CONTENTS

SYLLABUS

INTERNET AND E-COMMERCE

SECTION-A

Architectural Framework of E-commerce
Web architecture, web browser, HTTP, TCP/IP, Webserver, HTML, CGI, Scripts standards:- EDIFACT, edi.

SECTION-B

Security Issue
Introduction to viruse, worms, bombs and protective measure and security issue, firewalls, and proxy application gateways, secure, electronic transaction, public and private key encryption, digital signature, and digital certificate.

SECTION-C

Electronic Payments Systems
Digital cash, electronic signature, debit cards at point of scale, smart cards, online credit cards based systems, electronic fund EFT, payment gateways.

SECTION-D

Electronic Commerce Application
E-commerce banking, online shopping, business, models, and revenue models, online publishing, e-commerce in retail industry, CBS, digital copyrights, electronic data interchange, electronic fund transfer, electronic display board, electronic catalogue.

SECTION A

NOTES

UNIT 1 ARCHITECTURAL FRAMEWORK OF E-COMMERCE

★ LEARNING OBJECTIVES ★

- The Internet and the World Wide Web
- Packet—Switched Networks
- Internet Protocols
- Software for Web Servers
- Markup Languages and the Web

THE INTERNET AND THE WORLD WIDE WEB

A **computer network** is any technology that allows people to connect computers to each other. Computer networks and the Internet, which connects computer networks around the world to one another, form the basic technology structure that underlies all electronic commerce.

This section introduces you to the hardware and software technologies that make electronic commerce possible. First, you will learn how the Internet and the World Wide Web work. Then, you will learn about other technologies that support the Internet, the Web, and electronic commerce. In this section, you will be introduced to several complex networking technologies. Millions of people use the Internet every day, but only a small percentage of them really understand how it works. The **Internet** is a large system of interconnected computer net- works that spans the globe. Using the Internet, you can communicate with other people throughout the world by means of electronic mail; read online versions of newspapers, magazines, academic journals, and books; join discussion groups on almost any conceivable topic; participate in games and simulations; and obtain free computer software. In recent years, the Internet has allowed commercial enterprises to connect with one another and with customers. Today, all kinds of businesses provide

NOTES

information about their products and services on the Internet. Many of these businesses use the Internet to market and sell their products and services.

The part of the Internet known as the **World Wide Web**, or, more simply, the **Web**, is a subset of the computers on the Internet that are connected to one another in a specific way that makes them and their contents easily accessible to each other. The most important thing about the Web is that it includes an easy-to-use standard interface. This interface makes it possible for people who are not computer experts to use the Web to access a variety of Internet resources.

Origins of the Internet

In the early 1960s, the U.S. Department of Defense became concerned about the possible effects of nuclear attack on its computing facilities. The Defense Department realized that the weapons of the future would require powerful computers for coordination and control.

The powerful computers of that time were all large mainframe computers, so the Defense Department began examining ways to connect these computers to each other and also connect them to weapons installations distributed all over the world. The Defense Department agency charged with this task hired many of the best communications technology researchers and, for many years, funded research at leading universities and institutes to explore the task of creating a worldwide network that could remain operational, even if parts of the network were destroyed by enemy military action or sabotage. These researchers worked to devise ways to build networks that could operate independently—that is, networks that did not require a central computer to control network operations.

Early computer networks used leased telephone company lines for their connections. Telephone company systems of that time established a single connection between sender and receiver for each telephone call, and that connection carried all data along a single path. When a company wanted to connect computers it owned at two different locations, the company placed a telephone call to establish the connection, and then connected one computer to each end of that single connection. The Defense Department was concerned about the inherent risk of this single-channel method for connecting computers, and its researchers developed a different method of sending information through multiple channels. In this method, files and messages are broken into packets that are labeled electronically with codes for their origins, sequences, and destinations. In 1969, Defense Department researchers in the Advanced Research Projects Agency (ARPA) used this network model to connect four computers—one each at the University of California at Los Angeles, SRI International, the University of California at Santa Barbara,

and the University of Utah—into a network called the ARPANET. The ARPANET was the earliest of the networks that eventually combined to become what we now call the Internet. Throughout the 1970s and 1980s, many researchers in the academic community connected to the ARPANET and contributed to the technological developments that increased its speed and efficiency. At the same time, researchers at other universities were creating their own networks using similar technologies.

NOTES

New Uses for the Internet

Although the goals of the Defense Department network were to control weapons systems and transfer research files, other uses for this vast network began to appear in the early 1970s.

E-mail was born in 1972 when Ray Tomlinson, a researcher who used the network, wrote a program that could send and receive messages over the network. This new method of communicating became widely used very quickly. The number of network users in the military and education research communities continued to grow. Many of these new participants used the networking technology to transfer files and access computers remotely.

The first e-mail mailing lists also appeared on these networks. A **mailing list** is an e-mail address that forwards any message it receives to any user who has subscribed to the list. In 1979, a group of students and programmers at Duke University and the University of North Carolina started **Usenet**, an abbreviation for **User's News Network**. Usenet allows anyone who connects to the network to read and post articles on a variety of subjects. Usenet survives on the Internet today, with more than 1000 different topic areas that are called **newsgroups**. Other researchers even created game-playing software for use on these interconnected networks. Although the people using these networks were developing many creative applications, use of the networks was limited to those members of the research and academic communities who could access them. Between 1979 and 1989, these network applications were improved and tested by an increasing number of users. The Defense Department's networking software became more widely used in academic and research institutions as these organizations recognized the benefits of having a common communications network. As the number of people in different organizations using these networks increased, security problems were recognized. These problems have continued to become more important,. The explosion of personal computer use during the 1980s also helped more people become comfortable with computers. In the late 1980s, these independent academic and research networks merged into what we now call the Internet.

NOTES

Commercial Use of the Internet

As personal computers became more powerful, affordable, and available during the 1980s, companies increasingly used them to construct their own internal networks. Although these networks included e-mail software that employees could use to send messages to each other, businesses wanted their employees to be able to communicate with people out side their corporate networks. The Defense Department network and most of the academic networks that had teamed up with it were receiving funding from the **National Science Foundation (NSF)**. The NSF prohibited commercial network traffic on its networks, so businesses turned to commercial e-mail service providers to handle their e-mail needs. Larger firms built their own networks that used leased telephone lines to connect field offices to corporate headquarters.

In 1989, the NSF permitted two commercial e-mail services, MCI Mail and CompuServe, to establish limited connections to the Internet for the sole purpose of exchanging e-mail transmissions with users of the Internet. These connections allowed commercial enterprises to send e-mail directly to Internet addresses, and allowed members of the research and education communities on the Internet to send e-mail directly to MCI Mail and CompuServe addresses. The NSF justified this limited commercial use of the Internet as a service that would primarily benefit the Internet's noncommercial users. As the 1990s began, people from all walks of life—not just scientists or academic researchers—started thinking of these networks as the global resource that we now know as the Internet. Although this network of networks had grown from four Defense Department computers in 1969 to more than 300,000 computers on many interconnected networks by 1990, the greatest growth of the Internet was yet to come.

Growth of the Internet

In 1991, the NSF further eased its restrictions on commercial Internet activity and began implementing plans to privatize the Internet. The privatization of the Internet was substantially completed in 1995, when the NSF turned over the operation of the main Internet connections to a group of privately owned companies. The new structure of the

Internet was based on four **network access points (NAPs)** located in San Francisco, New York, Chicago, and Washington, D.C., each operated by a separate telecommunications company. As the Internet grew, more companies opened more NAPs in more locations. These companies, known as **network access providers**, sell Internet access rights directly to larger customers and indirectly to smaller firms and individuals through other companies, called **Internet service providers (ISPs).**

NOTES

The Internet was a phenomenon that had truly sneaked up on an unsuspecting world.The researchers who had been so involved in the creation and growth of the Internet just accepted it as part of their working environment. However, people outside the research community were largely unaware of the potential offered by a large interconnected set of computer networks. Figure 1.1 shows the consistent and dramatic growth in the number of **Internet hosts**, which are computers directly connected to the Internet.

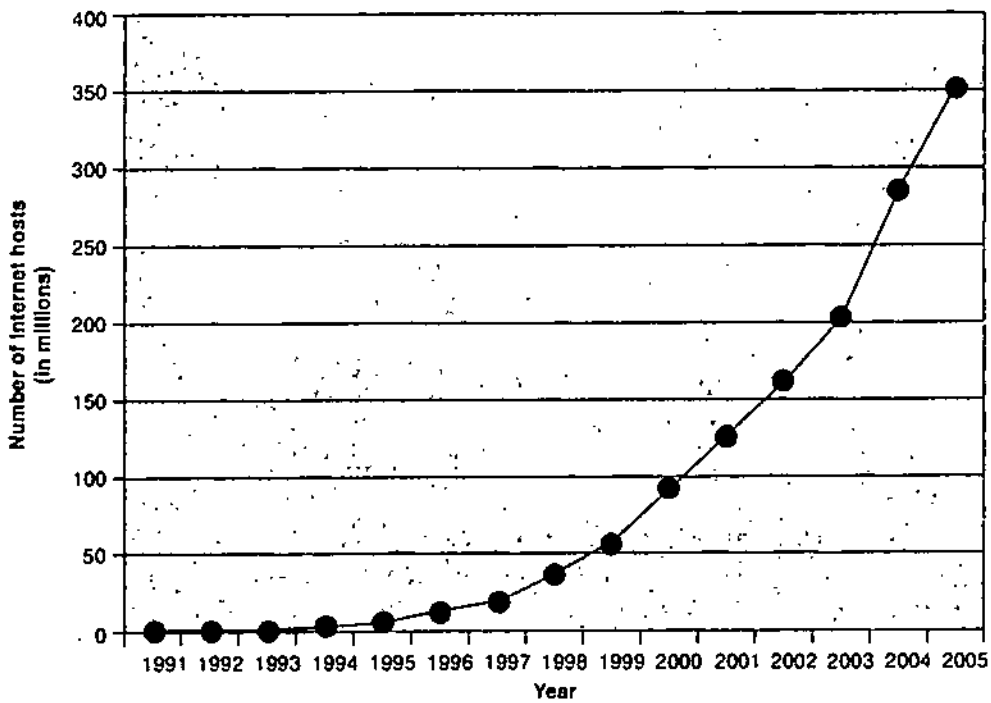


Figure 1.1. *Growth of Internet.*

As more people gain access to the Web, commercial interest in using the Web to conduct business will continue to increase, and the variety of non business uses will become even greater. In the rest of this section, you will learn how Internet and Web technologies work to enable electronic commerce.

In 30 years, the Internet has grown to become one of the most amazing technological and social accomplishments of the last century. Millions of people, most of whom are not computer researchers or experts, now use this complex, interconnected network of computers. These computers run thousands of different software packages. The computers are located in almost every country of the world. Every year, billions of dollars change hands over the Internet in exchange for all kinds of products and services. All of this activity occurs with no central coordination point or control, which is especially ironic given that he Internet began as a way for the military to maintain control while under attack.

NOTES

The opening of the Internet to business activity helped dramatically increase its growth; however, there was another development that worked hand in hand with the commercialization of the Internet to spur its growth. That development was the World Wide Web.

Emergence of the World Wide Web

The Web is software that runs on computers that are connected to the Internet. The network traffic generated by Web software is the largest single category of traffic on the Internet today, outpacing e-mail, file transfers, and other data transmission traffic. But the Web is more a way of thinking about and organizing information storage and retrieval than it is a specific technology. As such, its history goes back many years. Two important innovations that became key elements of the Web are hypertext and graphical user interfaces.

The Development of Hypertext

In 1945, **Vannevar Bush**, who was director of the U.S. Office of Scientific Research and Development, wrote an article in The Atlantic Monthly about ways that scientists could apply the skills they learned during World War II to peacetime activities. The article included a number of visionary ideas about future uses of technology to organize and facilitate efficient access to information. Bush speculated that engineers would eventually build a machine that he called the Memex, a memory extension device that would store all of a person's books, records, letters, and research results on microfilm. Bush's Memex would include mechanical aids, such as microfilm readers and indexes, that would help users quickly and flexibly consult their collected knowledge.

In the 1960s, Ted Nelson described a similar system in which text on one page links to text on other pages. Nelson called his page-linking system **hypertext**. Douglas Engel bart, who also invented the computer mouse, created the first experimental hypertext system on one of the large computers of the 1960s. In 1987, Nelson published Literary Machines, a book in which he outlined project Xanadu, a global system for online hypertext publishing and commerce. Nelson used the term hypertext to describe a page-linking system that would interconnect related pages of information, regardless of where in the world they were stored.

In 1989, Tim Berners-Lee was trying to improve the laboratory research document handling procedures for his employer, CERN : European Laboratory for Particle Physics. CERN had been connected to the Internet for two years, but its scientists wanted to find better ways to circulate their scientific papers and data among the high-energy physics research community throughout the world. Berners-Lee proposed a hypertext develop ment project

NOTES

intended to provide this data-sharing functionality. Over the next two years, Berners-Lee developed the code for a hypertext server program and made it available on the Internet. A **hypertext server** is a computer that stores files written in the hypertext markup language and lets other computers connect to it and read these files. Hypertext servers used on the Web today are usually called **Web servers.**

Hypertext Markup Language (HTML), which Berners-Lee developed from his original hypertext server program, is a language that includes a set of codes (or tags) attached to text. These codes describe the relationships among text elements. For example, HTML includes tags that indicate which text is part of a header element, which text is part of a paragraph element, and which text is part of a numbered list element. One important type of tag is the hypertext link tag. A **hypertext link**, or **hyperlink**, points to another location in the same or another HTML document.

Graphical Interfaces for Hypertext

Several different types of software are available to read HTML documents, but most people use a Web browser such as Netscape Navigator or Microsoft Internet Explorer. A **Web browser** is a software interface that lets users read (or browse) HTML documents and move from one HTML document to another through text formatted with hypertext link tags in each file. If the HTML documents are on computers connected to the Internet, you can use a Web browser to move from an HTML document on one computer to an HTML document on any other computer on the Internet.

An HTML document differs from a word-processing document in that it does not specify how a particular text element will appear. For example, you might use word-processing software to create a document heading by setting the heading text font to Arial, its font size to 14 points, and its position to centered. The document displays and prints these exact settings whenever you open the document in that word processor. In contrast, an HTML document simply includes a heading tag with the heading text. Many different browser programs can read an HTML document. Each program recognizes the heading tag and displays the text in whatever manner each program normally displays headings. Different Web browser programs might each display the text differently, but all of them display the text with the characteristics of a heading.A Web browser presents an HTML document in an easy-to-read format in the browser's graphical user interface. A **graphical user interface (GUI)**is a way of presenting program control functions and program output to users. It uses pictures, icons, and other graphical elements instead of displaying just text. Almost all personal computers today use a GUI such as Microsoft Windows or the Macintosh user interface.

NOTES

The World Wide Web

Berners-Lee called his system of hyperlinked HTML documents the World Wide Web. The Web caught on quickly in the scientific research community, but few people outside that community had software that could read the HTML documents. In 1993, a group of students led by Marc Andreessen at the University of Illinois wrote Mosaic, the first GUI program that could read HTML and use HTML hyperlinks to navigate from page to page on computers anywhere on the Internet. Mosaic was the first Web browser that became widely available for personal computers, and some Web surfers still use it today.

Programmers quickly realized that a functional system of pages connected by hypertext links would provide many new Internet users with an easy way to access information on the Internet. Businesses recognized the profit-making potential offered by a worldwide network of easy-to-use computers. In 1994, Andreessen and other members of the members of the University of Illinois Mosaic team joined with James Clark of **Silicon Graphics** to found Netscape Communications (which is now owned by **Time Warner**). Its first product, the Netscape Navigator Web browser program based on Mosaic, was an instant success. Netscape became one of the fastest-growing software companies ever. **Microsoft** created its Internet Explorer Web browser and entered the market soon after Netscape's success became apparent. A number of other Web browsers exist, but Internet Explorer dominates the market today.

The number of Web sites has grown even more rapidly than the Internet itself. The number of Web sites is currently estimated at more than 75 million, and individual Web pages number more than 20 billion because each Web site might include hundreds or even thousands of individual Web pages. Therefore, nobody really knows how many Web pages exist. For example, researchers at **BrightPlanet** estimate that the number of Web sites could be more than 500 million. Figure 1.2 shows how the growth rate of the Web increased dramatically between 1997 and 2000. After a brief consolidation period during 2001–2002, the Web is once again showing rapid growth.

As more people gain access to the Web, commercial interest in using the Web to conduct business will continue to increase, and the variety of non business uses will become even greater.

NOTES

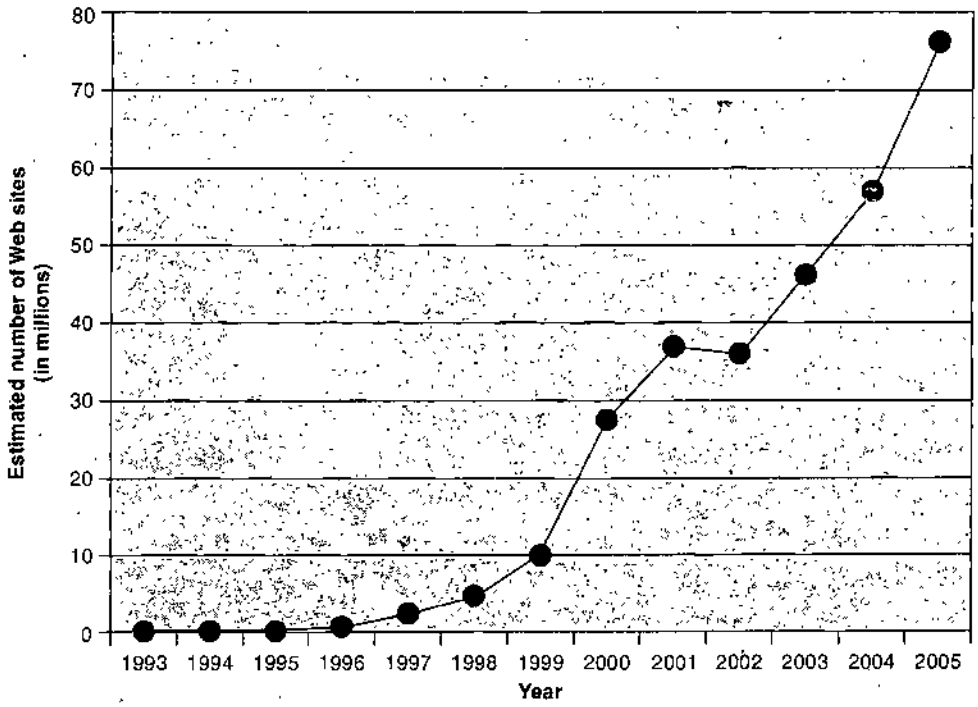


Figure 1.2. *Growth of the World Wide Web.*

Web Architecture Extensibility

This basic web architecture is fast evolving to serve a wider variety of needs beyond static document access and browsing. The Common Gateway Interface (CGI) extends the architecture to three-tiers by adding a back-end server that provides services to the Web server on behalf of the Web client, permitting dynamic composition of web pages. Helpers/plug-ins and Java/JavaScript provide other interesting Web architecture extensions.

- **Common Gateway Interface**(CGI)—CGI is a standard for interfacing external programs with Web servers (see Figure 1.3). The server hands client *requests* encoded in URLs to the appropriate registered CGI program, which executes and returns results encoded as MIME messages back to the server. CGI's openness avoids the need to extend HTTP. The most common CGI applications handle HTML <FORM> and <ISINDEX> commands.
  - CGI programs are executable programs that run on the Web server. They can be written in any scripting language (interpreted) or programming language (must be compiled first) available to be executed on a Web server, including C, C++, Fortran, PERL, TCL, Unix shells, Visual Basic, Applescript, and others. Security precautions typically require that CGI programs be run from a specified directory (e.g, /cgi-bin) under control of the webmaster (Web system administrator), that is, they must be registered with the system.

NOTES

- Arguments to CGI programs are transmitted from client to server via environment variables encoded in URLs. The CGI program typically returns HTML pages that it constructs on the fly.
- Some problems with CGI are :
  - the CGI interface requires the server to execute a program
  - the CGI interface does not provide a way to share data and communications resources so if a program must access an external resource, it must open and close that resource. It is difficult to construct transactional interactions using CGI.
- The current version is CGI/1.3. W3C and others are experimenting with next generation object-oriented APIs based on OMG IDL; Netscape provides Netscape Server API (NSAPI) and Progress Software and Microsoft provide Internet Server API (ISAPI).

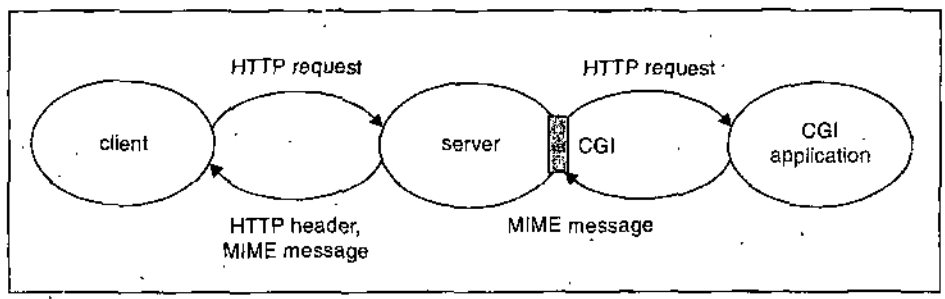


Figure 1.3. *A backend CGI program provides services to the WWW server on behalf of the client.*

- **Helpers/Plug-ins.** When a client browser retrieves a file, it launches an installed helper application or plug-in to process the file based on the file's MIME-type (see below). For example, it may launch a Postscript or Acrobat reader, or MPEG or QuickTime player. A helper application runs external to the browser while a plug-in runs within the browser. For information on how to create new Netscape Navigator plug-ins, see The Plug-in Developer's Guide.
- **Common Client Gateway (CCI).** This gateway allows a third-party application to remotely control the Web browser client. Netscape Client APIs 2.0 (NCAPIs) depends on platform specific native methods of interprocess communication (IPC). They plan to support DDE and OLE2 for Windows clients, X properties for UNIX clients, and Apple Events for Macintosh clients.
- **Extensions to HTTP.** W3C and IETF Application Area HTTP Working Group are working together on current and future versions of HTTP. The HTTP-NG project is assessing two implementation approaches to HTTP "replacements" :

NOTES

- Spero's approach-allows many requests per connection, the requests can be asynchronous and the server can respond in any order, allowing several transfers in parallel. A "session layer" divides the connection into numerous channels. Control messages (GET requests, meta information) are returned in a control channel; each object is returned in its own channel.
- W3C approach-Jim Gettys at W3C is using Xerox ILU (a CORBA variant) to implement an ILU transport similar to Spero's session protocol. The advantages of this approach are openness with respect to pluggable transport protocols, support for multiple language environments, and a step towards viewing the "web of objects." Related to this approach, Netscape recently announced future support for OMG Internet Inter-ORB Protocol (IIOP) standard on both client and server. This will provide a uniform and language neutral object interchange format making it easier to construct distributed object applications.

- **Java/ JavaScript.** Java is a cross-platform WWW programming language *modeled after C++ from* Sun Microsystems. Java programs embedded in HTML documents are called *applets* and are specified using <APPLET> tags. The HTML for an applet contains a *code* attribute that specifies the URL of the compiled applet file. Applets are compiled to a platform-independent bytecode which can be *safely* downloaded and executed by the Java interpreter embedded into the Web browser. Browsers that support Java are said to be Java-enabled. If performance is critical, a Java applet can be compiled to native machine language on the fly. Such a compiler is known as a Just-In-Time (JIT) compiler. JavaScript is a scripting language designed for creating dynamic, interactive Web applications that link together objects and resources on both clients and servers. A client JavaScript can recognize and respond to user events such as mouse clicks, form input, and page navigation, and query the state or alter the performance of an applet or plug-in. A server JavaScript script can exhibit behavior similar to common gateway interface (CGI) programs. JavaScript scripts are embedded in HTML documents using <SCRIPT> tags. Similar to Java applets, JavaScript scripts are directly interpreted within the client's browser and are therefore platform-independent.
- The IETF Security Area Web Transaction Security (WTS) Working Group is working on security services for WWW. As chartered, it has produced Internet-drafts of a Requirements for Web Transaction Security and a Secure HyperText Transfer Protocol specification plus Security Extensions For HTML.

NOTES

PACKET – SWITCHED NETWORKS

A network of computers that are located close together—for example, in the same building—is called a **local area network**, or a **LAN.** Networks of computers that are connected over greater distances are called **wide area networks**, or **WANs**. The early models (dating back to the 1950s) for WANs were the circuits of the local and long-distance telephone companies of the time, because the first early WANs used leased telephone company lines for their connections. A telephone call establishes a single connection path between the caller and receiver. Once that connection is established, data travels along that single path. Telephone company equipment (originally mechanical, now electronic) selects specific telephone lines to connect to one another by closing switches.

These switches work like the switches you use to turn lights on and off in your home, except that they open and close much faster, and are controlled by mechanical or electronic devices instead of human hands.

The combination of telephone lines and the closed switches that connect them to each other is called a **circuit**. This circuit forms a single electrical path between caller and receiver. This single path of connected circuits switched into each other is maintained for the entire length of the call. This type of centrally controlled, single-connection model is known as **circuit switching**. Although circuit switching works well for telephone calls, it does not work as well for sending data across a large WAN or an interconnected network like the Internet. The Internet was designed to be resistant to failure. In a circuit-switched network, a failure in any one of the connected circuits causes the connection to be interrupted and data to be lost. Instead, the Internet uses packet switching to move data between two points. On a **packet-switched** network, files and e-mail messages are broken down into small pieces, called **packets**, that are labeled electronically with their origins, sequences, and destination addresses. Packets travel from computer to computer along the interconnected networks until they reach their destinations. Each packet can take a different path through the interconnected networks, and the packets may arrive out of order. The destination computer collects the packets and reassembles the original file or e-mail message from the pieces in each packet.

Routing Packets

As an individual packet travels from one network to another, the computers through which the packet travels determine the best route for getting the packet to its destination. The computers that decide how best to forward each packet are called **routing computers, router computers, routers, gateway computers** (because they act as the gateway from a LAN or WAN

NOTES

to the Internet), or **border routers** (because they are located at the border between the organization and the Internet). The programs on router computers that determine the best path on which to send each packet contain rules called **routing algorithms**. The programs apply their routing algorithms to information they have stored in **routing tables** or **configuration tables**. This information includes lists of connections that lead to particular groups of other routers, rules that specify which connections to use first, and rules for handling instances of heavy packet traffic and network congestion.Individual LANs and WANs can use a variety of different rules and standards for creating packets within their networks. The network devices that move packets from one part of a network to another are called hubs, switches, and bridges. Routers are used to connect networks to other networks. As technologies have improved, many of the distinctions between these different types of network devices have become blurred. You can take a data communications and networking class to learn more about these network devices and how they work.

When packets leave a network to travel on the Internet, they must be translated into a standard format. Routers usually perform this translation function. As you can see, routers are an important part of the infrastructure of the Internet. When a company or organization becomes part of the Internet, it must connect at least one router to the other routers(owned by other companies or organizations) that make up the Internet. Figure 1.4 is a diagram of a small portion of the Internet that shows its router-based architecture. The figure shows only the routers that connect each organization's WANs and LANs to the Internet, not the other routers that are inside the WANs and LANs or that connect them to each other within the organization.

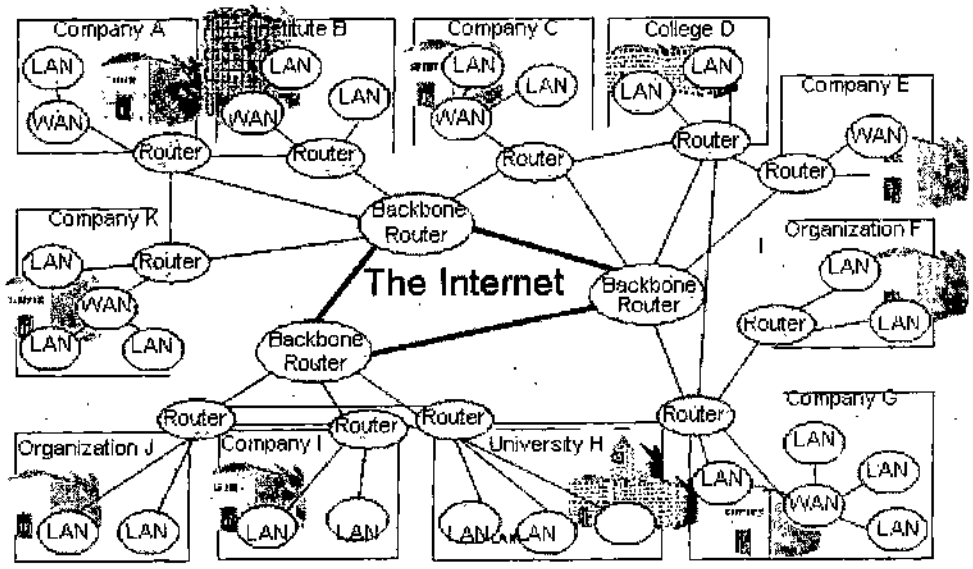


Figure 1.4. *Router-based architecture of the Internet.*

NOTES

The Internet also has routers that handle packet traffic along the Internet's main connecting points. These routers and the telecommunications lines connecting them are collectively referred to as the **Internet backbone**. These routers, sometimes called **backbone routers**, are very large computers that can each handle more than 50 million packets per second! By building in multiple packet paths, the designers of the Internet created a degree of redundancy in the system that allows it to keep moving packets, even if one or more of the routers or connecting lines fails.

INTERNET PROTOCOLS

ARPANET, connected only a few universities and research centers. This experimental network grew during the next few years and used the **Network Control Protocol (NCP)**. A **protocol** is a collection of rules for formatting, ordering, and error-checking data sent across a network. For example, protocols determine how the sending device indicates that it has finished sending a message, and how the receiving device indicates that it has received (or not received) the message. A protocol also includes rules about what is allowed in a transmission and how it is formatted. Computers that communicate with each other must use the same protocol for data transmission. In the early days of computing, each computer manufacturer created its own protocol, so computers made by different manufacturers could not be connected to each other. This practice was called **proprietary architecture** or **closed architecture**. The **open architecture** philosophy developed for the evolving ARPANET, which later became the core of the Internet, included the use of a common protocol for all computers connected to the Internet and four key rules for message handling :

- Independent networks should not require any internal changes to be connected to the network.
- Packets that do not arrive at their destinations must be retransmitted from their source network.
- Router computers act as receive-and-forward devices; they do not retain information about the packets that they handle.
- No global control exists over the network.

The open architecture approach has contributed to the success of the Internet because computers manufactured by different companies (Apple, Dell, Hewlett-Packard, Sun, etc.) can be interconnected. The ARPANET and its successor, the Internet, use routers to isolate each LAN or WAN from the

NOTES

other networks to which they are connected. Each LAN or WAN can use its own set of protocols for packet traffic within the LAN or WAN, but must use a router (or similar device) to move packets onto the Internet in its standard format (or protocol). Following these simple rules makes the connections between the interconnected networks operate effectively.

TCP/IP

The Internet uses two main protocols : the **Transmission Control Protocol (TCP)** and the **Internet Protocol (IP)**. Developed by Internet pioneers Vinton Cerf and Robert Kahn, these protocols are the rules that govern how data moves through the Internet and how network connections are established and terminated. The acronym **TCP/IP** is commonly used to refer to the two protocols.

The TCP controls the disassembly of a message or a file into packets before it is transmitted over the Internet, and it controls the reassembly of those packets into their original formats when they reach their destinations. The IP specifies the addressing details for each packet, labeling each with the packet's origination and destination addresses. Soon after the new TCP/IP protocol set was developed, it replaced the NCP that ARPANET originally used.

In addition to its Internet function, TCP/IP is used today in many LANs. The TCP/IP protocol is provided in most personal computer operating systems commonly used today, including Linux, Macintosh, Microsoft Windows, and UNIX.

IP Addressing

The version of IP that has been in use for the past 20 years on the Internet is **I Internet Protocol version 4**, abbreviated **IPv4**. It uses a 32-bit number to identify the computers connected to the Internet. This address is called an **IP address**. Computers do all of their internal calculations using a **base 2** (or **binary**) number system in which each digit is either a 0 or a 1, corresponding to a condition of either off or on. IPv4 uses a 32-bit binary number that allows more than 4 billion different addresses (2^{32}= 4,294,967,296).

When a router breaks a message into packets before sending it onto the Internet, the router marks each packet with both the source IP address and the destination IP address of the message. To make them easier to read, IP numbers (addresses) appear as four numbers separated by periods. This notation system is called **dotted decimal** notation. An IPv4 address is a 32-bit number, so each of the four numbers is an 8-bit number (4 × 8 = 32).

In most computer applications, an 8-bit number is called a **byte**; however, in networking applications, an 8-bit number is often called an **octet**. In

NOTES

binary, an octet can have values from 00000000 to 11111111; the decimal equivalents of these binary numbers are 0 and 255, respectively.

Because each of the four parts of a dotted decimal number can range from 0 to 255, IP addresses range from 0.0.0.0 (written in binary as 32 zeros) to 255.255.255.255 (written in binary as 32 ones). Although some people find dotted decimal notation to be confusing at first, most do agree that writing, reading, and remembering a computer's address as 216.115.108.245 is easier than 11011000011100110110110011110101, or its full decimal equivalent, which is 3,631,433,189.

Today, IP addresses are assigned by three not-for-profit organizations : the **American Registry for Internet Numbers (ARIN)**, the **Reséaux IP Européens (RIPE)**, and the **Asia-Pacific Network Information Center (APNIC)**. These registries assign and manage IP addresses for various parts of the world : ARIN for North America, South America, the Caribbean, and sub-Saharan Africa; RIPE for Europe, the Middle East, and the rest of Africa; and APNIC for countries in the Asia-Pacific area. These organizations took over IP address management tasks from the Internet Assigned Numbers Authority (IANA), which performed them under contract with the U.S. government when the Internet was an experimental research project.

You can use the **ARIN Whois** page at the ARIN Web site to search the IP addresses owned by organizations in North America. You can enter an organization name into the search box on the page, then click the Submit Query button, and the Who is server returns a list of the IP addresses owned by that organization. For example, performing a search on the word Carnegie displays the IP address blocks owned by Carnegie Bank, Carnegie Mellon University, and a number of other organizations whose names begin with Carnegie. You can also enter an IP address and find out who owns that IP address. If you enter "3.0.0.0" (without the quotation marks), you will find that General Electric owns the entire block of IP addresses from 3.0.0.0 to 3.255.255.255. General Electric can use these addresses, which number approximately 16.7 million, for its own computers or it can lease them to other companies or individuals to whom it provides Internet access services.

In the early days of the Internet, the 4 billion addresses provided by the IPv4 rules cer tainly seemed to be more addresses than an experimental research network would ever need. However, about 2 billion of those addresses today are either in use or unavailable for use because of the way blocks of addresses were assigned to organizations. The new kinds of devices on the Internet's many networks, such as wireless personal digital assistants and cell phones that can access the Web, promise to keep demand high for IP addresses.

Network engineers have devised a number of stopgap techniques to stretch the supply of IP addresses. One of the most popular techniques is **subnetting**,

which is the use of reserved private IP addresses within LANs and WANs to provide additional address space.

NOTES

Private IP addresses are a series of IP numbers that are not permitted on packets that travel on the Internet. In subnetting, a computer called a **Network Address Translation (NAT) device** converts those private IP addresses into normal IP addresses when it forwards packets from those computers to the Internet. The **Internet Engineering Task Force (IETF)** worked on several new protocols that could solve the limited addressing capacity of IPv4, and in 1997, approved **Internet Protocol version 6 (IPv6)** as the protocol that will replace IPv4. The new IP is being implemented gradually because the two protocols are not directly compatible. The process of switching over to IPv6 will take at least another 10 years; however, network engineers have devised ways to run both protocols together on interconnected networks. The major advantage of IPv6 is that it uses a 128-bit number for addresses instead of the 32-bit number used in IPv4. The number of available addresses in IPv6 (2^{128}) is 34 followed by 37 zeros—billions of times larger than the address space of IPv4. The new IP also changes the format of the packet itself. Improvements in networking technologies over the past 20 years have made many of the fields in the IPv4 packet unnecessary. IPv6 eliminates those fields and adds fields for security and other optional information. IPv6 has a shorthand notation system for expressing addresses, similar to the IPv4 dotted decimal notation system. However, because the IPv6 address space is much larger, its notation system is more complex. The IPv6 notation uses eight groups of 16 bits ($8 \times 16 = 128$). Each group is expressed as four hexadecimal digits and the groups are separated by colons; thus, the notation system is called **colon hexadecimal** or **colon hex.**

A **hexadecimal (base 16)** numbering system uses 16 digits (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c,d, e, and f). An example of an IPv6 address expressed in this notation is : *CD18:0000:0000:AF23:0000:FF9E:61B2:884D. To save space,* the zeros can be omitted, which reduces this address to : CD18:::AF23:: FF9E :61B2:884D.

Domain Names

The founders of the Internet were concerned that users might find the dotted decimal notation difficult to remember. To make the numbering system easier to use, they created an alternative addressing method that uses words. In this system, an address such as www.thomson.com is called a domain name.

Domain names are sets of words that are assigned to specific IP addresses. Domain names can contain two or more word groups separated by periods.

NOTES

The right most part of a domain name is the most general. Each part of the domain name becomes more specific as you move to the left.

For example, the domain name www.sandiego.edu contains three parts separated by periods. Beginning at the right, the name "edu" indicates that the computer belongs to a four-year educational institution. The institution, University of San Diego, is identified by the name "sandiego." The "www" indicates that the computer is running software that makes it a part of the World Wide Web. Most, but not all, Web addresses follow this "www" naming convention. For an example of an exception, the group of computers that operate the **Yahoo! Games** service is named games.yahoo.com.The rightmost part of a domain name is called a **top-level domain** (or **TLD**). For many years, these domains have included a group of general domains—such as.edu,.com, and.org—and a set of country domains. Since 1998, the **Internet Corporation for Assigned Names and Numbers (ICANN)** has had responsibility for managing domain names and coordinating them with the IP address registrars. ICANN is also responsible for setting standards for the router computers that make up the Internet. In 2000, ICANN added seven new TLDs. Four of these TLDs (.biz,.info,.name, and.pro) are general domains, the other three (.aero,.coop, and.museum) are sponsored domains. A **sponsored top-level domain (sTLD)** is a TLD for which an organization other than ICANN is responsible. The sponsor of a specific sTLD must be a recognized institution that has expertise regarding and is familiar with the community that uses the sTLD. For example, the.aero sTLD is sponsored by SITA, an air transport industry association that has expertise in and is familiar with airlines, airports, and the aerospace industry. Although these new domain names were chosen after much deliberation and consideration of more than 100 possible new names, many people were highly critical of the selections (see, for example, the **ICANNWatch** Web site).

In 2002, ICANN came under additional fire for acting in ways that many people thought violated the democratic principles on which the organization was founded. In 2005, ICANN approved a new sTLD for adult content sites (.xxx) as a part of its normal deliberations on 10 proposed new sTLDs. The U.S. Commerce Department, responding to pressure from conservative political groups, ordered ICANN to delay implementing the.xxx domain. Many observers believe that this intervention has seriously damaged the independence of ICANN. You can learn more about these issues on the Web sites of the **Internet Governance Project** and the **Convergence Center at Syracuse University**. Increases in the number of TLDs can make it more difficult for companies to protect their corporate and product brand names. Figure 1.5 presents a list of the general TLDs, including the 2000 additions, and some of the more frequently used country TLDs.

NOTES

Original general TLDs		Country TLDs		General TLDs added in 2000	
TLD	Use	TLD	Country	TLD	Use
.com	Commercial	.au	Australia	.biz	Businesses
.edu	Four-year educational institution	.ca	Canada	.info	General use
		.de	Germany	.name	Individual people
.gov	U.S. federal government	.fi	Finland	.pro	Professionals (accountants, lawyers, physicians)
.mil	U.S. military	.fr	France		
.net	General use	.jp	Japan		
.org	Not-for-profit organization	.se	Sweden		
		.uk	United Kingdom		

Figure 1.5. *Top-level domain names.*

Web Page Request and Delivery Protocols

The Web is software that runs on computers that are connected to each other through the Internet. **Web client computers** run software called **Web client software** or **Web browser software**. Web client software sends requests for Web page files to other computers, which are called Web servers. A Web server computer runs software called **Web server software**.

Web server software receives requests from many different Web clients and responds by sending files back to those Web client computers. Each Web client computer's Web client software renders those files into a Web page. Thus, the purpose of a Web server is to respond to requests for Web pages from Web clients. This combination of client computers running Web client software and server computers running Web server software is called a **client/server architecture.**

The set of rules for delivering Web page files over the Internet is in a protocol called the **Hypertext Transfer Protocol (HTTP)**, which was developed by Tim Berners-Lee in 1991.

When a user types a domain name (for example, www.yahoo.com) into a Web browser's address bar, the browser sends an HTTP-formatted message to a Web server computer at Yahoo! that stores Web page files. The Web server computer at Yahoo! then responds by sending a set of files (one for the Web page and one for each graphic object, sound, or video clip included on the page) back to the client computer. These files are sent within a message that is HTTP formatted. To initiate a Web page request using a Web browser, the user types the name of the protocol, followed by the characters "// :" before the domain name. Thus, a user would type http :// www.yahoo.com to go to the Yahoo! Web site. Most Web browsers today automatically insert the http :// if the user does not include it. The combination of the protocol name and the domain name is called a **Uniform Resource Locator (URL)** because it lets the user locate a resource (the Web page) on another computer (the Web server).

NOTES

Electronic Mail Protocols

Electronic mail, or **e-mail**, that is sent across the Internet must also be formatted according to a common set of rules. Most organizations use a client/server structure to handle e-mail. The organization has a computer called an **e-mail server** that is devoted to handling e-mail. The software on that computer stores and forwards e-mail messages. People in the organization might use a variety of programs, called **e-mail client software**, to read and send e-mail. These programs include **Microsoft Outlook**, **Mozilla Thunderbird**, **Netscape Messenger**, **Pegasus Mail**, **Qualcomm Eudora**, and many others. The e-mail client software communicates with the e-mail server software on the e-mail server computer to send and receive e-mail messages.

Many people also use e-mail on their computers at home. In most cases, the e-mail servers that handle their messages are operated by the companies that provide their connections to the Internet. An increasing number of people use e-mail services that are offered by Web sites such as **Yahoo! Mail** or **Hotmail**. In these cases, the e-mail servers and the e-mail clients are operated by the owners of the Web sites. The individual users only see the e-mail client software (and not the e-mail server software) in their Web browsers when they log on to the Web mail service.

With so many different e-mail client and server software choices, standardization and rules are very important. If e-mail messages did not follow standard rules, an e-mail message created by a person using one e-mail client program could not be read by a person using a different e-mail client program. As you have already learned in this chapter, rules for computer data transmission are called protocols.

SMTP and POP are two common protocols used for sending and retrieving e-mail.

Simple Mail Transfer Protocol (SMTP) specifies the format of a mail message and describes how mail is to be administered on the e-mail server and transmitted on the Internet. An e-mail client program running on a user's computer can request mail from the organization's e-mail server using the **Post Office Protocol (POP)**. A POP message can tell the e-mail server to send mail to the user's computer and delete it from the e-mail server; send mail to the user's computer and not delete it; or simply ask whether new mail has arrived.

The POP provides support for **Multipurpose Internet Mail Extensions (MIME)**, which is a set of rules for handling binary files, such as word-processing documents, spreadsheets, photos, or sound clips, that are attached to e-mail messages.

NOTES

IMAP, the **Interactive Mail Access Protocol**, is a newer e-mail protocol that performs the same basic functions as POP, but includes additional features. For example, IMAP can instruct the e-mail server to send only selected e-mail messages to the client instead of all messages. IMAP also allows the user to view only the header and the e-mail sender's name before deciding to download the entire message. POP allows users to search for and manipulate only those e-mail messages that they have downloaded to their computers. IMAP lets users create and manipulate mail folders (also called mailboxes), delete messages, and search for certain parts of a message while the e-mail is still on the e-mail server; that is, the user does not need to download the e-mail before working with it. The tools that IMAP provides are important to the increasing number of people who access their e-mail from different computers at different times. IMAP lets users manipulate and store their e-mail on the e-mail server and access it from any number of computers. POP allows users to access new e-mail messages from only one PC after they download the old messages to another PC. The main drawback to IMAP is that users' e-mail messages are stored on the e-mail server. As the number of users increases, the size of the e-mail server's disk drives must also increase. In general, server computers use faster (and thus, more expensive) disk drives than desktop computers. Therefore, it is more expensive to provide disk storage space for large quantities of e-mail on a server computer than to provide that same disk space on users' desktop computers. You can learn more about IMAP at the University of Washington's **IMAP Connection** Web site.

Unsolicited Commercial E-Mail (UCE, Spam)

Spam, also known as **unsolicited commercial e-mail (UCE)** or **bulk mail**, is electronic junk mail and can include solicitations, advertisements, or e-mail chain letters. The origin of the term spam is generally believed to have come from a song performed by British comedy troupe Monty Python about Hormel's canned meat product, SPAM. In the song, an increasing number of people join in repeating the songs chorus : "Spam spam spam spam,spam spam spam spam, lovely spam, wonderful spam..." Just as in the song, e-mail spam is a tiresome repetition of meaningless text that eventually drowns out any other attempt at communication. Besides wasting people's time and their computer disk space, spam can consume large amounts of Internet capacity. If one person sends a useless e-mail to a million people, that unsolicited mail consumes Internet resources for a few moments that would otherwise be available to other users. Spam has always been an annoyance, but in recent years companies are increasingly finding it to be a major problem. In addition to consuming bandwidth on company networks and space on e-mail servers, spam distracts employees who are trying to do their jobs and requires them to spend time deleting the unwanted messages.

NOTES

A considerable number of spam messages include content that is offensive to the recipient. Some companies worry that their employees might sue them, arguing that offensive spam they receive while working contributes to harassment by creating a hostile work environment.

Web Clients and Web Servers

When people use their Internet connections to become part of the Web, their computers become Web client computers on a worldwide client/server network. Client/server architectures are used in LANs, WANs, and the Web. In a client/server architecture, the client computers typically request services, such as printing, information retrieval, and database access, from the server, which processes the clients' requests. The computers that perform the server function usually have more memory and larger, faster disk drives than the client computers they serve.

The Internet connects many different types of computers running different types of operating system software. Because Web software is platform neutral, it lets these computers communicate with each other easily and effectively. This platform neutrality has been (and continues to be) a critical ingredient in the rapid spread and widespread acceptance of the Web. Figure 1.6 shows how the Web's platform neutrality provides multiple interconnections among a wide variety of client and server computers.

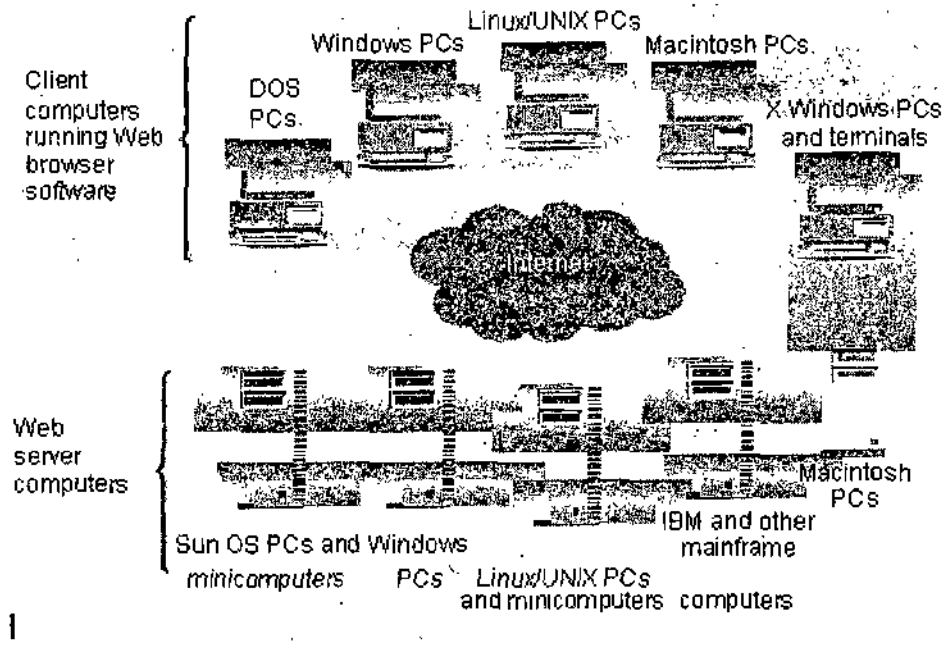


Figure 1.6. *Platform neutrality of the Web.*

NOTES

Various Meanings of "Server"

All computers that are connected to the Internet and contain documents that their owners have made publicly available through their Internet connections are called Web servers.

Unfortunately, the term "server" is used in many different ways by information systems professionals. These multiple uses of the term can be confusing to people who do not have a strong background in computer technology. You are likely to encounter a number of different uses of the word "server."

A **server** is any computer used to provide (or "serve") files or make programs available to other computers connected to it through a network (such as a LAN or a WAN). The software that the server computer uses to make these files and programs available to the other computers is sometimes called **server software**. Sometimes this server software is included as part of the operating system that is running on the server computer. Thus, some information systems professionals informally refer to the operating system software on a server computer as server software, a practice that adds considerable confusion to the use of the term "server."

Some servers are connected through a router to the Internet. these servers can run software, called Web server software, that makes files on those servers available to other computers on the Internet. When a server computer is connected to the Internet and is running Web server software (usually in addition to the server software it runs to serve files to client computers on its own network), it is called a Web server.

SOFTWARE FOR WEB SERVERS

Some Web server software can run on only one computer operating system, while some can run on several operating systems. In this section, you will learn about the operating system software used on most Web servers, the Web server software itself, and other programs, such as Internet utilities and e-mail software, that companies often run on Web servers or other computers as part of electronic commerce operations.

Operating Systems for Web Servers

Operating system tasks include running programs and allocating computer resources such as memory and disk space to programs. Operating system software also provides input and output services to devices connected to the computer, including the keyboard, monitor, and printers. A computer must have an operating system to run programs. For large systems, the operating

NOTES

system has even more responsibilities, including keeping track of multiple users logged on to the system and ensuring that they do not interfere with one another.

Most Web servers run on computers that use one of the following operating systems :

Microsoft Windows NT Server, Microsoft Windows 2000 Server or Server 2003 products, Linux, or one of several UNIX-based operating systems, such as Solaris or FreeBSD. Many companies believe that **Microsoft server products** are simpler for their information systems staff to learn and use than UNIX-based systems. Other companies worry about the security weaknesses caused by the tight integration between application software and the operating system in Microsoft products. UNIX-based Web servers are more popular, and many users believe that UNIX is a more secure operating system on which to run a Web server.

Linux is an open-source operating system that is fast, efficient, and easy to install.

Open-source software is developed by a community of programmers who make the software available for download at no cost. Other programmers then use the software, work with it, and improve it. Those programmers can submit their improved versions of the software back to the community. You can learn more about open-source software at the **Open Source Initiative** Web site.

An increasing number of companies that sell computers intended to be used as Web servers include the Linux operating system in default configurations. Although Linux can be downloaded free from the Web, most companies buy it through a commercial distributor.

These commercial distributions of Linux include useful additional software, such as installation utilities, and a support contract for the operating system. Commercial Linux distributors that sell versions of the operating system with utilities for Web servers include **Caldera**, **Mandrake**, **Red Hat**, and **SuSE**. **Sun Microsystems** sells Web server hardware along with its UNIX-based operating system, **Solaris.**

Web Server Software

This section describes the most commonly used Web server programs today : Apache HTTP Server, Microsoft Internet Information Server (IIS), and Sun Java System Web Server (JSWS) (often called by its former names, Sun ONE, iPlanet Enterprise Server, and Netscape Enterprise Server). These popularity rankings were accumulated through surveys done by **Netcraft**, a networking consulting company in Bath, England, known throughout the world for its Web server survey. Netcraft continually conducts surveys to

tally the number of Web sites in existence and measure the relative popularity of Internet Web server software.

Apache HTTP Server

NOTES

Apache is an ongoing group software development effort. Rob McCool developed Apache while he was working at the University of Illinois at the **NCSA** in 1994. Several Webmasters from around the world created their own extensions to the server and formed an e-mail group so that they could coordinate their changes (known as "patches") to the system. The system consisted of the original core system with a lot of patches—thus, it became known as "a patchy" server, or simply, "Apache." The Apache Web server is currently available on the Web at no cost as open-source software. Apache HTTP Server has dominated the Web since 1996 because it is free and performs very efficiently. It is powerful enough that IBM includes it in its WebSphere application server package. Other Web server products, such as **Zeus**, are based on the Apache open-source code. Currently, Apache is used on 65 to 70 percent of all Web servers, which means it is more widely used than all other Web server software packages combined.

Apache runs on many operating systems (including FreeBSD-UNIX, HP-UX, Linux, Microsoft Windows, SCO-UNIX, and Solaris) and the hardware that supports them Microsoft Internet Information Server **Microsoft Internet Information Server (IIS)** comes bundled with current versions of Microsoft Windows Server operating systems. IIS is used on many corporate intranets because many companies have adopted Microsoft products as their standard products.

Small sites running personal Web pages use IIS, as do some of the largest electronic commerce sites on the Web. Most current surveys estimate that about 20 to 25 percent of all Web servers run some version of IIS. In recent years, the number of Web sites running IIS has been decreasing. Most industry observers believe this decrease has occurred because IIS has been the victim of several well-publicized security breaches. These security breaches allowed Web servers running IIS to be attacked successfully and defaced.

IIS, as a Microsoft product, was originally designed to run only on the Windows NT and Windows 2000 operating systems. It has been released for Microsoft Windows Server 2003 and runs on the Windows XP operating system, but it is not included as a standard part of Windows XP. IIS supports the use of ASP, ActiveX Data Objects, and SQL database queries. IIS also includes the Microsoft FrontPage Web site development tool and other reporting tools. IIS's inclusion of ASP provides an application environment in which HTML pages, ActiveX components, and scripts can be combined to produce dynamic Web pages.

NOTES

Sun Java System Web Server (Sun ONE, iPlanet, Netscape)

A descendant of the original NCSA Web server program, Sun Java System Web Server (JSWS) was formerly sold under the names Sun ONE, Netscape Enterprise Server, and iPlanet Enterprise Server. When AOL (now Time Warner) purchased Netscape in 1999, the company formed a partnership with Sun Microsystems to support and continue to develop Netscape server products. This partnership was named iPlanet and was operated under a three-year agreement that expired in March 2002. When the partnership ended, iPlanet became a part of Sun because the Web server and electronic commerce software that iPlanet sells are more closely related to Sun's businesses than to Time Warner's businesses.

Sun JSWS is not free, but its licensing fee is reasonable. The fee varies with the processing power of the server on which it is installed, but most Web sites pay between $1400 and $5000 for their licenses. The Sun software runs on many operating systems, including HP-UX, Solaris, and Windows. According to recent estimates, Sun JSWS runs on about 1 percent of all Web servers. However, some of the busiest and best-known sites on the Internet, including BMW, Dilbert, E*TRADE, Excite, Lycos, and Schwab, run (or have run some version of Sun JSWS. Reports from consulting firms such as Gartner, Inc. show that Sun JSWS is in use at more than 40 percent of all public Web sites and at more than 60 percent of the top 100 enterprise Web sites.

Like most other server programs, Sun JSWS supports dynamic application develop ment for server-side applications. Sun JSWS provides connectivity to a number of database products as well.

MARKUP LANGUAGES AND THE WEB

Web pages can include many elements, such as graphics, photographs, sound clips, and even small programs that run in the Web browser. Each of these elements is stored on the Web server as a separate file. The most important parts of a Web page, however, are the structure of the page and the text that makes up the main part of the page. The page structure and text are stored in a text file that is formatted, or marked up, using a text markup language. A **text markup language** specifies a set of tags that are inserted into the text.

These **markup tags**, also called **tags**, provide formatting instructions that Web client software can understand. The Web client software uses those instructions as it renders the text and page elements contained in the other files into the Web page that appears on the screen of the client computer.

NOTES

The markup language most commonly used on the Web is HTML, which is a subset of a much older and far more complex text markup language called **Standard Generalized Markup Language (SGML)**. Figure 1.7 shows how HTML, XML, and XHTML have descended from the original SGML specification. SGML was used for many years by the publishing industry to create documents that needed to be printed in various formats and that were revised frequently. In addition to its role as a markup language, SGML is a **meta language**, which is a language that can be used to define other languages. Another markup language that was derived from SGML for use on the Web is **Extensible Markup Language (XML)**, which is increasingly used to mark up information that companies share with each other over the Internet. XML is also a meta language because users can create their own markup elements that extend the usefulness of XML (which is why it is called an "extensible" language).

The **World Wide Web Consortium (W3C)**, a not-for-profit group that maintains standards for the Web, presented its first draft form of XML in 1996; the W3C issued its first formal version recommendation in 1998. Thus, it is a much newer markup language than HTML. In 2000, the W3C released the first version of a recommendation for a new markup language called **Extensible Hypertext Markup Language (XHTML)**, which is a reformulation of HTML version 4.0 as an XML application. The Online Companion includes a link to the **W3C XHTML Version 1.0 Specification.**

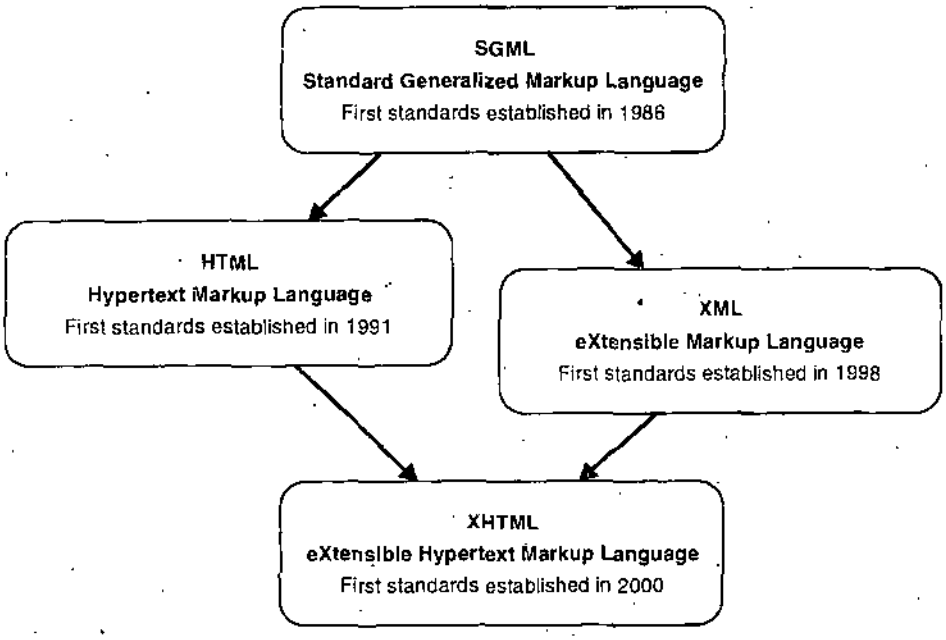


Figure 1.7. *Development of markup languages*

NOTES

Standard Generalized Markup Language

Since the 1960s, publishers have used markup languages to create documents that can be formatted once, stored electronically, and then printed many times in various layouts that each interpret the formatting differently. U.S. Department of Defense contractors also used early markup languages to create manuals and parts lists for weapons systems. These documents contained many information elements that were often reprinted in different versions and formats. Using electronic document storage and programs that could interpret the formats to produce different layouts saved a tremendous amount of retyping time and cost.

A **Generalized Markup Language (GML)** emerged from these early efforts to create standard formatting styles for electronic documents. In 1986, after many elements of the standard had been in use for years, the **International Organization for Standardization (ISO)** adopted a version of GML called Standard Generalized Markup Language (SGML). SGML offers a system of marking up documents that is independent of any software application. Many organizations, such as the Association of American Publishers, Hewlett-Packard, and Kodak, use SGML because they have complex document management requirements.

SGML is nonproprietary and platform independent and offers user-defined tags. However, it is not well suited to certain tasks, such as the rapid development of Web pages.

SGML is costly to set up and maintain, requires the use of expensive software tools, and is hard to learn. Creating document-type definitions in SGML can be expensive and time consuming.

Hypertext Markup Language

HTML includes tags that define the format and style of text elements in an electronic document. HTML also has tags that can create relationships among text elements within one document or among several documents. The text elements that are related to each other are called **hypertext elements.**

HTML is easier to learn and use than SGML. HTML is the prevalent markup language used to create documents on the Web today. The early versions of HTML let Web page designers create text-based electronic documents with headings, title bar titles, bullets, lines, and ordered lists. As the use of HTML and the Web itself grew, HTML creator Berners-Lee turned over the job of maintaining versions of HTML to the W3C. Later versions of HTML included tags for tables, frames, and other features that helped Web designers create more complex page layouts. The W3C maintains detailed information about HTML versions and related topics on its **W3C HTML Page.**

NOTES

The process for approval of new HTML features takes a long time, so Web browser software developers created some features, called **HTML extensions**, that would only work in their browsers. At various times during the history of HTML, both Microsoft and Netscape enabled their Web browsers to use these HTML extension tags before those tags were approved by the W3C. In some cases, these tags were enabled in one browser and not the other. In other cases, the tags used were never approved by the W3C or were approved in a different form than the one implemented in the Web browser software. Web page designers who wanted to use the latest available tags were often frustrated by this state of affairs. Many of these Web designers had to create separate sets of Web pages for the different types of browsers, which was inefficient and expensive. Most of these tag difference issues were resolved when the W3C issued the specification for HTML version 4.0 in 1997, although enough of them remain to cause regular problems for Web designers.

HTML Tags

An HTML document contains document text and elements. The tags in an HTML document are interpreted by the Web browser and used by it to format the display of the text enclosed by the tags. In HTML, the tags are enclosed in angle brackets (<>). Most HTML tags have an **opening tag** and a **closing tag** that format the text between them. The closing tag is preceded by a slash within the angle brackets. The general form of an HTML element is :

<tagname properties> Displayed information affected by tag </tagname>

Two good examples of HTML tag pairs are the boldface character-formatting tags and the italic character-formatting tags. For example, a Web browser reading the following line of text :

<B>A Review of the Book <I>HTML Is Fun!</I></B>

would recognize the <B> and </B> tags as instructions to display the entire line of text in bold and the <I> and </I> tags as instructions to display the text enclosed by those tags in italics. The Web browser would display the text as :

A Review of the Book *HTML Is Fun!*

Some Web browsers allow the user to customize the interpretations of the tags, so that different Web browsers might display the tagged text differently. For example, one Web browser might display text enclosed by bold tags in a blue color instead of displaying the text as bold. Tags can be written in either lowercase or uppercase letters; the tag <b> has the exact same meaning as the tag <B>. Although most tags are two-sided (they use both an opening and a closing tag), some are not. Tags that only require opening tags are

NOTES

known as one-sided tags. The tag that creates a line break (</br>) is a common one-sided tag. Some tags, such as the paragraph tag (...), are two-sided tags for which the closing tag is optional. Designers often omit the optional closing tags, although many Web designers argue that this practice is poor markup style.

In a two-sided tag set, the closing tag position is very important. For example, if you were to omit the closing bold tag in the preceding example, any text that followed the line would be bolded. Sometimes an opening tag contains one or more property modifiers that further refine how the tag operates. A tag's property may modify a text display, or it may designate where to find a graphic element. Figure 1.8 shows some sample text marked up with HTML tags and Figure 1.9 shows this text as it appears in a Web browser. The tags in these two figures are among the most common HTML tags in use today on the Web.

Other frequently used HTML tags (not shown in the figures) let Web designers include graphics on Web pages and format text in the form of tables. The text and HTML tags that form a Web page can be viewed when the page is open in a Web browser by using the menu commands View, Source (in Internet Explorer) or View, Page Source (in Netscape Navigator). A number of good Web sources (such as the **W3C Getting Started with HTML** page) and textbooks are available that describe HTML tags and their uses, and you may wish to consult them for an in-depth look at HTML.

```
<html>
    <head>
        <title>HTML Tag Examples</title>
    </head>
    <body>
        <h1>This text is set in Heading One tags</h1>
        <h2>This text is set in Heading Two tags</h2>
        <h3>This text is set in Heading Three tags</h3>

        <p>
        This text is set within Paragraph tags. It will appear
        as one paragraph; the text will wrap at the end of each
        line that is rendered in the web browser no matter where
        the typed text ends. The text inside paragraph tags is
        rendered without regard to extra spaces typed in the text,
        such as these :          character formatting can also
        be applield within Paragraph tags. For example, <b>this
        text is set in bold</b>, <font face="Arial">this text is
        set in Arial</font>, and <i>this text is set in italics</i>.
        </p>

        <pre>
The preformatted tag instructs the web browser to render the text
    exatly the way it is typed,
as in this example.
```

NOTES

```
</pre>

<p>
HTML includes tags that instruct the web browser to place
text in bulleted or numbered lists :
</p>

<ul>
    <li>Bulleted list item one</li>
    <li>Bulleted list item two</li>
    <li>Bulleted list item three</li>
</ul>

<ol>
    <li>Numbered list item one</li>
    <li>Numbered list item two</li>
    <li>Numbered list item three</li>
</ol>

<p>
HTML also includes tags for left, center, and right justification :
</p>

<div align="left">Text aligned left</div>
<div align="center">Text aligned center</div>
<div align="right">Text aligned right</div>

<p>
The most important tag in HTML is the Anchor Hypertext
Reference tag, which is the tag that provides a link to
another web page (or another location in the same web page).
For example, the underlined text
<a href="http://www.course.com/">Course Technology</a>
is a hyperlink to the web page of the publisher of this book.
</p>

  </body>

</html>
```

Figure 1.8. *Text marked up with HTML tags.*

This text is set in Heading One tags

This text is set in Heading Two tags

This text is set in Heading Three tags

This text is set within Paragraph tags. It will appear as one paragraph, the text will wrap at the end of each line that is rendered in the Web browser no matter where the typed text ends. The text inside Paragraph tags *is rendered without regard to extra* spaces typed in the text, such as these Character formatting can also be applied within Paragraph tags. For example, **this text is set in bold**, this text is set in Arial, and *this text is set in italics.*

The Preformatted tag instructs the Web browser to render the text
    exactly the way it is typed,
as in this example.

HTML includes tags that instruct the Web browser to place text in bulleted or numbered lists :

NOTES

- Bulleted list item one
- Bulleted list item two
- Bulleted list item three

1. Numbered list item one
2. Numbered list item two
3. Numbered list item three

HTML also includes tags for left, center and right justification

Text aligned left

Text aliged center

Text aliged right

The most important tag in HTML is the Anchor Hypertext Reference tag, which is the tag that provides a link to another Web page (or another location in the same Web page). For example, the underlined text Course Technology is a hyperlink to the Web page of the publisher of this book.

Figure 1.9. *Text marked up with HTML tags as it appears in a Web browser.*

HTML Links

The Web organizes interlinked pages of information residing on sites around the world. Hyperlinks on Web pages form a "web" of those pages. A user can traverse the interwoven pages by clicking hyperlinked text on one page to move to another page in the web of pages.

Users can read Web pages in serial order or in whatever order they prefer by following hyperlinks.

An electronic commerce Web site can use links to direct customers to pages on the company's Web server. The way links lead customers through pages can affect the usefulness of the site and can play a major role in shaping customers' impressions of the company. Two commonly used link structures are linear and hierarchical. A **linear hyperlink structure** resembles conventional paper documents in that the reader begins on the first page and clicks the Next button to move to the next page in a serial fashion. This structure works well when customers fill out forms prior to a purchase or other agreement. In this case, the customer reads and responds to page one, and then moves on to the next page. This process continues until the entire form is completed. The only Web page navigation choices the user typically has are Back and Continue.

Another link arrangement is called a hierarchical structure. In a **hierarchical hyperlink structure**, the Web user opens an introductory page called a **home page** or **start page**. This page contains one or more links to other pages, and those pages, in turn, link to other pages. This hierarchical arrangement resembles an inverted tree in which the root is at the top and the branches are below it. Hierarchical structures are good for leading

NOTES

customers from general topics or products to specific product models and quantities. A company's home page might contain links to help, company history, company officers, order processing, frequently asked questions, and product catalogs. Many sites that use a hierarchical structure include a page on the Web site that contains a map or listing of the Web pages in their hierarchical order. This page is called a **site map**. Figure 1.10 illustrates the linear and hierarchical structures. Of course, pages combining linear and hierarchical structures are also possible.

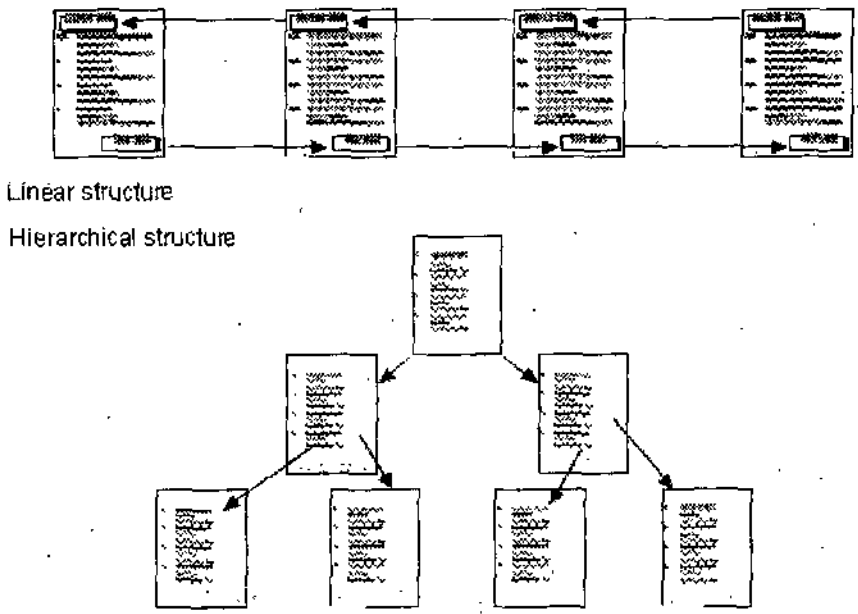


Figure 1.10. *Two alternative hyperlink structures.*

In HTML, hyperlinks are created using the HTML **anchor tag.** Whether you are linking to text within the same document or to a document on a distant computer, the anchor tag has the same basic form :

<A HREF="address">Visible link text</A>

Anchor tags have opening and closing tags. The opening tag has a hypertext reference (HREF) property, which specifies the remote or local document's address. Clicking the text following the opening link transfers control to the HREF address, wherever that happens to be. A person creating an electronic resume on the Web might want to make a university's name and address under the Education heading a hyperlink instead of plain text.

Anyone viewing the résumé can click the link, which leads the reader to the university's home page. The following example shows the HTML code to create a hyperlink to another Web server :

<A HREF="http ://www.sandiego.edu">University of San Diego</A>

NOTES

Similarly, the résumé could include a local link to another part of the same document with the following marked up text :

<A HREF="#references">References are found here</A>

In both of these examples, the text between the anchors appears on the Web page as a hyperlink. Most browsers display the link in blue and underline it. In most browser software, the action of moving the mouse pointer over a hyperlink causes the mouse pointer to change from an arrow to a pointing hand.

Scripting Languages and Style Sheets

Versions of HTML released by the W3C after 1997 include an HTML tag called the object tag and include support for cascading style sheets. Web designers can use the object tag to embed scripting language code on HTML pages. The most common scripting languages used on Web pages are JavaScript, JScript, Perl, and VBScript. Scripts written in these languages and embedded on Web pages can execute programs on computers that display those pages.

Cascading style sheets (CSS) are sets of instructions that give Web developers more control over the format of displayed pages. Similar to document styles in word-processing programs, CSS let designers define formatting styles that can be applied to multiple Web pages. The set of instructions, called a **style sheet**, is usually stored in a separate file and is referenced using the HTML style tag; however, it can be included as part of a Web page's HTML file. The term cascading means that designers can apply many style sheets to the same Web page, one on top of the other. For example, a three-stage cascade might include one style sheet with formatting instructions for text within heading 1 tags, a second style sheet with formatting instructions for text within heading 2 tags, and a third style sheet with formatting instructions for text within paragraph tags. A designer who later decides to change the formatting of heading 2 text can just replace the second style sheet with a different one.

```
<html>
    <head>
        <title>Countried</title>
    </head>
    <body>
        <h1>Countries</h1>
        <h2>CountryName</h2>
        <h3>CapitalCity</h3>
```

NOTES

```
    <h4>AreaInSquareKilometers</h4>
    <h5>OfficialLanguage</h5>
    <h6>VotingAge</h6>

    <h2>Argentina</h2>
    <h3>Buenos Aires</h3>
    <h4>2,766,890</h4>
    <h5>Spanish</h5>
    <h6>18</h6>

    <h2>Austria</h2>
    <h3>Vienna</h3>
    <h4>83,858</h4>
    <h5>German</h5>
    <h6>19</h6>

    <h2>Barbados</h2>
    <h3>Bridgetown</h3>
    <h4>430</h4>
    <h5>English</h5>
    <h6>18</h6>

    <h2>Belarus</h2>
    <h3>Minsk</h3>
    <h4>207,600</h4>
    <h5>Byelorussian</h5>
    <h6>18<h6>

  </body>

</html>
```

Figure 1.11. *Country list data marked up with HTML tags.*

Extensible Markup Language (XML)

As the Web grew, HTML continued to provide a useful tool for Web designers who wanted to create attractive layouts of text and graphics on their pages. However, as companies began to conduct electronic commerce on the Web, the need to present large amounts of data on Web pages also became important. Companies created Web sites that contained lists of inventory items, sales invoices, purchase orders, and other business data. The need to keep these lists updated was also important and posed a new challenge for many Web designers. The tool that had helped these Web designers create useful Web pages, HTML, was not such a good tool for presenting or maintaining information lists.In the late 1990s, companies began turning to XML to help them maintain Web pages that contained large amounts of data. XML uses paired start and stop tags in much the same way as database software defines a record structure. For example, a company that sells products on the Web might have Web pages that contain descriptions and photos of the products it sells. The Web pages are marked up with HTML tags, but the product information elements themselves, such as prices, identification numbers, and quantities on hand, are marked up with XML tags. The XML document is embedded within the HTML document.

NOTES

XML includes data management capabilities that HTML cannot provide. To better understand the strengths of XML and weaknesses of HTML in data management tasks, consider the simple example of a Web page that includes a list of countries and some basic information about each country. A Web designer might decide to use HTML tags to show each information item the same way for each country. Each information item would use a different tag. Assume that the Web designer in this case decided to use the HTML heading tags to present the data. Figure 1.12 shows the data and the HTML heading tags for four countries (this is only an example; the actual list would include more than 150 countries).

The first item in the list provides the definitions for each tag. Figure 1.12 shows this HTML document as it appears in a Web browser.

Countries

CountryName

CapitalCity

AreaInSquareKilometers

OfficialLanguage

VotingAge

Argentina

Buenos Aires

2,766,890

Spanish

18

Austria

Vienna

83,858

German

19

Barbados

Bridgetown

NOTES

430

English

18

Belarus

Minsk

207,600

Byelorussian

18

Figure 1.12. *Country list data as it appears in a Web browser.*

These figures reveal some of the shortcomings of using HTML to present a list of items when the meaning of each item in the list is important. The Web designer in this case used HTML heading tags. HTML has only six levels of heading tags; thus, if the individual items had any more information elements than shown in this example (such as population and continent), this approach would not work at all. The Web designer could use various combinations of text attributes such as size, font, color, bold, or italics to distinguish among items, but none of these tags would convey the meaning of the individual data elements.

The only information about the meaning of each country's listing appears in the first list item, which includes the definitions for each element. In the late 1990s, Web profession also began to consider XML as a list-formatting alternative to HTML that would more effectively communicate the meaning of data. XML differs from HTML in two important respects. First, XML is not a markup language with defined tags. It is a framework within which individuals, companies, and other organizations can create their own sets of tags. Second, XML tags do not specify how text appears on a Web page; the tags convey the meaning (the semantics) of the information included within them. To understand this distinction between appearance and semantics, consider the list of countries example again. In XML, tags can be created for each fact that define the meaning of the fact. Figure 1.12 shows the countries data marked up with XML tags. Some browsers, such as Internet Explorer, can render XML files directly without additional instructions. Figure 1.13 shows the country list XML file as it would appear in an Internet Explorer browser window.

NOTES

```
<?xml version="1.0"?>

<CountriesList>

    <Country Name = "Argentina">
        <CapitalCity>Buenos Aires</CapitalCity>
        <AreaInSquareKilometers>2,766,890</AreaInSquareKilometers>
        <OfficialLanguage>Spanish</OfficialLanguage>
        <VotingAge>18</VotingAge>
    </Country>

    <Country Name = "Austria">
        <CapitalCity>Vienna</CapitalCity>
        <AreaInSquareKilometers>83,858</AreaInSquareKilometers>
        <OfficialLanguage>German</OfficialLanguage>
        <VotingAge>19</VotingAge>
    </Country>

    <Country Name = "Barbados">
        <CapitalCity>Bridgetowns</CapitalCity>
        <AreaInSquareKilometers>430</AreaInSquareKilometers>
        <OfficialLanguage>English</OfficialLanguage>
        <VotingAge>18</VotingAge>
    </Country>

    <Country Name = "Belarus">
        <CapitalCity>Minsk</CapitalCity>
        <AreaInSquareKilometers>207,600</AreaInSquareKilometers>
        <OfficialLanguage>Byeiorussian</OfficialLanguage>
        <VotingAge>18</VotingAge>
    </Country>

</CountriesList>
```

Figure 1.13. *Country list data marked up with XML tags.*

```
<?xml version="1.0"?>
- <CountriesList>
  - <CountryName="Argentina">
      <CapitalCity>BuenosAires</CapitalCity>
      <AreaInSquareKilometers>2,766,890</AreaInSquareKilometers>
      <OfficialLanguage>Spanish</OfficialLanguage>
      <VotingAge>18</VotingAge>
    </Country>
  - <CountryName="Austria">
      <CapitalCity>Vienna</CapitalCity>
      <AreaInSquareKilometers>83,858</AreaInSquareKilometers>
      <OfficialLanguage>German</OfficialLanguage>
      <VotingAge>19</VotingAge>
    </Country>
  - <CountryName="Barbados">
      <CapitalCity>Bridgetown</CapitalCity>
      <AreaInAquareKilometers>430</AreaInSquareKilometers>
      <OfficialLanguage>English</OfficialLanguage>
      <VotingAge>18</VotingAge>
    </Country>
```

```
- <CountryName="Belarus">
    <CapitalCity>Minsk</CapitalCity>
    <AreaInSquareKilometers>207,600</AreaInSquareKilometers>
    <OfficialLanguage>Byelorussian</OfficialLanguage>
    <VotingAge>18</VotingAge>
  </Country>
</CountriesList>
```

Figure 1.14. *Country list data marked up with XML tags as it would appear in Internet Explorer.*

The first line in the XML file shown in Figures 1.13 and 1.14 is the declaration, which indicates that the file uses version 1.0 of XML. XML markup tags are similar in appearance to SGML markup tags, thus the declaration can help avoid confusion in organizations that use both. The second line and the last line are the root element tags. The root element of an XML file contains all of the other elements in that file and is usually assigned a name that describes the purpose or meaning of the file. The other elements are called child elements; for example, Country is a child element of CountriesList. Each of the other attributes is, in turn, a child element of the Country element. The names of these child elements were created specifically for use in this file.

If programmers in another organization were to create a file with country information,they might use different names for these elements (for example, "Capital" instead of "CapitalCity"), which would make it difficult for the two organizations to share information.

Thus, the greatest strength of XML, that it allows users to define their own tags, is also its greatest weakness.

To overcome that weakness, many companies have agreed to follow common standards for XML tags. These standards, in the form of data type definitions (DTDs) or XML schemas, are available for a number of industries, including the **ebXML** initiative for electronic commerce standards, the **eXtensible Business Reporting Language (XBRL)** for accounting and financial information standards, **LegalXML** for information in the legal profession, and **MathML** for mathematical and scientific information. A number of industry groups have formed to create standard XML tag definitions that can be used by all companies in that industry. **RosettaNet** is an example of such an industry group. In 2001 the W3C released a set of rules for XML document interoperability that many researchers believe will help resolve incompatibilities between different sets of XML tag definitions. A set of XML tag definitions is sometimes called an **XML vocabulary**. Hundreds of publicly defined XML vocabularies are currently circulating, many of which are registered with the **XML Registry**. You can learn more about XML by reading the **W3C XML Pages.**

NOTES

Although it is possible to display XML files in some Web browsers, XML files are not intended to be displayed in a Web browser. XML files are intended to be translated using another file that contains formatting instructions or to be read by a program. Formatting instructions are often written in the **Extensible Stylesheet Language (XSL)**, and the programs that read or transform XML files are usually written in the Java programming language. These programs, sometimes called **XML parsers**, can format an XML file so it can appear on the screen of a computer, a wireless PDA, a mobile phone, or some other device.

A diagram showing one way that a Web server might process an HTTP request for an XML page appears in Figure 1.15.

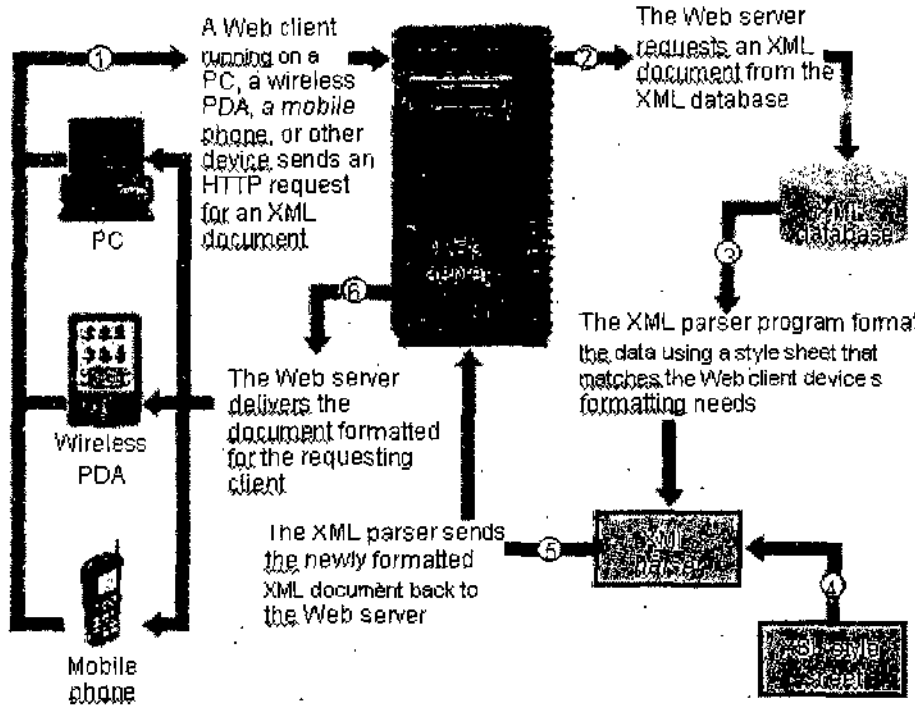


Figure 1.15. *Processing a request for an XML page.*

HTML and XML Editors

Web designers can create HTML documents in any general-purpose text editor or word processor. However, one of the special-purpose HTML editors can help Web designers create Web pages much more easily. There are many freeware, shareware, and commercial HTML editors available for download on the Internet, including CoffeeCup, HomeSite, and CuteHTML. HTML editors are also included as part of more sophisticated Web site design and creation programs that are sometimes called Web page builder software. With these programs, Web designers can create and manage complete Web sites, including features for database access, graphics, and

NOTES

fill-in forms. These programs display the Web page as it will appear in a Web browser in one window and display the HTML-tagged text in another window. The designer can edit in either window and changes are reflected in the other window. For example, the designer can drag and drop objects such as graphics onto the Web browser view page and the program automatically generates the HTML tags to position the graphics.

Web site design and creation software also provides maintenance tools that allow the designer to create a Web site on a PC and then upload the entire site (HTML documents, graphics files, and so on) to a Web server computer. When the site needs to be edited later, the designer can edit the copy of the site on the PC and instruct the program to synchronize those changes on the copy of the site that resides on the Web server. Examples of Web site design and creation programs include **Microsoft FrontPage** and **Macromedia Dreamweaver.**

XML files, like HTML files, can be created in any text editor. However, programs designed to make the task of designing and managing XML files easier are also available. These programs include Epic Editor, TurboXML, XMetal, and XML Spy. These programs provide tag validation and XML creation capabilities in addition to making the job of marking up text with XML tags more efficient.

STUDENT ACTIVITY

1. Explain the web client and web servers.

2. Write short notes on HTML.

NOTES

SUMMARY

- In this unit you learned about the history of the Internet and the Web, including how these technologies emerged from research projects and grew to be the supporting infrastructure for electronic commerce today. You also learned about the protocols, programs, languages, and architectures that support the Internet and the World Wide Web. TCP/IP is the protocol suite used to create and transport information packets across the Internet. IP addresses identify computers on the Internet. Domain names such as www.amazon.com also identify computers on the Internet, but those names are translated into IP addresses by the routing computers on the Internet. HTTP is the set of rules for transferring Web pages and requests for those Web pages on the Internet. POP, SMTP, and IMAP are protocols that help manage e-mail. Unsolicited commercial e-mail (or spam) has become a major irritation for internet users.
- Hypertext Markup Language, or HTML, was derived from the more generic meta language SGML. HTML defines the structure and content of Web pages using markup symbols called tags. Over time, HTML has evolved to include a large number of tags that accommodate graphics, Cascading Style Sheets, and other Web page elements. Hyperlinks are HTML tags that contain a URL. The URL can be a local or remote computer. The better HTML editors facilitate Web page construction with helpful tools and drag-and-drop capabilities.
- Extensible Markup Language, or XML, is also derived from SGML. However, unlike HTML, XML uses markup tags to describe the meaning, or semantics, of the text, rather than its display characteristics. XML offers businesses hope for a common language that they will be able to use to describe products, services, and even business processes to each other in common, shared databases. XML could help companies dramatically reduce the costs of handling inter company information flows.

SELF ASSESSMENT QUESTIONS

1. What were the main forces that led to the commercialization of the Internet ? Summarize your answer in about 100 words.
2. Describe in two paragraphs the origins of HTML. Explain how markup tags work in HTML, and describe the role of at least one person involved with HTML's development.

NOTES

3. In about 200 words, compare the POP e-mail protocol to the IMAP e-mail protocol. Describe situations in which you would prefer to use one protocol or the other and explain the reasons for your preference.
4. In about 400 words, describe the similarities and differences between XML and HTML. Provide examples of at least two situations in which you would use XML and two situations in which you would use HTML.

SECTION B

NOTES

UNIT 2 SECURITY ISSUES

★ LEARNING OBJECTIVES ★

- Introduction
- Security for Client Computers
- Communication Channel Security
- Security for Server Computers
- Organizations that Promote Computer Security

INTRODUCTION

In the early days of the Internet, one of its most popular uses was electronic mail. Despite e-mail's popularity, people have often worried that a business rival might intercept e-mail messages for competitive gain. Another fear was that employees' nonbusiness correspondence might be read by their supervisors, with negative repercussions. These were significant and realistic concerns.

Today, the stakes are much higher. The consequences of a competitor having unauthorized access to messages and digital intelligence are now far more serious than in the past. Electronic commerce, in particular, makes security a concern for all users. A typical worry of Web shoppers is that their credit card numbers might be exposed to millions of people as the information travels across the Internet. Recent surveys show that more than 80 percent of all Internet users have at least "some concern" about the security of their credit card numbers in electronic commerce transactions. This shows the fear shoppers have expressed for many years about credit card purchases over the phone.

Consumers are now more comfortable giving their credit card numbers and other information over the phone, but many of those same people fear providing that same information on a Web site. people are concerned about personal information they provide to companies over the Internet.

NOTES

Increasingly, people doubt that these companies have the willingness and the ability to keep customers' personal information confidential. This unit examines security in the context of electronic commerce, presenting an introduction to important security problems and some solutions to those problems.

Computer security is the protection of assets from unauthorized access, use, alteration, or destruction. There are two general types of security : physical and logical. **Physical security** includes tangible protection devices, such as alarms, guards, fireproof doors, security fences, safes or vaults, and bombproof buildings. Protection of assets using nonphysical means is called **logical security**. Any act or object that poses a danger to computer assets is known as a **threat.**

Managing Risk

Countermeasure is the general name for a procedure, either physical or logical, that recognizes, reduces, or eliminates a threat. The extent and expense of countermeasures can vary, depending on the importance of the asset at risk. Threats that are deemed low risk and unlikely to occur can be ignored when the cost to protect against the threat exceeds the value of the protected asset. For example, it would make sense to protect from tornadoes a computer network in Oklahoma City, where there is significant and regular tornado activity, but not to protect a similar network in Los Angeles, where tornadoes are rare. The risk management model shown in Figure 2.1 illustrates four general actions that an organization could take, depending on the impact (cost) and the probability of the physical threat. In this model, a tornado in Oklahoma would be in quadrant II, whereas a tornado in Southern California would be in quadrant IV.

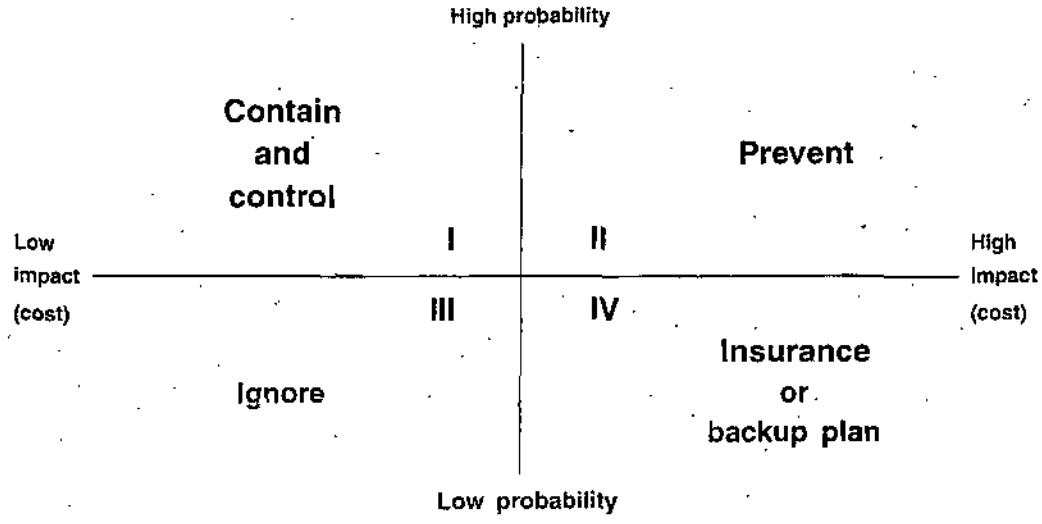


Figure 2.1. *Risk management model.*

NOTES

The same sort of risk management model applies to protecting Internet and electronic commerce assets from both physical and electronic threats. Examples of the latter include impostors, eavesdroppers, and thieves. An **eavesdropper**, in this context, is a person or device that can listen in on and copy Internet transmissions. People who write programs or manipulate technologies to obtain unauthorized access to computers and networks are called **crackers or hackers.**

A cracker is a technologically skilled person who uses their skills to obtain unauthorized entry into computers or network systems—usually with the intent of stealing information or damaging the information, the system's software, or even the system's hardware. Originally, the term hacker was used to describe a dedicated programmer who enjoyed writing complex code that tested the limits of technology. Although the term hacker is still used in a positive way—even as a compliment—by computer professionals (who make a strong distinction between the terms hacker and cracker), the media and the general public usually use the term to describe those who use their skills for ill purposes. Some IT people also use the terms **white hat hacker** and **black hat hacker** to make the distinction between good hackers and bad hackers.

To implement a good security scheme, organizations must identify risks, determine how to protect threatened assets, and calculate how much to spend to protect those assets. In this chapter, the primary focus in risk management protection is on the central issues of identifying the threats and determining the ways to protect assets from those threats, rather than on the protection costs or value of assets.

Computer Security Classifications

Computer security is generally classified into three categories : secrecy, integrity, and necessity (also known as denial of service). **Secrecy** refers to protecting against unauthorized data disclosure and ensuring the authenticity of the data source. **Integrity** refers to preventing unauthorized data modification. **Necessity** refers to preventing data delays or denials (removal). Secrecy is the best known of the computer security categories. Every month, newspapers report on break-ins to government computers or theft of stolen credit card numbers that are used to order goods and services. Integrity threats are reported less frequently and, thus, may be less familiar to the public. For example, an integrity violation occurs when an Internet e-mail message is intercepted and its contents are changed before it is forwarded to its original destination. In this type of integrity violation, which is called a **man-in-the-middle exploit**, the contents of the e-mail are often changed in a way that negates the message's original meaning. Necessity violations take several forms, and they occur relatively frequently. Delaying a message or completely destroying it can have grave consequences. Suppose that a

NOTES

message sent at 10 :00 a.m. to an online stockbroker includes an order to purchase 1000 shares of IBM at market price. If the stockbroker does not receive the message (because an attacker delays it) until 2 :30 p.m. and IBM's stock price has increased by $3, the buyer loses $3000.

Security Policy and Integrated Security

Any organization concerned about protecting its electronic commerce assets should have a **security policy** in place. A security policy is a written statement describing which assets to protect and why they are being protected, who is responsible for that protection, and which behaviors are acceptable and which are not. The policy primarily addresses physical security, network security, access authorizations, virus protection, and disaster recovery. The policy develops over time and is a living document that the company and security officer must review and update at regular intervals.

Both defense and commercial security guidelines state that organizations must protect assets from unauthorized disclosure, modification, or destruction. However, military security policy differs from commercial policy because military applications stress separation of multiple levels of security. Corporate information is usually classified as either "public" or "company confidential." The typical security policy concerning confidential company information is straightforward : Do not reveal company confidential information to anyone outside the company.

The first step an organization must take in creating a security policy is to determine which assets to protect from which threats. For example, a company that stores its customers' credit card numbers might decide that those numbers are an asset that must be protected from eavesdroppers. Then, the organization must determine who should have access to various parts of the system. Next, the organization determines what resources are available to protect the assets identified. Using the information it has acquired, the organization develops a written security policy. Finally, the organization commits resources to building or buying software, hardware, and physical barriers that implement the security policy. For example, if a security policy disallows any unauthorized access to customer information, including credit card numbers and credit history, then the organization must either create or purchase software that guarantees end-to-end secrecy for electronic commerce customers.

A comprehensive plan for security should protect a system's privacy, integrity, and availability (necessity), and authenticate users. When these goals are used to create a security policy for an electronic commerce operation, they should be selected to satisfy the list of requirements. These requirements provide a minimum level of acceptable security for most electronic commerce operations.

NOTES

The Network Security Library, which is sponsored by GFI Software (a company that sells security and messaging software), is a good source for information about security policies. The Network Security Library includes a number of white papers that provide guidance on how to craft a workable security policy. **Information Security Policy World** is another Web site that provides information about security policy matters.

Although absolute security is difficult to achieve, organizations can create enough barriers to deter most intentional violators. With good planning, organizations can also reduce the impact of natural disasters or terrorist acts. Integrated security means having all security measures working together to prevent unauthorized disclosure, destruction, or modification of assets. A security policy covers many security concerns that must be addressed by a comprehensive and integrated security plan. Specific elements of a security policy address the following points :

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

In this unit, you will explore these security policy issues with a focus on how they apply to electronic commerce in particular. The electronic commerce security topics in this unit are organized to follow the transaction processing flow, beginning with the consumer and ending with the Web server (or servers) at the electronic commerce site. Each logical link in the process includes assets that must be protected to ensure security : client computers, the communication channel on which the messages travel, and the Web servers, including any other computers connected to the Web servers.

SECURITY FOR CLIENT COMPUTERS

Client computers, usually PCs, must be protected from threats that originate in software and data that are downloaded to the client computer from the Internet. In this section, you will learn that active content delivered over the Internet in dynamic Web pages can be harmful. Another threat to client computers can arise when a malevolent server site masquerades as a legitimate Web site. Users and their client computers can be duped into revealing information to those Web sites. This section explains these threats, describes how they work, and outlines some protection mechanisms that can prevent or reduce the threats they pose to client computers.

NOTES

Cookies

The Internet provides a type of connection between Web clients and servers called a stateless connection. In a **stateless connection**, each transmission of information is independent; that is, no continuous connection (also called an **open session**) is maintained between any client and server on the Internet. Cookies are small text files that Web servers place on Web client computers to identify returning visitors. Cookies also allow Web servers to maintain continuing open sessions with Web clients. An open session is necessary to do a number of things that are important in online business activity. For example, shopping cart and payment processing software both need an open session to work properly. Early in the history of the Web, cookies were devised as a way to maintain an open session despite the stateless nature of Internet connections. Thus, cookies were invented to solve the stateless connection problem by saving information about a Web user from one set of server-client message exchanges to another.

There are two ways of categorizing cookies : by time duration and by source. The two kinds of time duration cookie categories include **session cookies**, which exist until the Web client ends the connection (or "session"), and **persistent cookies**, which remain on the client computer indefinitely. Electronic commerce sites use both kinds of cookies. For example, a session cookie might contain information about a particular shopping visit and a persistent cookie might contain login information that can help the Web site recognize visitors when they return to the site on subsequent visits. Each time a browser moves to a different part of a merchant's Web site, the merchant's Web server asks the visitor's computer to send back any cookies that the Web server stored previously on the visitor's computer.

Another way of categorizing cookies is by their source. Cookies can be placed on the client computer by the Web server site, in which case they are called **first-party cookies**, or they can be placed by a different Web site, in which case they are called **third-party cookies**. A third-party cookie originates on a Web site other than the site being visited. These third-party Web sites usually provide advertising or other content that appears on the Web site being viewed. The third-party Web site providing the advertising is often interested in tracking responses to their ads by visitors who have already seen the ads on other sites. If the advertising Web site places its ads on a large number of Web sites, it can use persistent third-party cookies to track visitors from one site to another. Earlier in this book, you learned about DoubleClick and similar online ad placement services that perform this function.

The most complete way for Web site visitors to protect themselves from revealing private information or being tracked by cookies is to disable cookies entirely. The problem with this approach is that useful cookies are blocked

NOTES

along with the others, requiring visitors to enter information each time they revisit a Web site. The full resources of some sites are not available to visitors unless their browsers are set to allow cookies. For example, most distance learning software used by schools to deliver online courses does not work properly in student Web browsers unless cookies are enabled.

Web users can accumulate large numbers of cookies as they browse the Internet. Most Web browsers have settings that allow the user to refuse only third-party cookies or to review each cookie before it is accepted. Some browsers, such as **Netscape Navigator**, **Mozilla**, **Mozilla Firefox**, and **Opera**, provide comprehensive cookie management functions.

Another approach is to use one of the many third-party programs, called **cookie blockers**, that prevent cookie storage selectively. Some of these programs, such as **WebWasher**, plug into a browser and allow users to block cookies from the Web servers that load advertising banners into Web pages. Other cookie blocking programs, such as **Cookie Pal**, allow cookies to be filtered by Internet (IP) address, allowing in the "good" cookies and denying storage to all others. **Cookie Crusher** is another program that controls cookies before they are stored on a user's hard drive.

WebSideStory provides software that Web site managers can use to analyze Internet traffic at their sites. The company also sells a reporting service to Web sites that provides information about who visits their sites and what sites the visitors came from. WebSideStory's HitBox software collects and warehouses data from Web site visitors remotely, securely, and anonymously. The company does allow Web site visitors to opt out of these cookies.

Web Bugs

Some advertisers send images (from their third-party servers) that are included on Web pages, but are too small to be visible. A **Web bug** is a tiny graphic that a third-party Web site places on another site's Web page. When a site visitor loads the Web page, the Web bug is delivered by the third-party site, which can then place a cookie on the visitor's computer. A Web bug's only purpose is to provide a way for a third-party Web site (the identity of which is unknown to the visitor) to place cookies from that third-party site on the visitor's computer. The Internet advertising community sometimes calls Web bugs "clear GIFs" or "1-by-1 GIFs" because the graphics can be created in the GIF format with a color value of "transparent" and can be as small as 1 pixel by 1 pixel.

Active Content

Until the debut of executable Web content, Web pages could do little more than display content and provide links to related pages with additional

NOTES

information. The widespread use of active content has changed the situation. **Active content** refers to programs that are embedded transparently in Web pages and that cause action to occur. For example, active content can display moving graphics, download and play audio, or implement Webbased spreadsheet programs. Active content is used in electronic commerce to place items into a shopping cart and compute a total invoice amount, including sales tax, handling, and shipping costs. Developers use active content because it extends the functionality of HTML and moves some data processing chores from the busy server machine to the user's client computer. Unfortunately, because active content elements are programs that run on the client computer, active content can damage the client computer. Thus, active content can pose a threat to the security of client computers.

Active content is provided in several forms. The best-known active content forms are cookies, Java applets, JavaScript, VBScript, and ActiveX controls. Other ways to provide Web active content include graphics, Web browser plug-ins, and e-mail attachments.

JavaScript and VBScript are **scripting languages**; they provide scripts, or commands, that are executed. An **applet** is a small application program. *Applets typically run within the Web called zombies. Zombie attacks can be* very difficult to trace to their creators.

Viruses, Worms, and Antivirus Software

The potential dangers lurking in e-mail attachments get a lot of news coverage and *are the most familiar to the general population. E-mail attachments* provide a convenient way to send nontext information over a text-only system—electronic mail. Attachments can contain word-processing files, spreadsheets, databases; images, or virtually any other information you can imagine. Most programs, including Web browser e-mail programs, display *attachments by automatically executing an associated program; for example,* the recipient's Excel program reads an attached Excel workbook file and opens it, or Word opens and displays a Word document. Although this activity itself does not cause damage, Word and Excel macro viruses inside the loaded files can damage a client computer and reveal confidential information *when those files are opened.*

A virus is software that attaches itself to another program and can cause damage when the host program is activated. A worm is a type of virus that replicates itself on the computers that it infects. Worms can spread quickly through the Internet. A **macro virus** is a type of virus that is coded as a small program, called a macro, and is embedded in a file. You have probably read about or have personally experienced recent examples of e-mail attachment-borne virus attacks.

NOTES

E-mail attachments containing viruses and other malicious software are reported daily. Some of the most famous in recent years include the ILOVEYOU virus, also known as the "love bug," and its variants. The ILOVEYOU virus was eventually traced to a 23-year-old computer science student who lived in the Philippines. The virus spread through the Internet with amazing speed as an e-mail message. It infected the computer of anyone who opened the e-mail attachment and clogged e-mail systems with thousands of copies of the useless e-mail message. The virus spread quickly because it automatically sent itself to as many as 300 addresses stored in a computer's Microsoft Outlook address book. Besides replicating itself explosively through e-mail, the virus caused other harm, destroying digital music and photo files stored on the target computers. The ILOVEYOU virus also searched for other users' passwords and forwarded that information to the original perpetrator. Within days, the virus spread to 40 million computers in more than 20 countries and caused an estimated $9 billion in damages—most of it in lost worker productivity.

In 2001, the incidences of virus and worm attacks increased. With more than 40,000 reported security violations occurring that year, the parade of attacks included Code Red and Nimda virus-worm combinations, each affecting millions of computers and costing billions of dollars to clean up. Both Code Red and Nimda are examples of a **multivector virus**, so called because they can enter a computer system in several different ways (vectors). Even though Microsoft issued security patches that should have stopped the Code Red virusworm, it continued to propagate throughout the Internet in 2002. Both the original Code Red virus and a variant called Code Red 2 infected thousands of new computers during the year.

New virus-worm combinations also appeared in 2002 and 2003, including a version of the Code Red virus called Bugbear. Bugbear was spread through Microsoft Outlook e-mail clients. The person receiving the e-mail did not even have to click on an attachment to run the malicious code—Bugbear started itself through a security loophole in the connection between Outlook and the Internet Explorer browser. Of course, Microsoft issued a security patch for the browser, but many users did not install the patch (or, in many cases, even know about it). When launched, Bugbear first checked to see if the computer was running antivirus software. **Antivirus software** detects viruses and worms and either deletes them or isolates them on the client computer so they cannot run. If antivirus software existed on the system, Bugbear attempted to destroy it. Then it installed a Trojan horse program on the computer that let attackers access the computer through the Internet and upload or download files at will. (Bugbear was difficult to eliminate from an infected computer because it gave its own files a randomly generated name; thus, the virus files had different names on every infected computer.)

NOTES

Bugbear would then send out e-mail messages with attachments that would infect the recipients. It did not create its own e-mail messages, but took previously sent e-mail messages that were on the computer and resent them to different addresses. This often fooled recipients because the e-mail messages had subject headers that seemed normal and did not hint that the e-mail might contain a virus. Figure 2.2 summarizes some of the major viruses, worms, and Trojan horses that have plagued Internet users over the years.

Symantec and **McAfee**, among other companies, keep track of viruses and sell antivirus software. You can follow the links in the Online Companion to those companies to find descriptions of thousands of viruses. Antivirus software is only effective if the antivirus data files are kept current. The data files contain virus-identifying information that is used to detect viruses on a client computer. Because people generate new viruses by the hundreds every month, users must be vigilant and update their antivirus data files regularly so that the newest viruses are recognized and eliminated. Some Web e-mail systems, such as Yahoo! Mail, let users scan attachments using antivirus software before downloading e-mail. In these cases, the antivirus software is run by the Web site and the user does not need to take any action to keep the software updated.

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 template, which infects any new Word document created on that computer.

NOTES

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 the infected computer. 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 computers. 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 defaces 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.
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, a 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.This 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 ten minutes of propagation.
2003	Sobig	Trojan Horse	Sobig turns infected computers into spam relay 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 peforms 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 zombies for mass mailing or attacking other computers.

Figure 2.2. *Major viruses, worms, and Trojan horses.*

NOTES

Digital Certificates

One way to control threats from active content is to use digital certificates. A **digital certificate** or digital ID is an attachment to an e-mail message or a program embedded in a Web page that verifies that the sender or Web site is who or what it claims to be. In addition, the digital certificate contains a means to send an encrypted message—encoded so others cannot read it—to the entity that sent the original Web page or e-mail message. In the case of a downloaded program containing a digital certificate, the encrypted message identifies the software publisher (ensuring that the identity of the software publisher matches the certificate) and indicates whether the certificate has expired or is still valid. The digital certificate is a **signed** message or code. Signed code or messages serve the same function as a photo on a driver's license or passport. They provide proof that the holder is the person identified by the certificate. Just like a passport, a certificate does not imply anything about either the usefulness or quality of the downloaded program. The certificate only supplies a level of assurance that the software is genuine. The idea behind certificates is that if the user trusts the software developer, signed software can be trusted because, as proven by the certificate, it came from that trusted developer.

Digital certificates are used for many different types of online transactions, including electronic commerce, electronic mail, and electronic funds transfers. A digital ID verifies a Web site to a shopper and, optionally, identifies a shopper to a Web site. Web browsers or e-mail programs exchange digital certificates automatically and invisibly when requested to validate the identity of each party involved in a transaction.

Figure 2.3 displays the digital certificate owned by Amazon.com. Whenever a browser indicates that it has established secure communication with a Web site; that is, when a lock appears in the browser's status line, the user can double-click the lock (the exact procedure varies somewhat from browser to browser) to display the Web site's digital certificate.

A digital certificate for software is an assurance that the software was created by a specific company. The certificate does not attest to the quality of the software, just to the identity of the company that published it. Digital certificates are issued by a **certification authority (CA)**. A CA can issue digital certificates to organizations or individuals. A CA requires entities applying for digital certificates to supply appropriate proof of identity. Once the CA is satisfied, it issues a certificate. Then, the CA signs the certificate, and its stamp of approval is affixed in the form of a public encryption key, which "unlocks" the certificate for anyone who receives the certificate attached to the publisher's code.

Digital certificates cannot be forged easily. A digital certificate includes six main elements, including :

NOTES

- Certificate owner's identifying information, such as name, organization, address, and so on.
- Certificate owner's public key (you will learn more about public and private keys later in this unit).
- Dates between which the certificate is valid.
- Serial number of the certificate.
- Name of the certificate issuer.
- Digital signature of the certificate issuer.

A **key** is simply a number—usually a long binary number—that is used with the encryption algorithm to "lock" the characters of the message being protected so that they are undecipherable without the key. Longer keys usually provide significantly better protection than shorter keys. In effect, the CA is guaranteeing that the individual or organization that presents the certificate is who or what it claims to be Identification requirements vary

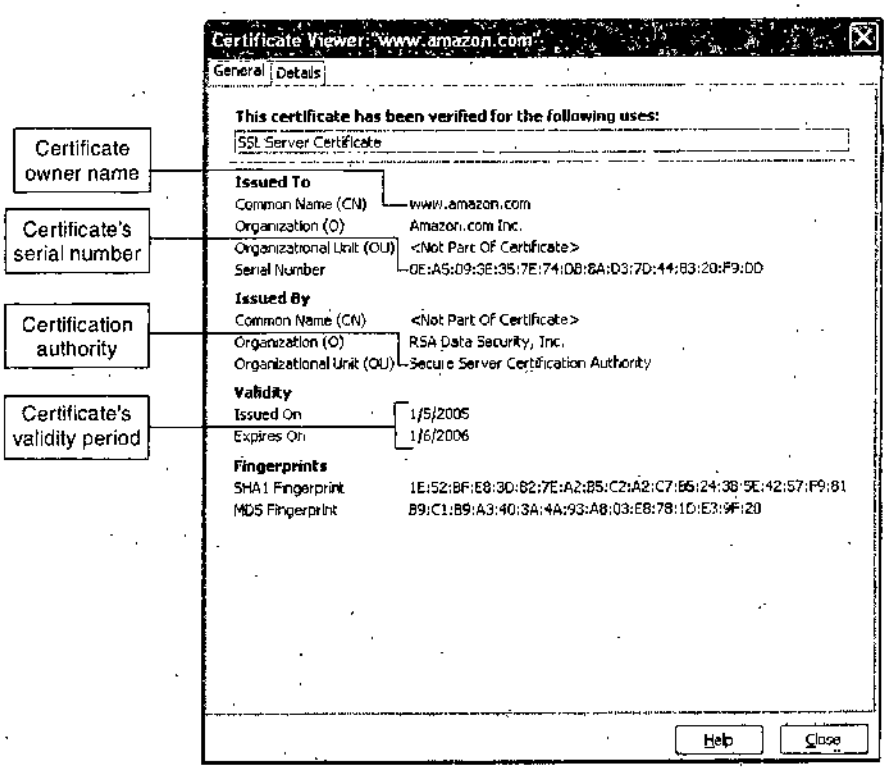


Figure 2.3. *Amazon.com's digital certificate.*

from one CA to another. One CA might require a driver's license for individuals' certificates; others might require a notarized form or fingerprints. CAs usually publish identification requirements so that any Web user or site accepting certificates from each CA understands the stringency of that CA's validation procedures. There are only a small number of CAs because the certificates issued are only as trustworthy as the CA itself, and only a few

NOTES

companies have decided to build the reputation needed to be a successful seller of digital certificates. Two of the most commonly used CAs are **Thawte** and **VeriSign**, but other companies such as **Entrust** and **Equifax Secure** also offer CA services. The digital certificate for Amazon.com (information about this certificate appears in the dialog box shown in Figure 2.3) was issued by VeriSign. As you examine the certificates of various Web sites, you will notice that many of them indicate that the issuer is "RSA Data Security," which is the division of VeriSign that issues many of its digital certificates.

Certificates are classified as low, medium, or high assurance, based largely on the identification requirements imposed on certificate seekers. The fees charged by CAs vary with the level of assurance provided; higher level assurance are more expensive. For example, VeriSign provides certificate issuing and revocation services and offers several classes of certificates—from Class 1 through Class 4—that are differentiated by assurance level, which is the confidence level one can assume based on the process the CA uses to verify the owner's identity. Class 1 certificates are the lowest level and bind e-mail addresses and associated public keys. Class 4 certificates apply to servers and the server organizations. Requirements for Class 4 certificates are significantly greater than those for Class 1. VeriSign's Class 4 certificate, for example, offers assurance of the individual's identity and that person's relationship to the specified company or organization.

Digital certificates expire after a period of time (often one year). This built-in limit provides protection for both users and businesses. Limited-duration certificates guarantee that businesses and individuals must submit their credentials for re-evaluation periodically. The expiration date appears in the certificate itself and in the dialog boxes that browsers display when a Web page or applet that has a digital certificate is about to be opened. Certificates become invalid on their expiration dates or when they are intentionally revoked by the CA. If the CA determines that a Web site has begun delivering malicious code, it will refuse to issue new certificates to that site and revoke any existing certificates it might already have obtained.

Steganography

The term **steganography** describes the process of hiding information (a command, for example) within another piece of information. This information can be used for malicious purposes. Frequently, computer files contain redundant or insignificant information that can be replaced with other information. This other information resides in the background and is undetectable by anyone without the correct decoding software. Steganography provides a way of hiding an encrypted file within another file so that a casual observer cannot detect that there is anything of importance in the container file. In this two-step process, encrypting the file protects it from being read, and steganography makes it invisible.

NOTES

Many security analysts believe that the terrorist organization Al Qaeda used steganography to hide attack orders and other messages in images that its confederates posted on Web sites. Messages hidden using steganography are extremely difficult to detect. This fact, combined with the fact that there are millions of images on the Web, makes the use of steganography by global terrorist organizations a deep concern of governments and security professionals. The Online Companion includes a link to a site with more information about **Steganography and Digital Watermarking.**

Physical Security for Clients

In the past, physical security was a major concern for large computers that ran important business functions such as payroll or billing; however, as networks (including intranets and the Internet) have made it possible to control important business functions from client computers, concerns about physical security for client computers have become greater. Many of the physical security measures used today are the same as those used in the early days of computing; however, some interesting new technologies have been implemented as well.

Devices that read fingerprints are now available for personal computers. These devices, which cost less than $200, provide a much stronger protection than traditional password approaches. In addition to fingerprint readers, companies can use other biometric security devices that are more accurate and, of course, cost more. A **biometric security device** is one that uses an element of a person's biological makeup to perform the identification. These devices include writing pads that detect the form and pressure of a person writing a signature, eye scanners that read the pattern of blood vessels in a person's retina or the color levels in a person's iris, and scanners that read the palm of a person's hand (rather than just one fingerprint) or that read the pattern of veins on the back of a person's hand.

COMMUNICATION CHANNEL SECURITY

The Internet serves as the electronic connection between buyers (in most cases, clients) and sellers (in most cases, servers). The most important thing to remember as you learn about communication channel security is that the Internet was not designed to be secure. Although the Internet has its roots in a military network, that network was not designed to include any significant security features. It was designed to provide redundancy in case one or more communications lines were cut. In other words, the goal of the Internet's packet-switching design was to provide multiple alternative paths on which

NOTES

critical military information could travel. The military always sends sensitive information in an encrypted form so that the content of messages traveling over any network—even if intercepted—remain secret. The security of messages traversing the military predecessors to the Internet was provided by software that operated independently of the network to encrypt messages. As the Internet developed, it did so without any significant security features that became a part of the network itself.

Today, the Internet remains largely unchanged from its original, insecure state. Message packets on the Internet travel an unplanned path from a source node to a destination node. A packet passes through a number of intermediate computers on the network before reaching its final destination. The path can vary each time a packet is sent between the same source and destination points. Because users cannot control the path and do not know where their packets have been, it is possible that an intermediary can read the packets, alter them, or even delete them. That is, any message traveling on the Internet is subject to secrecy, integrity, and necessity threats. This section describes these problems in more detail and outlines several solutions for those problems.

Secrecy Threats

Secrecy is the security threat that is most frequently mentioned in articles and the popular media. Closely linked to secrecy is privacy, which also receives a great deal of attention. Secrecy and privacy, though similar, are different issues. Secrecy is the prevention of unauthorized information disclosure. **Privacy** is the protection of individual rights to nondisclosure. The **Privacy Council**, which helps businesses implement smart privacy and data practices, created an extensive Web site surrounding privacy—covering both business and legal issues. Secrecy is a technical issue requiring sophisticated physical and logical mechanisms, whereas privacy protection is a legal matter. A classic example of the difference between secrecy and privacy is e-mail.

A company might protect its e-mail messages against secrecy violations by using encryption (you will learn more about encryption later in this chapter). In encryption, a message is encoded into an unintelligible form that only the proper recipient can convert back into the original message. Secrecy countermeasures protect outgoing messages. E-mail privacy issues address whether company supervisors should be permitted to read employees' messages randomly. Disputes in this area center around who owns the e-mail messages : the company, or the employees who sent them. The focus in this section is on secrecy, preventing unauthorized persons from reading information they should not be reading.

NOTES

One significant threat to electronic commerce is theft of sensitive or personal information, including credit card numbers, names, addresses, and personal preferences. This kind of theft can occur any time anyone submits information over the Internet because it is easy for an ill-intentioned person to record information packets (a secrecy violation) from the Internet for later examination. The same problems can occur in e-mail transmissions. Software applications called **sniffer programs** provide the means to record information that passes through a computer or router that is handling Internet traffic. Using a sniffer program is analogous to tapping a telephone line and recording a conversation. Sniffer programs can read e-mail messages and unencrypted Web client-server message traffic such as user logins, passwords, and credit card numbers.

Periodically, security experts find electronic holes, called **backdoors**, in electronic commerce software. These can be left open accidentally by the software developer, or they can be left open intentionally. Either way, content is exposed to secrecy threats. A backdoor allows anyone with knowledge of the existence of the backdoor to cause damage by observing transactions, deleting data, or stealing data. In 2000, the Cart32 shopping cart software made by McMurtrey/Whitaker & Associates was found to have a backdoor through which credit card numbers could be obtained by anyone with a backdoor password. The company quickly supplied a patch to eliminate the backdoor. Although the backdoor resulted from a programming error and not from intentional efforts, the consequences were serious for merchants that used the software—their customers' credit card numbers were available to hackers around the world.

Credit card number theft is an obvious problem, but proprietary corporate product information or prerelease data sheets mailed to corporate branches can be intercepted and passed along easily, too. Confidential information can be considerably more valuable than information about credit cards, which usually have spending limits. Stolen corporate information can be worth millions of dollars.

Here is an example of how an online eavesdropper might obtain confidential information. Suppose a user logs on to a Web site that contains a form with text boxes for name, address, and e-mail address. When the user fills out those text boxes and clicks the Submit button, the information is sent to the Web server for processing. Some Web servers obtain and track that data by collecting the text box responses and placing them at the end of the server's URL (which appears in the address box of the user's Web browser). This long URL (with the text box responses appended) is included in all HTTP request and response messages that travel between the user's browser and the server.

So far, no violations have occurred. Suppose, however, that the user decides not to wait for a response from the server. Instead, the user visits another

NOTES

Web site. The server at this second Web site might be set up to collect Web demographics. If it is, it logs the URL from which the user just came by capturing it from the HTTP request message that the browser sends. Web sites use this URL logging technique for the completely legitimate purpose of identifying sources of customer traffic. However, any employee at the second site who has access to the server log can read the part of the URL that includes the information entered into those text boxes on the first site, thus obtaining that user's confidential information.

Web users continually reveal information about themselves when they use the Web. This information includes IP addresses and the type of browser being used. Such data exposure is a secrecy breach. Several Web sites offer an anonymous browser service that hides personal information from sites visited. One of these sites, **Anonymizer**, provides a measure of secrecy to Web surfers who use the site as a portal (the beginning site from which they visit other sites). Anonymizer places its address on the front end of any URLs that the user visits. This shield reveals only the Anonymizer Web site URL to other Web sites that the user visits. This can make anonymous Web surfing possible, but tedious, because each URL that the user wants to visit must be typed in the text box on the Anonymizer home page. To make the process easier, Anonymizer and other companies provide browser plug-in software that users can download and install for an annual subscription fee. Figure 2.4 shows Anonymizer's home page.

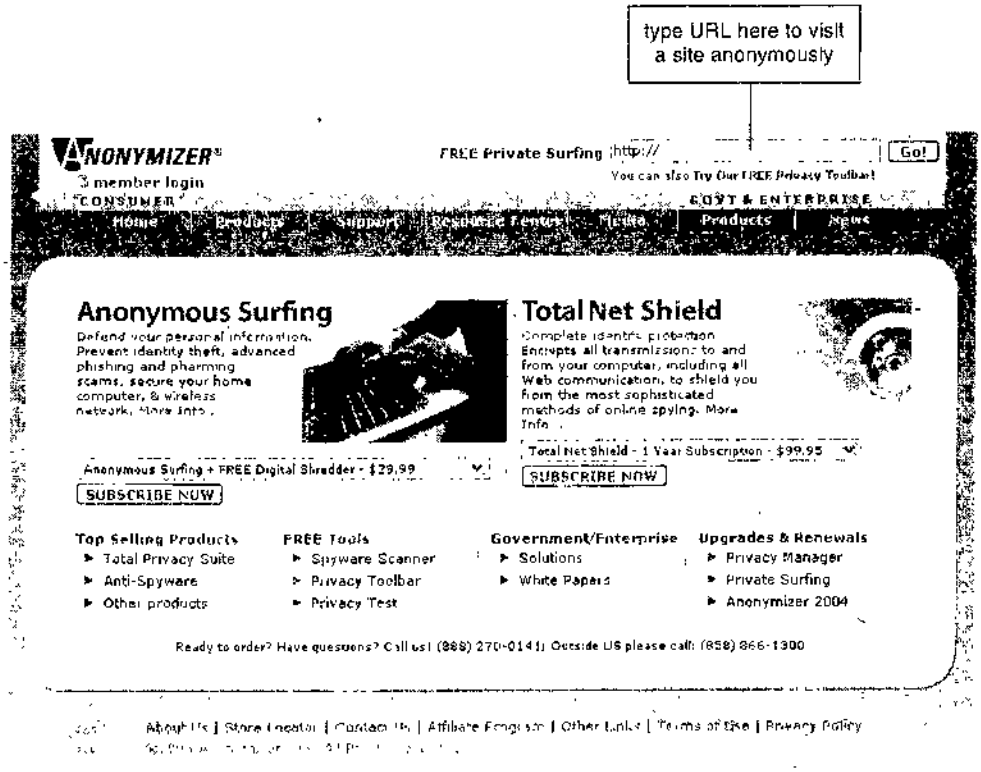


Figure 2.4. *Anonymizer home page.*

NOTES

Integrity Threats

An integrity threat, also known as **active wiretapping**, exists when an unauthorized party can alter a message stream of information. Unprotected banking transactions, such as deposit amounts transmitted over the Internet, are subject to integrity violations. Of course, an integrity violation implies a secrecy violation because an intruder who alters information can read and interpret that information. Unlike secrecy threats, where a viewer simply sees information he or she should not, integrity threats can cause a change in the actions a person or corporation takes because a mission-critical transmission has been altered.

Cybervandalism is an example of an integrity violation. **Cybervandalism** is the electronic defacing of an existing Web site's page. The electronic equivalent of destroying property or placing graffiti on objects, cybervandalism occurs whenever someone replaces a Web site's regular content with his or her own content. Recently, several cases of Web page defacing involved vandals replacing business content with pornographic material and other offensive content.

Masquerading or **spoofing**—pretending to be someone you are not, or representing a Web site as an original when it is a fake—is one means of disrupting Web sites. **Domain name servers (DNSs)** are the computers on the Internet that maintain directories that link domain names to IP addresses. Perpetrators can use a security hole in the software that runs on some of these computers to substitute the addresses of their Web sites in place of the real ones to spoof Web site visitors.

For example, a hacker could create a fictitious Web site masquerading as www.widgets. com by exploiting a DNS security hole that substitutes his or her fake IP address for Widgets.com's real IP address. All subsequent visits to Widgets.com would be redirected to the fictitious site. There, the hacker could alter any orders to change the number of widgets ordered and redirect shipment of those products to another address. The integrity attack consists of altering an order and passing it to the real company's Web server. The Web server is unaware of the integrity attack and simply verifies the consumer's credit card number and passes on the order for fulfillment. Major electronic commerce sites that have been the victims of masquerading attacks in recent years include Amazon.com, AOL, eBay, and PayPal. Some of these schemes combine spam with spoofing. The perpetrator sends millions of spam e-mails that appear to be from a respectable company. The e-mails contain a link to a Web page that is designed to look exactly like the company's site. The victim is encouraged to enter username, password, and sometimes even credit card information. These exploits, which capture confidential customer information, are called **phishing expeditions**. The most common

NOTES

victims of phishing expeditions are users of online banking and payment system (such as PayPal) Web sites.

Necessity Threats

The purpose of a **necessity threat**, also known by other names such as a delay, denial, or denial-of-service (DoS) threat, is to disrupt normal computer processing, or deny processing entirely. A computer that has experienced a necessity threat slows processing to an intolerably slow speed. For example, if the processing speed of a single ATM transaction slows from one or two seconds to 30 seconds, users will abandon ATMs entirely. Similarly, slowing any Internet service drives customers to competitors' Web or commerce sites—possibly discouraging them from ever returning to the original commerce site. In other words, slower processing can render a service unusable or unattractive. For example, an online newspaper that reports three-day-old news is worth very little.

DoS attacks remove information altogether, or delete information from a transmission or file. One documented denial attack caused selected PCs that have Quicken (an accounting program) installed to divert money to the perpetrator's bank account. The denial attack denied money from its rightful owners. In another famous DoS attack against high-profile electronic commerce sites such as Amazon.com and Yahoo!, the attackers used zombie computers to send a flood of data packets to the sites. This overwhelmed the sites' servers and choked off legitimate customers' access. Prior to the attack, perpetrators located vulnerable computers and loaded them with the software that attacked the commerce sites. The Internet Worm attack of 1998, which disabled thousands of computer systems that were connected to the Internet, was the first recorded example of a DoS attack.

Threats to the Physical Security of Internet Communications Channels

The Internet was designed from its inception to withstand attacks on its physical communication links. Recall from Chapter 2 that the main purpose of the U.S. government research project that led to the development of the Internet was to provide an attack resistant technology for coordinating military operations. Thus, the Internet's packet-based network design precludes it from being shut down by an attack on a single communications link on that network.

However, an individual user's Internet service can be interrupted by destruction of that user's link to the Internet. Few individual users have multiple connections to an ISP. However, larger companies and organizations (and ISPs themselves) often do have more than one link to the main backbone of the Internet. Typically, each link is purchased from a different network

NOTES

access provider. If one link becomes overloaded or unavailable, the service provider can switch traffic to another network access provider's link to keep the company, organization, or ISP (and its customers) connected to the Internet.

Threats to Wireless Networks

Networks can use wireless access points (WAPs) to provide network connections to computers and other mobile devices within a range of several hundred feet. If not protected, a wireless network allows anyone within that range to log in and have access to any resources connected to that network. Such resources might include any data stored on any computer connected to the network, networked printers, messages sent on the network, and, if the network is connected to the Internet, free access to the Internet. The security of the connection depends on the Wireless Encryption Protocol (WEP), which is a set of rules for encrypting transmissions from the wireless devices to the WAPs.

Companies that have large wireless networks are usually careful to turn on WEP in devices, but smaller companies and individuals who have installed wireless networks in their homes often do not turn on the WEP security feature. Many WAPs are shipped to buyers with a default login and password already set. Companies that install these WAPs sometimes fail to change that login and password. This has given rise to a new avenue of entry into networks.

In some cities that have large concentrations of wireless networks, attackers drive around in cars using their wireless-equipped laptop computers to search for accessible networks. These attackers are called **wardrivers**. When wardrivers find an open network (or a WAP that has a common default login and password), they sometimes place a chalk mark on the building so that other attackers will know that an easily entered wireless network is nearby. This practice is called **warchalking**. Some warchalkers have even created Web sites that include maps of wireless access locations in major cities around the world. Companies can avoid becoming targets by simply turning on WEP in their access points and changing the logins and passwords to something other than the manufacturers' default settings.

In 2002, Best Buy was using wireless point-of-sale (POS) terminals in some of its 1900 stores. The wireless POS terminals could be moved easily from one area of the store to another, and they helped Best Buy handle large customer flows better than it could using only fixed POS terminals. Unfortunately, Best Buy failed to enable WEP on these terminals. A customer who had just purchased a wireless card for his laptop decided to launch a sniffer utility program on the laptop in his car in the parking lot. The customer was able to intercept data from the POS terminals, including transaction

details and what he said looked like credit card numbers. Best Buy stopped using the wireless POS terminals when the story appeared on several Web sites and newswire services.

NOTES

Encryption Solutions

Encryption is the coding of information by using a mathematically based program and a secret key to produce a string of characters that is unintelligible. The science that studies encryption is called **cryptography**, which comes from a combination of the two Greek words krypto and grapho, which mean "secret" and "writing," respectively. That is, cryptography is the science of creating messages that only the sender and receiver can read.

Cryptography is different from steganography, which makes text undetectable to the naked eye. Cryptography does not hide text; it converts it to other text that is visible, but does not appear to have any meaning. What an unauthorized reader sees is a string of random text characters, numbers, and punctuation.

Encryption Algorithms

The program that transforms normal text, called **plain text**, into **cipher text** (the unintelligible string of characters) is called an **encryption program**. The logic behind an encryption program that includes the mathematics used to do the transformation from plain text to cipher text is called an **encryption algorithm**. There are a number of different encryption algorithms in use today. Some have been developed by the U.S. government and others have been developed by IBM and other commercial enterprises. You can learn more about the development of encryption algorithms, including an evaluation of currently available algorithms, by consulting a Web security textbook (see, for example, the Mackey reference in the For Further Study and Research section at the end of this chapter).

Messages are encrypted just before they are sent over a network or the Internet. Upon arrival, each message is decoded, or **decrypted**, using a **decryption program**—a type of encryption-reversing procedure. Encryption algorithms are considered so vitally important to preserving security within the United States that the National Security Agency has control over their dissemination. Some encryption algorithms are considered so important that the U.S. government has banned publication of details about them. Currently, it is illegal for U.S. companies to export some of these encryption algorithms. Web pages containing software whose distribution is restricted include warnings about U.S. export laws. The Freedom Forum Online contains a number of articles on lawsuits and legislation surrounding encryption export laws. Critics consider publication restrictions a freedom of speech issue. If

NOTES

you are interested in reading more about the latest arguments in the ongoing debates over freedom of speech and export law, search the **Freedom Forum** using the keyword "encryption" as the search term.

One property of encryption algorithms is that someone can know the details of the algorithm and still not be able to decipher the encrypted message without knowing the key that the algorithm used to encrypt the message. The resistance of an encrypted message to attack attempts depends on the size (in bits) of the key used in the encryption procedure. A 40-bit key is currently considered to provide a minimal level of security. Longer keys, such as 128-bit keys, provide much more secure encryption. A sufficiently long key can help make the security unbreakable.

The type of key and associated encryption program used to lock a message, or otherwise manipulate it, subdivides encryption into three functions :

- Hash coding
- Asymmetric encryption
- Symmetric encryption

Hash Coding

Hash coding is a process that uses a **hash algorithm** to calculate a number, called a **hash value**, from a message of any length. It is a fingerprint for the message because it is almost certain to be unique for each message. Good hash algorithms are designed so that the probability of two different messages resulting in the same hash value, which would create a **collision**, is extremely small. Hash coding is a particularly convenient way to tell whether a message has been altered in transit because its original hash value and the hash value computed by the receiver will not match after a message is altered.

Asymmetric Encryption

Asymmetric encryption, or **public-key encryption**, encodes messages by using two mathematically related numeric keys. In 1977, Ronald Rivest, Adi Shamir, and Leonard Adleman invented the RSA Public Key Cryptosystem while they were professors at MIT. Their invention revolutionized the way sensitive information is exchanged. In their system, one key of the pair, called a **public key**, is freely distributed to the public at large—to anyone interested in communicating securely with the holder of both keys. The public key is used to encrypt messages using one of several different encryption algorithms. The second key—called a **private key**—belongs to the key owner, who keeps the key secret. The owner uses the private key to decrypt all messages received.

NOTES

Here is an overview of how an asymmetric encryption system works : If Herb wants to send a message to Allison, he obtains Allison's public key from any of several well-known public places. Then, he encrypts his message to Allison using her public key. Once the message is encrypted, only Allison can read the message by decrypting it with her private key. Because the keys are unique, only one secret key can open the message encrypted with a corresponding public key, and vice versa. Reversing the process, Allison can send a private message to Herb using Herb's public key to encrypt the message. When he receives Allison's message, Herb uses his private key to decrypt the message and then read it. If they are sending e-mail to one another, the message is secret only while in transit. Once a message is downloaded from the mail server and decoded, it is stored in plain text on the recipient's machine for all to view.

One of the most popular technologies used to implement public-key encryption today is called Pretty Good Privacy (PGP). PGP was invented in 1991 by Phil Zimmerman, who charged businesses for use of PGP, but allowed individuals to use PGP at no cost. PGP is a set of software tools that can use several different encryption algorithms to perform public-key encryption. The PGP business was purchased by Network Associates in 1997 and sold back to the product's developers, who formed PGP Corporation in 2002. Today, individuals can download free versions of PGP for personal use from the PGP Corporation site and from the PGP International site. Individuals can use PGP to encrypt their e-mail messages to protect them from being read if they are intercepted on the Internet. The PGP Corporation site sells licenses to businesses that want to use the technology to protect business communication activities.

Symmetric Encryption

Symmetric encryption, also known as private-key encryption, encodes a message with one of several available algorithms that use a single numeric key, such as 456839420783, to encode and decode data. Because the same key is used, both the message sender and the message receiver must know the key. Encoding and decoding messages using symmetric encryption is very fast and efficient. However, the key must be guarded. If the key is made public, then all messages sent previously using that key are vulnerable, and both the sender and receiver must use new keys for future communication.

It can be difficult to distribute new keys to authorized parties while maintaining security and control over the keys. The catch is that to transmit anything privately, it must be encrypted. This includes the new, secret key. Another significant problem with private keys is that they do not scale well

NOTES

in large environments such as the Internet. Each pair of users on the Internet who wants to share information privately must have their own private key. That results in a huge number of key-pair combinations, similar to a telephone system of private lines without switching stations. Enabling 12 people to have a private key pair between all pairs (or private telephone lines between each pair) would require 66 private keys. In general, n individual Internet clients require (n(n-1))/2 private key pairs.

In secure environments such as the defense sector, using private-key encryption is simpler, and it is the prevalent method to encode sensitive data. Distribution of classified information and encryption keys is straightforward in the defense sector. It requires guards (two-person control) and secret transportation plans. The Data Encryption Standard (DES) is a set of encryption algorithms adopted by the U.S. government for encrypting sensitive or commercial information. It is the most widely used private-key encryption system. However, the DES private-key size is increased periodically because individuals are using increasingly fast computers to break messages encoded with shorter keys. In 1999, for example, the Electronic Frontier Foundation's Deep Crack key breaker used 100,000 PCs on the Internet to break a DES-encrypted test message in under 23 hours (see the EFF DES Cracker Project for more information).

Today, the U.S. government uses a stronger version of the Data Encryption Standard, called Triple Data Encryption Standard (Triple DES or 3DES). Triple DES offers good protection because it cannot be cracked even with today's supercomputers. Experts expect that it will continue to be extremely difficult to crack for the next several years. However, the U.S. government's National Institute of Standards and Technology (NIST) has developed a new encryption standard designed to keep government information secure.

The new standard is called the Advanced Encryption Standard (AES). In February 2001, the NIST announced that the four-year development process had been successful and that two cryptography researchers from Belgium had created the algorithm chosen for AES. The algorithm's name is Rijndael (pronounced "rain doll"); you can learn more about the development process and the algorithm at the NIST's AES Algorithm (Rijndael) Web site.

Comparing Asymmetric and Symmetric Encryption Systems

Public-key (asymmetric) systems provide several advantages over private-key (symmetric) encryption methods. First, the combination of keys required to provide private messages between enormous numbers of people is small. If n people want to share secret information with one another, then only n unique public-key pairs are required-far fewer than an equivalent private-key system. Second, key distribution is not a problem. Each person's public

NOTES

key can be posted anywhere and does not require any special handling to distribute. Third, public-key systems make implementation of digital signatures possible. This means that an electronic document can be signed and sent to any recipient with nonrepudiation. That is, with public-key techniques, it is not possible for anyone other than the signer to produce the signature electronically; in addition, the signer cannot later deny signing the electronic document.

Public-key systems have disadvantages. One disadvantage is that public-key encryption and decryption are significantly slower than private-key systems. This extra time can add up quickly as individuals and organizations conduct commerce on the Internet. Public-key systems do not replace private-key systems, but serve as a complement to them. Public-key systems are used to transmit private keys to Internet participants so that additional, more efficient communication can occur in a secure Internet session. Figure 2.5 shows a graphical representation of the hashing, private-key, and public-key encryption methods: Figure 2.5 (*a*) shows hash coding; Figure 2.5 (*b*) depicts private-key encryption; and Figure 2.5 (*c*) illustrates public-key encryption.

Several encryption algorithms exist that can be used with secure Web servers. The U.S. government approves the use of several of these inside the United States. Electronic commerce Web servers can accommodate most of these algorithms because they must be able to communicate with a wide variety of Web browsers.

The **Secure Sockets Layer (SSL)** system developed by Netscape Communications and the Secure Hypertext Transfer Protocol (S-HTTP) developed by CommerceNet are two protocols that provide secure information transfer through the Internet. SSL and S-HTTP allow both the client and server computers to manage encryption and decryption activities between each other during a secure Web session.

SSL and S-HTTP have different goals. SSL secures connections between two computers, and S-HTTP sends individual messages securely. Encryption of outgoing messages and decryption of incoming messages happens automatically and transparently with both SSL and S-HTTP.

NOTES

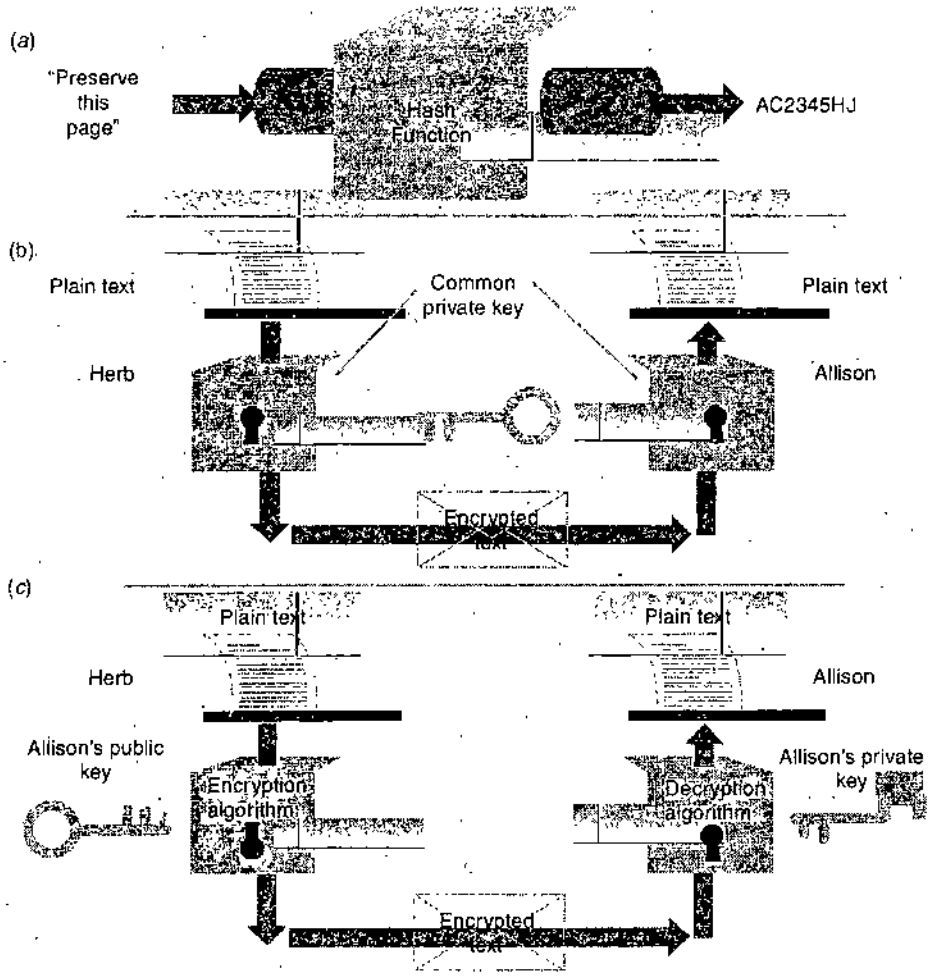


Figure 2.5. *(a) hash coding, (b) private-key, and (c) public-key encryption.*

Secure Sockets Layer (SSL) Protocol

SSL provides a security "handshake" in which the client and server computers exchange a brief burst of messages. In those messages, the level of security to be used for exchange of digital certificates and other tasks is agreed upon. Each computer identifies the other. After identification, SSL encrypts and decrypts information flowing between the two computers. This means that information in both the HTTP request and any HTTP response is encrypted. Encrypted information includes the URL the client is requesting, any forms containing information the user has completed (which might include a credit card number), and HTTP access authorization data, such as usernames and passwords. In short, all communication between SSL-enabled clients and servers is encoded. When SSL encodes everything flowing between the client and server, an eavesdropper receives only unintelligible information.

SSL can secure many different types of communication between computers in addition to HTTP. For example, SSL can secure FTP sessions, enabling

NOTES

private downloading and uploading of sensitive documents, spreadsheets, and other electronic data. SSL can secure Telnet sessions in which remote computer users can log on to corporate host machines and send their passwords and usernames. The protocol that implements SSL is HTTPS. By preceding the URL with the protocol name HTTPS, the client is signifying that it would like to establish a secure connection with the remote server.

Secure Sockets Layer allows the length of the private session key generated by every encrypted transaction to be set at a variety of bit lengths (such as 40-bit, 56-bit, 128-bit, and 168-bit). A **session key** is a key used by an encryption algorithm to create cipher text from plain text during a single secure session. The longer the key, the more resistant the encryption is to attack. A Web browser that has entered into an SSL session indicates that it is in an encrypted session (most browsers use an icon in the browser status bar). Once the session is ended, the session key is discarded permanently and not reused for subsequent secure sessions.

Here is how SSL works with an exchange between a client and an electronic commerce site : Remember that SSL has to authenticate the commerce site and encrypt any transmissions between the two computers. When a client browser sends a request message to a server's secure Web site, the server sends a hello request to the browser (client). The browser responds with a client hello. The exchange of these greetings, or the handshake, allows the two computers to determine the compression and encryption standards that they both support.

Next, the browser asks the server for a digital certificate—proof of identity. In response, the server sends to the browser a certificate signed by a recognized certification authority. The browser checks the serial number and certificate fingerprint on the server certificate against the public key of the CA stored within the browser. Once the CA's public key is verified, the endorsement is verified. That action authenticates the Web server.

Both the client and server agree that their exchanges should be kept secure because they involve transmitting credit card numbers, invoice numbers, and verification codes over the Internet. To implement secrecy, SSL uses public-key (asymmetric) encryption and private-key (symmetric) encryption. Although public-key encryption is handy, it is slow compared to private-key encryption. That is why SSL uses private-key encryption for nearly all its secure communications. Because it uses private-key encryption, SSL must have a way to get the key to both the client and server without exposing it to an eavesdropper. SSL accomplishes this by having the browser generate a private key for both to share. Then the browser encrypts the private key it has generated using the server's public key. The server's public key is stored in the digital certificate that the server sent to the browser during the authentication step. Once the key is encrypted, the browser sends it to

NOTES

the server. The server, in turn, decrypts the message with its private key and exposes the shared private key.

From this point on, public-key encryption is no longer used. Instead, only private-key encryption is used. All messages sent between the client and the server are encrypted with the shared private key, also known as the session key. When the session ends, the session key is discarded. A new connection between a client and a secure server starts the entire process all over again, beginning with the handshake between the client browser and the server. The client and server can agree to use 40-bit encryption or 128-bit encryption. The client and server also agree on which specific encryption algorithm to use. Figure 2.6 illustrates the SSL handshake that occurs before a client and server exchange private-key encoded business information for the remainder of the secure session.

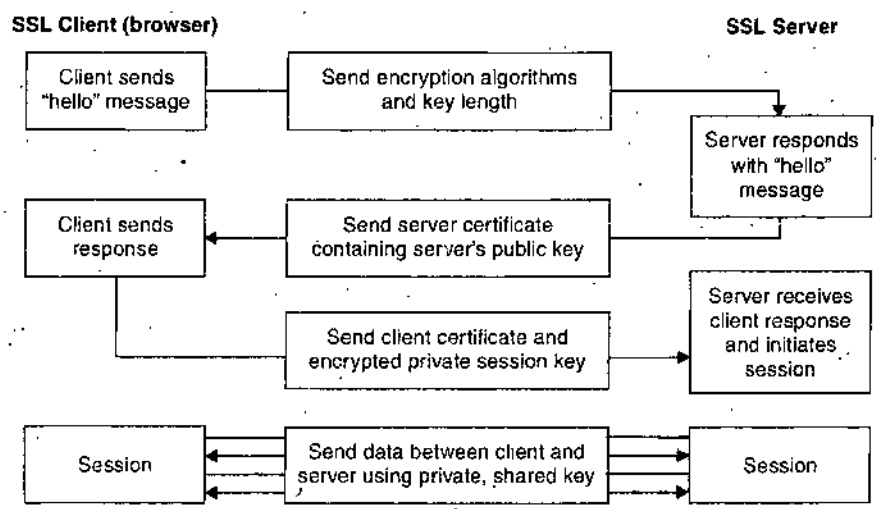


Figure 2.6. *Establishing an SSL session.*

Secure HTTP (S-HTTP)

Secure HTTP (S-HTTP) is an extension to HTTP that provides a number of security features, including client and server authentication, spontaneous encryption, and request/response nonrepudiation. The protocol was developed by **CommerceNet**, a consortium of organizations interested in promoting electronic commerce. S-HTTP provides symmetric encryption for maintaining secret communications and public-key encryption to establish client/server authentication. Either the client or the server can use S-HTTP techniques separately. That is, a client browser may require security through the use of a private (symmetric) key, whereas the server may require client authentication by using public-key techniques.

The details of S-HTTP security are conducted during the initial negotiation session between the client and server. Either the client or the server can

NOTES

specify that a particular security feature be required, optional, or refused. When one party stipulates that a particular security feature be required, the client or server continues the connection only if the other party (client or server) agrees to enforce the specified security. Otherwise, no secure connection is established. Suppose the client browser specifies that encryption is required to render all communications secret. In such a situation, the transactions of a high-fashion clothing designer purchasing silk from a Far East textile house will remain confidential. Eavesdropping competitors cannot learn which fabrics are featured next season. On the other hand, the textile mill may insist that integrity be enforced so that quantities and prices quoted to the purchaser remain intact. In addition, the textile mill may want assurances that the purchaser is who he or she claims to be, not an imposter. A form of nonrepudiation, this security property provides positive confirmation of an offer by a client and makes it impossible for the client to deny ever having made the offer.

S-HTTP differs from SSL in the way it establishes a secure session. SSL carries out a client/server handshake exchange to set up a secure communication, but S-HTTP sets up security details with special packet headers that are exchanged in S-HTTP. The headers define the type of security techniques, including the use of private-key encryption, server authentication, client authentication, and message integrity. Header exchanges also stipulate which specific algorithms each side supports, whether the client or the server (or both) supports the algorithm, and whether the security technique (for example, secrecy) is required, optional, or refused. Once the client and server agree to security implementations enforced between them, all subsequent messages between them during that session are wrapped in a secure container, sometimes called an envelope. A **secure envelope** encapsulates a message and provides secrecy, integrity, and client/server authentication. In other words, it is a complete package. With it, all messages traveling on the network or Internet are encrypted so that they cannot be read. Messages cannot be altered undetectably because integrity mechanisms provide a detection code that signals a message has been altered. Clients and servers are authenticated with digital certificates issued by a recognized certification authority. The secure envelope includes all of these security features. S-HTTP is no longer used by many Web sites. SSL has become a more generally accepted standard for establishing secure communication links between Web clients and Web servers.

You have learned how encryption provides message secrecy and confidentiality, and you have learned how digital certificates serve to authenticate a server to a client, and vice versa. However, you have not learned how to implement message integrity. The methods that allow you to

ensure that an interloper does not change a message in transit appear in the next section.

Ensuring Transaction Integrity with Hash Functions

NOTES

Electronic commerce ultimately involves a client browser sending payment information, order information, and payment instructions to the Web server and that server responding with a confirmation of the order details. If an Internet interloper alters any of the order information in transit, harmful consequences can result. For instance, the perpetrator could alter the shipment address so that he or she receives the merchandise instead of the original customer. This is an example of an **integrity violation**, which occurs whenever a message is altered while in transit between the sender and receiver.

Although it is difficult and expensive to prevent a perpetrator from altering a message, there are security techniques that allow the receiver to detect when a message has been altered. When the receiver—a Web server, for example—receives a damaged message, the receiver simply asks the sender to retransmit the message. Apart from being annoying, a damaged message harms no one as long as both parties are aware of the alteration. Harm occurs when unauthorized message changes go undetected by the message's sender and receiver.

A combination of techniques creates messages that are both tamperproof and authenticated. Additionally, those techniques provide the property of nonrepudiation—making it impossible for message creators to claim that the message was not theirs or that they did not send it. To eliminate fraud and abuse caused by messages being altered, two separate algorithms are applied to a message. First, a hash algorithm is applied to the message. Hash algorithms are **one-way functions**, meaning that there is no way to transform the hash value back to the original message. This approach is acceptable because a hash value is compared only with another hash value to see if there is a match—the original, prehash values are never compared with one another.

All encryption programs convert text into a **message digest**, which is a small integer number that summarizes the encrypted information. A hash algorithm uses no secret key; the message digest it produces cannot be inverted to produce the original information; the algorithm and information about how it works are publicly available; and finally, hash collisions are nearly impossible. Once the hash function computes a message's hash value, that value is appended to the message. Suppose the message is a purchase order containing the customer's address and payment information. When the merchant receives the purchase order and attached message digest, he

NOTES

or she calculates a message digest value for the message (exclusive of the original attached message digest). If the message digest value that the merchant calculates matches the message digest attached to the message, the merchant then knows the message is unaltered—that is, no interloper altered the amount or the shipping address information. Had someone altered the information, then the merchant's software would compute a message digest value different from the message digest that the client calculated and sent along with the purchase order.

Ensuring Transaction Integrity with Digital Signatures

Hash functions are not a complete solution. Because the hash algorithm is public and (by design) widely known, anyone could intercept a purchase order, alter the shipping address and quantity ordered, re-create the message digest, and send the message and new message digest on to the merchant. Upon receipt, the merchant would calculate the message digest value and confirm that the two message digest values match. The merchant is fooled into concluding that the message is unadulterated and genuine. To prevent this type of fraud, the sender encrypts the message digest using his or her private key.

An encrypted message digest (message hash value) is called a **digital signature**. A purchase order accompanied by a digital signature provides the merchant with positive identification of the sender and assures the merchant that the message was not altered. Because the message digest is encrypted using a public key, only the owner of the public/private key pair could have encrypted the message digest. Thus, when the merchant decrypts the message with the user's public key and subsequently calculates a matching message digest value, the result is proof that the sender is authentic. Furthermore, matching hash values prove that only the sender could have authored the message (non-repudiation) because only his or her private key would yield an encrypted message that could be decrypted successfully by an associated public key. This solves the spoofing problem.

If necessary, both parties can agree to provide transaction secrecy in addition to the integrity, nonrepudiation, and authentication that the digital signature provides. Simply encrypting the entire string—digital signature and message—guarantees message secrecy. Used together, public-key encryption, message digests, and digital signatures provide a high level of security for Internet transactions. Figure 2.7 illustrates how a digital signature and a signed message are created and sent.

NOTES

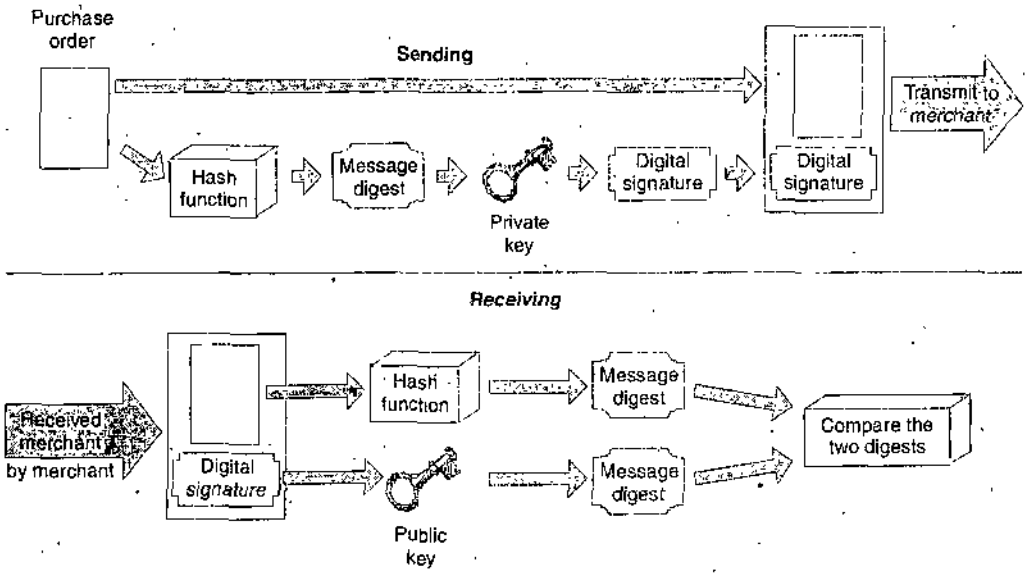


Figure 2.7. *Sending and receiving a digitally signed message*

In 2000, U.S. President Bill Clinton signed a bill that gave digital signatures the same legal status as traditional signatures. Clinton first signed the paper version of the new digital signature legislation with a pen. Then, he signed the electronic version of the bill with a smart card containing his digital signature. After doing so, the name "Bill Clinton" appeared on the screen under the text of the new law entitled Electronic Signatures in Global and National Commerce Act. People can now electronically sign all sorts of legal documents, such as online car lease agreements, loan papers, and purchase orders.

The European Union followed closely on the heels of the U.S. legislation and required all of its member countries to enact digital signature laws by mid-2001. Most Canadian provinces had also enacted digital signature legislation by the end of 2001. Other countries have passed or are working toward passing laws that enable the use of digital signatures.

Guaranteeing Transaction Delivery

As you learned earlier in this chapter, denial or delay-of-service attacks remove or absorb resources. Neither encryption nor a digital signature protects information packets from theft or slowdown. However, the Transmission Control Protocol (TCP) half of the TCP/IP pair is responsible for end-to-end control of packets. When it reassembles packets at the destination in the correct order, it handles all the details when packets do not appear. Among TCP's duties are to request that the client computer resend data when packets seem to be missing. That is, no special computer security protocol beyond TCP/IP is required as a countermeasure against denial attacks. TCP/IP builds checks into the data so that it can tell when data packets are altered, inadvertently or otherwise.

NOTES

SECURITY FOR SERVER COMPUTERS

The server is the third link in the client-Internet-server electronic commerce path between the user and a Web server. Servers have vulnerabilities that can be exploited by anyone determined to cause destruction or acquire information illegally. One entry point is the Web server and its software. Other entry points are any back-end programs containing data, such as a database and the server on which it runs. Although no system is completely safe, the Web server administrator's job is to make sure that security policies are documented and considered in every part of the electronic commerce operation.

Web Server Threats

Web server software, as you learned in Chapter 8, is designed to deliver Web pages by responding to HTTP requests. Although Web server software is not inherently high-risk software, it has been designed with Web service and convenience as the main design goals. The more complex the software, the greater the probability that it contains coding errors or security weaknesses.

A Web server can compromise secrecy if it allows automatic directory listings. The secrecy violation occurs when the contents of a server's folder names are revealed to a Web browser. This happens frequently and is caused when a user enters a URL, such as http ://www.somecompany.com/FAQ/, and expects to see the default page in the FAQ directory. The default Web page that the server normally displays is named index.htm or index.html. If that file is not in the directory, a Web server that allows automatic directory listings displays all of the file and folder names in that directory. Then, visitors can click folder names at random and open folders that might otherwise be off limits. Careful site administrators turn off this folder name display feature. If a user attempts to browse a folder where protections prevent browsing, the Web server issues a warning message stating that the directory is not available.

Web servers can compromise security by requiring users to enter a username and password. The username and password can be subsequently revealed when the user visits multiple pages within the same Web server's protected area if the server requires that users reestablish their usernames and passwords for each protected page they visit. This repeated information requirement is necessary because the Web is stateless—it cannot remember what happened during the last transaction. The most convenient way to remember a user name and password is to store the user's confidential information in a cookie on his or her computer. That way, the Web server can request confirmation of the data by requesting that the computer send a cookie. Although cookies are not inherently unsafe, a Web server should

NOTES

not ask a Web browser to transmit a cookie in unencrypted form. The **W3C Security FAQ** provides additional information about server security.

One of the most sensitive files on a Web server is the file that holds Web server username and password pairs. If that file is compromised, an intruder can enter privileged areas masquerading as someone else. Such an intruder can obtain usernames and passwords if that information is readily available and not encrypted. Most Web servers store user authentication information in encrypted form.

The passwords that users select can be a threat. Users sometimes select passwords that are guessed easily, such as mother's maiden name, name of a child, a telephone number, or some easily obtained identification number, such as a Social Security number. **Dictionary attack programs** cycle through an electronic dictionary, trying every word in the book as a password. Users' passwords, once broken, may provide an opening for illegal entry into a server that can remain undetected for a long time. To prevent dictionary attacks, many organizations use a dictionary check as a preventive measure in their password assignment software. When a user selects a new password, the password assignment software checks the password against its dictionary and, if it finds a match, refuses to allow the use of that password. An organization's password assignment software dictionary typically includes common words, names (including common pet names), acronyms that are commonly used in the organization, and words or characters (including numbers) that have some meaning for the user requesting the password (for example, employees might be prohibited from using their employee numbers as passwords).

Database Threats

Electronic commerce systems store user data and retrieve product information from databases connected to the Web server. Besides storing product information, databases connected to the Web contain valuable and private information that could damage a company irreparably if disclosed or altered. Most large-scale database systems include security features that rely on usernames and passwords. Once a user is authenticated, select portions of the database become available to that user. However, some databases either store username/password pairs in an unencrypted table, or they fail to enforce security altogether and rely on the Web server to enforce security. If unauthorized users obtain user authentication information, they can masquerade as legitimate database users and reveal or download confidential and potentially valuable information. Trojan horse programs hidden within the database system can also reveal information by changing the access rights of various user groups. A Trojan horse can even remove access controls within a database, giving all users complete access to the data—including intruders.

NOTES

Other Programming Threats

Web server threats can arise from programs executed by the server. Java or C++ programs that are passed to Web servers by a client, or that reside on a server, frequently make use of a buffer. A **buffer** is an area of memory set aside to hold data read from a file or database. A buffer is necessary whenever any input or output operation takes place because a computer can process file information much faster than the information can be read from input devices or written to output devices. Programs filling buffers can malfunction and overfill the buffer, spilling the excess data outside the designated buffer memory area. This is called a **buffer overrun** or **buffer overflow** error. Usually, this occurs because the program contains an error or bug that causes the overflow. Sometimes, however, the buffer overflow is intentional. The Internet Worm of 1988 was such a program. It caused an overflow condition that eventually consumed all resources until the affected computer could no longer function.

A more insidious version of a buffer overflow attack writes instructions into critical memory locations so that when the intruder program has completed its work of overwriting buffers, the Web server resumes execution by loading internal registers with the address of the main attacking program's code. This type of attack can open the Web server to severe damage because the resumed program—which is now the attacker program—may regain control of the computer, exposing its files to disclosure and destruction by the attacking program. **The Red Hat Linux Buffer Overflow Attacks Web Page** describes the buffer vulnerabilities of Web servers that run on the Linux operating system. Good programming practices can reduce the potential damage from buffer overflows and some computers include hardware that works with the operating system to limit the effects of buffer overflows that are intentionally programmed to create damage.

A similar attack, one in which excessive data is sent to a server, can occur on mail servers. Called a **mail bomb**, the attack occurs when hundreds or even thousands of people each send a message to a particular address. The attack might be launched by a large team of well-organized hackers, but more likely the attack is launched by one or a few hackers who have gained control over others' computers using a Trojan horse virus or some other method of turning those computers into zombies. The accumulated mail received by the target of the mail bomb exceeds the allowed e-mail size limit and can cause e-mail systems to malfunction. Although it is fairly easy to track the people responsible for the attack, it is debilitating nonetheless.

Threats to the Physical Security of Web Servers

Web servers and the computers that are networked closely to them, such as the database servers and application servers used to supply content and

NOTES

transaction-processing capabilities to electronic commerce Web sites, must be protected from physical harm. For many companies, these computers have become repositories of important data (information about customers, products, sales, purchases, and payments). They have also become important parts of the revenue-generating function in many businesses. As key physical resources, these computers and related equipment warrant high levels of protection against threats to their physical security.

As you learned in Chapter 8, many companies use CSPs to host Web sites. Even large companies that own servers and have IT staff to maintain those servers often put the computers in a CSP facility. The security that CSPs maintain over their physical premises (see earlier section on Threats to the Physical Security of Internet Communications Channels) is, in many cases, stronger than the security that a company could provide for computers maintained at its own location.

Companies can take additional steps to protect their Web servers. Many companies maintain backup copies of server contents at a remote location. If the Web server operation is critical to the continuation of the business, a company can maintain a duplicate of the entire Web server physical facility at a remote location. In the case of a natural disaster or a terrorist attack, the Web operations can be switched over in a matter of seconds to the backup location. Examples of mission-critical Web servers that would warrant such a comprehensive (and expensive) level of physical security include airline reservation systems, stock brokerage firm trading systems, and bank account clearing systems.

Some companies rely on their service providers to help with Web server security. Major service providers that offer managed services, such as **Level 3**, **PSINet**, and **Verio Security Services**, often include Web server security as an add-on service. Other companies hire smaller, specialized security service providers to handle security (see Learning From Failures—Pilot Network Services to learn more about one alternative to this approach). Having a service provider handle security usually adds an additional $1000 to $3000 per month to the bandwidth charges. The specialized security firms often charge two to three times more than that for their services and e-mails were not being returned quickly. On the afternoon of April 25, 2001, Pilot employees received four e-mails. The first explained that telephones would be disconnected that evening. The second asked all employees to turn in their mobile phones and pagers. The third announced that the chief financial officer had resigned. The final e-mail stated that all employees were out of a job as of 4 :30 p.m.

Pilot's clients, many of which found out about the collapse from the Pilot employees who had been servicing their accounts, were in serious trouble. Connections to the Internet vanished with no warning. The companies that

NOTES

had used Pilot to host entire Web operations were in an even worse situation. A group of Pilot customers convinced AT&T (the provider of Pilot's Internet connections) to continue to carry traffic from Pilot, even though Pilot had not paid AT&T. Providian Financial, a major bank holding company and credit card processor, sent its own employees into Pilot operations centers to keep Providian's Web servers operating. Other Pilot customers that were Providian's competitors protested loudly. Most Pilot customers were concerned that their Web servers were suddenly open and vulnerable to attack.

Several of Pilot's competitors tried to raise funding to take over the business, but all of those attempts failed, and on May 9, 2001—two weeks after the collapse—AT&T cut Internet service and Pilot was liquidated. Pilot's former customers were scrambling to hire security staff, find alternative hosting firms, or join forces with other companies to keep their electronic commerce sites operating. The lesson from this failure is that security is a critical part of an electronic commerce operation. It should be handled with the same care that a company would use to protect any physical asset. If any part of the security function is handed over to another company, that company's condition becomes an important concern and must be monitored carefully.

Access Control and Authentication

Access control and authentication refers to controlling who and what has access to the Web server. Most people who work with Web servers in electronic commerce environments do not sit at a keyboard connected to the server. Instead, they access the server from a client computer. Recall that authentication is verification of the identity of the entity requesting access to the computer. Just as users can authenticate servers with which they are interacting, servers can authenticate individual users. When a server requires positive identification of a user, it requests that the client send a certificate.

The server can authenticate a user in several ways. First, the certificate represents the user's admittance voucher. If the server cannot decrypt the user's digital signature contained in the certificate using the user's public key, then the certificate did not come from the true owner. Otherwise, the server is certain that the certificate came from the owner. This procedure prevents fraudulent certificates of "admission" to a secure server. Second, the server checks the timestamp on the certificate to ensure that the certificate has not expired. A server will reject an expired certificate and provide no further service. Third, a server can use a callback system in which the user's client computer name and address are checked against a list of usernames and assigned client computer addresses. Such a system works especially well in an intranet where usernames and client computers are controlled closely and assigned systematically. On the Internet, a callback system is more difficult to manage—particularly if client users are mobile and work

NOTES

from different locations. It is easy to see how certificates issued by trusted CAs play a central role in authenticating client computers and their users. Certificates provide attribution—irrefutable evidence of identity—if a security breach occurs.

Usernames and passwords can also provide some element of protection. To authenticate users using passwords and usernames, the server must acquire and store a database containing rightful users' passwords and usernames. Many Web server systems store usernames and passwords in a file. Large electronic commerce sites usually keep username/password combinations in a separate database with built-in security features.

The easiest way to store passwords is to maintain usernames in plain text and encrypt passwords using a one-way encryption algorithm. With the plain text username and encrypted password stored, the system can validate users when they log on by checking the usernames they enter against the list of usernames stored in the database. The password that a user enters when he or she logs on to a system is encrypted. Then the resulting encrypted password from the user is checked against the encrypted password stored in the database. If the two encrypted versions of the password match for the given user, the login is accepted. That is why even a system administrator cannot tell you what your forgotten password is on most systems. Instead, the administrator must assign a new temporary password that the user can change to another password. Passwords are not immune to discovery, and a person truly intent on stealing a password can often figure out a way to do so.

Note that the site visitor can save his or her username and password as a cookie on the client computer, which allows access to subscription areas of the site without entering the username and password on subsequent site visits. The trouble with that system of cookies is that the information might be stored on the client computer in plain text. If the cookie contains login and password information, then that information is visible to anyone who has access to the user's computer.

Web servers often provide access control list security to restrict file access to selected users. An **access control list (ACL)** is a list or database of files and other resources and the usernames of people who can access the files and other resources. Each file has its own access control list. When a client computer requests Web server access to a file or document that has been configured to require an access check, the Web server checks the resource's ACL file to determine if the user is allowed to access that file. This system is especially convenient to restrict access of files on an intranet server so that individuals can only access selected files on a need-to-know basis. The Web server can exercise fine control over resources by further subdividing file access into the activities of read, write, or execute. For example, some

NOTES

users may be permitted to read the corporate employee handbook, but not allowed to update or write to the file. Only the human resources (HR) manager would have write access to the employee handbook, and that access privilege is stored along with the HR manager's ID and password in an ACL.

Firewalls

A **firewall** is software or a hardware and software combination that is installed in a network to control the packet traffic moving through it. Most organizations place a firewall at the Internet entry point of their networks. The firewall provides a defense between a network and the Internet or between a network and any other network that could pose a threat. Firewalls have the following characteristics :

- All traffic from inside to outside and from outside to inside the network must pass through it.
- Only authorized traffic, as defined by the local security policy, is allowed to pass through it.
- The firewall itself is immune to penetration.

Those networks inside the firewall are often called **trusted**, whereas networks outside the firewall are called **untrusted**. Acting as a filter, firewalls permit selected messages to flow into and out of the protected network. For example, one security policy a firewall might enforce is to allow all HTTP (Web) traffic to pass back and forth, but disallow FTP or Telnet requests either into or out of the protected network. Ideally, firewall protection should prevent access to networks inside the firewall by unauthorized users, and thus prevent access to sensitive information. Simultaneously, a firewall should not obstruct legitimate users. Authorized employees outside the firewall ought to have access to firewall-protected networks and data files. Firewalls can separate corporate networks from one another and prevent personnel in one division from accessing information from another division of the same company. Using firewalls to segment a corporate network into secure zones serves as a coarse need-to-know filter.

Large organizations that have multiple sites and many locations must install a firewall at each location that has an external connection to the Internet. Such a system ensures an unbroken security perimeter that is effective for the entire corporation. In addition, each firewall in the organization must follow the same security policy. Otherwise, one firewall might permit one type of transaction to flow into the corporate network that another excludes. The result is an unwanted access that is permitted throughout the corporation because one firewall left a small security door open to the entire network.

NOTES

Firewalls should be stripped of any unnecessary software. Because the firewall computer is used only as a firewall and not as a general-purpose computing machine, only essential operating system software and firewall-specific protection software should remain on the computer. Having fewer software programs on the system should reduce the chances for malevolent software security breaches. Access to a firewall should be restricted to a console physically connected directly to the firewall machine. Otherwise, remote administration of the firewall must be provided, which opens up the possibility of a break in the firewall by an imposter remotely accessing the firewall along the same path that an administrator would use.

Firewalls are classified into the following categories : packet filter, gateway server, and proxy server. **Packet-filter firewalls** examine all data flowing back and forth between the trusted network (within the firewall) and the Internet. Packet filtering examines the source and destination addresses and ports of incoming packets and denies or permits entrance to the packets based on a preprogrammed set of rules.

Gateway servers are firewalls that filter traffic based on the application requested. Gateway servers limit access to specific applications such as Telnet, FTP, and HTTP. Application gateways arbitrate traffic between the inside network and the outside network. In contrast to a packet-filter technique, an application-level firewall filters requests and logs them at the application level, rather than at the lower IP level. A gateway firewall provides a central point where all requests can be classified, logged, and later analyzed. An example is a gateway-level policy that permits incoming FTP requests, but blocks outgoing FTP requests. That policy prevents employees inside a firewall from downloading potentially dangerous programs from the outside.

Proxy server firewalls are firewalls that communicate with the Internet on the private network's behalf. When a browser is configured to use a proxy server firewall, the firewall passes the browser request to the Internet. When the Internet sends back a response, the proxy server relays it back to the browser. Proxy servers are also used to serve as a huge cache for Web pages.

One problem faced by companies that have employees working from home is that the location of computers outside the traditional boundaries of the company's physical site expands the number of computers that must be protected by the firewall. This **perimeter expansion** problem is particularly troublesome for companies that have salespeople using laptop computers to access confidential company information from all types of networks at customer locations, vendor locations, and even public locations, such as airports.

Another problem faced by organizations connected to the Internet is that their servers are under almost constant attack. Crackers spend a great deal

NOTES

of time and energy on attempts to enter the servers of organizations. Some of these crackers use automated programs to continually attempt to gain access to servers. Organizations often install intrusion detection systems as part of their firewalls. **Intrusion detection systems** are designed to monitor attempts to login to servers and analyze those attempts for patterns that might indicate a cracker's attack is underway. Once the intrusion detection system identifies an attack, it can block further attempts that originate from the same IP address until the organization's security staff can examine and analyze the access attempts and determine whether they are an attack.

In addition to firewalls installed on organizations' networks, it is possible to install software-only firewalls on individual client computers. These firewalls are often called **personal firewalls**. The use of personal firewalls, such as **ZoneAlarm**, has become an important tool in the protection of expanded network perimeters for many companies. Many home computer users are installing personal firewalls on their home networks.

ORGANIZATIONS THAT PROMOTE COMPUTER SECURITY

Following the occurrence of the Internet Worm of 1988, a number of organizations were formed to share information about threats to computer systems. These organizations are devoted to the principle that sharing information about attacks and defenses for those attacks can help everyone create better computer security. Some of the organizations began at universities; others were launched by government agencies. In this section, you will learn about some of these organizations and their resources.

CERT

In 1988, a group of researchers met to study the infamous Internet Worm attack soon after it occurred. They wanted to understand how worms worked and how to prevent damage from future attacks of this type. The National Computer Security Center, part of the National Security Agency, initiated a series of meetings to figure out how to respond to future security breaks that might affect thousands of people. Soon after that meeting of security experts in 1988, the U.S. government created the Computer Emergency Response Team and housed it at Carnegie Mellon University in Pittsburgh. The organization is now operated as part of the federally funded Software Engineering Institute at Carnegie Mellon, and it has changed its legal name from the Computer Emergency Response Team (which had been abbreviated to "CERT" by most people who wrote and talked about it) to **CERT.** CERT still maintains an effective and quick communications infrastructure among security experts so that security incidents can be avoided or handled quickly.

NOTES

Today, CERT responds to thousands of security incidents each year and provides a wealth of information to help Internet users and companies become more knowledgeable about security risks. CERT posts alerts to inform the Internet community about security events, and it is regarded as a primary authoritative source for information about viruses, worms, and other types of attacks.

Other Organizations

CERT is the most prominent of these organizations and has formed relationships, such as the **Internet Security Alliance**, with other industry associations. However, CERT is not the only computer security resource. In 1989, one year after CERT was formed, a cooperative research and educational organization called the Systems Administrator, Audit, Network, and Security Institute was launched. Now known as the **SANS Institute**, this organization includes more than 150,000 members who work in computer security consulting firms and information technology departments of companies as auditors, systems administrators, and network administrators.

Many SANS education and research efforts yield resources such as news releases, research reports, security alerts, and white papers that are available on the Web site at no cost. SANS also sells publications to generate funds that it uses for research and educational programs. The SANS Institute operates the **SANS Internet Storm Center**, a Web site that provides current information on the location and intensity of computer attacks throughout the world. Purdue University's Center for Education and Research in Information Assurance and Security **(CERIAS)** is a center for multidisciplinary research and education in information security. The CERIAS Web site provides resources in computer, network, and communications security and includes a section on information assurance. The **Center for Internet Security** is a not-for-profit cooperative organization devoted to helping companies that operate electronic commerce Web sites reduce the risk of disruptions from technical failures or deliberate attacks on their computer systems. It also provides information to auditors who review such systems and to insurance companies that provide coverage for companies who operate such systems. **Microsoft Security Research Group** is a privately sponsored site that offers free information about computer security issues. For current information about computer security, you can visit **CSO Online**, which carries articles that have appeared in CSO Magazine along with other news items related to computer security.

The U.S. government has several Web sites devoted to security enhancement efforts. The **U.S. Department of Justice's Cybercrime** site offers information about computer crimes and intellectual property violations.

NOTES

The U.S. Department of Homeland Security operates the **National Infrastructure Protection Center** (NIPC) Web site, which provides information about threats to U.S. infrastructure, including its computing infrastructure.

Computer Forensics and Ethical Hacking

A small group of firms, endorsed by corporations and security organizations, have the unlikely job of breaking into client computers. Called **computer forensics experts** or **ethical hackers**, these computer sleuths are hired to probe PCs and locate information that can be used in legal proceedings. The field of **computer forensics** is responsible for the collection, preservation, and analysis of computer-related evidence. Ethical hackers are often hired by companies to test computer security safeguards.

STUDENT ACTIVITY

1. Write short notes on Steganography.

2. Explain the difference between asymmetric and symmetric encryption systems.

NOTES

SUMMARY

- Electronic commerce is vulnerable to a wide range of security threats. Attacks against electronic commerce systems can disclose or manipulate proprietary information. The three general assets that companies engaging in electronic commerce must protect are client computers, computer communication channels, and Web servers. Key security provisions in each of these parts of the Web client-Internet-Web server linkage are secrecy, integrity, and available service. Threats to commerce can occur anywhere in the commerce chain. News accounts of virus attacks have kept Web users aware of the security risks to client computers. Antivirus software is also an important element in the protection of client computers. More subtle threats are delivered as client-side applets. Java, JavaScript, and ActiveX controls run on client machines and have the potential to breach security. Cookies, if not controlled and used properly, can present threats to client computers.
- Communication channels, in general, and the Internet, in particular, are especially vulnerable to attacks. The Internet is a vast network and because no control exists over the nodes through which Internet traffic passes, information sent through the Internet is vulnerable to unauthorized disclosure. This can lead to disclosure of private information, alteration of critical business documents, and theft or loss of important business messages. Encryption provides secrecy, and several forms of encryption are available that use hash functions or other more complex algorithms. They include private-key and public-key techniques. Although *public-key encryption eliminates the problem of sharing a secret key, it* is much slower than private-key encryption. Private-key encryption is used during most commerce sessions because it is fast and efficient. Integrity protections ensure that messages between clients and servers are not altered. Digital certificates provide both integrity controls and user authentication. A trusted third party such as a certification authority can provide digital certificates to users and organizations. Several Internet protocols, including Secure Sockets Layer and Secure HTTP, use encryption to provide secure Internet transmission capabilities. As wireless networks have grown to become important parts of the data communication infrastructure, security concerns have increased. Although many wireless networks (especially home networks) are installed without security features, wireless encryption methods that make them more secure are available. Most wireless networks installed in businesses today do have wireless encryption.
- Web servers are susceptible to security threats. Programs that run on servers have the potential to damage databases, abnormally terminate

NOTES

server software, or make subtle changes in proprietary information. Attacks can come from within the server in the form of programs, or they can come from outside the server. One type of external attack can occur when a message overflows a server's internal storage region and overwrites crucial information. Overwritten information is replaced with either data or instructions that cause other programs on the server to execute. Backup copies of servers provide redundancy in the case of a physical threat to a server. The Web server must be protected from both physical threats and Internet-based attacks on its software. Protections for the server include access control and authentication, provided by username and password login procedures and client certificates. Firewalls can be used to separate trusted inside computer networks and clients from untrusted outside networks, including other divisions of a company's enterprise network system and the Internet.

A number of organizations have been formed to share information about computer security threats and defenses. CERT, the SANS Institute, and similar organizations address security outbreaks by linking knowledgeable security experts. When large security outbreaks occur, the members of these organizations join together and discuss methods to locate and eliminate the threat. Computer forensics firms that undertake attacks against their clients' computers can play an important role in helping identify security weaknesses.

KEY TERMS

Access control list (ACL)
Active content
Active wiretapping
ActiveX
Advanced Encryption Standard (AES)
Antivirus software
Applet
Asymmetric encryption
Backdoor
Biometric security device
Black hat hacker
Buffer
Buffer overrun (buffer overflow)
Certification authority (CA)
Cipher text
Collision
Computer forensics
Computer forensics expert
Computer security
Cookie blocker
Countermeasure
Cracker
Cryptography
Cybervandalism
Data Encryption Standard (DES)
Decrypted

NOTES

Decryption program
Dictionary attack program
Digital certificate (digital ID)
Digital signature
Domain name server (DNS)
Eavesdropper
Encryption
Encryption algorithm
Encryption program
Ethical hacker
Firewall
First-party cookies
Gateway server
Hacker
Hash algorithm
Hash coding
Hash value
Integrity
Integrity violation
Intrusion detection system
Java sandbox
JavaScript
Key
Logical security
Macro virus
Mail bomb
Man-in-the-middle exploit
Masquerading (spoofing)
Message digest
Multivector virus
Necessity
Necessity threat (delay, denial, or denial-of-service threat)
One-way function
Open session
Packet-filter firewall
Perimeter expansion
Persistent cookie
Personal firewall
Phishing expeditions
Physical security
Plain text
Plug-ins
Pretty Good Privacy (PGP)
Privacy
Private key
Private-key encryption
Proxy server firewall
Public key
Public-key encryption
Scripting language
Secrecy
Secure envelope
Secure Sockets Layer
Security policy
Session cookie
Session key
Signed (message or code)
Sniffer program
Stateless connection
Steganography
Symmetric encryption
Third-party cookies
Threat
Triple Data Encryption Standard (Triple DES, 3DES)
Trojan horse
Trusted (network)
Untrusted (network)

Untrusted Java applet
Warchalking
Wardrivers
Web bug
White hat hacker
Worm
Zombie.

NOTES

SELF ASSESSMENT QUESTIONS

1. In about 200 words, explain why Web sites use cookies. In your answer, discuss the reasons that cookies were first devised and explain where cookies are stored. You can use the links in the Online Companion to help with your research.
2. In about 100 words, describe steganography and explain its connection to the topic of online security. You can use the links in the Online Companion to help with your research.
3. In about 200 words, explain the differences between public-key encryption and private-key encryption. List advantages and disadvantages of each encryption method. Explain which method you would use for e-mail sent from a field sales office to corporate headquarters. Assume that the e-mail regularly includes highly confidential information about upcoming sales opportunities.
4. In about 300 words, describe the security threats that a company will face when it implements a wireless network. Assume that the company occupies the six middle floors in a 12-story office building that is located in a downtown business area between two other buildings of similar height. Briefly explain how the company could reduce the risks it faces.

❑❑❑

SECTION C

NOTES

UNIT 3 ELECTRONICS PAYMENT SYSTEMS

★ LEARNING OBJECTIVES ★

- Introduction
- Online Payment Basics
- Payment Cards
- Electronic Cash
- Electronic Wallets
- Stored-Value Cards
- Intrernet Technologies and the Banking Industry

INTRODUCTION

In 1991, a teenager named Max Levchin immigrated from the Ukraine to the United States. Settling in Chicago, Levchin had a burning interest in cryptography. Growing up in a Soviet police state convinced him that the ability to send coded messages that could not be read or intercepted was both important and useful. He majored in computer science at the University of Illinois and spent many hours at the school's **Center for Supercomputing**, pursuing his passion for making and breaking codes. When he graduated in 1998, he wanted to follow the American dream of turning his knowledge into money, so he headed for the heart of the computer industry in Palo Alto, California. Levchin's plan to build the ultimate transmission encryption scheme has not yet panned out, but he has managed to turn his knowledge into a successful business. As cofounder and chief technical officer of **PayPal**, an online payment processing company that you will learn about in this chapter, Levchin has used his expertise in cryptography and computer security to protect the firm from losses that could destroy it.

PayPal, founded in 1999, operates a service that lets people exchange money over the Internet. It has become the most used payment system for clearing

NOTES

auction transactions on eBay. People can also use PayPal to send money to anyone who has an e-mail address and to receive money.

PayPal charges very small fees to business users and no fees at all to individuals, so its profit margins are small. However, it has grown so rapidly that its thin profit margins are realized on a very large number of users. A single, well-organized, large-scale fraud attack on PayPal, however, could put the company out of business quickly. Levchin's current contribution to the company's success is his development of payment surveillance software that continually monitors PayPal transactions. The software searches millions of transactions as they occur every day and looks for patterns that might indicate fraud. The software notifies PayPal managers immediately when it finds something suspicious.

The software appears to be working very well. Companies that process credit card transactions have experienced much larger fraud occurrence rates on the Web (about 1.13 percent) than in physical stores (about.70 percent). PayPal claims to have kept its fraud rate below.50 percent. As long as PayPal can keep its fraud rate low, it can continue to charge lower transaction fees than its competitors and still make a profit. Some industry observers believe that PayPal's ability to avoid high fraud rates could make it a serious competitor to banks in other areas of financial transaction handling, such as credit card processing.

PayPal's largest customer group has always been the participants (buyers and sellers) on the auction Web site eBay. As you will learn in this chapter, eBay spent three years working to establish its own payments service that could compete effectively with PayPal. In October 2002, eBay finally gave up and bought PayPal for $1.4 billion. PayPal continues to offer payment services under its own name as a division of eBay.

ONLINE PAYMENT BASICS

An important function of electronic commerce sites is the handling of payments over the Internet. Most electronic commerce involves the exchange of some form of money for goods or services. As you learned in Chapter 5, many companies use electronic funds transfers (EFTs) or financial EDI to make online payments. In this chapter, you will learn about a number of online payment alternatives that are available to individual consumers.

Online payment systems for consumer electronic commerce are still evolving. A number of proposals and implementations of payment systems currently compete for dominance. Regardless of format, electronic payments are far cheaper than mailing paper checks. Electronic payments can be convenient for customers and can save companies money. Estimates of the cost of billing one person by mail range between $1 and $1.50. Sending bills and receiving

NOTES

payments over the Internet can drop the transaction cost to an average of 50 cents per bill. The total savings is huge when the unit cost is multiplied by the number of customers who could use electronic payment. For example, a telephone company in a major metropolitan area might have 5 million customers, each of whom receives a bill every month. In one year, a savings of 50 cents on each of those 60 million bills adds up to about $30 million. The environmental impact is also significant. Those 60 million paper bills weigh about 1.7 million pounds. It takes 2200 trees to make that much paper—along with the energy consumed and the wastes generated in the paper-making process.

Today, four basic ways to pay for purchases dominate both traditional and electronic business-to-consumer commerce. Cash, checks, credit cards, and debit cards account for more than 90 percent of all consumer payments in the United States. A small but growing percentage of consumer payments are made by electronic transfer. The most popular consumer electronic transfers are automated payments of auto loans, insurance payments, and mortgage payments made from consumers' checking accounts. Figure 3.1 shows the estimated proportions of the $6.7 trillion in payments projected for 2005 in the United States for all types of consumer commerce, online and offline.

Credit cards are by far the most popular method that consumers use to pay for online purchases. Recent surveys have found that more than 85 percent of worldwide consumer Internet purchases are paid for with credit cards. In the United States, the proportion is about 96 percent.

Another payment medium is limited-use scrip. **Scrip** is digital cash minted by a company instead of by a government. Most scrip cannot be exchanged for cash; it must be exchanged for goods or services by the company that issued the scrip. Scrip is like a gift certificate that is good at more than one store. In the early days of the Web, many experts predicted that scrip would become a popular way of making payments for consumer goods and services

Type	Number of transactions	Dollar value of transactions
Cash	35%	15%
Checks	21%	32%
Credit cards	19%	26%
Debit cards	17%	12%
Electronic transfers	5%	11%
Other	3%	4%

Adapted from Table 1182, 2004-2005 Statistical Abstract of the United States, Washington, D.C.: U.S. Census Bureau, p. 746.

Figure 3.1. *Payment methods for all types of U.S. consumer transactions, 2005 projections*

NOTES

services online. Unfortunately for many investors and at least two companies (see the Learning from Failures feature), this turned out not to be true. Most current scrip offerings, such as **eScrip**, focus on the not-for-profit fundraising market. This market consists mainly of primary and secondary schools in the United States.

Merchants should offer their customers payment options that are safe, convenient, and widely accepted. The key is to determine which choices work the best for the company and its customers. The information in this chapter will help you make those decisions. Companies such as Payment Online, shown in Figure 3.2, sell packages of payment processing services to Web merchants that allow those merchants to accept several different types of payments.

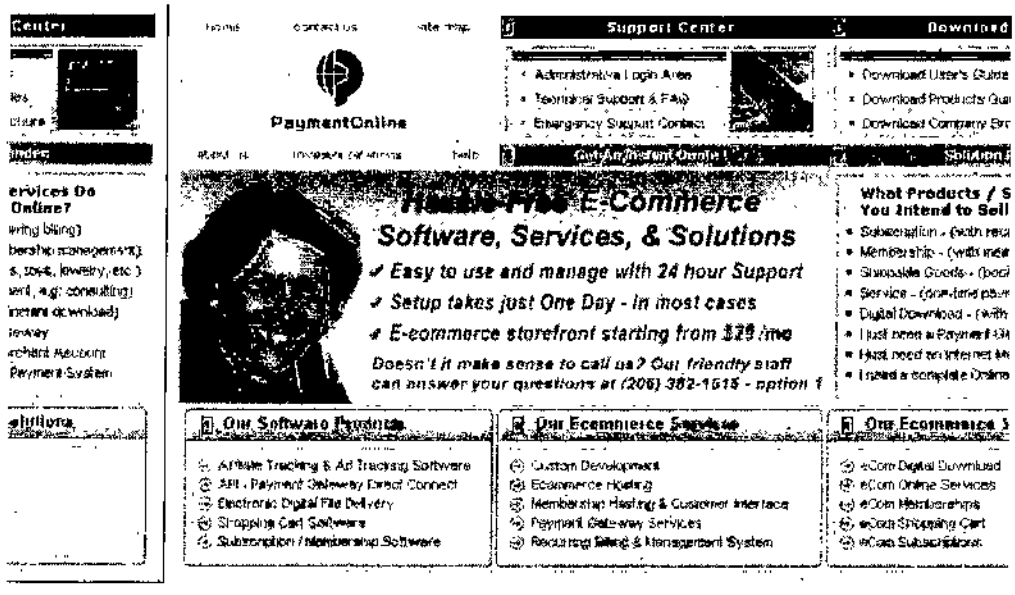


Figure 3.2. *Payment processing service offerings of Payment Online.*

You will learn about four different payment technologies in this chapter : payment cards, electronic cash, software wallets, and smart cards (also called stored-value cards). Each technology has unique properties, costs, advantages, and disadvantages. Some are methods that are already popular and widely accepted; others are only beginning to catch on and have an unclear future. All of these electronic payment methods can work well for B2C Web commerce sites.

PAYMENT CARDS

Businesspeople often use the term **payment card** as a general term to describe all types of plastic cards that consumers (and some businesses) use

NOTES

to make purchases. The main categories of payment cards are credit cards, debit cards, and charge cards.

A **credit card**, such as a **Visa** or a **MasterCard**, has a spending limit based on the user's credit history; a user can pay off the entire credit card balance or pay a minimum amount each billing period. Credit card issuers charge interest on any unpaid balance. Many consumers already have credit cards, or are at least familiar with how they work. Credit cards are widely accepted by merchants around the world and provide assurances for both the consumer and the merchant. A consumer is protected by an automatic 30-day period in which he or she can dispute an online credit card purchase. Merchants that already accept credit cards in an offline store can accept them immediately for online payment because they already have established a mechanism for accepting credit card payments. Online credit card purchases are similar to telephone purchases in that the card holder is not present and cannot provide proof of identity as easily as he or she can when standing at the cash register. Online and telephone purchases are often called **card not present transactions** and both require an extra degree of security.

A debit card looks like a credit card, but it works quite differently. Instead of charging purchases against a credit line, a **debit card** removes the amount of the sale from the cardholder's bank account and transfers it to the seller's bank account. Debit cards are issued by the cardholder's bank and usually carry the name of a major credit card issuer, such as Visa or MasterCard, by agreement between the issuing bank and the credit card issuer. By branding their debit cards (with the Visa or MasterCard name), banks ensure that their debit cards will be accepted by merchants who recognize the credit card brand names.

A **charge card**, offered by companies such as **American Express**, carries no spending limit, and the entire amount charged to the card is due at the end of the billing period. Charge cards do not involve lines of credit and do not accumulate interest charges. (Note : In addition to its charge card products, American Express also offers credit cards, which do have credit limits and which do accumulate interest on unpaid balances.) In the United States, many retailers, such as department stores and oil companies that own gas stations, issue their own charge cards. In the rest of this chapter, the term "payment card" refers to credit cards, debit cards, and charge cards.

Many consumers have concerns about providing their payment card numbers to vendors online, especially when the vendor is unknown to them. To address this concern, several payment card companies now offer cards with disposable numbers. These cards, sometimes called **single-use cards**, give consumers a unique card number that is valid for one transaction only. This prevents an unscrupulous vendor from using the card number to complete unauthorized

NOTES

transactions on the consumer's account or selling the card number to others. In 2000, American Express was the first to offer single-use cards. A few other card issuers followed suit, but the number of companies that offer single-use cards continues to be small. Neither Visa nor MasterCard have required all of their issuing banks to provide single-use cards; the only major issuing banks to do so are MBNA and Citigroup. J.P. Morgan offers a single-use version of its Discover card. In 2004, American Express stopped offering its single-use card, but many industry analysts believe that consumer interest in these types of cards will continue to grow. The problem with single-use cards thus far has been that they require consumers to behave differently and not enough consumers see the benefit of learning how to use this new product. As concerns over stolen credit card numbers increase, this benefit could become compelling.

Advantages and Disadvantages of Payment Cards

Payment cards have several features that make them an attractive and popular choice with both consumers and merchants in online and offline transactions. For merchants, payment cards provide fraud protection. When a merchant accepts payment cards for online payment or for orders placed over the telephone, the merchant can authenticate and authorize purchases using a payment card processing network. For U.S. consumers, payment cards are advantageous because the Consumer Credit Protection Act limits the cardholder's liability to $50 if the card is used fraudulently. Once the cardholder notifies the card's issuer of the card theft, the cardholder's liability ends. Frequently, the payment card's issuer waives the $50 consumer liability when a stolen card is used to purchase goods. Some other countries have similar laws, but this type of protection is not common for holders of credit cards issued outside the United States. The lack of this type of protection does limit the willingness of non-U.S. consumers to use payment cards for online purchases.

Perhaps the greatest advantage of using payment cards is their worldwide acceptance. Payment cards can be used anywhere in the world, and the currency conversion, if needed, is handled by the card issuer. For online transactions, payment cards are particularly advantageous. When a consumer reaches the electronic checkout, he or she enters the payment card number and his or her shipping and billing information in the appropriate fields to complete the transaction. The consumer does not need any special hardware or software to complete the transaction.

Payment cards have one significant disadvantage for merchants when compared to cash. Payment card service companies charge merchants per-transaction fees and monthly processing fees. These fees can add up, but merchants view them as a cost of doing business. Any merchant that does

NOTES

not accept payment cards for purchases risks losing a significant portion of sales to other merchants that do accept payment cards. The consumer pays no direct transaction-based fees for using payment cards, but the prices of goods and services are slightly higher than they would be in an environment free of payment cards. Most consumers also pay an annual fee for credit cards and charge cards. This annual fee is much less common on debit cards.

Payment cards provide built-in security for merchants because merchants have a higher assurance that they will be paid through the companies that issue payment cards than through the sometimes slow direct invoicing process. To process payment card transactions, a merchant must first set up a merchant account. The series of steps in a payment card transaction is usually transparent to the consumer. Several groups and individuals are involved : the merchant, the merchant's bank, the customer, the customer's bank, and the company that issued the customer's payment card. All of these entities must work together for customer charges to be credited to merchant accounts (and vice versa when a customer receives a payment card credit for returned goods).

Payment Acceptance and Processing

Most people are familiar with the use of payment cards : In a physical store, the customer or a sales clerk runs the card through the online payment card terminal and the card account is charged immediately. The process is slightly different on the Internet, although the purchase and charge processes follow the same rules. Payment card processing has been made easier over the past two decades because Visa and MasterCard, along with MasterCard's international affiliate, **MasterCard International** (formerly known as Europay), have implemented a single standard for the handling of payment card transactions called the **EMV standard** (EMV is derived from the names of the companies : Europay, MasterCard, and Visa).

In a brick-and-mortar store, customers walk out of the store with purchases in their possession, so charging and shipment occur nearly simultaneously. Online stores and mail order stores in the United States must ship merchandise within 30 days of charging a payment card. Because the penalties for violating this law can be significant, most online and mail order merchants do not charge payment card accounts until they ship merchandise. Payment card transactions follow these general steps once the merchant receives a consumer's payment card information,

1. The merchant authenticates the payment card to ensure it is valid and not stolen.
2. The merchant checks with the payment card issuer to ensure that credit or funds are available and puts a hold on the credit line or the funds needed to cover the charge.

NOTES

3. Settlement occurs, usually a few days after the purchase, which means that funds travel between banks and are placed into the merchant's account.

Open and Closed Loop Systems

In some payment card systems, the card issuer pays the merchants that accept the card directly and does not use an intermediary, such as a bank or clearinghouse system. These types of arrangements are called **closed loop systems** because no other institution is involved in the transaction. American Express and Discover Card are examples of closed loop systems.

Open loop systems involve three or more parties. Suppose an Internet shopper uses his or her Visa card issued by the First Bank of Woodland to purchase an item from Web Wonders, whose bank account is at the Hackensack Commerce Bank. The banking system includes one or more intermediary banks that coordinate the transfer of funds from the First Bank of Woodland to the Hackensack Commerce Bank. Whenever a third party, such as the intermediary banks in this example, processes a transaction, the system is called an **open loop system**. Systems using Visa or MasterCard are the most visible examples of open loop systems. Many banks issue both cards. Unlike American Express or Discover, neither Visa nor MasterCard issues cards directly to consumers. Visa and MasterCard are **credit card associations** that are operated by the banks who are members in the associations. These member banks, which are also called **customer issuing banks**, issue credit cards to individual consumers and are responsible for establishing customer credit limits.

Merchant Accounts

A **merchant bank** or **acquiring bank** is a bank that does business with sellers (both Internet and non-Internet) that want to accept payment cards. In other words, to process payment cards for Internet transactions, an online merchant must set up a **merchant account**. When the merchant's bank collects credit card receipts on behalf of the merchant from the payment card issuer, it credits their value to the merchant's account.

A merchant must provide business information before the bank will provide an account through which the merchant can process payment card transactions. Typically, a new merchant must supply a business plan, details about existing bank accounts, and a business and personal credit history. The merchant bank wants to be sure that the merchant has a good prospect of staying in business and wants to minimize its risk. An online merchant that appears disorganized is less attractive to a merchant bank than a well-organized online merchant.

NOTES

The type of business also influences the bank's likelihood of granting the account. In some industries, merchant banks will be reluctant to offer a merchant account because of the type of business; some businesses have a higher likelihood of customers repudiating payment card charges than others. For example, a business that sells a guaranteed weight loss scheme—a business in which many customers might want their money back—will find many merchant banks unwilling to provide an account. The bank assesses the level of risk in the business based on the type of business and the credit information that is provided. Merchant banks must estimate what percentage of sales are likely to be contested by cardholders. When a cardholder successfully contests a charge, the merchant bank must retrieve the money it placed in the merchant account in a process called a **chargeback**. To ensure that sufficient funds are available to cover chargebacks, a merchant bank might require a company to maintain funds on deposit in the merchant account. For example, a new or risky business that plans to make $100,000 in sales each month might be required to keep $50,000 or more on deposit in its merchant account.

One problem facing online businesses is that the level of fraud in online transactions is much higher than either in-person or telephone transactions of the same nature (that is, the same amount and the same type of good or service being purchased). Fewer than 5 percent of all credit card transactions are completed online, but those transactions are responsible for about 50 percent of the total dollar amount of credit card fraud. A Celent Communications study reported in Credit Card Management (see the reference in the For Further Study and Research section at the end of this chapter) has projected that online credit card fraud will be over $2 billion by 2007 and will amount to 62 percent of all credit card fraud.

Several third-party Internet and Web-based services are available to handle all the details of processing payment card transactions. The next section discusses payment card processing options for Internet stores.

Processing Payment Cards Online

Software packaged with electronic commerce software can handle payment card processing automatically, or merchants can contract with a third party to handle payment card processing. Several companies, called **payment processing service providers**, offer these services. **InternetSecure**, for example, allows merchants to concentrate on business while it provides secure payment card services. InternetSecure supports payments with Visa and MasterCard for Canadian and United States accounts. The company provides risk management and fraud detection and handles transactions from online merchants using existing, bank-approved payment card processing

NOTES

infrastructure, secure links, and firewalls. InternetSecure notifies the merchant of all approved orders and also supplies authorization codes to buyers of digital content, who can download their purchases upon payment card approval. InternetSecure ensures that the transactions it processes are credited to the correct merchant's account.

First Data provides merchant payment card processing services with the **ICVERIFY** and **WebAuthorize** programs. ICVERIFY is intended for small retailers that use Microsoft Windows electronic cash registers and point-of-sale terminal systems. WebAuthorize is for large enterprise-class merchant sites.

Services such as ICVERIFY and WebAuthorize connect directly to a network of banks called the **Automated Clearing House (ACH)** and to credit card authorization companies. You can learn more about ACHs by following the Online Companion links to the **Electronic Payments Network**, **NACHA-The Electronic Payments Association**, **The Clearing House**, and the U.S. Federal Reserve Bank's **FedACH** site. Banks connect to an ACH through highly secure, private leased telephone lines. The merchant sends the card information to a payment card authorization company, which reviews the customer account and, if it approves the transaction, sends the credit authorization to the issuing bank. Then the issuing bank deposits the money in the merchant's bank account through the ACH. The merchant's Web site receives confirmation of the acceptance of the consumer transaction. After receiving notification of acceptance or rejection of the transaction, the merchant Web site confirms the sale to the customer over the Internet. In addition, the merchant site usually sends an e-mail confirmation of the sale to the consumer with details about the purchase price and shipping information.

Other payment card processing companies include VeriSign's **PayFlow Link** system and InfoSpace's **Authorize.Net**. PayFlow is an online payment system developed by Cyber-Cash that is now operated by VeriSign. Authorize.Net is an online, real-time payment card processing service that allows merchants to link their sites to the Authorize.Net system by simply inserting a small block of HTML code into their transaction page. With Authorize.Net, a customer's order is encrypted and transferred to the Authorize.Net server. The server, in turn, relays the transaction to a bank network through a private leased line. Merchants must have an Authorize.Net account to use the service. Customers are usually not aware that the transaction is being handled by a third-party supplier. Check the Online Companion links for more details about these services.

ELECTRONIC CASH

NOTES

Although credit cards dominate online payments today, electronic cash shows promise for the future. **Electronic cash** (also called e-cash or digital cash) is a general term that describes any value storage and exchange system created by a private (nongovernmental) entity that does not use paper documents or coins and that can serve as a substitute for government-issued physical currency. A significant difference between electronic cash and scrip is that electronic cash can be readily exchanged for physical cash on demand. Because electronic cash is issued by private entities, there is a need for common standards among all electronic cash issuers so that one issuer's electronic cash can be accepted by another issuer. This need has not yet been met. Each issuer has its own standards and electronic cash is not universally accepted, as is government-issued physical currency.

As you learned in the previous section, banks that issue credit cards make money by charging merchants a processing fee on each transaction. This fee ranges from 1 percent to 4 percent of the value of the transaction. Often, banks impose a minimum fee of 20 cents or more per transaction. Many banks charge electronic commerce sites more than similar brick-and-mortar stores—up to $1 more per credit card transaction. The cost of an online transaction can be 50 percent higher than the cost to process the same transaction for a brick-and-mortar retailer.

Many stores that accept credit cards require a minimum purchase amount of $10 or $15. Merchants impose a minimum purchase amount because the bank fees for small purchase amounts would be greater than the profits on those transactions. The same is true for Internet purchases. Small purchases are not profitable for merchants that accept only credit cards for payment. There is a market for small purchases on the Internet—purchases below $10. This is one potentially significant market for electronic cash. With very low fixed costs, electronic cash provides the promise of allowing users to spend, for example, 50 cents for an online newspaper, or 80 cents to send an electronic greeting card.

Electronic cash has another factor in its favor : Most of the world's population do not have credit cards. Many adults cannot obtain credit cards due to minimum income requirements or past debt problems. Children and teens—eager purchasers representing a significant percentage of online buyers—are ineligible, simply because they are too young. People living in most countries other than the United States hold few credit cards because they have traditionally made their purchases in cash. For all of these people, electronic cash provides the solution to paying for online purchases.

NOTES

Even though there have been many failures in the last few years in electronic cash introductions, the idea of electronic cash just refuses to die. Electronic cash shows particular promise in two applications : the sale of goods and services priced less than $10—the lower threshold for credit card payments—and the sale of all goods and services to those without credit cards.

Micropayments and Small Payments

Internet payments for items costing from a few cents to approximately a dollar are called **micropayments**. Micropayment champions see many applications for such small transactions, such as paying 5 cents for an article reprint or 25 cents for a complicated literature search. However, micropayments have not been implemented very well on the Web yet. Another barrier to micropayments is a matter of human psychology. Researchers have found in a number of studies that many people prefer to buy small value items in fixed price chunks rather than in individual small increments, even when buying the small increments would cost less money overall. A good example of this behavior is the preference most mobile telephone users have for fixed monthly payment plans over charges based on minutes used. The comfort of knowing the exact amount of the monthly bill is more important to many people than getting the lowest price on the minutes used.

The payments that are between $1 and $10 do not have a generally accepted name (some industry observers use the term micropayment to describe any payment of less than $10); in this book, the term **small payments** will be used to include all payments of less than $10.

Two companies now offer products for handling small payments that use credit cards as an alternative to electronic cash. The logic behind these products is that credit cards are more widely accepted than electronic cash. **Yaga** has targeted its product to large media companies such as Hearst, Time, and Ziff-Davis. These companies want to sell copies of articles from their publications, but the transaction fees charged by credit card processors make such sales unprofitable. Yaga accumulates charges made by an individual and then processes them in one lump sum at the end of a month or longer period. If a site visitor obtained six articles in a month, Yaga allows the site to process a credit card charge once (incurring just one transaction fee) instead of six times. **BitPass** targets smaller content providers—individual authors and musicians—by offering site visitors an account that they can draw against at any BitPass participating site. A customer authorizes BitPass to make a small (usually $3) charge to the customer's credit card to create that customer's BitPass account. The customer can then draw down the BitPass account at participating content vendor sites.

NOTES

Privacy and Security of Electronic Cash

All electronic payment schemes have issues that must be resolved satisfactorily to allay consumers' fears and give them confidence in the technology. Concerns about electronic payment methods include privacy and security, independence, portability, and convenience. Privacy and security questions are probably the most important issues that have to be addressed with any payment system to be used by consumers. Consumers want to know whether transactions are vulnerable and whether the electronic currency can be copied, reused, or forged.

Electronic cash has unique security problems. Electronic cash should have two important characteristics in common with physical currency. First, it must be possible to spend electronic cash only once, just as with traditional currency. Second, electronic cash ought to be anonymous, just as hard currency is. That is, security procedures should be in place to guarantee that the entire electronic cash transaction occurs only between two parties, and that the recipient knows that the electronic currency being received is not counterfeit or being used in two different transactions. Ideally, consumers should be able to use electronic cash without revealing their identities—this prevents sellers from collecting information about individual or group spending habits. Companies in the electronic cash business include **eCharge** and **Valista.**

Electronic cash has the advantages of being independent and portable. When electronic cash is independent, it is unrelated to any network or storage device. That is, electronic cash is really not free-floating currency if its existence depends on a particular proprietary storage mechanism that is specially designed to hold one type of electronic cash. Electronic cash should ideally be able to pass transparently across international borders and be converted automatically to the recipient country's currency. Electronic cash portability means that it must be freely transferable between any two parties. Credit and debit cards do not possess this property of portability or transferability between every combination of two parties. In a credit card transaction, the payment recipient must already have a merchant account established with a bank. A merchant account is not required for a business to receive electronic cash.

Perhaps the most important characteristic of cash is convenience. If electronic cash requires special hardware or software, it is not convenient for people to use. Chances are good that people will not adopt an electronic cash system that is difficult to use.

Holding Electronic Cash : Online and Offline Cash

Two widely accepted approaches to holding cash exist today : online storage and offline storage. Online cash storage means that the consumer does not

NOTES

personally possess electronic cash. Instead, a trusted third party—an online bank—is involved in all transfers of electronic cash and holds the consumers' cash accounts. Online systems work by requiring merchants to contact the consumer's bank to receive payment for a consumer purchase, which helps prevent fraud by confirming that the consumer's cash is valid. This resembles the process of checking with a consumer's bank to ensure that a credit card is still valid and that the consumer's name matches the name on the credit card.

Offline cash storage is the virtual equivalent of money kept in a wallet. The customer holds it, and no third party is involved in the transaction. Protection against fraud is still a concern, so either hardware or software safeguards must be used to prevent fraudulent or double-spending. **Double-spending** is spending a particular piece of electronic cash twice by submitting the same electronic currency to two different vendors. By the time the same electronic currency clears the bank for a second time, it is too late to prevent the fraudulent act. The encryption techniques used to prevent double-spending are described later in this unit.

Advantages and Disadvantages of Electronic Cash

Billing for goods and services that customers purchase is part of any business. Traditional billing methods in the brick-and-mortar paradigm are costly and involve generating invoices, stuffing envelopes, buying and affixing postage to the envelopes, and sending the invoices to the customers. Meanwhile, the Accounts Payable Department must keep track of incoming payments, post accounts in the database, and ensure that customer data is current.

Online stores have many of the same payment collection inefficiencies as their brick-and-mortar cousins. Most online customers use credit cards to pay for their purchases. Online auction customers also use conventional payment methods, including checks and money orders. Electronic cash systems, though less popular than other payment methods, provide advantages and disadvantages that are unique to electronic cash.

For the most part, electronic cash transactions are more efficient (and therefore less costly) than other methods, and that efficiency should foster more business, which eventually means lower prices for consumers. Transferring electronic cash on the Internet costsless than processing credit card transactions. Conventional money exchange systems require banks, bank branches, clerks, automated teller machines, and an electronic transaction system to manage, transfer, and dispense cash. Operating this conventional money exchange system is expensive.

Electronic cash transfers occur on an existing infrastructure—the Internet—and through existing computer systems. Thus, the additional costs that

NOTES

users of electronic cash must incur are nearly zero. Because the Internet spans the globe, the distance that an electronic transaction must travel does not affect cost. When considering moving physical cash and checks, distance and cost are proportional—the greater the distance that the currency has to go, the more it costs to move it. However, moving electronic currency from Los Angeles to San Francisco costs the same as moving it from Los Angeles to Hong Kong. Merchants can pay other merchants in a business-to-business relationship, and consumers can pay each other. Electronic cash does not require that one party obtain an authorization, as is required with credit card transactions.

Electronic cash does have disadvantages, and they are significant. Using electronic cash provides no audit trail. That is, electronic cash is just like real cash in that it cannot be easily traced. Because true electronic cash is not traceable, another problem arises : money laundering. **Money laundering** is a technique used by criminals to convert money that they have obtained illegally into cash that they can spend without having it identified as the proceeds of an illegal activity. Money laundering can be accomplished by purchasing goods or services with ill-gotten electronic cash. The goods are then sold for physical cash on the open market.

Just as physical currency can be counterfeited, electronic cash is susceptible to forgery. However, it is much more difficult to forge electronic cash than it is to use a fraudulently obtained credit card number. There are several other potentially damaging digital economic factors that might result from the use of electronic cash. These factors have to do with the expansion of the money supply when banks loan electronic cash on consumer and merchant accounts in traditional bank accounts. You can learn more about these economic factors by following the links to **Understanding the Digital Economy** and **The Economic and Social Impacts of Electronic Commerce** in the Online Companion.

Electronic cash has been successful in some parts of the world, but it has not yet become a global commercial success. Making electronic cash a popular alternative payment system requires wide acceptance and a solution to the problems of multiple electronic cash standards. Customers do not want to have to carry a dozen different brands of electronic cash to be able to purchase goods from a majority of the merchants that accept electronic cash. Establishing electronic cash as a popular payment method requires that a standard be developed for electronic cash disbursement and acceptance—a standard that individual vendors then implement for their individual electronic cash systems. Electronic cash from different vendors must be easily interchangeable so that customers can exchange one cash type for another when needed.

NOTES

How Electronic Cash Works

To begin using electronic cash, a consumer opens an account with an electronic cash issuer (such as a bank that issues electronic cash or a private vendor of electronic cash, such as PayPal) and presents proof of identity. The consumer can then withdraw electronic cash by accessing the issuer's Web site and presenting proof of identity, such as a digital certificate issued by a certification authority, or a combination of a credit card number and a verifiable bank account number. After the issuer verifies the consumer's identity, it gives the consumer a specific amount of electronic cash and deducts the same amount from the consumer's account. In addition, the issuer might charge a small processing fee. The consumer can store the electronic cash in an electronic wallet (described later in this chapter) on his or her computer, or on a stored-value card (also described later in this chapter). In addition, the consumer can authorize the issuer to make payments to third parties from the electronic cash account.

Providing Security for Electronic Cash

You have already learned about one significant problem with electronic cash : its potential for double-spending. The main deterrent to double-spending is the threat of detection and prosecution. Cryptographic algorithms are the keys to creating tamperproof electronic cash that can be traced back to its origins. A two-part lock provides anonymous security that also signals when someone is attempting to double-spend cash. When a second transaction occurs for the same electronic cash, a complicated process comes into play that reveals the attempted second use and the identity of the original electronic cash holder. Otherwise, electronic cash that is used correctly maintains a user's anonymity. This double-lock procedure protects the anonymity of electronic cash users and simultaneously provides built-in safeguards to prevent double-spending. Figure 3.3 shows a graphic representation of this double-spending detection process using a double-lock system.

Double-spending can neither be detected nor prevented with truly anonymous electronic cash. **Anonymous electronic cash** is electronic cash that bills and coins, cannot be traced back to the person who spent it. One way to be able to trace electronic cash is to attach a serial number to each electronic cash transaction. That way, cash can be positively associated with a particular consumer. That does not solve the double-spending problem, however. Although a single issuing bank could detect whether two deposits of the same electronic cash are about to occur, it is impossible to ascertain who is at fault in such a situation—the consumer or the merchant. Of course, electronic cash that contains serial who is at fault in such numbers is no

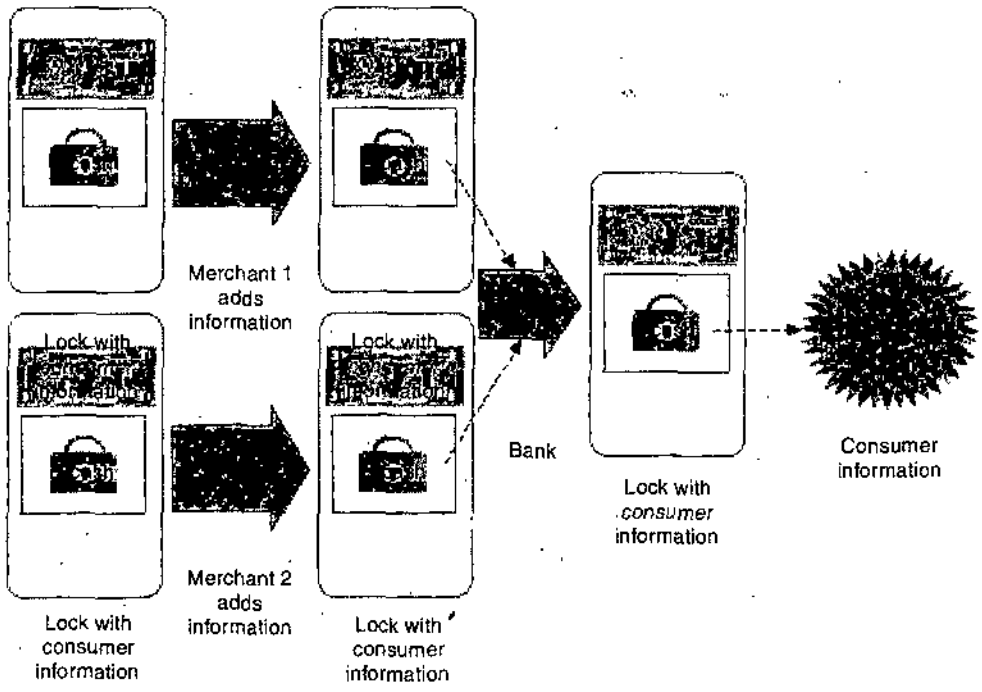


Figure 3.3. *Detectingc double spending of electronic cash.*

longer anonymous, and anonymity is one reason to acquire electronic cash in the first place. Electronic cash containing serial numbers also raises a number of privacy issues, because merchants could use the serial numbers to track spending habits of consumers.

Creating truly anonymous electronic cash requires a bank to issue electronic cash with embedded serial numbers such that the bank can digitally sign the electronic cash while removing any association of the cash with a particular customer. The process begins when a consumer creates a random serial number that he or she sends to the bank issuing the electronic cash. The bank uses the consumer's random serial number along with the bank's digital signature and sends the random number, electronic cash, and digital signature as one package back to the user. When the user receives the electronic cash bundle, the user extracts the original random serial number and keeps the bank's digital signature. The consumer can now spend the electronic cash, which is digitally signed by the bank. When the consumer spends the electronic cash and the merchant passes it along to the issuing bank, the bank validates the electronic cash because it contains the bank's digital signature. However, the bank cannot determine the identity of the spender. It only knows that the electronic cash is genuine.

Electronic Cash Systems

Electronic cash has not been nearly as successful in the United States as it has been in Europe and Japan. In the United States, most consumers have

NOTES

credit cards, debit cards, charge cards, and checking accounts. These payment alternatives work well for U.S. consumers in both online and offline transactions. In most other countries of the world, consumers overwhelmingly prefer to use cash. Because cash does not work well for online transactions, electronic cash fills an important need for consumers in those countries as they conduct B2C electronic commerce. This type of need does not exist in the United States because U.S. consumers already use payment cards for traditional commerce, and these payment cards work well for electronic commerce.

KDD Communications (KCOM) is the Internet subsidiary of Kokusai Denshin Denwa, which is Japan's largest global phone company. KCOM has its own NetCoin electronic cash system and offers electronic cash through its NetCoin Center. Shoppers can go to the Net-Coin Center and obtain electronic cash that can be stored on their computers. Then, they can shop online for recipes or travel directories, or download MP3 music for less than a dollar per song. Other content providers, such as Japanese newspapers, provide access to their newspaper archives and charge a small fee to retrieve articles. Japan even has a donation site where visitors can donate electronic coins to charitable organizations.

Specific reasons for past failures of electronic cash systems in the United States are not completely clear. Some industry observers blame the failure on the way that many electronic cash systems were implemented. Most of these systems required the user to download and install complicated client-side software that ran in conjunction with the browser. Also, there were a number of competing technologies; therefore, no standards were ever developed for the entire electronic cash system. The absence of electronic cash standards means that consumers are faced with choosing from an array of proprietary electronic cash alternatives—none of which are interoperable. Interoperable software runs transparently on a variety of hardware configurations and on different software systems.

Despite their rough start, not all electronic cash ventures have failed. Next, you will learn about some of the Internet companies that currently offer electronic cash services and bill presentment and payment systems.

CheckFree

CheckFree, the largest online bill processor in the world, provides online payment processing services to both large corporations and individual Internet users. CheckFree provides infrastructure and software that permits users to pay all their bills with online electronic checks. CheckFree provides part of the technology that the Web portal Yahoo! uses to provide its **Yahoo! Bill Pay** service (see Figure 3.4).

NOTES

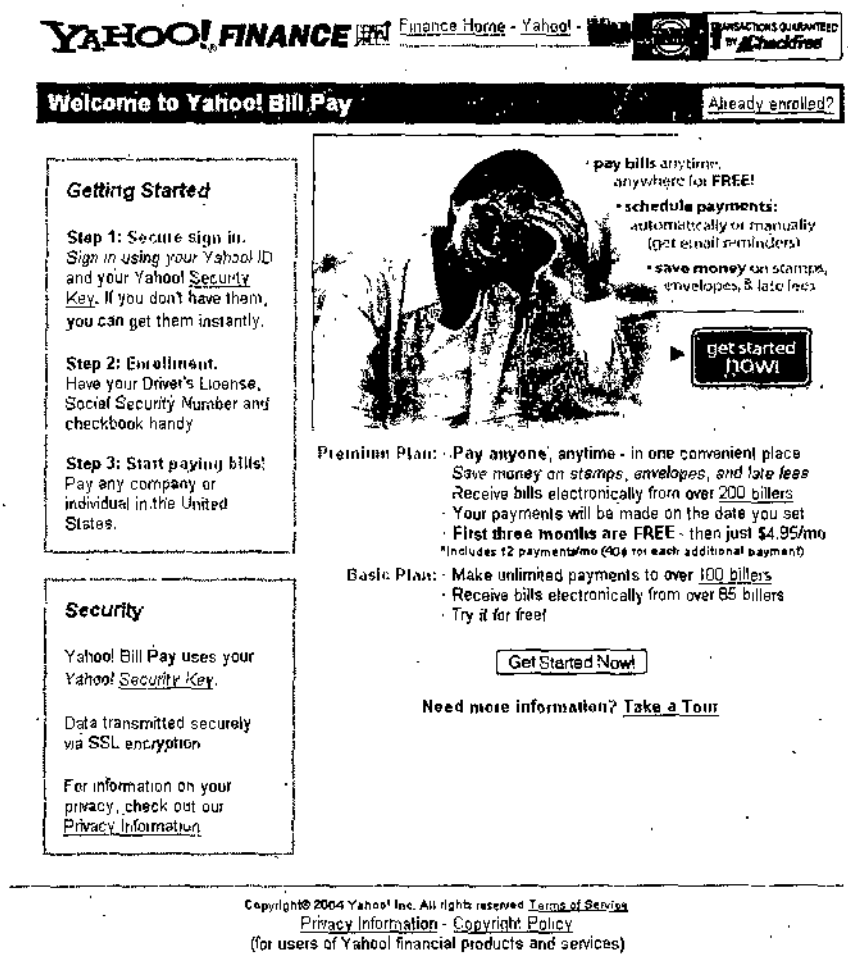


Figure 3.4. *Yahoo! Bill Pay service.*

Clickshare

Clickshare is an electronic cash system aimed at magazine and newspaper publishers. Clickshare's technology has occasionally been called a micropayment-only system; however, the ability to make micropayments is only one of Clickshare's features. Users with an ISP that supports Clickshare are registered automatically with Clickshare. When users click links leading to other sites that are registered with Clickshare, they can make purchases on those sites without having to register again. Clickshare keeps track of transactions and bills the user's ISP. The ISP, which already has an account relationship with the user, then bills the user for his or her purchases.

Another feature of Clickshare is that it tracks where a user travels on the Internet. This feature has significant value to advertisers and marketers that want to measure audience preferences; however, it does defeat anonymity, and anonymity is one reason that consumers might want to use Clickshare. The micropayment capability is, according to the company, a by-product of the core functionality of tracking identified users. Clickshare tracks users

NOTES

payment sites, such as Citibank's c2it payments service, but these have been less successful than nonbank entries into the business. In 2003, Citibank closed its c2it operation. Citibank does allow its customers to make peer-to-peer transfers from their checking accounts; however, that service requires the customer initiating the transfer to have a checking account with the bank.

ELECTRONIC WALLETS

As consumers are becoming more enthusiastic about online shopping, they have begun to tire of repeatedly entering detailed shipping and payment information each time they make online purchases. Filling out forms ranks high on online customers' lists of gripes about online shopping. To address these concerns, many electronic commerce sites include a feature that allows a customer to store name, address, and credit card information on the site. However, consumers must enter their information at each site with which they want to do business. An **electronic wallet** (sometimes called an **e-wallet**), serving a function similar to a physical wallet, holds credit card numbers, electronic cash, owner identification, and owner contact information and provides that information at an electronic commerce site's checkout counter. Electronic wallets give consumers the benefit of entering their information just once, instead of having to enter their information at every site with which they want to do business.

Electronic wallets make shopping more efficient. When consumers select items to purchase, they can then click their electronic wallet to order the items quickly. In the future, wallets could serve their owners by tracking purchases and maintaining receipts for those purchases. Maintaining records of a consumer's purchasing habits is something that online giants such as Amazon.com have mastered, but an enhanced digital wallet could reverse that process and use a Web robot to suggest where the consumer might find a lower price on an item that he or she purchases regularly.

Electronic wallets fall into two categories based on where they are stored. A **server-side electronic wallet** stores a customer's information on a remote server belonging to a particular merchant or wallet publisher. The main weakness of server-side electronic wallets is that a security breach could reveal thousands of users' personal information—including credit card numbers—to unauthorized parties. Typically, server-side electronic wallets employ strong security measures that minimize the possibility of unauthorized disclosure.

A **client-side electronic wallet** stores a consumer's information on his or her own computer. Many of the early electronic wallets were client-side

NOTES

wallets that required users to download the wallet software. This need to download software onto every computer used to make purchases is a chief disadvantage of client-side wallets. Server-side wallets, on the other hand, remain on a server and thus require no download time or installation on a user's computer. Before a consumer can use a server-side wallet on a particular merchant's site, the merchant must enable that specific wallet. Each wallet vendor must convince a large number of merchants to enable its wallet before it will be accepted by consumers. Thus, only a few server-side wallet vendors will be able to succeed in the market.

A disadvantage of client-side wallets is that they are not portable. For example, a clientside wallet is not available when a purchase is made from a computer other than the computer on which the wallet resides.

In a client-side electronic wallet, the sensitive information (such as credit card numbers) is stored on the user's computer instead of the wallet provider's central server. This removes the risk that an attack on a client-side electronic wallet vendor's server could reveal the sensitive information. However, an attack on the user's computer could yield that information. Most security analysts agree that storing sensitive information on client computers is safer than storing that information on the vendor server because it requires attackers to launch many attacks on user computers, which are more difficult to identify (even though the user computers are less likely than a vendor server to have strong security features installed). It also prevents the easily identified servers of the wallet vendors from being attractive targets for such attacks.

For a wallet to be useful at many online sites, it should be able to populate the data fields in any merchant's forms at any site that the consumer visits. This accessibility means that the electronic wallet manufacturer and merchants from many sites must coordinate their efforts so that a wallet can recognize what consumer information goes into each field of a given merchant's forms.

Electronic wallets store shipping and billing information, including a consumer's first and last names, street address, city, state, country, and postal code. Most electronic wallets also can hold many credit card names and numbers, affording the consumer a choice of credit cards at the online checkout. Some electronic wallets also hold electronic cash from various providers.

A number of companies entered the electronic wallet business, including major firms such as MasterCard. Most of these companies have abandoned their efforts because current versions of all major browsers now include a feature that remembers names, addresses, and other commonly requested information and provides a one-click completion of fields on Web forms that

request that information. Two survivors in the e-wallet arena are Microsoft.NET Passport and Yahoo! Wallet.

NOTES

Microsoft.NET Passport

Microsoft.NET Passport (often referred to as Passport or Microsoft Passport) is a server-side electronic wallet operated by Microsoft. Anyone who obtains a Hotmail account, which is Microsoft's free e-mail service, is signed up automatically for a Passport account. People who use Microsoft MSN Internet access service also must sign up for a Passport account. Passport functions in the same way as most other electronic wallets—by completing order forms automatically. All of the personal data entered into a Passport wallet is encrypted and password protected.

Passport consists of four integrated services : Passport single sign-in service (SSI), Passport Wallet service, Kids Passport service, and public profiles. The sign-in service allows a user to sign in at a participating Web site using his or her username and password. The Passport Wallet service provides standard electronic wallet functions, such as secure storage and form completion of credit card and address information. When requested by a participating merchant, a consumer's secure information is released to the merchant so that the consumer does not need to enter data into a form. The Kids Passport service helps parents protect and control their children's online privacy, and the public profiles service allows consumers to create a public page of information about themselves.

Yahoo! Wallet

Yahoo! Wallet is a server-side electronic wallet offered by the Web portal site Yahoo! The Yahoo! Wallet functions in the same way as most other electronic wallets—by completing order forms automatically with identifying information and credit card payment information. Yahoo! Wallet lets users store information about several major credit and charge cards, along with Visa and MasterCard debit cards.

Yahoo! Wallet is accepted by thousands of Yahoo! Store merchants (these are merchants on the Yahoo! Shopping section of the portal), and also can be used to pay for air-plane tickets and hotel reservations booked through the Yahoo! Travel section of the portal. Yahoo! Wallet also works when users pay for premium services at Yahoo!, such as extra mail storage or Web hosting fees on the Yahoo! GeoCities Plus or Website Services portions of the site. Sellers on Yahoo! Auctions can pay their auction fees using the Yahoo! Wallet, too.

Yahoo! has the advantage of hosting a number of services and shops that it can be certain accommodate its own wallet; thus, it is certain to have a large number of merchants (including itself) that accept its wallet.

NOTES

Many industry observers and privacy rights activist groups are concerned about electronic wallets because they give the company that issues the electronic wallet access to a great deal of information about the individual using the wallet. Several groups have attempted to enact standards intended to address wallet privacy concerns.

W3C Micropayment Standards Development Activity

Wallet information includes identification of the users and a complete record of their online purchasing activity. An alternative to having individual companies offer electronic wallet services is to have standards for electronic wallets built into the structure of the Web itself. With open standards, many different companies could offer electronic wallet services that would work on many different Web sites. This approach would distribute the information gathering and storage among a number of companies and thus reduce the risk of having one company in control of so much private information.

The World Wide Web Consortium (W3C) conducted an active standards development activity for micropayments in electronic commerce for several years. Although the activity has now been closed, the **W3C Electronic Commerce Interest Group (ECIG)** developed a set of standards called the **Common Markup for Micropayment Per-Fee-Links** before it ended its activities. This standard is a set of guidelines that provides an extensible and interoperable way to embed micropayment information in a Web page. An **extensible system** is one that developers can add to (or extend) without voiding any earlier work on the system. Although the ECIG standard showed promise, it was not adopted by a sufficient number of merchants and payment system operators to become successful.

The ECML Standard

The W3C initiative was not the only attempt to develop standards for the operation of electronic wallets. A consortium of several high-tech companies and credit card companies proposed an alternative standard that would replace the competing electronic wallet standards with a single standard. The consortium of companies, which includes America Online, Compaq, Dell, IBM, Microsoft, Visa U.S.A., and MasterCard, agreed on a set of XML tags called **ECML**, or **Electronic Commerce Modeling Language**. However, ECML has also failed to catch on among companies that create and use electronic wallets.

Assuming that an acceptable standard will evolve, the ultimate success of electronic wallets will depend on the confidence that Internet users have in the technology. As the NetBank story (see the Learning from Failures feature) illustrates, customer confidence is an important part of the success of any Internet technology, especially when that technology controls a person's financial welfare.

NOTES

STORED-VALUE CARDS

Today, most people carry a number of plastic cards—credit cards, debit cards, charge cards, driver's license, health insurance card, employee or student identification card, and others. One solution that could reduce all those cards to a single plastic card is called a stored-value card.

A **stored-value card** can be an elaborate smart card with a microchip or a plastic card with a magnetic strip that records the currency balance. The main difference is that a smart card can store larger amounts of information and includes a processor chip on the card. The card readers needed for smart cards are different, too. Common stored-value cards include prepaid phone, copy, subway, and bus cards. Many people use the terms "stored-value card" and "smart card" interchangeably.

Magnetic Strip Cards

Most magnetic strip cards hold value that can be recharged by inserting them into the appropriate machines, inserting currency into the machine, and withdrawing the card; the card's strip stores the increased cash value. Magnetic strip cards are passive; that is, they cannot send or receive information, nor can they increment or decrement the value of cash stored on the card. The processing must be done on a device into which the card is inserted. Although both magnetic strip cards and smart cards can store electronic cash, a smart card is better suited for Internet payment transactions because it has some processing capability.

Smart Cards

A **smart card** is a stored-value card that is a plastic card with an embedded microchip that can store information. Credit, debit, and charge cards currently store limited information on a magnetic strip. A smart card can store about 100 times the amount of information that a magnetic strip plastic card can store. A smart card can hold private user data, such as financial facts, encryption keys, account information, credit card numbers, health insurance information, medical records, and so on.

Smart cards are safer than conventional credit cards because the information stored on a smart card is encrypted. For example, conventional credit cards show your account number on the face of the card and your signature on the back. The card number and a forged signature are all that a thief needs to purchase items and charge them against your card. With a smart card, credit theft is much more difficult because the key to unlock the encrypted information is a PIN; there is no visible number on the card that a thief can identify, nor is there a physical signature on the card that a thief can see and use as an example for a forgery.

Smart cards have been in use for more than a decade. Popular in Europe and parts of Asia, smart cards so far have not been as successful in the United States. In Europe and Japan, smart cards are being used for telephone calls at public phones and for television programs delivered by cable to people's homes. The cards are also very popular in Hong Kong, where many retail counters and restaurant cash registers have smart card readers. The city's transportation companies—subways, buses, railways, trams, and ferries—joined together and created a smart card called the Octopus that lets commuters use one card for all of their public transportation needs. The Octopus can be reloaded at any transportation location or at 7-Eleven stores throughout Hong Kong. The **Hong Kong Citybus** Web page with information about the Octopus Card appears in Figure 3.6.

Smart cards are beginning to appear in the United States. In San Francisco, the Bay Area **Metropolitan Transportation Commission** created a smart card system patterned after the Octopus Card. This system, TransLink, is the first integrated ticketing system for public transportation in the United States. The transportation smart card, implemented in a 2002 pilot program, allows commuters to ride most modes of public transit available in the city, including trains, buses, cabs, and ferries, by simply waving a single card near a reader device in transit vehicles or in stations. TransLink users can reload their smart cards at several retail outlets or directly from their bank accounts. The pilot program was a success and TransLink became available to all Bay Area transit customers in 2006.

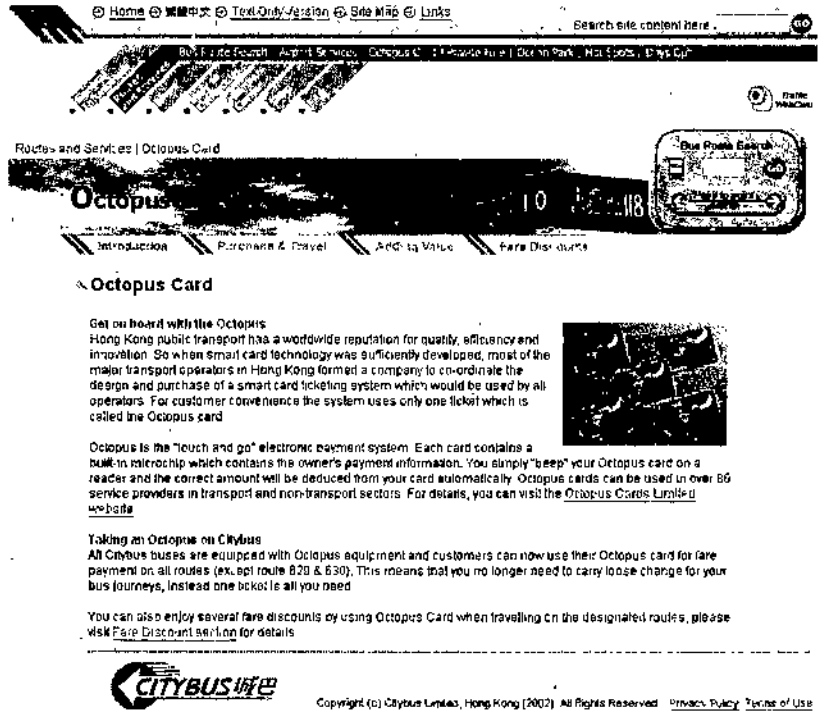


Figure 3.6. *Octopus smart card information on the Hong Kong Citybus site.*

NOTES

Visa introduced its smart card, the **smart Visa card**, in 2000. One of the first major promotions of the new Visa card occurred in late 2002 when retailer Target introduced its Target Visa smart card for use in Target stores and on the Target.com Web site. The Target Visa includes electronic wallet and automated login information for the Target.com Web site, but it also functions as a normal Visa card at other merchants. American Express has also released a smart card called **Blue.**

In the United States, the **Smart Card Alliance** advances the benefits of smart cards. The organization promotes the widespread acceptance of multiple-application smart card technology. Its members include companies in banking, financial services, computer technology, healthcare, telecommunications, and a number of government agencies. The Alliance focuses on information exchange and member interaction. Every member of the Alliance recognizes that smart cards can succeed in the United States only if a critical mass of smart cards supports applications—both physical and Internet-based—of interest to consumers. The Alliance promotes compatibility among smart cards, card reader devices, and applications.

INTERNET TECHNOLOGIES AND THE BANKING INDUSTRY

As you learned earlier in this chapter, the largest dollar volume of payments today are still made using paper checks. These paper checks are processed through the world's banking system. The other major payment forms in use today also involve banks in one way or another. This section outlines how Internet technologies are providing new tools and creating new threats for the banking industry.

Check Processing

In the past, checks were processed physically by banks and clearinghouses. When a person wrote a check to pay for an item at a retail store, the retailer would deposit the check in its bank account. The retailer's bank would then send the paper check to a clearing house, which would manage the transfer of funds from the consumer's bank to the retailer's account. The paper check would then be transported to the consumer's bank, which might then send the cancelled check to the consumer. In recent years, many banks have stopped sending cancelled checks to their consumer account holders to save postage. Despite these savings, the cost of transporting tons of paper checks around the country has grown each year.

In addition to the transportation costs, another disadvantage of using paper checks is the delay that occurs between the time that a person writes a

NOTES

check and the time that check clears the person's bank. This delay (which is similar to the delay you learned about earlier in PayPal accounts, and which is also called float) makes it possible to write checks a few days before money is in the account to cover those checks. In effect, the bank's customer obtains the free use of funds for a few days and the bank loses the use of those funds for the same time period. Although the delay normally lasts only a few days, there are times when it can become significantly longer. Railroad and airline strikes, for example, have caused the float to be extended. The most recent incidents that caused a significant increase in the float were the terrorist attacks of September 3, 2001.

Banks have been working for years to develop technologies that will help them reduce the float. In 2004, a U.S. law went into effect that many bankers believe will eventually eliminate the float. This law, called the **Check Clearing for the 21st Century Act** (or, more simply, **Check 21**), permits banks to eliminate the movement of physical checks entirely. In a Check 21-compliant world, the retailer can scan the customer's check. The scanned image is transmitted instantly through a clearing system and posts almost immediately to both accounts (that is, the withdrawal from the customer's account and the deposit to the retailer's account occur instantly), eliminating any float on the transaction.

You can learn more about the Check 21 law and its implementation by using the links in the Online Companion to the **BAI Check 21 Resource Center**, the **Federal Reserve Bank Check 21 Services** pages, or the **American Bankers Association Check 21 Resource Center.**

Phishing Attacks

Although phishing expeditions can be launched against all types of online businesses, they are of particular concern to financial institutions because their customers expect a high degree of security to be maintained over the personal information and resources that they entrust to their online financial institutions.

The basic structure of a phishing attack is fairly simple. The attacker sends e-mail messages (such as the one shown in Figure 3.7) to a large number of recipients who might have an account at the targeted Web site (PayPal is the targeted site in the example shown in the figure). The e-mail message tells the recipient that his or her account has been compromised and it is necessary for the recipient to log in to the account to correct the matter. The e-mail message includes a link that appears to be a link to the login page of the Web site. However, the link actually leads the recipient to the phishing attack perpetrator's Web site, which is disguised to look like the targeted Web site. The unsuspecting recipient enters his or her login name and password, which the perpetrator captures and then uses to access the

NOTES

recipient's account. Once inside the victim's account, the perpetrator can access personal information, make purchases, or withdraw funds at will.

Date : [Date removed] 08:05:42+0600
From : "Services PayPal" <services@paypal.com>
Subject : PayPal Account sensitive features are access limited !
To : [E-mail addresses removed]

Dear valued PayPal member :

PayPal is committed to maintaining a safe environment for its community of buyers and sellers. To protect the security of your account. PayPal employs some of the most advanced security systems in the world and our anti-fraud teams regularly screen the PayPal system for unusual activity.

Recently, our Account Review Team identified some unusual activity in your account. In accordance with PayPal's User Agreement and to ensure that you account has not been compromised, access to your account was limited. Your account access will remain limited until this issue has been resolved. This is a fraud prevention measure meant to ensure that your account is not compromised.

In order to secure your account and quickly restore full access, we may require some specific information from you for the following reason :

We would like to ensure that you account was not accessed by an unauthorized third party. Because protecting the security of your account is our primary concern, we have limited access to sensitive PayPal account features. We understand that this may be an inconvenience but please understand that this temporary limitationj is for your protection.

Case ID Number : PP-040-187-541.

We encourage you to log in and restore full access as soon as possible. Should access to your account remain limited for an extended period of time, it may result in further limitations on the use of your account.

However, failure to restore your records will result isn account suspension. Please update your records within 48 hours. Once you have updated your account records, your PayPal session will not be interrupted and will continue as normal.

To update your PayPal records click on the following link :
http://www.paypal.com/cgi-bin/webscr ?cmd=_login-run

Thank you for your prompt attention to this matter. Please understand that this is a security measure meant to help protect you and your account. We apologize for any inconvenience.

Sincerely,
PayPal Account Review Department

PAyPal Email ID PP522

Accounts Management As outlined in our User Agreement, PayPal will periodically send you informationj about site changes and enhancements.

Visit our Privacy Policy and User Agreement if you have any questions.
http://www.paypal.com/egi-bin/websci?amd::o/gen/ua/oolcy_privacy-outside

Figure 3.7. *Phishing e-mail message.*

NOTES

The links in phishing e-mails are usually disguised. One common way to disguise the real URL is to use the "@" sign, which causes the Web server to ignore all characters that precede the "@" and only use the characters that follow it. For example, a link that displays :

https ://paypal.com@218.36.41.188/fl/login.html

looks like it is an address at PayPal. However, the "@" sign causes the Web server to ignore the "paypal.com" and instead takes the victim to a Web page at the IP address "218.36.41.188."

In the e-mail shown in the figure, the link appears in the victim's e-mail client software as :

https ://paypal.com/cgi-bin/webscr ?cmd=_login-run

but when the victim clicks the link, the browser opens a completely different URL :

http ://leasurelandscapes.com/snow/webscr.dll

Instead of the URL it shows in the e-mail client, the link in the phishing e-mail actually includes following JavaScript code :

```
<A onmouseover="window.status='https ://www.paypal.com/cgi-bin/webscr?
cmd=_login-run'; return true" onmouseout="window.status='https ://www.
paypal.com/cgi-bin/webscr ?cmd=_login-run'"href="http ://
leasurelandscapes.com/snow/webscr.dll">https ://www.paypal.com/cgi-bin/
webscr ?cmd=_login-run</A>
```

This code is invisible in many e-mail clients, so the victim might never know that the Web browser has opened a phony site. Phishing attack perpetrators use a variety of other tricks to hide the URLs, including code that pops up windows that look exactly like a browser address bar. The window is coded to pop up over the browser's address bar. You can learn more about the details of phishing techniques by visiting the Web sites of the **Conferences on Email and Anti-Spam**. and the **Anti-Phishing Working Group**.

Organized Crime, Identity Theft, and Phishing Attacks

U.S. laws define **organized crime**, also called **racketeering**, as unlawful activities conducted by a highly organized, disciplined association for profit. The associations that engage in organized crime are often differentiated from less organized groups such as gangs and from organized groups that conduct unlawful activities for political purposes, such as terrorist organizations. Organized crime associations have traditionally engaged in criminal activities such as drug trafficking, gambling, money laundering, prostitution, pornography production and distribution, extortion, truck hijacking, fraud, theft, and insider trading. Often these activities are carried out simultaneously with legitimate business activities, which provide cover for the illegal activities.

NOTES

The Internet has opened new opportunities for organized crime in their traditional types of criminal activities and in new areas such as generating spam (which you learned about in earlier chapters), phishing, and identity theft. **Identity theft** is a criminal act in which the perpetrator gathers personal information about a victim and then uses that information to obtain credit. After establishing credit accounts, the perpetrator runs up charges on the accounts and then disappears. Figure 3.8 includes a list of the types of personal information that identity thieves most want to obtain (listed in approximate order of usefulness to the criminal).

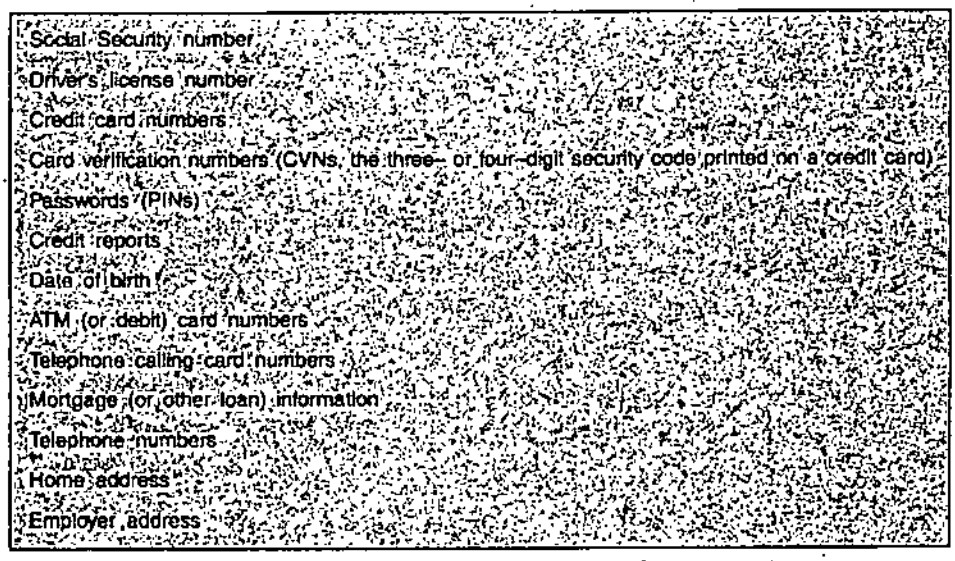


Figure 3.8. *Types of personal information most useful to identity thieves.*

Large criminal organizations can be highly efficient perpetrators of identity theft because they can exploit large amounts of personal information very quickly and efficiently. These organizations can use phishing attacks to gather personal information and then use it to perpetrate identity theft and other crimes. These criminal organizations often sell or trade information that they cannot use immediately to other organized crime entities around the world. Some of these criminal transactions are even conducted online. For example, a hacker who has planted zombie programs on a large number of computers (thus creating a **zombie farm**) might sell the right to use the zombie farm to an organized crime association that wants to launch a phishing attack (when a zombie farm is used this way, the attack is sometimes called a **pharming attack**). Individuals who commit these crimes have always posed a serious threat, but organized crime's entry into this activity increases the threat. There are two elements in phishing, the collection of the information (done by **collectors**) and the use of the information (done by **cashers**). The skills needed to perform these two activities are different. By facilitating transactions between collectors and cashers (and by participating

as one or both), crime organizations have increased the efficiency and volume of phishing activity overall.

More than 2 million people fall victim to phishing attacks each year and experience financial losses exceeding $900 million. Most experts believe that the percentage of online crime commited by organized crime associations will continue to increase in the future because it is so profitable.

NOTES

Phishing Attack Countermeasures

Since spam is a key element of phishing attacks, any protocol change that improves e-mail recipients' ability to identify the source of an e-mail message will also help to reduce the threat of phishing attacks.

The most important step that companies can take today, however, is to educate their Web site users. Most online banking sites continually warn their customers that the site never sends e-mail that asks for account information or that asks the recipient to log into their Web site and make changes to his or her account information. PayPal occasionally interrupts its own log-in screen sequence to insert a page that provides information about phishing attacks.

Many companies, especially those that operate financial Web sites, have contracted with consulting firms that specialize in anti-phishing work. These consultants monitor the Web for new Web sites that use the company's name or logo and move quickly to shut down those sites. Most phishing perpetrators set up their entrapping Web sites a few days before they launch their e-mail campaign, so this technique can be effective. Another anti-phishing technique is to monitor online chat rooms that are used by criminals. By watching for offers of stolen credit card information and other phishing exploits, consultants can identify phishing schemes that are under way.

The incidence of phishing attacks has grown rapidly over the past two years and most industry analysts expect that phishing will be a problem that will plague online businesses for the near future. Phishing can be an extremly profitable criminal activity and as more companies increase their defenses, analysts expect phishing perpetrators to become even better at working around those defenses.

STUDENT ACTIVITY

1. Explain the basic function of online payment system.

2. How electronic wallets work ? Explain.

SUMMARY

NOTES

- Online stores can accept a variety of forms of payment. Credit, debit, and charge cards (payment cards) are the most popular forms of payment on the Internet. They are ubiquitous, convenient, and easy to use.
- Electronic cash, one form of online payment, has been slow to catch on in the United States. A number of companies have faltered in recent years as they attempted to introduce electronic cash to the online world. Electronic cash is especially useful for making micropayments because the cost of processing payment cards for small transactions is greater than the profit on such transactions. Electronic cash shares several benefits with real cash : it is portable, anonymous, and usable for international transactions. Electronic cash can be stored online or offline. A third party, such as a bank, stores online electronic cash. The consumer holds offline cash in specially designed wallets.
- Electronic wallets provide convenience to online shoppers because they hold payment card information, electronic cash, and personal consumer identification. Electronic wallets eliminate the need for consumers to re-enter payment card and shipping information at a site's electronic checkout counter. Instead, the electronic wallet automatically fills in form information at sites that recognize the particular wallet software's technology. One persistent problem with electronic wallets is the lack of an internationally accepted standard. Both the W3C and the ECML standards group have created standards; however, neither has seen wide adoption by merchants, consumers, or wallet providers. With a single wallet standard, merchants would be more willing to install electronic, wallet-friendly software on their commerce sites.
- Stored-value cards, including smart cards and magnetic strip cards, are physical devices that hold information, including cash value, for the cardholder. Magnetic strip cards have limited capacity. Smart cards can store greater amounts of data on a microchip embedded in the card and are intended to replace the collection of plastic cards people now carry, including payment cards, driver's licenses, and insurance cards. Trials of smart cards in a few U.S. cities have proved disappointing; however, smart cards are popular in other parts of the world. Visa and American Express have introduced smart cards. Unlike electronic cash or payment cards, smart cards require merchants to install new hardware that can read the smart cards.
- Banks still process most monetary transactions, and a large part of the dollar volume of those transactions is still done by writing checks.

NOTES

Increasingly, banks are using Internet technologies to process those checks. Phishing expeditions and identity theft, especially when perpetrated by large criminal organizations, create a significant threat to online financial institutions and their customers. If not controlled, this threat could reduce the general level of confidence that consumers have in online business and hurt the growth of electronic commerce.

KEY TERMS

Acquiring bank
Anonymous electronic cash
Automated Clearing House (ACH)
Card not present transactions
Cashier
Charge card
Chargeback
Check 21
Client-side electronic wallet
Closed loop system
Collector
Credit card
Credit card association
Customer issuing bank
Debit card
Double-spending
Due diligence
Electronic cash
Electronic Commerce Modeling Language (ECML)
Electronic wallet (e-wallet)
EMV standard
Extensible system
Float
Identity theft
Interoperable software
Merchant account
Merchant bank
Micropayments
Money laundering
Open loop system
Organized crime
Payment card
Payment processing service provider
Peer-to-peer (P2P) payment system
Pharming attack
Racketeering
Scrip
Server-side electronic wallet
Single-use card
Small payments
Smart card
Stored-value card
Zombie farm

SELF ASSESSMENT QUESTIONS

NOTES

1. Write two paragraphs in which you define "scrip" and outline the advantages and disadvantages of scrip for consumers.
2. In about 100 words, describe the difficulties that can arise for merchants that want to process "card not present" credit card transactions.
3. In about 200 words, outline the reasons why a consumer who owns a credit card would want to use an electronic payment system, such as PayPal, for an Internet transaction. In an additional 200 words, outline the reasons that a small merchant might want to use an electronic payment system in addition to, or instead of, accepting credit cards.
4. In one paragraph, outline the problems that a company might encounter if it were to conduct international transactions using electronic cash.
5. In about 100 words, explain what electronic wallets are and how they can be useful to consumers.
6. In about 200 words, outline the advantages and disadvantages of smart cards for online merchants.

❑❑❑

SECTION D

NOTES

UNIT 4 E-COMMERCE APPLICATIONS

★ LEARNING OBJECTIVES ★

- E-Banking
- Online Shopping
- Revenue Models
- Online Publishing
- Revenue Models in Transition
- Electronic Data Interchange
- EDi on the Internet
- E-Retailing
- Electronic Fund Transfer

E-BANKING

Security First Network Bank (SFNB; www.sfnb.com/) was the first internet bank. It provides most of the banking services on the web. Therefore, you can do your banking with your fingers instead of your feet. Looking at e-banking, we can distinguish between two distinct models :

1. Pure cyberbanks.
2. Traditional banks that provide e-banking to complement their retail banking.

SFNB. is a pure cyberbank, while the homepage of Bank of America (www.bankofamerica.com) illustrates the second model.

While not all banks offer the full range of services on the internet, banks in both the aforementioned groups offer a varied range of services including :

1. personal banking.
2. commercial banking for both small businesses and large corporations.
3. financial services.

There are significant advantages for both the individual or corporation as well as the bank in using e-banking. An individual doing personal banking on the internet can, amongst other things, pay bills, do account transfers, make queries on account balances, obtain statements, in some cases view images of checks, etc., and import transactions directly into home account management software. Furthermore, one can make such transactions 24 hours a day from any place with internet access around the world.

In addition to these, a number of banks offer personal financial services including making personal loan applications on the internet. All these represent a large increase in convenience and time saving for the bank customer, saving him trips to the bank branch, queuing, etc.

The advantages to the banking institutions themselves include :

1. reduction in the number of retail banking branches, saving rentals or ownership of the related properties.
2. reduction in staffing because of the reduction in paper processing as well as face-to-face bank teller contact.
3. bringing about increase in the time the bank hangs on to the money before making the required transfers, leading to increase in interest received by the banks.

These advantages are so significant that some banks offer customers a number of incentives to -switch to internet banking, such as free checks, reduced fees, increased deposit rates, etc.

ONLINE SHOPPING

Books, Music, and Videos

Retailers using the Web catalog model to sell books, music, and videos have been among the most visible examples of electronic commerce. In 1994, a 29-year-old Wall Street financial analyst named Jeff Bezos became intrigued by the rapid growth of the Internet. Looking for a way to capitalize on this new marketing tool, he made a list of 20 products that he thought would sell well on the Internet. After some intense analysis, he determined that books were at the top of that list. Bezos had no experience in the book-selling business, but he realized that books were small-ticket commodity items and were easy and inexpensive to ship. He knew many customers would be willing to buy books without inspecting them in person and that books could be impulse purchase items if properly promoted. More than 4 million book titles are in print at any one time throughout the world; however, even the

NOTES

largest physical bookstore cannot stock more than 200,000 books. Bezos had identified a strategic opportunity for selling online. Twelve years later, **Amazon.com**, the company Bezos formed to sell books on the Internet, has annual sales of more than $8 billion and more than 70 million customers. Amazon.com has evolved to become a general retailer that sells books, music, videos, consumer electronics, housewares, tools, and many other items.

The rapid growth of Amazon.com inspired many booksellers to undertake electronic commerce. A number of well-established companies that operated physical bookstores, such as **Barnes & Noble**, **Blackwell's**, **Books-A-Million**, and **Powell's Books**, all adopted the Web catalog model in their online sales endeavors. Borders eventually decided to close its site and have Amazon.com handle its online business, but the other companies continue to operate their own sites successfully.

Luxury Goods

For some types of products, people are still reluctant to buy through a Website. This is particularly true for luxury goods and high-fashion clothing items. The Websites of couturiers **Vera Wang** and **Versace**, for example, were not constructed to generate revenue directly, but to provide information to shoppers who would visit the physical stores to examine items they had seen on the sites. Such sites tend to make heavy use of graphics and animation. **Evian**, the purveyor of premium-priced bottled water, went so far as to create a Website that works well only on computers that are connected to the Internet by a broadband connection. Evian intentionally designed its site for a select, affluent group of customers. The Flash animation takes a long time to download to computers that have an inexpensive dial-up modem connection. Tiffany & Co. is an upscale jewelry and gift retailer that has designed its site to be viewed by customers with broadband connections. The site has a large number of graphic and animated elements that would take a long time to display on a computer not connected through a broadband connection.

Clothing Retailers

A number of apparel sellers have adapted their catalog sales model to the Web, including **bebe**, **Gap**, **Lands' End**, **L.L. Bean**, **Talbots**, and **Wet Seal.** Unlike sellers in the high-fashion clothing category previously discussed, these Web stores display photos of casual and business clothing with prices, sizes, colors, and tailoring details. Their intent is to have customers examine the clothing and place orders through the Website. Lands' End pioneered the idea of online Web shopping assistance with its Lands' End Live feature in 1999.

NOTES

A Web customer with a question can initiate a text chat with a customer service representative or click a button on the Web page to have the representative call. In addition to answering questions, the representative can offer suggestions by pushing Web pages to the customer's browser.

Many of Lands' End's competitors (including Eddie Bauer, L.L. Bean, and Talbots) added similar text chat and call-back features to their sites. More recently, Lands' End added personal shopper and virtual model features to its site. The **personal shopper** is an intelligent agent program that learns the customer's preferences and makes suggestions. The **virtual model** is a graphic image built from customer measurements on which customers can try clothes. About 15 percent of visitors to the site use the virtual model and, on average, dress the model 40 times during a visit. Lands' End has found that the dollar amount of orders placed by customers who use the virtual model is about 10 percent larger than other orders. The Canadian company that developed this Website feature, **My Virtual Model**, has sold the technology to a number of other clothing retailers. A person who constructs a virtual model on one of those sites can use that same model on the other sites.

Lands' End also has a feature that allows two shoppers to browse the Website together from different computers. Only one of the shoppers can purchase items, but either shopper can select items to view. These items appear in both Web browsers.

In the fast-changing clothing business, retailers have always had to deal with the problem of overstocks—products that did not sell as well as hoped. Many retailers use outlet stores to sell their overstocks. Lands' End found that its overstocks Web page worked so well that it has closed some of its physical outlet stores. An online overstocks store works well because it reaches more people than a physical store and it can be updated more frequently than a printed overstocks catalog.

In addition to general apparel retailers, a number of specialty retailers opened stores on the Web. For example, women's shoe retailers such as **Steve Madden** and **Nine West** use the Web catalog model to sell directly to consumers on their sites.

One problem that the Web presents for clothing retailers of all types is that the color settings on computer monitors vary widely. It is difficult for customers to get an accurate idea of what the product's color will look like when it arrives. Until technology solves this problem, most online clothing stores will send a fabric swatch on request. The swatch also gives the customer a sense of the fabric's texture—an added benefit not provided by catalogs. Most Web catalog retailers also have generous return policies that allow customers to return unused merchandise for any reason.

NOTES

Flowers and Gifts

Gift retailers also use the Web catalog revenue model. Florist **1-800-Flowers** created an online extension to its highly successful telephone order business to compete with online—only florists such as **Calyx & Corolla** and **Proflowers.com**. Chocolatier **Godiva** offers business gift plans on its site. For gift shoppers who want a familiar brand name, shopping mall mainstays **Hickory Farms** and **Mrs. Fields Cookies** both have created Web catalog sites. **Harry and David**, famous for its trademarked "Fruit-of-the-Month" club, opened an informational Website to promote its existing catalog business. The company was surprised by the volume of sales leads that the site generated, and quickly added online ordering features to the site, which appear in Figure 4.1.

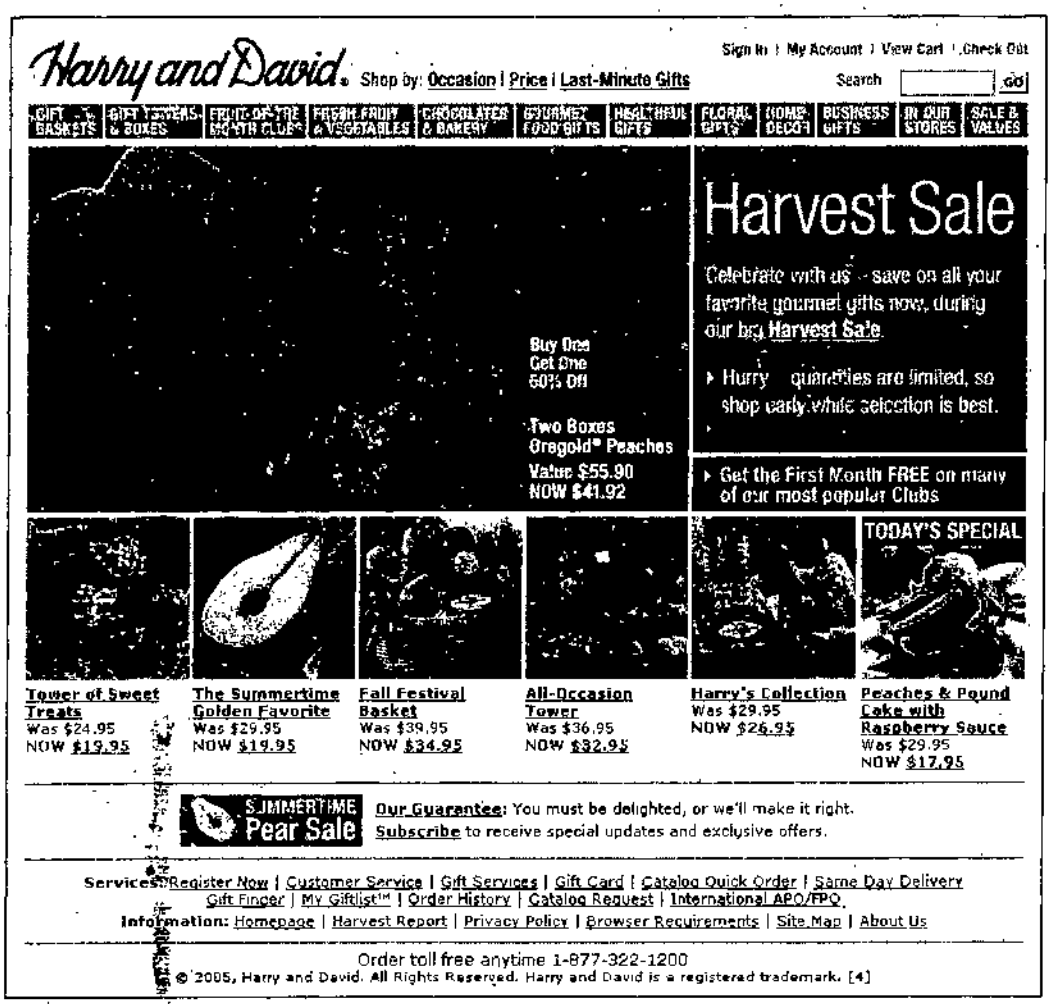


Figure 4.1. *Harry and David home page.*

General Discounters

A number of new companies have started retail operations on the Web. Some of these completely new businesses, such as **Buy.com**, operate as

NOTES

Web-based deep discounters. Borrowing a concept from the physical world's Wal-Marts and discount club stores, these discounters sell merchandise such as computer equipment, software, consumer electronics, books, music CDs, and sports equipment at extremely low prices.

Some of these Web discount retailers originally sold advertising on their sites to subsidize their low product prices. Beyond.com closed its retail operation and now sells the software it created for operating a Web catalog site. Buy.com changed its approach because advertising revenues were not sufficient subsidies. Buy.com now relies on the same volume-purchasing strategy as physical world retailers to keep prices low. As in the physical world, the online discount retail business is fiercely competitive and many of these companies operate on thin margins—and consequently earn little profit. Cyberian Outpost began business in 1995 as one of the first retailers on the Web. In 2001, after six years of winning awards for customer service, it ran out of cash and was purchased by Fry's Electronics, which continues to operate the **Outpost.com** Website as a subsidiary.

Traditional discount retailers, such as **Costco**, **Kmart**, **Target**, and **Wal-Mart**, were slow to introduce electronic commerce on their Websites. Many industry observers criticized these traditional retailers for their slow entry into online sales; however, those same industry observers now expect the traditional retailers to do very well competing against the retailers that started on the Web.

REVENUE MODELS

Not all electronic commerce initiatives have the goal of providing revenue; some are undertaken to reduce costs or improve customer service. Many companies create one Website to handle both B2C and B2B sales. Even when companies create separate sites (or separate pages within one site), they often use the same revenue model for both types of sales.

Electronic Catalog Revenue Models

Many companies sell goods and services on the Web using an adaptation of a mail order catalog revenue model that is more than 100 years old. In 1872, a traveling salesman named Aaron Montgomery Ward started selling dry goods to farmers through a one-page list. Richard Sears and Alvah Roebuck began mailing catalogs to farmers and small-town residents in 1895. Both Montgomery Ward (which closed in 2001) and Sears, Roebuck & Company grew to become dominant retailers in the United States by the 1950s, with retail stores serving urban markets in addition to the catalog business that served their rural and small-town markets.

NOTES

In this traditional catalog-based retail revenue model, the seller establishes a brand image, and then uses the strength of that image to sell through printed information mailed to prospective buyers. Buyers place orders by mail or by calling the seller's toll-free telephone number. This revenue model, which is often called the **mail order** or **catalog model**, has proven to be successful for a wide variety of consumer items, including apparel, computers, electronics, housewares, and gifts.

Companies can take this catalog model online by replacing or supplementing their print catalogs with information on their Websites. When the catalog model is expanded this way, it is often called the **Web catalog revenue model**. Customers can place orders through the Website or by telephone. This flexibility is important because many consumers are still reluctant to buy on the Web. In the first few years of consumer electronic commerce, most shoppers used the Web to obtain information about products and compare prices and features, but then made their purchases by telephone. These shoppers found early Websites hard to use and were often afraid to send their credit card numbers over the Internet. Although these fears are less prevalent today, most companies that use the Web catalog revenue model do give customers a way to complete the payment part of the transaction by telephone or by mail.

Many of the most successful Web catalog sales businesses are firms that were already operating in the mail order business and simply expanded their operations to the Web. Other companies that use the Web catalog revenue model adopted it after realizing that the products they sold in their physical stores could also be sold on the Web. This additional sales outlet did not require them to build additional stores, yet provided access to customers throughout the world. Types of businesses using the Web catalog revenue model include sellers of computers and consumer electronics; books, music, and videos; luxury goods; clothing; flowers and gifts; and general discount merchandise. In the next sections, you will learn how these types of businesses have applied the Web catalog revenue model to their operations.

Computers and Consumer Electronics

Leading computer manufacturers such as **Apple**, **Dell**, **Gateway**, **Hewlett-Packard**, and **Sun Microsystems** have had great success selling on the Web. All of these companies sell a full range of products—from small desktop computers to large server computers—to individuals, businesses, and other organizations through their Websites.

Dell has been a leader in allowing customers to specify exactly the configuration of computers they order on the Web. Dell created value by designing its entire business around offering this high degree of configuration flexibility to its customers. Other personal computer manufacturers that sell

NOTES

directly to customers on the Web have followed Dell's lead by offering visitors different ways to access product information. These sites usually offer links to specific products and pages designed for specific categories of customers, such as home, small business, education, or government users.

Retailers of consumer electronics products have also been active in undertaking electronic commerce using the Web catalog revenue model. Companies such as **Crutchfield** and **The Sharper Image** expanded their successful mail order catalog operations to include Websites such as the Sharper Image site shown in Figure 4.2. Other companies that had strong retail presences in their physical stores, such as **Best Buy**, **Circuit City**, **The Good Guys!**, **J&R Music World**, and **Radio Shack**, also opened Websites to sell the same products that they had been selling in their stores.

Figure 4.2. *Sharper Image home page.*

Digital Content Revenue Models

Firms that own written information (words or numbers) or rights to that information have embraced the Web as a new and highly efficient distribution

NOTES

mechanism. **LexisNexis** began as a legal research tool, and it has been available as an online product for years. Today, LexisNexis offers a variety of information services, including legal information, corporate information, government information, news, and resources for academic libraries. The original legal information product exists on the Web today as **Lexis.com** and provides full-text search of court cases, laws, patent databases, and tax regulations. In the past, law firms had to subscribe to and install expensive dedicated computer systems to obtain access to this information.

The Web has given LexisNexis customers much more flexibility in how they purchase information. Through the Lexis.com Website, law firms can subscribe to several versions of the service that are customized for different firm sizes and usage patterns. The Website even offers a credit card charge option for infrequent users who do not want a subscription. LexisNexis has used the Web to improve the delivery and variety of its existing product line and has been able to devise new products that take advantage of the Web's features.

ProQuest, a Website that sells digital copies of published documents, has its roots in two businesses : the former Bell and Howell learning materials business and University Microfilms International (UMI). These firms acquired *reproduction rights to a variety of published and unpublished materials.* For example, UMI had contracts with most North American universities to publish all doctoral dissertations and masters theses on demand. ProQuest offers digital versions of these documents for sale, along with a number of newspapers, journals, and other specialized academic publications. Many schools and libraries have subscriptions to ProQuest. **Ovid** and **EBSCO Information Services** also sells subscriptions to digital versions of journals to corporate and university libraries. These companies sell access to bibliographic databases and electronic journals to schools, companies, and libraries as well. The EBSCO Information Services home page that appears in Figure 4.3 shows the types of services it offers.

Dow Jones, a business-focused publisher of newspapers such as The Wall Street Journal and Barron's, was one of the first publishers to create a Website for selling subscriptions to digitized newspaper, magazine, and journal content. The Dow Jones Interactive site offered a customized digital clipping service that provided subscribers with a daily e-mail message of news on topics of interest to them. In 2002, Dow Jones and Reuters, a British company, joined to create an online content management and integration service called **Factiva**. In addition to the content and services previously offered on the Dow Jones Interactive site, Factiva gives companies *the ability to integrate their existing content (such as a corporate library)* with Dow Jones and Reuters news sources.

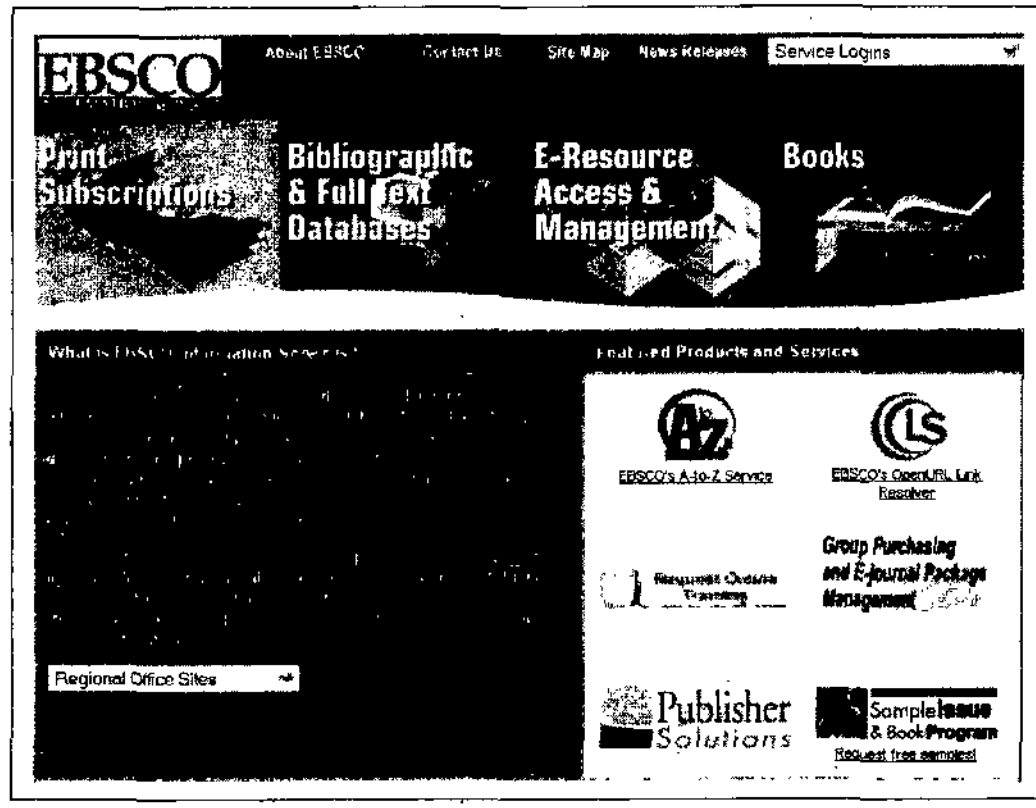


Figure 4.3. *EBSCO Information Services home page.*

One of the first academic organizations to make the transition to electronic distribution on the Web was (not surprisingly) the Association for Computer Machinery (ACM). The **ACM Digital Library** offers subscriptions to electronic versions of its journals to its members and to library and institutional subscribers. Academic publishing has always been a difficult business in which to make a profit because the base of potential subscribers is so small. Even the most highly regarded academic journals often have fewer than 2000 subscribers. To break even, academic journals often must charge each subscriber hundreds or even thousands of dollars per year. Electronic publishing eliminates the high costs of paper, printing, and delivery, and makes dissemination of research results less expensive and more timely.

As was the case for other technologies, such as VCRs and subscription cable television, many of the early commercial users of Web technology were dealers in adult-themed entertainment material. Many of the first profitable sites on the Web were sellers of adult digital content. These sites pioneered the online processing of credit card payment transactions and many different digital video technologies that are now used by all types of businesses on the Web.

NOTES

Advertising-Supported Revenue Models

The **advertising-supported revenue model** is the one used by network television in the United States. Broadcasters provide free programming to an audience along with advertising messages. The advertising revenue is sufficient to support the operations of the network and the creation or purchase of the programs. Many observers of the Web in its early growth period believed that the potential for Internet advertising was tremendous. Web advertising grew from essentially zero in 1994 to $2 billion in 1998. However, Web advertising was flat or declining in the years 2000 through 2002. Since then, Web advertising has once again started to grow, but at much lower rates than in the early years of the Web. After trying to develop profitable advertising-supported revenue models on the Web, most companies today are considerably less optimistic about the general potential of these revenue models. However, a few information sites, such as **About.com**, **HowStuffWorks**, and the ***Drudge Report***, are successful in using advertising-supported revenue models. The sites that have been successful tend to be sites that attract a specific group of visitors to which advertisers can direct specific messages. For example, About.com and HowStuff-Works both provide pages of information that are directed at visitors with highly focused interests. A visitor looking for an explanation of how heating stoves work on either of these sites would be a good prospect for advertisers that sell heating stoves. The site would not need to obtain any specific information from the visitor, the fact that the visitor is viewing the heating stoves information page is enough justification for charging an advertiser a higher rate for ads placed on those pages.

The overall success of online advertising has been hampered by two major problems. First, no consensus has emerged on how to measure and charge for site visitor views. Since the Web allows multiple measurements, such as number of visitors, number of unique visitors, number of click-throughs, and other attributes of visitor behavior, it has been difficult for Web advertisers to develop a standard for advertising charges. In addition to the number of visitors or page views, stickiness is a critical element in creating a presence that attracts advertisers. The **stickiness** of a Website is its ability to keep visitors at the site and attract repeat visitors. People spend more time at a **sticky** Website and are thus exposed to more advertising.

The second problem is that very few Websites have sufficient numbers of visitors to interest large advertisers. Most successful advertising on the Web is targeted to very specific groups. The set of characteristics that marketers use to group visitors is called **demographic information**, which includes such things as address, age, gender, income level, type of job held, hobbies, and religion. It can be difficult to determine whether a given Website is

attracting a specific market segment unless that site collects demographic information from its visitors—information that visitors are increasingly reluctant to provide because of privacy concerns.

NOTES

Web Portals

Few general-interest sites have generated sufficient traffic to be profitable based on advertising revenue alone. The drop in advertising rates and spending that occurred between 2000 and 2002 created difficulties for even the largest advertising-supported sites. One of the leading general-interest sites is **Yahoo!**, which was one of the first Web directories. A **Web directory** is a listing of hyperlinks to Web pages. Because so many people use Yahoo! number of visitors. This large number of visitors made it possible for Yahoo! to expand its Web directory into one of the first portal sites. A **portal** or **Web portal** is a site that people use as a launching point to enter the Web (the word "portal" means "doorway"). A portal almost always includes a Web directory and search engine, but it also includes other features that help visitors find what they are looking for on the Web and thus make the Web more useful. Most portals include features such as shopping directories, white pages and yellow pages searchable databases, free e-mail, chat rooms, file storage services, games, and personal and group calendar tools.

Because the Yahoo! portal's search engine presents visitors' search results on separate pages, it can include advertising on each results page that is triggered by the terms in the search. For example, when the Yahoo! search engine detects that a visitor has searched on the term "new car deals," it can place a Ford ad at the top of the search results page. Ford is willing to pay more for this ad because it is directed only at visitors who have expressed interest in new cars. This example demonstrates one attractive option for identifying a target market audience without collecting demographic information from site visitors. Unfortunately, only a few high-traffic sites are able to generate significant advertising revenues this way.

Besides Yahoo!, the main portal sites using the advertising-supported revenue model today are **AOL**, **AltaVista**, **Excite**, **Google**, **Lycos**, **Netscape**, and **MSN**. Smaller general interest sites, such as the Web directory **refdesk.com**, have had more difficulty attracting advertisers than the larger search engine sites. This may change in the future as more people use the Web. Another type of portal that may be able to earn a profit with smaller numbers of visitors is the portal that offers items of interest to a specialized interest group.

NOTES

ONLINE PUBLISHING

Many newspapers publish all or part of their print content on the Web. The **Internet Public Library Online Newspapers** page includes links to hundreds of newspaper sites around the world. It is unclear whether a newspaper's presence on the Web helps or hurts the newspaper's business as a whole. Although it provides greater exposure for the news-paper's name and a larger audience for advertising that the paper carries, it also can take away sales from the print edition. Like retailers or distributors whose online sales lead to the loss of their brick-and-mortar sales, publishers also experience sales losses as a result of online distribution. Newspapers and other publishers worry about these sales losses because they are very difficult to measure. Some publishers have conducted surveys in which they ask people whether they do not buy the newspaper because the content they want to see is available online, but the results of such surveys are not very reliable.

In addition to the concern about lost sales of print editions, most newspaper publishers have found that the cost of operating their Websites cannot be covered by the revenue they generate from selling advertising on the sites. Thus, many newspaper publishers are currently experimenting with various other ways of generating revenue from their Websites. You will learn about these alternative revenue models later in this chapter. Because newspapers are now using several different online revenue models, you will see newspapers mentioned in the discussions of several different revenue models.

Targeted Classified Advertising Sites

Although attempts to create general-interest Websites that generate sufficient advertising revenue to be profitable have met with mixed results, sites that target niche markets have been more successful. For newspapers, classified advertising is very profitable; thus, Websites that specialize in providing only classified advertising do have profit potential. This is especially true if they can reach a narrow target market and charge higher rates because the advertising reaches the right audience.

One implementation of the advertising-supported revenue model that is successful is Web employment advertising. Industry analysts estimate that online recruiting site revenues will exceed $80 billion by 2007. Companies such as **CareerBuilder.com** offer international distribution of employment ads. As the number of people using the Web increases, these businesses will be able to move beyond their current focus on technology and higher-level jobs and include advertising for all kinds of positions. These sites can use the same approach that Web directories and search engine sites use to offer advertisers target markets. When a visitor specifies an interest in, for

NOTES

example, engineering jobs in Dallas, the results page can include a targeted banner ad for which an advertiser will pay more because it is directed at a specific segment of the audience.

Employment ad sites can also target specific categories of job seekers by including short articles on topics of interest. These articles increase the site's stickiness and attract people who are not necessarily looking for a job. This is a good tactic because people who are not looking for a job are often the candidates most highly sought by employers. The **Monster.com** page directed at management-level job applicants (as distinguished from entry-level job applicants or executive-level job applicants) appears in Figure 4.4. This page offers links to articles, reports, a message board, and chat sessions that might interest a mid-career manager. It also offers a subscription to a newsletter for managers.

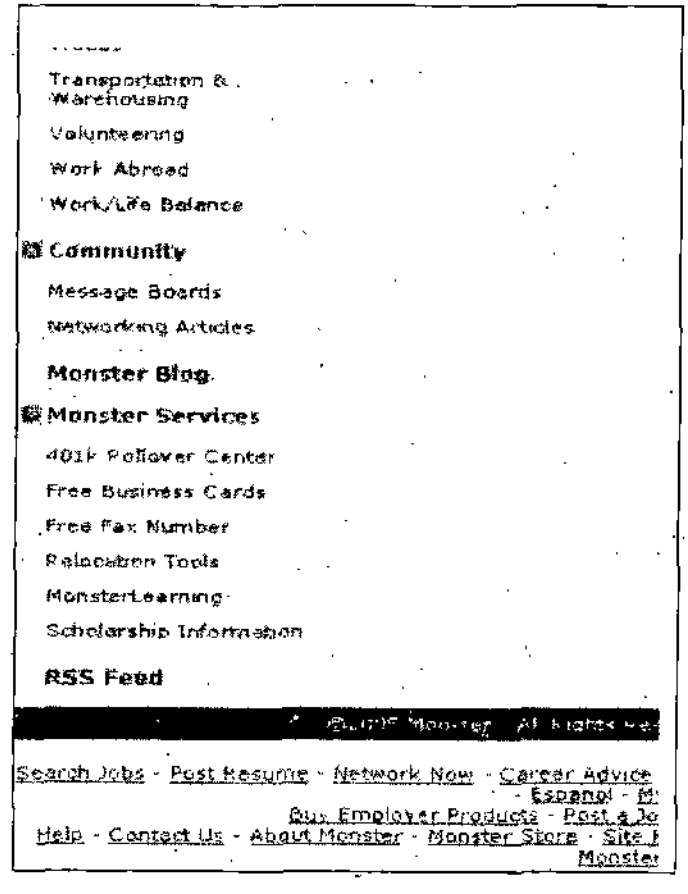


Figure 4.4. *Monster.com page for management-level job candidates.*

Another type of classified advertising Website that can generate sufficient revenue to be profitable is the used vehicle site. Trader Publishing has printed advertising newspapers for many years and now operates the **AutoTrader.com**, **CycleTrader.com**, and **BoatTrader.com** sites. These sites accept paid advertising from individuals and companies that want to

NOTES

sell cars, motorcycles, and boats. Trader Publishing charges a fee for each listing and gives the seller the option of running the ad on the Website only or on the Web and in the print version of the advertising newspaper. If the product has a dedicated following, this type of site can be successful by catering to small audiences. For example, the **VetteFinders** site sells classified ads for Corvette automobiles only.

Any product that is likely to be useful after the original buyer uses it provides the potential for a classified advertising site. People who want to sell used musical instruments can place ads on the **Musicians Buy-Line** site. Comic book collectors will find classified ads directed to them at **ComicLink.com**. Golfers who have given up the game or moved on to better clubs can place classified ads for their old equipment on the **Golf Classifieds.**

Advertising-Subscription Mixed Revenue Models

In an **advertising-subscription mixed revenue model**, which has been used for many years by traditional print newspapers and magazines, subscribers pay a fee and accept some level of advertising. On Websites that use the advertising-subscription revenue model, subscribers are typically subjected to much less advertising than they are on advertising supported sites. Firms have had varying levels of success in applying this model and a number of companies have moved to or from this model over their lifetimes.

Two of the world's most distinguished newspapers, ***The New York Times*** and ***The Wall Street Journal***, use a mixed advertising-subscription model. The New York Times version is mostly advertising supported, but the newspaper has experimented in recent years with charging fees for access to various parts of its site. In 2005, The New York Times began charging a fee for access to its Op Ed and news columns. The newspaper also charges for access to its premium crossword puzzle pages. The New York Times also provides a searchable archive of articles dating back to 1996 and charges a small fee for viewing any article older than one week. The Wall Street Journal's mixed model is weighted more heavily to subscription revenue. The site allows nonsubscriber visitors to view the classified ads and certain stories from the newspaper, but most of the content is reserved for subscribers who pay an annual fee for access to the site. Visitors who already subscribe to the print edition are offered a reduced rate on subscriptions to the online edition.

Note that both of these newspapers use one version of this revenue model for their print editions and another version for their online editions. More and more newspapers and magazines are finding that they need to use different revenue models for their print and online editions.

Some newspapers, including ***The Washington Post*** and the ***Los Angeles Times***, use another variation of the mixed revenue model. These newspapers

do not charge any subscription fees for access to their Websites. Instead, they offer current stories free of charge on their Websites, but require visitors to pay for articles retrieved from their archives. The Los Angeles Times did charge for access to its entertainment listings and reviews for a time, but it ended that experiment in 2005. In general, newspaper sites today are relying on advertising to provide revenue. Although Website advertising revenue is less than 3 percent of total revenue for most newspapers, it is growing steadily.

Business Week offers yet another variation on the mixed model theme. It offers some free content at its **Business Week online** site, but requires visitors to buy a subscription to the Business Week print magazine if they want to gain access to the entire site. Subscribers who want to read archived articles that are more than five years old are levied an additional charge per article. Business Week does place content in the subscriber section of its Website before the magazine appears on the newsstands or is delivered to subscribers.

Sports fans visit the **ESPN** site for all types of sports-related information. Leveraging its brand name from its cable television businesses, ESPN is one of the most visited sites on the Web. It sells advertising and offers a vast amount of free information, but die-hard fans can subscribe to its Insider service to obtain access to even more sports information. Thus, ESPN uses a mixed model that includes advertising and subscription revenue, but it only collects the subscription revenue from Insider subscribers, who make up only a small portion of site visitors.

Consumers Union, the publisher of product evaluations and ratings monthly magazine Consumer Reports, operates a Website, **ConsumerReports.org**, that relies heavily on subscriptions. Consumers Union is a not-for-profit organization that does not accept advertising as a matter of policy because it might appear to influence its research results. Thus, the site is supported by a combination of subscriptions and a small amount of charitable donations. The Website does offer some free information as a way to attract subscribers and fulfill its organizational mission of encouraging improvements in product safety.

Fee-for-Transaction Revenue Models

In the **fee-for-transaction revenue model**, businesses offer services for which they charge a fee that is based on the number or size of transactions they process. Some of these services lend themselves well to operating on the Web. To the extent that companies can offer Website visitors the information they need about the transaction, companies can offer much of the personal service formerly provided by human agents. If customers are willing to enter transaction information into Website forms, these sites can

NOTES

provide options and execute transactions much less expensively than traditional transaction service providers. The removal of an intermediary, such as a human agent, from a value chain is called **disintermediation.** The introduction of a new intermediary, such as a fee-for-transaction Website, into a value chain is called **reintermediation.**

Travel Agents

Travel agents earn commissions on each airplane ticket, hotel reservation, auto rental, or vacation that they book. These commissions are paid to the travel agent by the transportation or lodging provider. The travel agency revenue model involves receiving a fee for facilitating a transaction. The value added by a travel agent is that of information consolidation and filtering. A good travel agent knows many things about the traveler's destination and knows enough about the traveler to select the information elements that are useful and valuable to the traveler. Computers, particularly computers networked to large databases, are very good at information consolidation and filtering. In fact, travel agents have used networked computers, such as the **Sabre** system, for many years to make reservations for their customers.

When the Internet emerged as a new way to network computers and then became available to commercial users, a number of online travel agencies began doing business on the Web. Existing travel agencies did not, in general, rush to the new medium. They believed that the key value they added, personal customer service, could not be replaced with a Website. Therefore, the first Web-based travel agencies were new entrants. One of these sites, **Travelocity**, is based on the same Sabre system that traditional travel agents use. (Travelocity is also owned by Sabre.)

Microsoft also established a position in the online travel agency business with its **Expedia** subsidiary. **Travelocity**, **Expedia**, **Hotels.com**, and **Hotel Discount Reservations** are regularly listed among the top electronic commerce sites in surveys and industry analyst rankings. All four are profitable. In 2001, a consortium of five major U.S. airlines (American, Continental, Delta, Northwest, and United) launched a new Web travel site, **Orbitz**. A number of consumer groups and the attorneys general of 20 states expressed concern over possible antitrust issues that could arise with a site such as Orbitz, which is sponsored by competing airlines. For example, Orbitz offers a monetary incentive to airlines that agree to offer Orbitz customers their lowest fares at all times. That means that the airline cannot offer a special low fare on its own Website (or on another site such as Travelocity or Expedia) unless it also makes that fare available through Orbitz. The site launch was met with mixed reviews in surveys and criticism from industry analysts. The site encountered some technical difficulties; however, the site did immediately generate significant amounts of visitor

NOTES

traffic. Within a year, Orbitz had become one of the three most visited travel sites on the Web. The Orbitz home page appears in Figure 4.5.

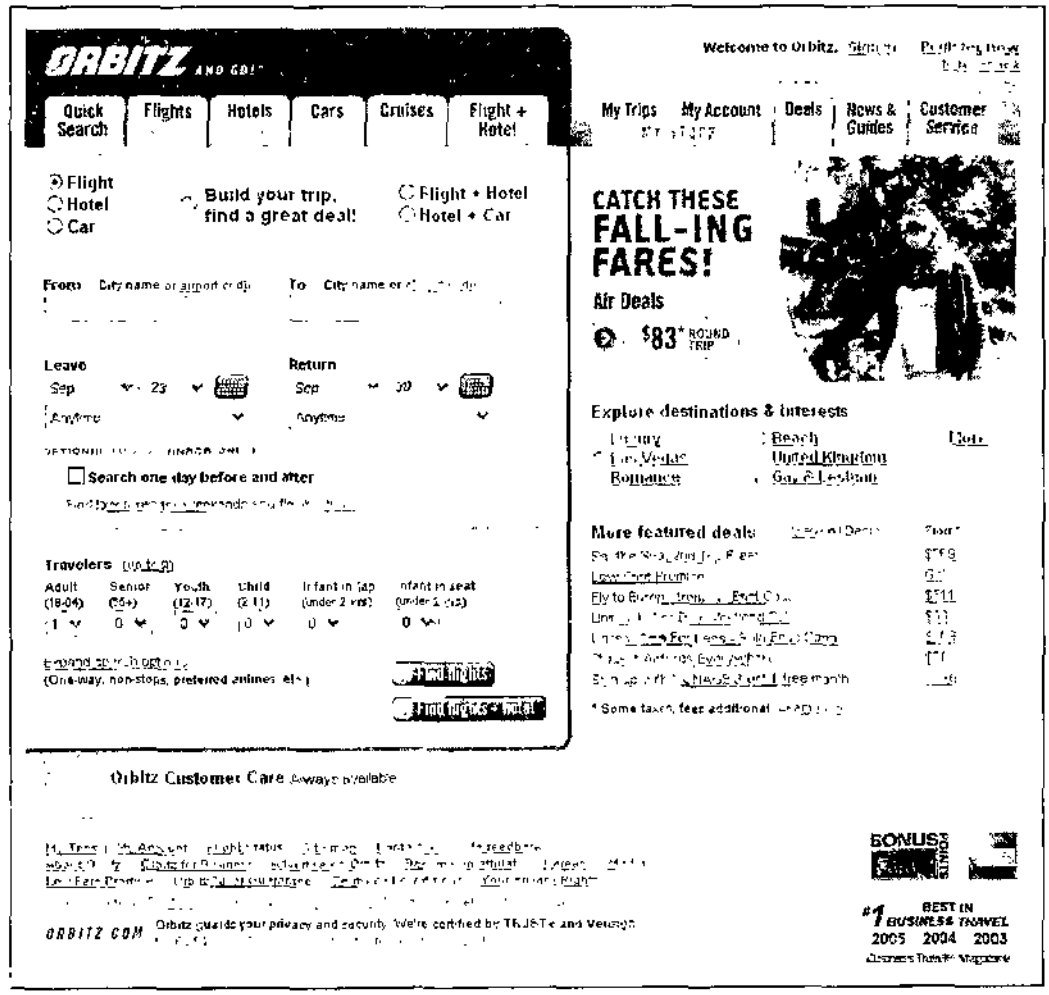


Figure 4.5. *Orbitz home page.*

In addition to earning commissions from the transportation and lodging providers, these sites generate advertising revenue from ads placed on travel information pages. These ads are similar to those on search engine results pages because advertisers can target them without obtaining demographic details about the site visitor. For example, if you are booking a flight to Chicago, the page that lists airline ticket options may also carry a banner ad for a hotel in Chicago or a car rental company that is running a promotion in the Chicago area.

Many traditional travel agents are finding themselves squeezed out of the business today. Airlines are reducing or even eliminating the commissions they pay to travel agents on each ticket. Many travel agents (including the online travel sites) now charge their customers a flat fee for processing a ticket on an airline that has reduced or eliminated the fees it pays to travel agents.

Although these changes have hurt all travel agents, some industry observers believe that the large online travel agencies will have a better chance of surviving any shakeout that occurs in the business. Other industry observers note that smaller traditional travel agents often specialize in cruises or finding specialized hotel accommodations. Both cruise lines and hotels still view travel agents as an important part of their selling strategy and continue to pay reasonable commissions to travel agents on the sales that they make.

Some travel agents have been successful by following a reintermediation strategy with a focus on specific groups of travelers. These travel agents identify a group of travelers with specific needs and create travel packages designed for that group. For example, surf vacations have become increasingly popular in recent years. The stereotypical surfer of years gone by (a young unemployed male) has been replaced by a much broader demographic. Today's surfers often have significant financial resources and enjoy surfing in exotic locations. Websites such as **WaveHunters.com** and **WannaSurf** have followed a reintermediation strategy and cater to this highly specialized market in ways that generalist travel agents have not.

Automobile Sales

Auto dealers buy cars from the manufacturer and sell them to consumers. They provide showrooms and salespeople to help customers learn about product features, arrange financing, and make a purchase decision. Most auto dealers negotiate the prices at which they sell their cars; thus, the salesperson's job also includes extracting the highest possible price from the consumer. Many people do not like negotiating car prices, especially if they have taken the time to learn about car features, arrange financing, and are ready to purchase a car without further assistance from a salesperson.

Autobytel and other firms offer knowledgeable consumers an option that removes the salesperson from the process. Autobytel and similar firms, such as **MSN Autos** and **CarsDirect.com**, provide an information service to car buyers. Each of these firms implements the fee-for-transaction revenue model in a slightly different way. For example, CarsDirect.com offers customers the ability to select a specific car (model, color, options) at a price it determines. CarsDirect.com then finds a local dealer that has such a car and is willing to sell it for the CarsDirect.com price. Alternatively, **Autoweb.com** and **Autobytel** locate dealers in the buyer's area that are willing to sell the car specified by the buyer (including make, model, options, and color) for a small premium over the dealer's nominal cost. The buyer can purchase the car from the dealer without negotiating with a salesperson. Autobytel and Autoweb.com charge participating dealers a fee for this service. In effect, firms such as Autobytel, Autoweb.com, and CarsDirect.com are taking the salesperson out of the value chain. To the extent that the salesperson provides

NOTES

little or no value to the consumer, these firms are reducing the transaction costs in the process. The car salesperson is disintermediated and the Website becomes the new intermediary in the transaction, which is an example of reintermediation.

Stockbrokers

Stock brokerage firms also use a fee-for-transaction model. They charge their customers a commission for each trade executed. In the past, stockbrokers offered investment advice and made specific buy and sell recommendations to customers. They did not charge for this advice, but they did charge relatively high commissions on the trades they handled for their customers. After the U.S. government deregulated the securities trading business in the early 1970s, a number of discount brokers opened. These discount brokers distinguished themselves from the established "full-line" brokerage houses by not offering any investment advice and charging very low commissions. Because the full-line brokers had failed to provide value to some of their customers, those customers were very happy to move their business to the discount brokers.

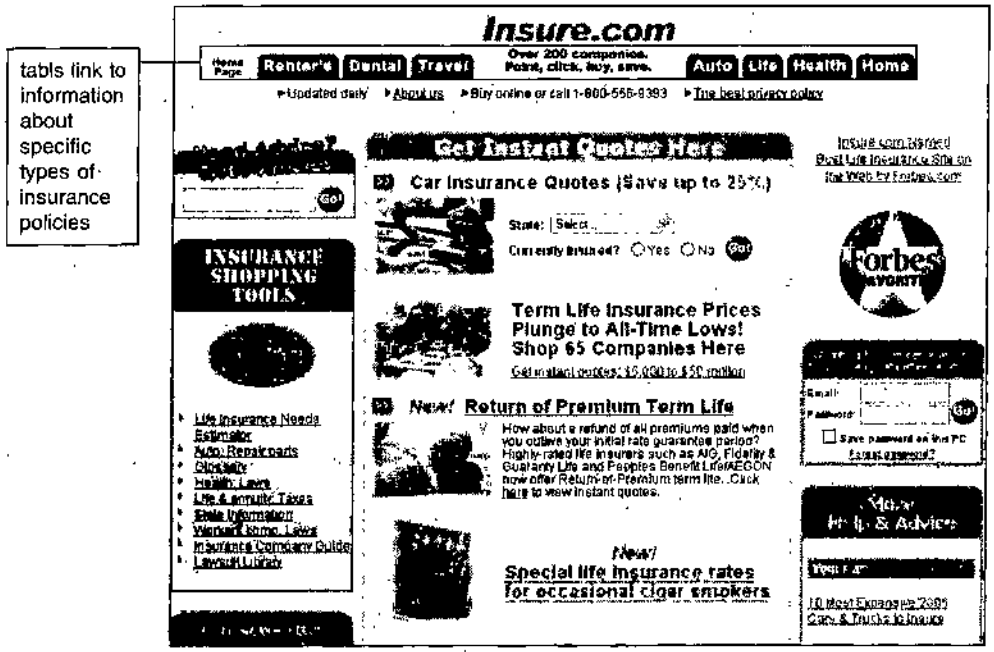
The Web made it possible for firms such as **E*TRADE** and Datek (later purchased by **Ameritrade**) to offer investment advice (posted on Web pages) similar to that offered by a full-line broker, without incurring many of the costs of distributing the advice (such as stockbroker salaries, overhead, and the costs of printing and mailing newsletters). Web-based brokerage firms could also offer fast execution of trades that customers entered into Web page forms. Thus, in the 1990s, discount brokers who had taken business away from full-line brokers for 15 years faced new competition from online firms. Of course, the full-line brokers found that they were losing business to both the discount brokers and the online brokers. In response, both discount brokers (such as **Charles Schwab** and **Ameritrade**) and full-line brokers (such as **Merrill Lynch** and **Smith Barney**) opened new stock trading and information Websites.

The online brokers are offering customers the same kind of transaction cost reductions as the online auto buying sites. Stockbrokers are finding themselves disintermediated in the same way as car salespeople. Online brokers are offering an alternative service that has greater perceived value for many investors today.

Insurance Brokers

Other sales agency businesses are moving to the Web. Although insurance companies themselves were slow to offer policies and investments for sale on the Web, a number of intermediaries that sell insurance policies from a variety of companies have been online since the early days of the Web.

Quotesmith, which began business in 1984 as a policy-quoting service for independent insurance brokers, decided in 1996 to offer its policy price quotes directly to the public over the Internet. By quoting policies and accepting applications directly, Quotesmith is disintermediating the independent insurance agents with whom it formerly worked. Quotesmith operates the **Insure.com** Website, which appears in Figure 4.6.



Copyright © 1984–2005 Quotesmith.com

Figure 4.6. *Quotesmith's Insure.com Website.*

Other Websites that offer insurance policy information, comparisons, and sales include **InsWeb**, **Answer Financial**, **Insurance.com**, and **YouDecide.com**, which was created by the human resources software development company **ProAct Technologies**. In response to the appearance of independent Websites that offered customers a way to compare prices from various insurance companies, **Progressive Insurance** decided to offer quotes on its Website with an interesting twist. The company provides quotes for its insurance products and also for its competitors' products. If a site visitor finds that one of the competitor's products is less expensive, Progressive provides a link to that company's site so site visitors can buy their insurance elsewhere. Progressive has always promoted itself as offering the lowest-priced insurance, and this is a way that the company reinforces its image. If it cannot offer the lowest price, the company invites potential customers to buy elsewhere. Progressive's well-advertised strategy encourages many insurance shoppers to visit the Progressive site instead of an independent comparison site. Today, many major insurance companies, such as **Allstate**, **GEICO**, and **State Farm Insurance**, offer information or policies for sale on their Websites.

NOTES

Event Tickets

Obtaining tickets for concerts, shows, and sporting events can be a challenge. Some venues only offer tickets for sale at their own box offices, and others sell tickets through ticket agencies that can be difficult for patrons to find. The Web offers event promoters an ability to sell tickets from one virtual location to customers practically anywhere in the world. Traditional ticket agencies such as **Ticketmaster** have opened shop online. Other companies, such as **Tickets.com** and **TicketWeb**, also offer a wide variety of tickets for events in many different locations. In addition to original sale of tickets, the Web has offered opportunities for those who deal in secondary market tickets (tickets that have already been sold by the event's producer and that are being offered for resale to other persons). Companies such as **StubHub** and **TicketsNow** operate as brokers to connect owners of tickets with buyers in this market. All of these electronic commerce initiatives reduce transaction costs for both buyers and sellers of tickets.

Real Estate and Mortgage Loan Brokers

Other fee-for-transaction businesses are also starting to open electronic commerce Websites, including real estate brokers and mortgage loan brokers. Online real estate brokers provide all of the services that a traditional broker might provide—except that online brokers provide these services through their Websites. Leading real estate sites include Web pioneers **eRealty** and **zipRealty.com**. Industry observers agree that these new online brokers do a much better job selling on the Web than traditional real estate brokers that have opened Websites, such as **Coldwell Banker** and **Prudential**. The industry's trade association, the National Association of Realtors, sponsors a Website, **Realtor.com**, that carries ads for houses listed by its member companies.

IndyMac Bank Home Lending offers mortgage loan seekers an online credit review and decision in minutes. Approved customers can then print an approval letter from their own computers and take it with them the same day to shop for a new house. This rapid decision-making ability and other customer service features have helped IndyMac become a leading mortgage banker successfully integrating the Internet into its business, funding more than $12 billion in home loans each year. Other successful mortgage brokers on the Web include **Ditech** and **E-LOAN**.

Fee-for-Service Revenue Models

Companies are offering an increasing variety of services on the Web for which they charge a fee. These are neither broker services nor services for which the charge is based on the number or size of transactions processed.

NOTES

The fee is based on the value of the service provided. These **fee-for-service revenue models** range from games and entertainment to financial advice and the professional services of accountants, lawyers, and physicians.

Online Games

Computer and video games are a huge industry. In the United States alone, more than $10 billion per year is spent on these types of games. An increasing portion of that revenue is generated online. Although many sites that offer games relied on advertising revenue in the past, a growing number now include premium games in their offerings. Site visitors must pay to play these premium games, either by buying and downloading software to install on their computers, or by paying a subscription fee to enter the premium games area on the site. Microsoft's **MSN Games by Zone.com**, Sony's **Station.com**, Real-Networks' **RealArcade**, and **Electronic Arts** are among the leading game sites that include subscription game services. For example, Sony's EverQuest adventure game draws more than 400,000 players who have purchased a $40 software package and pay $10 per month to continue playing the game. Most of the game sites charge a monthly subscription of between $5 and $20 for access to all their fee-based games offerings. The **Entertainment Software Association** is an industry group that tracks computer and video game use. Its Website includes a number of interesting statistics about computer game sales and demographics of game players. For example, more than 40 percent of frequent computer game players are over the age of 35!.

Concerts and Films

As more households obtain broadband access to the Internet, an increasing number of companies provide streaming video of concerts and films to paying subscribers. With a revenue model patterned after cable television companies, **Intertainer** began selling subscriptions for delivery of video content to computers and other devices through cable modem and DSL connections in 1999. Intertainer had built its business to more than 140,000 subscribers in 2002 when it closed and filed a lawsuit against several major media companies alleging that they were illegally controlling the market. Despite the ongoing law-suit, MGM Studios, Paramount Pictures, Sony Pictures Entertainment, Universal Studios, and Warner Brothers Studios formed a joint venture to build the **Movielink** site. Movielink offers downloadable movies drawn from the content owned by the joint venture partners and licensed from other content owners such as Walt Disney Pictures and Miramax. Movielink sells a 24-hour window of access to the downloaded movies for a $2 to $5 fee. RealNetwork's **RealOne SuperPass** subscription includes sporting events, music videos, comedy, and other entertainment offerings for $13 per month.

NOTES

The main technological limitation these companies face is that each additional customer who downloads a video stream requires that the provider purchase additional bandwidth from its ISP. Television broadcasters, on the other hand, need only pay the fixed cost of a transmitter—the airwaves are free and carry the transmission to an unlimited number of viewers at no additional cost. In contrast, as the number of an Internet-based provider's subscribers increases, the cost of the provider's Internet connection increases. However, if these Web entertainment companies can charge a high enough monthly fee, they should be able to cover the additional costs of technology upgrades and still make a profit.

Professional Services

State laws have been one of the main forces preventing U.S. professionals (such as physicians, lawyers, accountants, and engineers) from extending their practices to the Web. Since most professionals are licensed by individual states, state laws can effectively prevent them from practicing their professions on the Web because their patients or clients could be located in other states. If they were to offer their services over the Web, professionals could be charged with unlicensed practice in those other states. State laws that address the location of services are vague—it is difficult to determine where a service provided over the Internet actually occurred. This uncertainty arises because most state professional practice laws were written long before the Internet existed. Although some medical, legal, and other professional practices are using online services such as **MyDocOnline** to allow patients to make appointments, most practices are reluctant to do even that limited amount of business activity on the Web. The major concern expressed by physicians regards the protection of patients' privacy. Until the Web is perceived as more secure, most people will continue to be reluctant to make medical appointments, or even refill prescriptions, on the Web.

REVENUE MODELS IN-TRANSITION

Many companies have gone through transitions in their revenue models as they learn how to do business successfully on the Web. As more people use the Web to buy goods and services, and as the behavior of those Web users changes, companies often find that they must change their revenue models to meet the needs of those new and changing Web users. Some companies created electronic commerce Websites that needed many years to grow large enough to become profitable. This is not unusual; both CNN and ESPN took more than 10 years to become profitable and they had both created new businesses in television, which was an existing and well-established medium. After the investment community became reluctant to continue funding most

NOTES

Web businesses in 2000, many Web companies that were counting on additional investments to support them during their unprofitable growth phases were forced to either change their revenue models or go out of business.

This section describes the revenue model transitions undertaken by five different companies as they gained experience in the online world and faced the changes that occurred in that world. As the world embarks on the second wave of electronic commerce, these and other companies might well face the need to make further adjustments to their revenue models.

Subscription to Advertising-Supported Model

Microsoft founded its ***Slate* magazine** Website as an upscale news and current events publication. Because Slate included experienced writers and editors on its staff, many people expected the online magazine to be a success. Microsoft believed that the magazine had a high value, too. At a time when most online magazines (also called **e-zines**, or electronic magazines) were using an advertising-supported revenue model, Slate began charging an annual subscription fee after a limited free introductory period.

Although Slate drew a wide readership and received acclaim for its incisive reporting and excellent writing, it was unable to draw a sufficient number of paid subscribers. At its peak, Slate had about 27,000 subscribers generating annual revenue of $500,000, which was far less than the cost of creating the content and maintaining the Website. Slate is now operated as an advertising-supported site. Because it is a part of Microsoft, Slate does not report its own profit numbers, but most industry observers believe that the site does not earn a profit. Microsoft maintains the Slate site as part of its MSN portal, so it is likely that Slate increases the stickiness of the portal.

Advertising-Supported to Advertising-Subscription Mixed Model

Another upscale online magazine, ***Salon.com***, which has also received acclaim for its innovative content, has moved its revenue model in the direction opposite to Slate's transition. After operating for several years as an advertising-supported site, Salon.com now offers an optional subscription version of its site. The subscription offering was motivated by the company's inability to raise the additional money from investors that it needed to continue operations.

Subscribers pay $30 per year to view a version of the magazine called Salon Premium, which is free of advertising and can be downloaded for storage and later offline reading on the subscriber's computer. Premium subscribers also gain access to additional content such as downloadable music, e-books, and audio books.

NOTES

Advertising-Supported to Fee-for-Services Model

Xdrive Technologies opened its original advertising-supported Website in 1999. Xdrive offered free disk storage space online to users. The users saw advertising on each page and had to provide personal information that allowed Xdrive to send targeted e-mail advertising to them. Its offering was very attractive to Web users who had begun to accumulate large files, such as MP3 music files, and wanted to access those files from several computers in different locations.

After two years of offering free disk storage space, Xdrive found that it was unable to pay the costs of providing the service with the advertising revenue it had been able to generate. It switched to a subscription-supported model and began selling the service to business users as well as individuals. The amount of the monthly subscription is based on the amount of disk space reserved for the user. In recent years, disk drive costs have been dropping and Xdrive has frequently adjusted its monthly fee downward. Currently, Xdrive offers 5 GB of storage for about $10 per month. Other companies, such as **IBackup** and **Kela** have followed Xdrive's lead in offering online storage for a monthly fee.

Advertising-Supported to Subscription Model

Northern Light was founded in August 1997 as a search engine with a twist. In addition to searching the Web, it searched its own database of journal articles and other publications to which it had acquired reproduction rights. When a user ran a search, Northern Light returned a results page that included links to Websites and abstracts of the items in its own database. Users could then follow the links to Websites, which were free, or purchase access to the database items.

Thus, Northern Light's revenue model was a combination of the advertising-supported model used by most other Web search engines plus a fee-based information access service, similar to the subscription services offered by ProQuest and EBSCO that you learned about earlier in this chapter. The difference in the Northern Light model was that users could pay for just one or two articles (the cost was typically $1–$5 per article) instead of paying a large amount of money for unlimited access to its database on an annual subscription basis. Northern Light also offered subscription access to most of its database to companies. schools, and libraries, however.

In January 2002, Northern Light decided that the advertising revenue it was earning from the ads it sold on search results pages was insufficient to justify continuing to offer that service. It stopped offering public access to its search engine and converted to a new revenue model that was primarily

NOTES

subscription supported. Northern Light's main revenue source in its new model is from annual subscriptions to large corporate clients. It still offers an individual account option, however. A person interested in having the ability to search the Northern Light database can open an account, supply a credit card number, and be billed monthly for the articles accessed.

Multiple Transitions

Encyclopædia Britannica is an excellent example of a company that transferred its existing reputation for high quality to the Web. Encyclopædia Britannica has developed one of the most respected brand names in research and education over its many years in print publishing. It is particularly interesting that Encyclopædia Britannica began in 1768 as a sort of precomputer-age frequently asked questions (FAQ) list. A group of academics collected notes they had made while conducting research and decided to publish them as a series of articles.

Encyclopædia Britannica began its online expansion with two Web-based offerings. The Britannica Internet Guide was a free Web navigation aid that classified and rated information-laden Websites. It featured reviews written by Britannica editors who also selected and indexed the sites. The company's other Website, Encyclopædia Britannica Online, was available for a subscription fee or as part of the Encyclopædia Britannica CD package. Britannica used the free site to attract users to the paid subscription site.

In 1999, disappointed by low subscription sales, Britannica converted to a free, advertiser-supported site. The first day the new site, **Britannica.com**, became available at no cost to the public, it had more than 15 million visitors, forcing Britannica to shut down for two weeks to upgrade its servers.

The Britannica.com site then offered the full content of the print edition in searchable form, plus access to the Merriam-Webster's Collegiate Dictionary and the Britannica Book of the Year. One of the most successful aspects of the site was the way it integrated the Britannica Internet Guide Web-rating service with its print content. The Britannica Store sold the CD version of the encyclopedia along with other educational and scientific products to help generate revenue.

After two years of trying to generate a profit using this advertising-supported model, Britannica faced declining advertising revenues. In 2001, Britannica returned to a mixed model in which it offered free summaries of encyclopedia articles and free access to the Merriam-Webster's Collegiate Dictionary on the Web, with the full text of the encyclopedia available for a subscription fee of $50 per year or $5 per month.

NOTES

ELECTRONIC DATA INTERCHANGE

Electronic data interchange (EDI) is a computer-to-computer transfer of business information between two businesses that uses a standard format of some kind. The two businesses that are exchanging information are trading partners. Firms that exchange data in specific standard formats are said to be **EDI compatible**. The business information exchanged is often transaction data; however, it can also include other information related to transactions, such as price quotes and order status inquiries. Transaction data in business-to-business transactions includes the information traditionally included on paper invoices, purchase orders, requests for quotations, bills of lading, and receiving reports. The data on these five types of forms accounts for more than 75 percent of all information exchanged by trading partners in the United States. Thus, EDI was the first form of electronic commerce to be widely used in business—some 20 years before anyone used the term "electronic commerce" to describe anything!

It is very important that you understand what EDI is designed to accomplish and how it came to be the preferred way for businesses to exchange information, because most B2B electronic commerce is an adaptation of EDI or is based on EDI principles. Another important reason for being familiar with EDI is that EDI is still the method used for most electronic B2B transactions. According to one study (see the article by Richard Villars cited in For Further Study and Research at the end of this chapter), the dollar amount of EDI transactions in 2002 was three times the total amount of all other B2B electronic transactions. This section provides you with a brief history of EDI and explains how it works. It also explains why conducting EDI is better than processing mountains of paper transactions.

Early Business Information Interchange Efforts

The emergence of large business organizations in the late 1800s and early 1900s brought with it the need to create formal records of business transactions. In the 1950s, companies began to use computers to store and process internal transaction records, but the information flows between businesses continued to be printed on paper; purchase orders, invoices, bills of lading, checks, remittance advices, and other standard forms were used to document transactions. The process of using a person or computer to generate a paper form, mailing that form, and then having another person enter the data into the trading partner's computer was slow, inefficient, expensive, redundant, and unreliable. By the 1960s, businesses that engaged in large volumes of transactions with each other had begun exchanging transaction information on punched cards or magnetic tape. Advances in data communications technology during the 1960s and 1970s allowed trading

NOTES

partners to transfer data over telephone lines instead of shipping punched cards or magnetic tapes to each other.

Although these information transfer agreements between trading partners increased efficiency and reduced errors, they were not an ideal solution. Because the data translation programs that one trading partner wrote usually would not work for other trading partners, each company participating in this information exchange had to make a substantial investment in computing infrastructure. Only large trading partners could afford this investment, and even those companies had to perform a significant number of transactions to justify the cost. Smaller or lower-volume trading partners could not afford to participate in the benefits of these paper-free exchanges.

In 1968, a number of freight and shipping companies joined together to form the Transportation Data Coordinating Committee (TDCC), which was charged with exploring ways to reduce the paperwork burden that shippers and carriers faced. The TDCC created a standardized information set that included all the data elements that shippers commonly included on bills of lading, freight invoices, shipping manifests, and other paper forms. Instead of printing a paper form, shippers could convert information about shipments into a computer file that conformed to the TDCC standard format. The shipper could electronically transmit that computer file to any freight company that had adopted the TDCC format. The freight company translated the TDCC format into data it could use in its own information systems. The savings from not printing and handling forms, not entering the data twice, and not having to worry about error-correction procedures were significant for most shippers and freight carriers.

Although these early industry-specific data interchange efforts were very helpful, their benefits were limited to members of the industries that created standard-setting groups. In addition, most businesses that are in a particular industry buy goods and services from businesses that are in other industries. For example, a machinery manufacturer might buy materials from steel mills, paint distributors, electrical assembly contractors, and container manufacturers. Also, almost every business needs to buy office supplies and the services of freight and transportation companies. Thus, full realization of EDI's economies and efficiencies required standards that could be used by companies in all industries.

Emergence of Broader EDI Standards

After a decade of fragmented attempts at setting broader EDI standards, a number of industry groups and several large companies decided to mount a major effort to create a set of cross-industry standards for electronic components, mechanical equipment, and other widely used items. The

NOTES

American National Standards Institute (ANSI) has been the coordinating body for standards in the United States since 1918. **ANSI** does not set standards itself, but it has created a set of procedures for the development of national standards and it accredits committees that follow those procedures.

In 1979, ANSI chartered a new committee to develop uniform EDI standards. This committee is called the **Accredited Standards Committee X12 (ASC X12)**. The **ASC X12** committee meets three times each year to develop and maintain EDI standards. The committee and its subcommittees include information systems professionals from more than 800 businesses and other organizations. Membership is open to organizations and individuals who have an interest in the standards. The administrative body that coordinates ASC X12 activities is the **Data Interchange Standards Association (DISA).**

The ASC X12 standard has benefited from the participation of members from a wide variety of industries. The standard currently includes specifications for several hundred **transaction sets**, which are the names of the formats for specific business data interchanges. Figure 4.7 lists some of the more commonly used ASC X12 transaction sets.

Although the X12 standards were quickly adopted by major firms in the United States, in many cases, businesses in other countries continued to use their own national standards. In the mid-1980s, the United Nations Economic Commission for Europe invited both North American and European EDI experts to work together on designing a common set of EDI standards based on the successful experiences of U.S. firms in using the ASC X12 standards. In 1987, the United Nations published its first standards under the title **EDI for Administration, Commerce, and Transport (EDIFACT, or UN/EDIFACT)**. As you can see from Figure 4.8, a number of the commonly used UN/EDIFACT standard transaction sets are similar to those in the ASC X12 standard.

The ASC X12 organization and the UN/EDIFACT group agreed in late 2000 to develop one common set of international standards; however, no date for implementation of the common standards has been set. Both organizations created their transaction sets by extracting the information items from the paper forms used to document business transactions. Some critics of the current EDI standards argue that this reliance on forms has made it difficult for businesses to integrate EDI data flows into their business process-oriented information systems. Unfortunately, changing EDI transaction sets to follow business processes instead of paper transaction forms would require a complete redesign of standards that have become part of many organizations' computing infrastructures over the past 30 years.

NOTES

104 - Air Shipment Information	829 - Payment Cancellation Request
110 - Air Freight Details and Invoice	840 - Request for Quotation
125 - Multilevel Railcar Load Details	841 - Specifications/Technical Information
151 - Electronic Filing of Tax Return Data Acknowledgement	842 - Nonconformance Report
170 - Revenue Receipts Statement	843 - Response to Request for Quotation
180 - Return Merchandise Authorization and Notification	846 - Inventory Inquiry/Advice
204 - Motor Carrier Shipment Information	847 - Material Claim
210 - Motor Carrier Freight Details and Invoice	850 - Purchase Order
213 - Motor Carrier Shipment Status Inquiryry	853 - Routing and Carrier Instruction
214 - Transportation Carrier Shipment Status Message	854 - Shipment Delivery Discrepancy Information
304 - Shipping Instructions	855 - Purchase Order Acknowledgment
317 - Delivery/Pickup Order	856 - Ship Notice/Manifest
325 - Consolidation of Goods in Container	857 - Shipment and Billing Notice
350 - U.S. Customs Release Information	859 - Freight Invoice
404 - Rail Carrier Shipment Information	860 - Purchase Order Change Request–Buyer Initiated
410 - Rail Carrier Freight Details and Invoice	861 - Receiving Advice/Acceptance Certificate
421 - Estimated Time of Arrival and Car Scheduling	865 - Purchase Order Change Acknowledgment/Request–Seller-Initiated
440 - Shipment Weights	867 - Product Transfer and Resale Report
466 - Rate Request	869 - Order Status Inquiry
511 - Requisition	870 - Order Status Report
810 - Invoice	879 - Price Change
812 - Credit/Debit Adjustment	893 - Item Information Request
813 - Electronic Filing of Tax Return Data	920 - Loss or Damage Claim–General Commodities
820 - Payment Order/Remittance Advice	924 - Loss or Damage Claim–Motor Vehicle
828 - Debit Authorization	997 - Functional Acknowledgment
	998 - Set Cancellation

Figure 4.7. *Commonly used ASC X12 transaction sets.*

How EDI Works

Although the basic idea behind EDI is straightforward, its implementation can be complicated, even in fairly simple business situations. For example, consider a company that needs a replacement for one of its metal-cutting machines. This section describes the steps involved in making this purchase using a paper-based system, and then explains how the process would change using EDI. In both of these examples, assume that the vendor uses its own vehicles instead of a common carrier to deliver the purchased machine.

Paper-Based Purchasing Process

The buyer and the vendor in this example are not using any integrated software for business processes internally; thus, each information processing

NOTES

step results in the production of a paper document that must be delivered to the department handling the next step. Information transfer between the buyer and vendor is also paper-based and can be delivered by mail, courier, or fax.

AUTHOR	Authorization	IFTCCA	Forwarding/Transport Shipment Charge Calculation
BOPCUS	Balance of Payment Customer Transaction Report	IFTDGN	Dangerous Goods Notification
BOPDIR	Direct Balance of Payment Declaration	IFTFCC	International Transport Freight Costs/ Other Charges
BOPINF	Balance of Payment Information from Customer	IFTMAN	Arrival Notice
COARRI	Container Discharge/Loading Report	INVOIC	Invoice
COHAOR	Container Special Handling Order	INVRPT	Inventory Report
CONAPW	Advice on Pending Works	ORDCHG	Purchase Order Change Request
CONDPV	Direct Payment Valuation	ORDERS	Purchase Order
CONITT	Invitation to Tender	ORDRSP	Purchase Order Response
CONPVA	Payment Valuation	PAXLST	Passenger List
CONQVA	Quantity Valuation	PAYMUL	Multiple Payment Order
COPRAR	Container Discharge/Loading Order	PAYORD	Payment Order
COREOR	Container Release Order	PRODEX	Product Exchange Reconciliation
COSTCO	Container Stuffing/Stripping Confirmation	QALITY	Quality Data
COSTOR	Container Stuffing/Stripping Order	QUOTES	Quote
CREADV	Credit Advice	RECADV	Receiving Advice
CUSDEC	Customs Declaration	REMADV	Remittance Advice
CUSRES	Customs Response	REQDOC	Request for Document
DEBADV	Debit Advice	REQOTE	Request for Quote
DELFOR	Delivery Schedule	SSREGW	Notification of Registration of a Worker
HANMOV	Cargo/Goods Handling and Movement	STATAC	Statement of Account
IFCSUM	Forwarding and Consolidation Summary	SUPRES	Supplier Response

Figure 4.8. *Commonly used UN/EDIFACT transaction sets.*

Once the production manager in the operating unit decides that the metal-cutting machine needs to be replaced, the following process begins :

- The production manager completes a purchase requisition form and sends it to Purchasing. This requisition describes the machine that is needed to perform the metal-cutting operation.
- Purchasing contacts vendors to negotiate price and terms of delivery. When purchasing has selected a vendor, it prepares a purchase order and forwards it to the mail room.
- Purchasing also sends one copy of the purchase order to the Receiving Department so that Receiving can plan to accept delivery when scheduled; Purchasing sends another copy to Accounting to advise it of the financial implications of the order.

NOTES

- The mail room sends the purchase order it received from Purchasing to the selected vendor by mail or courier.
- The vendor's mail room receives the purchase order and forwards it to its Sales Department.
- The vendor's Sales Department prepares a sales order that it sends to its Accounting Department and a work order that it sends to Manufacturing. The work order describes the machine's specifications and authorizes Manufacturing to begin work on it.

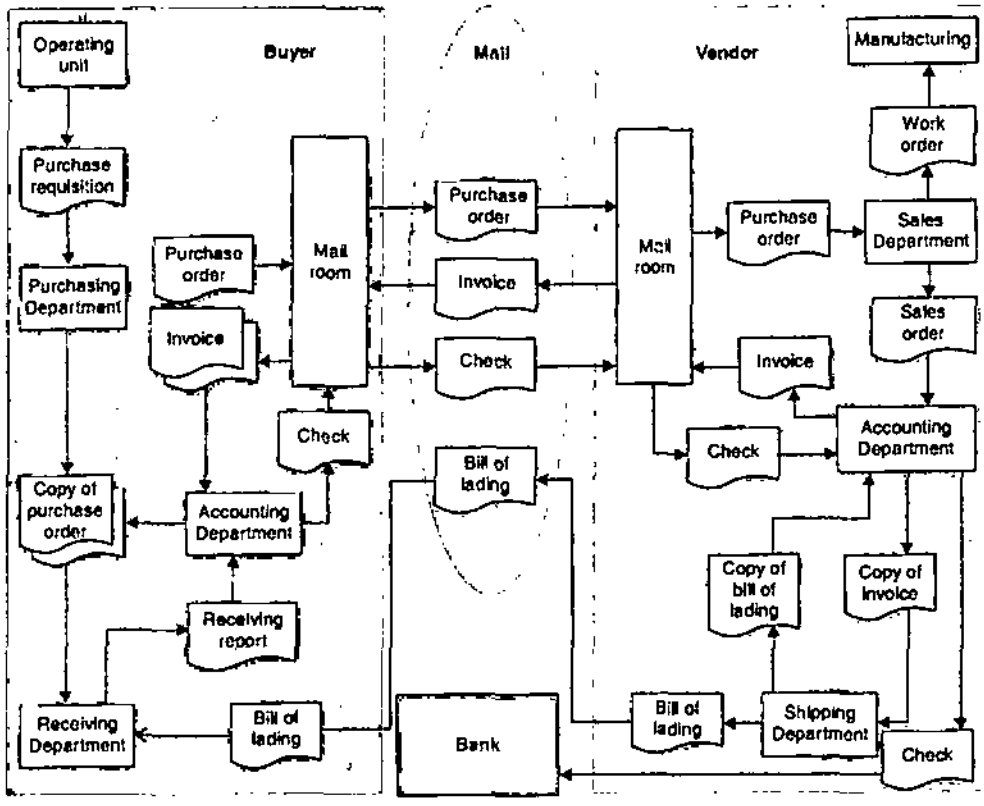


Figure 4.9. *Information flows in a paper-based purchasing process.*

- When the machine is completed, Manufacturing notifies Accounting and sends the machine to shipping.
- The Accounting Department sends the original invoice to the mail room and a copy of the invoice to the Shipping Department.
- The mail room sends the invoice to the buyer by mail or courier.
- The mail room sends the invoice to the buyer by mail or courier.
- The vendor's Shipping Department uses its copy of the invoice to create a bill of lading and sends it with the machine to the buyer.
- The buyer's mail room receives the invoice at about the same time as its Receiving Department receives the machine with its bill of lading.
- The buyer's mail room sends one copy of the invoice to Purchasing so the Purchasing Department knows that the machine was received, and sends the original invoice to Accounting.

NOTES

- The buyer's Receiving Department checks the machine against the bill of lading and its copy of the purchase order. If the machine is in good condition and matches the specifications on the bill of lading and the purchase order, Receiving completes a receiving report and delivers the machine to the operating unit.
- Receiving sends a completed receiving report to Accounting.
- Accounting makes sure that all details on its copy of the purchase order, the receiving report, and the original invoice match. If they do, Accounting issues a check and forwards it to the mail room.
- The buyer's mail room sends the check by mail or courier to the vendor.
- The vendor's mail room receives the check and sends it to Accounting.
- Accounting compares the check to its copies of the invoice, bill of lading, and sales order. If all details match, Accounting deposits the check in the vendor's bank and records the payment received.

EDI Purchasing Process

The information flows that occur in the EDI version of this sample purchasing process are shown in Figure 4.10. The mail service has been replaced with the data communications of an EDI network, and the flows of paper within the buyer's and vendor's organizations have been replaced with computers running EDI translation software.

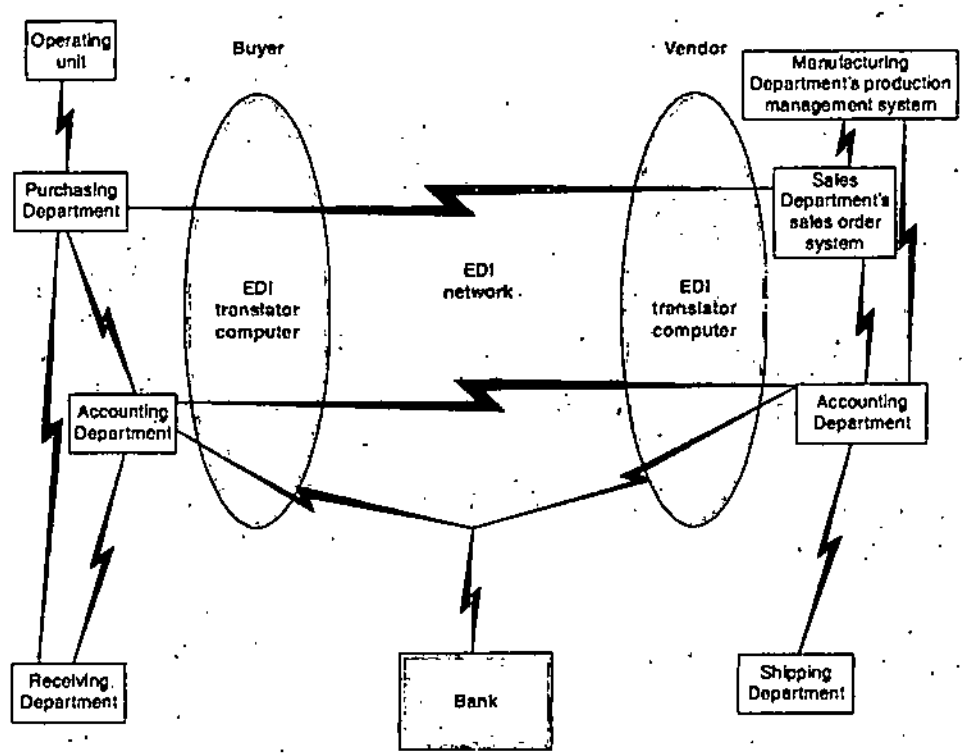


Figure 4.10. *Information flows in an EDI purchasing process.*

NOTES

In the EDI purchasing process, when the operating unit manager decides that the metal-cutting machine needs to be replaced, the following process begins :

- The operating unit manager sends an electronic message to its Purchasing Department. This message describes the machine that is needed to perform the metal-cutting operation.
- Purchasing contacts vendors by telephone, e-mail, or through their Websites to negotiate price and terms of delivery. After selecting a vendor, Purchasing sends a message to the Sales Department announcing the selection.
- The buyer's EDI translator computer converts this message to a standard format purchase order transaction set, and then forwards the message through an EDI network to the vendor.
- Purchasing also sends one electronic message to the buyer's Receiving Department so it can plan to accept delivery when it is scheduled; Purchasing sends another electronic message to the buyer's Accounting Department that includes details such as the agreed purchase price.
- The vendor's EDI translator computer receives the purchase order transaction set message and converts it to the file format used by the vendor's information systems.
- The converted purchase order details appear in the Sales Department's sales order system and are automatically forwarded to the production management system in Manufacturing and to the accounting system.
- The information that was automatically forwarded to Manufacturing describes the machine's specifications and authorizes Manufacturing to begin work on it.
- When the machine is completed, Manufacturing notifies Accounting and sends the machine to the vendor's Shipping Department.
- The vendor's Shipping Department sends an electronic message to its Accounting Department indicating that the machine is ready to ship.
- The vendor's Accounting Department sends a message to its EDI translator computer, which converts the message to the standard invoice transaction set and forwards it through the EDI network to the buyer.
- The buyer's EDI translator computer receives the invoice transaction set before its Receiving Department receives the machine. The computer then converts the invoice data to a format that the buyer's information systems can use. The invoice data becomes immediately available to both the buyer's Accounting and Receiving Departments.
- When the machine arrives, the buyer's Receiving Department checks the machine against the invoice information on its computer system. If the

NOTES

machine is in good condition and matches the specifications shown in the buyer's system, Receiving sends a message to Accounting confirming that the machine has been received in good order. It then delivers the machine to the operating unit.

- The buyer's Accounting Department system compares all details in the purchase order data, receiving data, and decoded invoice transaction set from the vendor. If all the details match, the accounting system notifies its bank to reduce the buyer's account and increase the vendor's account by the amount of the invoice. The EDI network may provide services that perform this task.

Value-Added Networks

EDI reduces paper flow and streamlines the interchange of information among departments within a company and between companies. These efficiencies were responsible for the benefits described in the GE Lighting example presented in the introduction to this chapter. The three key elements shown in Figure 4.11 that alter the process so dramatically are the EDI network (instead of the mail service) that connects the two companies and the two EDI translator computers that handle the conversion of data from the formats used internally by the buyer and the vendor to standard EDI transaction sets. Trading partners can implement the EDI network and EDI translation processes in several ways. Each of these ways uses one of two basic approaches : direct connection or indirect connection.

The first approach, called **direct connection EDI**, requires each business in the network to operate its own on-site EDI translator computer These EDI translator computers are then connected directly to each other using modems and dial-up telephone lines or dedicated leased lines. The dial-up option becomes troublesome when customers or vendors are located in different time zones, and when transactions are time-sensitive or high in volume. The dedicated leased-line option can become very expensive for businesses that must maintain many connections with customers or vendors. Trading partners that use different communications protocols can make either of the direct connection methods difficult to implement.

Instead of connecting directly to each of its trading partners, a company might decide to use the services of a value-added network. To use the services of a VAN, a company must install EDI translator software that iscompatible with the VAN. Often, the VAN supplies this software as part of its operating agreement.

To send an EDI transaction set to a trading partner, the VAN customer connects to the VAN using a dedicated or dial-up telephone line and then forwards the EDI-formatted message to the VAN. The VAN logs the message and delivers it to the trading partner's mail-box on the VAN computer. The

NOTES

trading partner then dials in to the VAN and retrieves its EDI-formatted messages from that mailbox. This approach is called **indirect connection EDI** because the trading partners pass messages through the VAN instead of connecting their computers directly to each other.

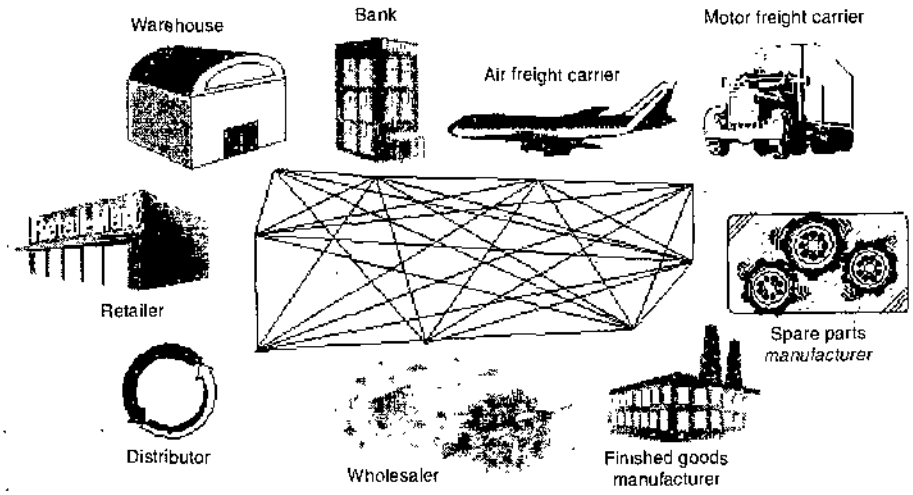


Figure 4.11. *Direct connection EDI.*

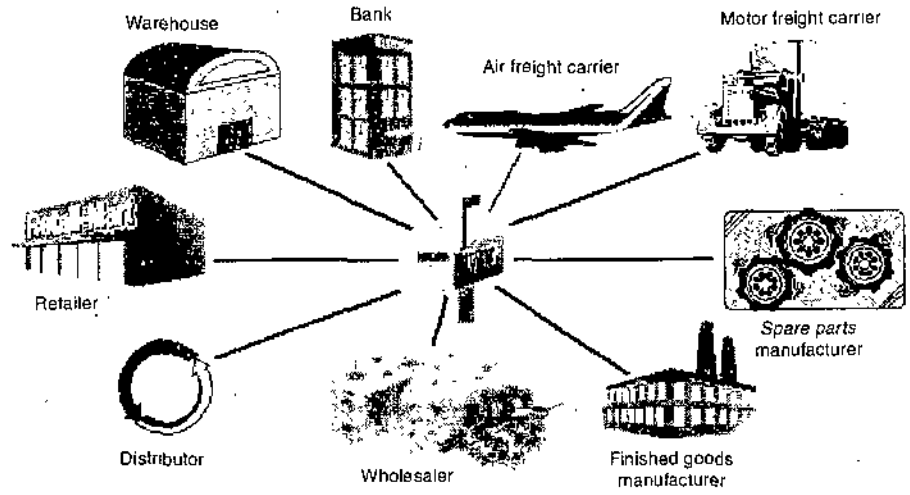


Figure 4.12. *Indirect connection EDI through a VAN.*

Companies that provide VAN services include **Descartes VAN Services**, **EC/EDI**, **GPAS**, **IBM Global Services**, **Kleinschmidt**, and the **Sterling Information Broker**. Advantages of using a VAN are as follows :

- Users need to support only the VAN's one communications protocol instead of many possible protocols used by trading partners.
- The VAN records message activity in an audit log. This VAN audit log becomes an independent record of transactions, and this record can be helpful in resolving disputes between trading partners.

NOTES

- The VAN can provide translation between different transaction sets used by trading partners (for example, the VAN can translate an ASC X12 set into a UN/EDIFACT set).
- The VAN can perform automatic compliance checking to ensure that the transaction set is in the specified EDI format.

VANs do have some disadvantages, however. One major issue is cost. Most VANs require an enrollment fee, a monthly maintenance fee, and a transaction fee. The transaction fee can be based on transaction volume, transaction length, or both. Trading partners with few transactions often find it difficult to justify the high fixed costs of the enrollment and monthly maintenance fees. For example, the up-front cost of implementing indirect connection EDI, including software, VAN enrollment fee, and hardware, can exceed $20,000. Other trading partners with high transaction volumes find the VAN's ongoing transaction-based fees prohibitive.

In the past, many vendors were forced into bearing the high costs of participating in EDI to satisfy the needs of one or two large customers. This happened frequently to suppliers of the auto industry and the retail merchandising industry. Using VANs can become cumbersome and expensive for companies that want to do business with a number of trading partners, each using different VANs. Although some VANs do offer the service of exchanging messages with other VANs, the cost of this service can be unpredictable. Also, inter-VAN transfers do not always provide a clear audit trail for use in dispute resolution. Firms precluded from adopting EDI by its high cost welcomed the Internet as a low-cost communications medium that could help them overcome some of the disadvantages of traditional EDI.

EDI ON THE INTERNET

As the Internet gained prominence as a tool for conducting business, trading partners using EDI began to view the Internet as a potential replacement for the expensive leased lines and dial-up connections required to support both direct and VAN-aided EDI. Companies that had been unable to afford EDI began to look at the Internet as an enabling technology that might get them back in the game of selling to large customers that demanded EDI capabilities from their suppliers.

The major roadblocks to conducting EDI over the Internet initially were concerns about security and the Internet's general inability to provide audit logs and third-party verification of message transmission and delivery. As the basic TCP/IP structure of the Internet was enhanced with secure protocols and other encryption schemes (you will learn about these in Chapter 10), businesses worried less about security issues; however, concerns still existed.

NOTES

The lack of third-party verification continues to be an issue because the Internet has no built-in facility for it. Because EDI transactions are business contracts and often involve large amounts of money, the issue of nonrepudiation is significant. **Nonrepudiation** is the ability to establish that a particular transaction actually occurred. It prevents either party from repudiating, or denying, the transaction's validity or existence. In the past, the nonrepudiation function was provided either by a VAN's audit logs for indirect connection EDI or a comparison of the trading partners' message logs for direct connection EDI.

E-RETAILING

The internet has allowed a new kind of specialization to emerge. Instead of specializing just in a special product line, they allow specialization in particular classes of customers and sellers. Thus, we see lastminute.com, which allows last minute purchases of travel tickets, gift, and entertainment to be matched against last minute sellers of the same items. Here, we see specialization not in a product line but in a class of purchasers and a class of sellers. This kind of specialization would not have been possible before we had the internet.

In addition to these specialized stores, we also get generalized e-stores where a store sells several product lines under a single management. Examples of these generalized stores include JC penny and Walmart.We also have the electronic counterpart of malls or e-malls. E-malls essentially provide a web-hosting service for your individual store much in the way that mall provide a hosting service in the sense of a physical location for your store.

Examples of these e-malls are Yahoo!Store, GEOShops, and CNET Stores :

In the future we may see the equivalent of franchise stores developing. One new class of business that is developing very quickly on the internet is the e-broker. The e-broker does not sell directly to a customer but brings the customer in touch with a particular supplier, so that a given set of criteria specified by the customer is satisfied. For example, the customer may want to buy goods at the cheapest price and so the e-broker would then do a search to find the supplier that would provide the cheapest goods. Or, a customer may want to find a particular kind of goods and the e-broker sets about determining which supplier would provide those goods. This area of e-broking is likely to grow very greatly in the near future.

In summary, we can, therefore, map traditional forms to e-retailing as follows :

NOTES

Specialized stores ® specialized e-stores

Generalized stores ® Generalized e-stores

Malls ® E-malls

Franchise stores ® ?

New form of business : e-broker

Benefits of E-Retailing

To the Customer

Customers enjoy a number of benefits from e-retailing. The first of these is **convenience**. It is convenient for the customer as he does not have to move from shop to shop physically in order to examine goods. He is able to sit in front of a terminal and search the net and examine the information on goods. The second aspect of convenience he gets is in terms of time. Normally, the traditional shop has an opening time and a closing time and the customer can only visit the shop within these periods. On the net, the customer can choose at any time to visit a site to examine the goods that are available and actually carry out his purchasing at one's own convenient time. The third type of convenience that the customer gets is that he has access to a search engine, which will actually locate the products that he describes' and also the site where they may be available, or perhaps even locate the sites where they may be available at the best price. The second type of benefit to customers is better information.

The Internet and the World Wide web are essentially communication media that allow retailers to put on quite extensive information related to their products, which is available to the customers. Furthermore, since the customer can look at several sites, he will be able to obtain different pieces of information from each site to build a far better picture for himself about the products that he is interested in. In some sites, there are customer reviews of different products as well as reviews by the business itself. An example of this can be found on Amazon.com. This allows-the customer to finesse his requirements before actually making the purchase. It also gives different sources of information.

The third type of benefit that the customer gets is **competitive pricing**. This is due to two factors.

- The first is lowered costs to the retailer because he does not have to maintain a physicalshowroom, he does not have to hire several shop assistants, and these savings can be passed on to customers in the form of reduced prices.
- Secondly, competitive pricing pressure that arises from the fact that the customer is now able to look at prices at several sites. Therefore, the

NOTES

pressure is always there on the retailer to maintain a competitive price for his products.

- The third benefit is **customization**. The customer can actually specify the features of the products that he would like and thus in some cases it is possible that the retailer may allow a customized product to be delivered.

An example of this is on the Dell site. The computer site allows shoppers to custom specify their own computer software and hardware configurations. Thus, the customer is able to select exactly what he wants. This ability to get the business to deliver a product that the customer specifies he wants is the essence of C2B e-commerce.

In summary, the benefits of e-retailing to the customer include :

- convenience
- better information
- competitive price.
- customization
- shopping anyWhere, anytime.

So with e-retailing, the customer can shop "anywhere around the globe without being restricted to his local vicinity. He could, for example, purchase goods over_ and have them delivered to a domestic address. He can also shop, as mentioned earlier at any time. These are very considerable benefits of e-retailing to the customer. These benefits could see larger and larger numbers of customers move more and more of their shopping on to e- retailing sites in the future.

To the Business

There are a number of benefits of e-retailing to the business itself.

- The first of these is **global reach**. The retailer now is no longer restricted to customers who are able to reach the store physically. They can be from anywhere around the globe. The retailer must, of course, deliver the goods of a purchase to the customer. We see later that has an impact on the types of goods that are most easily handled through e-retailing.
- The second benefit is better **customer service**. The use of email and the use of electronic interchange of messages between the customer and the retailer allows better communication between the customer and the retailer. These allow one to easily inquiries and deal with complaints. These also allow a much more rapid response time than was possible in the days of faxes and postal mail.

NOTES

- The third benefit is the **lowered capital cost to the retailer.** The retailer does not have to maintain showrooms, he can probably have lower inventories. Thus, while Amazon.com lists over a few million titles, it keeps an inventory of a few thousand best selling titles only. Therefore, the retailer has lower warehousing costs. He does not have to have many shop assistants who are physically answering questions and showing the customer goods.
- The fourth benefit to the retailer is **mass customization.** Based on requests by the customers, the retailer is now able to carry out mass customization with reduced time to market for the customized products.
- The next advantage is **targeted marketing.** The retailer is now able to pick on a specific targeted group of customers and direct marketing towards these customers. The retailer is also able to provide **more value-added services** in the way of better information, add-on services to basic services, or add-on options to products that he is selling.
- The last advantage to the retailer consists of **different new forms of specialized stores that he is now able to utilize.**

As we have mentioned previously, now he does not have to specialize his store based just on a product line but could choose to specialize his store based on a specialized targeted group of customers. It also creates new opportunities for niche marketing.

A summary of the benefits to the e-retailer are :

- global reach
- better customer service
- low capital cost
- mass customization
- targeted marketing
- more value-added services
- new forms of specialized stores and niche marketing.

ELECTRONIC FUNDS TRANSFER (EFT)

EFT is defined as "any transfer of funds initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorize a financial institution to debit or credit an account." EFT utilizes computer and telecommunication components both to supply and to transfer money or financial assets.

NOTES

Transfer is information-based and intangible. Thus EFT stands in marked contrast to conventional money and payment modes that rely on physical delivery of cash or checks (or other paper orders to pay) by truck, train, or airplane. Work on EFT can be segmented into three broad categories :

Banking and Financial Payments

- Large-scale or wholesale payments (*e.g.*, bank-to-bank transfer).
- Small-scale or retail payments (*e.g.*, automated teller machines and cash dispensers).
- Home banking (*e.g.*, bill payment).

Retailing Payments

- Credit cards (*e.g.*, VISA or MasterCard).
- Private label credit/debit cards (*e.g.*, J.C. Penney Card).
- Charge cards (*e.g.*, American Express).

On-line electronic commerce payments

- Token-based payment systems

  Electronic cash (*e.g.*, DigiCash)

  Electronic checks (*e.g.*, NetCheque)

  Smart cards or debit cards (*e.g.*, Mondex Electronic Currency Card).
- **Credit card-based payment systems**

  Encrypted credit cards (*e.g.*, World Wide Web formbased encryption) Third-party authorization numbers (*e.g.*, First Virtual)

Electronic Cash (E-cash)

E-cash focuses on replacing cash as the principal, payment vehicle in consumer-oriented electronic payments. Although it may be surprising to some, cash is still the most prevalent consumer payment instrument even after thirty years of continuous developments in electronic payment systems.

Cash remains the dominant form of payment for three reasons :

(1) lack of trust in the banking system,

(2) inefficient clearing and settlement of non-cash transactions, arid

(3) negative real interest rates paid on bank deposits.

These reasons seem like issues seen primarily in developing countries. Not true. Even in the most industrialized countries, the ratio of notes and coins in circulation per capita is quite large and is estimated to range from $446 to $2748. Consider the situation in two of the most industrialized nations in

NOTES

world : the United States and the United Kingdom. In the United States, there supposedly was about $300 billion of notes and coins in circulation in 1992. Interestingly, this number is not shrinking but growing at approximately 8 percent per year. Deposits by check are growing by only 6 percent per year. It has been reported that in the United Kingdom about a quarter of all "spontaneous" payments over 100 pounds sterling are still made with cash. For payments under five pounds sterling, the percentage is 98 percent. The predominance of cash indicates an opportunity for innovative business practice that revamps the purchasing process where consumers are heavy users of cash. To really displace cash, the electronic payment systems need to have some qualities of cash that current credit and debit cards lack. For example, cash is negotiable, meaning it can be given or traded to someone else. Cash is legal tender, meaning the payee is obligated to take it. Cash is a bearer instrument, meaning that possession is prima facie proof of ownership. Also, cash can be held and used by anyone even those who don't have a bank account, and cash places no risk on the part of the acceptor that the medium of exchange may not be good.

Now compare cash to credit and debit cards. First, they can't be given away because, technically, they are identification cards owned by the issuer and restricted to one user. Credit and debit cards are not legal tender, given that merchants have the right to refuse to accept them. Nor are credit and debit cards bearer instruments; their usage requires an account relationship and authorization system. Similarly, checks require either personal knowledge of the payer or a check guarantee system. Hence, to really create a novel electronic payment method, we need to do more than recreate the convenience that is offered by credit and debit cards. We need to develop e-cash that has some of the properties of cash.

Properties of Electronic Cash

Of the many ways that exist for implementing an e-cash system, all must incorporate a few common features. Specifically, e-cash must have the following four properties : monetary value, interoperability, irretrievability, and security.

E-cash must have a monetary value, bank authorized credit, or a bank-certified cashier's check. When e-cash created by one bank is accepted by others, reconciliation must occur without any problems. Stated, another way, e-cash without proper bank certification carries the risk that when deposited, it might be returned for insufficient funds.

E-cash must be interoperable—that is, exchangeable as payment for other e-cash, paper cash, goods or services, lines of credit, deposits in banking accounts, bank notes or obligations, electronic benefits transfers, and the like. Most e-cash proposals use a single bank. In practice, multiple banks

NOTES

are required with an international clearinghouse that handles the exchangeability issues because all customers are not going to be using the same bank or even be in the same country.

E-cash must be storable and retrievable. Remote storage and retrieval (*e.g.,* from a telephone or personal communications device) would allow users to exchange e-cash (*e.g.,* withdraw from and deposit into banking accounts) from home or office or while traveling. The cash could be stored on a remote computer's memory, in smart cards, or in other easily transported standard or special-purpose devices. Because it might be easy to create counterfeit cash that is stored in a computer, it might be preferable to store cash on a dedicated device that cannot be altered. This device should have a suitable interface to facilitate personal authentication using passwords or other means and a display so that the user can view the card's contents. One example of a device that can store e-cash is the Mondex card-a pocket-sized electronic wallet.

E-cash should not be easy to copy or tamper with while being exchanged; this includes preventing or detecting duplication and double-spending. Counterfeiting poses a particular problem, since a counterfeiter may, in the Internet environment, be anywhere in the world and consequently be difficult to catch without appropriate international agreements.

Detection is essential in order to audit whether prevention is working. Then there is the tricky issue of double spending. For instance, you could use your e-cash simultaneously to buy something in Japan, India, and England. Preventing double spending from occurring is extremely difficult if multiple banks are involved in the transaction. For this reason, most systems rely on post-fact detection and punishment. Now we will see the concept of Electronic Cash actually works.

Electronic Cash in Action

Electronic cash is based on cryptographic systems called "digital signatures". This method involves a pair of numeric keys (very large integers or numbers) that work in tandem : one for locking (or encoding) and the other for unlocking (or decoding). Messages encoded with one numeric key can only be decoded with the other numeric key and none other. The encoding key is kept private and the decoding key is made public. By supplying all customers (buyers and sellers) with its public key, a bank enables customers to decode any message (or currency) encoded with the bank's private key. If decoding by a customer yields a recognizable message;" the customer can be fairly confident that only the bank could have encoded it. These digital signatures are as secure as the mathematics involved and have proved over.the past two decades to be more resistant to forgery than handwritten signatures. Before e-cash can be used to buy products or ser-vices, it must be procured from a currency server.

NOTES

Purchasing E-cash from Currency Servers

The purchase of e cash from an on-line currency server (or bank) involves two steps :

(1) establishment of an account and

(2) maintaining enough money in the account to back the purchase.

Some customers might prefer to purchase e-cash with paper currency, either to maintain anonymity or because they don't have a bank account. Currently, in most e-cash trials all customers must have an account with a central on-line bank. This is overly restrictive for international use and multi-currency transactions, for customers should be able to access and pay for foreign services as well as local services. To support this access, e-cash must be available in multiple currencies backed by several banks. A service provider in one country could then accept tokens of various currencies from users in many different countries, redeem them with their issuers, and have the funds transferred back to banks in the local country. A possible solution is to use an association of digital banks similar to organizations like VISA to serve as a clearinghouse for many credit card issuing banks.

And finally, consumers use the e-cash software on the computer to generate a random number, which serves as the "note." In exchange for money debited from the customer's account, the bank uses its private key to digitally sign the note for the amount requested and transmits the note back to the customer.The network currency server, in effect, is issuing a "bank note," with a serial number and a dollar amount. By digitally signing it, the bank is committing itself to back that note with its face value in real dollars.This method of note generation is very secure, as neither the customer (payer) nor the merchant (payee) can counterfeit the bank's digital signature (analogous to the watermark in paper currency). Payer and payee can verify that the payment is valid, since each knows the bank's public key. The bank is protected against forgery, the payee against the bank's refusal to honor a legitimate note, and the user against false accusations and invasion of privacy.

How does this Process Work in Practice ?

In the case of DigiCash, every person using e-cash has an e-cash account at a digital bank (First Digital Bank) on the Internet. Using that account, people can withdraw and deposit e-cash. When an e-cash withdrawal is made, the PC of the e-cash user calculates how many digital coins of what denominations are needed to withdraw the requested amount. Next, random serial numbers for those coins will be generated and the blinding (random number) factor will be included. The ' " result of these calculations will be sent to the digital bank. The bank will encode the blinded numbers with its secret key (digital signature) and at the same time debit the account of the client for the same amount. The authenticated coins are sent back to the

NOTES

user and finally the user will take out the blinding factor that he or she introduced earlier. The serial numbers-plus their signatures are now digital coins; their value is guaranteed by the bank. Electronic cash can be completely anonymous. Anonymity allows free-dom of usage—to buy illegal products such as drugs or pornographic material or to buy legal product and services. This is accomplished in the following manner. When the e-cash software generates a note, it masks the original number or "blinds" the note using a random number and transmits it to a bank. The "blinding" carried out by the customer's software makes it impossible for anyone to link payment to payer. Even the bank can't connect the signing with the payment, since the customer's original note number was blinded when it was signed. In other words, it is a way of creating anonymous, untraceable currency. What makes it even more interesting is that users can prove unequivocally that they did or did not make a particular payment. This allows the bank to sign the "note" without ever actually knowing how the issued currency will be used. For those readers who are mathematically inclined, the protocol behind blind signatures is presented.

The customer's software chooses a blinding factor, R, independently and uniformly at random and presents the bank with (XR)E (mod PQ),where X is the note number to be signed and £ is the bank's public key.

1. The bank signs it : (XRE)D = RXD (mod PQ). D is the bank's private key.
2. On receiving the currency, the customer divides out the blinding factor : (RXD)/R = XD (mod PQ).
3. The customer stores XD, the signed note that is used to pay for the purchase of products or services. Since R is random, the bank cannot deter-mine X and thus cannot connect the signing with the subsequent payment. While blinding works in theory, it remains to be seen how it will be used in the real business world.

STUDENT ACTIVITY

1. How debit card is different from credit card ?

2. What are the benefits of E retailing for a customer ?

SUMMARY

NOTES

- In this section, you learned that businesses are using six main approaches to generate revenue on the Web : the Web catalog, digital content sales, advertising-supported, advertisingsubscription mixed, fee-for-transaction, and fee-for-service models. You learned how these models work and what kinds of businesses use which models. You also learned that some companies have changed models as they learned more about their customers and the business environment in which their Websites operate.
- Companies sometimes face the challenges of channel conflict and cannibalization either within their own organizations or with the companies that have traditionally provided sales distribution to consumers for them. You learned that business-to-consumer mobile commerce has not yet been widely successful; however, increasing bandwidth could make it possible for new services to emerge that will be successful.
- By understanding how the Web differs from other media and by designing a Website to capitalize on those differences, companies can create an effective Web presence that delivers value to visitors. Every organization must realize that visitors to its Website arrive with a variety of expectations, prior knowledge, and skill levels, and are connected to the Internet through different technologies. Knowing how these factors can affect the visitor's ability to navigate the site and extract information from the site can help organizations design better, more usable Websites. Enlisting the help of users when building test versions of the Website is also a good way to create a Website that represents the organization well.
- Firms must understand the nature of communication on the Web so they can use it to identify and reach the largest possible number of customers and qualified prospects. Using a many-to-one communications model enables Websites to effectively reach potential customers.
- Electronic payment means making payments electronically *i.e.*, through computer and telecommunication components.
- Electronic tokens are designed as electronic analogs of various forms of payment backed by a bank or financial institution.
- Electronic tokens are of three types : **Cash or real-time, Debit or prepaid and Credit or postpaid.**
- Electronic cash is based on cryptographic systems called "digital signatures".

NOTES

SELF ASSESSMENT QUESTIONS

1. Discuss the various Electronic Payment Systems.
2. How do you differentiate between traditional and E-retailing ?
3. Discuss various success factors for traditional retailing.
4. What is the difference between an electronic distributor and e-broker ?
5. Is Internet Commerce always global ? When does it become regional ?
6. Which business model was more successful : generalized e-brokers or specialized e-stores ?

❑❑❑