Chapter 1

INTERNET & WEBSITE ESTABLISHMENTS

1.0 OBJECTIVES

After studying this chapter you will be able to :

- explain internet resources available for commerce.
- discuss different web server technologies.
- describe applications and internet tools relevant to commerce
- explain what is minimalist website establishment.

1.1 INTRODUCTION

The Internet has revolutionized the computer and communications world like nothing before. The invention of the telegraph, telephone, radio, and computer set the stage for this unprecedented integration of capabilities. The Internet is at once a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location. The Internet represents one of the most successful examples of the benefits of sustained investment and commitment to research and development of information infrastructure. Beginning with the early research in packet switching, the government, industry and academia have been partners in evolving and deploying this exciting new technology. Today, terms like "abc@gmail.com" and "http://www.google.com" trip lightly off the tongue of the random person on the street.

The Internet today is a widespread information infrastructure, the initial prototype of what is often called the National (or Global or Galactic) Information Infrastructure. Its history is complex and involves many aspects - technological, organizational, and community. And its influence reaches not only to the technical fields of computer communications but throughout society as we move toward increasing use of online tools to accomplish electronic commerce, information acquisition, and community operations.

1.2 INTERNET RESOURCES FOR COMMERCE

Commercialization of the Internet

Commercialization is the process or cycle of introducing a new product into the market. The actual launch of a new product is the final stage of new product development, and the one where the most money will have to be spent for advertising, sales promotion, and other marketing efforts. In the case of a new consumer packaged goods, costs will be at least $10 million, but can reach up to $200 million. Commercialization of the Internet involved not only the development of competitive, private network services, but also the development of commercial products

implementing the Internet technology. In the early 1980s, dozens of vendors were incorporating TCP/IP into their products because they saw buyers for that approach to networking. Unfortunately they lacked both real information about how the technology was supposed to work and how the customers planned on using this approach to networking. Many saw it as a nuisance add-on that had to be glued on to their own proprietary networking solutions: SNA, DECNet, Netware, NetBios. The DoD had mandated the use of TCP/IP in many of its purchases but gave little help to the vendors regarding how to build useful TCP/IP products.

In 1985, recognizing this lack of information availability and appropriate training, Dan Lynch in cooperation with the IAB arranged to hold a three day workshop for ALL vendors to come learn about how TCP/IP worked and what it still could not do well. The speakers came mostly from the DARPA research community who had both developed these protocols and used them in day to day work. About 250 vendor personnel came to listen to 50 inventors and experimenters. The results were surprises on both sides: the vendors were amazed to find that the inventors were so open about the way things worked (and what still did not work) and the inventors were pleased to listen to new problems they had not considered, but were being discovered by the vendors in the field. Thus a two way discussion was formed that has lasted for over a decade.

After two years of conferences, tutorials, design meetings and workshops, a special event was organized that invited those vendors whose products ran TCP/IP well enough to come together in one room for three days to show off how well they all worked together and also ran over the Internet. In September of 1988 the first Interop trade show was born. 50 companies made the cut. 5,000 engineers from potential customer organizations came to see if it all did work as was promised. It did. Why? Because the vendors worked extremely hard to ensure that everyone's products interoperated with all of the other products - even with those of their competitors. The Interop trade show has grown immensely since then and today it is held in 7 locations around the world each year to an audience of over 250,000 people who come to learn which products work with each other in a seamless manner, learn about the latest products, and discuss the latest technology.

In parallel with the commercialization efforts that were highlighted by the Interop activities, the vendors began to attend the IETF meetings that were held 3 or 4 times a year to discuss new ideas for extensions of the TCP/IP protocol suite. Starting with a few hundred attendees mostly from academia and paid for by the government, these meetings now often exceed a thousand attendees, mostly from the vendor community and paid for by the attendees themselves. This self-selected group evolves the TCP/IP suite in a mutually cooperative manner. The reason it is so useful is that it is comprised of all stakeholders: researchers, end users and vendors.

Network management provides an example of the interplay between the research and commercial communities. In the beginning of the Internet, the emphasis was on defining and implementing protocols that achieved interoperation. As the network grew larger, it became clear that the sometime ad hoc procedures used to manage the network would not scale. Manual configuration of tables was replaced by distributed automated algorithms, and better tools were devised to isolate faults. In 1987 it became clear that a protocol was needed that would permit the elements of the network, such as the routers, to be remotely managed in a uniform way. Several protocols for this purpose were proposed, including Simple Network Management Protocol or SNMP (designed, as its name would suggest, for simplicity, and derived from an earlier proposal called SGMP), HEMS (a more complex design from the research community) and CMIP (from the OSI community). A series of meeting led to the decisions that HEMS would be withdrawn as a candidate for standardization, in order to help resolve the contention, but that work on both SNMP and CMIP would go forward, with the idea that the SNMP could be a more near-term solution and CMIP a longer-term approach. The market could choose the one it found more suitable. SNMP is now used almost universally for network based management.

In the last few years, we have seen a new phase of commercialization. Originally, commercial efforts mainly comprised vendors providing the basic networking products, and service providers offering the connectivity and basic Internet services. The Internet has now become almost a "commodity" service, and much of the latest attention has been on the use of this global information infrastructure for

support of other commercial services. This has been tremendously accelerated by the widespread and rapid adoption of browsers and the World Wide Web technology, allowing users easy access to information linked throughout the globe. Products are available to facilitate the provisioning of that information and many of the latest developments in technology have been aimed at providing increasingly sophisticated information services on top of the basic Internet data communications.

The Web breakthrough

Today, access to the internet is accomplished via a set of tools that make the internet easier to navigate. The web is one of the most effective methods to access and collect internet information because of its visual format and advanced features. Web application programs can also access many of the other internet services, such as Gopher, Usenet news, and file transfer, remote connectivity, can provide special access to data on the local intranet, such as database access, and can even customize programs for one's own needs. The web can be used as a complete presentation media for a company's corporate information or information on its products and services.

Sometimes the web servers are also called *web sites*. Web servers run on different types of hardware/software servers. The web server can be grouped into UNIX servers, Windows NT servers, VMS servers, Macintosh servers, OS/2 servers, and Windows 3.1 servers. A web server is a program that offers a service that can be reached over the network. An executive program is a client when it sends a request to a server and waits for a response. Conversely, a client can request services from many different servers. Common World Wide Web clients (browsers) available commercially include Explorer, Mozilla. The web clients can make requests of web servers and also other servers such as Gopher, FTP, news and mail servers.

New, innovative ideas have been developed around the web. For example, the weather reports have been available on the internet for years; when the web became available, local and national, weather forecasts became available with a click of button on a map of area. Other ideas include a food delivery service through an online menu; an office scheduling program for a large department; a technical support program where comments are mailed to the technical support staff and return calls are made directly by telephone or answered by e-mail; and a variety of electronic magazines and periodicals. Presently, there is a lot of government information available online on the internet: there are over 140 departments, national labs, institutes, state governments, and public utilities that are already connected to the internet.

In comparison to the ease and speed with which users can shop in virtual malls, paying for their purchases with a traditional credit card transaction or a check will increasingly appear to slow and cumbersome. Several innovators have recognized the need for "network cash", and have developed systems that make it easy for buyers and sellers to settle their accounts. Although internet users may view marketing and advertising information online, and even make a purchase decision based on that information, until deployment or SET, purchase transactions are primarily conducted over the telephone or fax machine for these reasons. Because of this, most markets on the internet still offer toll-free telephone and fax numbers within their online storefronts.

Publishers can save printing costs by publishing electronic information. Users can then use the browser to reach a company's servers for the latest information. Furthermore, facts and data can be updated immediately, without having to reprint outdated items. Any kind of data can be made available to people on the internet through the use of browsers, even a combination of graphics, text, video, and sound that presents a full multimedia experience to the people accessing the information. Small businesses can set up a presence on the internet by publishing a World Wide Web page with a local internet service provider. Then, using a browser, a customer can have direct, online access to the company, its products, and latest information included on the company's home web page.

How to connect to the internet

Terminal access services are the least expensive form of internet access. Terminal access provides an internet user with a dial-in service to the access

provider's network. Access is through a shared resource on someone else's link to the internet. The user is normally required to follow all rules regarding the usage of these services. The user dials into the remote network with a terminal application package and must connect to the remote computer system through a computer account. Once, the user has logged in to the remote machine the user can access the services of the internet. These connections allow a user to connect a local machine or network through a pair of modems, communication over regular telephone lines, to the remote network of the internet access provider. The speed of such a connection depends upon the speed of the modems in use.

Point-to-point dedicated link actually places a user's computer or network on the internet. This is a costlier option, since it involves the purchase of special hardware (router) or computer systems depending upon the type of service. Charges for a point-to-point network link vary depending upon the speed of access. It can range anywhere from $3000 per month for a dedicated DS1/T1 link, to $10,000 for a full speed Ethernet-protocol link. Point-to-point links come in a variety of forms and prices based on speed and security considerations. The internet access provider has such a link to other networks on the internet. The access provider can, in turn, connect the organization's machine and network to its own network and with the issue of internet addresses for the organizations computer, the user can be on the internet. This kind of link also requires that the user run TCP/IP stack software at the local site. Such software varies in cost and availability depending upon the computer operating system at the local site.

Higher speeds than achievable with dial-up connections are possible here. This includes the use of frame relay over 56-kbps/1.544-Mbps links and dedicated lines operating at DS1 (1.544 Mbps) or at DS3 speeds (approx 45 Mbps). Even higher speeds are possible through technologies such as Asynchronous Transfer Mode (ATM): speeds from 45 to 622 Mbps are achievable, although these are still relatively rare. Other technologies such as ISDN offer cost-effective methods at reasonably fast speeds of 56 kbps in US and 64kbps in Asia. These higher speed services often require network equipment such as routers and digital lines. These solutions are viable when the amount of data traffic over the link exceeds 1 GB a day or if speed of access is of importance.

Browsers

Browsers are sometimes also called web clients since they get information from a server. A web browser or Internet browser is a software application for retrieving, presenting, and traversing information resources on the World Wide Web. An *information resource* is identified by a Uniform Resource Identifier (URI) and may be a web page, image, video, or other piece of content Hyperlinks present in resources enable users to easily navigate their browsers to related resources.

Although browsers are primarily intended to access the World Wide Web, they can also be used to access information provided by Web servers in private networks or files in file systems. Some browsers can also be used to save information resources to file systems. The primary purpose of a web browser is to bring information resources to the user. This process begins when the user inputs a Uniform Resource Identifier (URI), for example *http://en.wikipedia.org/*, into the browser. The prefix of the URI determines how the URI will be interpreted. The most commonly used kind of URI starts with *http:* and identifies a resource to be retrieved over the Hypertext Transfer Protocol (HTTP). Many browsers also support a variety of other prefixes, such as *https:* for HTTPS, *ftp:* for the File Transfer Protocol, and *file:* for local files. Prefixes that the web browser cannot directly handle are often handed off to another application entirely. For example, *mailto:* URI's are usually passed to the user's default e-mail application and *news:* URI's are passed to the user's default newsgroup reader.

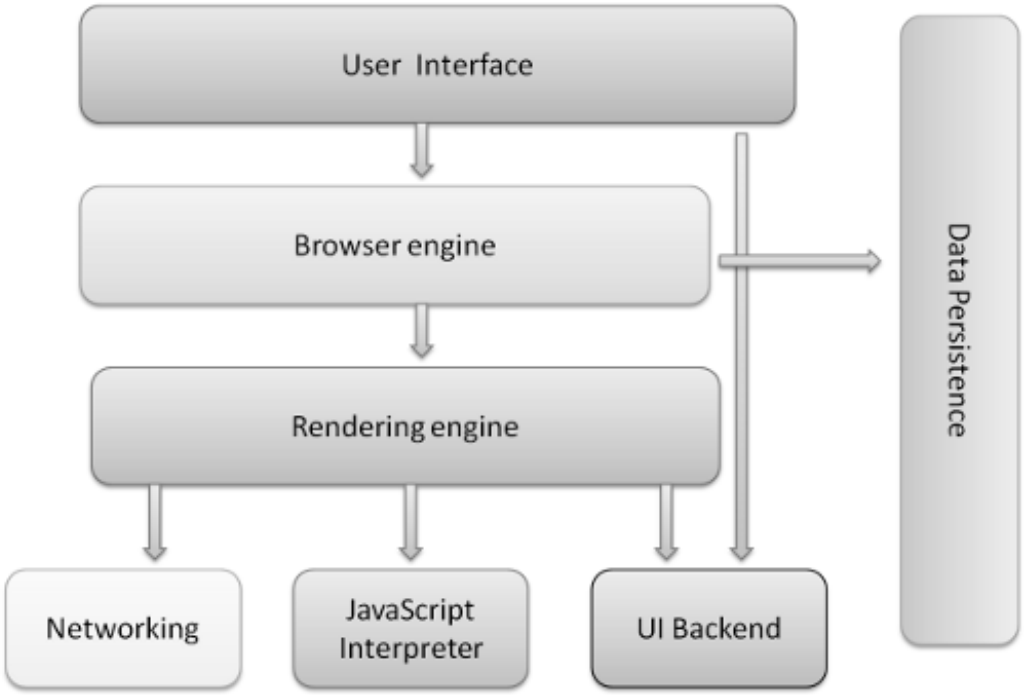
In the case of *http*, *https*, *file*, and others, once the resource has been retrieved the web browser will display it. HTML is passed to the browser's layout engine to be transformed from markup to an interactive document. Aside from HTML, web browsers can generally display any kind of content that can be part of a web page. Most browsers can display images, audio, video, and XML files, and often have plug-ins to support Flash applications and Java applets. Upon encountering a file of an unsupported type or a file that is set up to be downloaded rather than displayed, the browser prompts the user to save the file to disk.

Interactivity in a web page can also be supplied by JavaScript, which usually does not require a plug-in. JavaScript can be used along with other technologies to allow "live" interaction with the web page's server via AJAX. Information resources may contain hyperlinks to other information resources. Each link contains the URI of a resource to go to. When a link is clicked, the browser navigates to the resource indicated by the link's target URI, and the process of bringing content to the user begins again.

The browser's main components are:

1. The user interface - this includes the address bar, back/forward button, bookmarking menu etc. Every part of the browser display except the main window where you see the requested page.
2. The browser engine - the interface for querying and manipulating the rendering engine.
3. The rendering engine - responsible for displaying the requested content. For example if the requested content is HTML, it is responsible for parsing the HTML and CSS and displaying the parsed content on the screen.
4. Networking - used for network calls, like HTTP requests. It has platform independent interface and underneath implementations for each platform.
5. UI backend - used for drawing basic widgets like combo boxes and windows. It exposes a generic interface that is not platform specific. Underneath it uses the operating system user interface methods.
6. JavaScript interpreter. Used to parse and execute the JavaScript code.
7. Data storage. This is a persistence layer. The browser needs to save all sorts of data on the hard disk, for examples, cookies. The new HTML specification (HTML5) defines 'web database' which is a complete (although light) database in the browser.

Figure 1.1 Browser's main components



There are five major browsers used today - Internet Explorer, Firefox, Safari, Chrome and Opera. According to the W3C browser statistics, currently, the usage share of Firefox, Safari and Chrome together is nearly 60%. So nowadays open source browsers are a substantial part of the browser business.

1.1 & 1.2 Check your Progress

Fill in the blank.

a. ……..is the process or cycle of introducing a new product into the market.

b. The…….is one of the most effective methods to access and collect internet information.

c. ……actually places a user's computer or network on the internet.

d. ……..are sometimes also called web clients since they get information from a server.

1.3 WEB SERVER TECHNOLOGIES

- **HTML**

HTML, which stands for Hypertext Markup Language, is the predominant markup language for web pages. A markup language is a set of markup tags, and HTML uses markup tags to describe web pages. HTML is written in the form of HTML elements consisting of "tags" surrounded by angle brackets (like <html>) within the web page content. HTML tags normally come in pairs like and . The first tag in a pair is the start tag, the second tag is the end tag (they are also called opening tags and closing tags). The purpose of a web browser is to read HTML documents and display them as web pages. The browser does not display the HTML tags, but uses the tags to interpret the content of the page.

HTML elements form the building blocks of all websites. HTML allows images and objects to be embedded and can be used to create interactive forms. It provides a means to create structured documents by denoting structural semantics for text such as headings, paragraphs, lists, links, quotes and other items. It can embed scripts in languages such as JavaScript which affect the behavior of HTML web pages. HTML can also be used to include Cascading Style Sheets (CSS) to define the appearance and layout of text and other material. The W3C, maintainer of both HTML and CSS standards, encourages the use of CSS over explicit presentational markup.

Semantic HTML

Semantic HTML is a way of writing HTML that emphasizes the meaning of the encoded information over its presentation (look). HTML has included semantic markup from its inception, but has also included presentational markup such as <font>, <i> and tags. There are also the semantically neutral span and div tags. Since the late 1990s when Cascading Style Sheets were beginning to work in most browsers, web authors have been encouraged to avoid the use of presentational HTML markup with a view to the separation of presentation and content.

In a 2001 discussion of the Semantic Web, Tim Berners-Lee and others gave examples of ways in which intelligent software 'agents' may one day automatically trawl the Web and find, filter and correlate previously unrelated, published facts for the benefit of human users. Such agents are not commonplace even now, but some of the ideas of Web 2.0, price comparison websites may be coming close. The main difference between these web application hybrids and Berners-Lee's semantic agents lies in the fact that the current aggregation and hybridization of information is usually designed in by web developers, who already know the web locations and the API semantics of the specific data they wish to mash, compare and combine.

Good semantic HTML also improves the accessibility of web documents. For example, when a screen reader or audio browser can correctly ascertain the structure of a document, it will not waste the visually impaired user's time by reading out repeated or irrelevant information when it has been marked up correctly.

HTML editors

Know the difference between web design software and e-commerce software. Web design software (commonly referred to as "HTML editors") provides you with the basic tools for designing a website. Only those readers developing a brochure-ware site or going the email order processing route should consider using this type of

product. For those readers taking one of these paths to e-commerce, any of the following products should suffice:

- ***CoffeeCup HTML Editor*** (www.coffeecup.com). This software makes it easy for even a novice to create a website. It comes with more than 40 website templates, 125 JavaScripts, a DHTML menu builder, numerous graphics, wizards for frames, tables, forms, fonts, and more. It also provides helpful and easy-to-follow documentation on how to use the software. Cost $70.
- ***EZGenerator*** (www.ezgenerator.com). Working with this software is almost as easy as working with a word processor. You have to just type, select or drag-and-drop your pages to build your website. The product provides 2000 template variations so you can change the look and feel in one simple click of the mouse. It also automatically (well almost) creates your website navigation for you as you create new web pages and categories. Cost $100.
- ***HotDog Web Editor*** (www.sausagetools.com). This is one of the most popular HTML editors. The HotDog Pro 7.3 provides a comprehensive set of web editing tools including Linkbot, Interactor, and Paint Shop Pro. As such, the HotDog Pro provides the web designer with the complete tools for the creation and management of a professional website. But it still offers intuitive features and customizable tools so that even the novice user can create great looking websites. Cost $100.
- ***Microsoft FrontPage*** (www.Microsoft.com). If you are a first time web designer, this may be the product for you. Frontpage can help the novice to get their website up and running easily and quickly, especially if the designer is familiar with the Microsoft Office suite of products since it uses some of same buttons and commands. The WYSIWYG (What You See Is What You Get) interface is invaluable since you don't really need to understand HTML codes and scripts. This turnkey product also makes its easy to add DHTML effects (changes on demand are also quite simple). The product has an insert form function, too, which makes adding forms for emails and guest books a breeze. The primary problem with Frontpage 2002 is that if you aren't hosting your website yourself, you may have to work a bit harder to find a web-hosting service that allows FrontPage extensions. Cost $150.
- ***SiteDesigner*** (www.sitedesigner.com). SiteDesigner is a WYSIWYG website authoring tool, that has a drag and drop editor. This makes SiteDesigner extremely easy to use. Once you set up a master page for your site (using the templates that are included with SiteDesigner, or using your own images), every web page you create thereafter can inherit that master page's properties. The SiteDesigner generates extremely clean HTML code (some WYSIWYG editors add a lot of unnecessary codes meaning pages are harder to troubleshoot and take longer to load). Cost $100.
- ***Stone's WebWriter*** (www.webwriter.dk/english/index.htm). This award winning Danish no-nonsense HTML editor offers easy-to-use dialogues, right-click editing, code completion, and syntax high-lighting so you can design your website without knowing HTML. WebWriter is for the professional as well as the beginner. With WebWriter you can build JavaScript, Cascading Style Sheets, and image maps. Cost -Free (private use) to $800 (for a large enterprise that needs unlimited licenses).

Hypermedia

Hypermedia is used as a logical extension of the term hypertext in which graphics, audio, video, plain text and hyperlinks intertwine to create a generally non-linear medium of information. This contrasts with the broader term multimedia, which may be used to describe non-interactive linear presentations as well as hypermedia. It is also related to the field of Electronic literature. The term was first used in a 1965 article by Ted Nelson. The World Wide Web is a classic example of hypermedia, whereas a non-interactive cinema presentation is an example of standard multimedia due to the absence of hyperlinks.

Hypermedia may be developed a number of ways. Any programming tool can be used to write programs that link data from internal variables and nodes for external data files. Multimedia development software such as Adobe Flash, Adobe Director, Macromedia Authorware, and MatchWare Mediator may be used to create stand-alone

hypermedia applications, with emphasis on entertainment content. Some database software such as Visual FoxPro and FileMaker Developer may be used to develop stand-alone hypermedia applications, with emphasis on educational and business content management.

Hypermedia applications may be developed on embedded devices for the mobile and the Digital signage industries using the Scalable Vector Graphics (SVG) specification from W3C (World Wide Web Consortium). Software applications such as Ikivo Animator and Inkscape simplify the development of Hypermedia content based on SVG. Embedded devices such as iPhone natively support SVG specifications and may be used to create mobile and distributed Hypermedia applications.

- **Data Collection**

Web analytics is the measurement, collection, analysis and reporting of internet data for purposes of understanding and optimizing web usage. Web analytics is not just a tool for measuring website traffic but can be used as a tool for business research and market research. Web analytics applications can also help companies measure the results of traditional print advertising campaigns. It helps one to estimate how the traffic to the website changed after the launch of a new advertising campaign. Web analytics provides data on the number of visitors, page views, etc. to gauge the traffic and popularity trends which helps doing the market research.

There are two categories of web analytics; *off-site* and *on-site* web analytics. Off-site web analytics refers to web measurement and analysis regardless of whether you own or maintain a website. It includes the measurement of a website's *potential* audience (opportunity), share of voice (visibility), and buzz (comments) that is happening on the Internet as a whole. On-site web analytics measure a visitor's journey once *on your website*. This includes its drivers and conversions; for example, which landing pages encourage people to make a purchase. On-site web analytics measures the performance of your website in a commercial context. This data is typically compared against key performance indicators for performance, and used to improve a web site or marketing campaign's audience response. Historically, web analytics has referred to on-site visitor measurement. However in recent years this has blurred, mainly because vendors are producing tools that span both categories.

Many different vendors provide on-site web analytics software and services. There are two main technological approaches to collecting the data. The first method, *log-file analysis*, reads the log-files in which the web server records all its transactions. The second method, *page tagging*, uses JavaScript on each page to notify a third-party server when a page is rendered by a web browser. Both collect data that can be processed to produce web traffic reports.

In addition other data sources may also be added to augment the data. For example; e-mail response rates, direct mail campaign data, sales and lead information, user performance data such as click heat mapping, or other custom metrics as needed.

Web server log-file analysis

Web servers record some of their transactions in a log-file. It was soon realized that these log-files could be read by a program to provide data on the popularity of the website. Thus arose web log analysis software. In the early 1990s, web site statistics consisted primarily of counting the number of client requests (or *hits*) made to the web server. This was a reasonable method initially, since each web site often consisted of a single HTML file. However, with the introduction of images in HTML, and web sites that spanned multiple HTML files, this count became less useful. The first true commercial Log Analyzer was released by IPRO in 1994.

Two units of measure were introduced in the mid 1990s to gauge more accurately the amount of human activity on web servers. These were *page views* and *visits* (or *sessions*). A *page view* was defined as a request made to the web server for a page, as opposed to a graphic, while a *visit* was defined as a sequence of requests from a uniquely identified client that expired after a certain amount of inactivity, usually 30 minutes. The page views and visits are still commonly displayed metrics, but are

now considered rather rudimentary. The emergence of search engine spiders and robots in the late 1990s, along with web proxies and dynamically assigned IP addresses for large companies and ISPs, made it more difficult to identify unique human visitors to a website. Log analyzers responded by tracking visits by cookies, and by ignoring requests from known spiders.

The extensive use of web caches also presented a problem for log-file analysis. If a person revisits a page, the second request will often be retrieved from the browser's cache, and so no request will be received by the web server. This means that the person's path through the site is lost. Caching can be defeated by configuring the web server, but this can result in degraded performance for the visitor to the website.

Page tagging

Concerns about the accuracy of log-file analysis in the presence of caching, and the desire to be able to perform web analytics as an outsourced service, led to the second data collection method, page tagging or 'Web bugs'. In the mid 1990s, Web counters were commonly seen — these were images included in a web page that showed the number of times the image had been requested, which was an estimate of the number of visits to that page. In the late 1990s this concept evolved to include a small invisible image instead of a visible one, and, by using JavaScript, to pass along with the image request certain information about the page and the visitor. This information can then be processed remotely by a web analytics company, and extensive statistics generated.

The web analytics service also manages the process of assigning a cookie to the user, which can uniquely identify them during their visit and in subsequent visits. Cookie acceptance rates vary significantly between web sites and may affect the quality of data collected and reported. Collecting web site data using a third-party data collection server (or even an in-house data collection server) requires an additional DNS look-up by the user's computer to determine the IP address of the collection server. On occasion, delays in completing successful or failed DNS look-ups may result in data not being collected.

With the increasing popularity of Ajax-based solutions, an alternative to the use of an invisible image, is to implement a call back to the server from the rendered page. In this case, when the page is rendered on the web browser, a piece of Ajax code would call back to the server and pass information about the client that can then be aggregated by a web analytics company. This is in some ways flawed by browser restrictions on the servers which can be contacted with XmlHttpRequest objects.

Log-file analysis Vs page tagging

Both log-file analysis programs and page tagging solutions are readily available to companies that wish to perform web analytics. In some cases, the same web analytics company will offer both approaches. The question then arises of which method a company should choose. There are advantages and disadvantages to each approach.

Advantages of log-file analysis

The main advantages of log-file analysis over page tagging are as follows:

- The web server normally already produces log-files, so the raw data is already available. To collect data via page tagging requires changes to the website.
- The data is on the company's own servers, and is in a standard, rather than a proprietary, format. This makes it easy for a company to switch programs later, use several different programs, and analyze historical data with a new program. Page tagging solutions involve vendor lock-in.
- Log-files contain information on visits from search engine spiders. Although these should not be reported as part of the human activity, it is useful information for search engine optimization.

- Log-files require no additional DNS Lookups. Thus there are no external server calls which can slow page load speeds, or result in uncounted page views.
- The web server reliably records every transaction it makes. Page tagging may not be able to record all transactions. Reasons include:
    - Page tagging relies on the visitors' browsers co-operating, which a certain proportion may not do (for example, if JavaScript is disabled, or a hosts file prohibits requests to certain servers).
    - Tags may be omitted from pages either by oversight or between bouts of additional page tagging.
    - It may not be possible to include tags in all pages. Examples include static content such as PDFs or application-generated dynamic pages where re-engineering the application to include tags is not an option.

Log files - Data inaccuracies and limitations

- *Caching Servers, Browser Caching, and Proxies Servers*: Proxy servers used by most major companies and major ISPs (e.g. AOL), can create barriers for collecting data. For companies that rely on server-based measurements, proxy servers may prevent complete data from reaching the web server to be logged. For instance, if 3,000 people in a proxy group viewed a web page, the web server would only log it as one request because the proxy server requests the web page only once, and then distributes the web page to the 3,000 users in the proxy group. The result is an incomplete picture of visitor behavior.
- Similar issues may be caused by the use of browser navigation. When a visitor hits the "Back" or "Forward" button on their web browser, the web browser will use a locally cached copy of the web page that it saved from the last time the web page was visited. This results in a significant blind spot in the analytics, potentially masking site navigation and design issues that may be preventing visitors from accomplishing their goals on the site.
- *Robots and Spiders*: Even though web server log analysis based systems sometimes go to extraordinary measures to filter out machine-generated traffic, the ever-changing landscape of machine-generated traffic requires an enormous on-going investment to keep filters current and up to date. Machine generated traffic places the same load on web servers as human generated traffic and makes it difficult to understand what actual visitors are really doing, and therefore, whether marketing initiatives are truly being effective

Advantages of page tagging

The main advantages of page tagging over log-file analysis are as follows.

- Counting is activated by opening the page, not requesting it from the server. If a page is cached, it will not be counted by the server. Cached pages can account for up to one-third of all page views. Not counting cached pages seriously skews many site metrics. It is for this reason server-based log analysis is not considered suitable for analysis of human activity on websites.
- Data is gathered via a component ("tag") in the page, usually written in JavaScript, though Java can be used, and increasingly Flash is used.
- It is easier to add additional information to the tag, which can then be collected by the remote server. For example, information about the visitors' screen sizes, or the price of the goods they purchased, can be added in this way. With log-file analysis, information not normally collected by the web server can only be recorded by modifying the URL.
- Page tagging can report on events which do not involve a request to the web server, such as interactions within Flash movies, partial form completion, mouse events such as onClick, onMouseOver, onFocus, onBlur etc.
- The page tagging service manages the process of assigning cookies to visitors; with log-file analysis, the server has to be configured to do this.
- Page tagging is available to companies who do not have access to their own web servers.
- Lately page tagging has become a standard in web analytics.

Page Tags – Limitations

- *Implementation Effort***:** All pages that are to be tracked need to have the tag placed on each individual page, which may take a great deal of time and effort. Tags may also be embedded within a corporate template or via "server side includes."
- *Error Codes***:** Most sites would require additional configuration to allow for a tag based solution to collect error codes.
- *File Download Information***:** Most tag based solutions only allow for the tracking of the start of the download so it is unknown whether or not the download was completed successfully.
- *JavaScript Disabled on Browser***:** In the event that a user has JavaScript turned off on their browsers (currently estimated to be 2-3%), the potential exists to overlook the traffic from that segment of the population. However, the best of the client-side tracking technologies rely on JavaScript only for their ability to track unique users and set cookies and will still record requests for web resources even when JavaScript is turned off, meaning the data collection for this segment of users remains as accurate as web server log analysis solutions.

Network Data Collection

In addition to server log files and page tags, web analytics data can be collected through a methodology referred to as "network data collection". Network data collection can take on many forms and possible configurations. However, in almost all cases, web analytics data is collected from some sort of packet sniffer that resides on either the web servers themselves or sits on an independent piece of hardware (hub, switch, proxy server etc.) which is either in front of the web servers or has access to the requests being made to the web servers.

Network Data Collection - Advantages

In addition to the advantages that log files offer, network data collection has some strong advantages that should be seriously considered when formulating your data collection strategy.

- *Network Level Data*: Network data collection provides access to a more granular level of technical data that can be used to determine server response times to requests and identify network related issues that could be interfering with user experience.
- *Data Consolidation*: Often, network data collection simplifies the process of consolidating and combining data from many servers which is common to log files.
- *Additional Application Data***:** Some network data collectors are capable of collection application server variables and other additional fields of data that are not captured in log files and would be difficult or impossible to capture with page tags.
- *First Time Visit Cookie Setting***:** Some network data collectors are capable of setting a visitor identification cookie which is a superior method of setting this cookie as the first request the web server sees from a new visitor will not have the appropriate visitor identification cookie on it.
- *Search Engine Spider Reporting***:** Knowing the usage patterns of spiders can be valuable when engaging in search engine optimization. This data can be utilized to optimize the technology and content of the site for those spiders
- *Complete download data*: Log files make it possible to calculate the amount of downloads for files that are successfully completed vs. downloads that were not fully completed.
- *Server Error Code Reporting*: Error code data is automatically recorded in most log files and can provide valuable information into site functionality and design issues that would be difficult to detect through other means.

Network Data Collection - Limitations

Network data collection suffers from many of the same limitations as log files, and therefore, the best practice for implementing would normally involve the use of some amount of page tagging to capture data that would otherwise be missed by network data collection.

- *Server Load / Network Latency:* Network data collectors that are installed directly on web servers have to be carefully designed to minimize the amount of load that is introduced onto the servers. Additionally, when network data collectors are deployed on a hardware device, it is important to minimize any network latency that is introduced.
- *Data Loss Due to Overload:* Some network data collectors when overloaded with more than the maximum number of requests that the collector can handle will not be able to capture data during these periods and will result in data loss.
- *Additional Dependencies on IT Department to Implement:* Due to the insertion of an additional component either into the network or on the web servers, it is often the case where the IT department will require additional resources to test, install, and maintain network data collectors.

- **Publishing Systems**

For many businesses, publishing is a standard practice, which commonly overlaps with communication and marketing operations. The goal of publishing is to disseminate information to an audience in order to increase awareness of products, services, company operations, opportunities, etc.

Internet Publishing

Publishing is traditionally a print media operation, but today the Internet presents new possibilities for publishing with expanded capabilities. Unlike print media, it offers enhanced functionality such as powerful searching capabilities, sophisticated adaptable user interfaces, and the capability to create multimedia documents. The Internet extends the power of electronic media even further. As a global distribution channel, the Internet is a useful publishing tool to reach target audiences quickly, accurately and inexpensively.

Since there are many technologies to consider, the challenge is to determine which are best to reach the target audience. If the goal is to broadcast information in order to reach as many people as possible, the best strategy is to publish the information concurrently through multiple Internet technologies. This type of redundant publishing addresses the diversity of an audience's technological capabilities to ensure there is an appropriate channel for each member of the audience. In contrast, if the goal is to narrowcast, to disseminate information to a specific group of people, other technologies may have inherent advantages. Publishing on the Internet basically consists of making computer files available on one computer, usually called a server, and allowing others to view or download them via other computers, usually called clients.

The following technologies can be used for publishing on the Internet:

- Email Communication
- Mailings Lists
- Website Development Process
- Content Management Systems
- Public Discussion Technologies
- Internet Fax Services
- Telephony
- Video and Audio Streaming
- Advantages
- Limitations
- Online Catalogues
- Legacy Documents
- Integrated Publishing Systems

Advantages-

- Large-scale print publishing and distribution is expensive with non-diminishing printing and distribution costs (i.e., each page printed has an additional cost). The major expenses for Internet publishing are the time and effort plus the hardware and software required to create the information. Once a document is prepared electronically there are no additional costs for transmission based on volume (beyond possible increased bandwidth usage fees). This can put small

and medium-sized businesses on par with larger companies for large-scale publishing initiatives.

- A major advantage that email has over traditional print media is the ability to track and generate statistics on how many received the email, how many opened it and how many used it to access further information (click-through).
- Internet publishing offers the possibility of continually presenting updated information while print media requires physically reprinting the entire document. A website can be updated as new information becomes available and these updates can be further narrowcast to interested people through the use of multiple channels. This is especially useful for clients or employees who require information about a company, its products or policies. Internet publishing is also faster than print publishing as the printing, delivery and distribution stages are eliminated.
- Information published on the Internet can be integrated into other operations to create streamlined, continuous business processes. For example, a catalogue published on a website can be integrated with ordering forms and electronic payment systems to assist customers as they move from product awareness through to product purchase. Different audiences can receive different information packages or determine the form of publications they wish *to see.*

Limitations-

- Internet publishing does have some limitations. Bandwidth (the amount of data that can be transmitted in a fixed amount of time) is not infinitely available; therefore the size of published information, such as multimedia files, is an issue. By the nature of the technology, file sizes must be minimized to ensure efficient transmission. This is not much of a problem for transmitting text-based information, but it is for complex formats such as audio and video.
- Differences in hardware and Internet access speeds further complicate the design and delivery of documents. To overcome these problems the common practice is to design documents for the average user who is not expected to have the fastest computer and Internet connection. Some businesses partially circumvent this problem by publishing separate versions of a document for low and high bandwidth capabilities. Those who publish multi-lingual versions of documents may be publishing four or more versions. This practice may successfully serve different audiences but it increases the amount of work and cost required to publish and maintain the information.
- Web browser plug-ins presents another limitation. These helper programs enable the browser to display files that are not default format types. The goal of Internet publishing is to reach the audience and deliver documents that they are capable of viewing. Not everyone has all the plug-ins or ability (or desire) to download them as required. In practice this limits the types of file formats and complexity of documents that can be published.

Integrated Publishing Systems

One of the advantages of Internet publishing is that information can be published through multiple technologies to reach different audiences, at different times, for different purposes. Successful Internet publishing operations will use combinations of technologies. They will use push technology such as mailing lists and Internet fax and pull technology such as newsgroups and Internet telephony to effectively draw subscribers back to other published information. For example, a concise mailing list email message can inform subscribers about a new product and direct traffic back to the website for fuller product description and pricing.

Internet publishing systems are usually developed as required as each business will have different content, audiences and technical capabilities. Integrating components improves the odds of reaching the target audience as it allows information to be recycled, repackaged and distributed to different audiences for unique purposes.

Desktop publishing

It combines a personal computer and WYSIWYG (*What You See Is What You Get*) page layout software to create publication documents on a computer for either large scale publishing or small scale local multifunction peripheral output and

distribution. The term "desktop publishing" is commonly used to describe page layout skills. However, the skills and software are not limited to paper and book publishing. The same skills and software are often used to create graphics for point of sale displays, promotional items, trade show exhibits, retail package designs and outdoor signs.

There are two types of pages in desktop publishing, electronic pages and virtual paper pages to be printed on physical paper pages. All computerized documents are technically electronic, which are limited in size only by computer memory or computer data storage space. A web page is an example of an electronic page that is not constrained by virtual paper parameters. Most electronic pages may be dynamically re-sized, causing either the content to scale in size with the page or causing the content to re-flow. There is some overlap between desktop publishing and what is known as Hypermedia publishing (i.e. Web design, Kiosk, CD-ROM). Many graphical HTML editors such as Microsoft FrontPage and Adobe Dreamweaver use a layout engine similar to a DTP program. However, some Web designers still prefer to write HTML without the assistance of a WYSIWYG editor, for greater control and because these editors often result in code bloat.

List of desktop publishing softwares

- Adobe FrameMaker
- Adobe InDesign
- Adobe PageMaker
- CorelDRAW
- Corel Ventura
- iStudio Publisher
- Microsoft Office Publisher
- OpenOffice.org
- PageStream (used to be "Publishing Partner")
- QuarkXPress
- Ready,Set,Go
- Scribus
- Serif PagePlus

1.3 Check your Progress

1. Fill in the blanks

a. HTML, which stands for ……..

b. ……..is the measurement, collection, analysis and reporting of internet data.

c. The term …….. is commonly used to describe page layout skills.

2. Match the following

Column A		Column B
a.	HTML	1. Logical extension for hypertext
b.	Semantic HTML	2. Accuracy of log-file analysis
c.	Hypermedia	3. Markup language
d.	Page Tagging	4. Making computer files available on server
e.	Internet Publishing	5. Encoded information over presentation

1.4 INRERNET TOOLS RELEVANT TO COMMERCE

This section describes other internet tools that are available beside WWW.

Archie

It is a tool for indexing FTP archives, allowing people to find specific files. It is considered to be the first Internet search engine. The original implementation was written in 1990 by Alan Emtage, Bill Heelan, and J. Peter Deutsch, then students at McGill University in Montreal.

The earliest versions of archie simply contacted a list of FTP archives on a regular basis (contacting each roughly once a month, so as not to waste too much resource of the remote servers) and requested a listing. These listings were stored in local files to be searched using the UNIX grep command. Later, more efficient front-

and back-ends were developed, and the system spread from a local tool, to a network-wide resource, and a popular service available from multiple sites around the Internet. The collected data would be exchanged between the neighboring Archie servers. The servers could be accessed in multiple ways: using a local client (such as *archie* or *xarchie*); telneting to a server directly; sending queries by electronic mail; and later via a World Wide Web interface. The name derived from famous Archie comics.

File Transfer Protocol (**FTP**)

It is a standard network protocol used to copy a file from one host to another over a TCP/IP-based network, such as the Internet. FTP is built on client-server architecture and utilizes separate control and data connections between the client and server. FTP users may authenticate themselves using a clear-text sign-in protocol but can connect anonymously if the server is configured to allow it.

A host that provides an FTP service may additionally provide anonymous FTP access. Users typically log into the service with an 'anonymous' account when prompted for user name. Although users are commonly asked to send their email address in lieu of a password, no verification is actually performed on the supplied data; Where FTP access is restricted, a remote FTP (or FTPmail) service can be used to circumvent the problem.

A client makes a TCP connection to the server's port 21. This connection, called the *control connection*, remains open for the duration of the session, with a second connection, called the *data connection*, opened by the server **from** its port 20 to a client port (specified in the negotiation dialog) as required to transfer file data. The control connection is used for session administration (i.e., commands, identification, passwords) exchanged between the client and server using a telnet-like protocol. For example "RETR *filename*" would transfer the specified file from the server to the client. Due to this two-port structure, FTP is considered an *out-of-band*, as opposed to an *in-band* protocol such as HTTP.

The server responds on the control connection with three digit status codes in ASCII with an optional text message, for example "200" (or "200 OK.") means that the last command was successful. The numbers represent the code number and the optional text represent explanations (i.e., <OK>) or needed parameters (i.e., <Need account for storing file>). A file transfer in progress over the data connection can be aborted using an interrupt message sent over the control connection.

Gopher

The Gopher protocol is a TCP/IP Application layer protocol designed for distributing, searching, and retrieving documents over the Internet. Strongly oriented towards a menu-document design, the Gopher protocol was a predecessor of (and later, an alternative to) the World Wide Web. The protocol offers some features not natively supported by the Web and imposes a much stronger hierarchy on information stored on it. Its text menu interface is well-suited to computing environments that rely heavily on remote text-oriented computer terminals, which were still common at the time of its creation in 1991, and the simplicity of its protocol facilitated a wide variety of client implementations.

As part of its design goals, Gopher functions and appears much like a mountable read-only global network file system (and software, such as gopherfs, is available that can actually mount a Gopher server as a FUSE resource). At a minimum, whatever a person can do with data files on a CD-ROM, they can do on Gopher. A Gopher system consists of a series of hierarchical hyperlink-able menus. The choice of menu items and titles is controlled by the administrator of the server.

Similar to a file on a Web server, a file on a Gopher server can be linked to as a menu item from any other Gopher server. Many servers take advantage of this inter-server linking to provide a directory of other servers that the user can access.

Telnet

It is a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communications facility using a virtual terminal

connection. User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP). Telnet was developed in 1969 beginning with RFC 15, extended in RFC 854, and standardized as Internet Engineering Task Force (IETF) Internet Standard STD 8, one of the first Internet standards.

It is a terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers.

Veronica

This is a search engine system for the Gopher protocol, developed in 1992 by Steven Foster and Fred Barrie at the University of Nevada, Reno.

Veronica is a constantly updated database of the names of almost every menu item on thousands of Gopher servers. The Veronica database can be searched from most major Gopher menus. The name, although officially an acronym for "Very Easy Rodent-Oriented Net-wide Index to Computer Archives", was chosen to match that of the FTP search service known as Archie — Veronica Lodge being the name of another character from the Archie Comics.

Wide Area Information Servers (WAIS)

It is developed by Thinking Machines Inc. in 1988, is an indexing, searching, and retrieval tool that indexes a complete file instead of just the document title and allows users to search thousands of documents quickly and easily.

The WAIS client translates user queries into the WAIS protocol, and can query the WAIS directory of servers for relevant servers. The request is then transmitted to an appropriate set of servers. WAIS servers keep complete inverted indices on the contents of documents they store and execute full-text searches on them. In response to a query, a WAIS server returns a list of relevant object descriptors. These descriptors correspond to documents that contain words and phrases specified in the user query. The WAIS client displays the results of the query to the user and retrieves the selected documents from the corresponding servers.

Usenet

Usenet is a world-wide distributed discussion system. It consists of a set of "newsgroups" with names that are classified hierarchically by subject. "Articles" or "messages" are "posted" to these newsgroups by people on computers with the appropriate software -- these articles are then broadcast to other interconnected computer systems via a wide variety of networks. Some newsgroups are "moderated"; in these newsgroups, the articles are first sent to a moderator for approval before appearing in the newsgroup. Usenet is available on a wide variety of computer systems and networks, but the bulk of modern Usenet traffic is transported over either the Internet or UUCP (Unix-to-Unix copy).

In short, Usenet is a set of protocols for generating, storing and retrieving news "articles" (which resemble Internet mail messages) and for exchanging them among a readership which is potentially widely distributed.

Other internet applications

- **Internet Relay Chat** (**IRC**)

It is a form of real-time Internet text messaging (chat) or synchronous conferencing. It is mainly designed for group communication in discussion forums,

called *channels*, but also allows one-to-one communication via private message as well as chat and data transfers via Direct Client-to-Client.

IRC is an open protocol that uses TCP and optionally TLS. An IRC server can connect to other IRC servers to expand the IRC network. Users access IRC networks by connecting a client to a server. There are many client implementations such as mIRC or XChat and server implementations, e.g. the original IRCd. Most IRC servers do not require users to register an account but a user will have to set a nickname before being connected.

- **Internet Voice Chat (Voice over the internet)**

The first version of the Internet Voice Chat (IVC) shareware program became available in 1994. A direct link supporting compressed voice can be established between two computers connected to the internet using SLIP or PPP and running the IVC software. Users must know the IP address of the person they wish to call. Although this permits two-way voice communications through the internet at rates lower than standard long-distance rates, IVC has been more of a novelty than a useful application; this is because the internet is currently based on store-and-forward technology and so the quality is spotty at best.

1.5 INTERNET APPLICATIONS FOR COMMERCE

In the late 1990s (as well as today) many businesses were interested in investing in the Internet to expand their market. The Internet has the ability to reach out to consumers globally as well as providing more convenient shopping to the consumer. If planned and executed correctly, the Internet can greatly improve sales. However, there were many businesses in the early 2000s that did not plan correctly and that cost them their business. When user requests for any information, the system searches against information in a database and return the result as temporary, system-generated web pages for the end user to view.

As an incentive to use the internet order entry program, a company can provide documents and information for the customer using the same technology. Once a customer or subscriber inputs an order or subscribes through the company's web page order form, the customer can automatically be given access to another of the company's web pages, allowing the user to look up status information, search for documents and information, and download programs and files. With customization, the company's web site can limit customers to different levels of services and hide information from them based on their granted security. In order to respond to requests and searches, the web server of the organizations needs online access to a database of information. This database would best be located on the web server or on a computer connected on network to the web server.

Early web commerce revenue has been made in four areas: direct selling or marketing of a company's existing products and services, selling advertising space, charging fees for the actual content accessible on a website, and charging fees for online transaction or links.

- **Direct selling**

A gamut of companies has begun selling their products directly on the web. The web's reach can transform a small company into a global distributor. Large corporations that already have their distribution networks in place often find the web to be a niche channel and many still think it is too early to be profitable. Some believe the reason is that "Internet selling is too new", others believe that people are not certain, and changing behavior takes some time. Smaller companies and so-called cyberpreneurs are moving faster and getting more substantive results. For industries overrun by corporate chains, the web may help smaller companies level the playing field. An information-rich website can help specialist retailers provide the same services as a fancy store in big city.

While the "no location" aspect of web-based commerce can be advantageous, companies are also finding out that customers have a hard time discovering a

particular site among the hundreds of thousands out there. As a result, more web merchants are paying a sale commission as well as an advertising fee in exchange for prominent placement on high-traffic web sites, such as search engines and home pages of online service providers. For example, Amazon.com and 1-800-Flowers have entered into long-term exclusive agreements with America online to gain access to the service's 8.5 million customers. These two 1997 agreements were valued at $44 million in revenue.

In addition to the direct selling of advertising space for banners, banners have other uses on the Web. Yahoo and other search engines have been successful in selling "targeted banner-space". In this case, rather than simply buying display space for your banner on the Yahoo search page, you buy the right to have your banner displayed based on what the reader is looking for. For example, Ford might buy the right to have its banner displayed when a reader is searching for information on trucks. These programs have been very popular with advertisers.

- **SELLING ADVERTISING SPACE**

Selling banner advertising space is a great way to use your site's traffic to generate revenue, but it can be a bit tricky. The easiest option is to join a banner ad network, which will recruit advertisers, keep track of your earnings, and control banner ad placement on your site. In exchange for these services, the network will take a hefty percentage of the advertising money generated by your ad space.

Because there are more sites that want to sell advertising space than there are sites that want to buy advertisements, banner networks tend to be somewhat choosy about the publishers they recruit. Most banner networks set a minimum monthly traffic amount, which is often fairly high. A lot of the bigger banner networks require publishers to have upwards of 250,000 visitors a month to join a CPM program. Many banner networks do cater to a range of sites, setting up different **tiers** to divide publisher sites based on monthly traffic. This is a good service for advertisers because it lets them choose the range of sites that best fits their budget and marketing campaign. Additionally, most banner networks put certain restrictions on publisher site content. They may exclude sites featuring adult content or socially offensive material, and they may also exclude publishers that already feature too many advertisements.

If your site gets a good deal of traffic, more than 100,000 impressions per month, then you should be able to join a good banner network's CPM program. If you have a smaller site, you should look into banner network click-through programs, which tend to have lower minimum traffic requirements. You probably won't make much money in a click-through program, however, because you are only paid when visitors actually click on the banner, which is very seldom (typically, less than 1 percent of the people who see a banner will click on it).

Once you've joined as a publisher, banner networks operate very similarly to banner exchange programs. You put a piece of HTML code in the ad space on your site and the banner network takes care of the rest. They place banner ads they feel fit your site and track the relevant impressions or click-troughs so you will be paid correctly. As with exchange programs, you will probably end up with unsuitable banner ads on your site from time to time and you won't get a whole lot of control over the process.

Today, online publications and Internet companies have space for display ads built into their Web sites. Typically, that space gets filled with ads either the old-fashioned way -- through a salesperson -- or by a mix of computers and people called an ad network that automatically sells ads for the spot. But a significant portion of the available ad space called "inventory" remains unsold, or is sold for next to nothing. Enter the exchanges, which use automated systems to match buyers with sellers of unsold space. With ad exchanges, member advertisers specify the price they're willing to pay for a certain type of ad spot, such as a banner ad that will be viewed by a female in Boston. When a woman in Boston pulls up a Web page of an exchange member with banner slot available, software assesses the exchange's offer. If the price offered is better than the site's minimum rate for that page and higher than what it can get from other sources, such as ads sold by its sales staff, the site will usually accept the exchange-brokered offer. The exchange's computers can then deliver the winning ad to be displayed as the Web page loads on the consumer's PC. The exchange

immediately notifies the site if it doesn't have a buyer for the ad space, and the site can then put in a nonpaying house ad or try other means to unload it on the fly.

Web sites rely on data such as IP addresses -- identifiers for PCs connected to the Web -- to know the general location, gender and other characteristics of the Web surfer pulling up an advertisement. Sites also use cookies, small files stored on users' computers, to track their Web activity, such as recent searches. Web publishers say the cookies generally don't allow them or advertisers to know the actual identity of specific users -- and any data are made anonymous. But for a car maker who might want ads to be shown only to consumers who had previously visited auto sites or had done car-related Web searches, for example, the targeting such technology makes possible can be attractive. By bringing together a lot of ad sellers, exchanges can potentially help advertisers buy a larger quantity of such specifically targeted ads across different Web sites.

Selling Space Yourself

If you want to sell ad space, your task is to convince potential advertisers that placing a banner ad on your site is a good investment. You do this with traffic numbers, information about your visitors (called demographic data) and with specific content that relates to their product or service. Since you won't be using a network or exchange program, you'll also have to set up technology to track visitor traffic, so you can bill your advertisers correctly. Approaching advertisers, marketing your site, tracking traffic and collecting money from advertisers all require a lot of time and effort, but if you are committed to growing your Web site and only running banner ads that would appeal to your visitors, the payoff can certainly be worth the effort.

- **Pricing for content and services**

At present, no any standard structure available for pricing the web content or services. Even though it is very important to price your advertising formats correctly, it should all come down to one major factor - what are you offering of value and what will advertisers be prepared to pay? Of course, you know the marketplace you are in, but do you really know how much value advertisers are attaching to your product? If you don't know, ask! - it really is so important to remind yourselves that 'value' is what it all comes down to. If you offer value, then you can at least charge something for the advertising space!

So, what type of product do you offer and more importantly, what kind of customers will buy from you? If you run a website, which attracts 20,000 consumer visitors per month and your site is all about mobile phones, and then you'll probably be restricted in the overall scale of advertising fees. Why? Well, there are a lot of mobile phone websites out there, which are doing a similar job and may attract around the same amount of visitors within the same age group, demographics and buying habits. In this case, you'll probably charge the going rate and hope your revenue increases, as your visitor numbers and popularity do.

Now, let's have a look at the other end of the scale. You own a website with thousands of pages, which attracts over 300,000 of the world’s richest people. It is a very high quality product and you have a vast number of customers who pay a large annual fee to access exclusive luxury offers from big spending advertisers.

Make no mistake; buyers understand the prices behind marketing content. We're the ones who don't pay enough attention to it. Here are the components of the price from the buyer's perspective:

- **Time.** They have to spend time filling out the form and predict the amount of time they will need to absorb the content and probably deal with the emails and calls from pesky salespeople after the fact.
- **Privacy.** Buyers understand that they give away a piece of their privacy every time they fill out a form and engage with content.
- **Intention.** Buyers want the most valuable content they can get. They decide how to reveal about their intentions based on the value of the content to them.

They may also assume that a higher level of intent will net them more valuable content either in terms of quantity or depth.

- **Hierarchy.** Buyers are all-too aware of their positions in the chain of command. Those lower down on the corporate ladder are more willing to "spend" their information because they realize that it has less value than those higher up, whose buying power gives them more information riches combined with less willingness to spend it (kind of like rich people in the real economy).
- **Access.** Buyers understand that there are different levels of access to content depending on certain factors. They don't always know what those factors are, but they value access enough to lie. For example, many assume that a higher level of buying intent will get them more goodies, so they say they are ready to buy when they aren't. Many also assume that if they say that they are vice president instead of a director that they will receive better content and probably better treatment overall.
- **Relationship.** This price is one that high-level executives have been calculating for years as providers woo them with memberships in customer councils and invitations to private events. But it's less familiar to lower-level buyers, who are only beginning to calculate this piece as the economics of social media open up the privileges of relationship from cheesy tchotckes at trade shows to online social networks.
- **Account history.** Buyers assume that the price of content will change depending on the number of times they have engaged with you. Even the most basic lead scoring mechanism raises the price of content as buyers consume more of it i.e., If you download two white papers a week for a month, you should expect a call from a salesperson. Buyers get that or at least they will probably see the logic in the pricing.
- **Culture and location.** Culture, both corporate and social, affects the price that buyers are willing to pay for content. For example, research shows that Europeans value their privacy more than Americans meaning that their information may cost you more. And some companies have disclosure rules that make it hard for their executives to participate on customer advisory boards.

The price will change

We should evaluate our content pricing models to see if we're charging the right amounts. We should expect those prices to change as social media takes hold among buyers. For example, 99.9% of the links I click on in Twitter take me directly to the content advertised in the tweets. And when there is a gate, most Twitterers take the precious real estate needed to say that registration is necessary. Just as the web has gutted the business model of publishing it has also reduced the price of marketing content.

1.6 MINIMALIST WEBSITE ESTABLISHMENT

Creating a website, any web developer wants it to be attractive, eye-catching and exclusive, that is why one may try to fill it up with various design elements which will make a dramatic impression on the viewer. However, making your web pages visually rich doesn't always appear to be a winning solution. The same thing concerns websites with minimalist design - they cannot be viewed as ones with lack of idea or poor design. Vice versa, in order to create a good minimalist website you must have no less taste and style to establish really modern and beautiful web pages.

The solution you choose for your website construction may depend on your particular skills, likings and your experience. You may long for something complex and astounding which will amaze every visitor who opens your website pages but you can go for it only in case you can be responsible for the result. But if you don't have enough skills it is better to stick to simplicity and try your hand at creating minimalist website which will be both attractive and easy to establish. If you have never heard of constructing a website with minimalist design, following paragraphs will help you to understand the principles of minimalist design.

What is actually minimalism? Every web developer may see something particular and individual in this kind of design though the general name of minimalist

design is reduction - reduction of images, colors, structures etc. Moreover, minimalist design is known to contain less surplus elements and more meaningful ones which add to the elegance and quality of your website design. The main advantage minimalist websites are distinguished by implies the absence of noisy elements which often distract the attention or even annoy. Minimalist websites allow you to concentrate on the most important issues it concerns and delve into the very content interacting with it effectively.

You must always remember that visitors come to your website not for an impression from flashing ads, widgets and other visual elements; they actually come for the content kept within your web pages with its idea, meaning and usefulness. That is why minimalist website will come in handy in case you need to make your visitors focus on your web pages rich content. However, there are several points to take into account while establishing a website with minimalist design.

1. ***Follow your purpose.*** If you decided to stick to minimalism in your website design you need to remember that it requires implementing only necessary elements to get the most effective result. You should avoid complex techniques and heavy graphics - though they are very impressive that is not the main point of your minimalist website. Your customers will buy your items or subscribe to your services not because of interactive and amazing design but because your website will prove you are reliable and trustworthy partner.

2. ***Follow successful examples.*** Searching a bit you will see that a lot of the most winning websites which get much traffic and income are also created in minimalist style. These websites may look simple but remain among the most rated on the web because they provide their customers with comfortable and fast browsing allowing finding what the clients are looking for easily. So take into account the experience of those who have gained recognition and popularity using minimum design and maximum usability and follow such examples.

3. ***Make the navigation simple.*** Instead of implementing complex interactive menus try to make your website navigation as simple & convenient as possible. Do not forget that your aim is to establish a good minimalist website which must provide your clients with most usability. That is why making your website navigation simple and comprehensible will be the most brilliant idea every visitor can't but appreciate.

4. ***Try to use HTML and CSS.*** It is known that HTML and CSS techniques allow creating easy-to-use websites effectively. They will appear to be the most appropriate solution for your minimalist website and, moreover, do not require extra skills so you won't find it hard to use them even if you are not an experienced web developer. Moreover, avoiding simpler web development techniques will help you to avoid errors in website running and provides faster loading time which is very important for your minimalist website.

So if you are going to establish an attractive website with usable minimalist design to provide your customers with fast and easy browsing you should take into account the aspects listed above.

1.4, 1.5 & 1.6 Check your Progress

1. Match the following pair.

Column A	Column B
a. Archie	1. Constantly updated database
b. FTP	2. Indexing FTP archives
c. Gopher	3. File transfer protocol
d. Telnet	4. Search/retrieve document over the Internet
e. Veronica	5. Bidirectional text-oriented communications

2. Fill in the blanks.

a. Selling ……is a great way to use your site's traffic to generate revenue.

b. Web sites rely on data such as……

c. …….will come in handy in case you need to make your visitors focus on your web pages rich content.

1.7 SUMMARY

The web server mainly delivers documents, but it really knows nothing about the information in them. As an information delivery system, the web server works acceptably well. But, the web is an information space, in which information is published and users search for the information they need. Publishing and managing information on the web requires more than a delivery system, and web servers lack many services that are needed to make the web a reliable and useful information space.

The establishment, management, and maintenance of a website require a significant investment of time and resources on your part. But don't let these tasks overwhelm you. The best approach is to start with the basics:

- Design your site for ease of modification.
- Avoid sloppy formatting, numerous and gratuitous image maps, and superfluous links on every page.
- Know who will maintain and update your website and have more than one person that can easily step in and take control.

A website must be kept updated or its moneymaking potential is wasted. Most web operators will find that they need to rely on a blend of technologies to provide the proper website maintenance and management. Thankfully, the functions offered by website management and maintenance tools often overlap. Thus, if you look carefully before taking the leap, you may find it possible to save time and money by purchasing a single suite of tools that can handle most, if not all, of the tasks necessary for a properly managed site.

The developing business climate on the Internet is testing the limits of the current network architecture. The Net was designed for resilience, not for security. It was designed for easy information transfer, not for mass, regulated traffic. Internet culture is already going through a visible metamorphosis as commercial interest stake out their niche. It is becoming clear that traditional Internet systems like Usenet are not currently suited for the changes ahead. We have also had a taste of an advertising medium that is still in its earliest stages. The next generation of Internet users is paying directly for their use, by the hit or by the minute. For the first time, large numbers of users without a special interest in computers will seek information over the Net. The services offered will be used by people who do not necessarily understand anything about the network they are connected to. Personally, I am hoping that something better can be done on the Net, better than on television or the print media. The most valuable asset the Internet has is its sense of individualism and grass-roots input. Hopefully, the Internet will not become a space where advertisers set the moral standard. This has become the case in most other media, and could easily happen here as sites grow to depend on advertising revenue. All that can be said with true confidence is that the cultural atmosphere of the Internet will be very different in the years, and months to come.

Source : *www.gpayments.com(Link)*

1.8 CHECK YOUR PROGRESS - *ANSWERS*

1.1 & 1.2

1. a) Commercialization
b) Web
c) Point-to-point dedicated link
d) Browsers

1.3

1. a) Hypertext Markup Language
b) Web analytics
c) Desktop publishing

2.

a-3
b-5
c-1
d-2
e-4

1.4, 1.5 & 1.6

1. a-2
b-3
c-4
d-5
e-1

2. a) Banner advertising space
b) IP addresses
c) Minimalist website

1.9 QUESTIONS FOR SELF-STUDY

1. What is commercialization of internet? Explain.
2. What is web browser? What are its main components?
3. Write a short note on HTML.
4. What are different data collection technologies in web server? Explain in detail.
5. Explain in brief- different publishing techniques.
6. Write a note on internet application tools.
7. Explain - Internet applications for commerce?
8. What do you mean by minimized website establishment? How it is achieved?

1.10 SUGGESTED READINGS

Web Commerce Technology Handbook By Daniel Minoli Emma Minoli

Electronic commerce By Hossein Bidgoli

NOTES

Chapter 2

INTRODUCTION TO E-COMMERCE

2.0 OBJECTIVES

After studying this chapter you will be able to :

- discuss at the Electronic Data Interchange in depth.
- describe the concepts of e-commerce, its advantages/disadvantages & its applications.
- explain the concept of Commerce-Net advocacy.

2.1 INTRODUCTION

Commerce is, quite simply, the exchange of goods and services, usually for money. We see commerce all around us in millions of different forms. When you buy something at a grocery store you are participating in commerce. If you go to work each day for a company that produces a product, that is yet another link in the chain of commerce.

Despite the spectacular dot-com bust of a few years ago, the Internet has markedly changed the way we do business, whether it's finding new streams of revenue, acquiring new customers, or managing a business's supply chain. E-commerce is mainstream — enabling businesses to sell products and services to consumers on a global basis. As such, e-commerce is the platform upon which new methods to sell and to distribute innovative products and services electronically are tested.

The Web's influence on the world's economy is truly astonishing. The business world knows that the Web is one of the best ways for business such as manufacturers to sell their products directly to the public, brick-and-mortar retailers to expand their stores into unlimited geographical locations, and for entrepreneurs to establish a new business inexpensively.

When we think about commerce, we instinctively recognize several different roles:

- *Buyers* - these are people with money who want to purchase a good or service.
- *Sellers* - these are the people who offer goods and services to buyers. Sellers are generally recognized in two different forms: retailers who sell directly to consumers and wholesalers or distributors who sell to retailers and other businesses.

- *Producers* - these are the people who create the products and services that sellers offer to buyers. A producer is always, by necessity, a seller as well. The producer sells the products produced to wholesalers, retailers or directly to the consumer.

One way to look at e-commerce and its role in the business world is through value-chain analysis. Michael Porter introduced the value-chain concept in 1985. It consists of a series of activities designed to satisfy a business need by adding value (or cost) in each phase of the process. A typical business organization (or a division within a business organization) designs, produces, markets, delivers, and supports its product(s) or service(s). Each of these activities adds cost and value to the product or service that is eventually delivered to the customer. E-commerce, its applications, and its supporting technologies provide the business platform for realizing Porter's visions.

2.2 EDI (ELECTRONIC DATA INTERCHANGE)

- **What is EDI**

EDI means Electronic Data Interchange. It is nothing but the transfer of data between different companies using networks, such as the Internet. As more and more companies get connected to the Internet, EDI is becoming increasingly important as an easy mechanism for companies to buy, sell, and trade information. EDI refers to the electronic exchange of business information between two companies using a specific and structured format. The concept has been around since the 1970s and has traditionally been used to automate buyer-seller transactions such as invoices and purchase orders. But as more processes within a company become automated, EDI has expanded to areas such as inventory management and product distribution.

EDI occurs when one business transmits computer readable data in standard format to another business. The standard formats used in EDI contain the same information that businesses have always included in their standard paper invoices, purchase orders, and shipping documents.

EDI relies on standards, or common methods of defining classes of business data, which allow computers to recognize what data belongs to what department in a company. In the early days of EDI, many companies built in-house EDI standards, but as interest grew, industries started to agree on common standards, administered by standards organizations. These standards, which allow computers in different organizations to share information over privately built, closed networks known as value-added networks, led to the use of EDI for corporate purchasing.

- **How EDI works**

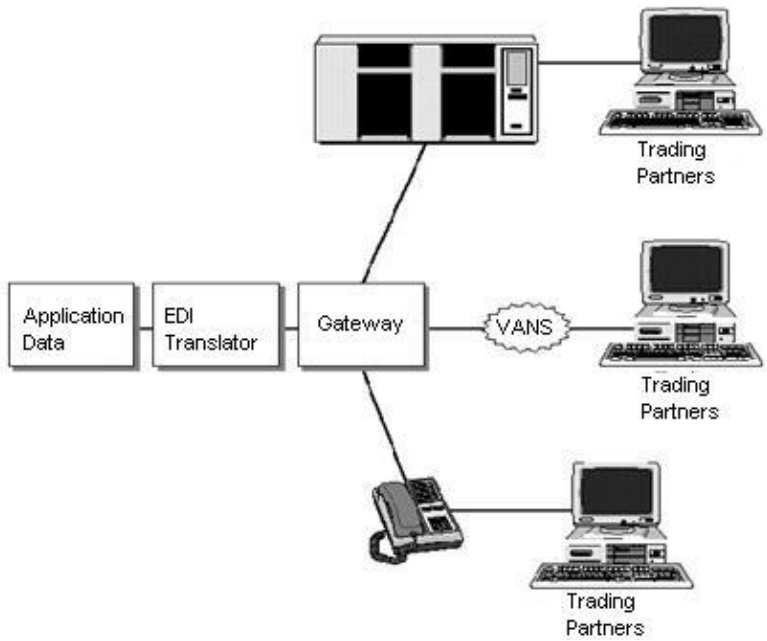


Fig 2.1 Electronic Data Interchange

From above figure it is clear that EDI is the electronic transfer of a standardized business transaction between a sender and receiver computer, over some kind of private network or value added network (VAN). The VANs use a

traditional-store-and-forward concept of handling data. Both sides would have to have the same application software and the data would be exchanged in an extremely rigorous format. In sectors such as retail, automotive, defense and heavy manufacturing, EDI was developed to integrate information across larger parts of an organization's value chain from design to maintenance so that manufacturers could share information with designers, maintenance and other partners and stakeholders. Before the widespread and commercial use of the Internet, the EDI system was very expensive to run mainly because of the high cost of the private networks. By 1996 no more than 50,000 companies in Europe and 44,000 in the USA were using EDI.

- **Advantages of EDI**

Following are some advantages of EDI:

- Accelerates the order–invoice–payment cycle from days or weeks to hours or minutes
- Decreases paperwork
- Expands the organization customer base
- Improves accuracy of information transfer
- Improves customer service
- Improves response and access to information
- Improves communications
- Improves cost efficiency
- Improves customer service
- Improves the competitiveness of an organization
- Improves the speed of transaction processing
- Improves the speed of information transfer

- **Disadvantages of EDI**

The disadvantages of EDI can be listed as follows:

1. **Concentration of control:** EDI causes management to rely more heavily on computer systems and places control in the hands of fewer individuals, potentially increasing risk.

2. **Data processing, application, and communications errors:** Errors in computer processing and communications systems may result in the transmission of incorrect trading information or the reporting of inaccurate information to management. Application errors or failures can also result in significant losses to trading partners.

3. **Potential loss of management and audit trails:** In some cases, EDI transaction data may not be maintained for a long period of time. Without proper consideration of legal and auditing issues, the entity may not be able to provide adequate or appropriate evidence, in hard copy or on magnetic media, for the legal dispute to be resolved favorably or for the audit to be completed cost effectively.
   Backup of the transactions must be made and maintained to guard against this possible problem.

4. **Reliance on third parties:** The organization will become more dependent on third parties to ensure security over transactions and continuity of processing. Also, EDI may share the same kinds of security threats associated with any electronic data communications and other e-commerce applications. A number of potential risks include the following:

- Confidential information could be exposed to unauthorized third parties or competitors.
- Third-party staff could introduce invalid and/or unauthorized transactions.
- Transactions could be lost because of disruptions of data processing at third-party network sites or en route to the recipient partner, causing business losses and inaccurate reporting.

5. **Total systems dependence:** All EDI transactions entered by an entity could be corrupted if the EDI-related application became corrupted. If the errors remained undetected, there could be an impact on cash flow, adverse publicity and loss of business confidence by customers and suppliers. Undetected errors in

transactions received from trading partners could cause losses from inappropriate operating decisions.

6. **Unauthorized transactions and fraud:** Increased access to computer systems can increase the opportunities to change an entity's computer records and those of its trading partners, enabling significant fraud to be committed. Where payment transactions are automatically generated by the system, payments can be manipulated or diverted, or they can be generated in error or at the wrong time intervals.

2.1 & 2.2 Check your Progress

1. Fill in the blanks.

a. Commerce is, quite simply, the exchange of …….. …….. usually for money.

b. EDI means ……..

c. EDI refers to the electronic exchange of business information between two companies using a …... format.

2. Answer in two / three sentences.

a. Define EDI.

……

……

b. Write some of the advantages of EDI.

……

……

2.3 WHAT IS E-COMMERCE?

- **History**

The meaning of electronic commerce has changed over the last 30 years. Originally, electronic commerce meant the facilitation of commercial transactions electronically, using technology such as Electronic Data Interchange (EDI) and Electronic Funds Transfer (EFT). These were both introduced in the late 1970s, allowing businesses to send commercial documents like purchase orders or invoices electronically. The growth and acceptance of credit cards, automated teller machines (ATM) and telephone banking in the 1980s were also forms of electronic commerce.

From the 1990s onwards, electronic commerce would additionally include enterprise resource planning systems (ERP), data mining and data warehousing. Perhaps it is introduced from the Telephone Exchange Office, or maybe not. The earliest example of many-to-many electronic commerce in physical goods was the Boston Computer Exchange, a marketplace for used computers launched in 1982. The first online information marketplace, including online consulting, was likely the American Information Exchange, another pre-Internet online system introduced in 1991.Although the Internet became popular worldwide in 1994, it took about five years to introduce security protocols and DSL allowing continual connection to the Internet.

And by the end of 2000, a lot of European and American business companies offered their services through the World Wide Web. Since then people began to associate a word "ecommerce" with the ability of purchasing various goods through the Internet using secure protocols and electronic payment services.

Supply Chain Management

Supply chain management (SCM) is changing as companies continue to look for ways to respond faster, improve service for customers, and maximize sales while decreasing costs. SCM solutions must support highly configurable products, such as computers and automobiles, global markets with local specifications, and widely dispersed suppliers and partners. Yet most companies' SCM solutions are linear, sequential, and designed for controlled conditions. They rely on accurate forecasting of demand, but are disconnected from the actual demand. Decisions are made centrally, and changes typically take days, weeks, or even months. However, companies

increasingly need to respond to changes in hours and minutes. Supply chains in this century must be adaptive and provide greater visibility, velocity, flexibility, and responsiveness to enable enterprise value networks to adapt to changes in supply and demand in real time.

- **What is E-Commerce?**

E-Commerce or Electronic Commerce is any form of business transaction in which the parties interact electronically over the Internet rather than by physical exchange. E-commerce is means of enabling and supporting the exchange of information, goods, and services between or among companies or between companies and their customers. It enables companies to be more efficient in their internal operations and more responsive to the needs and expectations of their customers. E-commerce technologies enable enterprises to exchange information instantaneously, eliminate paper-work, and advertise their products and services to the global market.

E-commerce is a subset of business, where products and services are advertised, bought and sold over the Internet. Any size business can have an e-commerce strategy. Many businesses have become extremely profitable through online sales. Dell Computers is a prime example. Small companies and even individuals can also market their products or services on a worldwide basis through E-Commerce. Large companies can reduce sales and stocking costs by selling online.

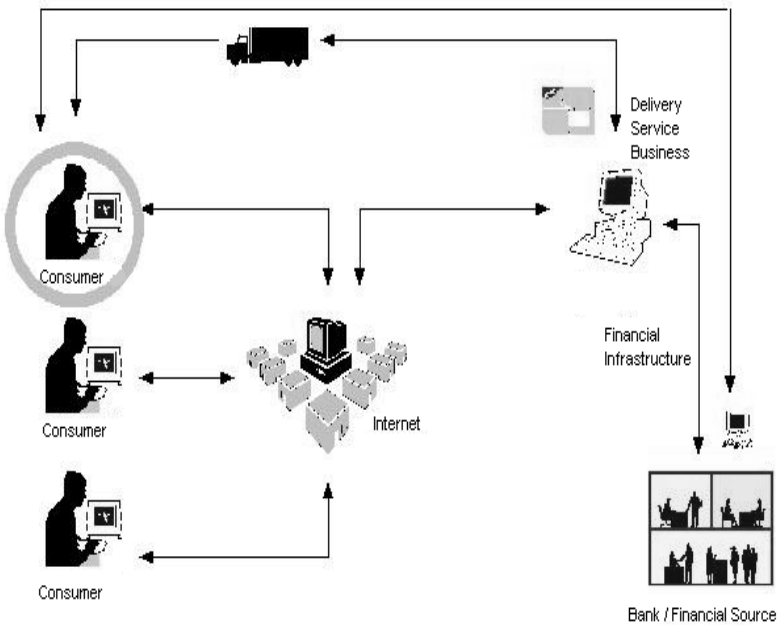


Fig 2.2 E-Commerce System

- **Why Use E-Commerce?**

Because the Internet provides a flexible and dynamic marketplace to exchange goods, services, and information with consumers and business partners , it is becoming increasingly important for businesses to use the Internet to reach new markets .The greatest business advantage of being online is the ability to market products both locally and globally. The following list offers some reasons for companies to build commerce-enabled Web sites:

- *Low Entry Cost*: A company can establish itself on the Internet, and open for business, with a relatively small investment. Thousands of companies operate simple, inexpensive sites that are successful in their markets.
- *Reduces Transaction Costs*: Dealing with customers over the Web , whether to process orders or to attend to customer support, is cheaper than traditional marketing methods. For example , Dell Computer Corporation estimates that it saves eight dollars each time a customer checks the status of an order at the Dell Web site , instead of calling the company.
- *Access to the global market*: With a traditional business , the target market may be the local community or , with a higher advertising budget , it may extend to neighboring communities.The Web extends the reach of even the smallest businesses by allowing them to market products globally.
- *Online distribution*: The Web enables businesses to distribute data and software online.
- *Secure market share*: Getting a business online protects its current offline market share from being eroded by an online entrepreneur. If a business enters the e-

commerce market too late , competitors who have already established a Web presence may make a successful market entry more difficult.

There are several basic steps you will need to accomplish before becoming E-Commerce Enabled.

- Getting a Merchant Bank Account
- Web Hosting
- Web Design Considerations
- Registering a Domain Name
- Obtaining a Digital Certificate

- **How Does E-Commerce Work?**

In its simplest form, e-commerce allows your company's product catalog to be hosted on a web server so that customers and potential customers can visit your site, see what you have to sell and then place orders. The majority of e-commerce sites that sell to general consumers ask you to pay for the items you want using a credit card, and so they present forms that can safely and securely capture this information, and perform automatic credit card authorization/ transaction without human intervention.

The e-commerce process works as follows:

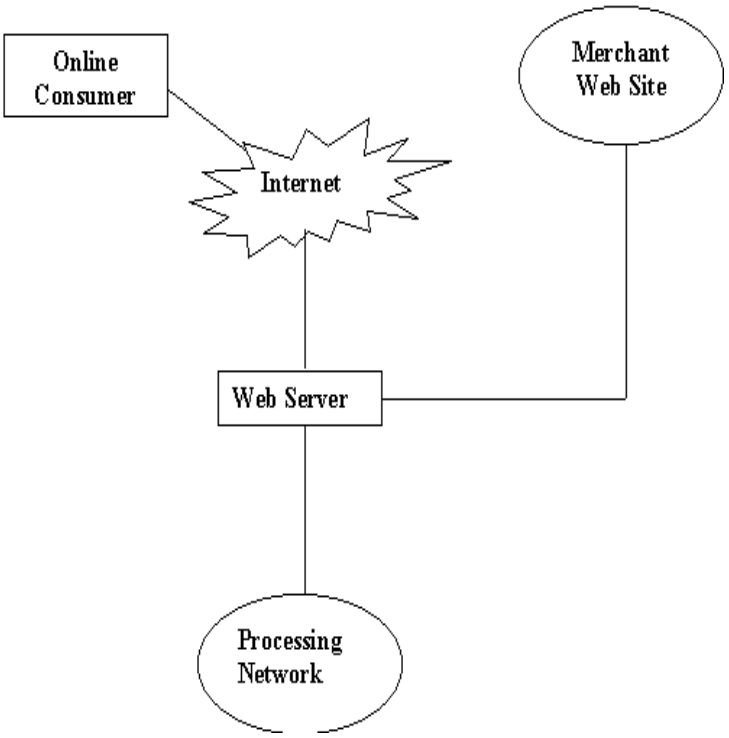


Fig 2.3 E-Commerce Process

- A consumer uses Web browser to connect to the home page of a merchant's Web site on the Internet.
- The consumer browses the catalog of products featured on the site and selects items to purchase . The selected items are placed in the electronic equivalent of a shopping cart.
- When the consumer is ready to complete the purchase of selected items , she provides a bill-to and ship-to address for purchase and delivery.
- When the merchant's Web server receives this information , it computes the total cost of the order--including tax , shipping , and handling charges--and then displays the total to the customer.
- The customer can now provide payment information , such as a credit card number , and then submit the order.
- When the credit card number is validated and the order is completed at the Commerce Server site , the merchant's site displays a receipt confirming the customer's purchase.
  - The Commerce Server site then forwards the order to a Processing Network for payment processing and fulfillment.

- **Key Drivers of E-Commerce**

It is important to identify the key drivers of e-commerce to allow a comparison between different countries. It is often claimed that e-commerce is more advanced in the USA than in Europe. These key drivers can be measured by a number of criteria that can highlight the stages of advancement of e-commerce in each of the respective countries. The criteria that can determine the level of advancement of e-commerce can be given as:

1. *Technological factors* – The degree of advancement of the telecommunications infrastructure which provides access to the new technology for business and consumers
2. *Political factors* – including the role of government in creating government legislation, initiatives and funding to support the use and development of e-commerce and information technology
3. *Social factors* – incorporating the level and advancement in IT education and training which will enable both potential buyers and the workforce to understand and use the new technology
4. *Economic factors* – including the general wealth and commercial health of the nation and the elements that contribute to it

These are mainly at the level of the firm and are influenced by the macro-environment and e-commerce, which include:

- *Organizational culture* – attitudes to research and development (R&D); its willingness to innovate and use technology to achieve objectives.
- *Commercial benefits* – in terms of cost savings and improved efficiency that impact on the financial performance of the firm.
- *Skilled and committed workforce* – that understands, is willing and able to implement new technologies and processes.
- *Requirements of customers and suppliers* – in terms of product and service demand and supply.
- *Competition* – ensuring the organization stays ahead of or at least keeps up with competitors and industry leaders.

These key drivers for the implementation of e-business can be put into the context of the classic economic equation of supply and demand illustrated in below figure.

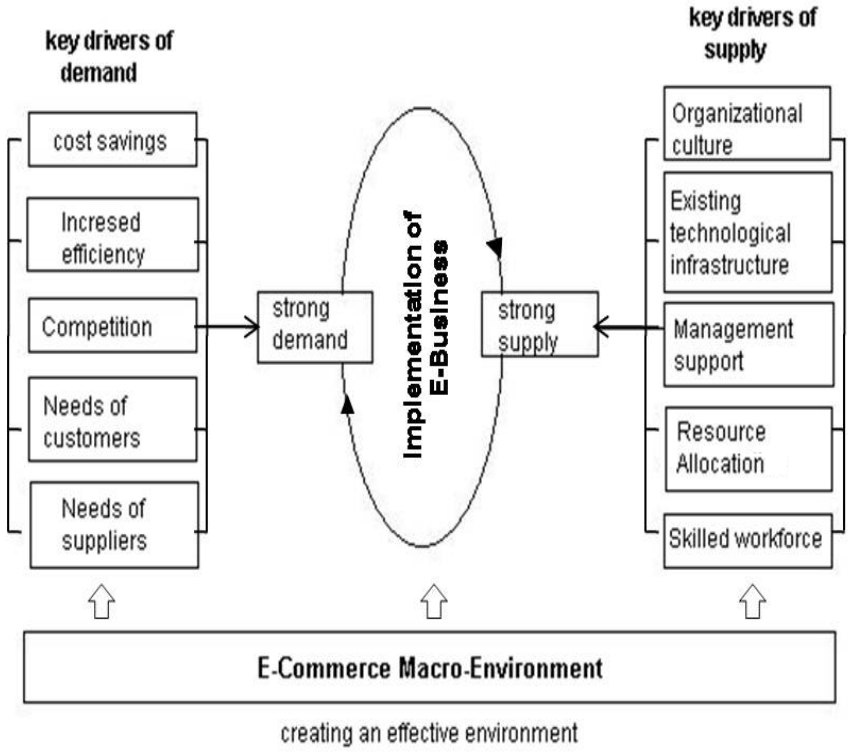


Figure 2.4 E-Commerce Drivers

Thus, e-commerce provides the infrastructure and environment that enables and facilitates e-business. Within this, the implementation of e-business is solely dependent on whether there is a demand by the organization and whether it can be supplied within the organization. Demand is created largely by the need to cut costs, improve efficiency, maintain competitive advantage and meet stakeholder requirements.

These business objectives can be met through the supply of a technological infrastructure to improve organizational processes, a willingness, ability and commitment to integrate new technology and improve working practice within the organization, and crucial to all this is the allocation of resources.

- **E-Commerce Vs. Traditional Commerce**

Although the goals and objectives of both e-commerce and traditional commerce are the same—selling products and services to generate profits—they do it quite differently. In e-commerce, the Web and telecommunications technologies play a major role. In e-commerce there may be no physical tore, and in most cases the buyer and seller do not see each other. Below table compares and contrasts traditional commerce and e-commerce.

Table 2.1 E-commerce vs. Traditional commerce

Activity	**Traditional commerce**	**E-commerce**
Product information	Magazines, flyers	Web sites Online catalogs
Business communications	Regular mail, phone	E-mail
Check product availability	Phone, fax, letter	E-mail, web sites, and extranets
Order generation	Printed forms	E-mail, web sites
Product acknowledgments	Phone, fax	E-mail, web sites, and EDI
Invoice generation	Printed forms	Web sites

However, it is important to notice that currently many companies operate with a mix of traditional and e-commerce. Just about all medium and large organizations have some kind of e-commerce presence. The Gap, Toys-R-Us, Wal-Mart Stores, and Sears are a few examples.

Components of a typical successful e-commerce transaction loop

E-commerce does not refer merely to a firm putting up a Web site for the purpose of selling goods to buyers over the Internet. For e-commerce to be a competitive alternative to traditional commercial transactions and for a firm to maximize the benefits of e-commerce, a number of technical as well as enabling issues have to be considered.

A typical e-commerce transaction loop involves the following major players and corresponding requisites:

The *Seller* should have the following components:

- Corporate Web site with e-commerce capabilities (e.g., a secure transaction server)

- A corporate intranet so that orders are processed in an efficient manner
- IT-literate employees to manage the information flows and maintain the e-commerce system

Transaction partners include:
- banking institutions that offer transaction clearing services (e.g., processing credit card payments and electronic fund transfers)
- National and international freight companies to enable the movement of physical goods within around and out of the country. For business-to-consumer transactions, the system must offer a means for cost-efficient transport of small packages (such that purchasing books over the Internet, for example, is not prohibitively more expensive than buying from a local store)
- Authentication authority that serves as a trusted third party to ensure the integrity and security of transactions

Consumers (in a business-to-consumer transaction) who:
- Form a critical mass of the population with access to the Internet and disposable income enabling widespread use of credit cards
- Possess a mindset for purchasing goods over the Internet rather than by physically inspecting items

Firms/Businesses (in a business-to-business transaction) that together form a critical mass of companies (especially within supply chains) with Internet access and the capability to place and take orders over the Internet

Government to establish:
- A legal framework governing e-commerce transactions (including electronic documents, signatures, and the like)
- Legal institutions that would enforce the legal framework (i.e., laws and regulations) and protect consumers and businesses from fraud, among others

And finally, the *Internet***,** the successful use of which depends on the following:
- A robust and reliable Internet infrastructure
- A pricing structure that doesn't penalize consumers for spending time on and buying goods over the Internet (e.g., a flat monthly charge for both ISP access and local phone calls)

For e-commerce to grow, the above components and factors have to be in place. The least developed factor is a barrier to the increased growth of e-commerce. For instance, a country with an excellent Internet infrastructure will not have high e-commerce figures if banks do not offer support and fulfillment services to e-commerce transactions. In countries that have significant e-commerce figures, a positive feedback loop reinforces each of these factors.

2.3 Check your Progress

1. Fill in the blanks.

a. Electronic Commerce is any form of business transaction in which the parties interact …….over the Internet rather than by physical exchange.

b. E-commerce provides the ……and ……. that enables and facilitates e-business.

2. Answer in Two-Three sentences.

a. Define E-Commerce.

……

……

b. What are the key drivers of E-Commerce?

……

……

2.4 BENEFITS OF E-COMMERCE

The previous sections have included discussions about what e-commerce is and its impact, but what are the benefits of e-commerce? What does it offer and why do it? The benefits of e-commerce can be seen to affect three major stakeholders: organizations, consumers and society.

❖ **Benefits of e-commerce to organizations**

- ***International Marketplace*** **:** What used to be a single physical marketplace located in a geographical area has now become a borderless marketplace including national and international markets. By becoming e-commerce enabled, businesses now have access to people all around the world. In effect all e-commerce businesses have become virtual multinational corporations.
- **Operational Cost Savings :** The cost of creating, processing, distributing, storing and retrieving paper-based information has decreased (see Intelmini-case).
- **Mass customization :** E-commerce has revolutionized the way consumers buy goods and services. The pull-type processing allows for products and services to be customized to the customer's requirements. In the past when Ford first started making motor cars, customers could have any color so long as it was black. Now customers can configure a car according to their specifications within minutes on-line via the www.ford.com website.
- *Enables reduced inventories* and overheads by facilitating 'pull'-type supply chain management – this is based on collecting the customer order and then delivering through JIT (just-in-time) manufacturing. This is particularly beneficial for companies in the high technology sector, where stocks of components held could quickly become obsolete within months. For example, companies like Motorola (mobile phones), and Dell (computers) gather customer orders for a product, transmit them electronically to the manufacturing plant where they are manufactured according to the customer's specifications (like color and features) and then sent to the customer within a few days.
- **Lower telecommunications cost :** The Internet is much cheaper than value added networks (VANs) which were based on leasing telephone lines for the sole use of the organization and its authorized partners. It is also cheaper to send a fax or e-mail via the Internet than direct dialing.
- **Digitization of products and processes :** Particularly in the case of software and music/video products which can be downloaded or e-mailed directly to customers via the Internet in digital or electronic format.
- *No more 24-hour-time constraints*. Businesses can be contacted by or contact customers or suppliers at any time.

❖ **Benefits of e-commerce to consumers**

- ***24/7 access*** **:** Enables customers to shop or conduct other transactions 24 hours a day, all year round from almost any location. For example, checking balances, making payments, obtaining travel and other information. In one case a pop star set up web cameras in every room in his house, so that he could check the status of his home by logging onto the Internet when he was away from home on tour.
- **More choices :** Customers not only have a whole range of products that they can choose from and customize, but also an international selection of suppliers.
- **Price comparisons :** Customers can 'shop' around the world and conduct comparisons either directly by visiting different sites, or by visiting a single site where prices are aggregated from a number of providers and compared (for example www.moneyextra.co.uk for financial products and services).
- **Improved delivery processes :** This can range from the immediate delivery of digitized or electronic goods such as software or audio-visual files by downloading via the Internet, to the on-line tracking of the progress of packages being delivered by mail or courier.
- *An environment of competition* where substantial discounts can be found or value added, as different retailers vie for customers. It also allows many individual customers to aggregate their orders together into a single order presented to

wholesalers or manufacturers and obtain a more competitive price (aggregate buying), for example www.letsbuyit.com.

❖ **Benefits of e-commerce to society**

- *Enables more flexible working practices*, which enhances the quality of life for a whole host of people in society, enabling them to work from home. Not only is this more convenient and provides happier and less stressful working environments, it also potentially reduces environmental pollution as fewer people have to travel to work regularly.
- *Connects people*. Enables people in developing countries and rural areas to enjoy and access products, services, information and other people which otherwise would not be so easily available to them.
- *Facilitates delivery of public services*. For example, health services available over the Internet (on-line consultation with doctors or nurses), filing taxes over the Internet through the Inland Revenue website.

2.5 THE LIMITATIONS OF E-COMMERCE

There are limitations to e-commerce. These again will be dealt with according to the three major stakeholders – organizations, consumers and society.

❖ **Limitations of e-commerce to organizations**

- Lack of sufficient system security, reliability, standards and communication protocols. There are numerous reports of websites and databases being hacked into, and security holes in software. For example, Microsoft has over the years issued many security notices and patches for their software. Several banking and other business websites, including Barclays Bank, Powergen and even the Consumers Association in the UK, have experienced breaches in security where a technical oversight or a fault in its systems led to confidential client information becoming available to all.
- Rapidly evolving and changing technology, so there is always a feeling of trying to catch up and not be left behind. Under pressure to innovate and develop business models to exploit the new opportunities which sometimes leads to strategies detrimental to the organization. The ease with which business models can be copied and emulated over the Internet increases that pressure and curtails longer-term competitive advantage.
- Facing increased competition from both national and international competitors often leads to price wars and subsequent unsustainable losses for the organization.
- Problems with compatibility of older and newer technology. There are problems where older business systems cannot communicate with web based and Internet infrastructures, leading to some organizations running almost two independent systems where data cannot be shared. This often leads to having to invest in new systems or an infrastructure, which bridges the different systems. In both cases this is both financially costly as well as disruptive to the efficient running of organizations.

❖ **Limitations of e-commerce to consumers**

- Computing equipment is needed for individuals to participate in the new digital economy, which means an initial capital cost to customers. A basic technical knowledge is required of both computing equipment and navigation of the Internet and the World Wide Web.
- Cost of access to the Internet, whether dial-up or broadband tariffs. Cost of computing equipment. Not just the initial cost of buying equipment but making sure that the technology is updated regularly to be compatible with the changing requirement of the Internet, websites and applications.
- Lack of security and privacy of personal data. There is no real control of data that is collected over the Web or Internet. Data protection laws are not universal and so

websites hosted in different countries may or may not have laws which protect privacy of personal data.

- Physical contact and relationships are replaced by electronic processes. Customers are unable to touch and feel goods being sold on-line or gauge voices and reactions of human beings.
- A lack of trust because they are interacting with faceless computers.

❖ **Limitations of e-commerce to society**

- Breakdown in human interaction. As people become more used to interacting electronically there could be an erosion of personal and social skills which might eventually be detrimental to the world we live in where people are more comfortable interacting with a screen than face to face.
- Social division. There is a potential danger that there will be an increase in the social divide between technical haves and have-nots – so people who do not have technical skills become unable to secure better-paid jobs and could form an underclass with potentially dangerous implications for social stability. Reliance on telecommunications infrastructure, power and IT skills, which in developing countries nullifies the benefits when power, advanced telecommunications infrastructures and IT skills are unavailable or scarce or underdeveloped.
- Wasted resources. As new technology dates quickly how you do dispose of all the old computers, keyboards, monitors, speakers and other hardware or software?
- Facilitates Just-In-Time manufacturing. This could potentially cripple an economy in times of crisis as stocks are kept to a minimum and delivery patterns are based on pre-set levels of stock which last for days rather than weeks.
- Difficulty in policing the Internet, which means that numerous crimes can be perpetrated and often go undetected. There is also an unpleasant rise in the availability and access of obscene material and ease with which pedophiles and others can entrap children by masquerading in chat rooms.

❖ **Examples of Companies Using E-Commerce**

- Amazon.com provides access to several million books electronically. It also sells music CDs, electronics, software, toys, video games, prescription drugs, and much more.
- EBay.com provides online auction service.
- Drugstore.com and CVS.com refill and sell new drugs and vitamins and other health and beauty products online.
- American Express successfully uses e-commerce for credit card transactions.
- Apple Computer sells computers online (apple.com).
- Auto-by-Tel sells cars over the Web.
- Charles Schwab, National Discount Brokers, and E-Trade have successfully used e-commerce for online security transactions.
- Cisco Systems sells data communications components over the Web.
- Dell Computer and Gateway sell computers through their web sites and allow customers to configure their systems on the Web and then purchase them.
- Epicurious sells exotic foods over the Web.
- Peapod sells groceries over the Web.
- Proctor & Gamble and IBM conduct order placements electronically.

2.4 & 2.5 Check your Progress

Answer in two – three sentences.

a. Write 4 benefits of E-Commerce to organizations.

……..

……..

b. Give the limitations of E-Commerce to consumers.

……..

……..

2.6 TYPES OF E-COMMERCE

The several categories of e-commerce in use today are classified based on the nature of the transactions, including business-to-consumer (B2C), business-to-business (B2B), consumer-to-consumer (C2C), consumer-to-business (C2B), non-business and government, and organizational (intra-business).

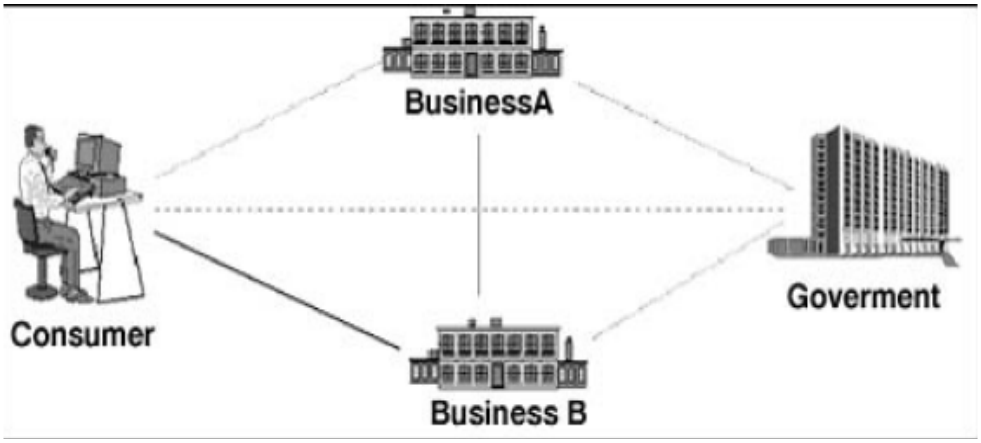


Table 2.2 Types of E-Commerce

Each of the type is described as:

Business-to-Business (B-to-B): The exchange of products, services or information between business entities. Web-based B-to-B includes:

- *Direct selling and support to business* (as in the case of Cisco where customers can buy and also get technical support, downloads, patches online).
- *E-procurement* (also known as industry portals) where a purchasing agent can shop for supplies from vendors, request proposals, and, in some cases, bid to make a purchase at a desired price. For example the auto-parts wholesaler (reliableautomotive.com); and the chemical B-to-B exchange (chemconnect.com).
- *Information sites* provide information about a particular industry for its companies and their employees. These include specialized search sites and trade and industry standards organization sites. E.g. newmarketmakers.com is a leading portal for B-to-B news.

In a B2B environment, purchase orders, invoices, inventory status, shipping logistics, and business contracts handled directly through the network result in increased speed, reduced errors, and cost savings. Wal-Mart Stores is a major player in B2B e-commerce. Wal-Mart's major suppliers (e.g., Proctor & Gamble, Johnson and Johnson, and others) sell to Wal-Mart Stores electronically; all the paperwork is handled electronically. These suppliers can access online the inventory status in each store and refill needed products in a timely manner.

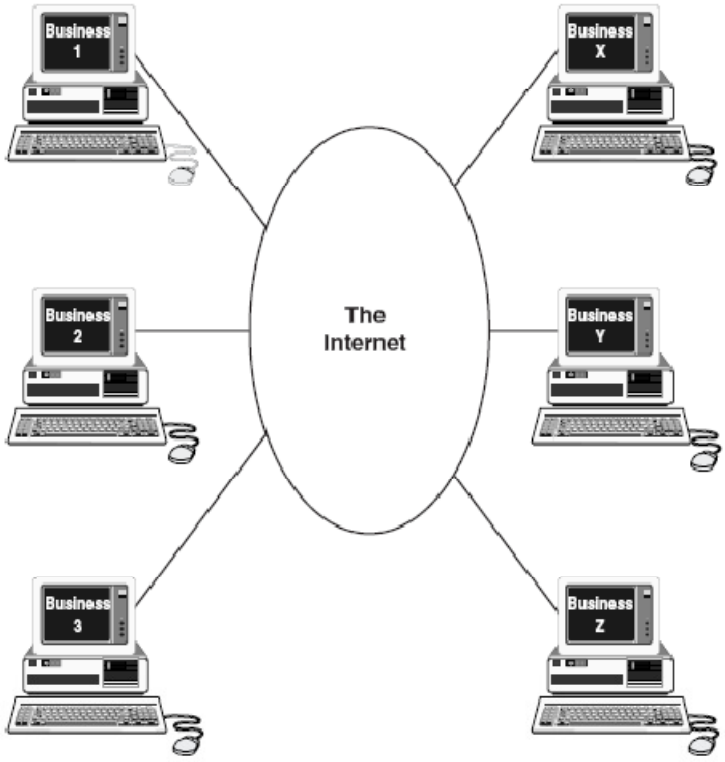


Figure 2.5 Business to Business (B-to-B) commerce

Business-to-consumer (B-to-C): The exchange of products, information or services between business and consumers in a retailing relationship. Some of the first examples of B-to-C e-commerce were amazon.com and dell.com in the USA and lastminute.com in the UK. In this case, the 'c' represents either consumer or customer.

In B2C e-commerce, businesses sell directly to consumers. Amazon.com, barnesandnoble.com, and Onsale.com are three good examples of this category. Some of the advantages of these e-commerce sites and companies include availability of physical space (customers can physically visit the store), availability of returns (customers can return a purchased item to the physical store), and availability of customer service in these physical stores.

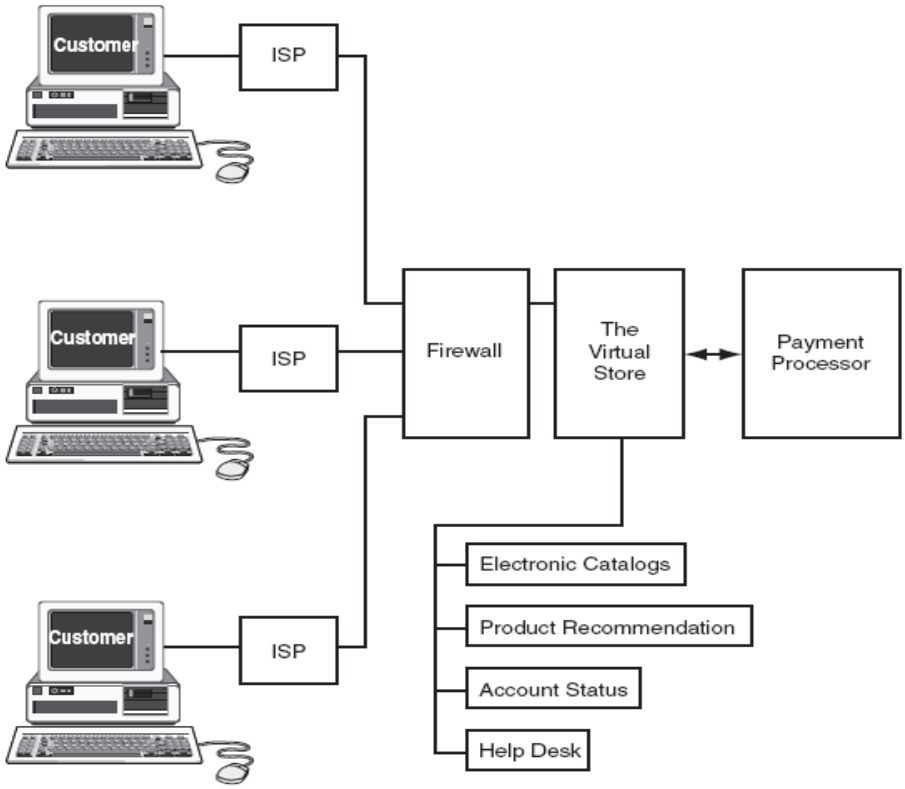


Figure 2.6 Business to Customer/Consumer (B-to-C) commerce

Business-to-Government (B-to-G): The exchange of information, services and products between business organizations and government agencies on-line. This may include,

- *E-procurement services*, in which businesses learn about the purchasing needs of agencies and provide services.
- *A virtual workplace* in which a business and a government agency could coordinate the work on a contracted project by collaborating on-line to coordinate on-line meetings, review plans and manage progress.
- *Rental of on-line applications and databases* designed especially for use by government agencies.

Business-to-Peer Networks (B-to-P): This would be the provision of hardware, software or other services to the peer networks. An example here would be Napster who provided the software and facilities to enable peer-networking.

Consumer-to-Business (C-to-B): This involves individuals selling to businesses. This may include a service or product that a consumer is willing to sell. In other cases an individual may seek sellers of a product and service. Companies such as priceline.com, travelbid.com, and mobshop.com for travel arrangements are examples of C2B. Individuals offer certain prices for specific products and services.

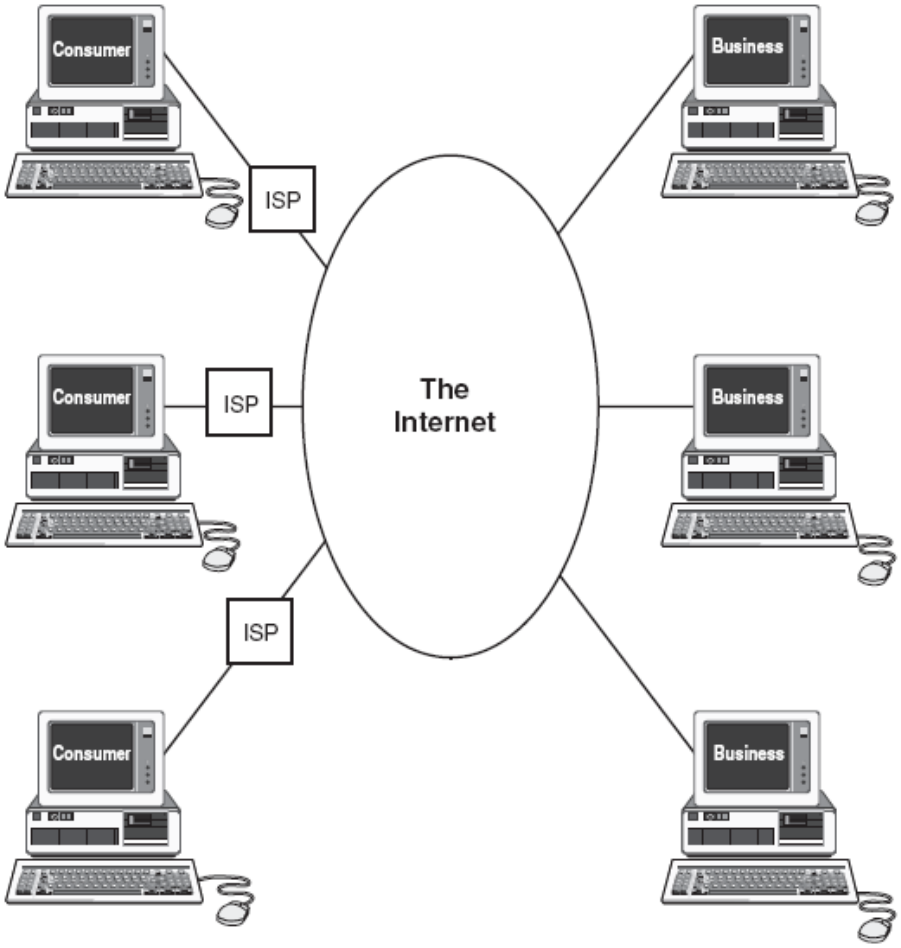


Figure 2.7 Consumer to Business (C-to-B) commerce

Consumer-to-Consumer (C-to-C): In this category consumers interact directly with other consumers. They exchange information such as:

- *Expert knowledge* where one person asks a question about anything and gets an e-mail reply from the community of other individuals, as in the case of the New York Times-affiliated abuzz.com website.
- *Opinions* about companies and products, for example epinions.com

There is also an exchange of goods between people both with consumer auction sites such as e-bay and with more novel bartering sites such as swapitshop.com, where individuals swap goods with each other without the exchange of money.

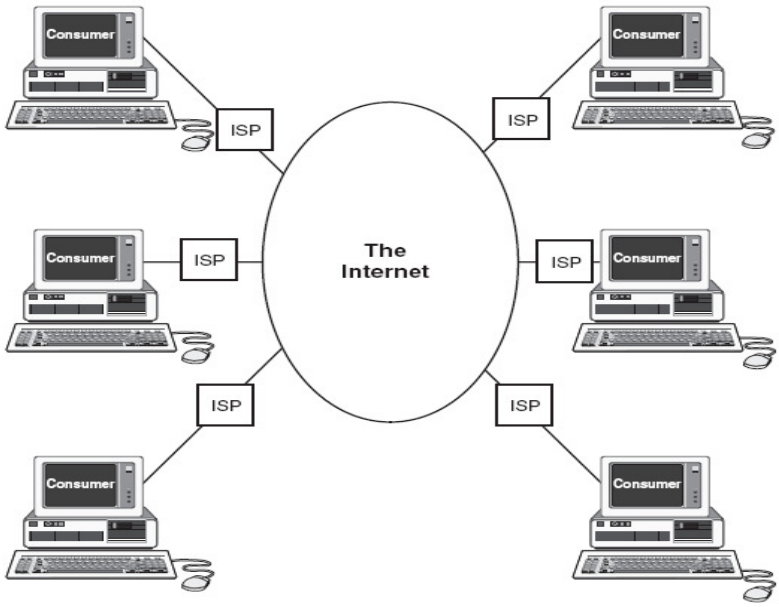


Figure 2.8 Consumer to Consumer (C-to-C) commerce

Consumer-to-Government (C-to-G): Examples where consumers provide services to government have yet to be implemented.

Consumer-to-Peer Networks (C-to-P): This is exactly part of what peer-to-peer networking is and so is a slightly redundant distinction since consumers offer their computing facilities once they are on the peer network.

Government-to-Business (G-to-B): The exchange of information, services and products between government agencies and business organizations. Government sites now enable the exchange between government and business of:

- Information, guidance and advice for business on international trading, sources of funding and support, facilities (e.g. www.dti.org.uk)
- A database of laws, regulations and government policy for industry sectors
- On-line application and submission of official forms (such as company and value added tax)
- On-line payment facilities

This improves accuracy, increases speed and reduces costs, so businesses are given financial incentives to use electronic-form submission and payment facilities.

Government-to-Consumer (G-to-B): (Also known as e-government). Government sites offering information, forms and facilities to conduct transactions for individuals, including paying bills and submitting official forms on-line such as tax returns.

Government-to-Government (G-to-G): (Also known as e-government). Government-to-government transactions within countries linking local governments together and also international governments, especially within the European Union, which is in the early stages of developing coordinated strategies to link up different national systems.

Government-to-Peer Network (G-to-P): As yet there is no real example of this type of e-commerce.

Peer–to-Peer Network (P-to-P): This is the communications model in which each party has the same capabilities and either party can initiate a communication session. In recent usage, peer-to-peer has come to describe applications in which users can use the Internet to exchange files with each other directly or through a mediating server.

Peer Network-to-Consumer (P-to-C): This is in effect peer-to-peer networking, offering services to consumers who are an integral part of the peer network.

Peer Network-to-Government (P-to-G): This has not yet been used, but if it was, it would be used in a similar capacity to the P-to-B model, only with the government as the party accepting the transaction.

Peer Network-to-Business (P-to-B): Peer-to-peer networking provides resources to business. For example, using peer network resources such as the spare processing

capacity of individual machines on the network to solve mathematical problems or intensive and repetitive DNA analyses which requires very high capacity processing power.

This framework can be used by organizations to segment their customers and distinguish the different needs, requirements, business processes, products and services that are needed for each.

1.6 Check Your Progress

Answer in two – three sentences.

1. Enlist the different types of E-Commerce.

……..

……..

2.7 THE BARRIERS TO E-COMMERCE

The drivers of e-commerce were identified and summarized in Figure 2.4. Conversely, there are also barriers to the growth and development of e-commerce. Numerous reports and surveys identify the different kinds of barriers, and many of them focus on security as being one of the largest problems for e-commerce. The issues that are relevant to the type of organization also differ. For example, large organizations have different needs and infrastructures to SMEs (medium sized enterprises).

The findings summarized in Figure 2.9 show that barriers to e-commerce can be seen as being relevant both to the macro-environment and the micro-environment level of the firm itself. Overall, all three (large organization, SME, small retailers) kinds of organizations have similar barriers but with different emphases.

Internet infrastructure deals with issues such as availability and quality of the Internet in terms of speed and reliability. This barrier is of particular concern to SMEs (medium sized enterprises) and B-to-C (retailers) organizations, since their business relies more on general consumers, and so the ease with which the general public can connect to the Internet has a direct impact on their Web-based business.

Technology infrastructure deals with issues of standardization of systems and applications, which is a particular concern for larger organizations who want to implement solutions such as value chain integration and e-supply chain management.

Security in its broadest term is one of the most significant barriers to e-commerce both within the organization and external to it. Identified as Security and Encryption; Trust and Risk; User Authentication and Lack of Public Key Infrastructure; Fraud and Risk of Loss it relates to the development of a broader security infrastructure and it also relates to the kinds of measures organizations can take to improve security. Although security is a major concern for all types of organizations, it is a dominant concern for companies in the B-to-C e-commerce retail sector, since it reflects the concerns and perceptions of users and potential customers that are conducting financial transactions on-line.

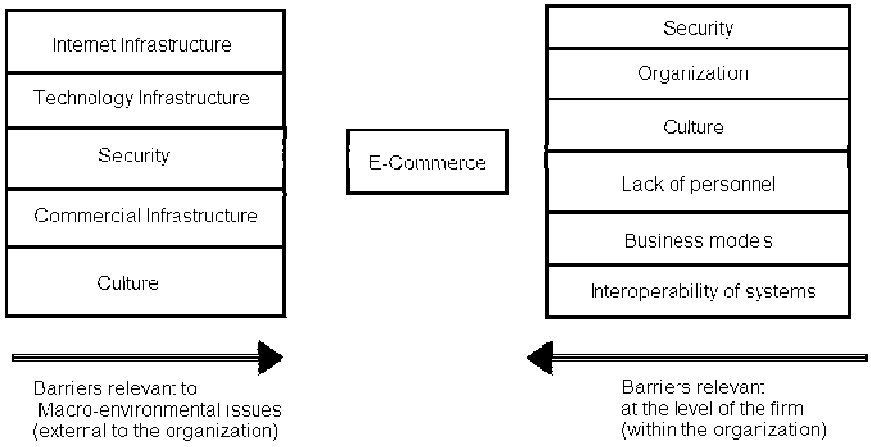


Figure 2.9 Barriers to E-Commerce

The commercial infrastructure relates to issues such as international trade agreements, taxation laws and other legal agreements that facilitate all kinds of on-line trading and so is a barrier relevant to all types of organizations.

At the level of the organization itself, there are many barriers to e-commerce that relate to issues of *organizational structure and culture*. These are most significant for large organizations that have to deal with change management issues. For example, there is a sense that much work still needs to be done to design the right organizational structure and corporate culture that will promote and be able to maximize the benefits of widespread-commerce applications. Additionally, there is a perception that business partners face similar organizational and technological problems, which raises the barrier further.

Another significant issue was found to be the *lack of qualified personnel* to implement in-house and third-party e-commerce systems. For SMEs, this is a particularly strong concern because internally they do not have sufficient resources to attract and maintain their own support staff to develop a sophisticated technology infrastructure. With regards to third parties, the qualified personnel tended to work for larger organizations, which were more concerned about serving the more lucrative larger clients than SMEs. One respondent noted that, 'small firms get lots of vague and general exhortations to go "online" but find it very difficult to get reliable, well informed advice and also to get honest, effective support from a Web services provider.

Another major barrier to the development of e-commerce was a *lack of proven business models*. This is a reflection of the instability of the whole dot com phenomenon, and the poor performance of the dot-coms on the world's stock exchanges in late 1999 and early 2000 after the dizzy heights to which dot-com companies rose in 1998–9. A financially successful business model has yet to emerge into the business world's limelight as the model to follow.

Interoperability of systems is identified as one of the major barriers for large US-based B-to-B corporations. This refers specifically to implementation and compatibility problems of integrating new e-commerce applications with existing legacy systems and resources within organizations. This problem also extends to interacting with systems of business partners and stakeholders. The fact that the USA is ahead in the adoption lifecycle of e-commerce suggests that these issues will become more prevalent in other nations that are further behind in the lifecycle. Thus there is a need for standards to be introduced to overcome issue of incompatibility and interoperability. For SMEs that have fewer legacy systems, the issues are more a matter of interoperability with partner systems.

Many of the top barriers recognized by respondents in 2000 were also top concerns in 1999, especially security. This illustrates a consistency and reliability of the measures being taken by the survey and also underlines the fact that they are not being addressed adequately. The two major changes were increased concern over lack of business models and lack of qualified personnel.

2.8 E-COMMERCE APPLICATIONS

Six major e-commerce sectors: Infrastructure: Applications, Portals, Content, Services and Exchanges.

Some common applications related to electronic commerce are:

- E-mail and Instant Messaging
- Documents, spreadsheets, database
- Accounting and finance systems
- Orders and shipment information
- Enterprise and client information reporting
- Domestic and international payment systems
- Newsgroup
- Online Shopping/Purchasing
- Video on demand
- Conferencing
- Online/Remote banking
- Electronic tickets
- Supply Chain Management
  E-Commerce provides support services including

- **Electronic checks (e-checks)** are similar to regular checks. They are used mostly in B2B
- **Electronic credit cards** make it possible to charge online payments to one's credit card account.
- **Purchasing cards,** the B2B equivalent of electronic credit cards.
- **Electronic cash (e-cash)** appears in three major forms: stored-value cards, smart cards, and person-to-person payments.
- **Electronic Bill Presentment and Payments** allow customers to pay their recurring monthly bills, such as telephone, utilities, credit cards, etc. online.
- **E-wallets** are mechanisms that provide security measures to EC purchasing. The wallet stores the financial information of the buyer, including credit card number, shipping, information, and more.
- **Virtual credit cards** are services that allow you to shop with an ID number and a password instead of with a credit card number.
- **e-infrastructure** (mostly technology consultants, system developers and integrators, hosting, security, and networks)
- **e-process** (mainly payments and logistics)
- **e-markets** (mostly marketing and advertising)
- **e-communities** (different audiences and business partners)
- **e-services** (CRM, PRM, and directory services)
- **e-content** (supplied by content providers)

2.9 E-COMMERCE AND ELECTRONIC BUSINESS

While some use e-commerce and e-business interchangeably, they are distinct concepts. In e-commerce, information and communications technology (ICT) is used in inter-business or inter-organizational transactions (transactions between and among firms/organizations) and in business-to-consumer transactions (transactions between firms/organizations and individuals).

In e-business, on the other hand, ICT is used to enhance one's business. It includes any process that a business organization (either a for-profit, governmental or non-profit entity) conducts over a computer-mediated network. A more comprehensive definition of e-business is: "The transformation of an organization's processes to deliver additional customer value through the application of technologies, philosophies and computing paradigm of the new economy."

In simple words, E-commerce describes the process of buying, selling, transferring, or exchanging products, services, and/or information via computer networks, including the Internet. E-business refers to a broader definition of e-commerce, not just the buying and selling of goods and services, but also servicing customers, collaborating with business partners, conducting e-learning, and processing electronic transactions.

Table 2.3 E-Business & E-Commerce

E-Business	E-Commerce
1) It's a continuous process right from initiation of sale offer to after sale customer caring.	1) It's a conclusion to a sale or a purchase activity through internet banking or credit card gateway.
2) Customer educating, Internet marketing and Business Research are done effectively.	2) It's an activity just done by website that accepts debit/credit cards and internet purchasing.
3) Uses internet for all its business activities.	3) It is the domain of E-Business

Three primary processes are enhanced in e-business:

1. *Production processes* which include procurement, ordering and replenishment of stocks, processing of payments, and electronic links with suppliers, production control processes.
2. *Customer-focused processes* which include promotional and marketing efforts, selling over the Internet, processing of customers purchase orders and payments, and customer support.
3. *Internal management processes* which include employee services, training, internal information-sharing, video conferencing, and recruiting. Electronic applications enhance information flow between production and sales forces to improve sales force productivity. Workgroup communications and electronic publishing of internal business information are likewise made more efficient.

- **Is the Internet economy synonymous with E-commerce and E-business?**

The Internet economy is a broader concept than e-commerce and e-business. It includes e-commerce and e-business. The Internet economy is related to all economic activities using electronic networks as a medium for commerce or those activities involved in both building the networks linked to the Internet and the purchase of application services such as the provision of enabling hardware and software and network equipment for Web-based/online retail and shopping malls (or "e-malls"). It is made up of three major segments: physical (ICT) infrastructure, business infrastructure, and commerce.

2.7, 2.8 & 2.9 Check your Progress

1. Fill in the blanks.

a. ……deals with issues of standardization of systems and applications.

b. …… of systems is identified as one of the major barriers for large US-based B-to-B corporations.

c. In e-commerce, ……..is used in inter-business or inter-organizational transactions

2.10 E-COMMERCE WITH WWW-INTERNET

This e-commerce market is the collective product of many individuals and organizations that cooperate to build it then compete on the products and services they sell. The result is an entrepreneurial explosion of applications and services, building on and adding value to each other so that no closed or proprietary market can match. By the year 2000, the Internet e-commerce market is projected to include one million companies and 100 million consumers; annual revenues from retail transactions exceeding, in the view of some, $50 billion, including 50 percent of all software sales and 25 percent of all music CDs; 25 percent of all business-to-business transactions will be accommodated by this medium.' Some of these opportunities are discussed next.

- **Opportunities**

On-line Web selling

There are four ways that Web commerce can be undertaken over the Internet. They are as follows:

- Toll-free or other telephone numbers. After Web browsing, order the goods by telephone or fax. The advantage of ordering through a toll- free number is that the whole transaction-security issue is skipped, although ordering by telephone is not as convenient as ordering online white browsing for goods.
- Shopping clubs. This approach requires new customers to join the club by submitting their credit card information via fax or telephone and subsequent purchases are billed to the credit card.
- Off-line ordering and paying. In this approach, customers send checks to the company for the goods they wish to purchase.

- On-line credit card entry. An increasing number of Web-based vendors now offer on-line order blanks for shoppers to enter their credit card number but do not encrypt the card number. This is a potential security risk, in that a hacker could read the credit card and make charges to it. The good news is that there is progress on credit card security on the Internet and for transmission of other materials (e.g., with the use of SEPP, SSL, and S-HTTP).

Virtual malls

The combination of the home PC and the Internet is making on-line services and shopping easier to implement. For example, MCI has created a large system for shopping based on the Netscape commercial server technology. Although we can view virtual malls as a subset of on-line Web selling, the shopping atmosphere and experience are somewhat different. These Web sites may be more expensive to develop because of the higher aesthetic quality of the cyberspace environment.

The following is a partial list of virtual shopping malls on the Internet:

Apollo advertising	http://apollo.co.uk
Branch Information Services	httplibranch.com:1080
MarketPlace.Com	http://xnarketplace.com
MarketNet	http://inkneo.uk
Interactive Super Mall	http://isupermall.com
Downtown Anywhere	http://awa.com
GNN Direct	http://gnn.comignnignndirect
Internet Mall	
httpliwww.mecklenveb.com:80/mall/imall.html	

Advertising

Organizations that provide well-known Web sites have come to realize that it is possible to charge a recurring fee to companies wishing to have pointers to their own information placed before the public. CNN was charging $7500 per week to place a pointer to a company page on its hot list which is seen by millions of people per day Silicon Graphics pays Hot Wired magazine $15,000 per month to have a direct link to its home page. Netscape Communication has charged $40,000 for a three-month advertisement placement on its Web site (the site received more than 400,000 hits per day). There are several advantages to advertising on the Internet. One of the most significant is that the sponsor can measure how many people see the information and can interact with them. This is superior to television or other forms of passive advertising. Some Internet news services (e.g., Infoseek) use filters to collect desired news information for the customer, and then use this demographics information to narrowcast or pointcast ads to the user/consumer.

Home banking and financial services

As it becomes easier for consumers to do network-based banking, the competition in traditional banking services will become more intense. CyberCash, DigiCash, and other companies are poised to change the nature of financial services delivery on the Internet. The move by some banks to reduce or eliminate fees for on-line banking may be viewed as service dumping into the market in order to fight off the rapidly emerging competition.

Catalog publishing

Many organizations have built home pages that incorporate electronic catalogs listing the products and services the company has to offer. Many of these companies do not yet offer on-line ordering of these products and services from their Web site, but stick with the traditional toll-free number (800 or 888) telephone support for ordering products. The major advantages of this model are that it complements the existing organizational structure and business model and does not require (evolving) transaction security over the Internet.

Interactive ordering

As was just described, many companies have catalogs of their goods and services available on WWW home pages, but they do not support Web-based interactive ordering. An increasing number of early adopter companies, however, do allow interactive ordering of their goods by implementing secure credit card payments over the Internet. The advantage to this integrated approach is that it further

automates the ordering process. However, as of press time, only a limited number of Web servers and browsers support transactional security with back-end clearance of credit cards and other payment issues.

The problem with making electronic Web payments "in the clear" is that the Internet is not a private network to which only a very limited and controlled population has access. Because the Internet is a public network, electronic transactions can in principle be intercepted and read by other servers on the network. Hackers can pick off logins and passwords. This can happen in one of three ways:

1. The hacker physically taps the communication line with a protocol analyzer. Likely, this would have to occur at the carrier central office (the ISP, LEC, CLEC, etc.) or at the server-location site (e.g., in the company's own location if it were an "inside job").
2. The hacker can reprogram the table of a network router to route information to one of his or her devices for further analysis. This would require either physical access to the router's management port or remote infiltration of that port by identifying its IP and/or dial-up address and then breaking through the access and privilege list of the router. However, the command-line interface of a router is fairly complex and vendor-dependent; the number of people with that kind of practical knowledge is small and they are generally paid "six figures" (implying that unless they are pathological or malicious, they should have no motive to break in).
3. The hacker can actually break into the server by frustrating its host security mechanism and then can read privileged information (login IDs, credit card information, etc.) from the end system in question.

One wonders which of these three methods is more popular with hackers. We tend to believe the latter rather than the former two. This is because these kinds of individuals tend to be more "computerniks" than "communicationniks"; computer information is more pervasive than communication information. It would be ironic that for all the bad publicity that the Internet receives about security if this were the case because then all infractions can be attributed to and cured by local host security measures, not networking measures; the only role that the Internet plays is to enable the hacker a venue of transport, which is otherwise a legitimate Internet function.

Using the same mechanisms, these hackers can read the contents of unencrypted e-mail or FTP files (or any type of electronic file being sent through the Internet). The Internet is vulnerable to these attacks because it is a decentralized network spread across hundreds of thousands of computers worldwide. Thus, there is a critical need to secure data, especially credit card—type electronic transactions.

Direct marketing

The Internet population of users is growing at 8 percent per month. The challenge that many businesses have is how to reach these users through marketing and advertising to motivate these users to buy their products. Direct marketers use the Internet to disseminate e-mail advertising their products and services. The only charge associated with Internet mailings is the flat monthly fee charged by access providers; however, setup costs such as the prices of powerful PCs, servers, software, and other expenses have to be taken into account in this equation. Direct marketers can utilize newsgroups and discussion forums which represent the audience most likely to purchase their products. Organizations can market their products on the Internet by posting press releases into newsgroups and mailing lists. Once a press release is posted to a newsgroup, all of the subscribers to the newsgroup will receive the release. Another way to market a company on the Internet is to incorporate a sign-off at the end of each of the messages a company posts on the Internet. This signature sit the end of the message is typically a couple of lines about the company and represents a low-key way to advertise.

- **Internet and WWW tools**

To begin the discussion of Internet tools, it must be noted that the Internet is neither new nor is it. Some mythologized entity. It grew out of the ARPAnet established in the mid-1970s; it was redesigned into the NSFNet in the mid-1980s; and it has been reengineered for full commercial status in the early to mid-1990s. On-line computer

searches have been available to researchers for decades and on-line information access for the general public has been available in France using the Minitel technology for well over a decade. Similarly, networks such as America Online have provided access to a variety of services and content for a number of years. The Internet is simply a network; that is, a set of interconnected routers. It is a set of local, long-haul, and international links. It, in itself, has no content. Organizations that connect their servers to the Internet and allow users to access them provide the content. Some companies specialize in content delivery What has made use of the Internet growth phenomenon are the simple to use network graphical user interfaces (NGUIs) that have appeared in the form of browsers. The use of standardized protocols to support data formatting (e.g., HTML) and data transfer (HTTP/TCP/IP) have given it scalability.

So, we choose to view the Internet just as a long-haul data (IP-based) network. Like AT&T or MCI's telephone network. In reality that is all it is, by itself. The interesting fact is, however, that as the national telephone network spread during the first three decades of this century, it supported a high-end, expensive service: long-distance calling was always considered an elite activity, so much so, in fact, that AT&T charged a premium (until divestiture of the Bell System in 1984) to those who could afford to make long-distance calls, in order to subsidize local calling. Eventually, the price came down after competition became vigorous in the 1980s and 1990s. The Internet, however, is going the other way around. It started out as a nearly free long-haul data service. Many see it as a flat-rate, volume-insensitive, distance- insensitive network. In the future, however, the charges for Internet use are likely to increase, as the Internet moves out of its academic genesis in the 1980s and into the full commercial limelight.

The key Internet applications of interest to electronic commerce are, as implied from the previous discussion, electronic mail, newsgroups, FTP archives, Telnet, WAIS, Gopher, World Wide Web (WWW), and agents. These tools provide the building blocks for organizations and businesses wishing to utilize the Internet for electronic commerce. The following sections will describe these access tools in detail:

Electronic mall

The least expensive and still the most predominant of the Internet information access mechanisms is e-mail. E-mail services allow companies to make information available to a large universe of recipients. Not only can e-mail be sent to people connected directly to the Internet, but it can also be sent to on-line networks connected to the Internet including, for example, commercial networks such as Prodigy, America Online, and CompuServe. Tens of millions of people are accessible on the Internet via e-mail. Mailing lists contain a list of e-mail addresses that can be reached by sending e-mail to a single multi- cast address, making e-mail useful for information dissemination. E-mail is often likely to be read and responded to soon after it arrives to a user's mailbox.

Internet e-mail uses a number of Internet protocols, including SMTP (RFC 822), MIME (RFC 1767), and Post Office Protocol (POP). RFC 822 is the protocol used to transfer a message from one e-mail system to another, and RFC 822 defines the standard format for Internet e-mail messages. Both are widely implemented and supported. SMTP can only support text messages and not, by itself, attachments with multiple body parts: SMTP cannot send any files that include non- printable characters; thus SMTP cannot send executables and other files incorporating binary data (i.e., Word for Windows files and Excel spreadsheets). As noted earlier, MIME is a set of extensions to Internet e-mail that provides support for non-text data and multiple body parts. A MIME object is carried within an SMTP message. When a MIME object contains non-text dlata, such as binary data, it is encoded as printable text, so that the integrity of the data is preserved as it travels through SMTP systems. The sender's MIME package encodes the binary data into printable text and the receiver's MIME package decodes the data back into its original form.

There are a number of ways that e-mail can be used for commerce and/or to gather information. For example, a business could write a monthly newsletter covering topics of interest to the company's customers. Unlike traditional newsletters, however, the company would not have to pay for physical distribution. E-mail can be an effective customer support tool. For example, a customer could register a complaint or ask for assistance from a company without having to hold on a phone line.

Newsgroups

Newsgroups are discussion forums where articles get posted as topics and replies get posted to create a thread (a thread is the series of responses to a message in a newsgroup). Articles can be posted to multiple newsgroups (cross-posting). A newsgroup can be established as moderated or read-only. Articles can be posted via e-mail, although many browsers now incorporate into their software the ability to view newsgroups. Newsgroup postings age and are deleted after a certain number of days or weeks; this aging varies based on a news server basis. Sites with limited disk space will age postings quicker than sites with a lot of disk space.

File Transfer Protocol

Although not as user-friendly and/or interactive as the World Wide Web, user/provider-initiated FTP can provide an inexpensive method to deliver information to customers, particularly for long technical materials such as manuals, specifications, RFPs/ FAQs. FTP is the way most Internet users get files from other Internet hosts (servers). FTP allows a user to log on to a remote host (server), but restricts the user to a limited set of commands. Next to e-mail, FTP is the most commonly used Internet service. Most FTP archives allow for public access via anonymous FTP. A system set up with anonymous FTP access allows any remote FTP user to log in to that system and transfer a set of files. The administrator of the FTP archive defines which files may be downloaded by remote users logging in to the system via anonymous FTP.G

An example of the use of FTP is electronic catalog shopping. A company could set up an FTP directory that has a price list and item descriptions. Customers could download the price list and view it on their home computers in a text editor. Pictures of the items could be in the FTP directory. The customers could read the descriptions and view the corresponding pictures.

Telnet

Telnet is a utility that allows users to log in to a remote system just as though they were logging in to a local system. Once logged in, the users have the same access to the system as though they logged in from a terminal attached directly to the system. This method requires computer skills. Also, the logged-in party tends to get access to a lot of the system capabilities, including operating system access. This implies that the party logging in must be trusted. Telnet and rlogin are probably the most powerful tools a hacker has.

WAIS

While the World Wide Web is a user-friendly interface for browsing data, it has somewhat limited search capabilities. WAIS allows users to search for specific data they are interested in. WAIS searches the documents in a list of servers for one or more keywords and reports back to the user which documents, if any, have occurrences of the keywords. WAIS is often used in conjunction with World Wide Web servers as the companion search engine. WAIS works by indexing documents a priori. Indexing of documents allows for quick searches when users send queries to the WAIS database. Together, the index software and the WATS database server allow users to create databases comprised of different types of documents, images, and other files and also give users access to the database through easy-to-use client software.

In older versions of WAIS the user looked through the resulting list of documents to find what was needed; newer WAIS software supports further searches by allowing the user to place entire documents into the keyword search engine and execute the search again. The WAIS search engine uses the documents as additional search information and looks for documents that not only match the user's original keywords, but are similar to the documents imported into the search. Newer search engines also allow users to utilize Boolean logic expressions (AND. OR, etc.) and wildcards in their searches. One of the problems with WAIS is that it requires a large amount of disk space. For example, the resulting index of a text-based document can be as large as or larger than the original document itself. WAIS servers with a large number of documents pay a premium in disk space.

Gopher

Gopher is one of the information search and retrieval tools that preceded the widespread use of WWW. Gopher's use is now commonly integrated with the more sophisticated browser interfaces. Gopher is a simple tool and relatively easily

implemented, but is an important capability. It can be described as a document delivery tool; in fact, Gopher can deliver documents, lists of documents, and indexes. Gopher servers can offer not only textual information, but also organized browsing lists of resources on the Internet. Gopher transparently links groups of file servers, each with their own accumulation of files and folders. One folder on a computer may access other folders located on another computer. Text files, sounds, and graphic images including photographs and drawings can be accessed and retrieved.

WWW

The World Wide Web, abbreviated as WWW and commonly known as the Web, is a system of interlinked hypertext documents accessed via the Internet. With a web browser, one can view web pages that may contain text, images, videos, and other multimedia and navigate between them by via hyperlinks. HTML, which stands for HyperText Markup Language, is the predominant markup language for web pages. A markup language is a set of markup tags, and HTML uses markup tags to describe web pages. The purpose of a web browser is to read HTML documents and display them as web pages. The browser does not display the HTML tags, but uses the tags to interpret the content of the page.

A website is a collection of related web pages, images, videos or other digital assets that are addressed relative to a common Uniform Resource Locator (URL), often consisting of only the domain name, or the IP address, and the root path ('/') in an Internet Protocol-based network. A web site is hosted on at least one web server, accessible via a network such as the Internet or a private local area network.

HTML elements form the building blocks of all websites. HTML allows images and objects to be embedded and can be used to create interactive forms. It provides a means to create structured documents by denoting structural semantics for text such as headings, paragraphs, lists, links, quotes and other items. It can embed scripts in languages such as JavaScript which affect the behavior of HTML web pages.

2.11 COMMERCE-NET ADVOCACY

CommerceNet sees itself as serving as the prototype for an open twenty-first-century Internet-based organization. CommerceNet and its members are developing elements of the infrastructure model for the future support of Web commerce. This is achieved through development, implementation, and expansion of the technical and institutional protocols required to impart electronic commerce to all worldwide markets. Launched in Silicon Valley in 1994, CommerceNet has grown to over 200 member companies and organizations worldwide. CommerceNet pioneered Web commerce by legitimizing the Internet as a place for business, developing key elements of the infra-structure such as security and payment, and fielding pilot demonstrations. Table 2.4 depicts the organization's activities and goals.

Table 2.4 Commerce-Net activities and goals

Advocacy	Promoting a legal and regulatory environment that fosters global commerce. CommerceNet engages businesses and governments in a constructive dialogue on issues such as trade, tariffs, taxation, privacy, and copyrights.
Business Outreach	Providing business decision makers with real-time knowledge to assist them in developing their Internet commerce strategies. CommerceNet provides executive briefings, seminars. Conferences and consulting services.
Vertical industry Solutions	Jump-starting key e-commerce by linking communities of interest involved in vertical market segments such as financial or health care services, manufacturing supply chains, or retail inventory management_
E-commerce Infrastructure	Defining an open architecture and populating it with interoperable network and e-commerce services from multiple vendors that enhance the basic reliability, performance, and security of the Net and provide essential services such as payments, directories, and ELM.

CommerceNet is a not-for-profit market and business development organization, with the mission of accelerating the growth of Internet commerce and creating business opportunities for its members. The organization focuses on precompetitive global and industry-wide issues, so that members can benefit from economies of scale and avoid competing on an ineffective basis. The organization approaches issues from a multidisciplinary perspective encompassing technology, business processes, and regulatory policies. CommerceNet operates as a virtual organization, relying heavily on the expertise and resources of *its* members as well as

other industry associations.

Members of CommerceNet include leading U.S. computer companies, VANs, Telcos, on-line services, money center banks, and credit card processors. During 1996 in partnership with Nielsen, Commerce- Net produced the first definitive survey documenting the explosive growth of the Internet marketplace; the re-contact follow-up Nielsen/ CommerceNet survey became available August 1996 (this study was quoted earlier). CommerceNet was involved, directly or indirectly, in the formation of many promising Internet startups, including Cyber-Cash, I/Pro, Internet Shopping Network, Netscape, Open Market, Saqqara, and Terisa Systems.

CommerceNet and its members developed and demonstrated the first security and payment protocols for the World Wide Web, paving the way for secure transactions. They are working on protocols for efficiently searching multiple directories and catalogs. CommerceNet also developed and distributed Internet starter kits for both users and service providers a year before commercial packages became available, *as* well as provided numerous development and site administration tools for corporate Webmasters, which led to successful commercial products.

CommerceNet organized more than 10 pilots to demonstrate the bottom-line potential of Internet commerce. Examples include an online RFQ bidding service for the electronics industry; a secure on-line system for filing withholding tax information; and the exchange of EDI payment instructions and confirmations over the Internet. Position papers on significant issues impacting the Internet marketplace are prepared and circulated to key government and industry leaders. The issues range from the unification of competing credit card payment protocols and the lifting of cryptography export controls, to the development of national guidelines for digital signature legislation.

Today, e-commerce is at a critical juncture. After an exhilarating start-up phase, further development hinges on bridging the chasm between early adopters and a true mass market. CommerceNet has identified four synergistic goals to ensure a successful transition:

- Developing the infrastructure to support mass-market Internet- based commerce on a global scale
- Jump-starting key vertical markets
- Engaging businesses in many more industries and geographic regions
- Creating a conducive legal and regulatory environment

CommerceNet is helping the industry converge on a standard architecture (which it calls E-co System) by endorsing key protocols and APIs and certifying the conformance and interoperability of its members' products. It is also organizing global *communities of interest* around important vertical markets. In real estate, for example, the marketplace must bring together buyers and sellers with numerous third parties such as newspapers, brokers, banks, title companies, termite inspectors, and multiple listing services. CommerceNet focuses on large international service industries such as finance, publishing, and shipping, as well as on manufacturing industries such as electronics, automobiles, and software, with international supply networks.

2.10 & 2.11 Check your Progress

1. State whether following sentences are True or False.

a. The advantage of ordering through a toll- free number is that the whole transaction-security issue is skipped.

b. Organizations that provide well-known Web sites have come to realize that it is impossible to charge a recurring fee to companies wishing to have pointers to their own information placed before the public.

c. CommerceNet is a not-for-profit market and business development organization

2. Match the following.

Column A	Column B
a. WWW	1. Information search and retrieval
b. WAIS	2. Interlinked hypertext documents
c. Gopher	3. Discussion forums
d. Newsgroups	4. Search for specific data

2.12 SUMMARY

The Internet has lead to the birth and evolution of electronic commerce or Ecommerce. E-commerce has now become a key component of many organizations in the daily running of their business. E-commerce challenges traditional organizational practices, and it opens up a vast array of issues that the organizations must address. By focusing on the varying levels of an organization, it soon becomes apparent what effect E-commerce can have. An understanding of the implication E-commerce has on such organizational divisions can help businesses gain understanding hence plan for its inevitable continuing evolution.

The surrounding of e-business may be new to this generation, but the same patterns of behavior occurred in the development of earlier technologies, including the steam engine, telegraphy, automobiles, airplanes, and radio. Similar to those culture changing technologies, many lessons were learned during the e-commerce gold rush. Surely, it's confusing, too many thought everything "e" was a magic bullet. But the technology that fueled that initial Internet bubble is what fuels the successful businesses of today. So, in the long term, e-business changed how business is conducted and it is here to stay. We are looking at the future business of the world.

The chapter provided a detailed definition of e-commerce and e-business and reviewed the major components of e-commerce. There is no one commonly agreed definition of e-commerce or e-business. Thus, there is a need to clarify terms being used and explain the context in which they are being applied. E-commerce has an impact on three major stakeholders, namely society, organizations and customers (or consumers). There are a number of advantages, which include cost savings, increased efficiency, customization and global marketplaces. There are also limitations arising from e-commerce which apply to each of the stakeholders. E-commerce was compared to traditional commerce and the major categories of e-commerce were defined, including business-to-consumer (B2C), business-to-business (B2B), consumer-to-consumer (C2C), organizational (intra-business), consumer-to-business (C2B), and non-business and government. The chapter explored the advantages and disadvantages of e-commerce and then explained major activities involved in a C2B e-commerce life cycle.

Electronic commerce is growing rapidly. A number of technologies have converged to facilitate the growth of e-commerce. The rapid advances in computer technology coupled with rapid acceleration in communication networks and the development of sophisticated software have revolutionized the way business is done. However, this is not sufficient to grow e-commerce applications. Proper management of enterprise information security resources is the need of the hour. With proper understanding of business needs and management of enterprise information security resources, e-commerce will immensely benefit every individual. These include information overload, reliability and security issues, and cost of access, social divisions and difficulties in policing the Internet. Successful e-commerce involves understanding the limitations and minimizing the negative impact while at the same time maximizing the benefits. In order to aid general understanding of e-commerce a number of frameworks have been introduced to explore it from different perspectives: the macro-environment, which identifies the interaction of technology, people, organizations, policy and technical standards working together to enable e-commerce; the different participants and the kind of e-commerce transactions that occur between them; and the degree of digitization that analyses product, processes and delivery agents in an organization. These frameworks help identify the elements of e-commerce and how businesses can better understand e-commerce and its practical applicability.

Source : *www.isaca.org (Link)*

2.13 CHECK YOUR PROGRESS – *ANSWERS*

2.1 & 2.2

1. a) Goods and services b) Electronic Data Interchange
c) Specific and structured

2. a) EDI means Electronic Data Interchange. It is nothing but the transfer of data between different companies using networks, such as the Internet.
b) Decreases paperwork, Expands the organization customer base, Improves customer service, Improves response and access to information, Improves communications, Improves cost efficiency, Improves customer service.

2.3 **1.** a) Electronically b) Infrastructure and environment

2. a) E-Commerce or Electronic Commerce is any form of business transaction in which the parties interact electronically over the Internet rather than by physical exchange.

b) Technological factors, Political factors, Social factors, Economic factors, Organizational culture, Commercial benefits, Skilled and committed workforce, Requirements of customers and suppliers, Competition.
Low Entry Cost, Reduces Transaction Costs, Access to the global market, Online distribution, Secure market share.

2.4 & 2.5

1. a) International marketplace, Operational cost savings, Mass customization, Enables reduced inventories, Lower telecommunications cost.

b) Computing equipment is needed, Cost of access to the Internet, Lack of security and privacy of personal data, Physical contact and relationships are replaced by electronic processes, lack of trust.
Amazon.com, EBay.com, American Express, Apple Computers, Cisco Systems, Dell Computers, IBM.

2.6

1.a) Business-to-Business,Business-to-consumer, Business-to-Government,Business-to-consumer,Business-to-overnment,Consumer-to-Business,Consumer-to-Consumer,Consumer-to-Government,Government-to-Business,Government-to-Government, Government-to-Consumer.

2.7, 2.8 & 2.9

1. a)Technology infrastructure
b)Interoperability
c)Information
and communications technology (ICT)

2.10 & 2.11

1. a) True
b) False
c) True

2. a-2
b-4
c-1
d-3

2.14 QUESTIONS FOR SELF-STUDY

1 Describe what is EDI?
1. Discuss the advantages and disadvantages of EDI.
2. Explain what E-Commerce is and how it works.
3. Explain advantages and disadvantages of E-Commerce.
4. What are the types of E-Commerce? Explain.
5. What are the barriers to E-Commerce?
6. Explain key factors of E-Commerce.
7. What are the E-Commerce applications?
8. Explain the difference between E-Business & E-Commerce
9. Write in brief: e-commerce with WWW-internet.
10. What is CommerceNet advocacy? Explain.

2.15 SUGGESTED READINGS

The Complete E-Commerce Book By Janice Reynolds

Web Commerce Technology Handbook By Daniel Minoli Emma Minoli

How E-commerce Works - HowStuffWorks "Business & Money"

NOTES

NOTES

Chapter 3

APPROACHES TO SAFE E-COMMERCE

3.0 OBJECTIVES

After studying this chapter you will be able to :

- explain about secure transport protocol and secure socket layer.
- describe secure electronic transaction.
- discuss how SEPP and SET work.
- discuss what is authentication and certificates.
- explain about security on web servers and enterprise networks.

3.1 INTRODUCTION

As business activity grows on the internet, security is becoming an important consideration to take into account and to address, to the stakeholder's satisfaction. From recent years, commerce on the internet is could account for over 10 billion payment transactions a year, representing an exchange of as much as $400 billion, although such numbers are clearly optimistic. In this context, security relates to three general areas:

1. Secure file/information transfers
2. Secure transactions
3. Secure enterprise networks, when used to support web commerce

This chapter presents a discussion on various tools and technologies for secure EPSs, including digital signatures, authentications, public key cryptography, certificates, certificate authorities, and the secure sockets layer (SSL), secure hypertext transfer protocol (HTTP) digital signatures, and public and private key secure electronic transmissions (SET).

Observers and proponents articulate the thesis that the security issue must be addressed quickly in order for companies to start investing in electronic commerce, there are indications that merchants are taking a wait-and-see attitude in electronic commerce on the internet until either there is a dominant standard or there is universal software that will support a variety of encryption and transaction schemes. The market is looking for a comprehensive solution that merchants and banks can use to support all functions. Computer security has several fundamental goals:

a. ***Privacy*****:** keep private documents private, using encryption, passwords, and **access-control systems.**

b. ***Integrity*****:** data and applications should be safe from modification without the owner's consent.

c. ***Authentication*****:** ensure that the people using the computer are the authorized users of that system.

d. ***Availability*****:** the end system and data should be available when needed by the authorized user.

3.2 SECURE TRANSPORT PROTOCOL AND TRANSACTION

In order to ensure the integrity and security of each electronic transaction, the FSTC's e-check technology and other EPSs utilize some or all of the following security measures. It should be noted that a number of these measures are used in other applications as well. For example, authentication is used for other security purposes, such as when logging onto a network, digital signatures is used for formal contracts, and so forth. In this chapter I explain the following seven measures and technologies that are directly related to EPSs:

- Digital signatures
- Authentication
- Public key cryptography
- Certificate authorities
- SSL
- Secure HTTP digital signatures
- Public and private key secure electronic transmission (SET)

Secure Hypertext Transfer Protocol (S-HTTP)

S-HTTP is a secure extension of HTTP developed by the CommerceNet Consortium. S-HTTP offers security techniques and encryption with RSA methods, along with other payment protocols. For secure transport, S-HTTP supports end-to-end secure transactions by incorporating cryptographic enhancements to be used for data transfer at the application level. This is in contrast to existing HTTP authorization mechanisms, which required the client to attempt access and be denied before the security mechanism is employed. S-HTTP incorporates public-key cryptography from RSA Data Security in addition to supporting traditional shared secret password and Kerberos-based security systems. The RSA Data Security ciphers used by S-HTTP utilize two keys; files encrypted by one can only be decrypted by application of the other key. A company generates a pair of these keys, publishes one and retains the other. When another company wishes to send a file to the first company, it encrypts the file with the published key of the intended recipient. The recipient decrypts it with the private key.

S-HTTP allows internet users to access a merchant's website and supply their credit card numbers to their web browsers; S-HTTP encrypts the card numbers, and the encrypted files are then sent to the merchant. Then, S-HTTP decrypts the files and relays back to the user's browsers to authenticate the shopper's digital signatures. The transaction proceeds as soon as the signatures are verified.

The term digital signature generally applies to the technique of appending a string of characters to an electronic message that serves to identify the sender or the originator of a message (the authentication function). In other words, digital signature includes any type of electronic message encrypted with a private key that is able to identify the origin of the message. Some digital signature techniques also serve to provide a check against any alteration of the text of the message after the digital signature was appended (the seal function). Early concerns were focused on the problem of the recipient being able to ensure that the message received was genuine and unaltered. However, there was reason to consider the potential legal problem of proving at a later time that the intended recipient did not himself alter the message to use as bogus evidence. This later capability (the integrity function) is of great interest in cases where legal documents are created using such digital signatures. Finally, privacy and confidentiality are of significant concerns in many instances where the sender wishes to keep the contents of the message private from all but the intended recipient.

Secure Socket Layer (SSL)

SSL is a layer that exists between the raw TCP/IP protocol and the application layer. While the standard TCP/IP protocol simply sends an anonymous error-free stream of information between two computers (or between two processes running on the same computer), SSL adds numerous features to that stream, including:

- Authentication and non-repudiation of the server, using digital signatures

- Authentication and non-repudiation of the client, using digital signatures
- Data confidentiality through the use of encryption
- Data integrity through the use of message authentication codes

Cryptography is a fast-moving field, and cryptographic protocols don't work unless both parties to the communication use the same algorithms. For that reason, SSL is an extensible and adaptive protocol. When one program using SSL attempts to contact another, the two programs electronically compare notes, determining the strongest cryptographic protocol that they share in common. This exchange is called the SSL Hello. SSL was designed for use worldwide, but it was developed in the United States and is included as part of programs that are sold by U.S. corporations for use overseas. For this reason, SSL contains many features designed to conform with the U.S. government's restrictive policies on the export of cryptographic systems

The SSL protocol introduced by Netscape Corporation provides a relatively secure method to encrypt data that are transmitted over a public network such as the Internet. SSL provides security for all Web transactions, including file transfer protocol (FTP), HTTP, and Telnet-based transactions. It provides an electronic wrapping around the transactions that go through the Internet. All the major web server vendors, including Microsoft and Netscape, support SSL. The open and nonproprietary nature of SSL is what makes it the preferred choice for TCP/IP application developers for securing sensitive data. Similar to any other security measure, SSL is not perfect. For example, the protocol is vulnerable to attacks on the SSL server authentication. Despite its vulnerabilities, when properly implemented, SSL can be a powerful tool for securing Web-sensitive data. SSL offers comprehensive security by offering authentication and encryption at the client and server sides.

It operates between the transport and the application layers in the network stack and uses both public and private key cryptography. Transport and application layers are two of the layers in the network stack in the open system interconnection (OSI) reference model. OSI is a seven-layer architecture defining the method of transmission of data from one computer to another through a network. It is used to describe the flow of data between the physical connection to the network and the end user application. It standardizes levels of service and types of interaction for computers exchanging information through a network. Each layer in the architecture performs a specific task. (1) The **application** layer is application dependent and performs different tasks in different applications. (2) The **presentation** layer formats the message. (3) The **session** layer is responsible for establishing a dialogue between computers. (4) The **transport** layer is responsible for generating the receiver's address and ensuring the integrity of the messages sent. (5) The **network** layer is responsible for message routing. (6) The **data link** layer oversees the establishment and control of communications link. (7) The **physical** layer specifies the electrical connections between the computer and the transmission medium. Both public and private key cryptography techniques have been around for a long time. Authentication begins when a client requests a connection to an SSL server. The client sends its public key to the server, which in turn generates a random message and sends it back to the client. Next, the client uses its private key to encrypt the message from the server and sends it back. All the server has to do at this point is decrypt the message using the public key and compare it to the original message sent to the client. If the messages match, then the server knows that it is from the client communicating with the intended client. To implement SSL in a web server, the following steps are followed:

1. Generate a key pair on the server.
2. Request a certificate from a certification authority.
3. Install the certificate.
4. Activate SSL on a security folder or directory.

It is not a good idea to activate SSL on all the directories because the encryption overhead created by SSL decreases system performance. One important drawback of SSL is that certificates and keys that originate from a computer can be stolen over a network or by other electronic means. One possible solution to this weakness is to use hardware tokens instead. Hardware tokens improve security tremendously because these tokens are more difficult to steal and they can be customized to individual users. This can be done in a number of ways, including using biometric techniques, such as fingerprint or retinal scan matching.

- **SSL Versions**

The SSL protocol was designed by Netscape for use with the Netscape Navigator. Version 1.0 of the protocol was used inside Netscape. Version 2.0 of the protocol shipped with Netscape Navigator Versions 1 and 2. After SSL 2.0 was published, Microsoft created a similar secure link protocol called PCT which overcame some of SSL 2.0's shortcomings. The advances of PCT were echoed in SSL 3.0. The SSL 3.0 protocol is being used as the basis for the Transport Layer Security (TLS) protocol being developed by the Internet Engineering Task Force.

- **Advantages**

- *Authentication:* Allows Web-enabled browsers and servers to authenticate each other.
- *Limits access:* Allows controlled access to servers, directories, files, and services.
- *Protects data:* Ensures that exchanged data cannot be corrupted without detection.
- *Shares information:* Allows information to be shared by browsers and servers while remaining out of reach to third parties.

- **Disadvantages**

- *Uses simple encryption:* This might increase the chances of being hacked by computer criminals.
- *Only point-to-point transactions:* SSL handles only point-to-point interaction. Credit card transactions involve at least three parties: the consumer, the merchant, and the card issuer. This limits its all-purpose applications.
- *Customer risk:* Customers run the risk that a merchant may expose their credit card numbers on its server; in turn, this increases the chances of credit card frauds.
- *Merchant's risk:* Merchants run the risk that a consumer's card number is fraudulent or that the credit card won't be approved.
- *Additional overhead:* The overhead of encryption and decryption means that secure HTTP (SHTTP) is slower than HTTP.

Alternatives

The good news is that the SSL and S-HTTP standards are converging into a single standard which will accommodate both protocols making the use of encrypted credit card transaction even easier to implement. A related capability is a certification authority to authenticate the public keys on which the RSA system relies. The goal is to assure users that a public key that seems to be associated with a company actually is and is not a spurious key. The authority requires a applicants to prove their identity. Those passing the tests are issued a certificate in which the applicant's public key is encrypted by the authority's private key. The CommerceNet certification authority perform due diligence on applicants, including reviews of articles of incorporation and credit reports.

An alternative to internet online credit card transactions is the use of digital cash (e-cash). Digital cash is a system by which online shopper's trade real dollars for internet credits to pay for goods and services. With digital cash, users transfer money from their traditional bank accounts to their digital cash accounts, converting real-world currency into digital coins that they store on their hard drive. When a user spends those coins on internet goods or services, the transaction is credited to the merchant's account by the clearing bank and the proceeds are deposited into the merchant's bank account. Digital coins can less easily be stolen or faked, which reduces the risk for both the buyer and seller.

3.1 & 3.2 Check your Progress

1. Fill in the blanks.

a. S-HTTP is a …… of HTTP developed by the Commerce Net Consortium.

b. SSL is a layer that exists between the raw …….. protocol and the application layer.

2. Answer the following in two- three sentences.

a. What is S-HTTP?

……

……

b. List the advantages of SSL

……

……

c. What are the disadvantages of SSL?

……

……

3.3 SECURE TRANSACTIONS

The protocols previously discussed support secure transitions, as well as more advanced secure transport capabilities. The secure transaction protocols discussed here are more narrowly focused.

For secure payments, internet hardware/software vendors have made a variety of announcements in the past couple of years related to the support for the most popular security payment protocols. Three methods have evolved in the recent past. Netscape Communications Corp and Microsoft Corp have promoted their respective payment protocols and installed them in World Word Web browsers and servers.

1. SEPP has been championed by MasterCard and Netscape and by other supporters; the American National Standards Institute (ANSI) is fast-tracking SEPP as a standard for the industry.
2. STT was developed jointly by Visa and Microsoft as a method to secure bankcard transations over open networks. STT uses cryptography to secure confidential information transfer, ensure payment integrity, and authenticate both merchants and cardholders. Confidentiality of information is ensured by the use of message encryption; payment information integrity is ensured by the use of digital signatures; cardholder account authentication is ensured by the use of digital signatures and cardholder credentials; merchant authentication is ensured by the use of digital signature and merchant credentials; and interoperability is ensured by the use of specific protocols and message formats.
3. At this juncture, it appears that SET will become the industry de facto standard. SET has emerged as a convergence of the previous standards and has a lot in common with SEPP. SET is expected to be rapidly incorporated into industrial strength “merchantware” already available from Netscape, Microsoft, IBM, and other software sellers.

NetBill is an electronic commerce model designed at Carnegie Mellon University’s Information Network Institute with the goal to reduce the cost of processing a transaction enough to accommodate purchase prices on the order of 10 cents per transaction. NetBill’s design is based on a central server that acts as an exchange point between vendors and customers. This approach is attractive because there is no prearranged relationship necessary between vendors and customers in order for business transaction to take place. Advantages of the NetBill business model are that it simplifies authentication, single statement billing, and access to account information. The disadvantages concern network and processing bottlenecks and privacy concerns.

NetBill's transaction framework uses a distributed transaction protocol with a centralized billing server to provide a funds transfer mechanism. Clients and service providers are authenticated to the billing server and to each other using Kerberos authentication services and private-key cryptography. After customers and vendors agree on a transaction and price, the billing server has an encrypted session with the customer. Once a transaction is successfully completed, goods are sent to the customer. The centralized billing system is cognizant of all transaction information, for example, participant's identity, account number, item purchased, amounts, and tax status, because of this, the transaction is not anonymous and is considered a fund-transfer system and not a digital cash system.

The following is a partial list of some of the companies that support secure transactions:

BizNet Technologies	http://rainer.bnt.com/vvv.html
CommerceNet	http://www.commerce.net
CyberCash	http://www.cybercash.com
Digicash	http://www.digicash.com

3.4 SECURE ELECTRONIC PAYMENT PROTOCOL (SEPP)

SEPP (Secure Electronic Payments Protocol) is an open specification for secure bank card transactions over the Internet that was jointly developed by IBM, Netscape, GTE, Cybercash and MasterCard. Building on the iKP protocol, SEPP messages are transmitted as Multi-purpose Internet Mail Extensions (MIME) attachments. A draft version was released for comment in November 1995. SEPP provides an embodiment of the iKP protocol intended for HTTP transactions and adapted to bank card payments; SEPP messages are transmitted with MIME and are based on common ASN.1 syntax including X.509 version 3 certificates and PKCS #7 "signed data". SEPP and STT were being merged into a joint Visa-MasterCard protocol called SET, Secure Electronic Transactions, as of this writing.

Several basic transaction messages are required in a SEPP-based environment; when variations to the canonical flow occur; additional data will be required in the supplementary messages (see the following list).

Messages for SEPP-compliant processing of payment transactions

- Purchase Order Request
- Authorization Request
- Authorization Response
- Purchase Order Inquiry
- Purchase Order Inquiry Response

Additional messages for on-line customer

- Initiate
- Invoice
- Purchase Order Response (with Purchase Order Status)

Message for offline (i.e., email) transactions or transactions sent to merchant not on-line with the acquirer

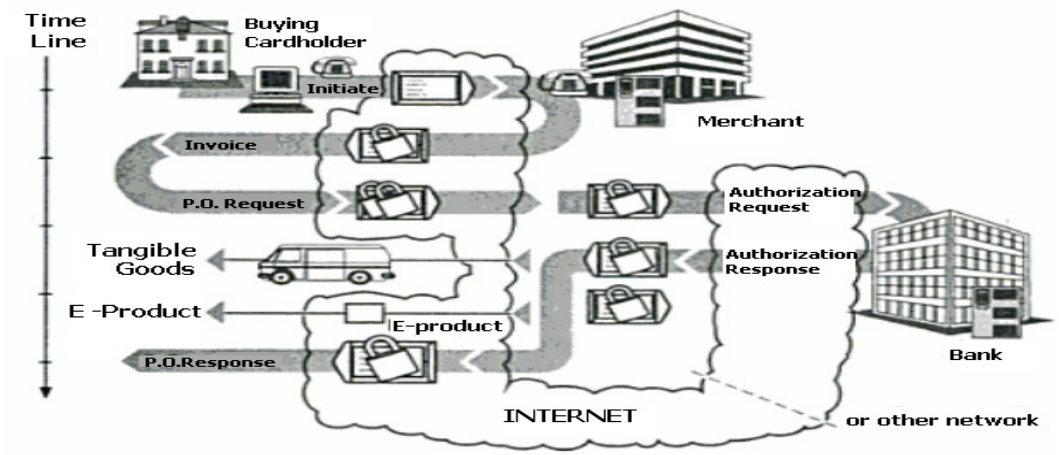
- Purchase Order Response (acknowledgement without authorization)

In simplified form, the transaction occurs as follows (see Figure 3.1 which shows some but not all of the transactions). The buying cardholder begins the transaction by sending the merchant an *Initiate* message. The merchant responds with an *Invoice* message containing information used by the buying cardholder to validate the goods and service and the transaction information. The buying cardholder then prepares a *Purchase Order Request* which contains goods and service order validation information and the buying cardholder's payment instructions which are encrypted in a manner so as to only be decrypted by the acquirer. The merchant receives the Purchase Order Request, formats an *Authorization Request*, and sends it to the acquirer. The Authorization Request contains the confidential card holder payment instructions. The acquirer processes the Authorization Request. The acquirer then responds to the merchant with an *Authorization Response*. The merchant will respond to the buying cardholder with a *Purchase Order Response* if a Purchase Order Response message was not previously sent. At a later time, the buying cardholder may initiate a *Purchase Order Inquiry* (this transaction is used to request order status from the merchant) to which the merchant will respond with a *Purchase Order Inquiry Response.*

The process of shopping is merchant-specific. The process of transaction capture, clearing, and settlement of the transaction is defined by the relationship between the merchant and the acquirer. In certain scenarios (e.g., shopping via a browser/electronic mall), the buying cardholder may have already specified the goods and services before sending a Purchase Order Request message. In other scenarios (e.g., merchandise selection from paper or CD-ROM-based catalogs), the order may be placed with the payment instructions in the Purchase Order Request message.

In an interactive environment, SEPP activities start when the buying cardholder sends a message to the merchant7 indicating an initiation of a SEPP payment session. This message is referred to as an Initiate message; it is used to request that the merchant prepare an invoice as the first step in the payment process. The merchant responds to the Initiate message with an Invoice message which contains the amount of the transaction, merchant identification information, and data used to validate subsequent transactions in the sequence.

Figure 3.1 Simplified SEPP process



The next transaction is initiated by the buying cardholder. This transaction is the Purchase Order Request. This message contains the payment instructions of the buying cardholder. This information us protected in such a manner as to provide a high level of confidentiality and integrity. The payment instructions are encrypted so that they can only be read by the acquirer.

The merchant sends an Authorization Request to the acquirer. The acquirer performs the following tasks:

- Authenticates the merchant
- Verifies the acquirer/merchant relationship
- Decrypts the payment instructions from the buying cardholder
- Validates that the buying cardholder certificate matches the account number used in the purchase
- Validates consistency between merchant's authorization request and the cardholder's payment instruction data
- Formats a standard authorization request to the issuer and receives the response
- Responds to the merchant with a validated authorization request response

The merchant responds to the buying cardholder with a Purchase Order Response indicating that either the merchant has received the Purchase Order Request message and the Authorization Request will be processed later or the Authorization Response has been processed by the acquirer.

The buying cardholder can request a status of the purchase order by using a Purchase Order Inquiry message. The merchant then responds with a Purchase Order Inquiry Response message. In the scenario supporting e-mail, the Purchase Order Request from the buying cardholder will be the first message and the Purchase Order Response from the merchant will be sent back to the buying cardholder via e-mail.

SEPP Architecture

In SEPP, the buying cardholder is represented by a cardholder workstation which, in the initial implementation, can be based on a World Wide Web browser. This

provides the buying cardholders with the flexibility to shop and conduct negotiations with the merchant system offering items for sale (e.g., Web server). The workstation may support all three stages of the electronic commerce process. Two designs of the cardholder workstations are supported. Integrated electronic commerce workstations include WWW browsers that have been designed to support electronic payments in an integrated fashion. As an alternative design, "bolt-on" payment software may be provided alongside an independent browser to implement the payment process. The protocols have been designed to ensure that such independent software may be invoked from the browsers at the appropriate times by particular data elements in the protocol exchange. Offline operation using e-mail or other non-interactive payment transactions are also supported by the protocol. Functions added to traditional WWW browsers to support electronic payments include encryption and decryption of payment data, certificate management and authentication, and support for electronic payment protocols.

To obtain a certificate, the buying cardholder's PC software interfaces with the certificate request server in the certificate management system. The certificate management system generates the certificates needed to identify the buying cardholder. The interface to the certificate request server is based on HTTP interactions; the certificate request server includes a WWW server to which the buying cardholder interfaces.

The buying cardholder's second and primary interface is with the merchant system. This interface supports the buying cardholder's segment of the payment protocol, which enables the buying cardholder to initiate payment, perform inquiries, and receive order acknowledgment and status. The buying cardholder also has an indirect interface to the acquirer gateway through the merchant system. This interface supports encrypted data sent to the merchant that is only capable of being decrypted by the merchant's acquirer. This enables the acquirer to mediate interactions between the buying cardholder and merchant, and by so doing, provide security services to the buying cardholder. This ensures that the buying cardholder is dealing with a valid merchant.

The merchant computer system is based on a Web server provides a convenient interface with the buying cardholder for the support of the electronic payments. In addition, the merchant interfaces with the acquirer gateway in the acquirer bank using the payment protocol to receive authorization and capture services for electronic payment transactions. The merchant also interfaces with the merchant registration authority in the acquirer bank. This is the interface through which a merchant requests and receives its public certificates to support the electronic commerce security functions. This interface may be to a computerized server; alternatively, this interface and service may be provided by manual means. The merchant needs to support SEPP protocols for the capture and authorization of electronic commerce transactions initiated by the buying cardholder. In addition, it needs to support security services (integrity, authentication, certificate management), as well as support the payment and communications functions themselves. A merchant may operate in a fully real-time electronic commerce mode, or it may perform authorization using SEPP protocols and rely on existing mechanisms for the capture process.

The SEPP acquirer consists of a traditional acquirer with the addition of an acquirer gateway and a merchant registration authority. The *acquirer gateway* is a system that provides electronic commerce services to the merchants in support of the acquirer and interfaces with the acquirer to support the authorization and capture of transactions. The acquirer gateway interfaces with the merchant system to support authorization and capture services for the merchant. The BankNet interface is basically the existing interface supporting acquirers today. The acquirer receives certificates from the offline certificate authority. The *merchant registration authority* is a workstation located at the acquirer bank that enables the acquirer to securely receive, validate, and forward merchant certificate requests to the certificate management system and to receive back certificates. The merchant registration authority has a cryptographic module for performing signature(s). It also manages certificate revocation lists for the bank's merchants.

The certificate management system consists of computer systems providing certificate authorities to support trusted, reliable, certificate-granting service to cardholders, merchants, and acquirers. This system also includes certificate request

servers to issue cardholder certificates through the WWW and interfaces with the acquirer's merchant registration authority to provide merchant certificates. The certificate management system also interfaces through BankNet to issuer banks to obtain authorization for the generation of certificates for cardholders.

BankNet is the existing financial network through which acquirers obtain authorization for payment from issuers. It is also used in SEPP for cardholder certificate authorization between the certificate request server and the issuers. BankNet provides interfaces based on ISO 8583- formatted messages.

3.5 SECURE ELECTRONIC TRANSACTION (SET)

Secure Electronic Transactions (SET) is an open protocol which has the potential to emerge as a dominant force in the securing of electronic transactions. Jointly developed by Visa and MasterCard, in conjunction with leading computer vendors such as IBM, SET is an open standard for protecting the privacy, and ensuring the authenticity, of electronic transactions. This is critical to the success of electronic commerce over the Internet; without privacy, consumer protection cannot be guaranteed, and without authentication, neither the merchant nor the consumer can be sure that valid transactions are being made. In other words, SET is a system for ensuring the security of financial transactions on the Internet. With SET, a user is given an electronic wallet (digital certificate) and a transaction is conducted and verified using a combination of digital certificates and digital signatures among the purchaser, a merchant, and the purchaser's bank in a way that ensures privacy and confidentiality. SET makes use of Netscape's Secure Sockets Layer (SSL), Microsoft's Secure Transaction Technology (STT), and Terisa System's Secure Hypertext Transfer Protocol (S-HTTP). SET uses some but not all aspects of a public key infrastructure (PKI).

The SET protocol reproduces the current structure of the credit card processing system and replaces every phone call or transaction slip of paper with an electronic version. This can generate a large number of data packets. The SET protocol offers packets of data for all these transactions, and each transaction is signed with a digital signature. This makes SET the largest consumer of certificates, and it makes banks by default one of the major distributors of certificates. IBM and GTE have announced plans to help banks offer certificates to their customers; these promises to be a significant market for developers of these large databases. One of the most active debates in the SET community is over who will pay for the SET certificate-revocation list. Certificate revocation is an essential part of the certificate process. There are several reasons why a certificate must be revoked before it expires. For example, a user might change organizations or lose his or her key pair, or an e-commerce site using SSL may discontinue its operations. In all these cases, the certificate needs to be revoked before it expires so that it cannot be used intentionally or unintentionally.

The SET protocol forces a transaction processor to check the lists regularly to catch transactions that might be generated by a lost or stolen certificate. In order to simplify the process of keeping the lists current and synchronized, the protocol defines a fingerprint to be a hash of the latest revocation list. A hash function accepts a variable-size message as input and generates a short fixed-sized tag as output. The transaction processors can compare fingerprints to ensure that their copy of the list matches the latest master list.

The following steps describe a typical flow of SET protocol messages through a SET transaction (see Figure 3.2).

1. The certificate authority issues certificates to cardholder.
2. The customer (cardholder) initiates a purchase.
3. The merchant requests authorization.
4. The cardholder authorization is provided.
5. The merchant ships products.

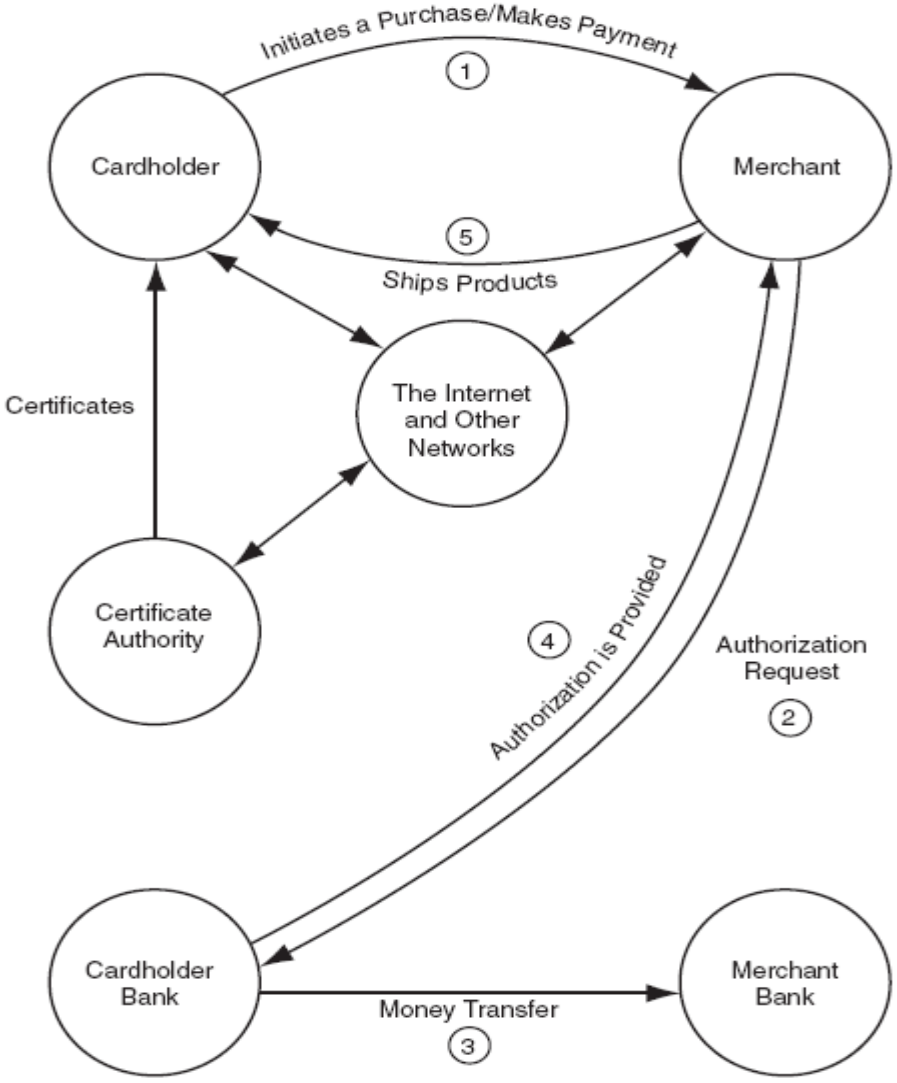


Figure 3.2 A secure electronic transmission (SET) transaction.

The confidentiality of messages in the SET payment environment is accomplished through encryption of the payment information using a combination of public key and private key algorithms. In general, public and private key cryptographic algorithms (the process of transforming readable text into cipher text and back again) are used together to encrypt the actual message contents with a short private key, which is distributed securely via the public–private key pair. The most important property of SET is that the credit card number is not revealed to the vendor. However, the SET protocol, despite strong support from Visa and MasterCard, has not emerged as a leading standard. The two major reasons for lack of widespread acceptance are (1) the complexity of SET and (2) the need for the added security that SET provides. However, this might change in the future as encryption technology becomes more commonly utilized in the e-business world.

Here's how SET works:

Assume that a customer has a SET-enabled browser such as Netscape or Microsoft's Internet Explorer and that the transaction provider (bank, store, etc.) has a SET-enabled server.

1. The customer opens a MasterCard or Visa bank account. Any issuer of a credit card is some kind of bank.
2. The customer receives a digital certificate. This electronic file functions as a credit card for online purchases or other transactions. It includes a public key with an expiration date. It has been through a digital switch to the bank to ensure its validity.
3. Third-party merchants also receive certificates from the bank. These certificates include the merchant's public key and the bank's public key.
4. The customer places an order over a Web page, by phone, or some other means.

5. The customer's browser receives and confirms from the merchant's certificate that the merchant is valid.
6. The browser sends the order information. This message is encrypted with the merchant's public key, the payment information, which is encrypted with the bank's public key (which can't be read by the merchant), and information that ensures the payment can only be used with this particular order.
7. The merchant verifies the customer by checking the digital signature on the customer's certificate. This may be done by referring the certificate to the bank or to a third-party verifier.
8. The merchant sends the order message along to the bank. This includes the bank's public key, the customer's payment information (which the merchant can't decode), and the merchant's certificate.
9. The bank verifies the merchant and the message. The bank uses the digital signature on the certificate with the message and verifies the payment part of the message.

The bank digitally signs and sends authorization to the merchant, who can then fill the order.

The SET protocol relies on two different encryption mechanisms, as well as an authentication mechanism. SET uses symmetric encryption, in the form of the aging Data Encryption Standard (DES), as well as asymmetric, or public-key, encryption to transmit session keys for DES transactions (IBM, 1998). Rather than offer the security and protection afforded by public-key cryptography, SET simply uses session keys (56 bits) which are transmitted asymmetrically – the remainder of the transaction uses symmetric encryption in the form of DES. This has disturbing connotations for a "secure" electronic transaction protocol – because public key cryptography is only used only to encrypt DES keys and for authentication, and not for the main body of the transaction. The computational cost of asymmetric encryption is cited as reason for using weak 56 bit DES (IBM, 1998), however other reasons such as export/import restrictions, and the perceived need by law enforcement and government agencies to access the plain-text of encrypted SET messages may also play a role.

Overview of symmetric and asymmetric cryptography

Modern cryptography uses encryption keys, which can encode (lock) and decode (unlock) messages when an encryption algorithm is used. Symmetric encryption works by using a single key, which must be known by all parties wishing to unlock the message.

If we apply a specific key to a message, using a good encryption algorithm, then it will be unreadable by unauthorized parties. If we then apply the same key to the encrypted message, then the message will be restored to its original form. However, this presents a problem, because we must find a secure means of transmitting the key to all parties.

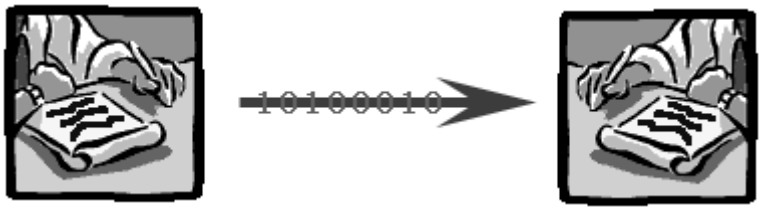


Figure 3.3 Symmetric encryption with a single key

Asymmetric encryption, also known as public-key encryption, frees us from this limitation. Asymmetric algorithms use two keys – a public and a private key. These keys are completely independent – a private key cannot be easily deduced from a public one. When we sign a message using someone's public key, only the holder of the private key can read it. We can place our public key out in the open, and rest assured that only the private key holder can read messages encrypted for him or her.

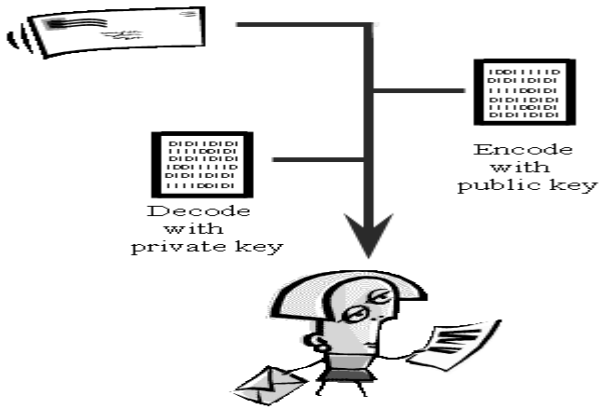


Figure 3.4 Asymmetric encryption with public and private key

In SET protocol, two different encryption algorithms are used are DES and RSA. The DES algorithm has been used since the 1970's. It is believed by some that the National Security Agency (NSA) of America played "an invisible hand in the development of the algorithm" (Schneier, 1996), and that they were responsible for reducing its key size from the original 128-bits to 56. DES quickly became a federal standard in 1976, and has been used ever since.

In the SET protocol, a DES 56-bit key is used to encrypt transactions. This level of encryption, using DES, can be easily cracked using modern hardware. In 1993, a brute-force DES cracking machine was designed by Michael Wiener – one which was massively parallel. For less than a million dollars (well within the budget of many large companies), a 56-bit DES key could be cracked in average time of 3.5 hours. For a billion dollars, which might be considered small change for a military or security organization such as the NSA or a foreign power, a parallel machine can be constructed that cracks 56-bit DES in a second (Schneier, 1996). Clearly, this is of great concern, since DES encrypts the majority of a SET transaction. As the power of computers grows, and the cost diminishes, such code-crackers may become more and more common.

One may wonder why such crippled cryptography would be used in a "secure" transaction protocol. One possible reason may be that the organizations involved recognize the desire by government organizations (both foreign and domestic to the US) to observe and monitor financial transactions conducted over the Internet. "Governments tend to look favorably upon SET based cryptography", and the prospect that any government with enough resources to build a code cracker could have access to people's financial transactions is disturbing. While many people believe that it is legitimate for a government to observe the financial transactions of its citizens, it is unthinkable that a "secure" protocol would allow those same transactions to be observed by foreign, and possibly hostile, governments.

Transaction Authenticity

Authentication is an important issue for users of electronic commerce. Consumers must have faith in the authenticity of the merchant, and merchants must have faith in the authenticity of the consumer. Without authentication, any individual could pose as a merchant, and defame a merchant's good name by failing to deliver goods and billing up credit card bills. Without authentication, any individual could pose as a consumer, ordering costly goods to an abandoned house or apartment, and defrauding the merchant. Without authentication, an individual could pose as a willing buyer, accept the goods, and then repudiate the transaction. Authentication is critical to achieving trust in electronic commerce.

Authentication is achieved through the use of digital signatures. Using a hashing algorithm, SET can sign a transaction using the sender's private key. This produces a small message digest, which is a series of values that "sign" a message. By comparing the transaction message and the message digest, along with the sender's public key, the authenticity of the transaction can be verified. Digital signatures are aimed at achieving the same level of trust as a written signature has in

real life. This helps achieve non-repudiation, as the consumer cannot later establish that the message wasn't sent using his private key[1].

Importance of secure transactions

Secure electronic transactions will be an important part of electronic commerce in the future. Without such security, the interests of the merchant, the consumer, and the credit or economic institution cannot be served. Privacy of transactions, and authentication of all parties, is important for achieving the level of trust that will allow such transactions to flourish. However, it is important that the encryption algorithms and key-sizes used will be robust enough to prevent observation by hostile entities (either criminal or foreign powers). The ideal of the secure electronic transactions protocol (SET) is important for the success of electronic commerce. However, it remains to be seen whether the protocol will be widely used because of the weakness of the encryption that it uses.

Some of the **advantages** of SET include the following:

- No opportunity for anyone to steal a credit card
- Neither a person listening in nor a merchant can use the information passed during a transaction for fraud
- Flexibility in shopping; if you have a phone you can shop.

Some of the **disadvantages** of SET include its complexity and high cost for implementation.

Authentication

Authentication is the process of verification of the authenticity of a person and/or a transaction. There are many tools available to confirm the authenticity of a user; for example, passwords and ID numbers are used to allow a user to log onto a particular site.

Why Authentication Matters

Like a passport or a driver's license, an SSL Certificate is issued by a trusted source, known as the Certificate Authority (CA). Many CAs simply verify the domain name and issue the certificate. VeriSign verifies the existence of your business, the ownership of your domain name, and your authority to apply for the certificate, a higher standard of authentication. VeriSign Extended Validation (EV) SSL Certificates meet the highest standard in the Internet security industry for Web site authentication as required by CA/Browser Forum. EV SSL Certificates give high-security Web browsers information to clearly display a Web site's organizational identity. The high-security Web browser's address bar turns green and reveals the name of the organization that owns the SSL Certificate and the SSL Certificate Authority that issued it. Because VeriSign is the most recognized name in online security, VeriSign SSL Certificates with Extended Validation will give Web site visitors an easy and reliable way to establish trust online.

How Authentication Works

Imagine receiving an envelope with no return address and a form asking for your bank account number. Every VeriSign SSL Certificate is created for a particular server in a specific domain for a verified business entity. When the SSL handshake occurs, the browser requires authentication information from the server. By clicking the closed padlock in the browser window or certain SSL trust marks (such as the VeriSign Secured Seal), the Web site visitor sees the authenticated organization name. In high security browsers, the authenticated organization name is prominently displayed and the address bar turns green when an Extended Validation SSL Certificate is detected. If the information does not match or the certificate has expired, the browser displays an error message or warning.

3.3, 3.4 & 3.5 Check your Progress

1. Fill in the blanks.

a. In SEPP, the buying cardholder is represented by a…….

b. …….. is an open protocol which has the potential to emerge as a dominant force in the securing of electronic transactions.

c. The confidentiality of messages in the SET payment environment is accomplished through encryption of the ……..

d. …….is the process of verification of the authenticity of a person and/or a transaction.

2. State whether following statements are true or false.

a. NetBill's transaction framework uses a distributed transaction protocol with a centralized billing server.

b. If we apply a specific key to a message, using a good encryption algorithm, then it will be easily readable to unauthorized parties.

c. Authentication is not an important issue for users of electronic commerce.

3.6 CERTIFICATES FOR AUTHENTICATION

Certificates provide a mechanism for establishing confidence in the relationship between a public key and the entity that owns the corresponding private key. A certificate can be thought of as similar to a driver's license. A driver's license is accepted by numerous organizations both public and private as a form of identification. This is mainly due to the legitimacy of the issuer, which is a government agency. Because organizations understand the process by which someone can obtain a driver's license, they can trust that the issuer verified the identity of the individual to whom the license was issued. Therefore, the driver's license can be accepted as a valid form of identification.

A digital certificate is a foolproof way of identifying both consumers and merchants. The digital certificate acts like a network version of a driver's license- it is not credit, but used in conjunction with any number of credit mechanisms, it verifies the user's identity. Digital certificates, which are issued by certificate authorities such as VeriSign and CyberTrust, include the holder's name, the name of the certificate authority, a public key for cryptographic use, and a time limit for the use of the certificate (most frequently, six months to a year).

The certificate typically includes a class, which indicates to what degree it has been verified. For example, VeriSign's digital certificates come in three classes. Class 1 is the easiest to get and includes the fewest checks on the user's background: only his or her name and e-mail address are verified. For class 2, the issuing authority checks the user's driver's license, Social Security number, and date of birth. Users applying for a class 3 certificate can expect the issuing authority to perform a credit check using a service such as Equifax, in addition to requiring the information required for class 2 certificates. See below Table.

Table 3.1 Certificate Classes

	Summary of confirmation of identity	Issuing authority private key protection	Certificate applicant and subscriber private key protection	Applications implemented or contemplated by users
Class 1	Automated unambiguous name and e-mail address search	PCA: trustworthy hardware; CA: trustworthy software or trustworthy hardware	PIN protected encryption software recommended but not required	Web browsing and certain e-mail usage
Class 2	Same as Class 1, plus automated enrollment information check and automated address check (Canada and United States only)	PCA and CA: trustworthy hardware	PIN protected encryption software required	Individual and intra- and intercompany e-mail, online subscriptions, password replacement, software validation
Class 3	Same as Class 1, plus personal presence and ID documents plus Class 2 automated ID check (Canada and United States only) for individuals; business records (or filings) for organizations	PCA and CA: trustworthy hardware	PIN protected encryption software required; hardware token recommended but not required	E-banking, corporate database access, personal banking, membership-based online services, content integrity services, e-commerce server, software validation

It is now becoming easier for vendors and for consumers to get digital certificates. VeriSign and CyberTrust, the two primary commercial issuers of digital certificates, can issue certificates via the web. Users of Microsoft Corp's Internet Explorer or Netscape Communications Corp's Navigator can take advantage of VeriSign's offer for a free six-month class 1 certificate. The U.S. Postal Service also is entering the market by offering digital certificate services as well as digital postmarks or e-mail.

One of the issues affecting the industry, however, is interoperability. The document Certification Practice Statement issued by VeriSign proposes interoperability approaches, but outcome was unknown at press time.

3.7 SECURITY ON WEB SERVERS AND ENTERPRISE NETWORKS

As discussed earlier, financial transaction security is a major concern for businesses that offer products or services over the internet. However there is also the need for security of the merchant (or other participating organization's) host. This is necessary in order to protect (1) files containing buyer's information (credit card lists, addresses, buying habits, etc) that might reside on the accessible web server, and (2) the overall information platform of the organizations (its enterprise network, the intranet, etc.).

Two general techniques are available:

1. Host-based security capabilities; these are means by which each and every computer on the system is made (more) impregnable.
2. Security watchdog systems which guard the set of internal inter-connected systems. Communication between the internal world and the external world must be funneled through these systems. These watchdog systems that deal with security within an organization's own enterprise network are called *firewalls*. A firewall allows a business to specify the level of access that will be afforded to network users. Proxies support transactions on behalf of a client in a two-step manner.

In general, both methods are required.

An internet site can set up an anonymous FTP site that allows any outside users to access files at the site (anonymous FTP is very useful to companies that wish to place documentation in the public domain; it also can be used to allow users to download software). This could be as a stand-alone system which is updated only by offline means (e.g., load a diskette) or by a physically separate port (e.g., console port); or, it could be a system outside the firewall (but still residing on the overall organization's network called a *bastion*. In either case, the host could allow access to all files on the system or to a subset of files. In any event, the access must be at the lowest level of security (i.e., with minimum privileges), otherwise a hacker might wither alter or delete files, use that system to jump off to another system, or create denial of service. This must be accomplished using host security mechanisms; the firewall

comes into play if the FTP system is located on the organization's network, for ease of updating.
These two general areas of security are discussed here. Table 3.2 depicts some strategies that can be used in the context of web commerce applications.

Host security is a discipline that goes back to the 1960s. Mainframes were perhaps endowed with more rigorous security capabilities than their successors. With even low-end PDs becoming servers, host-based security has suffered for a number of reasons ranging from corporate apathy, to lack of knowledge on the administrator's part, lack of products, and lack of machine power for running the security packages and the daemons.

The need and desire to protect a host is based on a whole range of premises, policies, and risk-avoidance reasons. Such a need should stand on its own merit. There will be financial, prestige, political, and organizational losses if some important data is compromised, lost, or improperly disseminated. These reasons should be enough to motivate organizations to develop sound security policies. This discussion focuses only on the matter of not allowing hackers to break in to a web server and compromise the financial information of the organization's web commerce customers (but as it implies, a system-wide policy is ultimately desirable).

Table 3.2 Some web commerce host security techniques

Open access to the company Web page to support e-commerce	Configure an external bastion host to function as the public access Web server (this could also support other functions, such as FTP).
Universal anonymous access to an FTP server for downloading catalogs and product information	Configure an external bastion host to function as the public access FTP server (this could also support other functions, such as Web).
Restricted access to an FTP server to allow preferred customers to download e-products, software, and patches	Configure an external bastion host to function as the FTP server (this could be the same as the preceding item but with more robust access privilege mechanisms). Or, configure an internal FTP server behind a packet filter; this allows only preferred customers access to the server; and supports full logging of all requests and files transferred.
One-time password support for one-time sales specials, electronic coupons, frequent customers, and so on	Configure an external bastion host with authentication mechanisms. Or, configure an internal proxy server running advanced authentication schemes such as Security Dynamics' SecurID card for all return-customers.

What should a company protect? The general answer is the organization's data, login access to the organization's hosts, and the availability of the organization's hosts to do productive work. Organizations must protect themselves from insider attacks, hackers, industrial spies, foreign governments, and other agencies. There are a number of reasons why hackers attempt to penetrate a system, as noted in Table 3.3. People talk about network attacks; what they mean is network-originated attacks.

Naturally, security comes at a price, including following:

- The financial resources spent in acquiring the constituent elements such as packet filters, proxy servers, log hosts, vulnerability detection tools, smart cards, and so on.
- The staff time spent configuring these tools, identifying and correcting security holes, and training the users about the new tools.
- The effort spent in routine administration and management (e.g., reconfiguration to allow/restrict new services/users, inspection log files access violations)
- The inconvenience to the users and the associated productivity costs.

However, if the advantages and potential (gain) of web commerce are to be realized, these costs have to be faced and absorbed.

Table 3.3 Possible reasons for Penetration

Denial of service	Incapacitating someone for a period of time, because they are a competitor, and frustrating the target's ability to make money
Embarrassment	Tampering with a competitor's Web page or performing other actions to embarrass competition or secure usable code
Impersonation	Theft of identity to gain something, including unauthorized access to other sites
Intellectual challenge	Trying to determine if the purported level of knowledge, intellectuality, capacity, or stature of certain individuals designing systems is real or is only self-aggrandizement
Maliciousness	Modifying someone else's data for nefarious reasons
Personal gain	Modification of information, such as altering personal credit ratings or bank account balances for personal gain
Stock manipulation	Create negative publicity about a company to bring down the stock value as part of a hostile takeover
Theft	Financial gain from the theft of credit card numbers, financial information, industrial espionage, competitors' business proposals, or technical specifications
Vandalism or revenge	Performed by disgruntled employee or ex-employee

Host-based security tools include the following:

- Monitoring and logging tools, including standard logging facilities publicly available tools such as *tcpdump* (this utility captures and dumps packets and headers of a variety of protocols), *argus* (IP-layer transaction auditing tool), *netlog* (a UNIX-specific logging utility that logs all UDP and TCP associations mode), *syslog* utility (a comprehensive logging facility that allows various applications or shell scripts to generate error messages), and so on.
- Filtering tools, such as *TCP Wrapper* which can be configured to restrict incoming requests. This utility is incorporated into the /etc/inetd.conf file so that the tcpd daemon is invoked instead of the regular service, allowing or denying particular services. It also sends a banner to the client, advertising services or displaying the IP address to verify that the address and host name actually match; it logs the results with syslog; and it transfers users to a "jail" environment.
- Enhanced versions of standard facilities, such as improved versions of FTP daemons and the *portmapper daemon*.
- Vulnerability-detection tools, such as *SATAN* (Security Administration Tool for Analyzing Networks), which is a UNIX program that checks both local and remote hosts for network vulnerabilities.

Host based security is an indispensible element of overall computer security, but it does not scale easily (for example, because of the large number of machines, heterogeneous environments with different operating systems or different releases of the same operating system, the need to manage numerous privilege disciplines, and other reasons). Nonetheless, the administrator must assume the responsibility to make all of this work.

The security concerns regarding web applications are exacerbated by the possible use of public-domain software, including Java applets. WWW servers, handle requests generally by either directly transferring static data to the clients or by running local programs such as CGI scripts to dynamically generate the results to client requests. URL requests can be of the form (among others) of HTTP, FTP, Telnet or Gopher, which cause the corresponding service to be run in the server.

Web security concerns include the following:

- Server-side security, which involves protecting hosts running the WWW servers themselves
- Client-side security, which relates to security issues involved in requesting WWW services
- Confidentiality, which aims at guaranteeing the privacy of information transmitted across the network between clients and servers

The goal of the administrator is to make sure that clients can access only those data or HTML files explicitly granted by the server and that clients can run only those local utilities or CGI scripts explicitly made available by server. As a basic security measure, clients should not be able to add new text or executables (such as CGI scripts) files; these files may well impact the operation of the server. The design

should be such that if servers are compromised, they should not be able to be used as launching platform for additional attacks.

Some basic precautions for the server are as follows:

- The httpd daemon server should be executable only by root and is to be typically invoked only at execution time.
- All files and directories in the server directory structure should be owned by root.
- The htdocs directory is openly accessible but should be modifiable only by root.
- The conf and logs directories should be totally inaccessible to anyone but root.

As related to CGI security, the following precautions (among others) should be taken when installing and configuring CGI scripts:

- Configure the server so that all CGI scripts reside in a single directory and set the attributes on this directory so that its contents are executable but not examinable.
- Do not allow users to install scripts in this directory.
- Inspect this directory regularly for newly adder scripts or scripts that have been modified recently based on the script timestamp or checksum.
- CGI scripts are typically invoked by the server after the client makes a particular selection or fills in a form and submits it. The client request or form information is transmitted to the server, who passes it to the appropriate CGI script. For security reasons, the CGI script should make no assumptions about the validity of the input or even where the input came from.
- Do not run any other network services on the server (such as FTP) which only provides additional security infraction opportunities.
- Remove all ability for remote logins such as rlogin or Telnet.
- Remove all nonessential compilers and programming tools that might be used by attackers to create or run programs on the server.
- Isolate the server from the rest of the network, possibly placing it outside of the firewall so that a compromised server does not harm the rest of the network.

On the client-side, web browsers are typically configured to invoke the appropriate viewer depending on the type of the file or applet downloaded from the server. While many browsers can already handle basic media (such as plaintext, HTML, and GIF files), they might rely on helper programs to view other files (such as PostScript files or JPEG files). This is a security liability in that it permits the execution of arbitrary commands that may be embedded in the incoming data (such commands as create file, read file, or delete file). In general, the administrator needs to educate users about the risks of downloading arbitrary files, particularly those that require users to modify their configuration files.

Enterprise Network Security

A firewall (also called a *secure internet gateway*) is a hardware device or software application that sits between your computer and the Internet and blocks all Internet traffic from reaching your computer that you have not specifically requested. What this means is that if you browse to a web site, the firewall will allow the traffic from that web site to reach your computer and therefore yourself. On the other hand, if you did not request information from that web site, and the web site sent traffic to you, it would be denied from reaching your computer because you did not specifically ask for it. This behavior can be changed if you wish.

A firewall supports communication-based security to screen out undesired communications which can cause havoc on the host. Host-based security is a critical element of overall computer security, although it does not scale easily; nonetheless, it must be employed. Ideally, an administrator uses all available tools, including host security and communication gateway security. It is like having two locks on a door: both methods should be used for increased assurance.

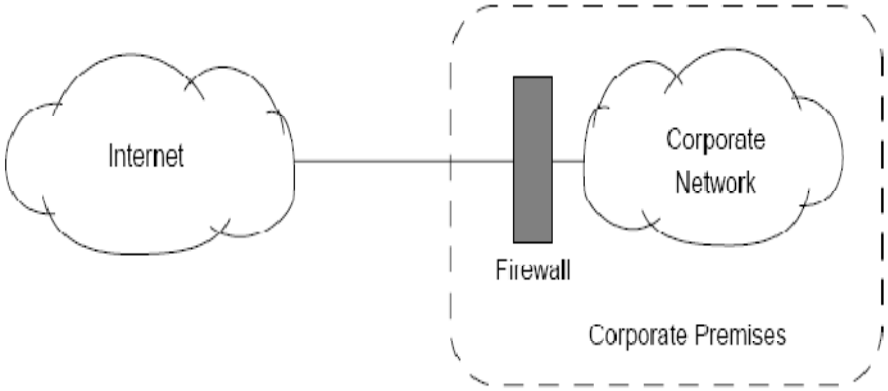


Figure 3.5 Firewall-controlled access from the internet

The firewall deployment in the enterprise network must support the following capabilities: (1) all traffic between the inside and outside must transit through the firewall; and (2) only authorized traffic based on the security policy is allowed transit. The firewall itself must be immune to penetrate.

Firewalls act as a single focus for the security policy of the organization and support advanced authentication techniques such as smartcards and one-time passwords (which can be difficult or expensive to implement on a per-host basis). In addition, they prevent the release of information such as DNS and finger information. Furthermore, they provide an identifiable location for logging alarms or trigger conditions.

Firewalls are typically configured to filter traffic based on one of two design policies:

- Permit. Unless specifically denied. This is weaker because it is impossible to be aware of all the numerous network utilities you may need to protect against. Specifically, this approach does not protect against new internet utilities.
- Deny, unless specifically permitted. This is stronger because the administrator can start off with a blank permit list and add only those functions that are explicitly required.

Packet filters

Packet filters act at the network and transport layers of the TCP/IP protocol. They filter IP protocol data units (PDUs) based on values in the IP PDU header or the UDP or TCP PDU headers. Packet filters parse the header contents of the IP PDU, apply these values against the filter rule set or access list, and determine whether to permit or deny the PDU.

Packet filters can range in complexity from simple dual-homed hosts to multi-homed screening routers that perform routing in addition to filtering. The basic packet filter is the dual-homed packet filter firewall. A router that supports scripting allows it to act as a screening router. The router may become a bottleneck; since it does not filter at the application level and hence must examine every PDU.

Packet filters can protect an entire network at a single location and they are transparent to users. However, packet filters have limitations. For example, they may be difficult to configure; they are difficult to test exhaustively; they do not inspect the application data or filter based in the user; and some protocols do not utilize fixed, predictable ports and are thus more difficult to filter properly.

Proxies and Bastions

A *proxy* is an interceptor host that acts on behalf of the real user. It filters application-level PDUs. The proxy server typically is a dual-homed device that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server. The proxy

server evaluates the request according to its filtering rules. For example, it may filter traffic by IP address or protocol. If the request is validated by the filter, the proxy provides the resource by connecting to the relevant server and requesting the service on behalf of the client. A proxy server may optionally alter the client's request or the server's response, and sometimes it may serve the request without contacting the specified server. In this case, it 'caches' responses from the remote server, and returns subsequent requests for the same content directly. Proxy servers can operate at either the application layer or the transport layer. Thus, there are two classes of proxy servers: application gateways, which operate at the application layer; and circuit-level gateways, which operate at the transport layer.

A proxy server has a large variety of potential purposes, including:

- To keep machines behind it anonymous (mainly for security).
- To speed up access to resources (using caching). Web proxies are commonly used to cache web pages from a web server.
- To apply access policy to network services or content, e.g. to block undesired sites.
- To log / audit usage, i.e. to provide company employee Internet usage reporting.
- To bypass security/ parental controls.
- To scan transmitted content for malware before delivery.
- To scan outbound content, e.g., for data leak protection.
- To circumvent regional restrictions.

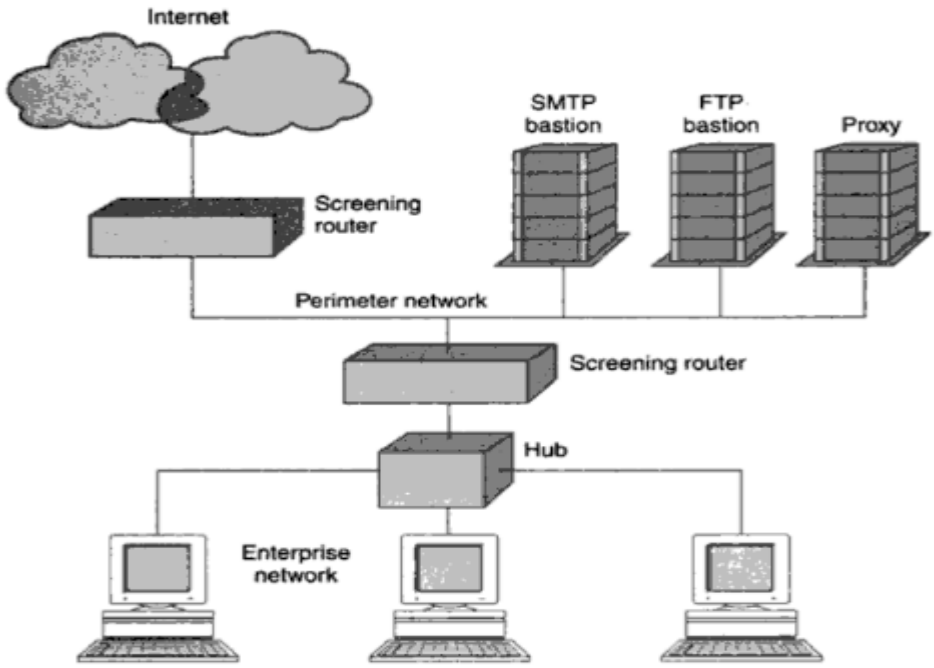


Figure 3.6 Firewall / Bastion architecture

The bastion host provides another level of protection. It is the system that is the organization's interface with the outside and the system with which external clients must connect to get access to the organization's internal servers. Since the bastion host is the most exposed system, it is typically the most fortified from a host-security point of view. Bastion hosts can be used in conjunction with a firewall in combination with packet filters, proxy servers, or both, as was seen in Fig. 3.6. Administrators should remove any services or features from the bastion host that they do not absolutely require. Because the bastion host is the most exposed host, it is the most likely to be compromised; hence, one should configure the remainder of the network to not be vulnerable if an infraction occurs at the bastion level (services that are already secure can be handled by packet filtering and need not be provided by the bastion host). A bastion does not necessarily have to be a proxy; just an application device or it could be a proxy.

3.6 & 3.7 Check your Progress

Fill in the blanks

a. ……provide a mechanism for establishing confidence in the relationship between a public key and the entity.
b. A digital certificate is a foolproof way of identifying both ……. and …….. ……
c. Firewall is also called as …….
d. …….act at the network and transport layers of the TCP/IP protocol.

3.8 SUMMARY

What does the future hold for e-commerce? I would say that once the trust is won and frauds are beaten, there will be an increasing market for e-Commerce. Shops are more and more congested, fuel cost more and more and internet connection and PC are getting cheaper and cheaper. When we put all this together one cannot avoid coming to a conclusion that there are huge possibilities for e-Commerce and it will probably increase exponentially. On the downside, some experts predict that it will be increasingly difficult for smaller companies to establish their presence. Customers are in most cases using brand information and internet search engine to find what they are looking, and there must be a hit before there is ecommerce. One the other hand if you compare for example for weekly newspaper add it is cheap advertising. And for those considering opening a virtual storefront, forthcoming technology and standards agreements will make it easier to create a site, to protect it against payment fraud, and to share information with suppliers and business partners.

A website needs total security architecture, i.e. security that exists in a number of layers — from the web server, to the applications, to the database, and to the extensions to other subsystems. Most brick-and-mortar businesses will have some kind of security program already installed, but, in all probability, it is not up to date. And if any part of the security architecture is not working as planned, then your whole security set-up is vulnerable.

Limit outside access. This is the first line of defense for any website. Some methods for accomplishing this are:

- Firewalls.
- User account security.
- Software security.
- Additional protection for sensitive data.

Protect your web server. The second line of defense is optimizing your web server so that it can resist most hacker attacks. For instance you must install antivirus software. Install a firewall. A firewall is a device that controls the flow of communication between internal networks and external networks, such as the Internet. It controls “port-level” access to a network and a website. A properly configured firewall also can act as a filter to prevent suspicious requests from ever arriving at the server or can be configured to drop any request that tries to address a server or server port that has not been specifically enabled by the policy of the firewall. More importantly, firewalls can verify that the request matches the kind of protocol (e.g., HTTP, FTP) that is expected on a particular port.

Implement monitoring and analysis solutions. The next line of defense is putting into place routine monitoring and, if your budget allows, analysis systems so that you know who and what is connecting to your systems, and interacting with your servers.

If your budget allows, retain a security expert to perform a detailed review of your web-based business internal procedures, network topology and permissions, access controls, hardware, software, and utilities that could possibly compromise your website.

Please note that even if you set up intricate levels of security, your website is never completely safe from a determined and skilled attacker. E-commerce operations are particularly hard to protect since they must be able to interact with their customers. Therefore, at the very least, build and maintain a good, state-of-the-art firewall and

encrypt sensitive data, such as credit card information. And don't forget to institute an on-going program of security monitoring, maintenance, and to perform an annual security audit.

Source : ***technet.microsoft.com(Link)***

3.9 CHECK YOUR PROGRESS - *ANSWERS*

3.1 & 3.2

1.

a) Secure extension

b) TCP/IP

2.

a) S-HTTP is a secure extension of HTTP developed by the CommerceNet Consortium. S-HTTP offers security techniques and encryption with RSA methods.

b) Authentication, Limits access, Protects data, Shares information

c) Use simple encryption, only point-to-point transactions, Customer risk, Merchants risk, Additional overhead

3.3, 3.4 & 3.5

1.

a) Cardholder workstation

b) Secure Electronic Transactions

c) Payment information

d) Authentication

2.

a) True

b) False

c) False

3.6 & 3.7

1.

a) Certificates

b) Consumers and merchants

c) Secure internet gateway

d) Packet filters

3.10 QUESTIONS FOR SELF - STUDY

1. Describe S-HTTP in brief.
2. What is SSL? Describe its advantages and disadvantages.
3. What is SEPP? Explain SEPP process and architecture.
4. What is SET? How it works?
5. Write advantages and disadvantages of SET.
6. Write short note on authentication.
7. What precautions should be taken in the case of security on web servers?
8. Explain the role of packet filters, proxies and bastions in enterprise network security.

3.11 SUGGESTED READINGS

The Complete E-Commerce Book By Janice Reynolds

NOTES

NOTES

Chapter 4

ELECTRONIC CASH & ELECTRONIC PAYMENT SCHEME

4.0 OBJECTIVES

After studying this chapter you will be able to :

- discuss internet monetary payment system.
- explain payment and purchase order process in transaction.
- discuss & describe detailed information about electronic cash.

4.1 INTRODUCTION

For many years the internet was just a place to browse for information, but with a growing number of consumers getting access to the Internet each month, businesses are beginning to accept the internet as a viable medium through which to market and sell products and services. By having a presence on the Internet with Web servers, businesses and merchants benefit by having another channel with which to reach consumers, Consumers benefit by having a convenient and immediate way of shopping and paying for merchandise Although electronic commerce in general and Web commerce in particular can be conducted utilizing traditional payment instruments, such as out-of-band (telephony 1-xxx), credit card number transfer; or SET-transferred account information, e-cash can facilitate many kinds of transactions. This chapter explores proposed payment systems, their advantages, and their disadvantages. This information is of interest to both merchants and buyers.

The major reason electronic commerce has not yet taken off to its full potential is because, until recently, there has not been a readily available, widely deployed foolproof way of preventing fraud and theft of sensitive financial information. SET technology will soon rectify this situation, its emergence and deployment, however; did not occur overnight-the technology builds on many other concepts of the pre-cursor systems. For electronic commerce to take oft; consumers and merchants must be able to identify and trust one another; prevent transmitted financial information from being tampered with, and easily complete transactions with any valid party.

Some merchants have discovered that far too many credit card numbers used by would-be buyers were canceled, stolen, over the limit, or just plain fictitious. These merchants need to find a way to reduce the number of had numbers they are receiving. This chapter focuses on internet monetary payment processes and security services necessary to support the electronic shopping. Since credit card transactions appear to be the most requested and movement means to transact on the Internet, the processes reflected in this discussion have a card-type or account- based flavor Account-based transactions may be equated to credit cards, prepaid cards, ATM cards, checking accounts, or any type of financial medium where an account must be verified before a monetary transaction occurs. Beyond the account-based transaction

is the concept of on-line electronic cash. While electronic cash also needs a form of verification, the processes vary somewhat from that of the account-based transaction. The issues and concepts surrounding electronic cash are discussed in the latter part of this chapter.

4.2 INTERNET MONETARY PAYMENT

- **Internet Monetary Payment and Security Requirements**

For consumers and merchants to be able to trust one another, prevent transmitted payment information from being tampered with, and complete transactions with any valid party, the following issues need to be addressed:

- Confidentiality of payment information
- Integrity of payment information transmitted via public networks
- Verification that an accountholder is using a legitimate account
- Verification that a merchant can accept that particular account
- Interoperability across software and network providers

Confidentiality of payment information

Payment information must be secure as it travels across the Internet. Without security, payment information could be picked up by hackers at the router, communication-line, or host level* possibly resulting in the production of counterfeit cards or fraudulent transactions. To provide security, account information and payment information will need to be encrypted. This technology has been around for decades. Cryptography protects sensitive information by encrypting it using number-theoretic algorithms parameterized on keys (bit strings). The resulting *cyphertext* can then be transmitted to a receiving party that decrypts the message using a specific key to extract the original information. There are two encryption methods used: symmetric cryptography and asymmetric cryptography

Symmetric cryptography, or more commonly called *secret-key* cryptography, uses the same key to encrypt and decrypt a message. Thus, a sender and receiver of a message must hold the same secret or key confidentially. A commonly used secret-key algorithm is the Data Encryption Standard (DES). See Fig. 4.1. *Asymmetric cryptography,* or *public-key* cryptography, uses two distinct keys: a *public* key and a *private* key. Data encrypted using the public key can only be decrypted using the corresponding private key. This allows multiple senders to encrypt information using a public key and send it securely to a receiver, who uses the private key to decrypt it. The assurance of security is dependent on the receiver protecting the private key See Fig. 4.2.

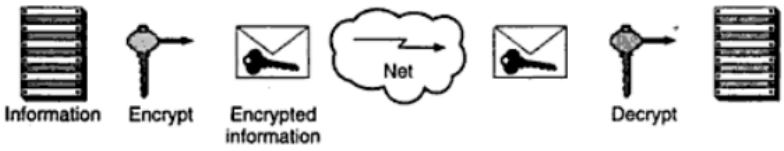


Figure 4.1 Symmetric/secret-key cryptography

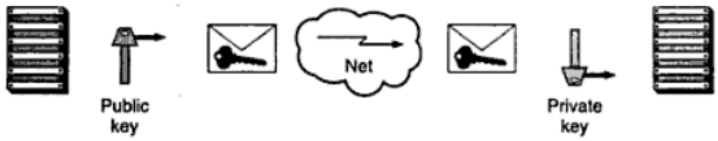


Figure 4.2 Asymmetric/public-key cryptography

For merchants to use secret-key cryptography, they would each have to administer individual secret *keys* to all their customers—and provide these keys through some secure channel. This approach is complex from an administrative perspective. The approach of creating key pair using public-key cryptography and publishing the public key is easier. This would allow customers to send secure payment information to merchants by simply downloading and using the merchant's public key. To further institute security and efficiency, public-key cryptography can be used with secret-key cryptography without creating a cumbersome process for the merchant.' To institute this process, the customer generates a random number used to encrypt payment information using DES. The corresponding DES key is then encrypted using the public key of the merchant. The DES-encrypted payment information and the encrypted DES key are then transmitted to the merchant. To decrypt the payment information, the merchant first decrypts the DES key then uses the DES key to decrypt the payment information. See Fig. 4.3.

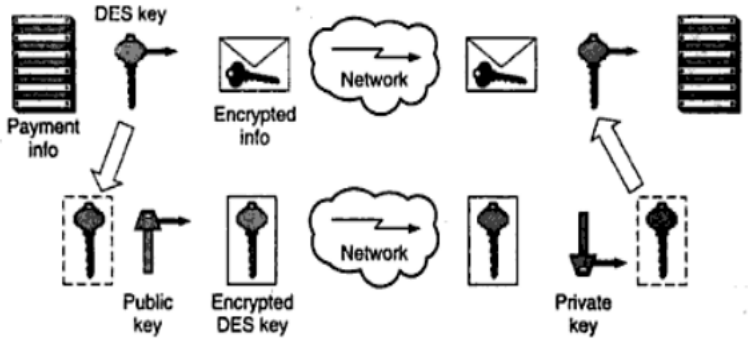


Figure 4.3 Secrete-key/public-key combination.

- **Payment information Integrity**

Payment information sent from consumers to merchants includes order information, personal data, and payment instructions. If any piece of the information is modified, the transaction may no longer be accurate. To eliminate this possible source of error or fraud, an arithmetic algorithm called *hashing,* along with the concept of digital signatures is employed. The hash algorithm generates a value that *is* unique to the payment information to be transferred. The value generated is called a *hash value* or *message digest.* A helpful *way* to view a hash algorithm is as a one-way public cipher, in that:

- It has no secret key.
- Given a message digest, there is no way to reproduce the original information.
- It is impossible to hash other data with the same value.

To ensure integrity, the message digest is transmitted with the payment information. The receiver (merchant) would then validate the message digest by recalculating it once payment information is received.

- **Account holder and merchant authentication**

Similar to the way card accounts are stolen and used today, it is possible for a person to use a stolen account and try to initiate an electronic commerce transaction. To protect against this, a process that links a valid account to a customer's digital signature needs to be established. A way to secure this link is by use of a trusted third party who could validate the public key and account of the customer. This third party could be one of many organizations, depending upon the type of account used. For example, if a credit card account were used, the third party could be one of the major credit card companies; if a checking account were used, the third party could be the Federal Clearinghouse or some other financial institution.

In any instance, the best way for a third party to validate the public key and account is by issuing the items to the customer, together under the digital signature of the third party Merchants would then decrypt the public key of the customer (using the public key of the third party) and, by definition of public-key cryptography, validate the public key and account of the customer. For the preceding to transpire, however, the following is assumed:

- The public key(s) of the third party (ies) is widely distributed.
- The public key(s) of the third party (ies) is highly trusted on face value.
- The third party(ies) issue public keys and accounts after receiving some proof of an individual's identity

So far, it has been assumed that error or fraud takes place only on the customer end of payment information transport. However, the possibility exists that a fraud agent may try and pose as a merchant for the purpose of gathering account information to be used in a criminal manner in the future. To combat this fraud, the same third-party process is used for merchants. For a merchant to be valid, the merchant's public key would need to be issued by a third party under the third party's digital signature. Customers would then decrypt the public key of the merchant using the public key of the third party. Again, for this process to occur, the assumptions previously identified would apply.

4.1 & 4.2 Check your Progress

Fill in the blanks.

a. ……..... must be secure as it travels across the Internet.

b. Asymmetric cryptography or public-key cryptography uses two distinct keys ….. and …….....

4.3 PAYMENT AND PURCHASE ORDER PROCESS

A purchase order (PO) is a commercial document issued by a buyer to a seller, indicating types, quantities, and agreed prices for products or services the seller will provide to the buyer. Sending a PO to a supplier constitutes a legal offer to buy products or services. Acceptance of a PO by a seller usually forms a one-off contract between the buyer and seller, so no contract exists until the PO is accepted. POs usually specify terms of payment, terms for liability and freight responsibility, and required delivery date.

There are several reasons why companies use PO's. PO's allow buyers to clearly and explicitly communicate their intentions to sellers, and sellers are protected in case of a buyer's refusal to pay for goods or services. POs also help a purchasing agent manage incoming orders and pending orders. Purchase orders also are an economical choice for a business because they streamline the purchasing process to a standard procedure.

Many Purchase Orders are no longer paper-based, but rather transmitted electronically over the Internet. It is common for electronic purchase orders to be used to buy goods or services online for services or physical goods of any type.

Account Holder Registration

Once the *account holder* receives the public key of the TP, the *registration* process can start. Once the *account holder's* software has a copy of the TP's public key, it encrypts the digests and transmits to the third party for further registration process (Fig. 4.4)

1. Encrypts the public key
2. Encrypts the information, message digest, and secrete key
3. The message digest after encrypting with TP public key, is forwarded for further transmission

The encrypted digest for registration is then received at the third party. Third party then decrypts it and then compares the message digests.

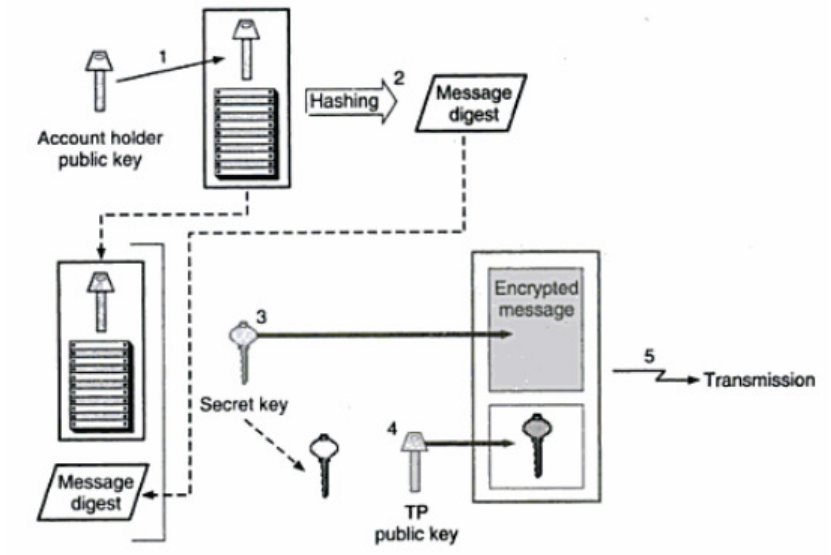


Figure 4.4 Account-holder registration

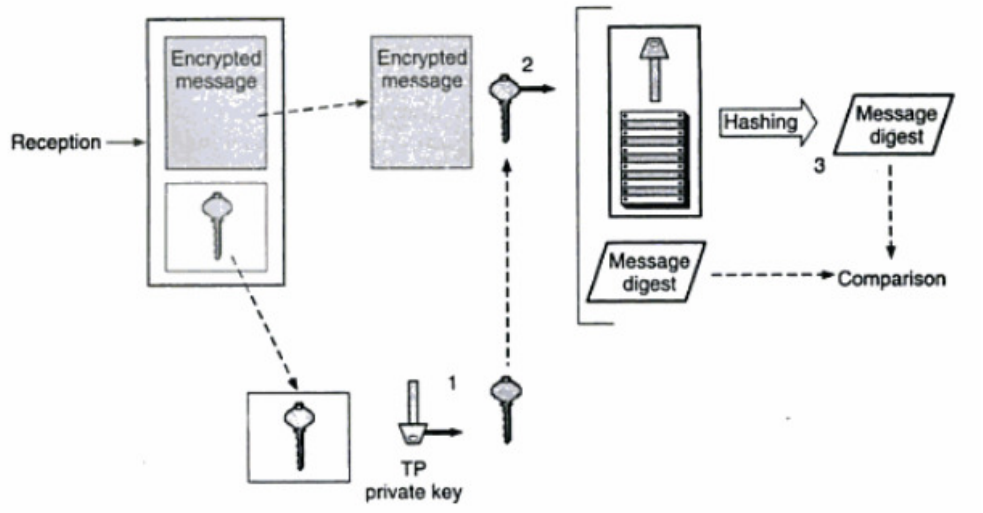


Figure 4.5 Third party receives registration

1. Decrypts the secret key
2. Decrypts the information, message digest, and account holder's public key
3. Computes and compares message digests

Assuming the message digests compute to the same value, the TP would continue the verification process using the account and personal information provided by the requesting account holder. It is assumed the TP would use its existing verification capabilities in processing personal information. If the information in the registration is verified, the TP certifies the account holder's public key and other pertinent account information by digitally signing it with the TP's private key. The certified documentation is then encrypted using a secret key, which is in turn encrypted with the account holder's public key. The entire response is then transmitted to the customer.

Upon receipt of the TP's response, the account holder's software would do the necessary decryption to obtain the certified documentation. The certified documentation* is then verified by the account holder by using the public key of the TP, thus checking the digital signature. Once validated, the certified documentation would be held by the account holder's software for future use in electronic commerce transactions.

Merchant registration

Merchants must register with TPs that correspond to particular account types that they wish to honor before transacting business with customers who share the same account types. For example, if a merchant wishes to accept Visa and MasterCard, that merchant may have to register with two TPs or find a PP that represents both. The merchant registration is similar to the account holder's registration process. Once merchant information is validated, certified documentation (CD) is transmitted to the merchant from the TP(s). The certified documentation is then stored on the merchant's computer for future use in electronic transactions.

Account holder (customer) ordering

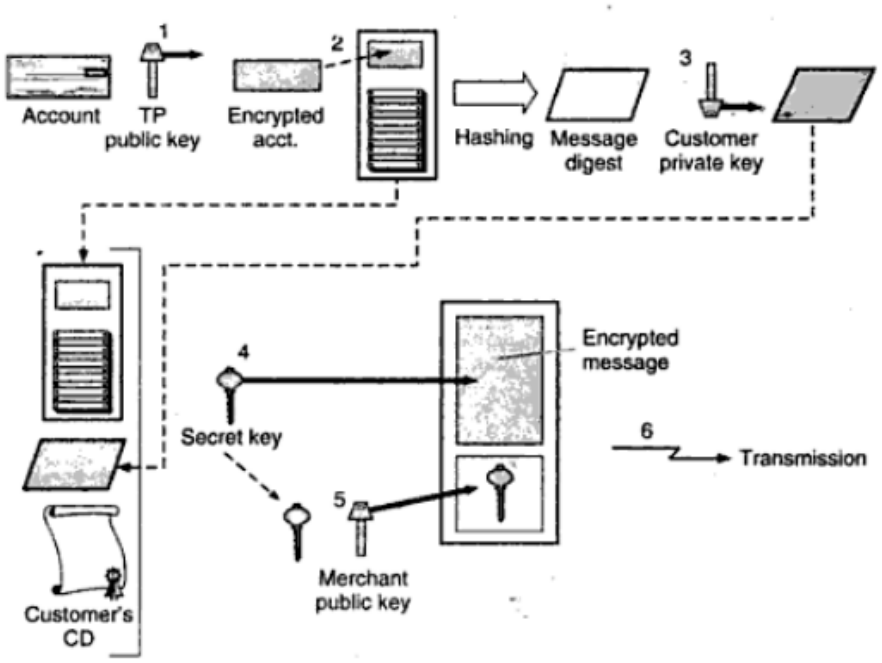
To send a message to a merchant the customer (account holder) must have a copy of the merchant's public key and a copy of the TP's public key that corresponds to the account type to be used. The order process starts when the merchant sends a copy of its CD to the customer. At some point prior to sending the CD, the merchant must request the customer to specify what type of account will be used so that the appropriate CD will be sent. After receipt of the appropriate merchant CD, the customer software verifies the CD by applying the TP's public key, thus verifying the digital signature of the VP. The software then holds the merchant's

CD to be used later in the ordering process. At this point, the customer is allowed to shop in the on-line environment provided by the merchant.

After shopping, customers fill out an order form that lists the quantity, description, and price of the goods and services they wish to receive. Once the order form is completed, the customer software does the following (see Fig. 4.6):

1. Encrypts account information with the TP's public key
2. Attaches encrypted account information to the order form
3. Creates a message digest of the order form and digitally signs it with the customer's private key
4. Encrypts the following with the secret key: order form (with encrypted account information), digital signature.

Figure 4.6 Customer ordering- order sent to merchant

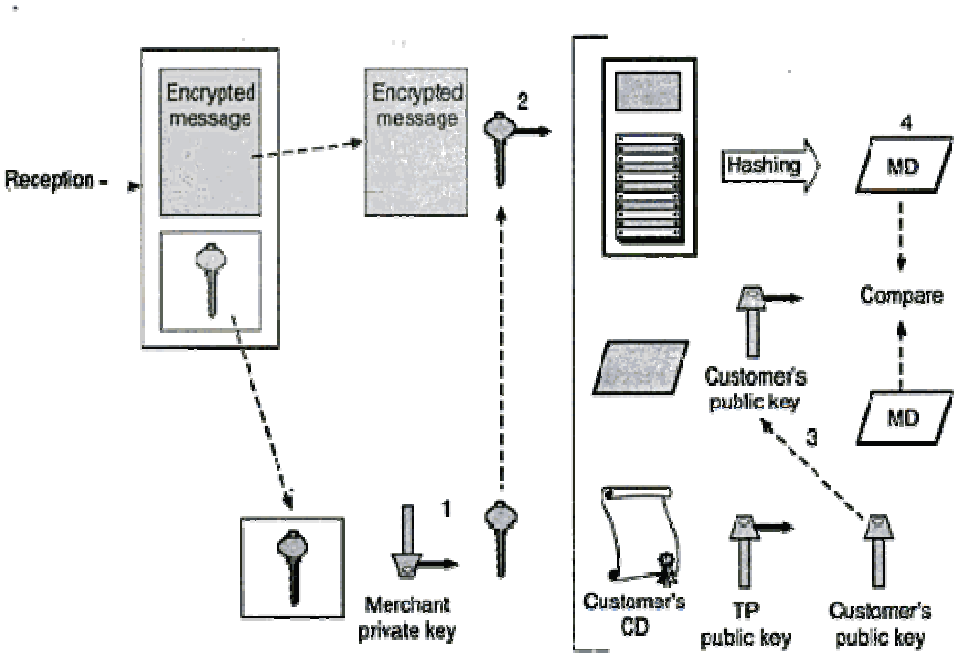


5. Encrypts secret key with the merchant's public key from the merchant's CD
6. Transmits the secret-key-encrypted message and encrypted secret key to the merchant

When the merchant software receives the order, it does the following (see Fig. 4.7):

1. Decrypts the secret key using the private key of the merchant
2. Decrypts the order form, digital signature, and customer's CD using the secret key
3. Decrypts the message digest using the customer's public key obtained from the customer's CD (and thus verifies the digital signature of customer)
4. Calculates the message digest from the order form and compares with the customer's decrypted message digest

Figure 4.7 Customer ordering-merchant receives order



Assuming that the message digests match, the merchant continues processing the order according to its own pre-established order fulfillment processes. One part of the order process, however, will include payment authorization which is discussed in the next section. After the order has been processed, the merchant's host should generate an order confirmation or receipt of purchase notifying the customer that the order has been processed. This receipt also serves as a proof of purchase equivalent to a paper receipt as currently received in stores. The way in which a customer receives the electronic receipt is similar to the encryption and digital signature processes previously described.

Payment authorization

During the processing of an order, the merchant will need to authorize (clear) the transaction with the PP responsible for that particular account. This authorization assures the merchant that the necessary funds or credit limit is available to cover the cost of the order. Also, note that the merchant has no access to the customer's account information since it was encrypted using the TP's public key; thus, it is required that this information be sent to the TP so that the merchant can receive payment authorization from the TP and that the proper customer account is debited for the transaction. It is assumed that the eventual fund transfer from some financial institution to the merchant (based upon PP payment authorization) and the debit transaction to the customer account takes place through an existing pre-established financial process.

In requesting payment authorization, the merchant software will send the TP the following information using encryption and the digital signature processes previously described:

- Merchant's CD
- Specific order information such as amount to be authorized, order number, date
- Customer's CD
- Customer's account information

After verifying the merchant, customer, and account information, the TP would then analyze the amount to be authorized. Should the amount meet some established criterion, the TP would send authorization information back to the merchant. Again, the way this information would be sent is similar to the encryption and digital signature processes previously described.

4.3 Check your Progress

1. Fill in the blanks

a. A purchase order is a commercial document issued by a ……. to a seller.

b. To send a message to a merchant the customer must have a copy of the ……. public key and a copy of the ……....public key.

c. …….assures the merchant that the necessary funds or credit limit is available to cover the cost of the order.

2. State whether following statements are true or false

a. Purchase Order's allow buyers to clearly and explicitly communicate their intentions to sellers.

b. Once the *account holder* receives the public key of the TP, the *registration* process stops.

4.4 ONLINE ELECTRONIC CASH

Online Ecash is a digital currency protocol developed by DigiCash and tested extensively on the Internet. Ecash uses public key encryption technologies to maintain the integrity of digital coins. By varying the encryption, Ecash can have strong or weak anonymity. DigiCash licenses Ecash technologies to banks, which convert outside money into digital currency and serve as currency servers in authenticating, clearing and settlement of accounts. Mark Twain Bank of St. Louis (http://www.marktwain.com) is the first electronic bank to license the Ecash technology that serves interface functions between dollar-denominated accounts and Ecash accounts.

As discussed in the introduction of this chapter, some transactions are better handled by e-cash, just as not all purchases are made by credit cards or check. E-cash works in the following way: a consumer opens an account with an appropriate bank. The consumer shows the bank some form of identification so that the bank knows who the consumer is. When cash is withdrawn, the consumer either goes directly to the bank or accesses the bank through the Internet and presents proof of identity. Once the proof is verified, the bank gives the customer some amount of e-cash. The e-cash is then stored on a PC's hard drive or possibly a PCMCIA card for later use. At some point in time, the consumer spends the e-cash by sending it to a merchant who validates the e-cash with the bank, which in turn deposits the e-cash in the merchant's account.

These transactions could all be done using public-key cryptography and digital signatures *as* discussed earlier. For example, the bank could give the consumer a message which equals x amount of money and digitally signs that message with its private key. When the consumer sends that message to a merchant, the merchant can verify the message by applying the bank's public key. Knowing that no one else other than the bank could have created the message, the merchant accepts it and deposits the value in the bank. Electronic cash boosts your purchasing power by making your money available to you 24×365. One can spend this digital money by accessing it online or offline.

Online Use of Electronic Cash

Electronic cash technology uses computers, local area networks, and the Internet for the transfer of money paid in exchange of services obtained. This process involves 3 entities: the buyer, the seller, and the service provider. Using this technology, money can be transferred online or offline. There are certain organizations such as Eagle Cash Technology (E-Cash), Octopus Card System, etc. which facilitate a secure transfer of money over the Internet between the seller and buyer. This enables one to do Internet shopping and enter in a transaction over the Internet while sitting in his house or office, in fact, from anywhere in the world. This saves time and physical efforts that one has to put in while physically going out and buying a ticket for air travel or for a movie, etc.

Within the Internet, dedicated local area networks and computers control the flow of digital or electronic cash between the entities or the bank accounts of the same

person - this form of money exists as bits and bytes inside computers memory. Electronic cash transfer systems depend on cryptology and the use of private and public keys for the encryption and decryption of the information that represents one's demand for transfer of money. It also uses digital signatures to verify the authenticity of source of demand.

Offline use of Electronic Cash

Can you recall when you last visited your bank personally? If you remember the day when you queued to deposit a check or withdraw some money from your bank account, then most probably you don't use a debit or credit card. These cards have a microchip embedded in them that stores the user's latest bank account information. Whenever a user makes use of credit or debit card to pay for his or her purchases, information in the chip is updated offline. Use of these cards have liberated people from carrying physical or paper money, and for this reason the term 'plastic money', was coined to describe electronic cash used through these cards. Use of these smart cards makes written checks, and withdrawal and deposit slips redundant. Automatic Teller Machines (ATMs) are important for the off-line use of electronic cash and using which one can use his credit or debit cards to withdraw money.

Problems with simple electronic cash

A problem with the c-cash example just discussed is that double- spending cannot be detected or prevented, since all cash would look the same. Part of this problem can be fixed by including unique serial numbers with the e-cash; now the merchant can verify with the bank whether anyone else has deposited e-cash with the associated serial numbers. In this scenario, the merchant must check with the bank for each transaction. Serial numbers, however, do not prevent double spending. While a bank can compare e-cash to see if there is duplication, there is no way to tell whether it was the consumer or the merchant who is trying to defraud the bank. This situation becomes even more difficult when the e-cash has passed through numerous parties before being checked with the bank.

Beyond the prevention of double-spending, e-cash with serial numbers is still missing a very important characteristic associated with real cash—it is not anonymous. When the bank sees e-cash from a merchant with a certain serial number, it can trace back to the consumer who spent it and possibly deduce purchasing habits. This frustrates the nature of privacy associated with real cash.

Preventing double-spending

While the preceding process protects the anonymity of the consumer and can identify when money has been double-spent, it still does not prevent consumers, or merchants for that matter, from double-spending.

To prevent double-spending, individuals must feel intimidated by some sort of legal prosecution—much in the same manner as the fact that counterfeiters of real cash will be prosecuted today. For individuals to believe in this threat there must be some way to identify them obtained from the double-spent e-cash. To create a process to identify double-spenders, but one that keeps the anonymity of lawful individuals requires the use of tamperproof software and complex cryptography algorithms.

The software used for withdrawing and receiving e-cash, must be tamperproof in that once an individual's identity verified by the bank) is placed in the software, it cannot he changed. Trying to change the identity or any coding of the software invalidates the software and any e-cash held by the software. The software prevents double-spending by encrypting an individual’s identity by using a random secret key generated for each piece of e-cash. The secret key is then encrypted using a special *two-part lock.* The encrypted identity and encrypted secret key is then attached to the e-cash. The property of the two-part lock is such that if the e-cash is double-spent, the two parts of the lock are opened revealing the secret key, and thus the identity of the individual who double-spent the cash.

When a consumer sends e-cash to a merchant, the merchant now receives the e-cash along with the encrypted identity of the consumer. Assuming the cash has not been double-spent; the merchant (merchant's software) adds information to the e-cash which unlocks one part of the two-part lock which is ultimately concealing the consumer's identity. Then the merchant, as previously described checks with the bank to ascertain that the money has not been double-spent. The bank in turn deposits the value of the e-cash in the merchant's account and maintains a record of the now half-unlocked e-cash.

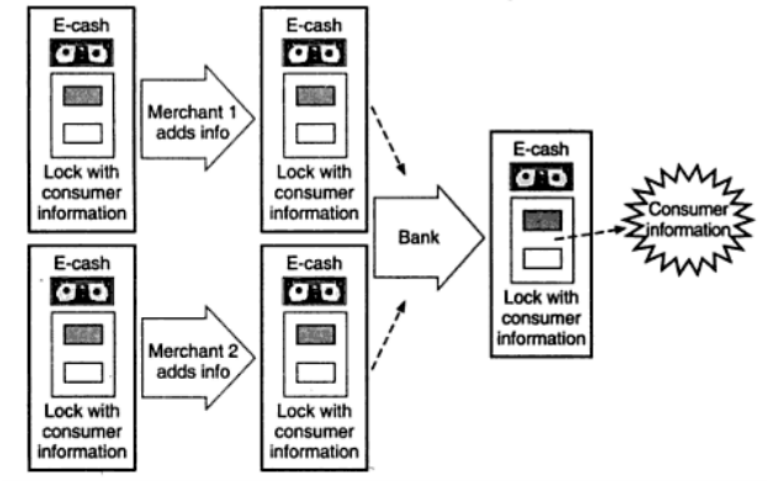
If a consumer tries to double-spend the e-cash with another merchant, that merchant adds information that unlocks another half of the two-part lock. The merchant now sends the e-cash to the bank to see if it has been double-spent. The bank, knowing the c-cash has been double-spent, is able to put the two parts of the two-part lock together, revealing the secret key, and thus the consumer's identity. Note that the two-part lock algorithm is complex enough not to allow the merchants or the bank to internally unlock both parts of the two- part system.

As not to be biased toward consumers, merchants that wish to use e-cash would be subject to the same process. (See Fig. 4.8)

E-cash interoperability

Consumers must be able to transact with any merchant or bank. Hence, process and security standards must exist for all hardware and software used in e-cash transactions. Interoperability can only be achieved by adherence to algorithms and processes in support of e-cash-initiated commerce. Since e-cash, in theory, can become the near equivalent of real cash, e-cash takes on many of the same economy- driving properties. Because of this, it would seem necessary for some type of government control over &cash transactions and the process and security standards associated with them. While only a single bank is mentioned in the e-cash examples, it is likely that the *bank* becomes a network of banks under the direct control of the Federal Reserve or similar institution outside of the United States.

Figure 4.8 Double-spending process depiction



Electronic payment schemes

This section provides a summary of the leading commercial electronic payment schemes that have been proposed in the past few years and the companies using them.

***Netscape*:**

Netscape's Secure Courier Electronic Payment Scheme, which has been selected by Intuit for secure payment between users of its Quicken home-banking program and banks, uses SEPP. SEPP's successor, SET, is now expected to see significant deployment. Companies working with MasterCard include Netscape, IBM, Open Market, CyberCash, and GTE Corporation. Netscape Navigator was planning to include Secure Courier, which encrypts data and authenticates individuals and merchants during Internet transactions.

***Microsoft*:**

Microsoft's STT is similar to SEPP/SET in that it provides digital signatures and user authentication for securing electronic payments. STT' is an embellished version of Netscape's SSL security tool and is compatible with SSL version 2.0. SIT provides such enhancements as stronger authentication (hr export and improved protocol efficiency by requiring fewer calls to initiate a communications session. STT is a general-purpose technology for securing financial transactions with applications beyond the Internet. Microsoft's Internet products, such as its Internet Explorer browser and the Merchant Web server, were planned to support STT' and Microsoft's Private Communications Technology (PCT security protocol; PCT offers general security for messaging and communications. NaBanco, the nation's largest credit card processor, will support Si'!', and Spyglass was planning to build Sri' into its Windows, UNIX, and Macintosh Web browsers and servers. The Internet Shopping Network also is imple-

menting the STT protocol and Microsoft's application programming interfaces. A movement toward SEPP/SET acceptance in the industry, in contrast with STT, has, however, been seen.

***Checkfree*:**

Checkfree Corporation provides on-line payment-processing services to major clients, including CompuSene, GEnie, Cellular One, Delphi Internet Services Corporation, and Sky-Tel. Checkfree employs a variety of mechanisms for handling such services, including Microsoft's STT, CyberCash, Netscape's SSL, and VeriSign's Digital ID. Checkfree has also announced intentions to support all security methods that achieve prominence in the marketplace, e.g. SET.

Together with CyberCash (see the next section), Checkfree developed Checkfree Wallet, a system that lets consumers and merchants undertake transactions easily and safely over the Internet. Checkfree Wallet has a client and a server component. The browser modules can be downloaded free from Checkfree's home page (http://www.checkfree.com) or a merchant's site for use with Netscape Navigator, Spyglass Mosaic, Quarterdeck Corporation's Mosaic, and The Wollongong Groups Emissary browsers.

CyberCash:

CyberCash's Secure Internet Credit Card Service delivers a safe, real-time solution for merchant processing of credit card payments over the Internet. The Credit Card Service lets any consumer with a valid credit card buy from any CyberCash enabled merchant. Designed to integrate fully with existing transaction processing systems used by banks and other financial institutions, the service provides automated and instantaneous authentication, enabling order processing to traverse the Internet 24 hours a day, 7 days a week.

It combines features from checks and cash. CyberCash is a digital cash software sys-tem which is used like a money order, guaranteeing payment to the merchant before the goods are shipped. CyberCash provides a (nearly) secure solution for sending credit card information across the Internet by using encryption techniques to encode credit card information. CyberCash wants a micropayment capability of 5 to 20 cents per transaction. There is a one-time charge to the customer to fill the coin purse and money never leaves the hank. The third party deciphers the transaction. To use CyberCash, a user must download the free CyberCash GUI; the user then executes the GUI to view merchandise on-line. The user then chooses the product he or she wishes to purchase and hits the pay button. At this juncture, the software automatically notifies the merchant to send an on-line invoice to the user, who then fills it out including name and credit card information. This information is then encrypted by the software and sent to the merchant. The merchant then sends the invoice and identification information to the CyberCash server. The CyberCash server then sends a standard credit card authorization to the merchant's bank and forwards the response to the merchant who then ships the goods to the user. See Fig 4.9. The entire process is conducted quickly and cheaply (CyberCash compares the cost per transaction to the price of a postage stamp). CyberCash's advantages are that it is easy and inexpensive to use and the user does not need to have any special accounts set up with CyberCash or with a bank. The main advantage to the merchant is that the goods are paid for before they are shipped.

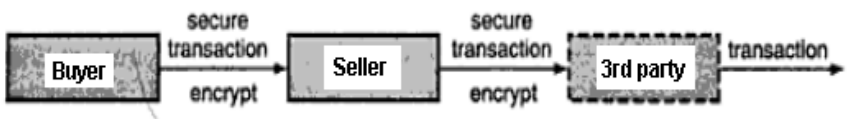


Figure 4.9 CyberCash electronic transaction process

VeriSign:

VeriSign is offering its digital signature technology for authenticating users as a component separate from encryption, which allows for export of stronger authentication. The U.S. government has (to date) embargoed export of strong encryption outside the United States, so many companies with divisions overseas are

increasing security using such authentication technologies as VeriSign's Digital ID. IBM is building support for Digital ID into its Web Browser and Internet Connection Secure Server for AIX and 03/2. IBM also is adopting Digital ID for use in its InfoMarket publishing network and clearinghouse. Digital his provide Web servers and clients with key authentication, privacy, and non-repudiation functions for electronic commerce?

DigiCash:

DigiCash is a software company whose products allow users to purchase goods over the Internet without using a credit card. The threat of privacy loss (where expenses can he easily traced) gave rise to the idea of anonymous e-cash, an electronic store of cash replacement funds, which can be loaded into a smart card for electronic purchases. This type of system, such *as* the one offered by the Netherlands' DigiCash NV (http://www.digicash.com), leaves no audit trail and ensures anonymous, untraceable transactions. An advantage of DigiCash is that it provides anonymity to the shopper because the bank replaces the user's digital signature with its own.

DigiCash is a software-only electronic cash system that provides complete privacy. The benefit of the DigiCash model is its ability to hold larger amounts of money than a credit card account. One person can hold more than one DigiCash account. The Mark Twain Bank of St. Louis is using the DigiCash Ecash system to let individuals and merchants exchange U.S. dollars electronically. Many Internet-based merchants have adopted Ecash: by mid-1996. 1000 buyers and 250 sellers were participating in the program (there were forecasts of 10,000 buyers participating by press time).

Users first need to download the DigiCash encryption software. They must then deposit money into a DigiCash bank via personal check or credit card in which they will receive digital coins in exchange. When purchasing goods; the users must send their e-mail requests to the DigiCash bank. The bank then checks the digital signatures of the users to verify that they are valid users. The bank then replaces the users' digital signature with the bank's digital signature and returns the money to the users. The users then send the e-cash to the merchant who accepts it based on its acceptance of the bank's digital signature.

The only micropayment system which was signing up customers at press time was DigiCash Ecash. Ecash is more complicated to design but cheaper to maintain than the credit/debit model. This is because accounting and auditing expenses are reduced (DigiCash claims that transaction costs are in the range of a penny each). Under this model, if Gabrielle wanes to buy from Emile, she sends him 10 cents worth of electronic currency purchased previously from a participating bank. Emile can deposit the currency or spend it in turn as he pleases. This decentralized transaction model has the virtue of making it harder for an authority to accumulate a master list of all the transactions conducted by a single buyer.

The downside of DigiCash transactions is that they are hard to trace, which does not make law enforcement officials or regulators happy, and there is no stop limit to financial risk. DigiCash is not foolproof in that it is possible for someone to steal a user's digital encryption key and use it for fraudulent purchases.

First Virtual Holdings:

First Virtual Holdings is targeting individuals and small businesses that want to buy and sell on the Internet but cannot afford an extensive on-line infrastructure. Using a First Virtual e-mail account and First Virtual's hosting systems to track and record the transfer of information, products, and payments for accounting and billing purposes, consumers and merchants can buy and sell goods on the Internet without sensitive information, such as credit card numbers, moving across the network. All sensitive information is delivered by telephone.

First Virtual hills the consumer using a designated credit card or checking account for all charges, and credits the seller's account for all payments earned. Users of the system include National Direct Marketing, Electronic Data Services. First USA. and Merchant Service. Shoppers access the First Virtual server (http://www.fv.com) and set up an account by giving their credit card numbers. Instead of getting digital money, the users get an on-line account. When purchasing goods; the shoppers give their account numbers to the merchant by entering it into the First Virtual server. The merchant then supplies a list of sales to First Virtual on a weekly basis. First Virtual

then notifies the customers via e-mail to confirm that they really want to purchase the goods. If they do not, then no money exchanges hands. If they do agree on the purchase, then First Virtual charges the users' credit card?

With First Virtual, the buyer has an account with the system and receives a password in exchange for a credit card number. The password is not protected while traveling over the Internet (this is not of interest to secure because First Virtual asks the buyer for an acknowledgment of each payment via out-of-band e-mail). The security of the

NetCash:

NetCash (http://www.netbank.com/-netcash/) is the Internet's answer to traveler's checks. To use NetCash, users must enter their checking account or credit card numbers into an on-screen form and e-mail it to the NetCash system. This entitles the users to purchase electronic coupons from NetCash for their face value plus a 2% commission. Each coupon is marked with a serial number. To purchase goods, the user browses NetCash's merchant list and selects products; at that juncture, buyers send their electronic coupons to the merchant. The merchant redeems the coupon at the NetCash bank (a computer program, not an actual bank) and NetCash takes 2 percent off the top as its fee. The NetCash system is not totally secure; hence, NetCash puts a limit of $100 on electronic transactions. NetCash does allow vendors to sell tangible goods which vendors ship via postal mail.

Other approaches:

This section lists a few other approaches that have appeared in the recent past.

-*Mondex* is based on smart-card technology initially backed by the United Kingdom's National Westminster and Midland Banks. The electronic purse is a handheld smart card; it remembers previous transactions and uses RSA cryptography. This has not proven to be successful: with the majority of the risk on the consumer's side, why would the consumer carry addition money when debiting ATMs are widely available?

-*NetMarket* (http://www.netmarket.com) receives user-ids and passwords over the Internet. User-id is good for a single merchant. This is similar to a private label credit card. After the first bill is paid, risk is reduced because the merchant knows the customer.

-*OpenMarket* (http://www.openmarketcom) handles credit card transactions via Web servers, hut it was planning to provide support for debit cards, checking accounts, and corporate purchase orders. It uses passwords and, optionally, two types of devices for response generation: secure Net key and secure ID shared-key cryptography. It will offer secure servers to merchants that support SHTTP and SSL

-*Global On-line* (http://www.globeonline.fr) uses on-line challenge/ response. It is based on a third party originating agreements; therefore, the seller has a higher cost to enter the market. (See Fig. 4.10)

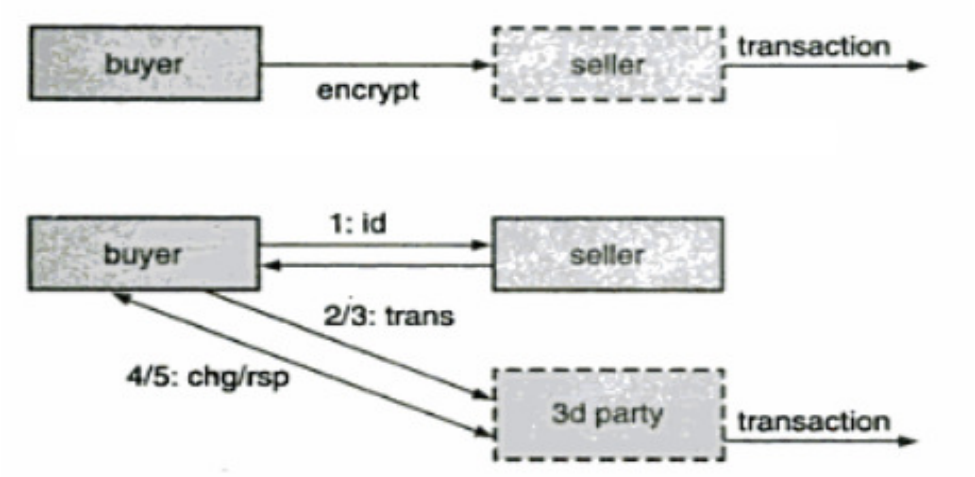
-Carnegie Mellon University's *NetBill* (http://www.ini.cmu.edu/ NETBILL/) supports micropayments. Micropayment systems can be divided into debit/credit (pay earlier/pay later) and digital cash (pay now). The NetBill system is an example of the former. Both buyers and sellers must have arranged accounts with a NetBill licensee perhaps a financial services company—prior to the transaction. When Gabrielle hits a *buy* link on a file carried on Emile's Web site, Emile's server delivers it in encrypted form, unreadable by her. A record of the transaction is sent to the NetBill server maintained by the licensee, which then checks Gabrielle's balance. Meanwhile, a NetBill client running on Gabrielle's desktop probes the integrity of Emile's transmission by matching what was sent against what was received. If both halves of the transaction check out, the NetBill server sends the decryption key to Gabrielle while debiting her account and crediting Emile's.

-NetBill hopes to pay for all costs—storage, processing, bandwidth, and management (including marketing, security, accounting, and software maintenance) out of a gross return of one or two cents per transaction plus a small percentage of the transaction value. While research suggests that many of these costs can be reduced significantly, customer and technical support costs remain unknown. New products naturally generate support calls, and users with money at stake are especially demanding. But pennies per transaction do not buy much of a service bureau. If the support lines cost out at $5 a call and an organization is getting one cent per transaction, one call wipes out the gross of 500 transactions. The prospects for any micropayment protocol will be mea-

sured by its success at automating customer support, in addition to providing security, reliability, quick response time, and ease of use.

-*Clickshare Corporation* (http://www.clickshare.com), which markets a micropayments system with the same name, has been delayed in part by resistance from one of its target markets: newspaper publishers. Clickshare differs from NetBill in that it envisions four interacting parties instead of three: the buyer, the seller or publisher, the buyer's *home base* (which might be an Internet access provider), and an account manager, which could be Clickshare itself or a licensee.

Figure 4.10 Global online transaction process



Under this model, if Gabrielle wants to buy a file from Emile for 10 cents, she first logs on to her home base, which attaches an identifying token to her URL. Next, she clicks on the link to Emile's site, which *is* hosted by the home base, and then, inside Ernile's site, she clicks on the desired file. Emile's server authenticates Gabrielle's home base token, delivers the file and sends copies of the transaction to both the home base and the account manager Gnbriolle's home base bills her for a dime; the account manager bills the home base for seven cents; and Emile bills the account manager for a nickel. The account manager is responsible for sending complete transaction records for users at specified periods.

As of early 1997, Clickshare found that the marketplace was not nearly as ready to go as people thought a year earlier. Publishers have not operated in an world in which articles are bought on a per- item basis. Newspaper management has historically depended on the model of aggregated content. Micropayments empower individual reporters and writers against the collective effort. Also, many publishers have hoped that their on-line effort could be supported with paid advertising, a more conventional support relationship.

-*Wallets and such.* Even in the absence of standards , vendors have been developing systems to handle sales over the Internet, and companies willing to accept that the products are not interoperable can support business before standards become widely deployed. As one example, VeriFone, a POS (point-of-sale; systems provider, has put together a suite of programs to support Web-based payments. vPOS is the merchant's receipt and transaction management system designed

Advantages and Disadvantages of Electronic Cash

Gone are the days when an individual had to carry around silver and gold coins. We now have the option of carrying paper money. Now, the amount of paper money that a person needs to carry around has also reduced considerably, thanks to electronic cash. But all is not what meets the eye! Continue reading to know all about e-cash, its uses and misuses!

You know how they say that the world economy has benefited from the use of electronic cash? Well, there are some who say that it hasn't. I personally have spent several sleepless nights wondering how can such contradictory statements exist for a concept that, by nature, is black and white? But on careful and detailed research, the well-known phrase "There are always two sides to a coin" came to my mind.

Electronic cash has made monetary transactions a piece of cake. Be it an amount in millions, or money transfer to a tiny town in another continent. E-cash transactions are fast, accurate and easy. But before we get to the "two sides" of this "coin", let's see how many forms it has

There are a few basic categories:

- **Anonymous**: This kind of e-cash works just like cash. Once a specific amount is withdrawn from an account, it can be used (or misused) without leaving a visible trail.
- **Identified**: We know this category popularly as PayPal or WebMoney. The usage and transfer of money in these systems is not entirely untraceable.
- **Online**: Obviously, it means that one needs to correspond with a bank (via the internet). The bank, then, gets in touch with the third party.
- **Offline**: One can directly conduct the transaction without any interference from the bank.
- **Smart Card**: Smart cards are like credit cards with a computer chip in them that stores the holder's money-related information. They are used in digital cash applications.

Interesting isn't it?
Now, coming to the *advantages* of e-cash:

- **Online Electronic Cash**

1. Anonymity and un-traceability can be maintained: User Id's are kept highly confidential.
2. No issues regarding "Double spending": Real-time checking of all transactions makes the possibility of multiple expenditures negligible.
3. No requirement of additional secure hardware: Existing POS (point of sale) hardware's can be updated and used.

- **Offline Electronic Cash**

1. Portable: This system is fully offline and portable.
2. Anonymity unless double spending: The user is anonymous unless he commits a double expenditure.
3. Detection of Double Spender: The bank can effectively detect a double spender.
4. Frequent synchronizations are not required: The bank doesn't need to synchronize its servers very often. This is mostly done via batch updates.

There are some more advantages. The online electronic cash systems that are operated through the Internet provide convenience to the user and the banker. The online system can be accessed through the Internet from anywhere in the world. Hence, the user does not have to actually go to the bank to transact any business. The online system also provides convenience to the banker, as he does not have to deal with long queues of people. This increases the speed of transactions in financial organizations. This advantage is supplemented by very good accuracy as the transactions are done with the help of machines and computers. The manual labor, involving the cashier, security and other bank staff is reduced.

The small-scale and the local level merchants can also access and transact in the global market. This can be easily accomplished through the facility of online shopping. Another advantage of online shopping is that the shopper can sit at home and purchase the goods he wants, with the help of a credit card. The 'smart' cards can also be restricted to specified payments. For example: the parents of a student studying in a far-off university can charge his smart card that can be used only for paying tuition fees. Another very good advantage of e-cash is that the transactions are all recorded in a database, so one does not have to keep wondering when and for what purpose one has spent money. The concept of smart card also reduces the possibility of robbery. The smart cards for withdrawal like the ATM cards are protected by passwords.

Overall, the concept of electronic cash provides the user with convenience in transactions. The user of the electronic cash technology does not always have to carry around physical cash. The offline e-cash smart cards are also sometimes referred to as plastic money.

Now, the *disadvantages* of this marvelous mode of transaction:

- **Online Electronic Cash**
  1. Communication Overheads: Security and anonymity cost become a bottleneck of the system. This can happen at times during real-time verifications.
  2. Massive Databases: The bank will have to maintain a detailed and confidential database.
  3. Synchronization: The bank needs to synchronize its server every time transaction is made. It would be insanely impractical to maintain.
- **Offline Electronic Cash**
  1. Prevention may not be Immediate: Double spending may not be prevented effectively and immediately.
  2. Implementation Expenditure: the required additional hardware is quite costly to install.

There are other cons to consider. E-transactions depend a lot on technology. Hence, power failure, unavailability of internet connection, undependable software and loss of records could be a hindrance in your way. The system of electronic cash is extremely convenient, but it is not a foolproof system. The online electronic cash system has the same problems as your email account and personal computer. The online facility can be or can also be infected with a virus, if sufficient security is not provided. Some of the disadvantages of electronic cash include serious misuse of a stolen smart card. Criminals who have strong knowledge of the technology of these systems can easily misuse it, if a reliable security system is not deployed. The phenomena of identity protection and credit history play a very important role in the working of the e-cash system. To safeguard the interests of the users, protection against identity theft has become the most important function of these service providers.

Many pros and cons are bound to appear as the technology of electronic cash develops even further. However, overcoming the cons of the technology will make e-cash, a very convenient system and a widely accepted, revolutionary mode of cash.

3.4 Check your Progress

1. Give answers in short.

a. Name any 4 Electronic payment schemes.

……

……

b. Write some of the advantages of e-cash.

……

……

c. What are the disadvantages of e-cash?

……

……

2. Match the following.

Column A	Column B
a. Netscape	1. Secure Internet Credit Card Service
b. Microsoft	2. Secure Courier Electronic Payment Scheme
c. CyberCash	3. Digital signature technology
d. VeriSign	4. STT

4.5 SUMMARY

Technology has inarguably made our lives easier. It has cut across distance, space and even time. One of the technological innovations in banking, finance and commerce is the Electronic Payments. Electronic Payments (e-payments) refers to the technological breakthrough that enables us to perform financial transactions electronically, thus avoiding long lines and other hassles. Electronic Payments provides greater freedom to individuals in paying their taxes, licenses, fees, fines and purchases at unconventional locations and at whichever time of the day, 365 days of the year. On the basis of present study, first remark is that despite the existence of variety of e-commerce payment systems, credit cards are the most dominant payment system. This is consequences of advantageous characteristics, most importantly the

long established networks and very wide users' base. Second, alternative e-commerce payment systems are some countries are debit cards. In fact, like many other studies, present study also reveals that the smart card based e-commerce payment system is best and it is expected that in the future smart cards will eventually replace the other electronic payment systems. Third, given the limited users bases, e-cash is not a feasible payment option. Thus, there are number of factors which affect the usage of e-commerce payment systems. Among all these user base is most important. Added to this, success of e-commerce payment systems also depends on consumer preferences, ease of use, cost, industry agreement, authorization, security, authentication, non-refutability, accessibility and reliability and anonymity and public policy.

Electronic payment schemes, a comprehensive index of electronic payment schemes and a brief overview of their relationship to the framework is provided. The framework consists of two axes, the levels of abstraction at which the protocol is analyzed and the payment model considered. Many businesses, including both the largest of corporations and small retailers, rely on electronic payment system, provided in most instances by the major banks, to accept payments. Essentially these systems provide companies with an efficient and secure means of collecting payments, transferring value and managing cash flows.

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, a form of online payment that is portable and anonymous, has been slow to catch on in the United States. A number of companies have failed as they attempted to introduce electronic cash to the online world. Electronic cash could be useful for making micropayments because the cost of processing payment cards for small transactions is greater than the profit on such transactions. Electronic cash can be stored online or offline. A third party, such as a bank, stores online electronic cash.

Banks still process most monetary transactions, and a large part of the dollar volume of those transactions is still done by writing checks. 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.

Source : *gesj.internet-academy.org.ge(Link)*

4.6 CHECK YOUR PROGRESS – ANSWERS

4.1 & 4.2

1.

a) Payment information
b) Public key and private key

4.3 **1.**

a) Buyer
b) Merchant, Third party
c) Payment authorization

2.

a) True

b) False

4.4

1.

a) Netscape's Secure Courier Electronic Payment Scheme, Microsoft's STT, Checkfree Corporation, CyberCash's Secure Internet Credit Card Service , VeriSign's digital signature technology, First Virtual Holdings, Mondex, NetMarket , OpenMarket, etc.

b) Anonymity and un-traceability can be maintained, No Double spending allowed, No requirement of additional secure hardware, Portable, detects a double spender, frequent synchronizations are not required, etc

c) Security and anonymity cost, its Massive Databases, need of repeated Synchronization; double spending may not be prevented effectively and immediately, and cost of required additional hardware, etc.

2. a-2 b-4 c-1 d-3

4.7 QUESTIONS FOR SELF STUDY

1. Write a note on Internet monetary payment and security requirements.
2. What is Payment information integrity? What is account holder & merchant authentication?
3. Explain in brief what payment and purchase order process is and how it works.
4. What is online electronic cash? Explain in detail.
5. What are the different electronic payment schemes proposed?
6. Write the advantages of e-cash.
7. What are the disadvantages of e-cash?

4.8 SUGGESTED READINGS

Web Security, Privacy & Commerce By Simson Garfinkel, Gene Spafford

Electronic Payment Systems for E-commerce

NOTES

NOTES

Chapter 5

INTERNET / INTRANET SECURITY ISSUES & SOLUTIONS

5.0 OBJECTIVES

After studying this chapter you will be able to :

- explain the need for computer security
- describe different security strategies, security techniques in commerce.
- discuss card transactions and its payment process.

5.1 INTRODUCTION

Every user of a computerized system; networked or not, including the merchant and the buyer, must determine the best methods to safeguard information that is considered proprietary. Just like with traditional credit cards and other financial instruments, the responsibility burdens both parties. Open public networks, such as the internet, offer little privacy or security on their own. There are numerous security-infraction vicissitudes today, mostly induced by poorly (if at all) implemented host security mechanisms. This chapter explores the various issues centered around Internet/Web security, whether or not specific security measures are needed and where, and the different alternatives that exist on implementing security.

5.2 NEED FOR COMPUTER SECURITY

Computers are an inseparable part of our lives today, life that has increasingly become technology driven. Besides work, we use computers for communicating, banking, entertainment, research – just to name a few. Besides hardware, security of the new-age machines is threatened by malicious software, viruses, Trojans etc. all designed to cripple a system. Loss of computer security leads to corruption or loss of data, misuse or theft of information, identity theft and unauthorized use of client information, transmission of computer viruses that can affect third parties and can lead to potential liability, services interruptions, security breaches at vital government installations that can threaten national safety. For corporate houses, loss of computer security can make vital difference in acquiring new work and sustaining current projects.

These are strong reasons to **computer support** the need for installing computer security systems. The first important requirement is licensed Anti-virus software. There are over 50,000 known viruses and 200 new viruses are discovered every month. The easiest method for spreading viruses is by e-mail attachments or instant messaging messages. Viruses can be disguised as greeting cards, funny images, or video and

audio file attachments. The computer needs to get updated with latest threats and that is possible only with original computer security software as it gets automatically updated every time the machine goes online.

The next important requirement is Firewall Software. This enhances computer security by controlling communications from it, prevents unwanted accesses and is capable of blocking outgoing and incoming IP addresses. Often computer security is compromised due to spyware that enters a machine by deceiving the user or through some software loopholes. Sometimes the user is tricked into unknowingly installing it or it piggybacks on desirable software. Hence, spyware removing software is a must in the computer security system. A pop-up blocker is another important element in securing computers. Malicious attackers are likely to use pop-up windows that are concealed as special offers to set up a malicious code on a computer.

Besides all these installations it is important to ensure correct practices to ensure computer security when accessing the Internet. Never download email attachments from unknown persons, do not share your banking details and passwords with unknown people, do not click on links inside emails, for financial transactions - type in the URL each time on your browser and take care when sharing flash drives. These are just some additional measure to ensure **computer security.** Always buy licensed, original Operating System Software and Anti Virus Software. While there are cyber laws to help track and punish breaches in computer security, it's better to be safe rather than sorry!

The Basics of Computer Security

- Make sure that the link between you and the Internet is safe. You need to have a hardware firewall installed between you and the Internet. Most recent devices that connect you to the Internet have one built in, but in any case you need to make sure that what you have is a state-full firewall. It should give your computer full access to the Internet, but block all traffic trying to access your network when originated from the Internet side.
- Secure your Internet router. Change the administrator password and if possible the administrative account name as well. Everyone who has bought that device will know what the default account and password is, so you must change these and make them difficult to guess. This is especially important if you have a wireless network.
- Install anti-virus software on your computer. Make sure it scans the computer for viruses at least once a week. Keep the software up to date and make sure that the virus definitions are updated every day. Also make sure that this is monitoring the computer all the time to help prevent it being infected in the first place.
- Install a personal firewall on your computer. Not only should this help limit the damage malware can do to your computer, but it should also reduce the chances of this spreading to other computers. Get in the habit of checking the dialogues that you are prompted with and only allow Internet access to applications that really need it.
- Install anti-spyware software on your computer. Make sure it fully scans your computer for spyware at least every week. Keep the software up to date and make sure that the definitions are updated every day. Also make sure that this monitors your computer all the time.
- Keep up to date with the security patches for your Operating System. Microsoft release security updates for Windows every month. However, make sure your computer is configured to automatically check for downloads every day and at a time when your computer is most likely to be turned on.
- Secure your wireless network. Do not broadcast your SSID (Service Set Identifier). Although it can be learned by someone who is determined, there is no point making things easy. So make sure this is disabled. Restrict access to your wireless network based on the MAC (Media Access Control) address of your computer. Yes, these can be faked, once known, but why make things simple? Implement WPA (Wi-Fi Protected Access) or WPA2, if you can, to further secure your wireless network. And use a pre-shared key which is not easy to guess.

Security threats to e-commerce

E-Commerce security requirements can be studied by examining the overall process, beginning with the consumer and ending with the commerce server. Considering each logical link in the "commerce chain", the assets that must be protected to ensure secure e-commerce include client computers, the messages travelling on the communication channel, and the web and commerce servers – including any hardware attached to the servers. While telecommunications are certainly one of the major assets to be protected, the telecommunications links are not the only concern in computer and e-commerce security. For instance, if the telecommunications links were made secure but no security measures were implemented for either client computers or commerce and web-servers, then no communications security would exist at all.

Client threats

Until the introduction of executable web content, Web pages were mainly static. Coded in HTML, static pages could do little more than display content and provide links to related pages with additional information. However, the widespread use of active content has changed this perception.

a) *Active content:* Active content refers to programs that are embedded transparently in web pages and that cause action to occur. Active content can display moving graphics, download and play audio, or implement web-based spreadsheet programs. Active content is used in e-commerce to place items one wishes to purchase into a shopping cart and to compute the total invoice amount, including sales tax, handling, and shipping costs. The best known active content forms are Java applets, ActiveX controls, JavaScript, and VBScript. Since active content modules are embedded in web pages, they can be completely transparent to anyone browsing a page containing them. Anyone can embed malicious active content in web pages. This delivery technique, called a *trojan horse*, immediately begins executing and taking actions that cause harm. Embedding active content to web pages involved in e-commerce introduces several security risks. Malicious programs delivered quietly via web pages could reveal credit card numbers, usernames, and passwords that are frequently stored in special files called cookies. Because the internet is stateless and cannot remember a response from one web page view to another, cookies help solve the problem of remembering customer order information or usernames or passwords. Malicious active content delivered by means of cookies can reveal the contents of client-side files or even destroy files stored on client computers.

b) M*alicious codes:* Computer viruses, worms and Trojan horses are examples of malicious code. A trojan horse is a program which performs a useful function, but performs an unexpected action as well. Virus is a code segment which replicates by attaching copies to existing executables. A worm is a program which replicates itself and causes execution of the new copy. These can create havoc on the client side.
c) *Server-side masquerading:* Masquerading lures a victim into believing that the entity with which it is communicating is a different entity. For example, if a user tries to log into a computer across the internet but instead reaches another computer that claims to be the desired one, the user has been spoofed. This may be a passive attack (in which the user does not attempt to authenticate the recipient, but merely accesses it), but it is usually an active attack (in which the masquerader issues responses to mislead the user about its identity).

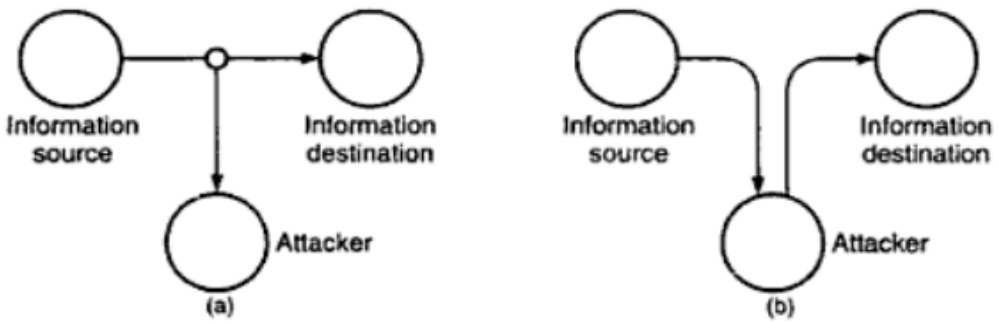


Figure 5.1 Security threads (a) passive threads (b) active threads

Communication channel threats

The internet serves as the electronic chain linking a consumer (client) to an e-commerce resource (commerce server). Messages on the internet travel a random path from a source node to a destination node. The message passes through a number of intermediate computers on the network before reaching the final destination. It is impossible to guarantee that every computer on the internet through which messages pass is safe, secure, and non-hostile.

a) **Confidentiality threats**: Confidentiality is the prevention of unauthorized information disclosure. Breaching confidentiality on the internet is not difficult. Suppose one logs-onto a website – say www.anybiz.com – that contains a form with text boxes for name, address, and e-mail address. When one fills out those text boxes and clicks the submit button, the information is sent to the web-server for processing. One popular method of transmitting data to a web-server is to collect the text box responses and place them at the end of the target server's URL. The captured data and the HTTP request to send the data to the server is then sent. Now, suppose the user changes his mind, decides not to wait for a response from the anybiz.com server, and jumps to another website instead – say www.somecompany.com. The server somecompany.com may choose to collect web demographics and log the URL from which the user just came (www.anybiz.com). By doing this, somecompany.com has breached confidentiality by recording the secret information the user has just entered.

b) **Integrity threats:** An integrity threat exists when an unauthorized party can alter a message stream of information. Unprotected banking transactions are subject to integrity violations. Cyber vandalism is an example of an integrity violation. Cyber vandalism is the electronic defacing of an existing website page. Masquerading or spoofing – pretending to be someone you are not or representing a website as an original when it really is a fake – is one means of creating havoc on websites. Using a security hole in a domain name server (DNS), perpetrators can substitute the address of their website in place of the real one to spoof website visitors. Integrity threats can alter vital financial, medical, or military information. It can have very serious consequences for businesses and people.

c) **Availability threats:** The purpose of availability threats, also known as delay or denial threats, is to disrupt normal computer processing or to deny processing entirely. For example, if the processing speeds of a single ATM machine transaction slows from one or two seconds to 30 seconds, users will abandon ATM machines entirely. Similarly, slowing any internet service will drive customers to competitors' web or commerce sites.

Server threats

The server is the third link in the client-internet-server trio embodying the e-commerce path between the user and a commerce server. Servers have vulnerabilities that can be exploited by anyone determined to cause destruction or to illegally acquire information.

a) **Web-server threats:** Web-server software is designed to deliver web pages by responding to HTTP requests. While web-server software is not inherently high-risk, it has been designed with web service and convenience as the main design goal. The more complex the software is, the higher the probability that it contains coding errors (bugs) and security holes.

b) **Commerce server threats:** The commerce server, along with the web-server, responds to requests from web browsers through the HTTP protocol and CGI scripts. Several pieces of software comprise the commerce server software suite, including an FTP server, a mail server, a remote login server, and operating systems on host machines. Each of this software can have security holes and bugs.

c) **Database threats:** E-commerce systems store user data and retrieve product information from databases connected to the web-server. Besides product information, databases connected to the web contain valuable and private information that could irreparably damage a company if it were disclosed or altered. Some databases store username/password pairs in a non-secure way. If

someone obtains user authentication information, then he or she can masquerade as a legitimate database user and reveal private and costly information.

d) **Common gateway interface threats:** A common gateway interface (CGI) implements the transfer of information from a web-server to another program, such as a database program. CGI and the programs to which they transfer data provide active content to web pages. Because CGIs are programs, they present a security threat if misused. Just like web-servers, CGI scripts can be set up to run with their privileges set to high – unconstrained. Defective or malicious CGIs with free access to system resources are capable of disabling the system, calling privileged (and dangerous) base system programs that delete files, or viewing confidential customer information, including usernames and passwords.

e) **Password hacking**: The simplest attack against a password-based system is to guess passwords. Guessing of passwords requires that access to the complement, the complementation functions, and the authentication functions be obtained. If none of these have changed by the time the password is guessed, then the attacker can use the password to access the system. Some of the hacking techniques are listed in below table.

Table 5.1 Some hacking techniques

Stolen access	Involves the use of another user's ID or password without permission to gain access to the Internet.
Stolen resources	Search for processors to store stolen software and databases (using the Internet as the navigation mechanism).
Internet virus (aka worm)	Virus designed to traverse through the network, passing through multiple processors and either sending information back to the originator or doing damage to the processors it passes through.
E-mail impostures	Sending e-mail while falsifying the *From* field.
E-mail snooping	E-mail passes through at least two nodes to be received; as the e-mail passes through these nodes, and is stored transiently, it is susceptible to people with system access (e.g., administrators), unless secured.
Sniffing	If a hacker has gained access to a host, the hacker may set up *sniffing* programs to observe traffic, storing information (IDs/passwords) that can be used to compromise other systems.
Spoofing	Assuming someone else's identity, whether it be a login ID, an IP address, a server, or an e-commerce merchant.
Async attacks	While programs are idle in host memory, a hacker may have the opportunity to access the program's data.
Trojan horses	Viruses concealed within a software package injected into a host. May be destructive or perform some covert activity designed to send data back to the hacker.
Back doors	Application/system programmers may implement a secret password that allows the programmer easy access to a host or application on the host; these passwords may be infiltrated.

5.1 & 5.2 Check your Progress

Fill in the blanks.

a. ……enhances computer security by controlling communications and it prevents unwanted accesses.

b. ……refers to programs that are embedded transparently in web pages and that cause action to occur.

c. Web-server software is designed to deliver web pages by responding to ……

d. A ……implements the transfer of information from a web-server to another program.

- **Policy Issues**

A useful security policy is quite general. It typically does not specify by name that certain people may or may not have access to certain information. Instead, it may state that the holders of certain positions have the authority to gain access to certain information. It may allow the holders of other positions to grant individuals access to information within some scope or set of checks and balances. A security policy may also state requirements that people must meet for access to information, as in the case of security clearances for access to classified national security information.

The Executive Branch of the US government (as well as branches of other governments) has a general security policy for the handling of sensitive information. This security policy involves giving an access class called a “security classification” to sensitive information and a clearance to individuals authorized to access it. No individual is granted access to information classified higher than that individual’s clearance. (For example, since “Top Secret” is higher than “Secret,” an individual with a “Secret” clearance is not permitted access to “Top Secret” information.) However, possession of a clearance at or higher than the classification of the information alone is not enough to gain access — that individual also must have a “need-to-know” the information, as judged by someone who already has access to the information.

To better understand how a general security policy such as this is enforced when computer systems are operating in different environments; consider three different modes of secure computing used in the Department of Defense: dedicated, system high, and multilevel. In a simple computation environment, protection or security is enforced by physical means external to the computer (fences, guards, and so on) in a dedicated mode of operation. In this mode, all users allowed access to the system are cleared for the highest level of information contained in the system and have a need-to-know for all the information in the system (that is, it is dedicated to processing for users with a uniform need-to-know for this information at a given single security level). All users, equipment, and information reside within this protective boundary or security perimeter. Everything within the security perimeter is considered benign. The computer system is not expected to seriously “defend” information from any of its users because they are considered non-malicious by virtue of their security clearances and need-to-know.

In another environment (called the system high mode), the computer not only provides computation but must internally provide mechanisms that separate information from users. This is because not all users of the system have a need-to-know for all the information it contains (but all are cleared for the highest level of information in the system).

Thus, one of the first steps in building a secure computer system is to interpret the security policy to be enforced in a way that allows it to apply to the internal entities of the computer system. A security policy is interpreted in terms of the permissible access modes (for example, read or write) between the active entities — subjects — and the passive entities — objects — to establish a technical security policy (or a “technical policy”) for the system. We therefore call the specific translation of a security policy into terms implemented on a computer the technical security policy, as distinct from the security policy stated in terms of people accessing information. To build a secure computer system, it is essential to have a technical security policy that is complete and precisely defined and interpreted.

A basic principle of computer security is that a given system can only be said to be “secure” with respect to some specific security policy, stated in terms of controlling access of persons to information. It is critical to understand the distinction between security policy (or technical security policy as defined above) and security mechanisms that enforce the security policy within a given computer system. For example, mechanisms might include type enforcement, segmentation, or protection rings. These are all mechanisms that may be used within a computer system to help enforce a security policy that controls access of persons to information, but none of these is itself a security policy. Such mechanisms provide functionality that enables the implementation of access control within the computer system, but they do not directly represent rules in the security policy world of persons and information. It has been shown that in general for any given security mechanism, there are security policies that the mechanism is not sufficient to enforce. Thus the mechanism is molded by the security policy that it is designed to support.

To understand the danger of mistaking security mechanisms for security policy, consider that some existing systems impose security mechanisms on users, but it is not at all clear what the security policy is that is being enforced. (Examples include the Unix “setuid” and “setgid” mechanisms) This creates the illusion of security, without providing real security.

A broad range of security policies that can be considered in two classes: access control policies and supporting policies. Access control policy is that portion of the security policy that specifies the rules for access control that are necessary for the security policy to be enforced. Supporting policy is that part which specifies the rules for associating humans with the actions which subjects take as surrogates for them in computers to access controlled information. The access control policies in turn fall into two classes: discretionary and mandatory. These two classes were originally referred to as discretionary and nondiscretionary. More recently, nondiscretionary has been called mandatory, but the meaning has been retained: Mandatory is still the complement of discretionary. For reasons that will become clearer below, protection against malicious software is offered only by an implementation of the reference monitor concept enforcing mandatory access control policies, though the reference monitor paradigm of subjects, objects, authorization functions, and reference functions is also used for discretionary access control.

Mandatory access control policy:

A mandatory access control policy provides an overriding constraint on the access of subjects to objects, with high assurance of protection possible, even in the face of Trojan horses and other forms of malicious software. In terms of the reference monitor concept, the idea is that we can affix a label to objects to reflect the access class of the information they hold. We can correspondingly affix a label to subjects to reflect the equivalence class of object sensitivity that the subject can access. The reference monitor compares the labels on subjects and objects, and grants a subject access, per the requested access mode, to an object only if the result of the comparison indicates that the access is proper.

Mandatory access control policies can provide protection against unauthorized modification of information (integrity) as well as protection against unauthorized disclosure (confidentiality). The labels in a specific mandatory access control policy can be selected to accomplish many different purposes for integrity and confidentiality. For example, they can reflect the US government’s security policy for confidentiality mentioned earlier, utilizing hierarchical classifications and security clearances (for example, Secret, Top Secret). They can reflect a corporate security policy (for example, Public, Proprietary for Confidentiality or Technical, and Management for Integrity). They can also reflect a partitioning of activities into separate spheres or compartments, with different individuals authorized access to information in different areas.

Discretionary access control policy:

Discretionary access control policies are so named because they allow the subjects in a computer system to specify who shall have access to information at their own discretion. In a system that incorporates both mandatory and discretionary access control policies, the discretionary access control policy serves to provide a finer granularity within (but cannot substitute for) the mandatory access control policy. For example, the military need-to-know security policy in which each individual has a responsibility to determine that another has a valid requirement for information, even though the other has a clearance for the information, is a common discretionary access control policy. In other cases, allow-ability of access within a discretionary access control policy may be based on the content or context of the information to be accessed or on the role of the user at the time of the access request — or it may involve complex conditions for determining allowable access. In contrast to mandatory access control policies, it need not be global or persistent. Alternatively, a system may incorporate only a discretionary access control policy if the mandatory access control policy is degenerate so that all subjects and objects belong to just a single (implicit) access class. This is the case for the system high mode of operation discussed earlier. A common example of a discretionary access control policy implementation is the ability of a computer user or a process which that user has executed to designate specific individuals as being authorized access to a given file. Many operating systems provide protection bit masks (for example, “owner,” “group,” and “world”), access control lists, or file passwords as mechanisms to support some form of discretionary access control policy.

A discretionary access control policy is useful in some environments, but it will not defend against Trojan horses or other forms of malicious software such as may be used to perform probing, penetration, or subversion attacks. This can be seen by considering a Trojan horse hidden in a useful program. The example Trojan horse is designed to make a copy, in a directory where the copy is not likely to be noticed right away, of all of the files that belong to a user who runs the program that are marked for reading only by that user. This copy is made readable by some other user who would not be intended to have access to the files. In contrast, consider a mandatory access control policy intended to provide confidentiality. Since the label is attached to any copy which is made and since the Trojan horse cannot change the label, the Trojan horse cannot give a user access to any file in a manner contrary to the mandatory access control policy. In other words, a mandatory access control policy does not prevent a copy from being made by a Trojan horse executing in a process with the same label (for example) as the file, but it does prevent the file's label from changing and prevents access to the file on a global and persistent basis. Discretionary access control policies offer no real protection against even such simply designed malicious software.

Supporting policy:

In addition to the access control policies (mandatory and discretionary), there are additional security requirements relating to the accountability of individuals for their security-relevant actions in the computer system. These requirements make up supporting policy. Supporting policy fundamentally "supports" the tie of people in access control policies, about people accessing information, to subjects acting as surrogates for people in computers. Supporting policy provides an environment for ensuring individual accountability for the enforcement and monitoring of the access control policies. In contrast to access control policy, which associates directly with the "theory of computer security" — the reference monitor concept — there is no corresponding "theory" that helps one verify the implementation of supporting policy. Fortunately, it is possible to analyze and test software performing supporting policy functions to reasonably conclude that it functions properly. In contrast, as we have said, it is not possible to do this for an implementation of access control policy. Supporting policy includes two subcategories: identification/authentication policy and audit policy.

The former supports the access control policies by specifying the requirements for authenticating the identity of an individual prior to allowing subjects to act as surrogates for that individual in attempting access. Identification/authentication policy provides the basis for the labels that are used in enforcing the mandatory access control policy to be associated with subjects acting as surrogates in the computer for individuals. In other words, it determines whether subjects may act as surrogates for a particular individual and what label is associated with such subjects. It also provides the basis for the membership of individuals in a group and more generally for controls on subjects consistent with the discretionary access control policy. Further, it provides the basis for recording the identity of the individual causing an auditable action to be performed by a subject acting as the user's surrogate. Audit policy provides the basis for the recording of those security relevant events that can be uniquely associated with an individual. The objective is to provide accountability for the security-relevant actions of individual users. We do not have much more to say in this essay about audit policy. The following paragraphs expand a bit on identification and authentication and other aspects of accountability, as supporting policy considerations.

Indirect access:

Any discussion of security policy would be incomplete if it did not address the often-overlooked topic of indirect access. Indirect access is access that occurs outside the security perimeter of the secure computer system. Indirect access is particularly important precisely because it is often overlooked in establishing a security policy for a computer system. Often, the security policy of a so-called secure system may contribute to illegal indirect access; conversely, the security policy of a secure system can contribute to preventing illegal indirect access. Of course, indirect access is not always overlooked. A description of what is meant by "clearances of system users" says, System users include not only those users with direct connections to the system but also those users without direct connections who might receive output or generate input that is not reliably reviewed for classification by a responsible individual.

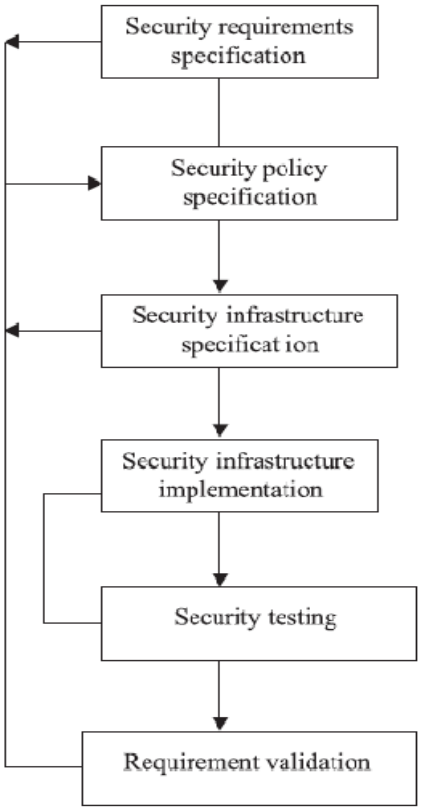
Implementing security for e-commerce

Let us now look at the fundamental strategic requirements an organization needs to consider if it wants to ensure that an e-commerce or online security project will be a success. Technology components of good online security, such as encrypted email, secure SSL websites, and intranets/extranets all have a role to play in protecting valuable data, but for security to be effective it must be designed as a whole and applied consistently across an organization and its IT infrastructure. There is a subtle difference in the design of a software system and that of a security system. While designing software, the functional correctness of applications is the prime concern. In fact, in software systems, the designer aims at ensuring that for reasonable input, the user gets reasonable output. This can be traced from the system specification. But in the case of security systems, the designer has to ensure that the system properties are preserved in the face of attack. Thus the system outputs should not be completely disastrous for unreasonable inputs. In security systems, there definitely can be active interference from the adversary and the system should be hardened to withstand that. Moreover, in security systems, more functionality implies more complex system and more security holes in the system. The steps to design security of a system is to model the system, identify the security properties to be preserved, model the adversary, and then ensure that the security properties are preserved under attacks. Detail modeling of the system and identification of the required security properties is possible. But it almost impossible to accurately model the adversaries and vulnerabilities of the system exploited by those adversaries. The result is that there nothing called “absolute security”. Thus to the designer, system security means: *under given assumptions about the system, no attack of a given form will destroy specified properties*. Thus system security in general and e-commerce security in particular is conceived of a *process* rather than a one-time developed *product*.

Security engineering life cycle

It is important to note that the e-commerce security need of an enterprise is dynamic rather than static and depends on the operational dynamics, shift or addition to business goals, technological advancement etc. Thereby, the process of designing and deploying an information security infrastructure is a continuous process of analysis, design, monitoring, and adaptation to changing needs. Often, the change in needs is frequent in the organizations.

Figure 5.2 Security engineering life cycle



In order to be survivable under such frequent changes, the process has to be developed from a life-cycle approach. This observation leads to the concept of "security engineering life-cycle". The security engineering life cycle consists of the following phases (figure 5.2):

- **Security requirement specification and risk analysis:** This is the first phase in the security engineering life cycle. It collects information regarding assets of the organization that need to be protected, threat perception on those assets, associated access control policies, existing operational infrastructure, connectivity aspects, services required to access the asset and the access control mechanism for the services.
- **Security policy specification:** This phase uses "security requirement specification" and "risk analysis report" as input and generates a set of e-commerce security policies. The policy statements are high-level rule-based and generic in nature, and, thereby, does not provide any insight to system implementation or equipment configuration.
- **Security infrastructure specification:** This phase analyses the "security requirement specification" and the "security policy specification" to generate a list of security tools that are needed to protect the assets. It also provides views on the location and purpose of the security tools.
- **Security infrastructure implementation**: The organization, in this phase, procures, deploys, and configures the selected security infrastructure at the system level.
- **Security testing:** In this phase, several tests are carried out to test the effectiveness of the security infrastructure, functionality of the access control mechanism, specified operational context, existence of known vulnerabilities in the infrastructure etc.
- **Requirement validation:** This phase analyses the extent of fulfillment of the security requirements of the e-commerce organization by the corresponding security policy and the implemented security infrastructure. Change in the business goal, operational environment, and technological advancement may lead to a fresh set of security requirements and thereby, triggering a new cycle of the "security engineering life cycle". Now, let us see the Security Requirements, Security Policy, Security Infrastructure, and Security Testing phases in greater detail.

Security requirements

During this phase, the security needs of an enterprise are identified. These needs are governed by the necessity to protect the following security attributes:

- ***Authentication:*** This is the ability to say that an electronic communication (whether via email or web) does genuinely come from who it claims to. Without face-to-face contact, passing oneself off as someone else is not difficult on the internet. Forging the "From:" field in an email header is a trivial matter, and far more sophisticated attacks are standard fare for hackers. In online commerce the best defense against being misled by an imposter is provided by unforgeable digital certificates from a trusted authority (such as VeriSign). Although anyone can generate digital certificates for them, a trusted authority demands real-world proof of identity and checks its validity before issuing a digital certificate. Only certificates from trusted authorities will be automatically recognized and trusted by the major web browser and email client software. Authentication can be provided in some situations by physical tokens (such as a drivers license), by a piece of information known only to the person involved (e.g. a PIN), or by a physical property of a person (fingerprints or retina scans). Strong authentication requires at least two or more of these. A digital certificate provides strong authentication as it is a unique token (the certificate itself) and requires a password (something known only to the owner) for its usage.

- ***Privacy:*** In online commerce, privacy is the ability to ensure that information is accessed and changed only by authorized parties. Typically this is achieved via encryption. Sensitive data (such as credit card details, health records, sales figures etc.) are encrypted before being transmitted across the open internet – via email or the web. Data which has been protected with strong 128-bit encryption may be intercepted by hackers, but cannot be decrypted by them within a short

time. Again, digital certificates are used here to encrypt email or establish a secure HTTPS connection with a web-server. For extra security, data can also be stored long-term in an encrypted format.

- ***Authorization:*** Authorization allows a person or computer system to determine if someone has the authority to request or approve an action or information. In the physical world, authentication is usually achieved by forms requiring signatures, or locks where only authorized individuals hold the keys. Authorization is tied with *authentication*. If a system can securely verify that a request for information (such as a web page) or a service (such as a purchase requisition) has come from a known individual, the system can then check against its internal rules to see if that person has sufficient authority for the request to proceed. In the online world, authorization can be achieved by a manager sending a digitally signed email (an email stamped by their personal digital certificate). Such an email, once checked and verified by the recipient, is a legally binding request for a service. Similarly, if a web-server has a restricted access area, the server can request a digital certificate from the user's browser to identify the user and then determine if they should be given access to the information according to the server's permission rules.

- ***Integrity:*** Integrity of information means ensuring that a communication received has not been altered or tampered with. Traditionally, this problem has been dealt with by having tight control over access to paper documents and requiring authorized officers to initial all changes made – a system with obvious drawbacks and limitations. If someone is receiving sensitive information online, he not onlywants to ensure that it is coming from who he expects it to (authentication), but also that it hasn't been intercepted by a hacker while in transit and its contents altered. The speed and distances involved in online communications requires a very different approach to this problem from traditional methods. One solution is afforded by using digital certificates to digitally "sign" messages. A travelling employee can send production orders with integrity to the central office by using their digital certificate to sign their email. The signature includes a hash of the original message – a brief numerical representation of the message content. When the recipient opens the message, his email software will automatically create a new hash of the message and will compare it against the one included in the digital signature. If even a single character has been altered in the message, the two hashes will differ and the software will alert the recipient that the email has been tampered with during transit.

- ***Non-repudiation:*** Non-repudiation is the ability to guarantee that once someone has requested a service or approved an action, they cannot turn around and say "I didn't do that!" Non-repudiation allows one to legally prove that a person has sent a specific email or made a purchase approval from a website. Traditionally non-repudiation has been achieved by having parties sign contracts and then have the contracts notarized by trusted third parties. Sending documents involved the use of registered mail, and postmarks and signatures to date-stamp and record the process of transmission and acceptance. In the realm of e-commerce, non-repudiation is achieved by using digital signatures. Digital signatures which have been issued by a trusted authority (such as VeriSign) cannot be forged and their validity can be checked with any major email or web browser software. A digital signature is only installed in the personal computer of its owner, who is usually required to provide a password to make use of the digital signature to encrypt or digitally sign their communications. If a company receives a purchase order via email which has been digitally signed, it has the same legal assurances as on receipt of a physical signed contract.

Security policy

The first step in securing an e-commerce venture is to formulate written security policies which clearly define the requirements for each component of the system (human, technological, legal) and how they interact. An organization's security policy defines its position on the protection of its physical and IT assets. It identifies the physical and intellectual property assets that are most valuable for the continued success of the company, and specifies how they should be protected. The security policy may cover issues like:

- What service types (e.g., web, FTP, SMTP) users may have access to
- What classes of information exist within the organization and which should be encrypted before being transmitted

- What client data does the organization hold? How sensitive is it? How is it to be protected?
- What class of employees may have remote access to the corporate network
- Roles and responsibilities of managers and employees in implementing the security policy
- How security breaches are to be responded to the security policy should also consider physical aspects of network security.
- Who has access to the corporate server?
- Is it in a locked environment or kept in an open office?
- What is the procedure for determining who should be given access?

The security policy regulates the activities of employees just as much as it defines how IT infrastructure will be configured. The policy should include details on how it is to be enforced and how individual responsibilities are determined. For it to be effective, the policy needs regular testing and review to judge the security measures. The review process needs to take into account any changes in technology or business practices which may have an influence upon security. Lastly, the policy itself needs to be regarded as a living document which will be updated at set intervals to reflect the evolving ways in which the business, customers and technology interact.

Security infrastructure

The security infrastructure is the implementation of the security policy. The security infrastructure is the technology which is chosen to secure the e-business and the rules by which it operates. Some examples of this include:

- enforcing password aging and expiration
- enforcing the complexity of passwords
- blocking prohibited outbound connections from the firewall
- requiring digital certificates to authenticate remote access connections to an organization's network
- requiring badges for physical access to building
- requiring all physical access to servers to be recorded in a written log

Again, the security infrastructure entails managing the behavior of both IT and human resources. It should be regularly policed:

- Who checks written logs?
- How often are firewall reports checked?

Finally, it must be enforced. The penalties for breaches of the security policy must be made clear to all employees and partners and must be enforced if policy requirements are broken or ignored.

Testing e-commerce security

The need for security testing of an organization arises due to two main factors. The primary factor is the importance of measuring the extent to which the security infrastructure implements the security policy and the security requirements of an organization. As the implementation of the security infrastructure needs human interventions, a proper security testing is needed to check out the existence of any "human error". The other factor is the vulnerability of the existing security infrastructure to the new threats and exploits. In recent years, the rate of arrival of new types of threat and new exploits has been alarming with respect to the information security context. This leads to the need for periodical security testing by which the vulnerability of the existing security infrastructure to the growing number of threats and exploits can be measured.

The main objective of security testing, therefore, includes

- Verification of the security requirement specification such as location of the asset(s), access control mechanism for the assets, operational context of the organization, existing system services and their access control mechanisms, and the connectivity within the organization and connectivity of the organization to the outside world
- Verification of the configuration of the security tools specified in the security infrastructure i.e. whether the security tools are properly installed and configured to maintain the security of the asset
- Verification of any gap between the proposed security infrastructure and the implemented security infrastructure
- Verification of the limitation of the proposed security infrastructure with respect to the known vulnerabilities

Thus, there are two aspects of testing – compliance checking and penetration testing.

Compliance checking: In compliance checking, it is seen whether the security infrastructure, that has been implemented, matches the security policy of the organization. A semi-automated tool can be used to match the policies with the existing infrastructure.

Penetration testing: In penetration testing, it is seen whether the existing security infrastructure of the organization is sufficient to ward off all possible security threats. Various automated and semi-automated security tools like Retina, Nessus etc. are available for penetration testing. They try and penetrate the organization's network and generate a report on the vulnerabilities and threats that are present in the network. The feedback from the testing phase is used to upgrade the security infrastructure and security policy of the organization. After that, the testing is carried out again. Thus, security engineering is an iterative and dynamic process where all the phases need to be carried out at regular intervals to ensure the security of an organization.

5.3 Check your Progress

1. Fill in the blanks.

a. A …….. policy provides an overriding constraint on the access of subjects to objects.

b. …….. policies allow the subjects in a computer system to specify who shall have access to information at their own discretion.

c. In compliance checking, it is seen whether the security infrastructure matches the ……..of the organization.

d. …… is access that occurs outside the security perimeter of the secure computer system.

5.4 ENCRYPTION

Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood. Imagine sending mail through the postal system in a clear envelope. Anyone with access to it can see the data. If it looks valuable, they might take it or change it. An SSL Certificate establishes a private communication channel enabling encryption of the data during transmission. Encryption scrambles the data, essentially creating an envelope for message privacy.
Each SSL Certificate consists of a public key and a private key. The public key is used to encrypt information and the private key is used to decipher it. When a Web browser points to a secured domain, a Secure Sockets Layer handshake authenticates the server (Web site) and the client (Web browser). An encryption method is established with a unique session key and secure transmission can begin. True 128-bit SSL Certificates enable every site visitor to experience the strongest SSL encryption available to them.

- **Conventional encryption**

The Conventional encryption was the only encryption available before the introduction of public key encryption. It is also called symmetric encryption or single key encryption. A conventional encryption scheme has five stages:

- Plain Text: It is the original message.
- Encryption Algorithm: It performs different transformations on the plain text.
- Secret Key: It is input to encryption algorithm.
- Cipher Text: It is the scrambled message as an output.
- Decryption Algorithm: It performs on cipher text and gives the original message as an output.

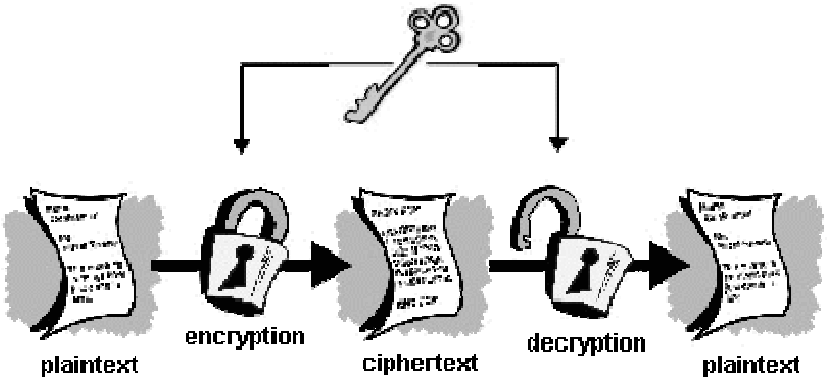


Figure 5.3 Conventional encryption

- **Public-Key encryption**

Cryptography is the process of protecting the integrity and accuracy of information by converting (encrypting) data into an unreadable format, called cipher text. Only those who possess a private key can decipher (decrypt) the message into plain text. Public key cryptography uses two keys, one public and one private, to encrypt and decrypt data, respectively. Generally, a designated authority issues this public–private key combination. The cryptographic certificates used with an e-check enable a check payee to determine the validity of the signature. Public key cryptography uses a pair of keys, one private and one public. In comparison, private key cryptography uses only one key for encryption. The advantage of the dual-key technique is that it allows the businesses to give away their public key to anyone who wants to send a message (sending a credit card number, for example). The sender can then encrypt the message with the public key and send it to the intended businessperson over the Internet or any other public network; the businessperson can then use the private key to decrypt the message. Naturally, the private key is not publicly known.

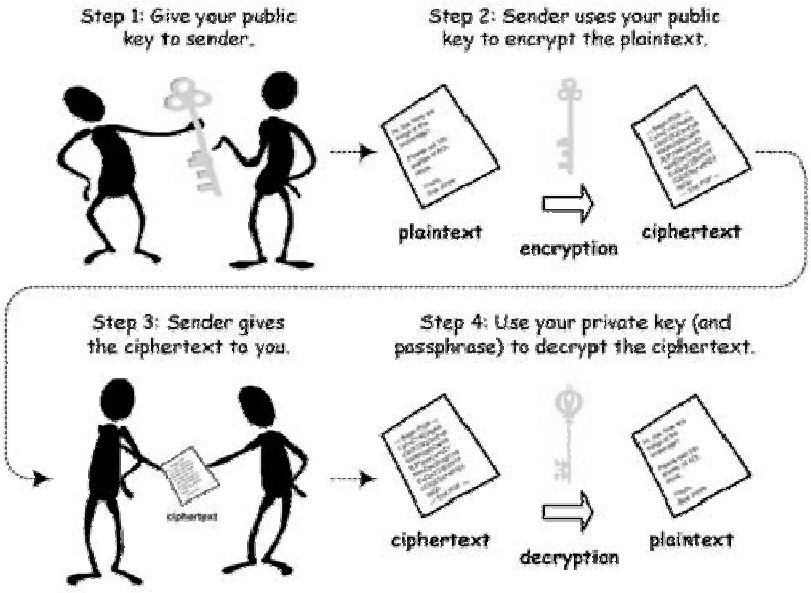


Figure 5.4 Asymmetric/Public-key encryption

It is also known as **asymmetric-key** encryption, public-key encryption uses two different keys at once -- a combination of a private key and a public key. The private key is known only to your computer, while the public key is given by your computer to any computer that wants to communicate securely with it. To decode an encrypted message, a computer must use the public key, provided by the originating computer, and its own private key. Although a message sent from one computer to another won't be secure since the public key used for encryption is published and available to anyone, anyone who picks it up can't read it without the private key. The key pair is based on prime numbers (numbers that only have divisors of itself and one, such as 2,

3, 5, 7, 11 and so on) of long length. This makes the system extremely secure, because there is essentially an infinite number of prime numbers available, meaning there are nearly infinite possibilities for keys. One very popular public-key encryption program is **Pretty Good Privacy (PGP)**, which allows you to encrypt almost anything.

Following table gives the difference between conventional and public-key encryption systems.

Table 5.2 Encryption Systems

Conventional encryption	Public-key encryption
The same algorithm with the same key can be used for encryption and decryption.	One algorithm is used for encryption and decryption with a pair of keys, one for encryption, and one for decryption.
The sender and receiver must share the algorithm and the key.	The sender and receiver must each have one of the matched pair of keys.
The key must be kept secret.	One of the two keys must be kept secret.
It must be impossible or at least impractical to decipher a message if no other information is available.	It must be impossible or at least impractical to decipher a message if no other information is available.
Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key	Knowledge of the algorithm plus one of the keys plus a sample of the ciphertext must be insufficient to determine the other key.

5.5 MASTER CARD / VISA TRANSACTION

In August 1996, MasterCard and Visa agreed to jointly develop the Secure Electronic Transaction (SET) Specification. SET aims at achieving secure, cost-effective, on-line transactions that will satisfy market demand in the development of a single, open industry specification. Visa and MasterCard have jointly developed the SET protocol as a method to secure payment card transactions over open networks. SET is being published as open specifications for the industry. These specifications are available to be applied to any payment service and may be used by software vendors to develop applications. Key additional participants are GTE, IBM, Microsoft, Netscape, SAIC, Terisa, and VeriSign.

- **Introduction**

Impact of electronic commerce

There is no question that electronic commerce, as exemplified by the popularity of the Internet, is going to have an enormous impact on the financial services industry. No financial institution will be left unaffected by the explosion of electronic commerce.

- The number of payment card purchases made through this medium will grow as Internet-based on-line ordering systems are created.
- Many banks are planning to support this new form of electronic commerce by offering card authorizations directly over the Internet.
- Several trials with electronic currency and digital cash are already under-way.

Projected use

With more than 30 million users in 1998, and 90 million projected to come on board in the next two years, the Internet is a new way for businesses to establish computer-based resources that can be accessed by consumers as well as business partners around the world.

Internet

The Internet is changing the way we access and purchase information, communicate and pay for services, and acquire and pay for goods. Financial

services such as bill payment, brokerage, insurance and home banking are now or soon will be available over the Internet. Any organization can become a global publisher by establishing an information site on the Internet's World Wide Web.

World Wide Web

The Web can display text, sound, images and even video, allowing merchants to transmit information directly to potential consumers around the world around the clock.

Consumer payment devices

With open networks, payments will increasingly be made by consumer- driven devices. As advanced technologies become more practical and affordable, the marketplace will move from 'brick and mortar' to more convenient locations such as the home or office. As financial services evolve, consumers will consolidate their payment needs into one multifunctional relationship product that enables widespread, around-the-clock access.

Publicity

Recently, an explosion of publicity has heralded the growth of the Internet and the possibilities for consumers and merchants to create a new type of shopping called *electronic commerce.* The publicity has focused on three areas:

- Marketing opportunities to develop new ways *to* browse, select and pay for goods and services to on-line consumers,
- New products and services, and
- Security risks associated with sending unprotected financial information across public networks.

All areas must be addressed to facilitate the future growth of payment card transaction volume in the electronic marketplace.

Role of payment systems

Payment systems and their financial institutions will play a significant role by establishing open specifications for payment card transactions that:

- Provide for confidential transmission,
- Authenticate the parties involved,
- Ensure the integrity of payment instructions for goods and services order data, and
- Authenticate the identity of the cardholder and the merchant to each other.

Procedures needed

Because of the anonymous nature of communications networks, procedures must be developed to substitute for existing procedures used in face-to-face or mail order/telephone order (MOTO) transactions including the authentication of the cardholder by the merchant. There is also a need for the cardholder to authenticate that the merchant accepts SET transactions and is authorized to accept payment cards.

Use of payment card products

Financial institutions have a strong interest in accelerating the growth of electronic commerce. Although electronic shopping and ordering does not require electronic payment, a much higher percentage of these transactions use payment card products instead of cash or checks. This will hold true both in the consumer marketplace and in the commercial marketplace.

Purpose of Secure Electronic Transaction

To meet these needs, the *Secure Electronic Transaction* (SET) protocol uses cryptography to:

- Provide confidentiality of information.
- Ensure payment integrity, and
- Authenticate both merchants and cardholders.

These specifications will enable greater payment card acceptance, with a level of security that will encourage consumers and businesses to make wider use of payment card products in this emerging market.

- **Requirements**

The following business requirements for secure payment processing with credit cards over the Internet and other networks:

- Provide confidentiality of payment and ordering information: It is necessary to assure cardholders that this information is safe and accessible only to the intended recipient. Confidentiality also reduces the risk of fraud by either party to the transaction or by malicious third parties. SET uses encryption to provide confidentiality.
- Ensure the integrity of all transmitted data: That is, ensure that no changes in content occur during transmission of SET messages. Digital signatures are used to provide integrity.
- Provide authentication that a cardholder is a legitimate user of a credit card account: A mechanism that links a cardholder to a specific account number reduces the incidence of fraud and the overall cost of payment processing. Digital signatures and certificates are used to verify that a cardholder is a legitimate user of a valid account.
- Provide authentication that a merchant can accept credit card transactions through its relationship with a financial institution: This is the complement to the preceding requirement. Cardholders need to be able to identify merchants with whom they can conduct secure transactions. Again, digital signatures and certificates are used.
- Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction: SET is a well-tested specification based on highly secure cryptographic algorithms and protocols.
- Create a protocol that neither depends on transport security mechanisms nor prevents their use: SET can securely operate over a "raw" TCP/IP stack. However, SET does not interfere with the use of other security mechanisms, such as IPSec and SSL/TLS.
- Facilitate and encourage interoperability among software and network providers: The SET protocols and formats are independent of hardware platform, operating system, and Web software.

- **Features**

Features of the specifications

These requirements are addressed by the following features of these specifications:

- Confidentiality of information
- Integrity of data
- Cardholder account authentication
- Merchant authentication
- Interoperability

For the sake of clarity, each of these features has been described as a distinct component. It should be noted, however, that these elements do not function independently; all security functions must be implemented.

Confidentiality of Information

To facilitate and encourage electronic commerce using payment card products, it will be necessary to assure cardholders that their payment information is safe and accessible only *by the* intended recipient. Therefore, cardholder account and payment information must be secured as it travels across the network, preventing interception of account numbers and expiration dates by unauthorized individuals.

- *On-line shopping:* In today's on-line shopping environment, payment instructions containing account information are often transmitted from cardholders to merchants over open networks with little or no security precautions. However, this account information provides the key elements needed to create counterfeit cards or fraudulent transactions.

- *Fraud:* While it is possible to obtain account information in other environments, there is a heightened concern about the ease of doing so with public network transactions. This concern reflects the potential for high volume fraud, automated fraud (such as using filters on all messages passing over a network to extract all payment card account numbers out of a data stream), and the potential for 'mischievous fraud that appears to be characteristic of some hackers.

Integrity of data

The specifications must guarantee that message content is not altered during the transmission between originator and recipient. Payment information sent from cardholders to merchants includes order information, personal data and payment instructions. If any component is altered in transit, the transaction will not be processed accurately In order to eliminate this potential source of fraud and/or error; SET must provide the means to ensure that the contents of all order and payment messages received match the contents of messages sent.

Cardholder account authentication

Merchants need a way to verify that a cardholder is a legitimate user of a valid branded payment card account number. A mechanism that uses technology to link a cardholder to a specific payment card account number will reduce the incidence of fraud and therefore the overall cost of payment processing. These specifications define the mechanism to verify that a cardholder is a legitimate user of a valid payment card account number.

Merchant authentication

The specifications must provide a way for cardholders to confirm that a merchant has a relationship with a financial institution allowing it to accept payment cards. Cardholders also need to be able to identify merchants with whom they can securely conduct electronic commerce.

Inlet-operability

The specifications must be applicable on a variety of hardware and software platforms and must include no preference for one over another. Any cardholder with compliant software must be able to communicate with any merchant software that also meets the defined standard.

- **Scope**

Use of payment cards

The SET specifications address a portion of the message protocols that are necessary for electronic commerce. It specifically addresses those parts of the protocols that use or impact the use of payment cards.

Within the scope

The following are within the scope of these specifications:

- Application of cryptographic algorithms (such as RSA and DES)
- Certificate message and object formats
- Purchase messages and object formats
- Authorization messages and object formats
- Capture messages and object formats
- Message protocols between participants

Outside the scope

The following are outside the scope of the set specifications:

- Message protocols for offers, shopping, delivery of goods. etc.
- Operational issues such as the criteria set by individual financial institutions for the issuance of cardholder and merchant certificates
- Screen formats including the content, presentation and layout of order entry forms as defined by each merchant
- General payments beyond the domain of payment cards
- Security of data on cardholder, merchant, and payment gateway systems including protection from viruses. trojan horse programs, and hackers

- **Concepts**

Interaction of participants

SET changes the way that participants in the payment system interact. In a face-to-face retail transaction or mail order transaction, the electronic processing of the transaction begins with the merchant or the acquirer. However in SET transaction, the electronic processing of the transaction begins with the cardholder,

Cardholder

In the electronic environment, consumers and corporate purchasers interact with merchants from personal computers over the Internet. A cardholder is an authorized holder of a payment card (e.g., MasterCard, Visa) that has been issued by an issuer.

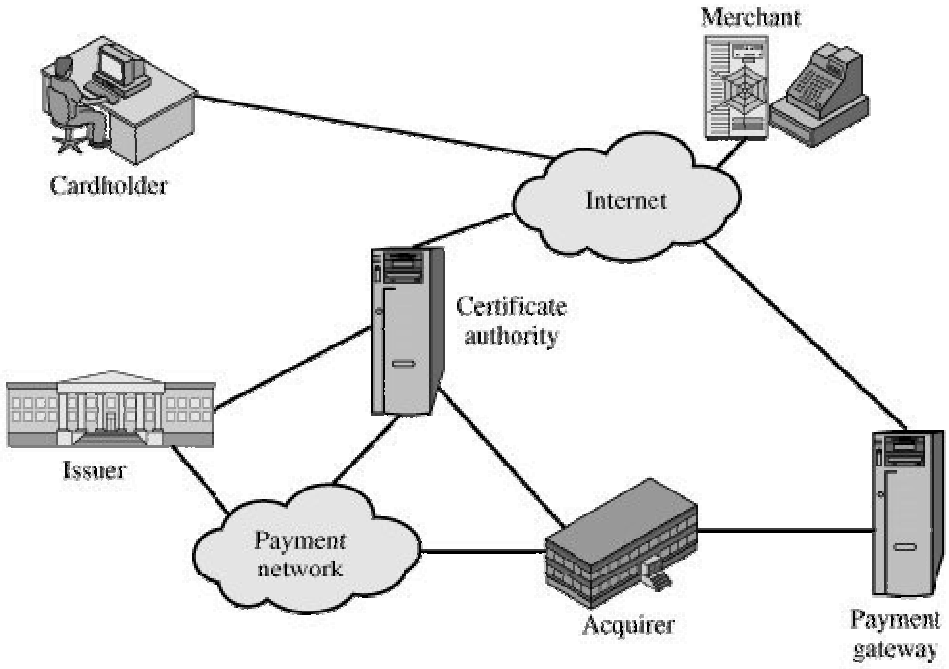


Figure 5.5 Secure Electronic Commerce components

Merchant

A merchant is a person or organization that has goods or services to sell to the cardholder. Typically, these goods and services are offered via a Web site or by electronic mail. A merchant that accepts payment cards must have a relationship with an acquirer.

Issuer

This is a financial institution, such as a bank, that provides the cardholder with the payment card. Typically, accounts are applied for and opened by mail or in person. Ultimately, it is the issuer that is responsible for the payment of the debt of the cardholder.

Acquirer

This is a financial institution that establishes an account with a merchant and processes payment card authorizations and payments. Merchants will usually accept more than one credit card brand but do not want to deal with multiple bankcard associations or with multiple individual issuers. The acquirer provides authorization to the merchant that given cards account is active and that the proposed purchase does not exceed the credit limit. The acquirer also provides electronic transfer of payments to the merchant's account. Subsequently, the acquirer is reimbursed by the issuer over some sort of payment network for electronic funds transfer.

Payment gateway

This is a function operated by the acquirer or a designated third party that processes merchant payment messages. The payment gateway interfaces between SET and the existing bankcard payment networks for authorization and payment functions. The merchant exchanges SET messages with the payment gateway over the Internet, while the payment gateway has some direct or network connection to the acquirer's financial processing system.

Certification authority (CA)

This is an entity that is trusted to issue X.509v3 public-key certificates for cardholders, merchants, and payment gateways. The success of SET will depend on the existence of a CA infrastructure available for this purpose. As discussed earlier, a hierarchy of CAs is used, so that participants need not be directly certified by a root authority.

Kinds of Shopping

- **Variety of experiences**

  There are many ways that cardholders will shop. This section describes two ways. The SET protocol supports each of these shopping experiences and should support others as they are defined.

- **On-line catalogues**

  The growth of electronic commerce can largely be attributed to the popularity of the World Wide Web. Merchants can tap into this popularity by creating virtual storefronts on the Web that contain on-line catalogues. These catalogues can be quickly updated as merchant's product offerings change or to reflect seasonal promotions.

Cardholders can visit these Web pages selecting items for inclusion on an order. Once the cardholder finishes shopping, the merchant's Web server can send a completed order form for the cardholder to review and approve.

Once the cardholder approves the order and chooses to use a payment card, the SET protocol provides the mechanisms for the cardholder to securely transmit payment instructions as well as for the merchant to obtain authorization and receive payment for the order.

- **Electronic catalogues**

  Merchants may distribute catalogues on electronic media such as diskettes or CD-ROM. This approach allows the cardholder to browse through merchandise off-line. With an on-line catalogue, the merchant has to be concerned about bandwidth and may choose to include fewer graphics or reduce the resolution of the graphics. By providing an off- line catalogue, such constraints are significantly reduced.

In addition, the merchant may provide a custom shopping application tailored to the merchandise in the electronic catalogue. Cardholders will shop by browsing through the catalogue and selecting items to include on an order.

Once the cardholder approves the order and chooses to use a payment card, an electronic message using the SET protocol can be sent to the merchant with the order and payment instructions. This message can be delivered on-line, such as to the merchant's Web page, or sent via a store-and-forward mechanism, such as electronic mail.

5.4, 5.4 & 5.5 Check your Progress

1. Fill in the blanks

a. Encryption is the conversion of data into a form, called……..that cannot be easily understood by unauthorized people.

b. ……is the process of converting encrypted data back into its original form, so it can be understood.

c. Public-key encryption uses two different keys at once, a combination of a …… and a ……

2. Match the following

Column A	Column B
a. Cardholder	1. Establishes an account with merchant
b. Merchant	2. Provides the payment card
c. Issuer	3. Issue X.509v3 public-key certificates
d. Acquirer	4. Process merchant payment messages
e. Payment Gateway	5. Authorized holder of a payment card
f. Certification Authority	6. Has goods or services to sell

5.6 PAYMENT PROCESSING

Table 5.3 lists the transaction types supported by SET. In what follows we look in some detail at the following transactions:

- Purchase request
- Payment authorization
- Payment capture

Table 5.3 SET Transaction Types

Cardholder registration	Cardholders must register with a CA before they can send SET messages to merchants.
Merchant registration	Merchants must register with a CA before they can exchange SET messages with customers and payment gateways.
Purchase request	Message from customer to merchant containing OI for merchant and PI for bank.
Payment authorization	Exchange between merchant and payment gateway to authorize a given amount for a purchase on a given credit card account.
Payment capture	Allows the merchant to request payment from the payment gateway.
Certificate inquiry and status	If the CA is unable to complete the processing of a certificate request quickly, it will send a reply to the cardholder or merchant indicating that the requester should check back later. The cardholder or merchant sends the Certificate Inquiry message to determine the status of the certificate request and to receive the certificate if the request has been approved.
Purchase inquiry	Allows the cardholder to check the status of the processing of an order after the purchase response has been received. Note that this message does not include information such as the status of back ordered goods, but does indicate the status of authorization, capture and credit processing.
Authorization reversal	Allows a merchant to correct previous authorization requests. If the order will not be completed, the merchant reverses the entire authorization. If part of the order will not be completed, the merchant reverses part of the amount of the authorization.

Table 5.3 SET Transaction Types	
Cardholder registration	Cardholders must register with a CA before they can send SET messages to merchants.
Capture reversal	Allows a merchant to correct errors in capture requests such as transaction amounts that were entered incorrectly by a clerk.
Credit	Allows a merchant to issue a credit to a cardholder's account such as when goods are returned or were damaged during shipping. Note that the SET Credit message is always initiated by the merchant, not the cardholder. All communications between the cardholder and merchant that result in a credit being processed happen outside of SET.
Credit reversal	Allows a merchant to correct a previously request credit.
Payment gateway certificate request	Allows a merchant to query the payment gateway and receive a copy of the gateway's current key-exchange and signature certificates.
Batch administration	Allows a merchant to communicate information to the payment gateway regarding merchant batches.
Error message	Indicates that a responder rejects a message because it fails format or content verification tests.

- **Purchase Request**

Before the Purchase Request exchange begins, the cardholder has completed browsing, selecting, and ordering. The end of this preliminary phase occurs when the merchant sends a completed order form to the customer. All of the preceding occurs without the use of SET.

The purchase request exchange consists of four messages: Initiate Request, Initiate Response, Purchase Request, and Purchase Response.

In order to send SET messages to the merchant, the cardholder must have a copy of the certificates of the merchant and the payment gateway. The customer requests the certificates in the Initiate Request message, sent to the merchant. This message includes the brand of the credit card that the customer is using. The message also includes an ID assigned to this request/response pair by the customer and a nonce used to ensure timeliness.

The merchant generates a response and signs it with its private signature key. The response includes the nonce from the customer, another nonce for the customer to return in the next message, and a transaction ID for this purchase transaction. In addition to the signed response, the Initiate Response message includes the merchant's signature certificate and the payment gateway's key exchange certificate.

The cardholder verifies the merchant and gateway certificates by means of their respective CA signatures and then creates the OI and PI. The transaction ID assigned by the merchant is placed in both the OI and PI. The OI does not contain explicit order data such as the number and price of items. Rather, it contains an order reference generated in the exchange between merchant and customer during the shopping phase before the first SET message. Next, the cardholder prepares the Purchase Request message (Figure 5.6). For this purpose, the cardholder generates a one-time symmetric encryption key, K_s. The message includes the following:

1. Purchase-related information. This information will be forwarded to the payment gateway by the merchant and consists of

    - The PI
    - The dual signature, calculated over the PI and OI, signed with the customer's private signature key
    - The OI message digests (OIMD)

The OIMD is needed for the payment gateway to verify the dual signature, as explained previously. All of these items are encrypted with K_s. The final item is

- The digital envelope. This is formed by encrypting K_s with the payment gateway's public key-exchange key. It is called a digital envelope because this envelope must be opened (decrypted) before the other items listed previously can be read.

The value of K_s is not made available to the merchant. Therefore, the merchant cannot read any of this payment-related information.

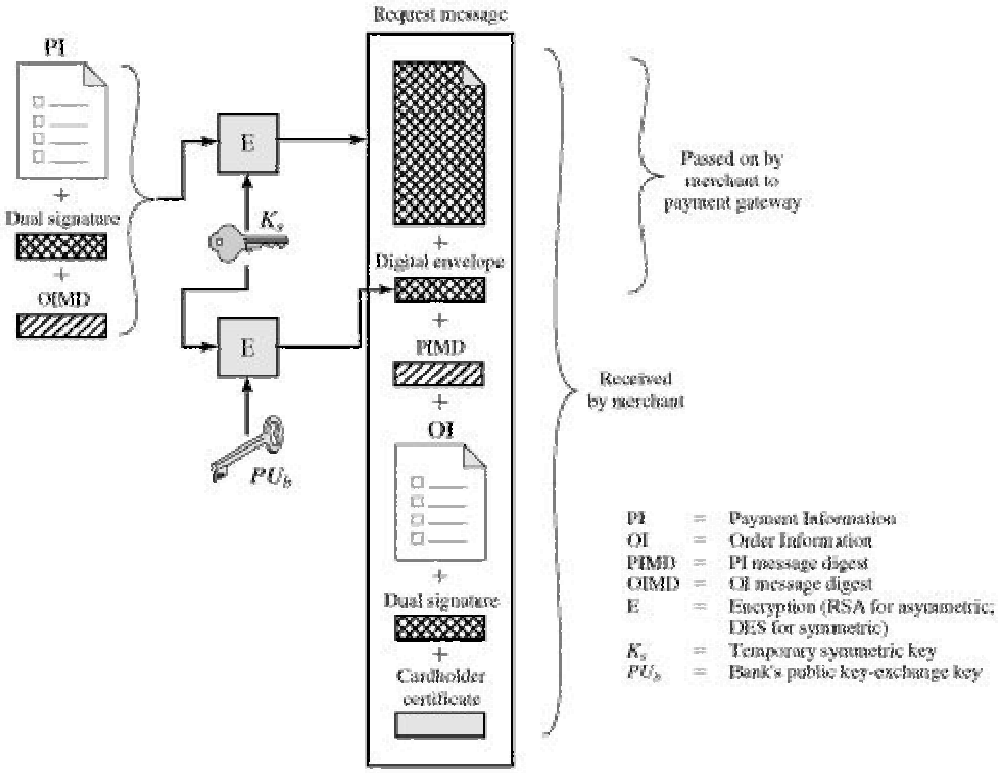
2. Order-related information. This information is needed by the merchant and consists of

   - The OI
   - The dual signature, calculated over the PI and OI, signed with the customer's private signature key
   - The PI message digest (PIMD)

3. The PIMD is needed for the merchant to verify the dual signature. Note that the OI is sent in the clear.

4. Cardholder certificate. This contains the cardholder's public signature key. It is needed by the merchant and by the payment gateway.

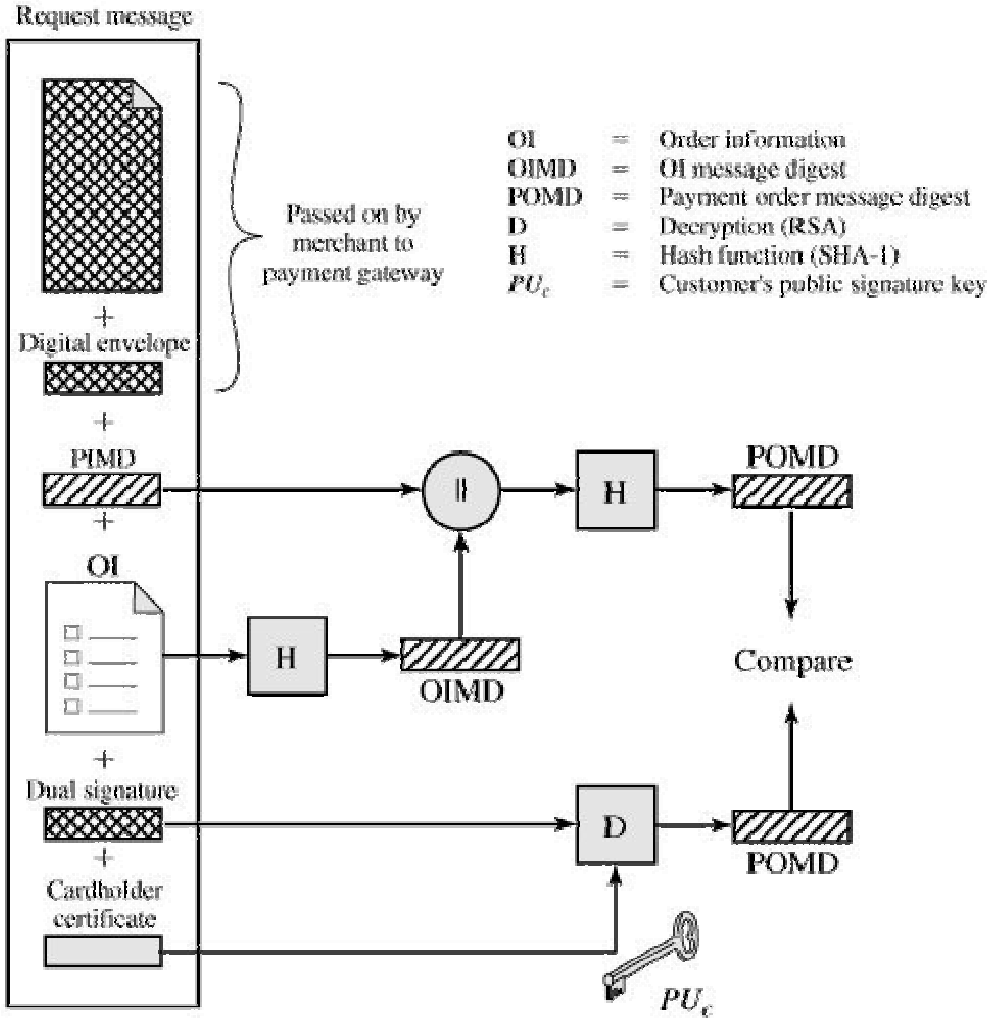
Figure 5.6 Cardholder Sends Purchase Request



When the merchant receives the Purchase Request message, it performs the following actions (Figure 5.7):

1. Verifies the cardholder certificates by means of its CA signatures.
2. Verifies the dual signature using the customer's public signature key. This ensures that the order has not been tampered with in transit and that it was signed using the cardholder's private signature key.
3. Processes the order and forwards the payment information to the payment gateway for authorization (described later).
4. Sends a purchase response to the cardholder.

Figure 5.7 Merchant Verifies Customer Purchase Request



The Purchase Response message includes a response block that acknowledges the order and references the corresponding transaction number. This block is signed by the merchant using its private signature key. The block and its signature are sent to the customer, along with the merchant's signature certificate.

When the cardholder software receives the purchase response message, it verifies the merchant's certificate and then verifies the signature on the response block. Finally, it takes some action based on the response, such as displaying a message to the user or updating a database with the status of the order.

- **Payment Authorization**

During the processing of an order from a cardholder, the merchant authorizes the transaction with the payment gateway. The payment authorization ensures that the transaction was approved by the issuer. This authorization guarantees that the merchant will receive payment; the merchant can therefore provide the services or goods to the customer. The payment authorization exchange consists of two messages: Authorization Request and Authorization response.

The merchant sends an Authorization Request message to the payment gateway consisting of the following:

1. Purchase-related information. This information was obtained from the customer and consists of
   - The PI
   - The dual signature, calculated over the PI and OI, signed with the customer's private signature key
   - The OI message digests (OIMD)
   - The digital envelope

2. Authorization-related information. This information is generated by the merchant and consists of

   - An authorization block that includes the transaction ID, signed with the merchant's private signature key and encrypted with a one-time symmetric key generated by the merchant
   - A digital envelope. This is formed by encrypting the one-time key with the payment gateway's public key-exchange key.

3. Certificates. The merchant includes the cardholder's signature key certificate (used to verify the dual signature), the merchant's signature key certificate (used to verify the merchant's signature), and the merchant's key-exchange certificate (needed in the payment gateway's response).

The payment gateway performs the following tasks:

1. Verifies all certificates
2. Decrypts the digital envelope of the authorization block to obtain the symmetric key and then decrypts the authorization block
3. Verifies the merchant's signature on the authorization block
4. Decrypts the digital envelope of the payment block to obtain the symmetric key and then decrypts the payment block
5. Verifies the dual signature on the payment block
6. Verifies that the transaction ID received from the merchant matches that in the PI received (indirectly) from the customer
7. Requests and receives an authorization from the issuer

Having obtained authorization from the issuer, the payment gateway returns an Authorization Response message to the merchant. It includes the following elements:

1. Authorization-related information. Includes an authorization block, signed with the gateway's private signature key and encrypted with a one-time symmetric key generated by the gateway. Also includes a digital envelope that contains the one-time key encrypted with the merchants public key-exchange key.
2. Capture token information. This information will be used to effect payment later. This block is of the same form as (1), namely, a signed, encrypted capture token together with a digital envelope. This token is not processed by the merchant. Rather, it must be returned, as is, with a payment request.
3. Certificate. The gateway's signature key certificate.

With the authorization from the gateway, the merchant can provide the goods or service to the customer.

- **Payment Capture**

To obtain payment, the merchant engages the payment gateway in a payment capture transaction, consisting of a capture request and a capture response message.

For the Capture Request message, the merchant generates, signs, and encrypts a capture request block, which includes the payment amount and the transaction ID. The message also includes the encrypted capture token received earlier (in the Authorization Response) for this transaction, as well as the merchant's signature key and key-exchange key certificates.

When the payment gateway receives the capture request message, it decrypts and verifies the capture request block and decrypts and verifies the capture token block. It then checks for consistency between the capture request and capture token. It then creates a clearing request that is sent to the issuer over the private payment network. This request causes funds to be transferred to the merchant's account.

The gateway then notifies the merchant of payment in a Capture Response message. The message includes a capture response block that the gateway signs and

encrypts. The message also includes the gateway's signature key certificate. The merchant software stores the capture response to be used for reconciliation with payment received from the acquirer.

4.6 Check your Progress
Answer the following

a. Write any four transaction types supported by SET.

……

……

5.7 SUMMARY

An introduction to Internet security issues the cost of security attacks, common threats and vulnerabilities, security controls, and resources discussed in more detail, Computer security attacks cost as much as $10 billion a year. An attack can damage data integrity, confidentiality or availability. Organizations must understand the potential costs: Vulnerabilities exist in all computer systems and all Internet services (SMTP, Telnet, FTP, HTTP, etc.). Email can be intercepted or spoofed. In Email spoofing an attacker assumes a false identity to solicit information or access. Hackers also exploit root compromises on old systems, poor passwords, IP spoofing, miss-configured networks, and packet sniffers. Internal attacks represent even more danger: over 80% of all break-ins come from internal staff or staff that has recently left an organization. Internet security starts with proper administrative and physical security. Firewalls and bastion hosts should be employed where necessary. Administrators should monitor and log all activity. For mail threats, an organization may consider authentication and/or encryption technologies.

System administrators should stay current on system vulnerabilities and controls. Resources include "double- edged swords" such as SATAN, ISS, and hacker discussion lists, as well as "lifeguards": CERT, FIRST, CIAC, NIST, COAST, and the many World-Wide-Web sites devoted to security issues. Organizations must understand security issues. They must stay current on tools (such as SATAN), security user groups, hacker web sites and liability issues. Still, the technological approach must reflect business needs: ease of use, industry standards, employee skill-sets, etc. To determine security needs, an organization can run a risk assessment workshop.

Based on an understanding of Internet risks, an organization can implement any of a number of security architectures. These can incorporate router controls, firewalls, authentication and encryption, and a number of other technologies. An organization should secure both its LAN and its Internet server. With the Internet, security policy and technology must reflect distributed computing. More entrances equal more risk. Both host-based (network) security and perimeter (firewall) security are essential. Firewalls should deny all access except that explicitly allowed. Similarly, hosts should provide no services except those explicitly intended.

Interactive Internet sites require secure methods for transferring data and financial transactions. The solutions include encryption and digital signature technology and policy initiatives such as Certificate Authorities and SET. The new paradigm of the Internet is the "active" interactive page. This increases the risk to users of encountering malicious code (viruses), tampered code, unknown authors and impersonations. Authentication and encryption are the key to secure data transmission, whether code, Email, or financial transactions.
One initiative to ensure data authentication is the Certificate Authority (CA) system. CA's are established organizations that verify a software publisher's identity. To apply for a certificate, a software publisher agrees to meet the CA's policies and submits the public key of its public/private key encryption. The CA publishes the public key and issues an identifying certificate that can be applied to an unlimited amount of code or other electronic items until it expires or is revoked. VeriSign was the first CA. GTE, AT&T and the United State Postal Service are in the process of becoming CAs.
In addition to ensuring secure transmission of code, major financial and software companies (Microsoft, Visa, and MasterCard) are designing means to ensure financial transmissions. The SET standard (a merging of STT and SEPP) is a universal

comprehensive bankcard payment protocol. SET uses message-based encryption to allow multi-party transactions, multiple transports (Email), and secure interaction.
As a result, organizations of all sizes should deploy a secure Web gateway that will protect against Web exploits in real time, will use both cloud-based and local content analysis techniques, provide granular policy management and application controls, integrate with messaging security capabilities, and provide support to users who access the Web and Web-based applications on mobile devices.

Source : *www.a3webtech.com (link)*

5.8 CHECK YOUR PROGRESS - *ANSWERS*

5.1 & 5.2

1.

a) Firewall Software
b) Active content
c) HTTP requests
d) Common gateway interface (CGI)

5.3

1.

a) Mandatory access control
b) Discretionary access control
c) Security policy
d) Indirect access

5.4 & 5.5

1.

a) A cipher text
b) Decryption
c) Private and Public

2.

a-5
b-6
c-2
d-1
e-4
f-3

5.6

1.

a) Cardholder registration, Merchant registration, Purchase request, Payment authorization, Payment capture, Certificate inquiry and status, Purchase inquiry, Credit.

5.9 QUESTIONS FOR SELF-STUDY

1. What is the need for computer security? Explain.
2. Write a short note on Active and Passive threats.
3. Discuss policy issues to implement in e-commerce security.
4. Explain with diagram security engineering life cycle.
5. What are the security requirements? Explain security policy.
6. What is encryption? Explain its types.
7. What is the difference between conventional encryption and public-key encryption?
8. What are the business requirements in MasterCard / Visa secure electronic transaction?
9. What are the payment system participants?
10. What is payment processing? How it works? Explain in detail.

5.10 SUGGESTED READINGS

Web Commerce Technology Handbook By Daniel Minoli Emma Minoli

NOTES

Chapter 6

LAW RELATED TO IT ACT

6.0 OBJECTIVES

After studying this chapter you will be able to :

- discuss the basic concepts of mobile computing.
- explain wireless computing concepts as it is an emerging technology.
- describe the different legal aspects of e-commerce.

6.1 INTRODUCTION

The use of mobile technologies is steadily on the increase, for both e-commerce and personal use. Mobile phones are a common sight today and many people own personal information management (PIM) devices or handheld computers, where they manage their schedule, contacts, and other essential functions. Employees on the move appreciate the value of staying connected with their enterprise and other resources through mobile phones. Most enterprises now have corporate mobile phone plans that make it easier for mobile employees to stay in touch and increase productivity.

With rapidly advancing technologies, most wireless carriers today offer transmission of data in addition to voice signals. For example, you can now receive e-mail on your mobile phone in addition to regular calls. With the growing proliferation of wireless enabled Personal Digital Assistants (PDAs), Blackberry mobile e-mail devices, and notebook PCs, it is all the more important to ensure that the mobile employees are connected to, and supported by, the enterprise. Although the terms “mobile” and “wireless” are often used interchangeably, they are two different things:

- Mobile devices are portable, electronic components that are used by mobile people to do their work.
- Mobile pertains to the ability of an entity to be on the move.
- Wireless pertains to the technology that allows transmission of voice, data, and other content through radio waves over the air, not restricted to physical cables or other physical mediums.

It is wireless technology that facilitates employee or enterprise mobility. Mobile devices depend on wireless technology to connect to the enterprise and conduct transfer of content in order to fulfill the users’ e-commerce needs.

It is not surprising that an increasing number of employees are demanding mobile support from their enterprise in order to maximize performance. Without a proper mobile strategy in place, most enterprises will fail to meet their cost and performance objectives. In fact, recent studies have shown that mobile employees connected to the enterprise are much more effective than if their enterprise did not support a mobile workplace. For employees whose work is mostly away from their desktops, this is an important issue.

Mobile employees have a long list of enterprise capabilities needed to support their work.
Here are some basic requirements:

- Adequate protection of information on wireless devices to ensure that confidential business information is not lost or stolen
- Wireless connection to enterprise assets using laptops, PDAs, mobile phones, and other devices for flexible access to business processes
- Mobile connection via laptops so that work can be done from anywhere
- Real-time synchronization of information to ensure accuracy and consistency
- Ability to receive appropriate alerts and messages to the mobile device in order to carry out required job functions with optimal efficiency.

The expectations previously listed are quite typical, and today's mobile infrastructure is able to deliver them with significant success. The wireless industry is continually evolving, with new developments springing up at an accelerated pace.

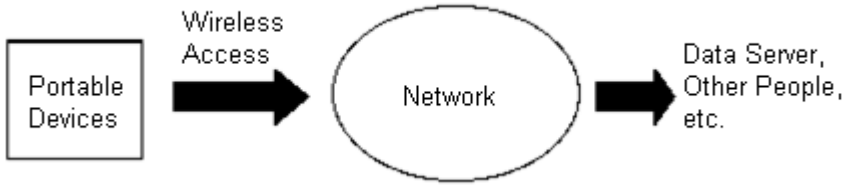
The line between computing and telephony is slowly blurring. Devices that combine the features of mobile phones and PDAs are becoming quite popular in the market today. Eventually, it will be one combined device you carry—where you do your scheduling, email, Web surfing, videoconferences, document management, and take all your business and personal calls. This would be a true all-around utility device. With data storage capabilities and network bandwidth steadily improving, it won't be long before you have the capabilities of a currently available high-end desktop computer available in a device that fits into your pocket. One can only speculate the ramifications this convergence of devices will have on the way you work and how enterprises will function.

6.2 BASICS OF MOBILE COMPUTING

The first phase was to make computers small enough so they can be easily carried i.e. Mobile devices. The second solution to the need for mobile computing was to replace wires with wireless communication media. The third phase was a combination of the first two, namely to use mobile devices in a wireless environment. Referred to as wireless mobile computing, this combination enables real-time connections between mobile devices and other computing environments.

In the traditional computing environment it was necessary to come to the computer to do some work on it. All computers were connected to each other, to networks, servers, etc. via wires.

Figure 6.1 Basic mobile computing environment



Mobile computing is associated with the mobility of hardware, data and software in computer applications. The study of this new area of computing has prompted the need to rethink carefully about the way in which mobile network and systems are conceived. Even though mobile and traditional distributed systems may appear to be closely related, there are a number of factors that differentiate the two, especially in terms of type of device (fixed/mobile),network connection (permanent/intermittent) and execution context (static/dynamic) Specialized class of distributed systems where some nodes can disengage from joint distributed operations, move freely in the physical space an reconnect to a possibly different segment of a computer network at a later stage in order to resume suspended activities. In short, Mobile computing is a generic term that refers to technologies that allow you to take your computer with you. In the past, this was limited to notebook computers and similar hardware that allowed you to physically bring your computer along. Today, however, this can be extended to software and web solutions that allow you to bring your computing experience without the bulky hardware.

There are three basic genres of mobile computing. The first uses mobile computers. These are computers or similar devices that are designed for mobile use.

They include notebooks, PDAs, and mobile phones. The second genre is remote connection. This type of mobility allows you to connect to your computer from remote locations and work as though you were sitting in front of it. The final type of technology is known as Desktop Virtualization. With this technology you take your software with you and recreate your computing experience on any available hardware.

- **Basic Terminology**

  - Personal digital assistant (PDA). A small portable computer, such as Palm handhelds and Pocket PC devices.
  - Short Message Service (SMS). A technology, in existence since 1991, that allows sending short text messages.
  - Enhanced Messaging Service (EMS). An extension of SMS that is capable of simple animation, tiny pictures, and short melodies.
  - Multimedia Messaging Service (MMS). The next generation of wireless messaging, this technology will be able to deliver rich media
  - Wireless Application Protocol (WAP). A technology that offers Internet browsing from wireless devices.
  - Smartphone's. Internet-enabled cell phones that can support mobile applications.
  - Wi-Fi (*Wireless Fidelity*). Refers to a standard 802.11b which most of the wireless local area networks are based on.
  - Global positioning system (GPS). A satellite based tracking system that enables the determination of a GPS device's location.
  - WLAN. Wireless local area network

- **Characteristics**

  - *Mobility* (and localization) implies portability based on the fact that users carry a mobile device everywhere they go. Therefore, users can initiate real-time contact with other systems from wherever they happen to be.
  - *Broad reach* is the characteristic that describes the accessibility of people. They can be reached at any time. Mobile computing has two major characteristics that differentiate it from other forms of computing: *mobility* and *broad reach.*

- **Attributes**

  - Ubiquity refers to the attribute of being available at any location at any given time. A mobile terminal in the form of a Smartphone or a PDA offers ubiquity.
  - Convenience. It is very convenient for users to operate in the wireless environment. All they need is an Internet enabled mobile device such as a Smartphone.
  - Instant connectivity. Mobile devices enable users to connect easily and quickly to the Internet, intranets, other mobile devices and databases.
  - Personalization. Personalization refers to customizing the information for individual consumers.
  - Localization of products and services. Knowing the users physically location at any particular moment is key to offering relevant products and services.
    The characteristics of M-commerce, mobility and broad reach break the barriers of geography and time. Creating unique value added attributes.

- **Drivers**

  - Widespread availability of mobile devices. The number of cell phones exceeds 1.3 billion
  - No need for a PC. The Internet can be accessed via Smartphone or other Internet-enabled wireless devices.
  - The handset culture. The widespread use of cell phones
  - Vendors are pushing m-commerce. Both mobile communication network operators and manufacturers of mobile devices.
  - Declining prices and increased functionalities.
  - Improvement of bandwidth. To properly conduct m-commerce, it is necessary to have sufficient bandwidth. 3G (third-generation) technologies provide the necessary bandwidth, at a data rate of up to 2 Mbps. The development of mobile computing and m-commerce is being driven by number of factors.

- **Applications**

The importance of Mobile Commerce has been highlighted in many fields of which a few are described below:

- In courts
- For Estate Agents
- Emergency Services
- In companies
- Stock Information Collation/Control
- Credit Card Verification
- Taxi/Truck Dispatch
- Electronic Mail/Paging

- ***Financial Services***

These services have the potential to turn a mobile device into a business tool, replacing banks, ATMs, and credit cards by allowing a user to conduct financial transactions any time and from anywhere Mobile financial applications include:

- Banking: offer mobile access to financial and account information.
- Wireless payments: provides mobile phones with a secure purchasing tools capable of instantly authorizing payments
- Micropayments: electronic payments for small-purchase amounts (generally less than $10)
- Wireless wallets: Software (e-wallet) that stores an online shopper's credit card numbers and other personal information.
- Bill payment services: Paying bills directly from a mobile device
- Brokerage services: stock trades and quotes
- Money transfers: from one account to another

- ***Intra-business and Enterprise Applications***

Today's m-commerce applications are mainly used within organizations.

- *Support of Mobile Workers***:** are those working outside the corporate premises. Service technicians, Sales personnel, Delivery workers, etc.
- *Wearable Devices.* Employees may be equipped with a special form of mobile wireless computing devices
  - Camera.
  - Screen.
  - Keyboard/Touch-panel display.
  - Speech translator
- *Job Dispatch.* To assign jobs to mobile employees, along with info about the task.
  - transportation (delivery of food, oil, newspapers, cargo, courier services)
  - Utilities measurement (gas, electricity, phone, water)
  - Field service (computer, office equipment, home repair)
  - Health care (visiting nurses, doctors, social services)
  - Security (patrols, alarm installation).

6.1 & 6.2 Check your Progress
Fill in the blanks.

a. It is ……..that facilitates employee or enterprise mobility.

b. ……. is associated with the mobility of hardware, data and software in computer applications.

6.3 WIRELESS COMPUTING CONCEPTS

- **Wireless Industry Standards**

No technology works in a vacuum. Many entities work at different levels to bring the technology to a more mature and usable state. Standards and specifications are first conceived, developed, and then implemented. Currently, most standards for the mobile e-commerce environment are focused on hardware- or infrastructure-related issues. Some of the more important standards organizations related to the wireless industry today include:

- Bluetooth Special Interest Group (SIG) is a volunteer organization run by employees from member companies. Members support a number of working groups that focus on specific areas, such as engineering, qualification, and marketing. The member companies build and qualify products under strict qualification procedures with regular testing of products at events sponsored by Bluetooth.
- The Institute of Electrical and Electronics Engineers (IEEE) does extensive research in technology spanning a broad spectrum. They created the 80211 standard for wireless networks, and are also instrumental in creating security protocols such as Wired Equivalent Privacy (WEP). The IEEE does not provide certifications of any kind for their specifications.
- Wireless Application Protocol (WAP) Forum offers a comprehensive certification and interoperability testing program that covers device testing, content verification, and a set of authoring guidelines to assist developers in providing interoperable WAP applications and services.
- Wireless Ethernet Compatibility Alliance (WECA) seeks to attest interoperability of products based on the 802.11b specification, and certify them Wireless Fidelity (Wi-Fi) compatible. They endorse Wi-Fi as the global wireless LAN standard across all market segments.

  Many other organizations such as the W3C, Wireless DSL Consortium, and other institutions have standards directly affecting the wireless industry, though they are not specific to wireless communications. For example, XML and Web services standards are increasingly part of the development and deployment to server and desktop processing, but they are equally applicable to wireless applications. Several new standards groups are being formed to address specific issues regarding mobile e-commerce.

- **Wireless Communication Platforms for LANS**

Despite the standards committees in the wireless industry, there is no single unifying standard. It is important for enterprises to consider all the aspects involved in mobile support while contemplating a strategy for mobile e-commerce. Some of the key criteria in choosing a wireless network specification include:

- Average size of transfers
- Number of devices in the wireless network
- Others
- Range of transmission
- Security measures
- Speed of network

Wireless networks may operate in one of two modes—on demand and infrastructure mode.

- **On Demand Mode (Peer-to-Peer)**

  Each mobile device, also known as a mobile client, communicates with the other devices in the network, within a specified transmission range or cell. This is described in Figure 6.1. If a client has to communicate with a device outside the specified cell, a client within that cell must act as a gateway and perform the necessary routing.

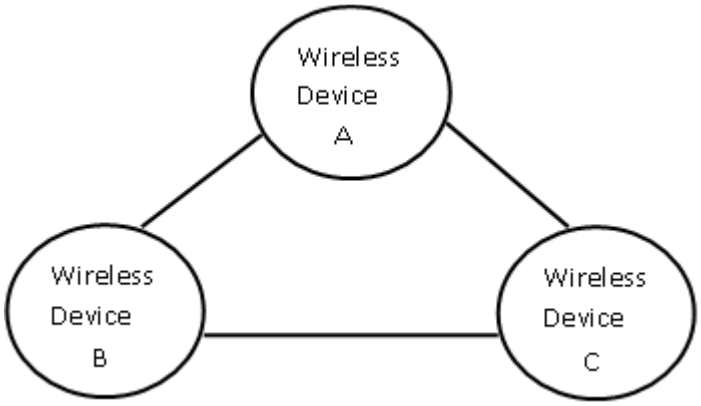


Figure 6.2 Peer-to-Peer (On demand) wireless network

- **Infrastructure Mode (Wireless LAN)**

Communications between multiple wireless clients are routed by a central station known as an "access point." The access point acts as a bridge and forwards all communications to the appropriate client in the network whether wireless or wired. Besides having routing mechanisms, the access point also has as a Dynamic Host Configuration Protocol (DHCP) server and other features that facilitate wireless communications in a small to large business environment. Residential gateways are similar to access points, but do not have advanced management features required for corporate networks or high-traffic environments.

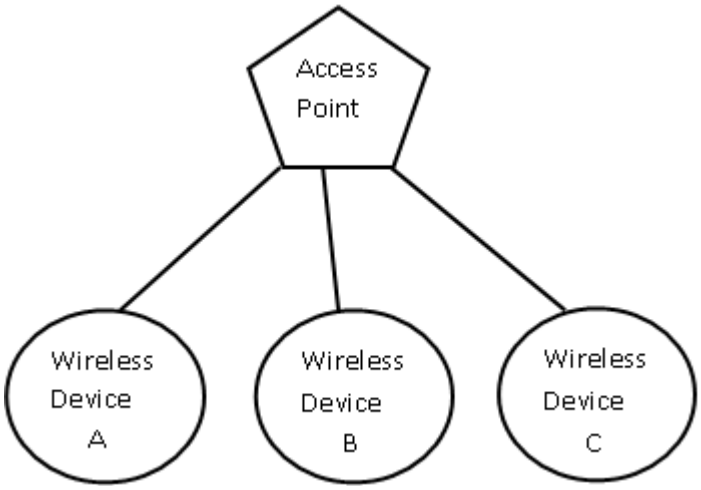


Figure 6.3 Wireless LAN (Infrastructure mode)

A wireless client must first be authenticated, and then associated with an access point before it can perform any communications. Figure 6.2 shows a typical wireless LAN environment. Enterprises that have a strong mobile e-commerce strategy must make a selection from the major wireless LAN specifications available in the market today.

- **802.11b**

The 802.11b specification was defined by the Institute of Electrical and Electronics Engineers (IEEE). The 802.11b is used as an extension of Ethernet to wireless communication, and as such is quite flexible about the different kinds of network traffic that passes over it. It is primarily used for Transmission Control Protocol/Internet Protocol (TCP/IP), but also supports AppleTalk and other PC file sharing standards. Disparate systems like PCs and Macs may communicate over 802.11b, using PC or Peripheral Component Interconnect (PCI) cards, and even some of the newer hardware, utilizing Universal Serial Bus (USB) and other forms of 802.11b based wireless network cards. Adapters for PDAs, such as Palm OS and PocketPC based devices are also available.

The 802.11b facilitates the wireless transmission of approximately 11 Mbps (Megabits per second) of raw data at distances ranging from a few feet to several hundred feet over the standard 2.4 GHz (Gigahertz) unlicensed band. The coverage

distance depends on line of sight, obstacles, and unforeseen obstacles. Several new protocols based on 802.11b, but not compatible with it, are also being released.

- **802.11a**

Protocol 802.11a transmits 54 Mbps over the 5 GHz band. This is ideal for large data file transfers and bandwidth intensive applications over a limited area. Although performance and throughput are significantly increased, the transmission range is notably reduced.

- **802.11g**

Protocol 802.11g transmits 22 Mbps over 2.4 GHz. This specification is considered to be the next generation wireless network platform for the enterprise, working twice as fast as the current 802.11b specification. However, this is still a work in progress. Note 802.11b has become the standard wireless network deployment platform for public short-range networks, such as those found at airports, hotels, conference centers, and coffee shops and restaurants.

- **Bluetooth**

This wireless network specification, defined by the Bluetooth Special Interest Group, is ideally suited for Personal Area Networks (PANs) that operate in short ranges and need a robust wireless network that allows transmission of bandwidth intensive information. Bluetooth specifications also promote inter-device communications, so mobile phones can communicate to PDAs, notebook PCs with laptops, and so on. Although it uses the unlicensed 2.4 GHz band for transmission, its transmission is faster than the 802.11b networks in both on demand and infrastructure modes. Bluetooth's range is, however, much less. Bluetooth technology works well for on demand networks and situations in which device-to-device communication is desired. For example, you can wirelessly connect from your PDA to a printer to print documents, or perhaps synchronize your desktop with your PDA over the air.

- **Wireless WANS**

At the core of most mobile computing applications are mobile networks. These are of two general types: the wide area and the local area. The wide area networks for mobile computing are known as **wireless wide area networks** (WWAN).

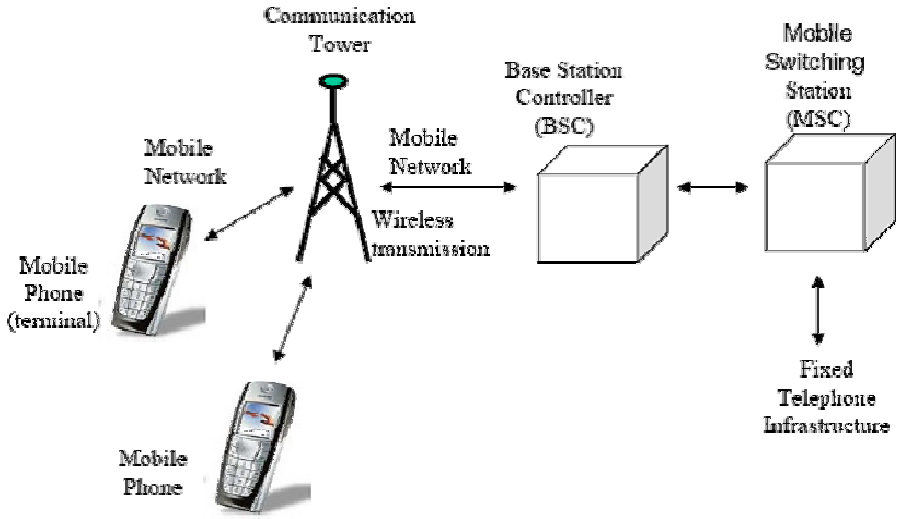


Figure 6.4 Wireless wide area network (WWAN)

The success of mobile computing depends on the capabilities of the WWAN communication systems

- **1G.** The first generation of wireless technology. It was an analog-based technology, in effect from 1979 to 1992.
- **2G.** The second generation of digital wireless technology. In existence today, 2G is based on digital radio technology and mainly accommodates text.

- **2.5G.** An interim technology based on GPRS (General Packet Radio Services) and EDGE (Enhanced Data Rates for Global Evaluation) that can accommodate limited graphics.
- **3G.** The third generation of digital wireless technology, which supports rich media such as video clips. It started in 2001 in Japan, and reached Europe in 2002 and the United States in 2003 (commercial adoption around 2004-5).
- **4G.** The expected next generation after 3G. 4G will provide faster display of multimedia and is expected between 2006 and 2010 (commercial adoption later than 2010.

Although the preceding architectures are specific to wireless LAN environments, employees that are outside the coverage area are required to connect through wireless carriers that provide support for a wireless wide area network (WAN) environment. There are several wireless WAN protocols used all over the world.

- ***Code Division Multiple Access (CDMA)***

With CDMA, a large number of users are able to access wireless channels on demand. Used by most digital mobile phone companies today, the performance is almost 8 to 10 times better than traditional analog cell phone systems. The latest generation of this technology is called 3G and is much anticipated by many mobile users.

- ***Global System for Mobile (GSM)***

  Global System for Mobile communication was deployed in 1992 and it uses the TDMA multiple access scheme.

  – There are three frequency bands defined for GSM: 900, 1800, and 900. Within the GSM 900 band, there are 174 frequencies with 200 kHz spacing.
  – The speech signal is processed in 20ms intervals, called speech frames. Each speech frame is compressed and coded using 244 bits. These 244 bits are then encoded with a channel code, interleaved, segmented, and transmitted in 8 TDMA time slots. Similar transmission formats are used for data services.

- ***HSCSD***

– High Speed Circuit Switched Data helps in achieving higher data rates by bundling several traffic channels. It allocates several TDMA slots within a TDMA frame. This allocation can be asymmetrical, i.e., more slots can be allocated on the downlink than on the uplink, which fits the typical user behavior of downloading more data compared uploading. But, HSCSD makes the traffic busty.

- ***GPRS***

  General Packet Radio Services is an extension to GSM that allows more efficient packet data transfer compared to traditional GSM data services. The principle is that a user can be constantly connected to the network without occupying any radio resources (frequency, time slots) until a data packet has to be transferred. When a packet is to be transferred, a temporary channel is assigned to the user; after completed transfer, the channel is quickly released again. GPRS allows many users to share the same timeslot, and also allows a single user to use more than one time slot. It uses an error detection and retransmission scheme to ensure that data packets are correctly delivered to the receiver.

- ***EDGE***

  Enhanced Data rates for GSM Evolution allows higher bit rates than GSM does. This is accomplished by using higher order modulation, 8-ary phase-shift keying instead of GSM's binary phase-shift keying.

- ***TETRA(Terrestrial Trunked Radio)***

  Trunked radio systems use many different carriers but only assign a specific carrier to a certain user for a short period of time according to demand.

- ***Mobile Networking through Mobile IP***

Mobile IP is a proposed standard protocol that builds on the Internet Protocol by making mobility transparent to applications and higher level protocols like TCP.

- ***Future Technologies***
  Multiple access technologies are potential contenders for what is already being called 4th Generation (4G). These are, in order of decreasing likelihood:

– Multiple-input multiple-output processing antennas, also described as spatial processing, space-time coding and "smart" antennas. It has for some time been recognized that spatial processing of multi-element antennas provides an added dimension for improvement beyond what is achieved by temporal processing.

– Orthogonal frequency-division multiplexing-and multiple access (OFDM), a modified spread spectrum approach which may provide for simplified processing and more rapid adaptation to channel conditions. In the forward direction (multiplexing) it substitutes orthogonal sine waves for the Walsh functions of CDMA. In the reverse direction (multiple access) it has characteristics of both FDMA and spread spectrum.

The differences between different wireless access technologies are given in below table

APPROACH	SDMA	TDMA	FDMA	CDMA
IDEA	Segment space into cells/sector	Segment sending time into disjoint time slots, demand driven or fixed patterns	Segment the frequency band into disjoint sub-bands	Spread the spectrum using orthogonal codes
TERMINALS	Any one terminal can be active in one cell/sector	All terminals are active for a short periods of time on the same frequency	Every terminals has its own frequency uninterrupted	All terminals can be active at the same place at the same moment, uninterrupted
SIGNAL SEPARETION	Cell structure/directed antennas	Synchronizatio n in the time domain	Filtering in the frequency domain	Code plus special receivers
ADVANTAGES	Very simple, increases capacity per km²	Established fully digital very flexible	Simple established robust	Flexible, less planning needed, soft hand over
DISADVANTAGE S	Inflexible antennas typically fixed	Guard space needed, synchronizatio n difficult	Inflexible frequencies are a scarce resource	Complex receivers, needs more complicated power control for a sender
COMMENT	Only in combination with TDMA and FDMA or CDMA useful	Stan dared in a fix networks, together with FDMA/SDMA used in many mobile networks	Typically combined with TDMA and SDMA	Still faces some problems, higher complexity, will be integrated with TDMA/FDMA

Table 6.1 Wireless digital access technologies

- **Facilitators of a Wireless Environment**

In order to facilitate a mobile e-commerce environment, participation of several partners is required, namely:

- Independent hardware vendors (IHVs)
- Independent software vendors (ISVs)
- Mobile device manufacturers
- Service providers (SPs)
- Wireless operators (or carriers)

- **Wireless Hardware**

There are numerous devices that are wireless-enabled to facilitate an efficient mobile workforce. Some of the top companies that provide these devices are:
Compaq: The makers of iPAQ handheld computers and notebook PCs. They are used in many enterprise settings due to their versatility and high performance. They use Microsoft's PocketPC platform as their operating system.

Kyocera: They specialize in mobile phones with PDA capabilities, using the Palm OS.

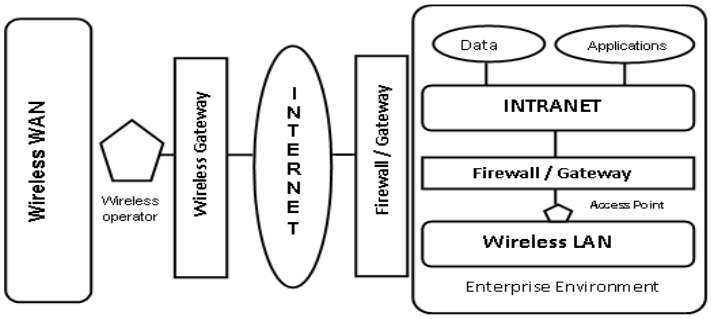
Nokia: The leading mobile phone manufacturer, with innovating products that combine mobile phones, PDAs, and other features.

Palm: Currently the leading provider of PDAs; their operating system, called Palm OS, is a popular platform for wireless application deployment.

- **Wireless Software**

The wireless software industry is still maturing; furthermore, although most of the players are niche solution providers, very few actually provide substantial value to enterprise deployments. Ranging from low footprint applications like mini-browsers or PDA utilities, to more sophisticated solutions like inter-device communications or global positioning systems, wireless software vendors are engaged in several innovative research and development initiatives. Companies such as Microsoft, Sun, Palm, and others are active in this area. When deploying a mobile e-commerce strategy, you have to consider the right combination of wireless network architecture, platforms, infrastructure components, devices, and applications in order to be successful.

Figure 6.5 A typical wireless architecture



Even with the absence of ubiquitous standards, the current wireless infrastructure is stable enough to support and deploy wireless applications developed for the mobile workforce. As wireless technologies mature, the quality and availability of wireless software will also grow. An important factor to consider is the need to secure and manage the enterprise infrastructure, while making all the necessary assets available to your mobile workforce.

- **Location-based Commerce**

The L-commerce services revolve around five key areas:
– *Location*: determining the basic position of a person or a thing (e.g., car or boat).
– *Navigation*: plotting a route from one location to another.
– *Tracking*: monitoring the movement of a person or a thing (e.g., a package or vehicle).
– *Mapping*: creating maps of specific geographical locations.
– *Timing*: determining the precise time at a specific location. Online language translation
Location-based commerce (L-commerce) refers to the localization of products and services. From a consumer's viewpoint, L-commerce offers safety. From a business supplier's point of view, L-commerce offers an opportunity to provide services that meet customers' needs.

- **L-Commerce Technologies**

Providing location-based services requires the following location-based and network technologies:

- Position Determining Equipment (PDE). This equipment identifies the location of the mobile device.
- Mobile Positioning Center (MPC). The MPC is a server that manages the location information sent from the PDE.
- Location-based technology. This technology consists of groups of servers that combine the position information with geographic- and location-specific content to provide an l-commerce service.
- Geographic content. Geographic contents consist of streets, road maps, addresses, routes, landmarks, land usage, Zip codes, and the like. (GIS)
- Location-specific content. Location-specific content is used in conjunction with the geographic content to provide the location of particular services.

- **L-Commerce Applications**

There are many applications related to Location Based Commerce:

- Location-based advertising.
    - The wireless device is detected, and similar to a pop-up ad on a PC, advertising is directed towards the PC.
    - A dynamic billboard ad will be personalized specifically for the occupant of an approaching car.
    - Ads on vehicles (taxicabs, trucks, buses) will change based on the vehicles location.
- E-911 emergency cell phone calls (in United States)
- Telemetric applications: integration of computers and wireless communications in order to improve information flow (On-Star system by GM)
- It can also be used for Enhanced billing, personalized portals, buddy finding, service call routing, to find nearest services, etc.

Limitations and Difficulties of Wireless Technologies

- Wireless is convenient and less expensive
- Limitations and political and technical difficulties inhibit wireless technologies
- Lack of an industry-wide standard
- Device limitations
    - E.g., small LCD on a mobile telephone can only displaying a few lines of text
    - E.g., browsers of most mobile wireless devices use wireless markup language (WML) instead of HTML

6.3 6.3 Check your Progress

1. Write full forms of the following

a. CDMA……..

b. GSM……..……..

c. GPRS……..……..

d. EDGE……..

e. TETRA……..

6.4 LEGAL ASPECTS OF E-COMMERCE

- **Legal Aspects**

The world is used to conducting business and commerce on signed paper documents. Two millennia of commerce have been based on the written document

with its value 'authorized' by the signature of a duly authorized officer. The current legal practice has paper documents and signatures affixed thereon as its foundation. Electronic documents and messages, without the familiar signatures and marks, have changes the scene. However, trade still wants to be assured that the electronic world is safe. The EC system must, therefore, offer at least the same level of reliability as that which obtains in the paper world notwithstanding the significant difference between the concepts embodied in electronic messages and paper documents. It is well known that frauds do take place in the traditional paper based commercial transaction. Signatures can be forged, paper document can be tampered with, and even the most secure marks, impression, emblems and seals can be forged. But then these are known, and trade as well as the legal community knows how to deal with these problems. Companies set aside funds to take care of losses due to such frauds. For example, credit-cards companies do know that a very small percentage of transaction is fraudulent in nature. The world is comfortable with these problems, since they have been there for as long as we have been trading.

The EC world, on the other hand, exposes us to issues, which were hitherto unknown, since they are directly the outcome of creating documents electronically, transmitting them over world-wide computer communication networks. Trading partners exchange documents electronically. They need to convince themselves that such documents are authentic when received over networks, and that their authentication can be established in case of dispute. Transactions may be electronic, but the key concept of admissibility of evidence and evidential value of electronic documents, which are central to the law, remain the same. There must be a way to prove that a message existed, that it was sent, was received, was not changed between the sending and receiving, and that it could not be read and interpreted by any third party intercepting or deliberately receiving it. The security of an electronic message, legal requirement, thus gets directly linked to the technical methods for security of computers and networks. From the legal angle, there is a further complication because the electronic message is independent of the actual medium used for storage transmission. The message can be stored on a floppy, a magnetic disk, or an optical disk. Likewise, it may be transmitted over a Local Area Network, a Wide Area Network, a private Value Added Network or the Internet. The physical medium could be coaxial cable, radio link, optical fiber or a satellite communication channel.

The legal issues of EC have generated tremendous interest among technologists, traders and legal experts. Many of the early EDI experiments, and even production systems went into operation without any legal interchange agreement between trading partners, between VANs and their customers. No laws for EC existed; in fact they are still in the making. In India, too the Indian Customs EDI system (ICES) Project got off the ground in 1995 without any EC/EDI law in existence, or even a proper interchange agreement.

- **E-Commerce's Law**

As discussed earlier, the legal requirement is to establish the authenticity of an electronic message or document. This includes integrity, confidentiality, and non-repudiation of origin and receipt of an electronic document in case of dispute. The UNCITRAL model EDI/EC Law defines an electronic data message as follows: "a Data message means, information generated, stored or communicated by electronic, optical or analogous means including but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy". This law proposes legal recognition of data messages, and defines 'writing', 'signature' and their admissibility and evidential value. Individual countries have been advised to enact this law with suitable modification that may be necessary in the national context.

In order to prevent fraudulent changes of electronic records, civil and criminal liabilities for misconduct are necessary to deter criminals, whether corporate insiders or hawkers, through appropriate promulgation of the computer Misuse Act or amendment of the existing criminal code. This would help protect against unauthorized use of, or access to computers, as well as unauthorized alteration or destruction of data. Likewise, the Digital Signature Act has also to be enacted to give sanctity to digital signatures, which is central to authenticating electronic documents. Alongside the *law* or rules for the establishment of Certification Authorities, Electronic Notaries would also be essential to permit the states to have access to keys for deciphering and tapping messages over the network to keep criminals under check and surveillance. This is necessary for national security, as also for preventing the use of this technology by smugglers, drugs peddlers and other criminals.

EC on the Internet will soon far surpass commerce conducted over private VANs. The use of the Internet for commerce opens up a Pandora's Box of problems that come with it. The legal issues revolve around protection of copyrights, trademarks, patents and electronic controls on the Web. The privacy of individual stands threatened, since data could be downloaded from various sites and collated. In case of dispute, procedural issues related to jurisdiction, venue, date and time rear their ugly heads, since it is difficult to define where the transaction has taken place and on what date time, for purpose of attributing responsibility.

- **EDI Interchange Agreement**

It is a known fact that a certain discipline is required in the conduct of commerce in the paper world. Simple activities such as preparation of invoices, drawing up commercial contracts, signing, dispatch, receipts etc. have to follow certain protocols agreed to by trading partners. These may be formal or in formal. In addition, acceptable rules of conduct are also necessary to achieve the kind of discipline required for smooth and effective trade and commerce. In the EDI world of electronic documents, this kind of discipline has been created through a set of rules that have developed in the form of interchange agreements within a number of user groups, national organization, and regions. At the international level, the UN has adopted the Model Interchange Agreement for the International Commercial Use of Electronic Data Interchange, which applies to the interchange of data and not to the underlying commercial contracts between the parties. It addresses the need for uniformity of agreement so that there are no barriers to international trade on account of different solutions for various problems being adopted by countries.

The UN has recommended that the member countries should take into account the terms and provisions of the Model Interchange Agreement when framing their own laws on EC. An interchange agreement may be made between trading partners. It establishes the rules they will adopt for using EDII ED transaction. It establishes the rules they will adopt for using EDI/EC transactions. It details the individual roles and legal responsibilities of trading partners for transmitting, receiving, and storing electronic messages. The signing of an interchange agreement signifies that the parties intend to be bound by it, and that they desire to operate within a legal framework. This can help reduce legal uncertainty in the electronic environment. Many of the conventions and agreements relating to international trade do not anticipate the use of EDIIEC. Many national laws, as noted above, also introduce uncertainty regarding the legal validity of electronic document. There are still very few national and international judgments ruling" on the validity of electronic documents, messages or signatures. It" is precisely in this kind of a scenario where clear legal rules and principles are absent; that an interchange agreement provides trading partners with readily available solutions the EDI/EC relationship between them. It provides a strong legal framework for ensuring that electronic documents will have a legal binding effect, subject to national laws and regulations.

The issues, which were addressed by the working party, which prepared this model Interchange Agreement, are as follows:

1. Selection of EDI messages, standards and the methods of communication.
2. Responsibilities for ensuring that the equipment, software and services are operated and maintained effectively;
3. Procedures for making any systems changes which may impair the ability of the trading partners to communicate. .
4. Security procedures and services;
5. The points at which EDI messages have legal effect;
6. The roles and contracts of any third-party service providers;
7. Procedures for dealing with technical errors;
8. The need (if any) for confidentiality;
9. Liabilities in the event of any delay or failure to meet agreed EDI communications requirement;
10. The laws governing the interchange of EDI messages and the arrangements of the parties.
11. Methods for resolving any possible disputes.

The interchange agreement is flexible enough to meet the requirement of all business sectors involved in international trade. Trading partners can feel confident that it addresses the recognized legal issues arising from commercial use of EDI in international trade, and provides a strong legal and practical framework for considering and recording the necessary business decisions.

- **Legal Issues for Internet Commerce**

Internet commerce raises legal issues through the provision of the following services:

- Online marketing
- Online retailing ordering of products and services
- Financial services such as banking and trading in securities.
- Exchange of electronic messages and documents
- EDI, electronic filing, remote employee access, electronic transactions.

Trade and commerce over the Internet give rise to several legal issues as given below.

- **Copyright and the Internet**

Copyright developed in the printed world to protect the economic interests of creative writers. Copyright law protects only the expression of an idea and idea itself. In due course it protects the originality of artists and innovators too. In recent times, however, the subject matter of copyright has further expanded. For example, the Copyright Designs and Patent Act, 1988 in the UK, allows protection of the following subject matter: Original literary, dramatic, musical and artistic works; the typographical arrangement of published editions of literary, dramatic or musical works; sound recordings; broadcasts; cable programs These have been broadly classified into two groups as 'author works' and 'media works' by Hector L. Macqueen. The multimedia capability of websites enables all types of work to be 'published' on the Internet in the sense that copies can be distributed to users/customers. The problems, however, is that unlike a paper copy, this copy can be readily duplicated and distributed further by the recipient. If the material is in the public domain there are no difficulties. But the copyright law applies to the downloaded matter, much the same way it applies to physical copies.

- **Issues Related to Jurisdiction**

The Internet allows anyone to set up a Website anywhere in the world. Its location could, however, be interpreted to decide the jurisdiction of disputes especially in EC. A Website may accept orders from visitors to the site as part of an Internet store or a shopping mall. For example, amazon.com is a bookstore retailing books. A court law may rule that the location of the Website determines the jurisdiction for that business. This is based on accepted legal practice. Jurisdiction determines which laws would be acceptable. EC on the Internet will grow if the parties doing business know what rules will govern what rules govern their activities.

- **Service Provider liability**

Many ISPs provide users access to shared websites, Usenet news, E-mail distribution list etc. These facilities can because by their users to upload unlawful, defamatory, copyright or trademarks infringing material. Unlawful material includes banned publications, hate propaganda, pornography and obscene material, without ISP having chance to review it. Liability for materials distributed in the Internet may be different for the Website operators, and the ISPs. AN ISP could be held liable for the bulletin boards, and for aiding and abetting the commission of an offence such as the distribution of photography. Similarly, third-party liability for defamation, web sites, etc: Thus the concerns include libel and defamation, liability for infringement of third-party rights, liability for hosting of unlawful materials.

- **Formation of an Enforceable Online Contract**

The growth of EC on the Internet depends to a large extent on the confidence of traders in forming legally enforceable contracts online. The key activities associated with the formation of an enforceable contract do take place on the Internet, viz. offer is communicated by the acceptor and acceptance is received by the offer or from the acceptor. An offer can be communicated orally or in writing; and in the EC environment through E-mail, Eform is valid, much the same way a fax message is. The offer or can

display terms and conditions as a legal notice, on his website. Visitor to the site, who chooses to proceed further, even after reading the notice, may be constructed as accepting the conditions imposed by it. However, the timing of the acceptance offer determines when the contract is formed. In this case the E-mail of acceptance has to reach the offer or who may say that the contract will be legal only after its receipt (in his notice placed on the Website). Legal issues are manifold. Whether it is EDI over VANs or EC over the Internet the primary concern of users is the existence and enforceability of appropriate laws for EC. 'N case of dispute, electronic document must be acceptable as legal evidence in courts of law. While the problems of acceptance of and confidence in electronic transactions are there, they are not insurmountable. There is sufficient awareness in, and synergy of action among trade, legal and EC technology communities to make EC happen through appropriate developments in their respective areas.

- **The standards**

There are various standards pertaining to the security aspects of enterprises. Some of them are ISO 17799 (Information technology – Code of practice for information security management) (ISO/IEC 2000), SSE-CMM (Systems security engineering – Capability maturity model) (SSE-CMM 2003) and COBIT (Control objectives for information and related technology) (COBIT 2000). ISO 17799 provides detailed guidelines on how a management framework for enterprise security should be implemented. It conceives ten security domains. Under each domain there are certain security objectives to be fulfilled. Each objective can be attained by a number of controls. The controls may prescribe management measures like guidelines and procedures, or some security infrastructure in the form of tools and techniques. It details various methods that can be followed by enterprises to meet security needs for e-commerce. It talks about the need for security policies, security infrastructure, and continuous testing in the same manner as has been detailed above.

The main objective of the COBIT is the development of clear policies and good practices for security and control in IT for worldwide endorsement by commercial, governmental and professional organizations. The SSE-CMM is a process reference model. It is focused upon the requirements for implementing security in a system or series of related systems that are in the Information Technology Security domain.

- **Indian IT Act 2000**

The Indian IT act was enacted on 7th June 2000 and was notified in the official gazette on 17th October 2000. It aims to provide a legal and regulatory framework for promotion of e-commerce and e-governance. It is applicable to the whole of India. Some of the major provisions contained in the IT Act 2000 are as follows:

- Electronic contracts will be legally valid
- Legal recognition of digital signatures
- Security procedure for electronic records and digital signature
- Appointment of certifying authorities and controller of certifying authorities, including recognition of foreign certifying authorities
- Various types of computer crimes defined and stringent penalties provided under the Act
- Establishment of Cyber Appellate Tribunal under the Act
- Act to apply for offences or contraventions committed outside India
- Power of police officers and other officers to enter into any public place and search and arrest without warrant
- Constitution of Cyber Regulations Advisory Committee who will advise the Central Government and Controller

However, there are a few more areas which should be taken care of in the subsequent amendments to the IT Act. These are as follows:

- Electronic fund transfer – Electronic payment system
- Digital copyright
- Taxation – Income tax, sales tax
- Consumer protection
- Sale or the conveyance of immovable property
-

6.4 Check your Progress

1. Fill in the blanks.

a. ……developed in the printed world to protect the economic interests of creative writers.

b. ……aims to provide a legal and regulatory framework for promotion of e-commerce and e-governance.

6.5 SUMMARY

The demand for and use of mobile technologies is increasing at a phenomenal rate. Simultaneously, the underlying landscape of mobile technologies is changing rapidly, creating the need for solutions to facilitate the long-term growth and success of mobile enterprise initiatives. It is important for software vendors to provide comprehensive solutions to manage, secure, and maintain the mobile applications infrastructure, while fostering development, integration, and access to applications and information over wireless mediums.

With the rapid technological advancements in Artificial Intelligence, Integrated Circuitry and increases in Computer Processor speeds, the future of mobile computing looks increasingly exciting. With the emphasis increasingly on compact, small mobile computers, it may also be possible to have all the practicality of a mobile computer in the size of a hand held organizer or even smaller. Use of Artificial Intelligence may allow mobile units to be the ultimate in personal secretaries, which can receive emails and paging messages, understand what they are about, and change the individual's personal schedule according to the message. This can then be checked by the individual to plan his/her day. The working lifestyle will change, with the majority of people working from home, rather than commuting

Finally, although it is one thing for organizations to keep up with the latest industry trends, making it happen in everyday life is a totally different story. Enterprises must contemplate developing a mobile e-commerce strategy.

Source : *www.bluehorse.in(Link)*

6.6 CHECK YOUR PROGRESS - *ANSWERS*

6.1 & 6.2

1. a) Wireless technology b) Mobile computing

6.3

1. a) Code Division Multiple Access
b) Global System for Mobile
c) General Packet Radio Services
d) Enhanced Data rates for GSM Evolution
e) Terrestrial Trunked Radio

6.4 1.a) Copyright b) The Indian IT act

6.7 QUESTIONS FOR SELF-STUDY

1. Discuss the basics of mobile computing
2. What are the wireless industry standards?
3. What are different wireless WAN protocols used? Explain.
4. Explain difference between various wireless access technologies.
5. Write a short note on location based commerce.
6. What are the legal aspects of e-commerce? Explain in detail.
7. Write a note on Indian IT act 2000.

NOTES

NOTES