COURSE TECHNOLOGY
CENGAGE Learning™

E-Business
Tenth Edition

Chapter 10
Online Security

Learning Objectives

In this chapter, you will learn:

- What security risks arise in online business and how to manage them
- How to create a security policy
- How to implement security on Web client computers
- How to implement security in the communication channels between computers

Learning Objectives (cont'd.)

- How to implement security on Web server computers
- What organizations promote computer, network, and Internet security

Online Security Issues Overview

- Early Internet days
  - Most popular use: electronic mail
- Today's higher stakes
  - Electronic mail, shopping, all types of financial transactions
- Common worry of Web shoppers
  - Stolen credit card as it transmits over the Internet
  - More likely to be stolen from computer where stored
- Chapter topic: security in the context of electronic commerce

Origins of Security on Interconnected Computer Systems

- Data security measures taken by Roman Empire
  - Coded information to prevent enemies from reading secret war and defense plans
- Modern electronic security techniques
  - Defense Department wartime use
    - "Orange Book": rules for mandatory access control
- Business computers
  - Initially adopted military's security methods
- Today's computing
  - Requires comprehensive computer security plans

Computer Security and Risk Management

- **Computer security**
  - Asset protection from unauthorized access, use, alteration, and destruction
- **Physical security**
  - Includes tangible protection devices
    - Alarms, guards, fireproof doors, security fences, safes or vaults, and bombproof buildings
- **Logical security**
  - Asset protection using nonphysical means

Computer Security and Risk Management (cont'd.)

- **Threat**
  - Any act or object posing danger to computer assets
- **Countermeasure**
  - Procedure (physical or logical)
    - Recognizes, reduces, and eliminates threat
  - Extent and expense of countermeasures
    - Vary depending on asset importance

Computer Security and Risk Management (cont'd.)

- Risk management model
  - Four general organizational actions
    - Impact (cost) and probability of physical threat
  - Also applicable for protecting Internet and electronic commerce assets from physical and electronic threats
- Electronic threat examples:
  - Impostors, eavesdroppers, thieves
- **Eavesdropper** (person or device)
  - Listen in on and copy Internet transmissions

Computer Security and Risk Management (cont'd.)

- **Crackers** or **hackers** (people)
  - Write programs; manipulate technologies
    - Obtain unauthorized access to computers and networks
- **White hat hacker** and **black hat hacker**
  - Distinction between good hackers and bad hackers
- Good security scheme implementation
  - Identify risks
  - Determine how to protect threatened assets
  - Calculate costs to protect assets

Elements of Computer Security

- **Secrecy**
  - Protecting against unauthorized data disclosure
  - Ensuring data source authenticity
- **Integrity**
  - Preventing unauthorized data modification
  - **Man-in-the-middle exploit**
    - E-mail message intercepted; contents changed before forwarded to original destination
- **Necessity**
  - Preventing data delays or denials (removal)
  - Delaying message or completely destroying it

Establishing a Security Policy

- **Security policy**
  - Assets to protect and why, protection responsibility, acceptable and unacceptable behaviors
  - Physical security, network security, access authorizations, virus protection, disaster recovery
- Military policy: stresses separation of multiple levels of security
- Corporate information classifications
  - Public
  - Company confidential

Establishing a Security Policy (cont'd.)

- Steps to create security policy
  - Determine assets to protect from threats
  - Determine access to various system parts
  - Identify resources to protect assets
  - Develop written security policy
  - Commit resources
- Comprehensive security plan goals
  - Protect privacy, integrity, availability; authentication
  - Selected to satisfy Figure 10-2 requirements

Establishing a Security Policy (cont'd.)

- Security policies information sources
  - WindowSecurity.com site
  - Information Security Policy World site
- Absolute security: difficult to achieve
  - Create barriers deterring intentional violators
  - Reduce impact of natural disasters and terrorist acts
- Integrated security
  - Having all security measures work together
    - Prevents unauthorized disclosure, destruction, modification of assets

Establishing a Security Policy (cont'd.)

- Security policy points
  - Authentication: Who is trying to access site?
  - Access control: Who is allowed to log on to and access site?
  - Secrecy: Who is permitted to view selected information?
  - Data integrity: Who is allowed to change data?
  - Audit: Who or what causes specific events to occur, and when?

Security for Client Computers

- Client computers
  - Must be protected from threats
- Threats
  - Originate in software and downloaded data
  - Malevolent server site masquerades as legitimate Web site
- Chapter topics organized to follow the transaction-processing flow
  - Beginning with consumer
  - Ending with Web server at electronic commerce site

Cookies and Web Bugs

- Internet connection between Web clients and servers
  - **Stateless connection**
    - Each information transmission is independent
    - No continuous connection (**open session**) maintained between any client and server
- Cookies
  - Small text files Web servers place on Web client
  - Identify returning visitors
  - Allow continuing open session

Cookies and Web Bugs (cont'd.)

- Time duration cookie categories
  - **Session cookies**: exist until client connection ends
  - **Persistent cookies**: remain indefinitely
  - Electronic commerce sites use both
- Cookie sources
  - **First-party cookies**
    - Web server site places them on client computer
  - **Third-party cookies**
    - Different Web site places them on client computer

Cookies and Web Bugs (cont'd.)

- Disable cookies entirely
  - Complete cookie protection
  - Problem
    - Useful cookies blocked (along with others)
    - Full site resources not available
- Web browser cookie management functions
  - Refuse only third-party cookies
  - Review each cookie before accepted
  - Provided by most Web browsers

Cookies and Web Bugs (cont'd.)

- **Web bug**
  - Tiny graphic that third-party Web site places on another site's Web page
  - Purpose
    - Provide a way for a third-party site to place cookie on visitor's computer
- Internet advertising community:
  - Calls Web bugs "clear GIFs" or "1-by-1 GIFs"
    - Graphics created in GIF format
    - Color value of "transparent," small as 1 pixel by 1 pixel

Active Content

- **Active content**
  - Programs embedded transparently in Web pages
  - Cause action to occur
  - E-commerce example
    - Place items into shopping cart; compute tax and costs
- Advantages
  - Extends HTML functionality
  - Moves data processing chores to client computer
- Disadvantages
  - Can damage client computer

Active Content (cont'd.)

- Crackers: embed malicious active content
- **Trojan horse**
  - Program hidden inside another program or Web page
    - Masking true purpose
  - May result in secrecy and integrity violations
- **Zombie** (Trojan horse)
  - Secretly takes over another computer
  - Launches attacks on other computers
- **Botnet** (**robotic network**, **zombie farm**)
  - All controlled computers act as an attacking unit

Graphics and Plug-Ins

- Graphics, browser plug-ins, and e-mail attachments can harbor executable content
- Graphic: embedded code can harm client computer
- Browser **plug-ins** (programs)
  - Enhance browser capabilities
  - Popular plug-ins: Adobe Flash Player, Apple's QuickTime Player, Microsoft Silverlight, RealNetworks' RealPlayer
  - Can pose security threats
    - 1999 RealPlayer plug-in
    - Plug-ins executing commands buried within media

Viruses, Worms, and Antivirus Software

- Programs display e-mail attachments by automatically executing associated programs
  - Macro viruses within attached files can cause damage
- Virus: software
  - Attaches itself to another program
  - Causes damage when host program activated
- **Worm**: virus
  - Replicates itself on computers it infects
  - Spreads quickly through the Internet
- **Macro virus**
  - Small program (macro) embedded in file

Viruses, Worms, and Antivirus Software (cont'd.)

- ILOVEYOU virus ("love bug")
  - Spread with amazing speed
  - Infected computers and clogged e-mail systems
  - Replicated itself explosively through Outlook e-mail
  - Caused other harm
- 2001 Code Red and Nimda: virus-worm combinations
  - **Multivector virus**: entered computer system in several different ways (vectors)
- 2002 and 2003: new virus-worm combinations
  - Example: Bugbear

Viruses, Worms, and Antivirus Software (cont'd.)

- **Antivirus software**
  - Detects viruses and worms
  - Either deletes or isolates them on client computer
- 2005 and 2006 Zotob
  - New breed of Trojan horse-worm combination
- 2007: Storm virus
- 2008 and continuing into 2009: Conflicker
- 2009 and 2010: URLzone and Clampi
  - New viruses designed specifically to hijack users' online banking sessions

Viruses, Worms, and Antivirus Software (cont'd.)

- 2010: new Trojan horse-worm combination attack
  - Spread through a computer operating system
  - Designed to target industrial equipment
    - German industrial giant Siemens' control systems
- 2011: Zeus and SpyEye combined
  - Targeted bank account information
  - Not visible in Microsoft Windows Task Manager
  - Intercept credit card or online banking data entered in Web browser

Viruses, Worms, and Antivirus Software (cont'd.)

- Companies that track viruses, sell antivirus software, provide virus descriptions on Web sites
  - Symantec (Symantec Security Response)
  - McAfee (McAfee Virus Information)
- Data files must be updated regularly
  - Recognize and eliminate newest viruses
- Some Web e-mail systems:
  - Provide and update antivirus software
    - Used to scan attachments before downloading
  - Example: Yahoo! Mail

Digital Certificates

- **Digital certificate** (**digital ID**)
  - E-mail message attachment or program embedded in Web page
  - Verifies sender or Web site
  - Contains a means to send encrypted message
  - **Signed** message or code
    - Provides proof of holder identified by the certificate
  - Used for online transactions
    - Electronic commerce, electronic mail, and electronic funds transfers

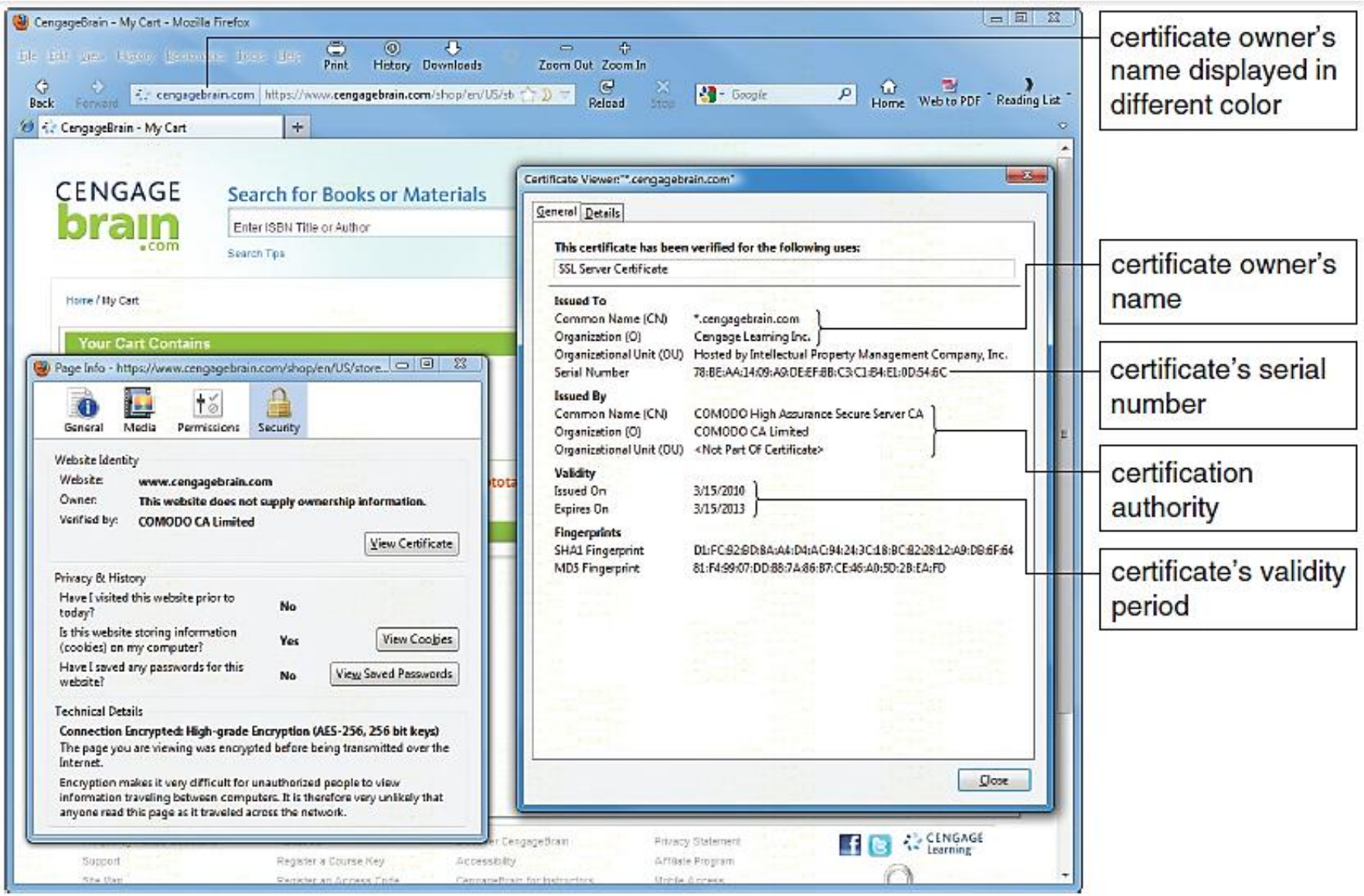

FIGURE 10-7 Delmar Cengage Learning's digital certificate information displayed in Firefox browser

Digital Certificates (cont'd.)

- Digital certificate for software:
  - Assurance software was created by specific company
  - Does not attest to quality of software
- **Certification authority** (**CA**)
  - Issues digital certificates to organizations, individuals
- Digital certificates cannot be forged easily
- Six main elements: owner's identifying information, owner's public key, dates certificate is valid, serial number, issuer name, issuer digital signature

Digital Certificates (cont'd.)

- **Key**
  - Number: usually long binary number
    - Used with encryption algorithm
    - "Lock" message characters being protected
  - Longer keys provide better protection
- Identification requirements vary
  - Driver's license, notarized form, fingerprints
- Companies offering CA services
  - Thawte, VeriSign, Comodo, DigiCert, Entrust, GeoTrust, RapidSSL.com

Digital Certificates (cont'd.)

- **Secure Sockets Layer-Extended Validation (SSL-EV) digital certificate**
  - Issued after more extensive verification confirmed
- Annual fees
  - $200 to more than $1500
- Digital certificates expire after period of time
  - Provides protection (users and businesses)
  - Must submit credentials for reevaluation periodically

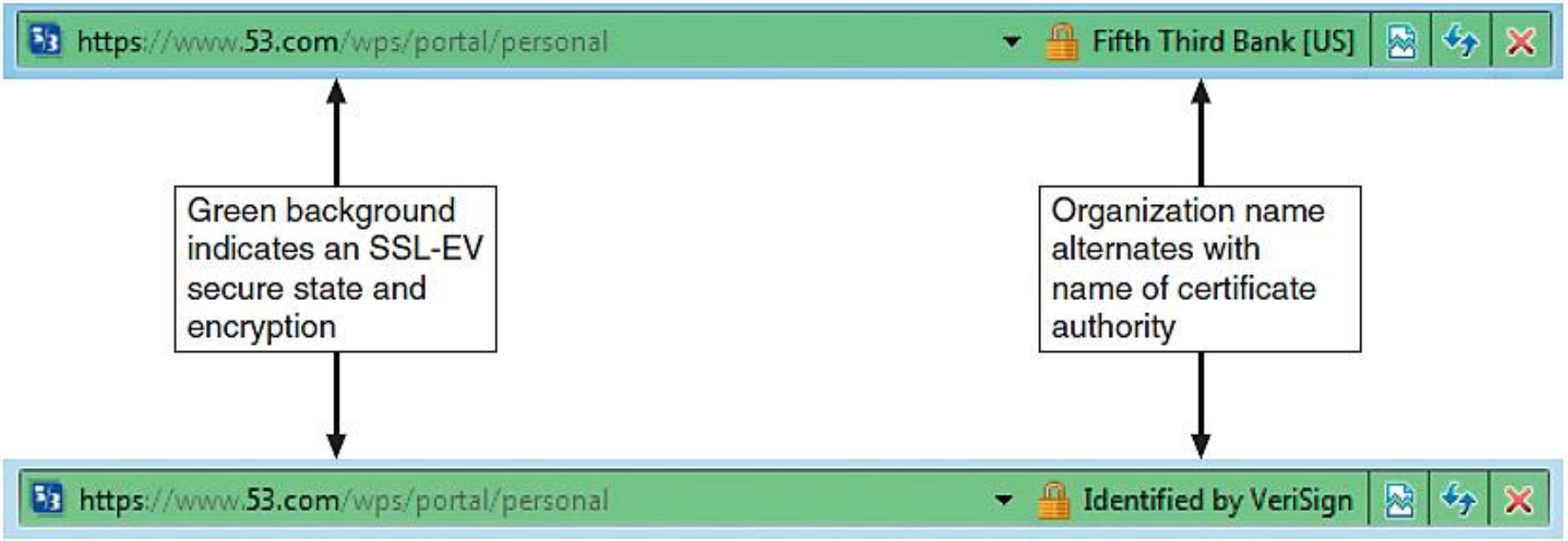

FIGURE 10-8 Internet Explorer address window display for an SSL-EV Web site

Steganography

- **Steganography**
  - Hiding information within another piece of information
- Can be used for malicious purposes
- Hiding encrypted file within another file
  - Casual observer cannot detect anything of importance in container file
  - Two-step process
    - Encrypting file protects it from being read
    - Steganography makes it invisible
- Al Qaeda used steganography to hide attack orders

Physical Security for Clients

- Client computers
  - Control important business functions
  - Same physical security as early systems
- New physical security technologies
  - Fingerprint readers (less than $100)
    - Stronger protection than password approaches
- **Biometric security device**
  - Identification using element of person's biological makeup
    - Writing pads, eye scanners, palm reading scanners, reading back of hand vein pattern

Client Security for Mobile Devices

- Security measures
  - Access password
  - **Remote wipe**: clears all personal data
    - Can be added as an app
    - Capability through corporate e-mail synchronization
  - Antivirus software
- **Rogue apps**: contain malware or collect information and forward to perpetrators
  - Apple App Store tests apps before authorizing sales
  - Android Market does less extensive testing
  - Users should not rush to install latest app

Communication Channel Security

- Internet
  - Not designed to be secure
  - Designed to provide redundancy
- Remains unchanged from original insecure state
  - Message traveling on the Internet
    - Subject to secrecy, integrity, and necessity threats

Secrecy Threats

- **Secrecy**
  - Prevention of unauthorized information disclosure
  - Technical issue
    - Requiring sophisticated physical and logical mechanisms
- **Privacy**
  - Protection of individual rights to nondisclosure
  - Legal matter

Secrecy Threats (cont'd.)

- E-mail message
  - Secrecy violations protected using encryption
    - Protects outgoing messages
  - Privacy issues address whether supervisors are permitted to read employees' messages randomly
- Electronic commerce threat
  - Sensitive or personal information theft
  - **Sniffer programs**
    - Record information passing through computer or router

Secrecy Threats (cont'd.)

- Electronic commerce threat (cont'd.)
  - **Backdoor**: electronic holes
    - Left open accidentally or intentionally
    - Content exposed to secrecy threats
    - Example: Cart32 shopping cart program backdoor
  - Stolen corporate information
    - Eavesdropper example
- Web users continually reveal information
  - Secrecy breach
  - Possible solution: anonymous Web surfing

Integrity Threats

- Also known as **active wiretapping**
  - Unauthorized party alters message information stream
- Integrity violation example
  - **Cybervandalism**
    - Electronic defacing of Web site
- **Masquerading** (**spoofing**)
  - Pretending to be someone else
  - Fake Web site representing itself as original

Integrity Threats (cont'd.)

- **Domain name servers** (**DNSs**)
  - Internet computers maintaining directories
    - Linking domain names to IP addresses
  - Perpetrators use software security hole
    - Substitute their Web site address in place of real one
    - Spoofs Web site visitors
- **Phishing expeditions**
  - Capture confidential customer information
  - Common victims
    - Online banking, payment system users

Necessity Threats

- Also known as **delay**, **denial**, **denial-of-service** (**DoS**) **attack**
  - Disrupt or deny normal computer processing
  - Intolerably slow-speed computer processing
    - Renders service unusable or unattractive
- **Distributed denial-of-service** (**DDoS**) **attack**
  - Launch simultaneous attack on a Web site via botnets
- DoS attacks
  - Remove information altogether
  - Delete transmission or file information

Necessity Threats (cont'd.)

- Denial attack examples:
  - Quicken accounting program diverted money to perpetrator's bank account
  - High-profile electronic commerce company received flood of data packets
    - Overwhelmed sites' servers
    - Choked off legitimate customers' access

Threats to the Physical Security of Internet Communications Channels

- Internet's packet-based network design:
  - Precludes it from being shut down
    - By attack on single communications link
- Individual user's Internet service can be interrupted
  - Destruction of user's Internet link
- Larger companies, organizations
  - Use more than one link to main Internet backbone

Threats to Wireless Networks

- **Wireless Encryption Protocol** (**WEP**)
  - Rule set for encrypting transmissions from the wireless devices to the wireless access points (WAPs)
- **Wardrivers**
  - Attackers drive around in cars
  - Search for accessible networks
- **Warchalking**
  - Place chalk mark on building
    - Identifies easily entered wireless network nearby
  - Web sites include wireless access locations maps

Threats to Wireless Networks (cont'd.)

- Preventing attacks by wardrivers
  - Turn on WEP
  - Change default login and password settings
- Example
  - Best Buy wireless point-of-sale (POS)
    - Failed to enable WEP
    - Customer launched sniffer program
    - Intercepted data from POS terminals

Encryption Solutions

- **Encryption**: coding information using mathematically based program, secret key
- **Cryptography**: science studying encryption
  - Science of creating messages only sender and receiver can read
- Steganography
  - Makes text undetectable to naked eye
- Cryptography converts text to other visible text
  - With no apparent meaning

Encryption Solutions (cont'd.)

- Encryption algorithms
  - **Encryption program**
    - Transforms normal text (**plain text**) into **cipher text** (unintelligible characters string)
  - **Encryption algorithm**
    - Logic behind encryption program
    - Includes mathematics to do transformation
  - **Decryption program**
    - Encryption-reversing procedure: message is decoded or **decrypted**
  - Key type subdivides encryption into three functions
    - Hash coding, asymmetric encryption, symmetric encryption

Encryption Solutions (cont'd.)

- **Hash coding**
  - Process uses **Hash algorithm**
  - Calculates number (**hash value**) from any length message
  - Unique message fingerprint
  - Good hash algorithm design
    - Probability of **collision** is extremely small (two different messages resulting in same hash value)
  - Determining message alteration during transit
    - Mismatch between original hash value and receiver computed value

Encryption Solutions (cont'd.)

- **Asymmetric encryption** (**public-key encryption**)
  - Encodes messages using two mathematically related numeric keys
  - **Public key**: one key freely distributed to public
    - Encrypt messages using encryption algorithm
  - **Private key**: second key belongs to key owner
    - Kept secret
    - Decrypt all messages received

Encryption Solutions (cont'd.)

- **Pretty Good Privacy** (**PGP**)
- Software tools using different encryption algorithms
  - Perform public key encryption
- Individuals download free versions
  - PGP Corporation site, PGP International site
  - Encrypt e-mail messages
- Sells business site licenses

Encryption Solutions (cont'd.)

- **Symmetric encryption** (**private-key encryption**)
  - Encodes message with one of several available algorithms
    - Single numeric key to encode and decode data
  - Message receiver must know the key
  - Very fast and efficient encoding and decoding
  - Key must be guarded

Encryption Solutions (cont'd.)

- Problems
  - Difficult to distribute new keys to authorized parties while maintaining security, control over keys
  - Private keys do not work well in large environments
- **Data Encryption Standard** (**DES**)
  - Encryption algorithms adopted by U.S. government
  - Most widely used private-key encryption system
  - Fast computers break messages encoded with smaller keys

Encryption Solutions (cont'd.)

- **Triple Data Encryption Standard** (**Triple DES**, **3DES**)
  - Stronger version of Data Encryption Standard
- **Advanced Encryption Standard** (**AES**)
  - Alternative encryption standard
  - Most government agencies use today
- Longer bit lengths increase difficulty of cracking keys

Encryption Solutions (cont'd.)

- Comparing asymmetric and symmetric encryption systems
  - Advantages of public-key (asymmetric) systems
    - Small combination of keys required
    - No problem in key distribution
    - Implementation of digital signatures possible
  - Disadvantages of public-key systems
    - Significantly slower than private-key systems
  - Public-key systems: complement rather than replace private-key systems

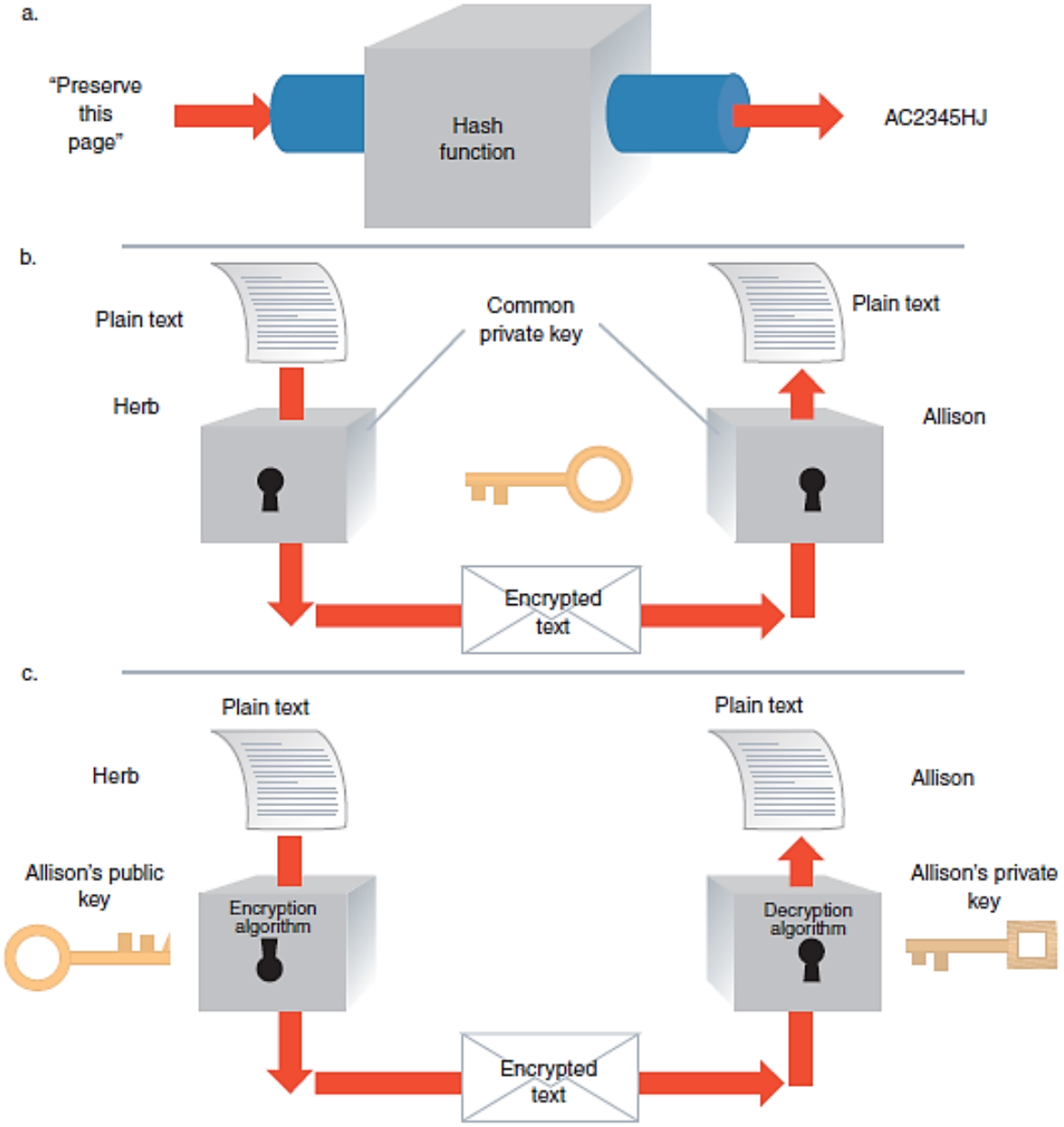

FIGURE 10-9 Comparison of (a) hash coding, (b) private-key, and (c) public-key encryption

Encryption Solutions (cont'd.)

- Web servers accommodate encryption algorithms
  - Must communicate with variety of Web browsers
- **Secure Sockets Layer** (**SSL**)
  - Goal: secures connections between two computers
- Secure Hypertext Transfer Protocol (S-HTTP)
  - Goal: send individual messages securely

Encryption Solutions (cont'd.)

- Secure sockets layer (SSL) protocol
  - Provides security "handshake"
  - Client and server exchange brief burst of messages
  - All communication encoded
    - Eavesdropper receives unintelligible information
  - Secures many different communication types
    - HTTP, FTP, Telnet
  - HTTPS: protocol implementing SSL
    - Precede URL with protocol name HTTPS

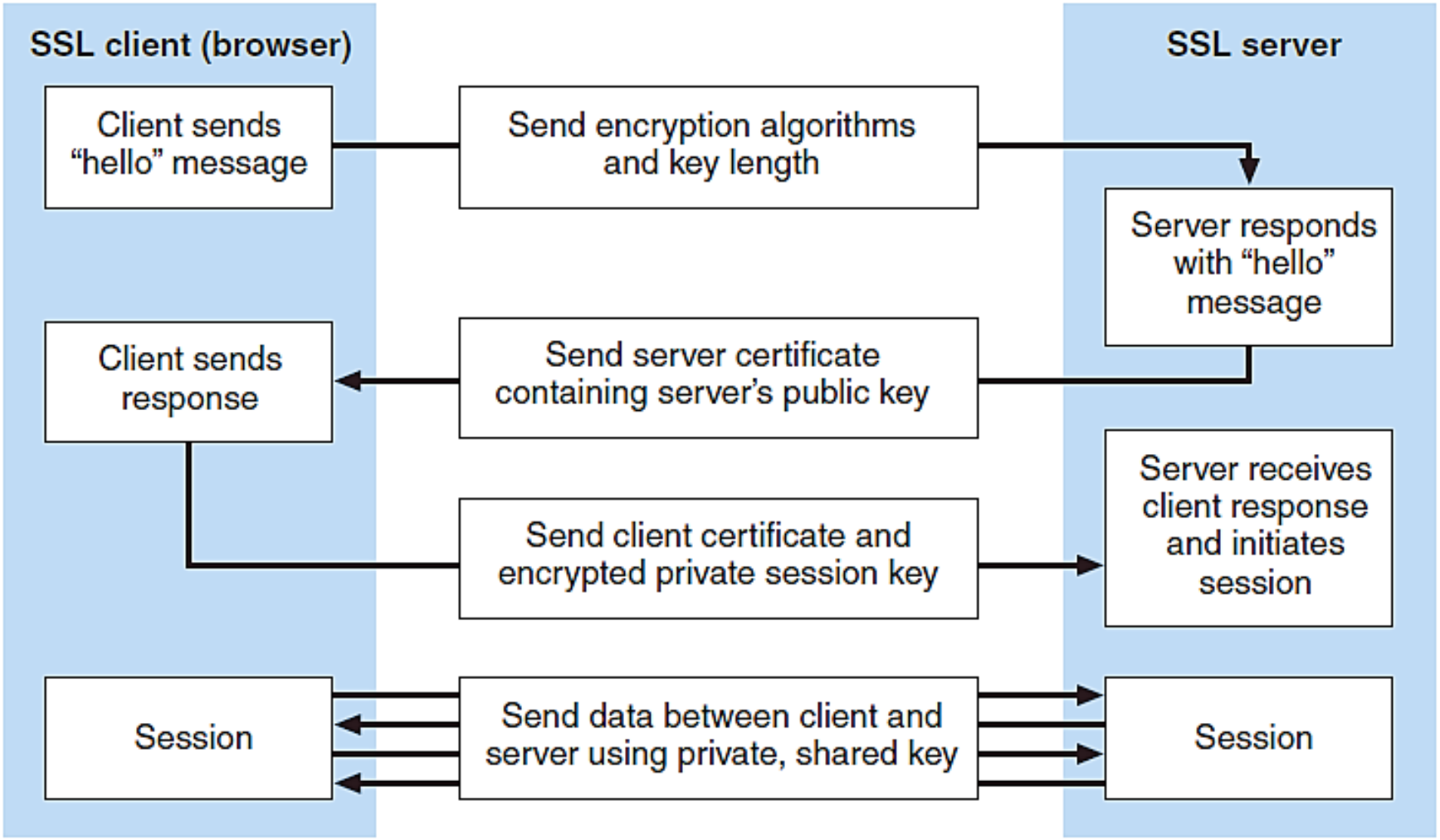

FIGURE 10-10 Establishing an SSL session

Encryption Solutions (cont'd.)

- Secure HTTP (S-HTTP)
  - Extension to HTTP providing security features
    - Client and server authentication, spontaneous encryption, request/response nonrepudiation
  - Symmetric encryption for secret communications
  - Public-key encryption to establish client/server authentication
  - **Session negotiation**: process between client and server of proposing and accepting (or rejecting) various transmission conditions

Encryption Solutions (cont'd.)

  - **Secure envelope** (complete package)
    - Encapsulates message
    - Provides secrecy, integrity, and client/server authentication
- SSL has become:
  - More generally accepted standard over S-HTTP

Security for Server Computers

- Server vulnerabilities
  - Exploited by anyone determined to cause destruction or acquire information illegally
- Entry points
  - Web server and its software
  - Any back-end programs containing data
- No system is completely safe
- Web server administrator
  - Ensures security policies documented; considered in every electronic commerce operation

Web Server Threats

- Compromise of secrecy
  - By allowing automatic directory listings
  - Solution: turn off folder name display feature
- Sensitive file on Web server
  - Holds Web server username-password pairs
  - Solution: store authentication information in encrypted form

Web Server Threats (cont'd.)

- Passwords that users select
  - Easily guessable
    - **Dictionary attack programs** cycle through electronic dictionary, trying every word as password
  - Solutions
    - User password requirements
    - Use password assignment software to check user password against dictionary
- Help creating very strong passwords:
  - Gibson Research Corporation's Ultra High Security Password Generator

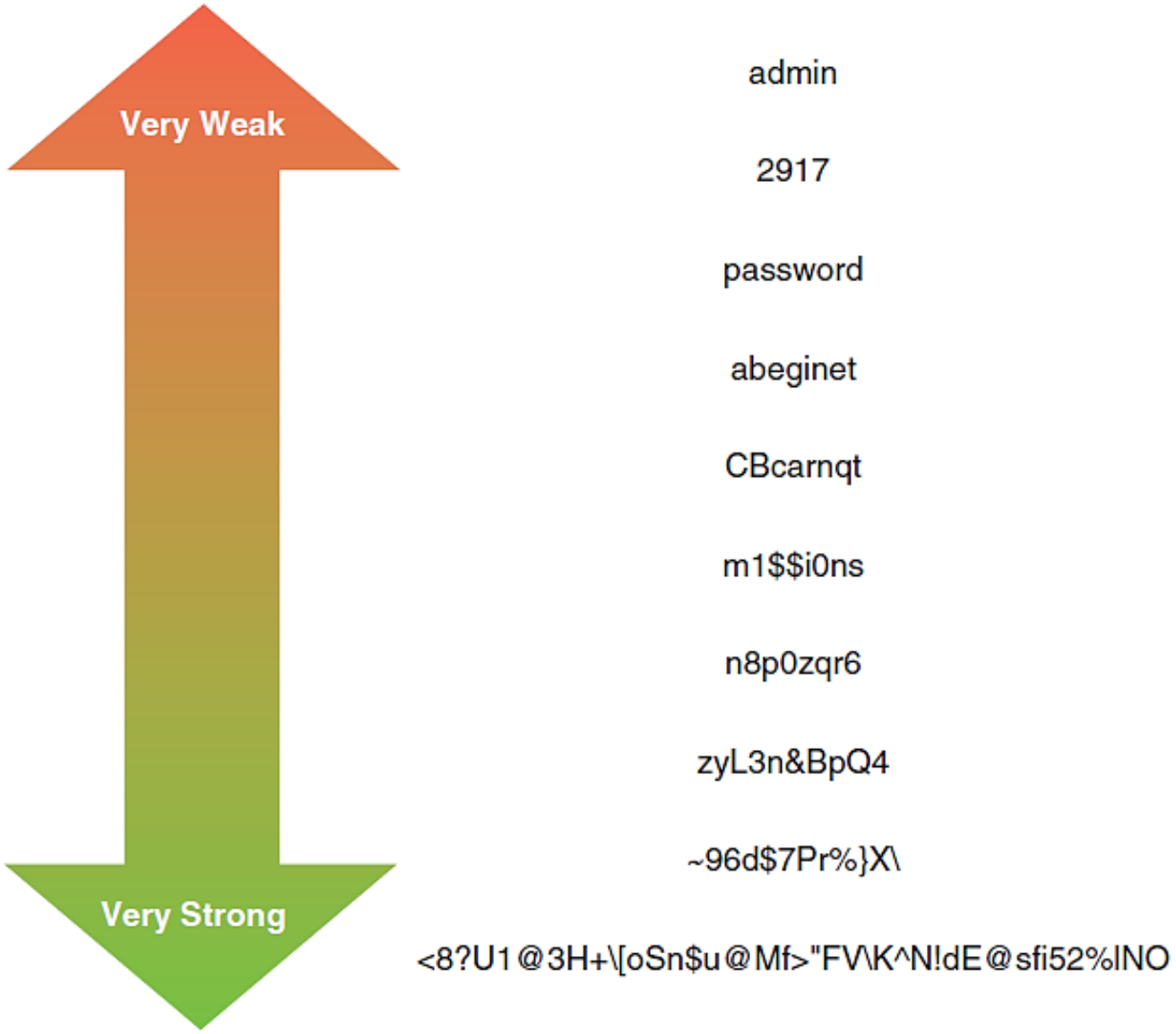

FIGURE 10-12 Examples of passwords, from very weak to very strong

Database Threats

- Usernames and passwords
  - Stored in unencrypted table
  - Database fails to enforce security altogether
    - Relies on Web server to enforce security
- Unauthorized users
  - Masquerade as legitimate database users
- Trojan horse programs hide within database system
  - Reveal information
  - Remove all access controls within database

Other Programming Threats

- Java or C++ programs executed by server
  - Passed to Web servers by client
  - Reside on server
  - Use a **buffer**
    - Memory area set aside holding data read from file or database
  - **Buffer overrun** (**buffer overflow)** error
    - Programs filling buffers malfunction and overfill buffer
    - Excess data spilled outside designated buffer memory
    - Cause: error in program or intentional
    - 1998 Internet worm

Other Programming Threats (cont'd.)

- Insidious version of buffer overflow attack
  - Writes instructions into critical memory locations
  - Web server resumes execution by loading internal registers with address of attacking program's code
- Reducing potential buffer overflow damage
  - Good programming practices
  - Some hardware functionality
- **Mail bomb** attack
  - Hundreds (thousands) send message to particular address

Access Control and Authentication

- Controlling who and what has access to Web server
- Authentication
  - Identity verification of entity requesting computer access
- Server user authentication
  - Server must successfully decrypt user's digital signature-contained certificate
  - Server checks certificate timestamp
  - Server uses callback system
- Certificates authenticate client computers and their users

Access Control and Authentication (cont'd.)

- Usernames and passwords
  - Provide some protection element
- Maintain usernames in plain text
  - Encrypt passwords with one-way encryption algorithm
- Problem
  - Site visitor may save username and password as a cookie
    - Might be stored in plain text
- **Access control list** (**ACL**)
  - Restrict file access to selected users

Firewalls

- **Firewall**
  - Software, hardware-software combination
  - Installed in a network to control packet traffic
- Placed at Internet entry point of network
  - Defense between network and the Internet
    - Between network and any other network
- Principles
  - All traffic must pass through it
  - Only authorized traffic allowed to pass
  - Immune to penetration

Firewalls (cont'd.)

- **Trusted**: networks inside firewall
- **Untrusted**: networks outside firewall
- Filter permits selected messages though network
- Separate corporate networks from one another
  - Coarse need-to-know filter
    - Firewalls segment corporate network into secure zones
- Large organizations with multiple sites
  - Install firewall at each location
    - All locations follow same security policy

Firewalls (cont'd.)

- Should be stripped of unnecessary software
- **Packet-filter firewalls**
  - Examine all data flowing back and forth between trusted network (within firewall) and the Internet
- **Gateway servers**
  - Filter traffic based on requested application
  - Limit access to specific applications
    - Telnet, FTP, HTTP
- **Proxy server firewalls**
  - Communicate with the Internet on private network's behalf

Firewalls (cont'd.)

- **Perimeter expansion** problem
  - Computers outside traditional physical site boundary
- Servers under almost constant attack
  - Install **intrusion detection systems**
    - Monitor server login attempts
    - Analyze for patterns indicating cracker attack
    - Block further attempts originating from same IP address
- Cloud computing: firewall products lagging behind
- **Personal firewalls**
  - Software-only firewalls on individual client computers
  - Gibson Research Shields Up! Web site

Computer Forensics and Ethical Hacking

- **Computer forensics experts** (**ethical hackers**)
  - Computer sleuths hired to probe PCs
  - Locate information usable in legal proceedings
  - Job of breaking into client computers
- **Computer forensics** field
  - Responsible for collection, preservation, and computer-related evidence analysis
- Companies hire ethical hackers to test computer security safeguards

Summary

- Physical and logical computer security important in electronic commerce
  - Security policy can identify risks and countermeasures to reduce risks
- Key security provisions
  - Secrecy, integrity, available service
- Client threats and solutions
  - Virus threats, active content threats, cookies
- Communication channels' threats and solutions
  - Encryption provides secrecy

Summary (cont'd.)

- Web Server threats and solutions
  - Threats from programs, backdoors
- Security organizations
  - Share information about threats, defenses
- Computer forensics
  - "Break into" computers searching for legal use data
  - Assist in identifying security weaknesses