E-commerce

business. technology. society.

Fifth Edition

Kenneth C. Laudon

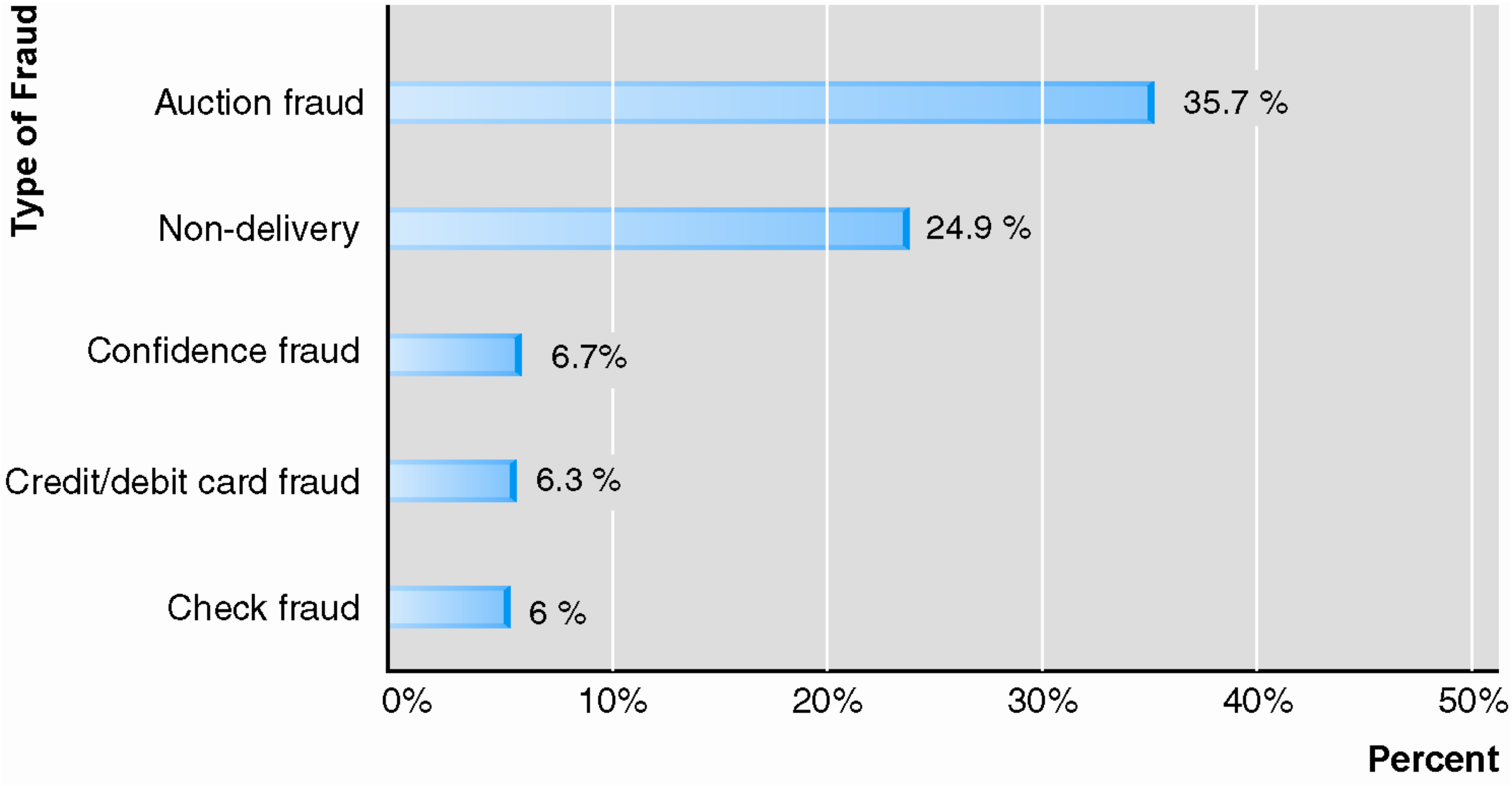
Carol Guercio Traver

Chapter 5

Online Security and Payment Systems

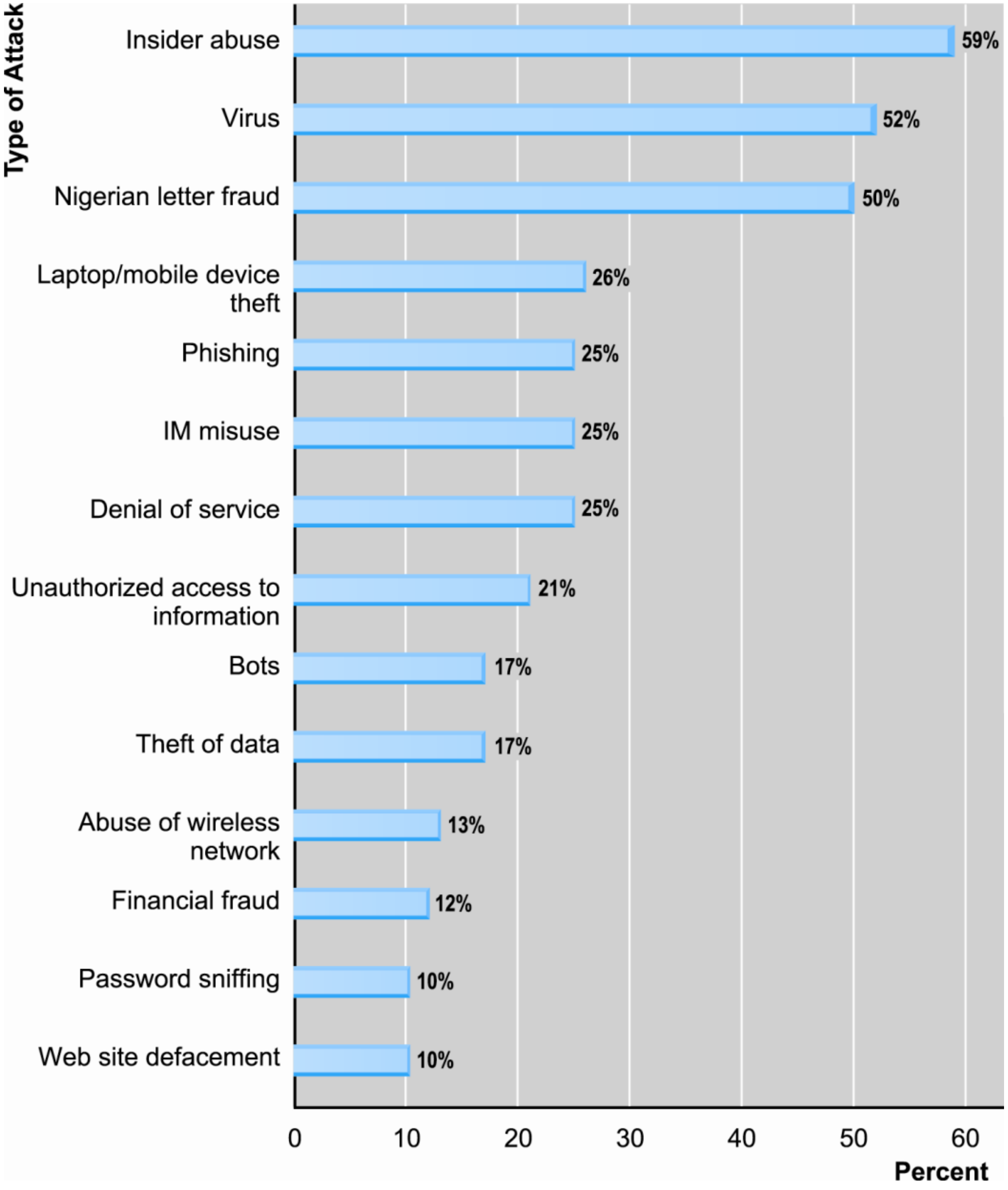
Categories of Internet Crime Complaints Reported to IC3

Figure 5.1, Page 262



Types of Attacks Against Computer Systems

Figure 5.3, Page 264

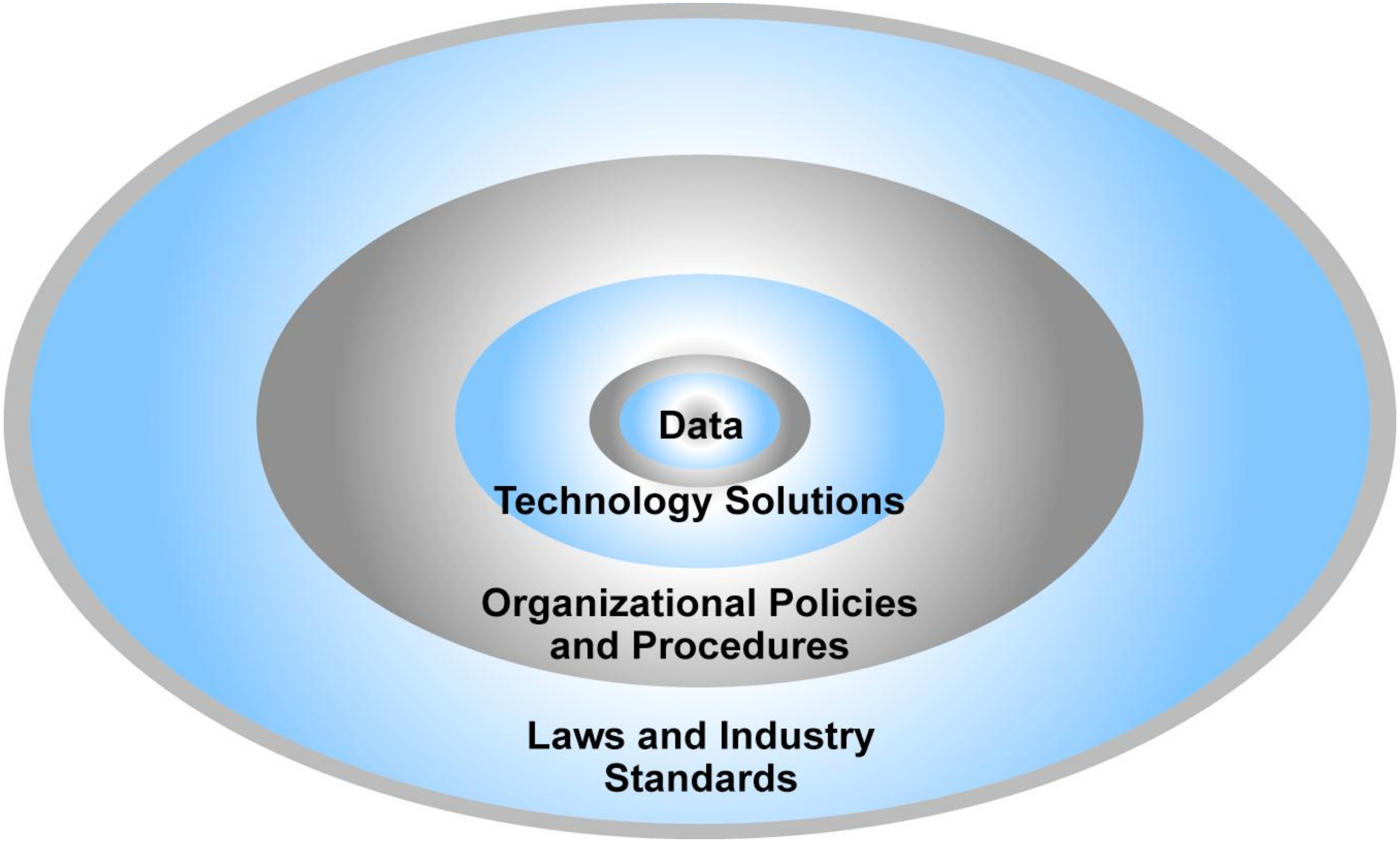


What Is Good E-commerce Security?

- 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 5.4, Page 267


Data
Technology Solutions
Organizational Policies and Procedures
Laws and Industry Standards

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

Table 5.2, Page 268

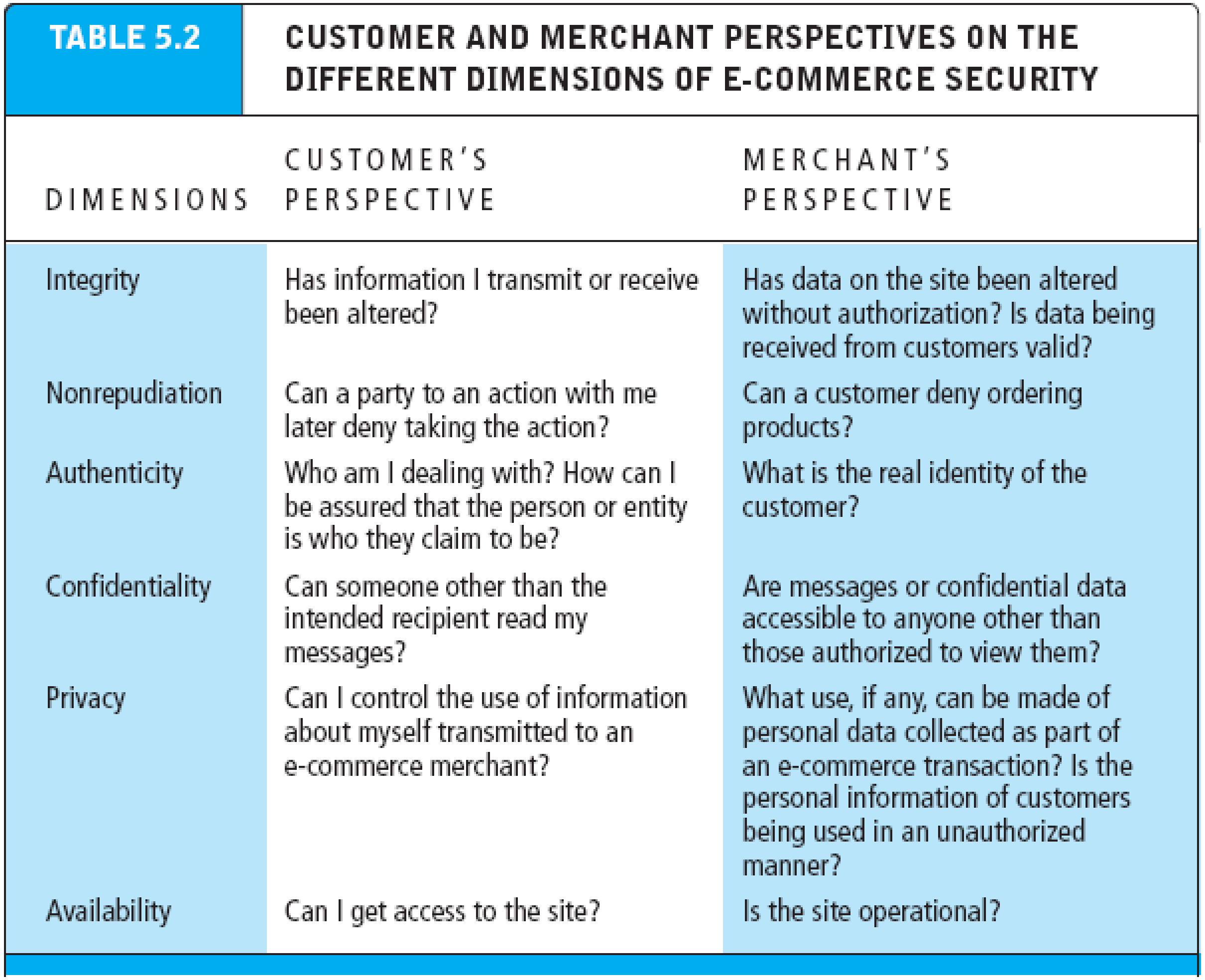


TABLE 5.2 CUSTOMER AND MERCHANT PERSPECTIVES ON THE DIFFERENT DIMENSIONS OF E-COMMERCE SECURITY

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

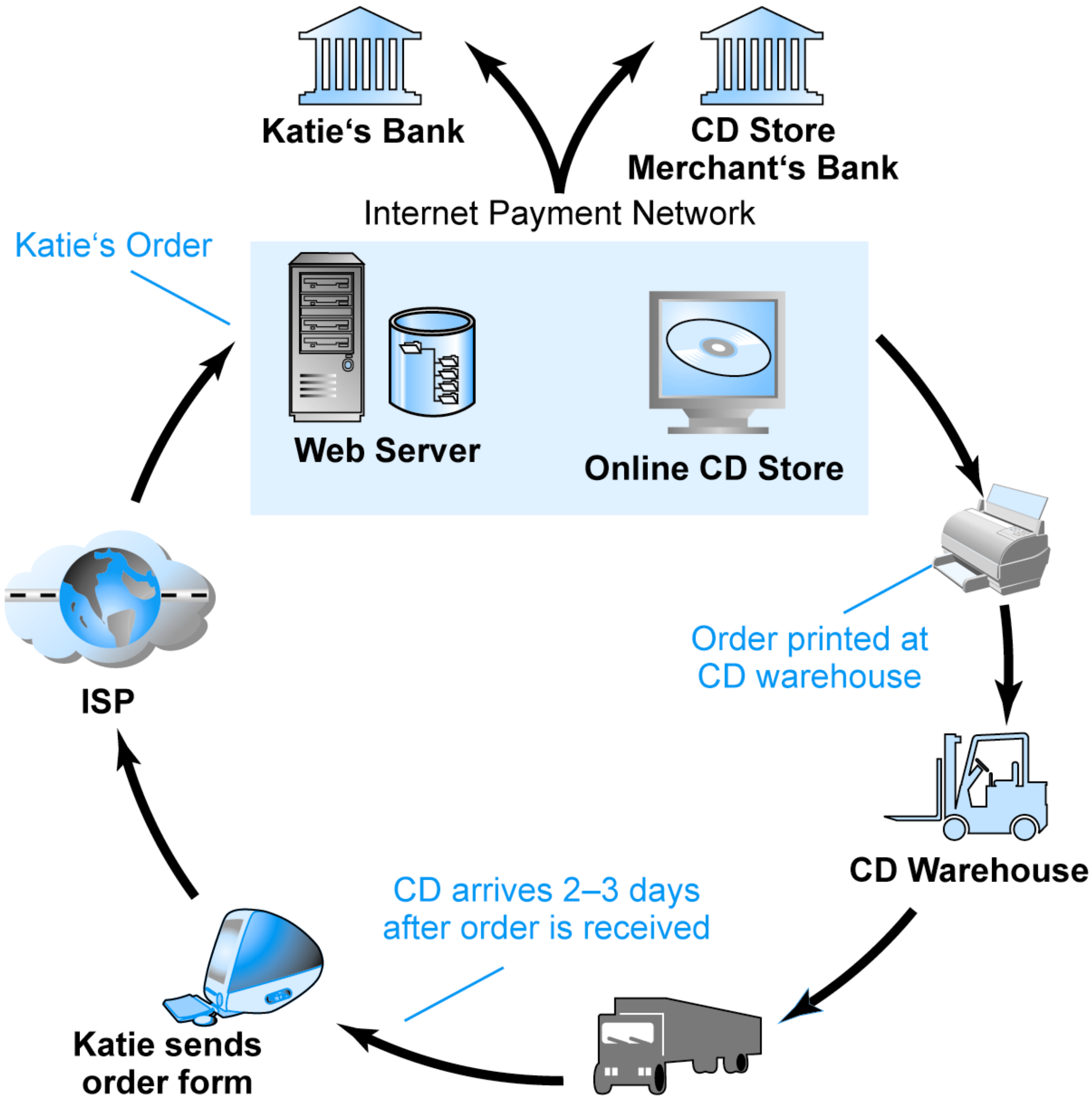
- Security vs. ease of use:
  - The more security measures added, the more difficult a site is to use, and the slower it becomes
- Security vs. desire of individuals to act anonymously
  - Use of technology by criminals to plan crimes or threaten nation-state

Security Threats in the E-commerce Environment

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

A Typical E-commerce Transaction

Figure 5.5, Page 270



SOURCE: Boncella, 2000.

Vulnerable Points in an E-commerce Environment

Figure 5.6, Page 271

Security Risks

Internet communications

Tapping and sniffing
Alteration of messages
Theft and fraud

Servers

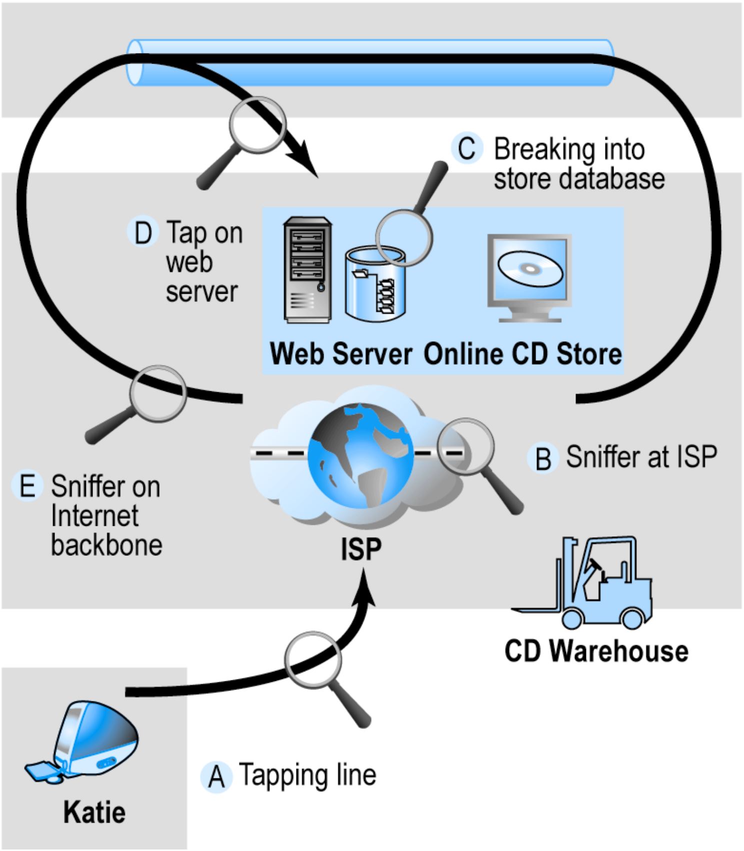
ISP
Merchant
Banks

DoS attack
Hacking
Malicious code attack
Theft and fraud
Line taps
Vandalism

Clients

Business
Home

Malicious code attack
Line taps
Physical loss of computer



SOURCE: Boncella, 2000.

Most Common Security Threats in the E-commerce Environment

- Malicious code (viruses, worms, Trojans)
- Unwanted programs (spyware, browser parasites)
- Phishing/identity theft
- Hacking and cybervandalism
- Credit card fraud/theft
- Spoofing (pharming)/spam (junk) Web sites
- DoS and DDoS attacks
- Sniffing
- Insider attacks
- Poorly designed server and client software

Unwanted Programs

- Installed without user’s informed consent
  - Browser parasites
    - Can monitor and change settings of a user’s browser
  - Adware
    - Calls for unwanted pop-up ads
  - Spyware
    - Can be used to obtain information, such as a user’s keystrokes, e-mail, IMs, etc.

Phishing and Identity Theft

- Any deceptive, online attempt by a third party to obtain confidential information for financial gain, e.g.
  - E-mail scam letter – most popular phishing attack
  - Spoofing legitimate financial institution’s Web site
- Use information to commit fraudulent acts (access checking accounts), steal identity
- One of fastest growing forms of e-commerce crime

Hacking and Cybervandalism

- Hacker:

  Individual who intends to gain access to computer systems beyond normal expectations. For example hacking into msconfig or registry file to improve computer performance.

- Cybervandalism:

  Intentionally disrupting, defacing, destroying Web site

- Types of hackers
  - White hats
  - Black hats/Cracker: Hacker with criminal intent
  - Grey hats

Credit Card Fraud

- Fear of stolen credit card information 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
- Online companies at higher risk than offline
- In development: New identity verification mechanisms

Spoofing (Pharming) and Spam (Junk) Web Sites

- Spoofing (Pharming)
  - Misrepresenting oneself by using fake e-mail addresses or masquerading as someone else
  - Threatens integrity of site; authenticity
- Spam (Junk) Web sites
  - Use domain names similar to legitimate one, redirect traffic to spammer-redirection domains

Other Security Threats

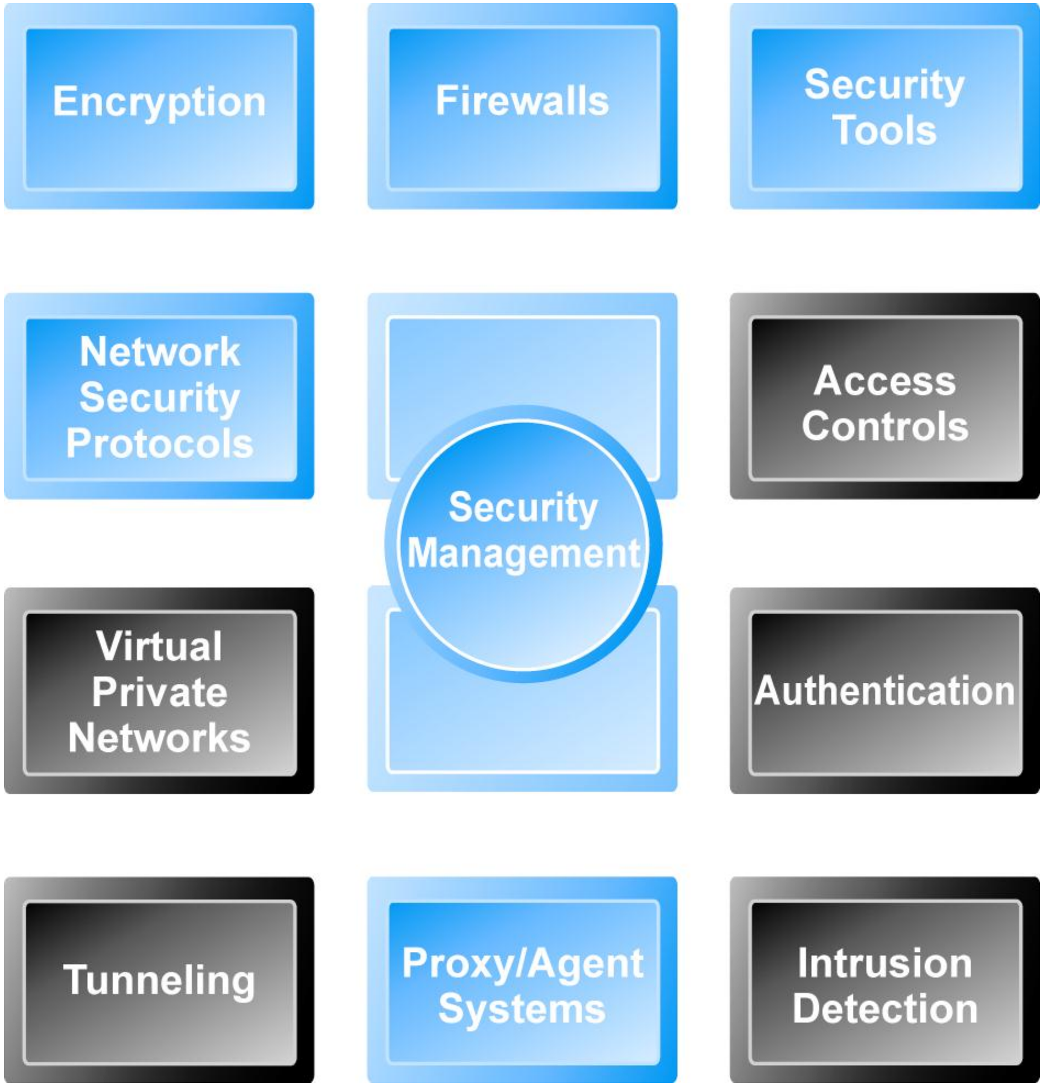
- Sniffing:
  - Eavesdropping program that monitors information traveling over a network; enables hackers to steal proprietary information from anywhere on a network
- Insider jobs
  - Single largest financial threat
- Poorly designed server and client software
  - Increase in complexity of software programs has contributed to 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 5.9, Page 284



Protecting Internet Communications: Encryption

- Encryption
  - Transforming plain text, data into cipher text that can’t be read by anyone other than sender and receiver
  - Secures stored information and information transmission
  - Provides:
    - Message integrity
    - Nonrepudiation
    - Authentication
    - Confidentiality

Symmetric Key Encryption

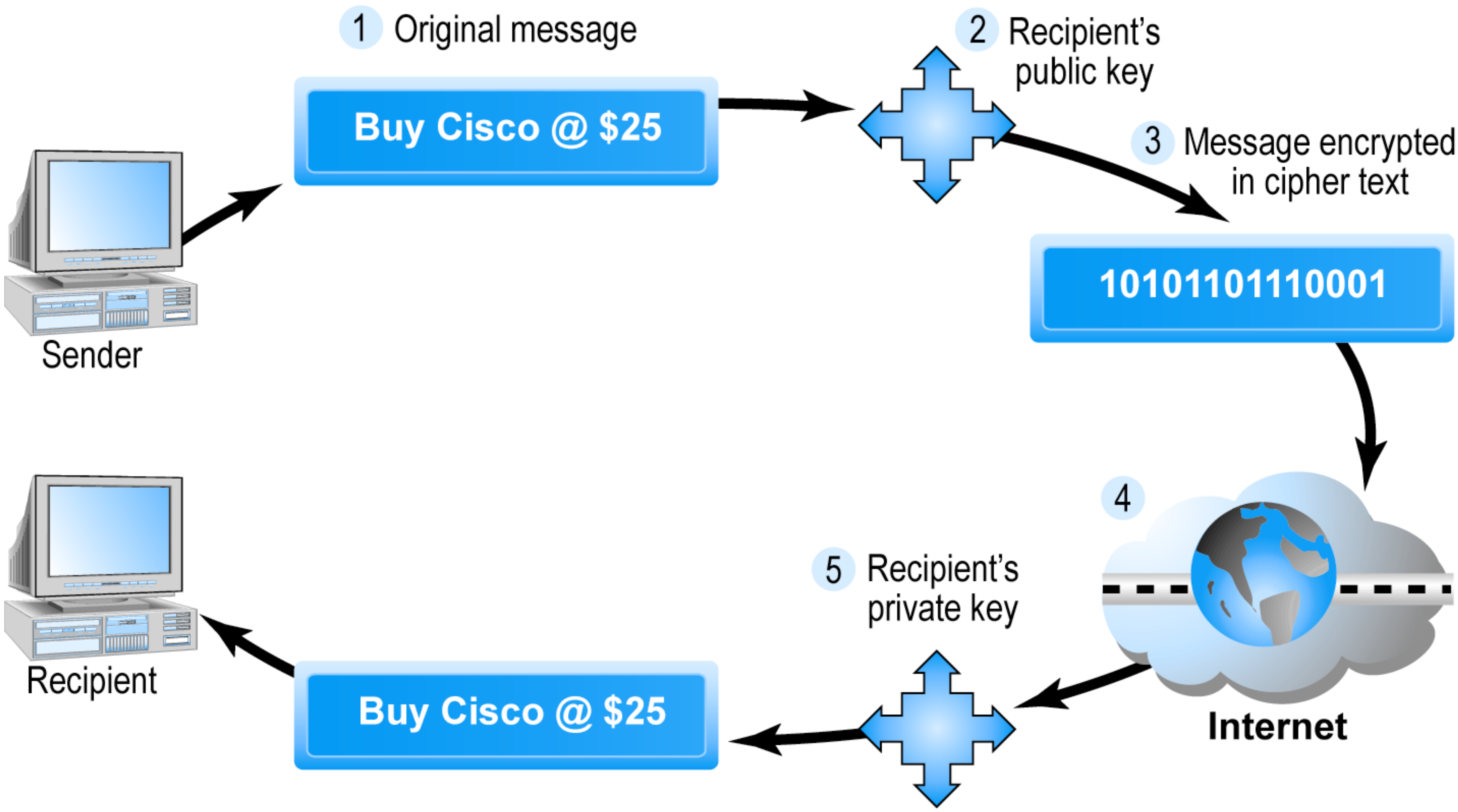
- Also known as secret key encryption
- Both sender and receiver use same digital key to encrypt and decrypt message
- Requires different set of keys for each transaction
- Advanced Encryption Standard (AES)
  - Most widely used symmetric key encryption
  - Uses 128-, 192-, and 256-bit encryption keys
- Other standards use keys with up to 2,048 bits

Public Key Encryption

- Uses two mathematically related digital keys: Public key (widely disseminated) and 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 his/her private key to decrypt it
- Disadvantages?

Public Key Cryptography – A Simple Case

Figure 5.10, Page 283

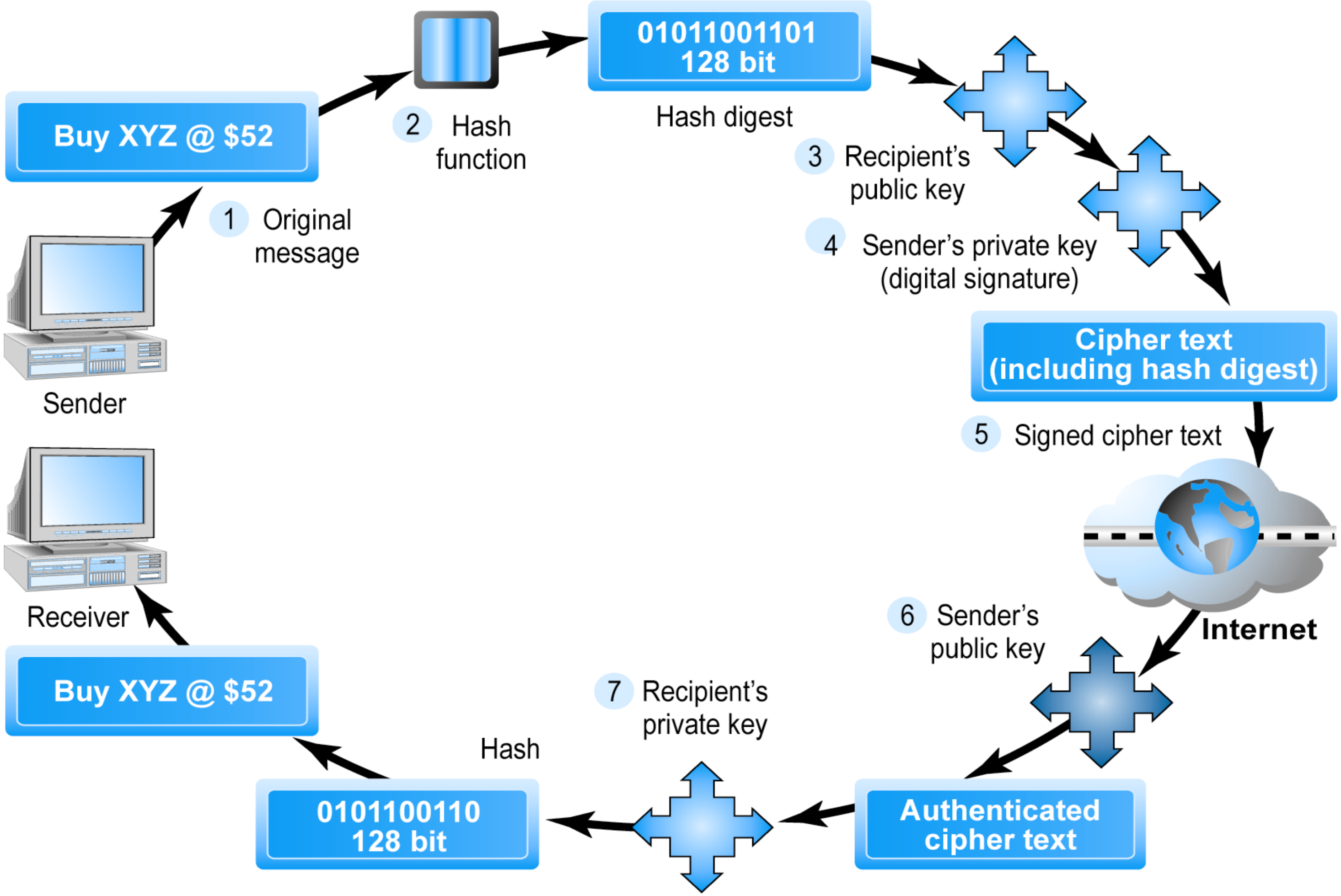


Public Key Encryption using Digital Signatures and Hash Digests

- Hash function: Mathematical algorithm that produces fixed-length number (128 bits) called message or hash digest. Apply hash function on the message to create a 128 bit hash result.
- Hash digest and message encrypted with recipient's public key.
- Entire cipher text then encrypted with sender's private key – creating digital signature – for authenticity, nonrepudiation (only sender could create digital signature)
- Receiver uses sender public key to open the message to authenticate it.
- Receiver then uses his/her private key to open the cypher text. Then the message is verified using hash result .
- Weaknesses: Four keys: public and private for sender and receiver. Slow

Public Key Cryptography with Digital Signatures

Figure 5.11, Page 288



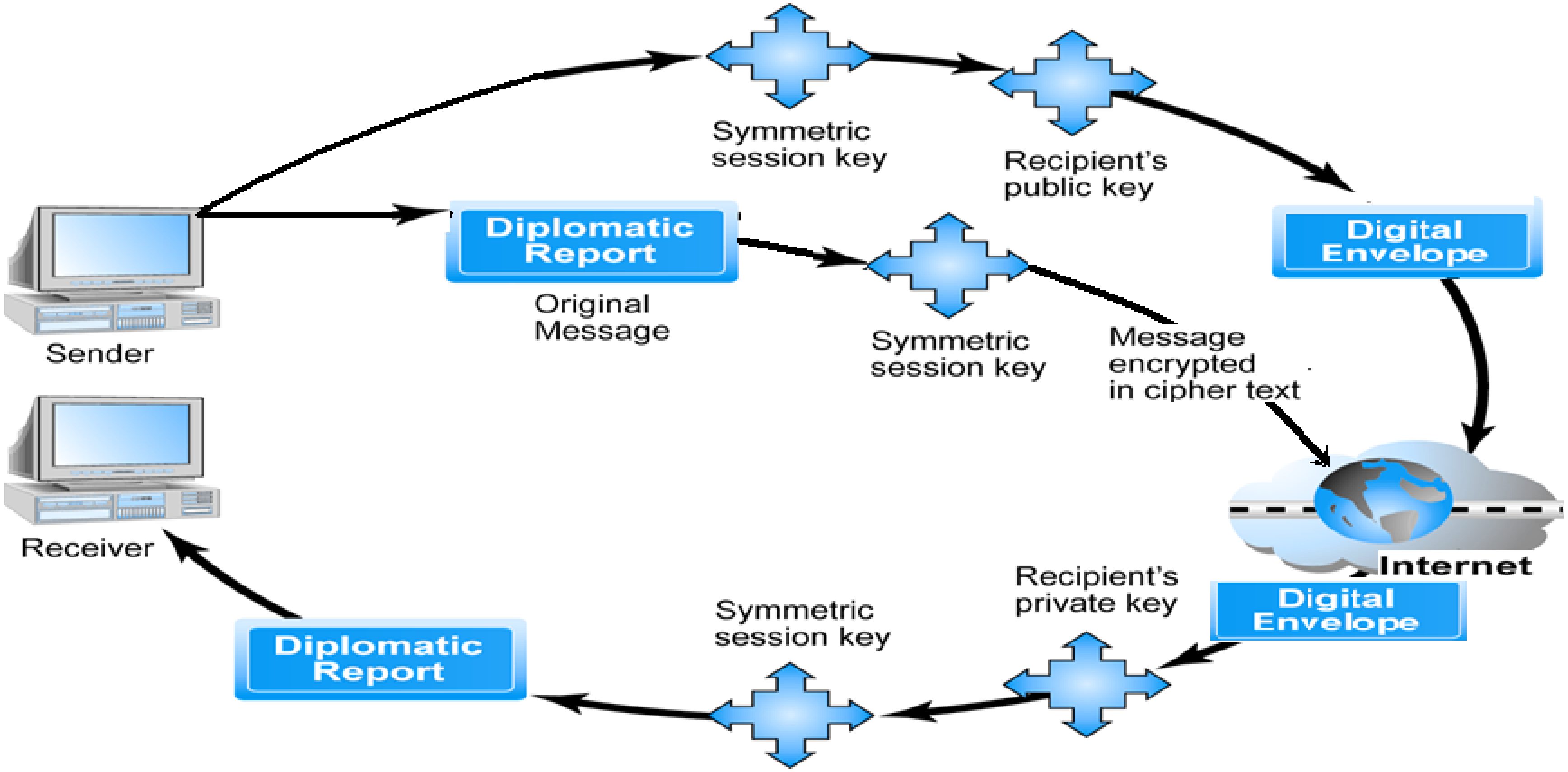
Weakness: slow, solution: Digital Envelope

Digital Envelopes

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

Public Key Cryptography: Creating a Digital Envelope

Figure 5.12, Page 290



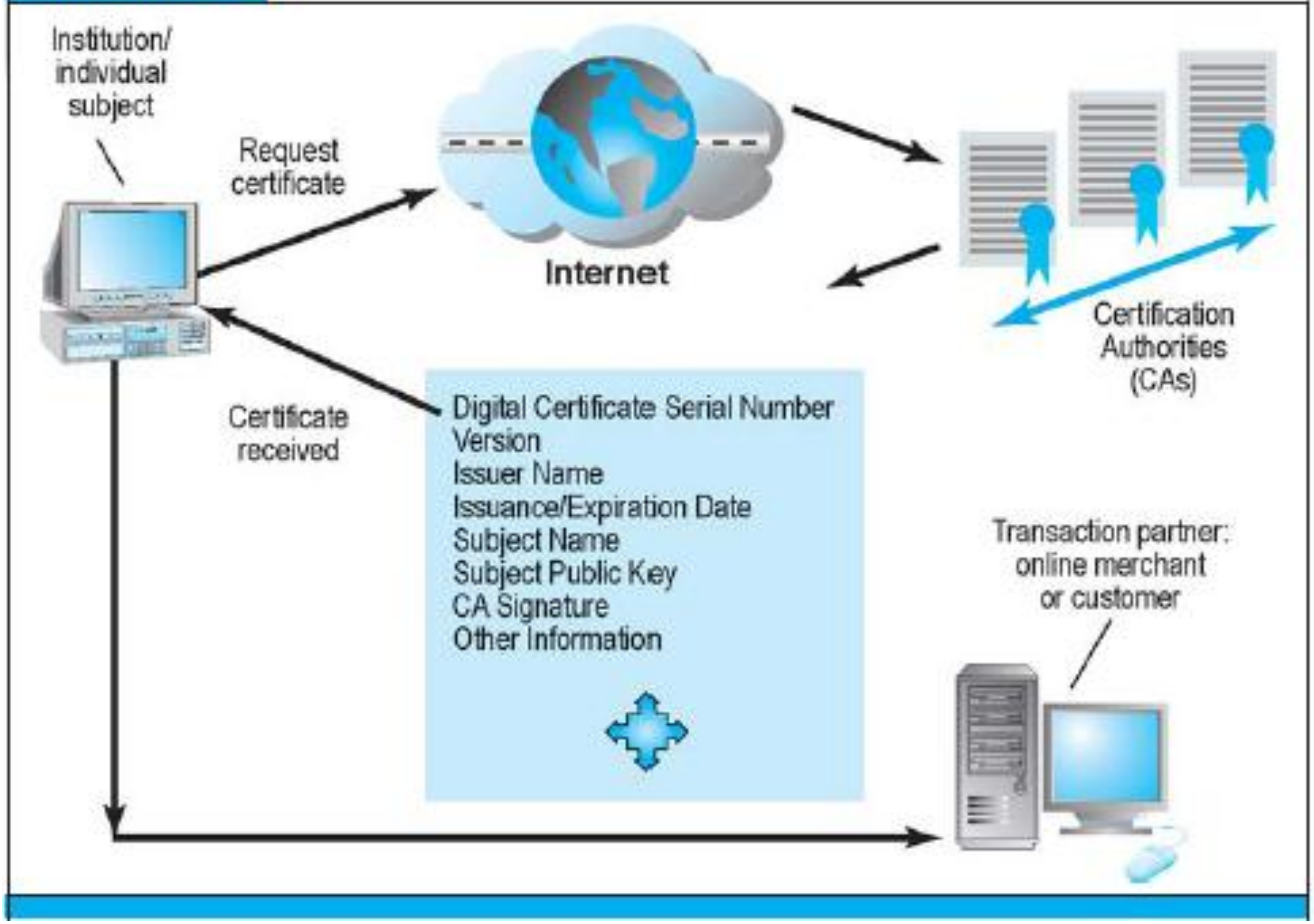
Digital Certificates and Public Key Infrastructure (PKI)

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

Digital Certificates and Certification Authorities

Figure 5.13, Page 291

FIGURE 5.13 DIGITAL CERTIFICATES AND CERTIFICATION AUTHORITIES



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 Society

In Pursuit of E-mail Privacy

Class Discussion

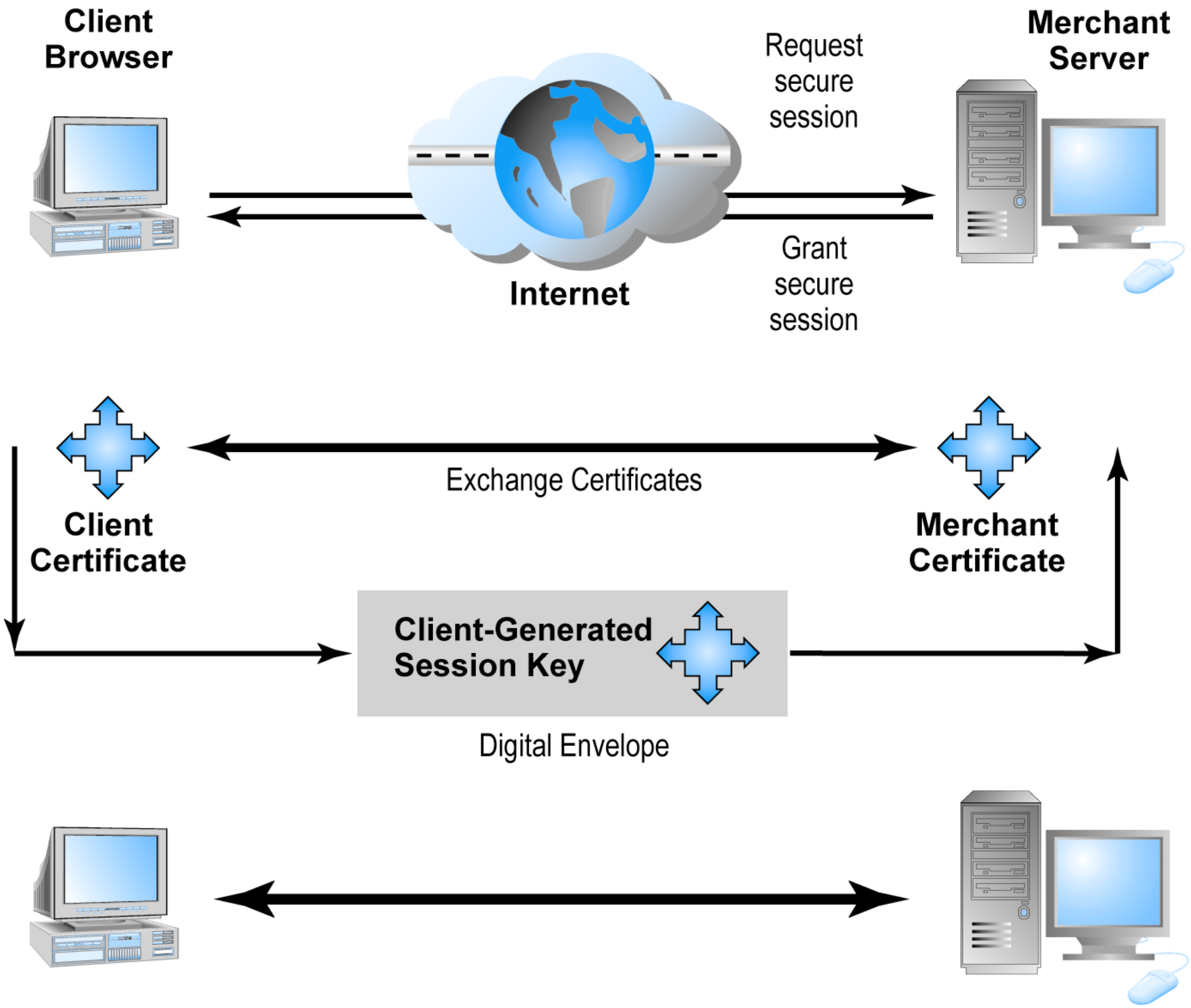
- What are some of the current risks and problems with using e-mail?
- What are some of the technology solutions that have been developed?
- Are these solutions compatible with modern law?
- Consider the benefits of a thorough business record retention policy. Do you agree that these benefits are worth giving up some control of your e-mail?

Securing Channels of Communication

- Secure Sockets Layer (SSL):
  - Establishes a secure, negotiated client-server session in which URL of requested document, along with contents, is encrypted
  - SET Protocol: Requires digital certificate
- S-HTTP:
  - Provides a secure message-oriented communications protocol designed for use in conjunction with HTTP
- Virtual Private Network (VPN):
  - Allows remote users to securely access internal network via the Internet, using Point-to-Point Tunneling Protocol (PPTP)

Secure Negotiated Sessions Using SSL

Figure 5.14, Page 295



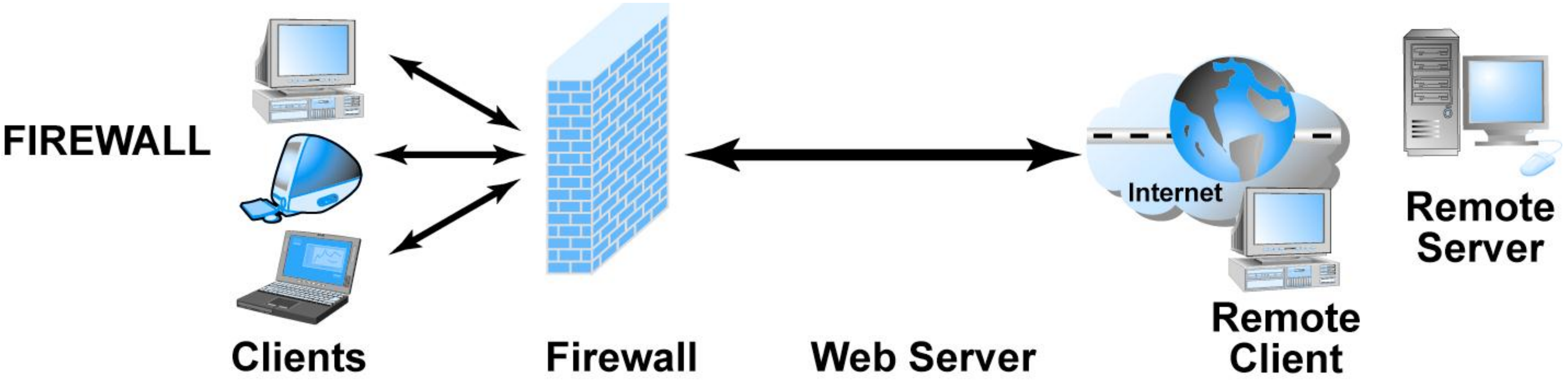
Session ID and methods of encryption negotiated.

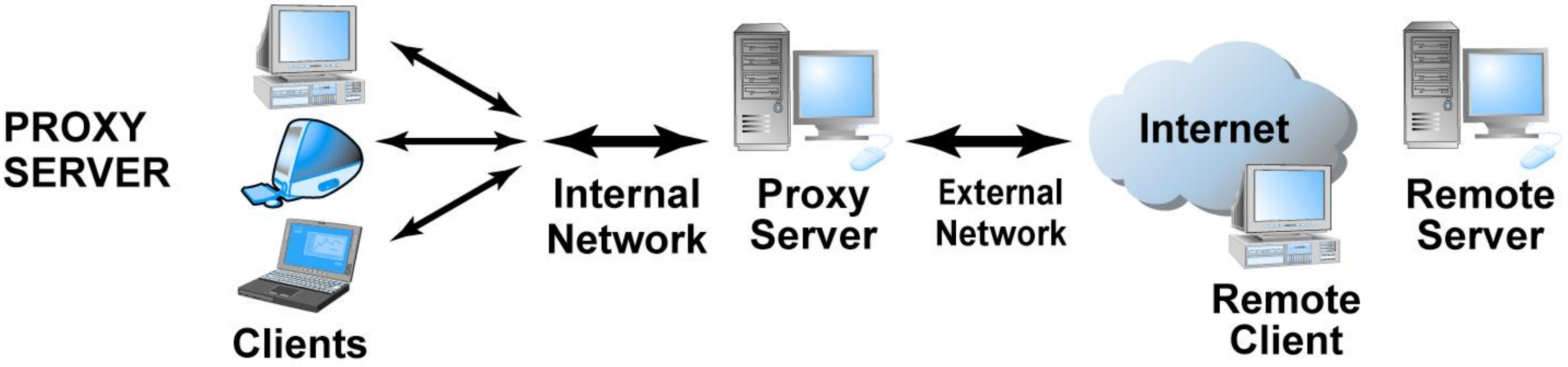
Certificates exchanged. Identity of both parties established.

Client generates session key, and uses server public key to create digital envelope. Sends to server. Server decrypts using private key.

Encrypted transmission using client-generated session key begins.

Protecting Networks: Firewalls and Proxy Servers





Protecting Servers and Clients

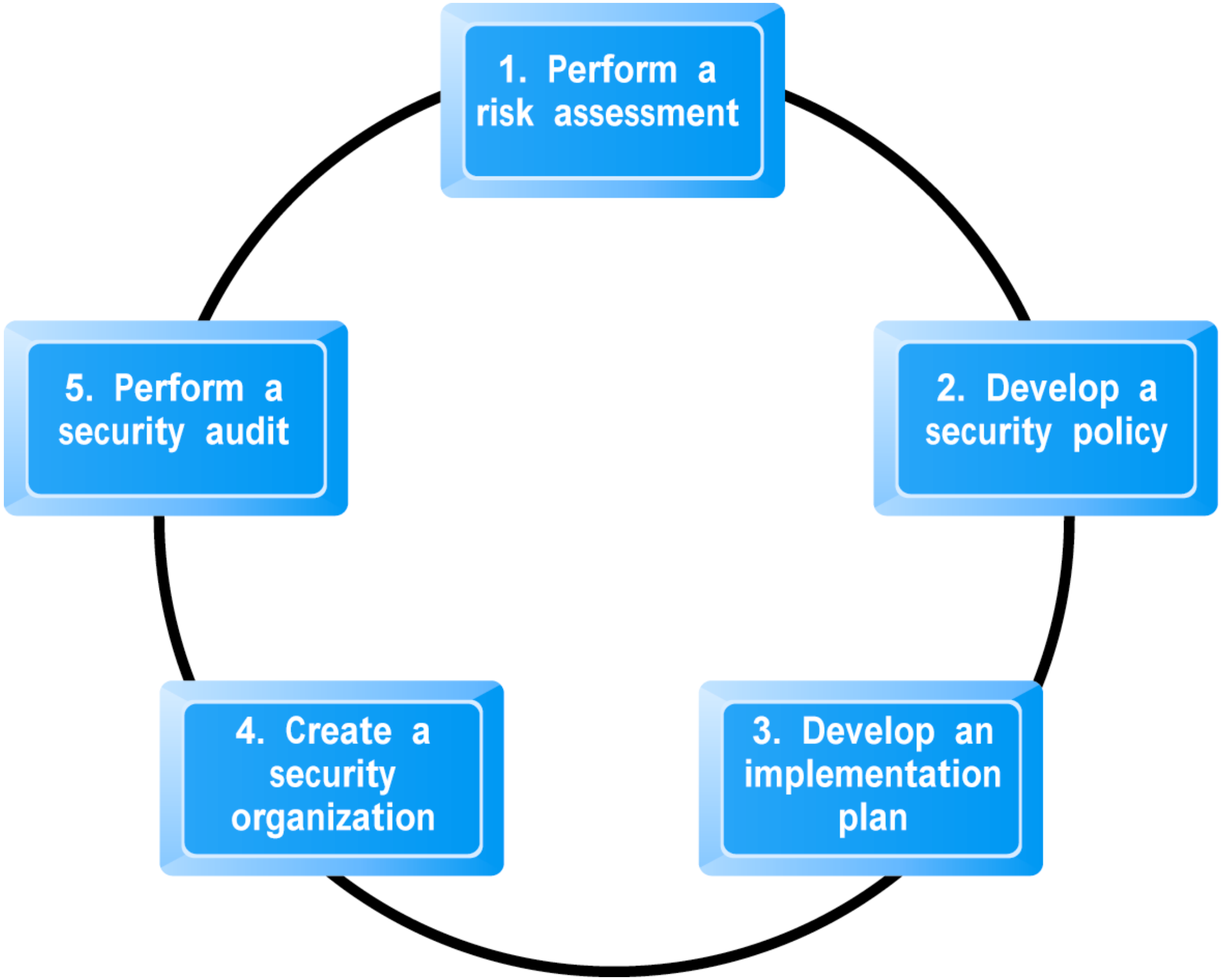
- Operating system controls:
  - Authentication and access control mechanisms
- Anti-virus software:
  - Easiest and least expensive way to prevent threats to system integrity
  - Requires daily updates

A Security Plan: Management Policies

- Risk assessment
- Security policy
- Implementation plan
    - Security organization
    - Access controls
    - Authentication: Multi-faction
    - Authorization policies
        - Authorization management systems
- Security audit

Developing an E-commerce Security Plan

Figure 5.16, Page 300


1. Perform a risk assessment
2. Develop a security policy
3. Develop an implementation plan
4. Create a security organization
5. Perform a security audit

The Role of Laws and Public Policy

- New laws have given authorities tools and mechanisms for identifying, tracing, prosecuting cybercriminals
  - National Information Infrastructure Protection Act of 1996: created National Infrastructure Protection Center
  - USA Patriot Act
  - Homeland Security Act
- CERT Coordination Center – private group
- Government policies and controls on encryption software
- OECD guidelines

Types of Payment Systems

- Cash
- Checking Transfer
- Credit Card
- Stored Value
- Accumulating Balance

E-commerce Payment Systems

- Credit cards are dominant form of online payment, accounting for around 60% of online payments in 2008
- Other e-commerce payment systems:
  - Digital wallets
  - Digital cash. Deposit money or credit card.
  - Online stored value payment systems. PayPal, Smartcards (contact and contacless).
  - Digital accumulating balance systems
  - Digital checking: PayByCheck

Digital Wallets

- Seeks to emulate the functionality of traditional wallet
- Most important functions:
  - Authenticate consumer through use of digital certificates or other encryption methods
  - Store and transfer value
  - Secure payment process from consumer to merchant
- Early efforts to popularize have failed
- Newest effort: Google Checkout

Online Stored Value Systems

- Permit consumers to make instant, online payments to merchants and other individuals
- Based on value stored in a consumer's bank, checking, or credit card account
- PayPal most successful system
- Smart cards
  - Contact smart cards: Require physical reader
    - Mondex
  - Contactless smart cards: Use RFID
    - EZPass
    - Octopus

Digital Accumulating Balance Payment Systems

- Allows users to make micropayments and purchases on the Web
- Users accumulate a debit balance for which they are billed at the end of the month
- Valista's PaymentsPlus
- Clickshare

Digital Checking Payment Systems

- Extends functionality of existing checking accounts for use as online shopping payment tool
- Example: PayByCheck

Wireless Payment Systems

- Use of mobile handsets as payment devices well-established in Europe, Japan, South Korea
- Japanese mobile payment systems
  - E-money (stored value)
  - Mobile debit cards
  - Mobile credit cards
- Not as well established yet in U.S, but with growth in Wi-Fi and 3G cellular phone systems, this is beginning to change

Electronic Billing Presentment and Payment (EBPP)

- Online payment systems for monthly bills
- 50% of households in 2008 used some EBPP; expected to grow to 75% by 2012
- Two competing EBPP business models:
  - Biller-direct: Dominant model
  - Consolidator: Third party aggregates consumer’s bills
- Both models are supported by EBPP infrastructure providers