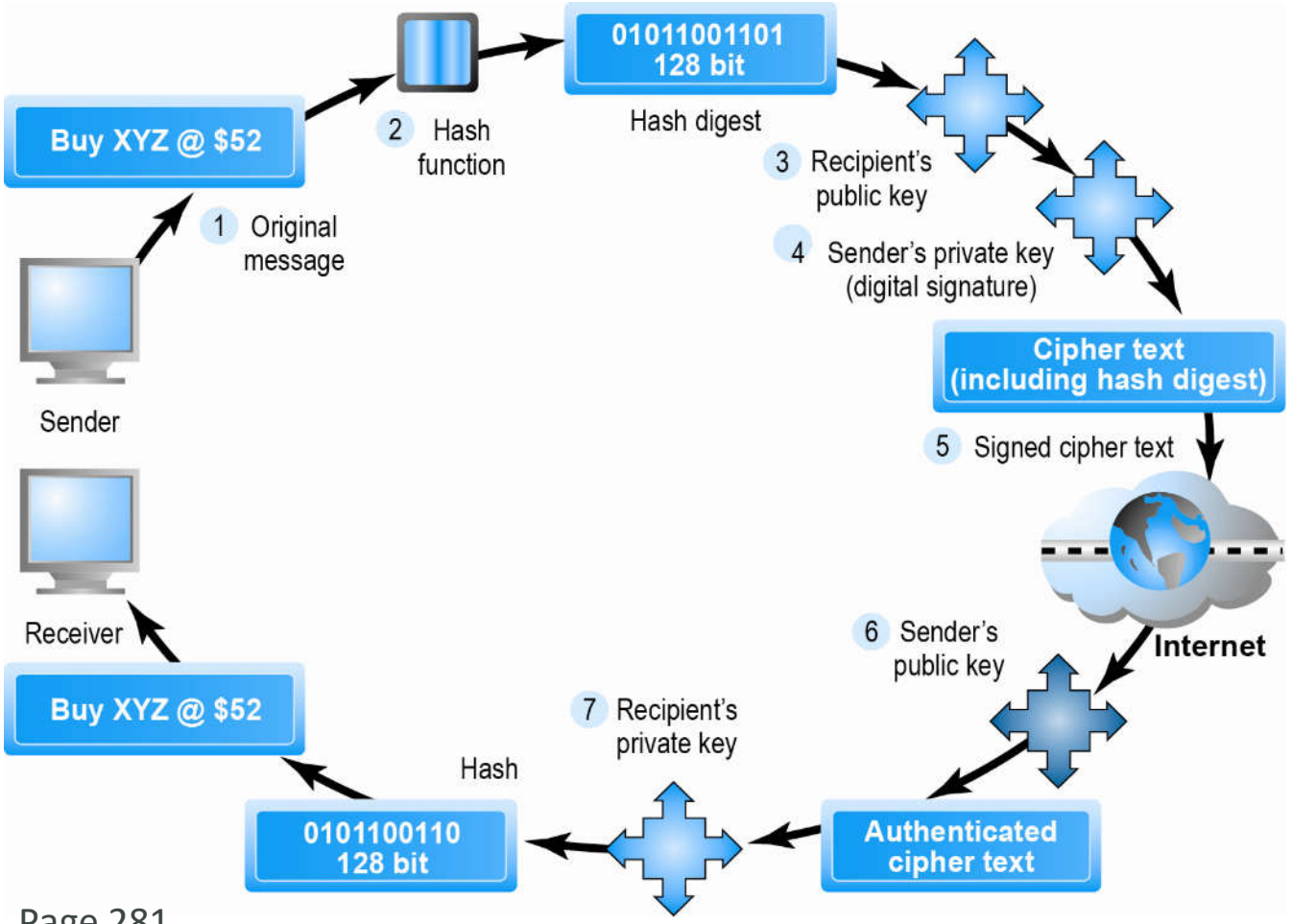

Figure 5.7, Page 281

Digital Envelopes

- **Address weaknesses of:**
  - Public key encryption
    - Computationally slow, decreased transmission speed, increased processing time
  - Symmetric key encryption
    - Insecure transmission lines
- **Uses symmetric key encryption to encrypt document**
- **Uses public key encryption to encrypt and send symmetric key**

Creating a Digital Envelope

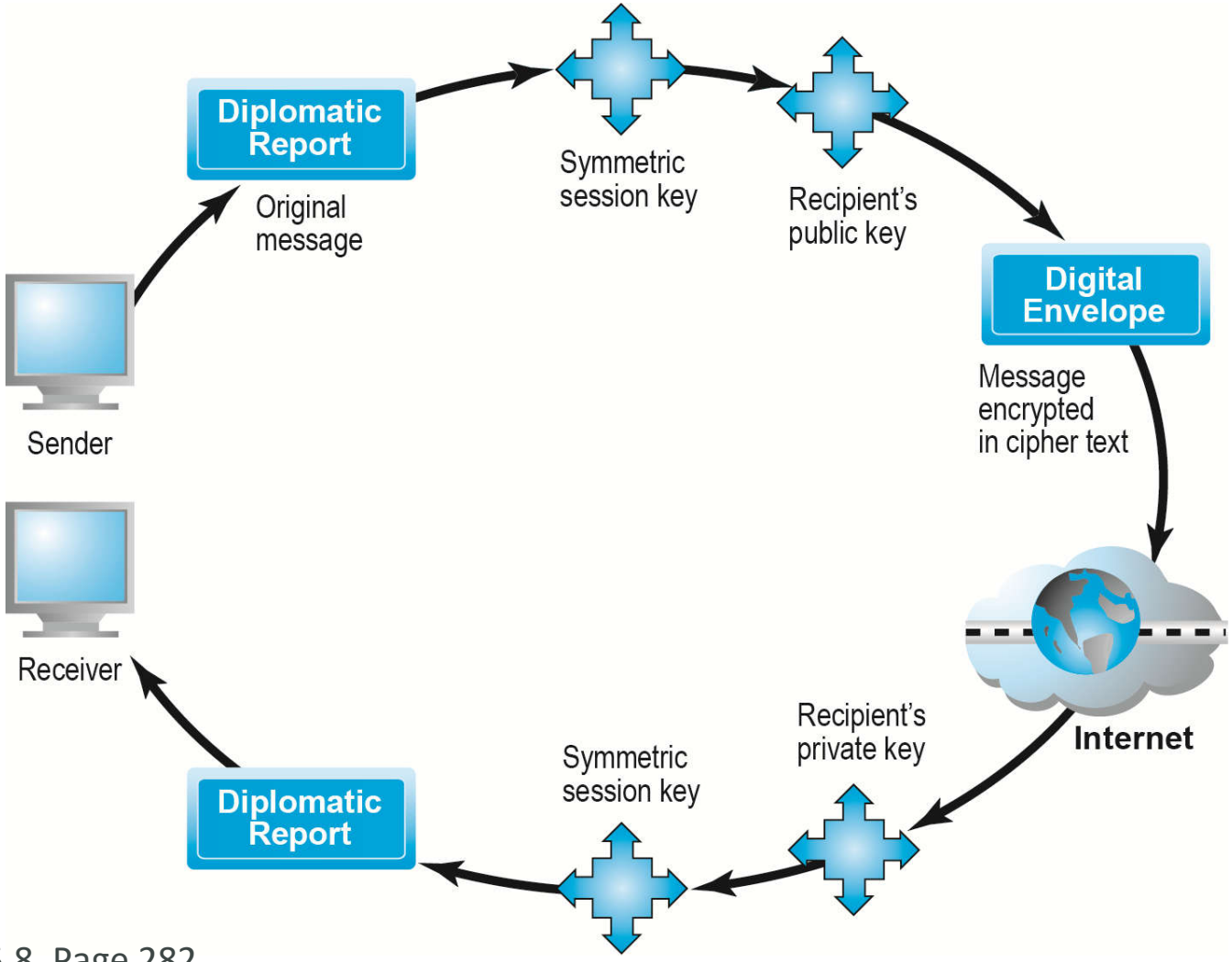

Figure 5.8, Page 282

Digital Certificates and Public Key Infrastructure (PKI)

- **Digital certificate includes:**
  - Name of subject/company
  - Subject's public key
  - Digital certificate serial number
  - Expiration date, issuance date
  - Digital signature of CA
- **Public Key Infrastructure (PKI):**
  - CAs and digital certificate procedures
  - PGP

Digital Certificates and Certification Authorities

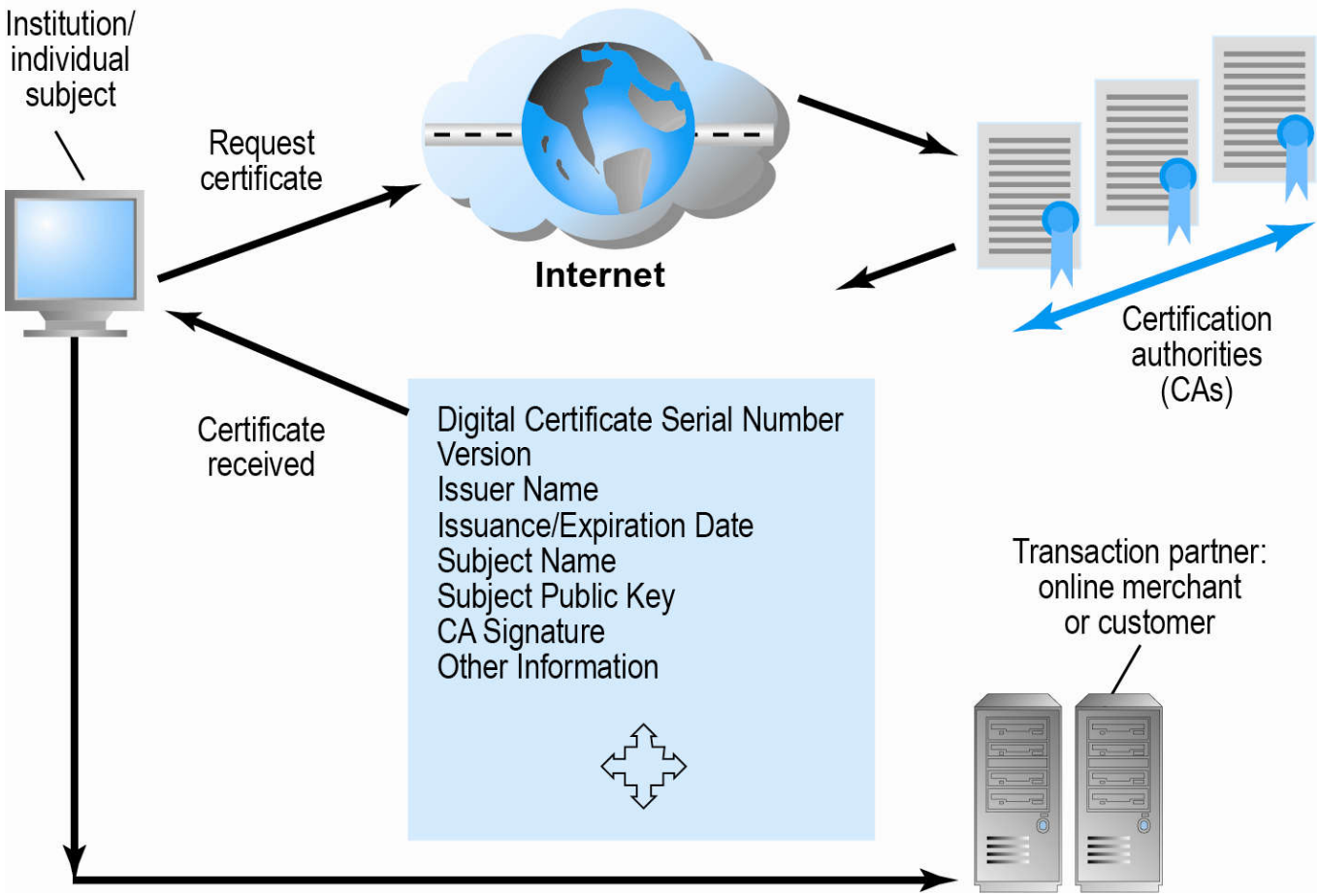

Figure 5.9, Page 283

Limits to Encryption Solutions

- **Doesn't protect storage of private key**
  - PKI not effective against insiders, employees
  - Protection of private keys by individuals may be haphazard
- **No guarantee that verifying computer of merchant is secure**
- **CAs are unregulated, self-selecting organizations**

Securing Channels of Communication

- **Secure Sockets Layer (SSL)/Transport Layer Security (TLS)**
  - Establishes secure, negotiated client–server session
- **Virtual Private Network (VPN)**
  - Allows remote users to securely access internal network via the Internet
- **Wireless (Wi-Fi) networks**
  - WPA2

Secure Negotiated Sessions Using SSL/TLS

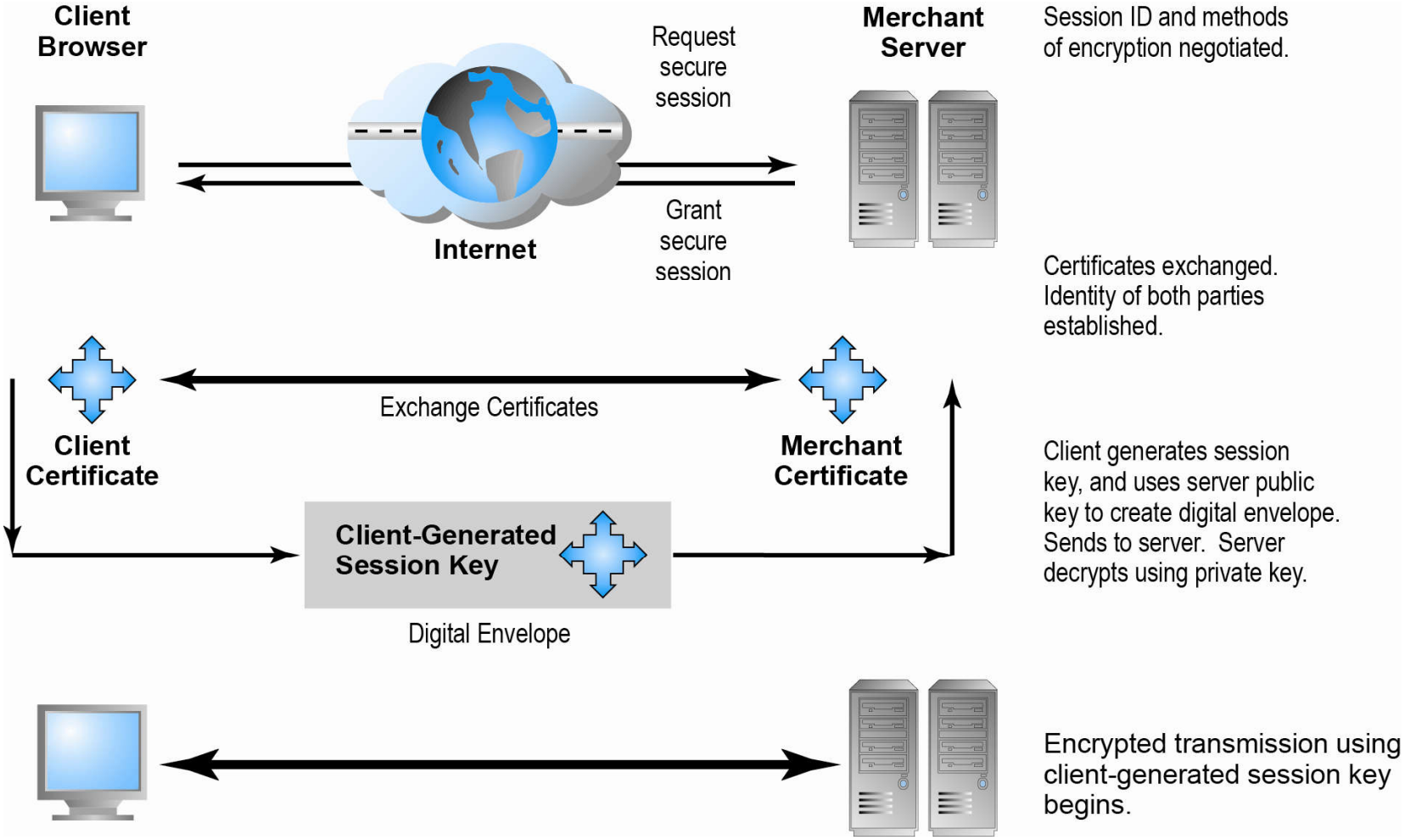

Figure 5.10, Page 286

Protecting Networks

- **Firewall**
  - Hardware or software
  - Uses security policy to filter packets
  - Two main methods:
    - Packet filters
    - Application gateways
- **Proxy servers (proxies)**
  - Software servers that handle all communications from or sent to the Internet
- **Intrusion detection systems**
- **Intrusion prevention systems**

Firewalls and Proxy Servers

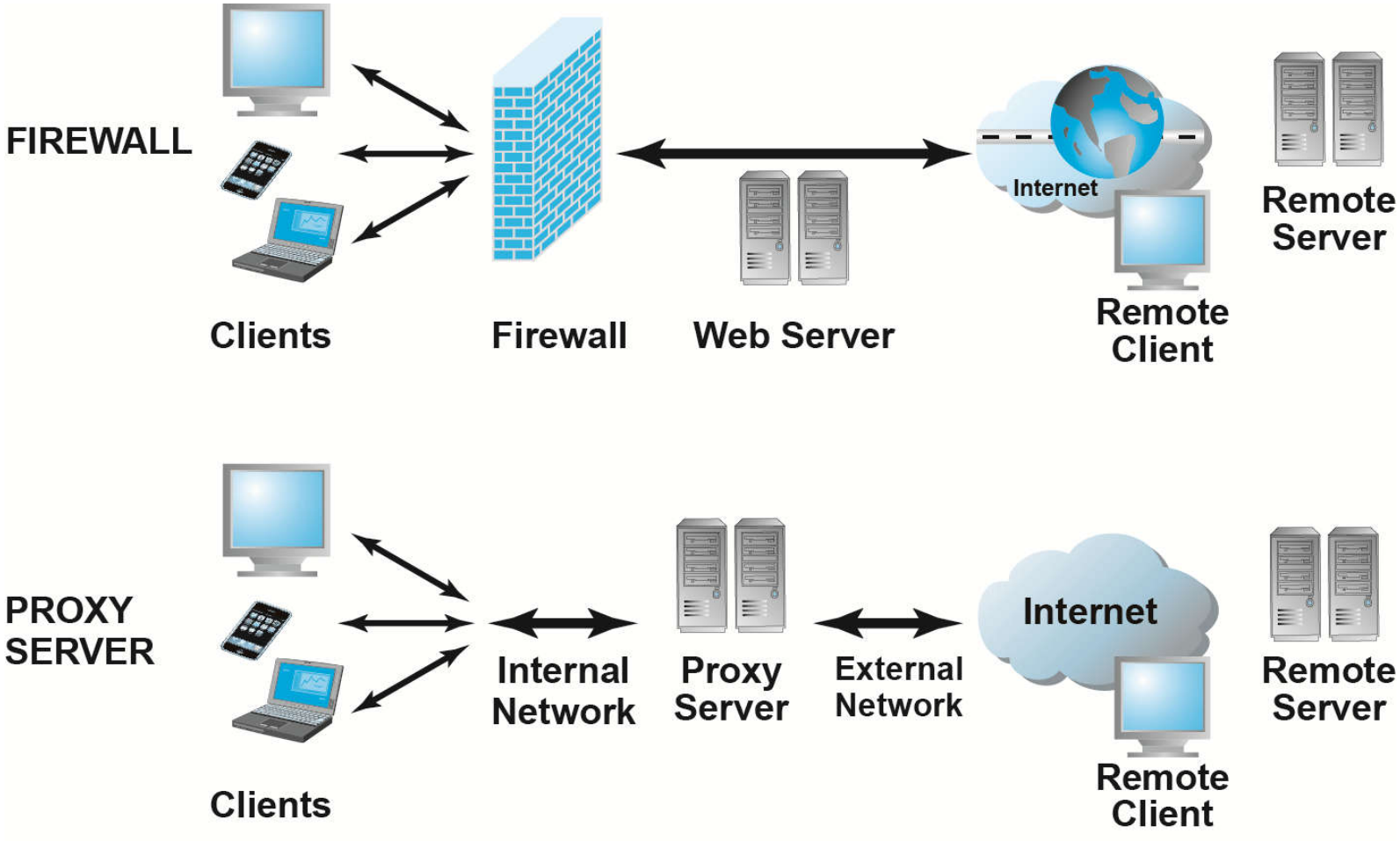

Figure 5.11, Page 289

Protecting Servers and Clients

- **Operating system security enhancements**
  - Upgrades, patches
- **Anti-virus software**
  - Easiest and least expensive way to prevent threats to system integrity
  - Requires daily updates

Management Policies, Business Procedures, and Public Laws

- **Worldwide, companies spend more than $65 billion on security hardware, software, services**
- **Managing risk includes:**
  - Technology
  - Effective management policies
  - Public laws and active enforcement

A Security Plan: Management Policies

- **Risk assessment**
- **Security policy**
- **Implementation plan**
  - Security organization
  - Access controls
  - Authentication procedures, including biometrics
  - Authorization policies, authorization management systems
- **Security audit**

Developing an E-commerce Security Plan

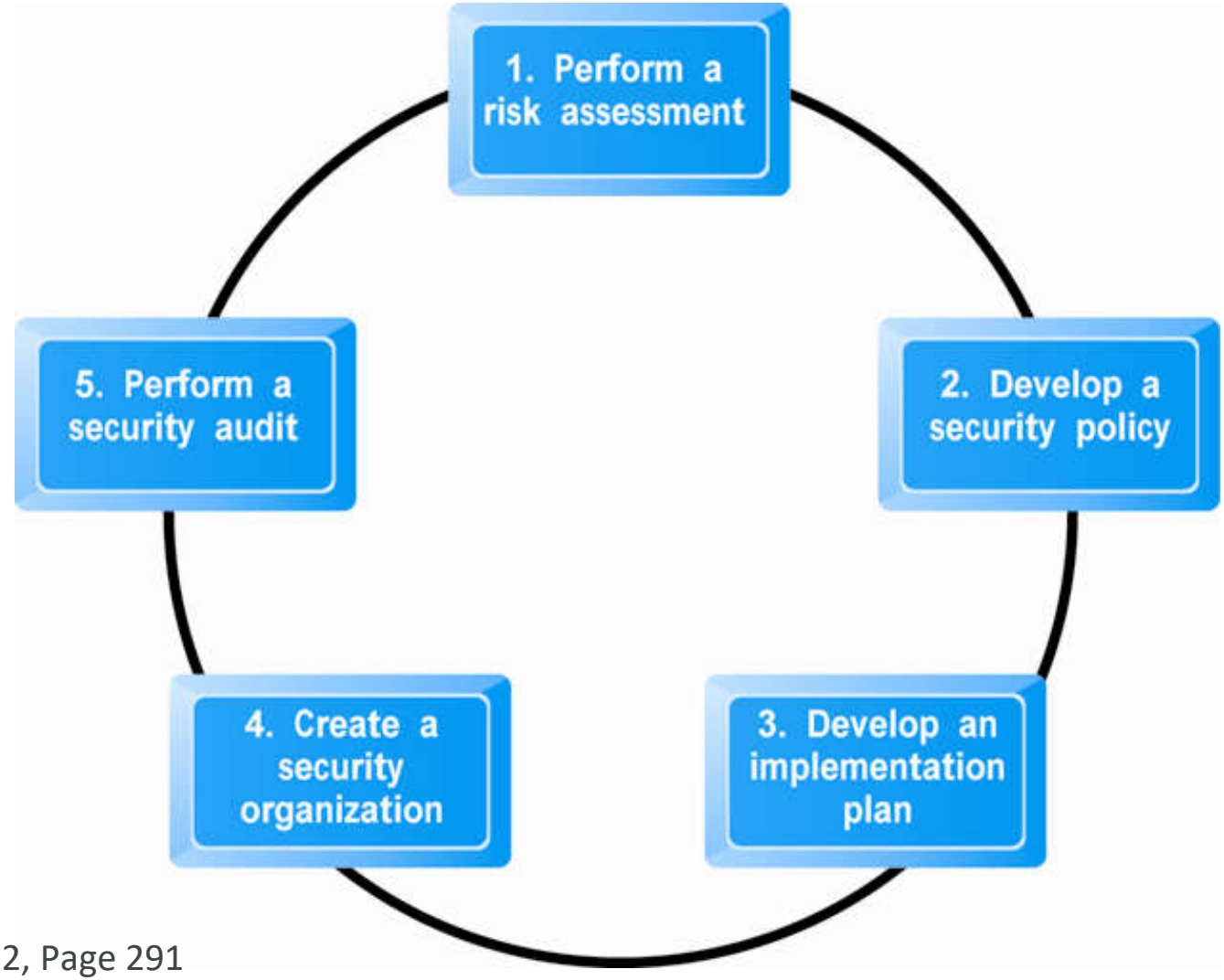

Figure 5.12, Page 291

The Role of Laws and Public Policy

- **Laws that give authorities tools for identifying, tracing, prosecuting cybercriminals:**
  - National Information Infrastructure Protection Act of 1996
  - USA Patriot Act
  - Homeland Security Act
- **Private and private-public cooperation**
  - CERT Coordination Center
  - US-CERT
- **Government policies and controls on encryption software**
  - OECD, G7/G8, Council of Europe, Wassener Arrangement

Types of Payment Systems

- **Cash**
  - Most common form of payment
  - Instantly convertible into other forms of value
  - No float
- **Checking transfer**
  - Second most common payment form in United States
- **Credit card**
  - Credit card associations
  - Issuing banks
  - Processing centers

Types of Payment Systems (cont.)

- **Stored value**
  - Funds deposited into account, from which funds are paid out or withdrawn as needed
  - Debit cards, gift certificates
  - Peer-to-peer payment systems
- **Accumulating balance**
  - Accounts that accumulate expenditures and to which consumers make period payments
  - Utility, phone, American Express accounts

Payment System Stakeholders

- **Consumers**
  - Low-risk, low-cost, refutable, convenience, reliability
- **Merchants**
  - Low-risk, low-cost, irrefutable, secure, reliable
- **Financial intermediaries**
  - Secure, low-risk, maximizing profit
- **Government regulators**
  - Security, trust, protecting participants and enforcing reporting

E-commerce Payment Systems

- **Credit cards**
  - 42% of online payments in 2013 (United States)
- **Debit cards**
  - 29% online payments in 2013 (United States)
- **Limitations of online credit card payment**
  - Security, merchant risk
  - Cost
  - Social equity

How an Online Credit Transaction Works

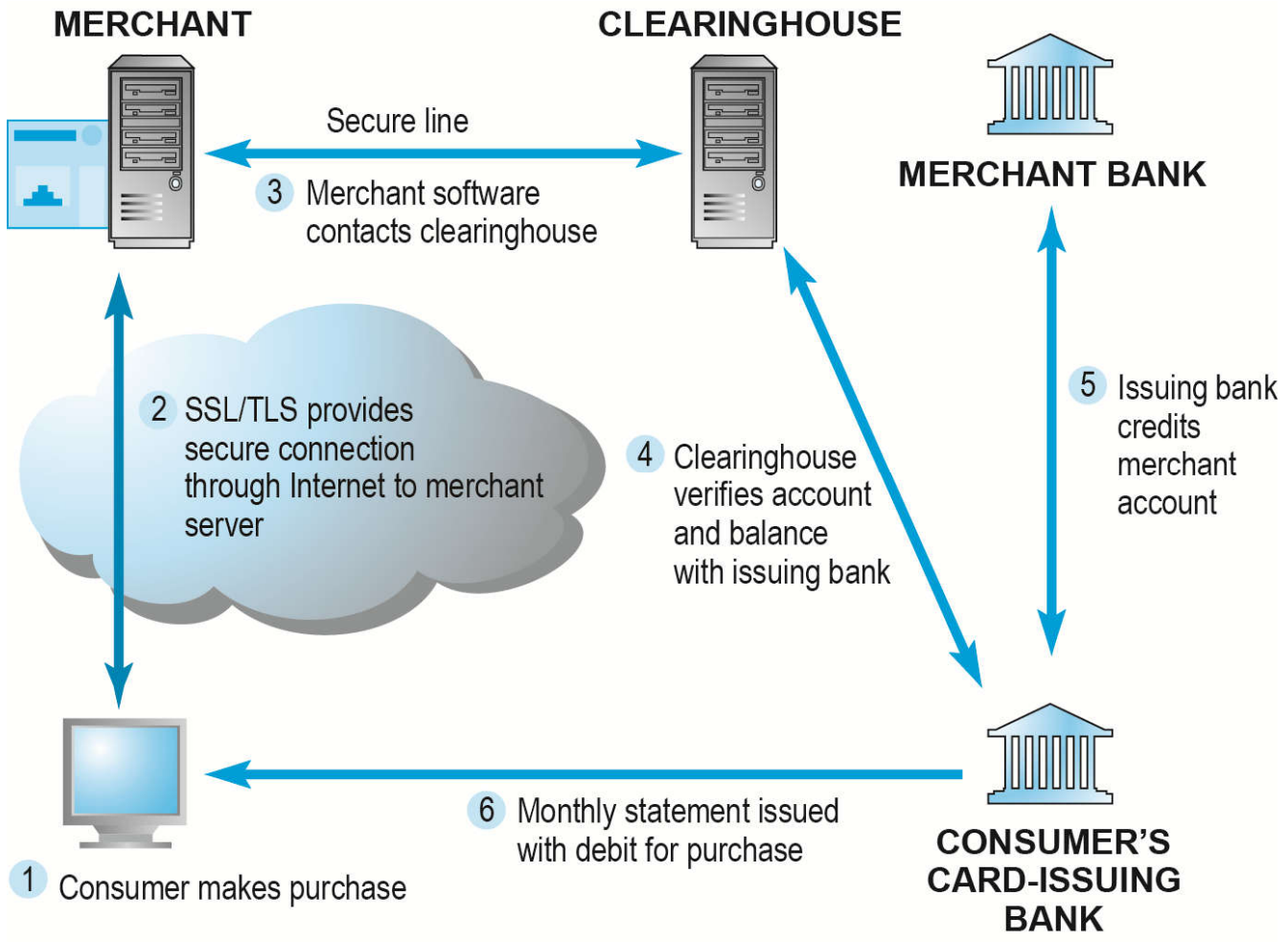

Figure 5.15, Page 302

Alternative Online Payment Systems

- **Online stored value systems:**
  - Based on value stored in a consumer's bank, checking, or credit card account
  - Example: PayPal
- **Other alternatives:**
  - Amazon Payments
  - Google Checkout
  - Bill Me Later
  - WUPay, Dwolla, Stripe

Mobile Payment Systems

- **Use of mobile phones as payment devices established in Europe, Japan, South Korea**
- **Near field communication (NFC)**
  - Short-range (2") wireless for sharing data between devices
- **Expanding in United States**
  - Google Wallet
    - Mobile app designed to work with NFC chips
  - PayPal
  - Square

Digital Cash and Virtual Currencies

- **Digital cash**
  - Based on algorithm that generates unique tokens that can be used in "real" world
  - Example: Bitcoin
- **Virtual currencies**
  - Circulate within internal virtual world
  - Example: Linden Dollars in Second Life, Facebook Credits

Bitcoin

- What are some of the benefits of using a digital currency?
- What are the risks involved to the user?
- What are the political and economic repercussions of a digital currency?
- Have you or anyone you know ever used Bitcoin?

Electronic Billing Presentment and Payment (EBPP)

- **Online payment systems for monthly bills**
- **50% of all bill payments**
- **Two competing EBPP business models:**
  - Biller-direct (dominant model)
  - Consolidator
- **Both models are supported by EBPP infrastructure providers**