CHAPTER 10: E-COMMERCE SECURITY

Electronic Commerce
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
Online Security Issues Overview

- Computer security
  - The protection of assets from unauthorized access, use, alteration, or destruction

- Physical security
  - Includes tangible protection devices

- Logical security
  - Protection of assets using nonphysical means

- Threat
  - Any act or object that poses a danger to computer assets
Managing Risk

- **Countermeasure**
  - General name for a procedure that recognizes, reduces, or eliminates a threat

- **Eavesdropper**
  - Person or device that can listen in on and copy Internet transmissions

- **Crackers or hackers**
  - Write programs or manipulate technologies to obtain unauthorized access to computers and networks
Computer Security Classifications

- **Secrecy**
  - Protecting against unauthorized data disclosure and ensuring the authenticity of a data source

- **Integrity**
  - Refers to preventing unauthorized data modification

- **Necessity**
  - Refers to preventing data delays or denials (removal)
Security Policy and Integrated Security

- A written statement describing
  - Which assets to protect and why they are being protected
  - Who is responsible for that protection
  - Which behaviors are acceptable and which are not
- First step in creating a security policy
  - Determine which assets to protect from which threats
## Requirements for Secure Electronic Commerce

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

**FIGURE 10-2** Requirements for secure electronic commerce
Security Policy and Integrated Security (continued)

Elements of a security policy

- Authentication
- Access control
- Secrecy
- Data integrity
- Audit
Security for Client Computers

- Stateless connection
  - Each transmission of information is independent

- Session cookies
  - Exist until the Web client ends connection
    - Cnn.com

- Persistent cookies
  - Remain on a client computer indefinitely
    - Amazon.com
Security for Client Computers (continued)

- First-party cookies
  - Cookies placed on a client computer by a Web server site
- Third-party cookies
  - Originates on a Web site other than the site being visited
- Web bug
  - Tiny graphic that a third-party Web site places on another site’s Web page
Information Stored in a Cookie on a Client Computer

**FIGURE 10-4** Information stored in a cookie on a client computer
Active Content

- **Programs** embedded transparently in Web pages that cause an action to occur
  - Windowsupdate.com (asks do you want to run an Active X control)

- Scripting languages
  - Provide scripts, or commands, that are executed

- Applet
  - Small application program
Dialog Box Asking for Permission to Open a Java Applet

FIGURE 10-5 Dialog box asking for permission to open a Java applet
Trojan horse
- Program hidden inside another program or Web page that masks its true purpose

Zombie
- Program that secretly takes over another computer to launch attacks on other computers
- Attacks can be very difficult to trace to their creators
Java Applets

- Java
  - Programming language developed by Sun Microsystems
- Java sandbox
  - Confines Java applet actions to a set of rules defined by the security model
- Untrusted Java applets
  - Applets not established as secure
JavaScript

- Scripting language developed by Netscape to enable Web page designers to build active content on the client side (in browser). Ex. Phone validation

- Can be used for attacks by
  - Executing code that destroys a client’s hard disk
  - Discloses e-mail stored in client mailboxes
  - Sends sensitive information to an attacker’s Web server
ActiveX Controls

- Object containing programs and properties that Web designers place on Web pages developed and run only on Microsoft technologies.

- Common programming languages used
  - C++ and Visual Basic

- Actions cannot be halted once they begin execution

- Unlike Java Script, has ability to access hard drive (Windows update)
Internet Explorer ActiveX Control Warning Message

![Security Alert]

An ActiveX object on this page may be unsafe. Do you want to allow it to initialize and be accessed by scripts?

**FIGURE 10-6** Internet Explorer ActiveX Control warning message
Viruses, Worms, and Antivirus Software

- Virus
  - Software that attaches itself to another program
  - Can cause damage when the host program is activated
- Macro virus
  - Type of virus coded as a small program (macro) and is embedded in a file
- Antivirus software
  - Detects viruses and worms
Digital Certificates

- A program embedded in a Web page that verifies that the sender or Web site is who or what it claims to be.

- Signed code or messages
  - Encrypted content that provides proof that the holder is the person identified by the certificate

- Certification authority (CA)
  - Issues digital certificates
Amazon.com’s Digital Certificate

FIGURE 10-7  Amazon.com’s digital certificate
Digital Certificates (continued)

- Main elements
  - Certificate owner’s identifying information
  - Certificate owner’s public key
  - Dates between which the certificate is valid
  - Serial number of the certificate
  - Name of the certificate issuer
  - Digital signature of the certificate issuer
Steganography

- Describes the process of hiding information within another piece of information (encryption)
- Provides a way of hiding an encrypted file within another file
- Messages hidden using steganography are difficult to detect
Communication Channel Security

- Secrecy
  - Prevention of unauthorized information disclosure
  - Privacy is the protection of individual rights to nondisclosure

- Sniffer programs
  - Provide the means to record information passing through a computer or router that is handling Internet traffic
Integrity Threats

- Exist when an unauthorized party can alter a message stream of information
- Cybervandalism
  - Electronic defacing of an existing Web site’s page
- Masquerading or spoofing
  - Pretending to be someone you are not
- Domain name servers (DNSs)
  - Computers on the Internet that maintain directories that link domain names to IP addresses
  - Globally around 16, referred to as K-root servers
Necessity Threats

- Purpose is to disrupt or deny normal computer processing

- DoS (denial of service) attacks
  - Remove information altogether
  - Delete information from a transmission or file
Threats to Wireless Networks

- Wardrivers
  - Attackers drive around using their wireless-equipped laptop computers to search for accessible networks

- Warchalking
  - When wardrivers find an open network they sometimes place a chalk mark on the building
Encryption Solutions

- **Encryption**
  - Using a mathematically based program and a secret key to produce a string of characters that is unintelligible

- **Cryptography**
  - Science that studies encryption
Encryption Algorithms

- Logic behind encryption programs
- Encryption program
  - Program that transforms normal text into cipher text
- Hash coding
  - Process that uses a hash algorithm to calculate a number from a message of any length
Asymmetric Encryption

- Encodes messages by using two mathematically related numeric keys
  - Public key
    - Freely distributed to the public at large
  - Private key
    - Belongs to the key owner, who keeps the key secret

www.pgp.com
Asymmetric Encryption (continued)

- Pretty Good Privacy (PGP)
  - One of the most popular technologies used to implement public-key encryption
  - Set of software tools that can use several different encryption algorithms to perform public-key encryption
  - Can be used to encrypt e-mail messages
Web Encryption

- Public-key (asymmetric) systems
  - Provide several advantages over private-key (symmetric) encryption methods
- Secure Sockets Layer (SSL)
  - Provide secure information transfer through the Internet
- SSL
  - Secures connections between two computers
- S-HTTP
  - Sends *individual* messages securely
- Digital signature
  - An encrypted message digest
Encryption Methods

FIGURE 10-9  (a) hash coding, (b) private-key, and (c) public-key encryption
Ensuring Transaction Integrity with Digital Signatures

- Hash algorithm
  - Anyone could
    - Intercept a purchase order
    - Alter the shipping address and quantity ordered
    - Re-create the message digest
    - Send the message and new message digest on to the merchant
Security for Server Computers

- Web server
  - Can compromise secrecy if it allows automatic directory listings
  - Can compromise security by requiring users to enter a username and password
- Dictionary attack programs
  - Cycle through an electronic dictionary, trying every word in the book as a password
Other Programming Threats

- **Buffer**
  - An area of memory set aside to hold data read from a file or database

- **Buffer overrun**
  - Occurs because the program contains an error or bug that causes the overflow

- **Mail bomb**
  - Occurs when hundreds or even thousands of people each send a message to a particular address
Firewalls

- Software or hardware and software combination installed on a network to control packet traffic
- Provides a defense between the network to be protected and the Internet, or other network that could pose a threat
Firewalls (continued)

- Characteristics
  - All traffic from inside to outside and from outside to inside the network must pass through the firewall
  - Only authorized traffic is allowed to pass
  - Firewall itself is immune to penetration

- Trusted
  - Networks inside the firewall

- Untrusted
  - Networks outside the firewall
Packet-filter firewalls
- Examine data flowing back and forth between a trusted network and the Internet (no mp3 files)

Gateway servers
- Firewalls that filter traffic based on the application requested (no IM programs)

Proxy server firewalls
- Firewalls that communicate with the Internet on the private network’s behalf (user accounts)
Organizations that Promote Computer Security

- CERT (cert.org)
  - Responds to thousands of security incidents each year
  - Helps Internet users and companies become more knowledgeable about security risks
  - Posts alerts to inform the Internet community about security events
Other Organizations

- SANS Institute
  - A cooperative research and educational organization

- SANS Internet Storm Center
  - Web site that provides current information on the location and intensity of computer attacks

- Microsoft Security Research Group
  - Privately sponsored site that offers free information about computer security issues

- www.sans.org
Computer Forensics and Ethical Hacking

- Computer forensics experts
  - Hired to probe PCs and locate information that can be used in legal proceedings

- Computer forensics
  - The collection, preservation, and analysis of computer-related evidence
Summary

Assets that companies must protect
  - Client computers
  - Computer communication channels
  - Web servers

Communication channels, in general, and the Internet, in particular are especially vulnerable to attacks

Encryption
  - Provides secrecy
Summary (continued)

- Web servers are susceptible to security threats
- Programs that run on servers might
  - Damage databases
  - Abnormally terminate server software
  - Make subtle changes in proprietary information
- Security organizations include CERT and SANS