

# Electronic Commerce Eighth Edition

## Chapter 10 *Electronic Commerce Security*

- ### Learning Objectives
- In this chapter, you will learn about:
- Online security issues
  - Security for client computers
  - Security for the communication channels between computers
  - Security for server computers
  - Organizations that promote computer, network, and Internet security
- Electronic Commerce, Eighth Edition 2

- ### Online Security Issues Overview
- Today's high stakes
    - Competitor access to messages; digital intelligence
    - Credit card number security
  - **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
- Electronic Commerce, Eighth Edition 3

- ### Online Security Issues Overview (cont'd.)
- **Logical security**
    - Protection of assets using nonphysical means
  - **Threat**
    - Any act or object possessing computer asset danger
  - **Countermeasure**
    - Procedure (physical or logical), *which...*
      - Recognizes, reduces, eliminates threat
    - Extent and expense of countermeasures
      - Depends on importance of asset at risk
- Electronic Commerce, Eighth Edition 4



## Managing Risk

- Risk management model (see Figure 10-1)
  - 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
- Examples of electronic threats
  - Impostors, eavesdroppers, thieves
- **Eavesdropper** (person or device)
  - Listen in on and copy Internet transmissions

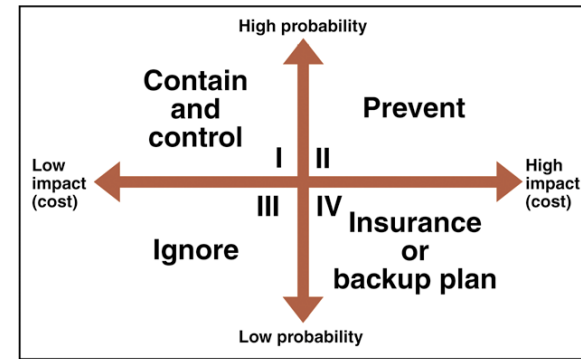
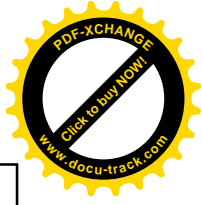


FIGURE 10-1 Risk management model

## Managing Risk (cont'd.)

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

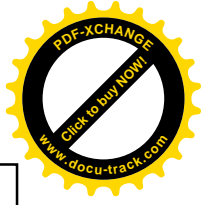
## Elements of Computer Security

- **Secrecy refers to...**
  - 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, aka denial of service**
  - Preventing data delays or denials (removal)
  - Delaying message or completely destroying it



## Security Policy and Integrated Security

- **Security policy:** living document
  - Assets to protect and why, protection responsibility, acceptable and unacceptable behaviors
  - **Covers:** Physical security, network security, access authorizations, virus protection, disaster recovery
- **Steps to create security policy**
  - Determine assets to protect from threats
  - Determine access to various system parts
  - Determine resources to protect identified assets
  - Develop written security policy
  - Commit resources



## Security Policy and Integrated Security (cont'd.)

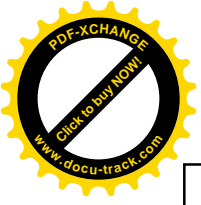
- **Military policy:** stresses separation of multiple levels of security
- **Commercial policy information classification:** “public” or “company confidential”
- **Comprehensive security plan goals**
  - Protect system’s privacy, integrity, availability; authenticate users
  - Selected to satisfy Figure 10-2 requirements
- **Security policies information sources**
  - The Network Security Library
  - Information Security Policy World Web site

Requirement	Meaning
Secrecy	Prevent unauthorized persons from reading messages and business plans, obtaining credit card numbers, or deriving other confidential information.
Integrity	Enclose information in a digital envelope so that the computer can automatically detect messages that have been altered in transit.
Availability	Provide delivery assurance for each message segment so that messages or message segments cannot be lost undetectably.
Key management	Provide secure distribution and management of keys needed to provide secure communications.
Nonrepudiation	Provide undeniable, end-to-end proof of each message’s origin and recipient.
Authentication	Securely identify clients and servers with digital signatures and certificates.

FIGURE 10-2 Requirements for secure electronic commerce

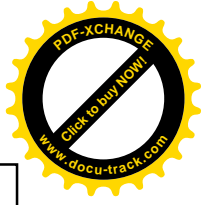
## Security Policy and Integrated Security (cont'd.)

- **Absolute security is difficult to achieve, but a company can...**
  - 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



## Security Policy and Integrated Security (cont'd.)

- E-commerce site 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
    - Users and their client computers are duped into revealing information

## Cookies

- Internet connection between Web clients and servers
  - **Stateless connection**
    - Independent information transmission
    - No continuous connection (**open session**) maintained between any client and server
- Cookies
  - Small text files Web servers place on Web client **which...**
  - Identify returning visitors
  - Allow continuing open session, **which is required by...**
    - shopping cart and payment processing

## Cookies (cont'd.)

- “Time duration” cookie category
  - **Session cookies:** exist until client connection ends
  - **Persistent cookies:** remain indefinitely **on client computer**
  - Electronic commerce sites use both
- “Source cookie” category
  - **First-party cookies**
    - Web server site places them on client computer
  - **Third-party cookies**
    - Different Web site (**e.g., web site which provides advertising to multiple web sites**) places them on client computer

## Cookies (cont'd.)

- **One can** disable cookies entirely
  - Complete protection from revealing private information
  - Problem
    - Useful cookies blocked (along with others)
    - Full site resources are not available – e.g., **online classes sometimes will not work properly if cookies are totally disabled**
- Web browser cookie management functions
  - Refuse only third-party cookies
  - Review each cookie before accepted
  - Provided by Microsoft Internet Explorer, Mozilla Firefox, Mozilla SeaMonkey, Opera

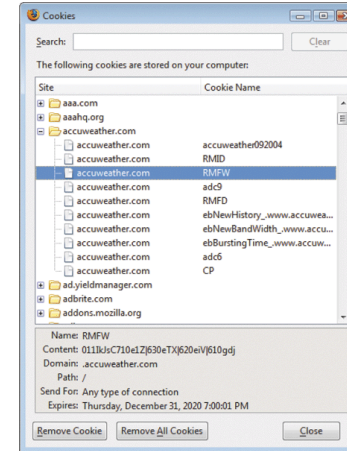


FIGURE 10-3 Mozilla Firefox dialog box for managing stored cookies

## Web Bugs

- **Web bug**
  - Tiny graphic that a third-party Web site places on another site's Web page
  - Purpose
    - Site visitor loads Web page
    - Web bug delivered by third-party site, **and it causes...**
    - Cookie **to be** placed 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 **which**
  - Cause action to occur – **programs to execute; which e.g., display moving graphics; download and play audio**
  - 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
  - Poses **security** threat to client computer

## Active Content (cont'd.)

- **Examples of how active content is provided:**  
Cookies, Java applets, JavaScript, VBScript, ActiveX controls, graphics, Web browser plug-ins, e-mail attachments
- **Scripting languages:** provide executable script – are commands
  - Examples: JavaScript and VBScript
- **Applet:** small application program
  - Typically runs within Web browser
    - Browsers include tools limiting applets' actions

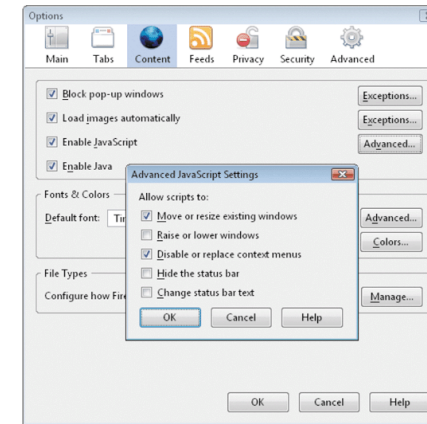


FIGURE 10-4 Advanced JavaScript settings in Mozilla Firefox

## Active Content (cont'd.)

- Active content modules
  - Embedded in Web pages (transparent)
- Crackers (**hackers**) can embed malicious active content in a web page. Called a...
- **Trojan horse**
  - Program hidden inside another program (Web page)
    - Masking true purpose
- **Zombie** (Trojan horse)
  - Secretly takes over another computer and can...
  - Launch attacks on other computers

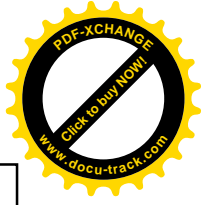
## Java Applets

- Java: platform-independent programming language
  - Provides Web page active content
  - Server sends applets with client-requested pages
  - Most cases: operation visible to visitor
  - Possibility: functions not noticed by visitor – such as reading/writing files
- Advantages
  - Adds functionality to business application's functionality; relieves server-side programs by offloading programs (applets) to run on the client machine
- Disadvantage
  - Possible security violations



## Java Applets (cont'd.)

- **Java sandbox**
  - Confines Java applet actions to set of rules defined by security model
  - Rules apply to all **untrusted Java applets, i.e., are...**
    - Not established as secure
  - Java applets running within sandbox constraints
    - No full client system access – e.g., **can not read/write files**
- Java applet security information
  - **Java Security Page**
    - Maintained by Center for Education and Research in Information Assurance and Security (CERIAS)



## JavaScript

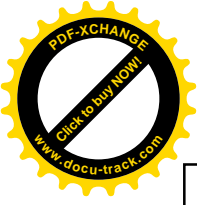
- **JavaScript**
  - Scripting language developed by Netscape
  - Enables Web page designers to build active content
  - Based loosely on Sun's Java programming language
  - Can be used for attacks
    - Cannot commence execution on its own
    - User must start ill-intentioned JavaScript program

## ActiveX Controls

- Objects that contain programs and properties Web designers place on Web pages
  - Perform particular tasks
- Run **specifically** on Windows operating systems computers
- **ActiveX** component construction **can use...**
  - Many different programming languages
    - Common: C++ and Visual Basic
- Executed on client computer
  - After downloading Web page containing embedded ActiveX control

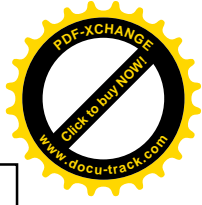
## ActiveX Controls (cont'd.)

- Comprehensive ActiveX controls list **can be seen at...**
  - Download.com ActiveX page
- Security danger
  - Execute like other client computer programs
  - Have access to full system resources
    - Cause secrecy, integrity, and necessity violations
  - Actions cannot be halted once started
- **Most web browsers can be configured to...**
  - Provide notice of Active-X download or install



## Graphics and Plug-Ins

- Graphics, browser plug-ins, and e-mail attachments can harbor executable content
- Code embedded in graphic might harm client computer
- **Plug-ins** (programs)
  - Enhance browser capabilities (normally beneficial)
    - Handle Web content that browser cannot handle – e.g., playing audio clips, play movies
  - Can pose security threats
    - 1999 RealPlayer plug-in – used to secretly gather information such as user's name, email address, zip code and other information
    - Plug-ins executing commands buried within media



## Viruses, Worms, and Antivirus Software

- **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
  - Clogged e-mail systems
  - Replicated itself explosively through Outlook e-mail
  - Caused other harm
- 2001 Code Red and Nimda
  - **Multivector virus:** entered computer system in several different ways (vectors)
- 2002 and 2003 Bugbear
  - New virus-worm combination

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

- 2005 and 2006 Zotob
  - New breed of Trojan horse-worm combination
- See figure 10-5 on pp 467-468 for list of major virus/worm names with descriptions
- **Antivirus software**
  - Detects viruses and worms
  - Either deletes or isolates them on client computer
  - **Symantec** and **McAfee**
    - Keep track of viruses, sell antivirus software
  - Only effective if antivirus data files kept current

Year	Name	Type	Description
1986	Brain	Virus	Written in Pakistan, this virus infects floppy disks used in personal computers at that time. It consumes empty space on the disks, preventing them from being used to store data or programs.
1988	Internet Worm	Worm	Robert Morris, Jr., a graduate student at Cornell University, wrote this experimental, self-replicating, self-propagating program and released it onto the Internet. It replicated faster than he had anticipated, crashing computers at universities, military sites, and medical research facilities throughout the world.
1991	Tequila	Virus	Tequila writes itself to a computer's hard disk and runs any time the computer is started. It also infects programs when they are executed. Tequila originated in Switzerland and was mostly transmitted through internet downloads.
1992	Michelangelo	Trojan horse	Set to activate on March 6 (Michelangelo's birthday), this Trojan horse overwrites large portions of the infected computer's hard disk.
1993	SatanBug	Virus	Infects programs when they run, causing them to fail or perform incorrectly. SatanBug was designed to interfere with antivirus programs so they cannot detect it.
1996	Concept	Virus, Worm	One of the first viruses to be written in Microsoft Word's macro language, Concept travels with infected Word document files. When an infected document is opened, Concept places macros in Word's default document templates, which infects any new Word document created on that computer.
1999	Melissa	Virus, Worm	Melissa is a Microsoft Word macro virus that spreads by e-mailing itself automatically from one user to another. It inserts comments from "The Simpsons" television show and confidential information from two infected computers. Melissa spread throughout the world in a few hours. Many large companies were inundated by Melissa. For example, Microsoft closed down its e-mail servers to prevent the spread of this virus within the company.
2000	ILOVEYOU	Virus, Worm	Arrives attached to an e-mail message with the subject line "ILOVEYOU" and infects any computer on which the attachment is opened. It sends itself to addresses in any Microsoft Outlook address book it finds on the infected computer. The virus destroys music and photo files stored on the infected computer. When it was launched, it clogged e-mail servers in many large organizations and slowed down the operation of the entire Internet.
2001	Code Red	Virus, Worm, Trojan horse	Code Red can infect Web servers and personal computers. It deletes Web pages and can be transmitted from Web servers to personal computers. It can give hackers control over Web server computers. Code Red can reinstall itself from hidden files after it is removed.

FIGURE 10-5 Major viruses, worms, and Trojan horses

Year	Name	Type	Description
2001	Nimda	Virus, Worm	Nimda modifies Web documents and certain programs on the infected computer. It also creates multiple copies of itself using various file names. It can be transmitted by e-mail, LAN, or from a Web server to a Web client.
2002	BugBear	Virus, Worm, Trojan horse	BugBear is spread through e-mail and through local area networks. It identifies antivirus software and attempts to disable it. BugBear can log keystrokes and store them for later transmission through a Trojan horse program that it installs on the infected computer. The program gives hackers access to the computer and allows file uploads and downloads.
2002	Klez	Virus, Worm	Klez is transmitted as an e-mail attachment and overwrites files, creates hidden copies of the original files, and attempts to disable antivirus software.
2003	Slammer	Worm	Slammer's primary purpose was to demonstrate how rapidly a worm could be transmitted on the Internet; it infected 75,000 computers in its first 10 minutes of propagation.
2003	Sobig	Trojan horse	Sobig turns infected computers into spamming points. Sobig transmits mass e-mails with copies of itself to potential victims.
2004	MyDoom	Worm, Trojan horse	MyDoom turns the infected computer into a zombie that will participate in a denial of service attack on a specific company's Web site.
2004	Sasser	Virus, Worm	Written by a German high school student, Sasser finds computers with a specific security flaw and then infects them. The infected computers are slowed by the virus, often to the point that they must be rebooted.
2005	Zotob	Worm, Trojan horse	Zotob performs port scans and infects computers that appear to have a specific security flaw. Once installed on a target computer, Zotob can log keystrokes, capture screens, and steal authentication credentials and CD software keys. Infected computers can also be used as proxies for mass mailing or attacking other computers.
2006	Nymem	Worm, Trojan horse	Nymem disables security and the sharing features. It destroys files created by Microsoft Office programs. Nymem activates on the third of each month and spreads itself by mass mailing.
2006	Leap	Worm, Virus	Leap (also called Ompa-Lcampa) infects programs that run on the Microsoft Windows operating system. Delivered over the chat instant messaging system, it can only spread within a specific network.
2007	Slim	Worm, Trojan horse	Slim gathers infected computers into a botnet from which it launches spam. It is spread as an e-mail containing HTML virus clips with an attachment that it alleges is a news film.

FIGURE 10-6 Major viruses, worms, and Trojan horses (continued)

## Digital Certificates

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

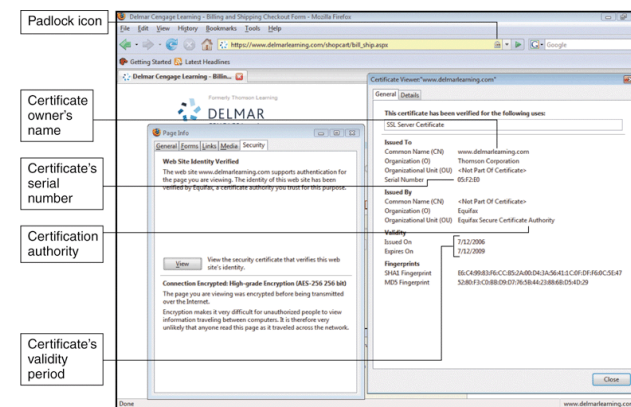
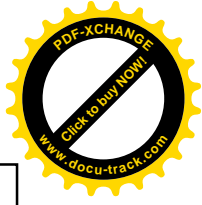


FIGURE 10-6 Delmar Learning's digital certificate information displayed in Firefox browser



## Digital Certificates (cont'd.)

- **Certification authority (CA)**
  - Issues digital certificates to organizations, individuals
- Digital certificates cannot be forged easily
- Six main elements
  - Certificate owner's identifying information
  - Certificate owner's public key – **more about keys later on**
  - Dates certificate is valid
  - Certificate serial number
  - Certificate issuer name
  - Certificate issuer digital signature



## Digital Certificates (cont'd.)

- **Key**
  - Number: usually long binary number
    - Used with encryption algorithm
    - “Lock” message characters being protected (undecipherable without key)
  - Longer keys provide significantly better protection
- Identification requirements vary
  - Driver's license, notarized form, fingerprints
- Companies offering CA services
  - Thawte, VeriSign, Entrust, Equifax Secure

## Digital Certificates (cont'd.)

- Classification
  - Low, medium, high assurance
    - Based largely on identification requirements
  - Determine CA service fee charged
- Digital certificates expire after period of time, **often, 1 year**
  - Provides protection (users and businesses). **Users...**
  - Must submit credentials for reevaluation periodically

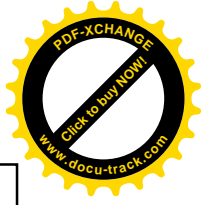
## Steganography

- Process of 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
- **Many security experts believe that Al Qaeda used steganography to hide attack orders in images posted on web sites**



## 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 devices
  - Identification using element of person's biological makeup
    - Writing pads, eye scanners, palm reading scanners, reading back of hand vein pattern



## Communication Channel Security

- Internet was not designed to be secure, **it was...**
  - Designed to provide redundancy
- **Largely** remains unchanged from original state
  - Message traveling on the Internet
    - Subject to secrecy, integrity, and necessity threats

## Secrecy Threats

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

Next slide has example of difference between secrecy and privacy

## Secrecy Threats (cont'd.)

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



## Secrecy Threats (cont'd.)

- Electronic commerce threat (cont'd.)
  - **Backdoors:** electronic holes
    - Left open accidentally or intentionally
    - Content exposed to secrecy threats
    - Example: Cart32 shopping cart program backdoor – credit card numbers were stolen until a patch was applied
  - Stolen corporate information
    - Eavesdropper example
- Web users continually reveal information
  - Secrecy breach
  - Possible solution: anonymous Web surfing, where the personal information you enter is not passed as. e.g., part of URL (which some sites do). Read page 475 for more detailed info regarding this.

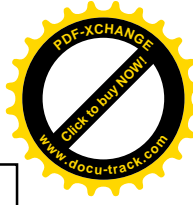


FIGURE 10-7 ShadowSurf.com home page

## Integrity Threats

- Also known as **active wiretapping**
  - Unauthorized party alters message information stream
- Integrity violation example
  - **Cyber vandalism**
    - Web site's page electronic defacing
- **Masquerading (spoofing)**
  - Pretending to be someone else
  - Fake Web site representing itself as original

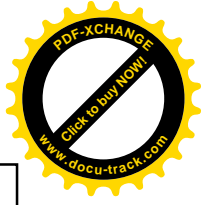
## Integrity Threats (cont'd.)

- **Domain name servers (DNSs)**
  - Internet computers maintaining directories which...
    - Link 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 – someone send genuine-looking email with link to genuine-looking website, which then...**
  - Captures confidential customer information
  - Common victims
    - Online banking, payment system users



## Necessity Threats

- Also known as **delay, denial, denial-of-service (DoS) threats**
  - Disrupt normal computer processing
  - Deny processing entirely
  - Intolerably slow-speed computer processing
    - Renders service unusable or unattractive
- DoS attacks
  - Remove information altogether
  - Delete transmission or file information



## Necessity Threats (cont'd.)

- Documented denial attacks
  - Quicken accounting program diverted money to perpetrator's bank account
    - Denied money from its rightful owners
  - Zombie computers sent flood of data packets to high-profile electronic commerce sites
    - Overwhelmed sites' servers – **Amazon & Yahoo!**
    - Choked off legitimate customers' access
  - 1988 Internet Worm attack
    - Disabled thousands of computers – **was the first recorded example of a DoS attack**

## 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...
  - User's Internet link destruction
- Larger companies, organizations **may have...**
  - More than one link to main Internet backbone, **so if problem with one, can use other one**

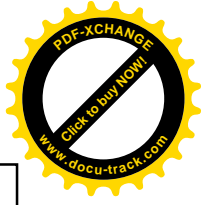
## Threats to Wireless Networks

- **Wardrivers**
  - Attackers drive around in cars
  - Use wireless-equipped computers searching for accessible networks
- **Warchalking**
  - Place chalk mark on building
    - Identifies easily entered wireless network nearby
  - Web sites include wireless access locations maps
- **To avoid being targeted...**
  - Turn on WEP in access points, **and**
  - Change default settings **which the wireless network comes with**



## Threats to Wireless Networks (cont'd.)

- Example
  - 2002: Best Buy wireless point-of-sale (POS)
    - Failed to enable WEP
    - Customer launched sniffer program **in the store's parking lot, and...**
    - Intercepted data from POS terminals



## Encryption Solutions

- **Encryption:** coding information using mathematically based program **and a** secret key
  - Produces unintelligible string of characters
- **Cryptography:** science studying encryption
  - Science of creating messages only sender and receiver can read, **which is different than...**
- Steganography
  - Makes text undetectable to naked eye
- Cryptography converts text to other visible text
  - The random text appears to have no meaning

## Encryption Solutions (cont'd.)

- Encryption algorithms **is an...**
  - **Encryption program**
    - Transforms normal text (**plain text**) into **cipher text** (unintelligible characters string)
  - **Encryption algorithm**
    - Logic behind encryption program
    - Includes mathematics to do transformation
  - Messages encrypted just before being sent
    - Upon arrival, message is decoded (decrypted)
  - **Decryption program:** encryption-reversing procedure

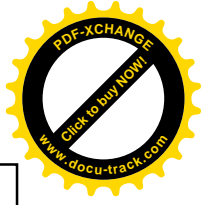
## Encryption Solutions (cont'd.)

- Encryption algorithms (cont'd.)
  - National Security Agency controls dissemination
  - U.S. government banned publication of details
    - Illegal for U.S. companies to export
  - **One property of encryption algorithms is that someone...**
    - May know algorithm details, **but will still...**
    - Not **be** able to decipher encrypted message without knowing key encrypting the message
  - Key type subdivides encryption into three functions
    - Hash coding, asymmetric encryption, symmetric encryption



## Encryption Solutions (cont'd.)

- Hash coding
  - **Hash algorithm** calculates number (**hash value**)
    - From any length message
  - Unique message fingerprint, **unique to the message, as it is based on the message**
  - Design of good hash algorithms
    - Probability of **collision** is extremely small (two different messages resulting in same hash value)
  - Determine whether message has been altered during transit
    - No match with original hash value and receiver computed value **if message has been altered**



## 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
    - **Private key is kept secret...**
    - **And is used to** decrypt all messages received

## Encryption Solutions (cont'd.)

- Asymmetric encryption (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, i.e., kept secret, by both sides**

## Encryption Solutions (cont'd.)

- Symmetric encryption (cont'd.)
  - Problems
    - Difficult to distribute new keys to authorized parties while maintaining security, control over keys, **as each pair of users who want to communicate need a unique key**
    - Private keys do not scale 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
      - e.g., 'Deep Crack' key breaker – used 100,000 computers on the internet to break a key in only 23 hours. See pg. 481 in book for more info regarding this.

## Encryption Solutions (cont'd.)

- Symmetric encryption (cont'd.)
  - **Triple Data Encryption Standard (Triple DES, 3DES)**
    - Stronger version of Data Encryption Standard
  - **Advanced Encryption Standard (AES)**
    - **U.S Gov't's NIST-developed encryption standard (National Institute of Standards and Technologies)**
    - Designed to keep government information secure
  - Longer bit lengths dramatically increase difficulty of cracking encryption protection

## 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 – **with symmetric, more difficult to send the private keys while keeping them secure. See bottom of page 480 in book for more information regarding this.**
    - Implementation of digital signatures possible
  - Disadvantages of public-key systems
    - Significantly slower than private-key systems
    - Do not replace private-key systems (complement them)

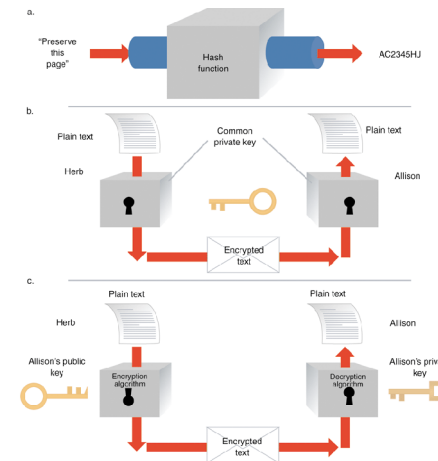
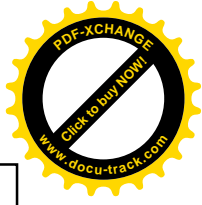


FIGURE 10-8 Comparison of (a) hash coding, (b) private-key, and (c) public-key encryption



## Encryption Solutions (cont'd.)

- Comparing asymmetric and symmetric encryption systems (cont'd.)
  - Web servers **can** accommodate **most** encryption algorithms, **because they...**
    - Must communicate with variety of Web browsers
- **Secure Sockets Layer (SSL)** system
  - Goal: secures connections between two computers
- Secure Hypertext Transfer Protocol (S-HTTP)
  - Goal: send individual messages securely
- Client and server computers manage encryption and decryption activities
  - Automatically and transparently



## Encryption Solutions (cont'd.)

- Secure sockets layer (SSL) protocol
  - Provides security “handshake” **between client and server**
  - 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 – **the ‘s’ at the end indicates that the client wants to establish a secure connection with the remote server**

## Encryption Solutions (cont'd.)

- Secure sockets layer (SSL) protocol (cont'd.)
  - Encrypted transaction generates private session key length
    - Bit lengths vary (40-bit, 56-bit, 128-bit, 168-bit)
  - **Session key**
    - Used by encryption algorithm
    - Creates cipher (**i.e., encrypted**) text from plain text during single secure session
  - Secrecy implemented using public-key (asymmetric) encryption and private-key (symmetric) encryption
    - **From a certain point and on in the process, a private-key encryption is used** for nearly all secure communications  
(read pp. 483-484 for more detailed information regarding this)

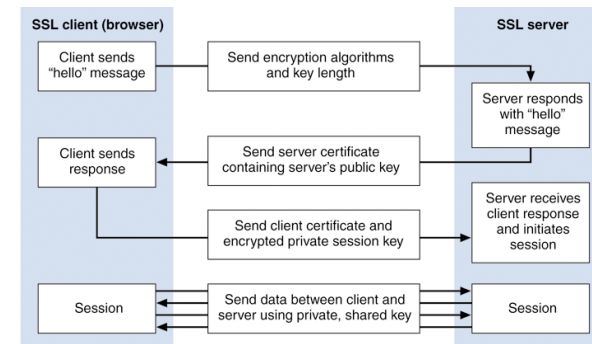
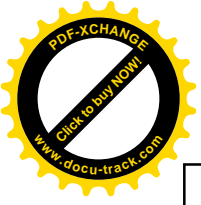
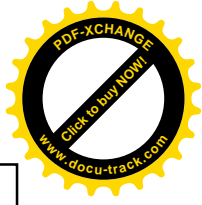


FIGURE 10-9 Establishing an SSL session



## Encryption Solutions (cont'd.)

- Secure HTTP (S-HTTP)
  - Extension to HTTP providing security features **such as...**
    - Client and server authentication, spontaneous encryption, request/response nonrepudiation
  - **Uses** Symmetric encryption for secret communications
  - **Uses** Public-key encryption to establish client/server authentication
  - Client or server can use techniques separately
    - **E.g.**, client **may request** browser security through private (symmetric) key, **and the...**
    - Server may require client authentication using public-key techniques



## Encryption Solutions (cont'd.)

- Secure HTTP (S-HTTP) (cont'd.)
  - Establishes secure session
    - SSL carries out client-server handshake exchange to set up secure communication
    - S-HTTP sets up security details with special packet headers exchanged in S-HTTP
  - Headers define type of security technique
  - Header exchanges state:
    - Which specific algorithms that each side supports
    - Whether client or server (or both) supports algorithm
    - Whether security technique is required, optional, or refused

## Encryption Solutions (cont'd.)

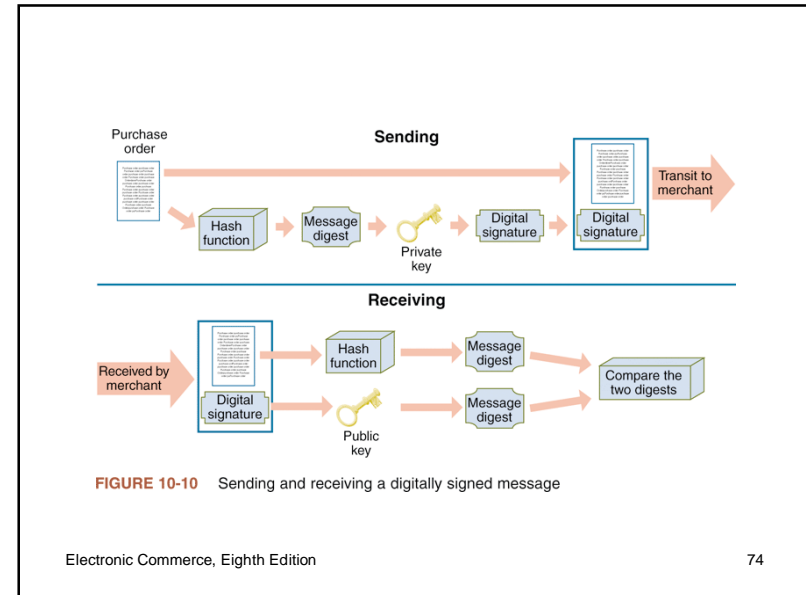
- Secure HTTP (S-HTTP) (cont'd.)
  - **Secure envelope** (complete package)
    - Encapsulates message
    - Provides secrecy (**no one can see contents of message**), integrity (**no one can modify contents of message**), and client/server authentication (**each 'side' is who they claim they are**)

## Ensuring Transaction Integrity with Hash Functions

- **Integrity violation**
  - Message altered while in transit between sender and receiver
    - Difficult and expensive to prevent, **but there are...**
    - Security techniques to detect
    - Harm: unauthorized message changes undetected
- Apply two algorithms to eliminate fraud and abuse:
  - Hash algorithms: **one-way functions**
    - No way to transform hash value back
  - **Encryption programs convert text into a "Message digest"**, which is a...
    - Small integer summarizing encrypted information

## Ensuring Transaction Integrity with Digital Signatures

- Hash algorithm calculates a unique number, called a 'message digest', based on the message text. The sender appends it to the message text. The receiver also creates a message digest, and it must match the sender's digest.
- Hash functions: potential for fraud – someone can intercept the transmission, alter the contents of the message, and create new 'message digest' (hashing algorithms are public). Receiver would then create same digest and is 'fooled'.
  - Solution: sender encrypts message digest using private key
- **Digital signature**
  - Encrypted message digest (message hash value)
- Digital signature provides:
  - Integrity, nonrepudiation, authentication
- Provide transaction secrecy
  - Encrypt entire string (digital signature, message)
- Digital signatures: same legal status as traditional signatures



## Guaranteeing Transaction Delivery

- Denial or delay-of-service attacks, e.g., **modifying a message**
- Encryption and digital signature **doesn't protect...**
  - Information packet protection from theft **or** slowdown
- Transmission Control Protocol (TCP)
  - Responsible for end-to-end packet control
    - Request that client resend when packets do not appear
- No special protocol beyond TCP/IP is required as countermeasure against denial attacks
  - TCP/IP builds in checks determining alteration **of packets**

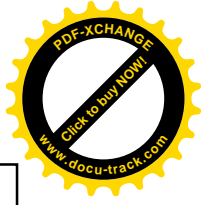
## Security for Server Computers

- 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, e.g., **a database and the server on which it runs**
- No system is completely safe
- Web server administrator
  - Ensures security policies documented; considered in every electronic commerce operation



## Web Server Threats

- Compromise of secrecy – server may be set up such that it...
  - Allows automatic directory listings
  - Solution: turn off folder name display feature
- Compromise of security
  - Requiring users to enter username and password
    - Subsequently revealed upon repeated information requirement
  - Solution
    - Use cookie to store user's confidential information
    - Encrypt cookie for transmission, otherwise it's not secure when transmitted



## Web Server Threats (cont'd.)

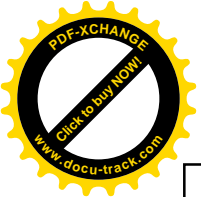
- Sensitive file on Web server
  - Holds Web server username-password pairs
  - Solution: store authentication information in encrypted form
- Passwords that users select
  - Easily guessable
    - **Dictionary attack programs** cycle through electronic dictionary, trying every word as password
  - Solution: use password assignment software to check user password against dictionary, and if it finds a match, doesn't allow that word as password

## Database Threats

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

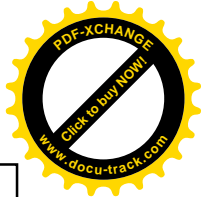
## Other Programming Threats

- 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 overflow buffer
    - Excess data spilled outside designated buffer memory
    - Cause: error in program or intentional
    - 1998 "Internet worm" did this



## 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, which then executes, exposing its files to disclosure and destruction
- Reducing potential buffer overflow damage
  - Good programming practices
  - Some hardware functionality – works with the operating system to limit the effects of buffer overflows
- **Mail bomb** attack
  - Hundreds (thousands) send message to particular address



## Threats to the Physical Security of Web Servers

- Protecting Web servers
  - Put computers in CSP facility
    - Security on CSP physical premise is generally maintained better
  - Maintain server content's backup copies at remote location
  - Rely on service providers
    - Offer managed services including Web server security...
  - Or, can hire smaller, specialized security service providers

## 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 to ascertain that it hasn't expired
  - Server uses callback system – in which the user's client computer name and address are checked against a list of computer names and addresses
- Certificates provide attribution (irrefutable evidence of identity) in a security breach

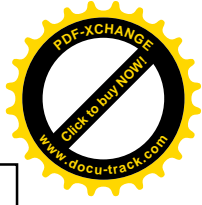
## Access Control and Authentication (cont'd.)

- Usernames and passwords provide some protection element
- Maintain usernames in plain text
  - Encrypt passwords with one-way encryption algorithm
- Problem when site visitor saves username and password as a cookie
  - Might be stored on client computer in plain text
- Use **access control list** security to restrict file access to selected users. Is a...
  - List (or database of files), of usernames of people allowed access to files, other resources



## Firewalls

- Software, hardware-software combination
  - Installed in a network
  - Control packet traffic
- Placed at Internet entry point of network
  - Defense between network and the Internet, or...
    - Between network and any other network
- Characteristics
  - 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
- **Can be used to** separate corporate networks from one another
  - Coarse need-to-know filter
    - Firewalls segment corporate network into secure zones
- Organizations with large multiple sites
  - Install firewall at each location
    - All locations follow same security policy

## Firewalls (cont'd.)

- **The firewall computer** should be stripped of unnecessary software – to reduce the chances of software security breaches
- **Packet-filter firewalls**
  - Examine all data flowing back and forth between trusted network (within firewall) and the Internet, and allows/denies access based on a pre-programmed set of rules
- **Gateway servers**
  - Filter traffic based on requested application
  - Limit access to specific applications, e.g.,...
    - Telnet, FTP, HTTP
- **Proxy server firewalls**
  - Communicate with the Internet on private network's behalf – the firewall passes the browser request to the internet, and the response is relayed back to the browser by the proxy server
  - In computer networks, a **proxy server** is a server (a computer system or an application program) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server. The proxy server evaluates the request according to its filtering rules. For example, it may filter traffic by IP address or protocol. If the request is validated by the filter, the proxy provides the resource by connecting to the relevant server and requesting the service on behalf of the client.

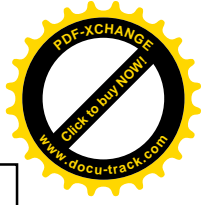
## Firewalls (cont'd.)

- **Perimeter expansion problem**
  - Computers outside traditional physical site boundary, e.g., employees from remote sites
- Servers under almost constant attack
  - Install **intrusion detection systems**
    - Monitor server login attempts
    - Analyze for patterns indicating cracker attack attempt
    - Block further attempts originating from same IP address
- **Personal firewalls**
  - Software-only firewalls on individual client computers
  - Gibson Research Shields Up! Web site



## Organizations that Promote Computer Security

- After Internet Worm of 1988
  - Organizations formed to share computer system threat information
  - Devoting principle
    - Sharing information about attacks and attack defenses helps everyone create better computer security
  - Some began at universities
    - Others launched by government agencies



## CERT

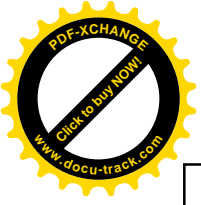
- **Computer Emergency Response Team**
- Housed at Carnegie Mellon University
  - Software Engineering Institute
- Maintains effective, quick communications infrastructure among security experts
  - **So that** security incidents **can be** avoided, handled quickly
- Provides security risk information
- Posts security events alerts
- Primary authoritative source for viruses, worms, and other types of attack information

## Other Organizations

- 1989: SANS Institute (**Systems Administrator, Audit, Network, and Security Institute**)
  - Education and research efforts
    - Research reports, security alerts, and white papers
  - **SANS Internet Storm Center** Web site
    - Current information on location, intensity of computer attacks worldwide
- CERIAS
  - Multidisciplinary information security research and education
  - CERIAS Web site
    - Computer, network, communications security resources

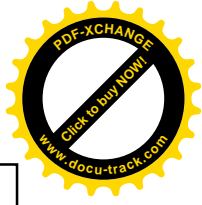
## Other Organizations (cont'd.)

- Center for Internet Security
  - Not-for-profit cooperative organization
  - Helps electronic commerce companies
- Microsoft Security Research Group
  - Privately sponsored site
- CSO Online
  - Articles from *CSO Magazine*
  - Computer security-related news items
- U.S. Department of Justice's Cybercrime site – **information regarding...**
  - Computer crimes; intellectual property violations



## 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

- E-commerce attacks disclose and manipulate proprietary information
  - Link secrecy, integrity, available service
- Client threats and solutions
  - Virus threats, active content threats, cookies
- Communication channels' threats and solutions
  - Internet vulnerable to attacks
- Web Server threats and solutions
  - Threats from programs, backdoors
- Security organizations and forensics