E-COMMERCE CONCEPTS AND APPLICATION DESIGN

Course Designer and Acquisition Editor

Centre for Information Technology and Engineering

Manonmaniam Sundaranar University

Tirunelveli

E-Commerce Concepts and Application Design

CONTENTS

ꕥ

Lecture 1

Electronic Commerce An Overview

Objectives

In this lecture you will learn the following

- What is E-Commerce
- Concepts of E-Commerce
- About Various Service

Coverage Plan

Lecture 1

1.1 Snap Shot

The increased computerization of our society is triggering major changes in the organization of work. Paper driven processes are being reengineered to capture the benefits of doing business electronically. Businesses are implementing electronic commerce (EC or E-Commerce) to meet the imperatives of an increasingly competitive world.

1.2 What is Electronic Commerce?

Electronic Commerce has unleashed yet another revolution, which is changing the way business buy and sell products and services. It is associated with buying and selling of information, products and services over computer communication networks. E-Commerce (EC) helps conduct traditional commerce through new ways of transferring and processing information, since it is information which is at the heart of any commercial activity. Information is electronically transferred from computer to computer, in an automated way. This has, in fact, transformed the way organizations operate.

E-Commerce refers to the paperless exchange of business information using Electronic Data Interchange, Electronic Mail, Electronic Bulletin Boards, Electronic Funds Transfer and other network-based technologies. It not only automates manual processes and paper transactions, but also helps organizations have started conducting EC over the Internet, the network of networks. The Internet has given yet another boost to E-Commerce because it is a low-cost alternative to the proprietary networks. E-Commerce standards are, however, under development. The more well known Electronic Data Interchange (EDI), the inter-organizational exchange of business documentation in structured, machine processable from over computer communication networks, is still the dominant part of E-Commerce.

Information gathering, processing, manipulating and distributing is common to trade and commerce, no matter what the commodity or service is that is being exchanged. Today, it is the velocity of information processing and dissemination which determines the speed of real commerce. Computers and networks, by virtue of their great speed, are creating electronic marketing with the potential to be more efficient in finding and interacting with customers, communication with trading partners and developing new products and markets.

On the one hand, Local Area Networks (LANs), and enterprise wide intra-networks have resulted in raising expectations for data access, communications and productivity throughout the business world. On the other, low-cost high-speed open networks interconnected as a single network, commonly known as the Internet, have kept pace with the requirements through the establishment of National Information Infrastructures, with high-speed National Information Highways being their main backbones. Widespread access to network communication tools including electronic mail awareness of the commercial potential of the Internet. While the Internet has already been successfully used for marketing, advertising and some commerce, much of its technical potential remains to be commercially harnessed. EDI is still the proven application for E-Commerce, although it is only one of the ways of doing electronic commerce.

1.3 Benefits of Electronic Commerce

Electronic Commerce is the business environment in which information for the buying selling and transportation of goods and services moves electronically. Electronic Commerce (EC) includes any technology that enables a company to do business electronically. Some of the direct benefits of Electronic Commerce are:

- Improves Productivity
- Cost Savings
- Streamlined Business Processes
- Better Customer Service
- Opportunities for New Businesses

Improved Productivity

Using electronic commerce, the time required to create, transfer and process a business transaction between trading partners is significantly reduced. Furthermore, human errors and other problems like duplication of records are largely eliminated with the reduction of data – entry in the Process. This improvement in speed and accuracy, plus the easier access to document and information, will result in increase in productivity.

Cost Savings

Based on the experience of a wide variety of early adopters of electronic commerce. Forrester Research has estimated that doing business on the Internet can result in cost savings of about

5% to 10% of sales. This cost savings stem from efficient communication, quicker turnaround time and closer access to markets.

Streamlined Business Processes

Cost savings are amplified when business go a step further and adapt their internal processes and back-end legacy systems to take advantage of electronic commerce, Inventories can be shaved if businesses use the Internet to share such information as promotional plans, point of sale data, and sales forecasts. Business processes can also be made more efficient with automation.

Better Customer Service

With electronic commerce ,there is better and more efficient communication with customers. In addition, customers can also enjoy the convenience of shopping at any hour, anywhere in the world.

Opportunities for New Businesses

Business over the Internet have a global customer reach. There are endless possibilities for businesses to exploit and expand their customer base.

Electronic commerce is the use of telecommunications and data Processing technology to improve the quality of transactions between business partners . It has existed in some form since the invention of the telegraph and early automated data processing equipment but its use has greatly increased. E-commerce improves organizational efficiencies by leveraging data processing, database storage and data communications technologies. Existing network facilities can be utilized to achieve great savings in labor costs and the reduction of paper storage and handling facilities .It has enabled firms to be more effective in improving the quality of standard goods and services and to offer a variety of new services. The global marketplace has become larger and wider than ever because of the expansion of e-commerce activity.

The growth of electronic commerce has been fueled by the availability by the availability of worldwide telecommunication networks along with enhanced information delivery techniques utilizing the various multimedia technologies Client-server architecture allows systems with different hardware and software platforms to interact in an open system computing environment.

Electronic commerce can be viewed form two business application perspectives. One perspective on e-commerce in business is to look at those businesses engaged in providing electronic commerce technology to help enable other businesses .**Internet Service Provider(ISP)** and private **commercial network providers** help the companies into **wide area networks(WAN)** for use in e-commerce activity .They may offer additional features such as protocol conversion and are they described as **Value Added Network (VAN).** Added Other types of firms specialize in helping organizations build electronic commercial sites .Software firms sell **data encryption** and other types of security –related technologies ,user interface programs and other types of software used to implement e-commerce . Other firms specialize in consulting and designing e-commerce applications such as World Wide web sites.

Another perspective on e-commerce is to examine the application uses to which a business uses such technologies. Linkage between business partners may be tightened through improvements in **Just-in-Time (JIT)** Supply logistics overall improvement in **supply chain management**. Consumer marketing and sales techniques like **shopping kioks** and home shopping techniques have removed barriers of distance and increased product awareness. **Electronic publishing** services, financial news and **remote banking** services are now available over networks. **Commercial databases** and library services provide general information resources .On-line job placement services are numerous and **distance education** and job training services can assist in career development .A wide variety of recreational and entertainment services are currently available and such services will expand dramatically in the near future .

The latter half of the 1990's has seen an explosion in the user of the Internet/Intranet and its accessibility to individuals, corporations, and educational institutions. This revolution has dramatically changed the way organizations conduct business with its consumers and with each other. The geographic boundaries that offer limited access to goods and services, are crumbling and companies of all sizes are busy building commerce solutions and adapting to new ways of doing business .The Internet/Intranet with inherent features like easy access , real –time information and low cost is a natural driver for commerce solutions .Further ,companies enticed with the promise of the following competitive advantage are undertaking electronic commerce projects:

- Broader market reach
- Increased efficiency and accuracy through automated order-processing.
- Inventory control, billing ,shipping and so forth
- Better customer service and support
- Instant communication with consumers and trading partners
- Improved profit margins through automated supply chain management
- Better forecasting of customer needs for goods and services
- Reduced labor costs
- Lower overall costs

Electronic commerce is often misunderstood to be limited to buying and selling of goods and services over the Internet. Actually, commerce solutions are a lot more than just the handling of business transactions and fund transfers over the internet .It defines new forms of doing business. In addition to providing buying and selling services, commerce solutions can provide a complete system of services built into an organization's digital nervous system so of supports the sales processes and provides total account management.

1.4 Various Services

The services that helps build the foundations of successful electronic commerce solutions are as follows:

1 Operating System Services
2 Developer Services
3 Data Services
4 Application Services
5 Store Services
6 Client Services

Operating System Services

Provide security, management communication and application hosting services. For example, Microsoft windows NT Server, Unix ware, etc.

Developer Services

Provide the tools necessary for component development, enterprise database development, team development and development lifecycle support. For Instance, Microsoft Visual Studio- Applications infrastructure and development suite of tools to enable the Microsoft Windows Distributed Network Architecture and provide tight integration and easy programmability across the platform.

Data Services

Provides services aimed towards data storage, simplified programmatic access and legacy data connectivity. Microsoft SQL Server can be used to store the information about users, products, orders, status, and so on OLE DB provides a mechanism to access any type of data store and to expose the data in a standard tabular format. Microsoft ActiveX Data Objects (ADO) provides a high level, object-oriented mechanism to access all OLE DB and ODBC compliant data. Microsoft SNA Server allows connectivity to mainframe based systems and enables application developers to expose and extend mainframe transaction applications through Component Object Model (COM) components.

Application Services

Processes information supplied by the user based upon business and data logic. Provides web services, application security and serves as a point of integration for store and Data Services. The following Application Services of Microsoft Windows NT server, can be used:

i. Internet Information server (IIS)- Web, FTP, SMTP Services, Active Server Pages providing an integration to the Store and Data Services.

ii. Component Object Model (COM)- Architecture for distributed application development encapsulating business and data logic.

iii. Microsoft Message Queue (MSMQ) provides transactional, asynchronous communication between distributed applications.

iv. Microsoft Transaction Server (MTS)- simplifies the development and deployment of sever-centric applications built using COM technologies and to ensure transactional integrity of transactions.

Store Services

Performs user management, order processing, information interchange running promotion, and advertisements, processing data based upon business logic and other commerce related services . For instance, Microsoft site Server Commerce Edited can be used for Store Services.

Client Services

Provides presentation, access, and validation services to the users of the commerce system .Microsoft Internet Explorer can be used for Page-based Internet/Intranet applications using components, DHTML, HTML, and scripting for rich user experience. Custom Microsoft Win32 based applications can be used for Win32 API-based applications with rich access to all system capabilities.

Figure 1.1 Illustrates the interaction between these services which help businesses design and implement flexible, scalable electronic commerce systems quickly and with reduced risk.

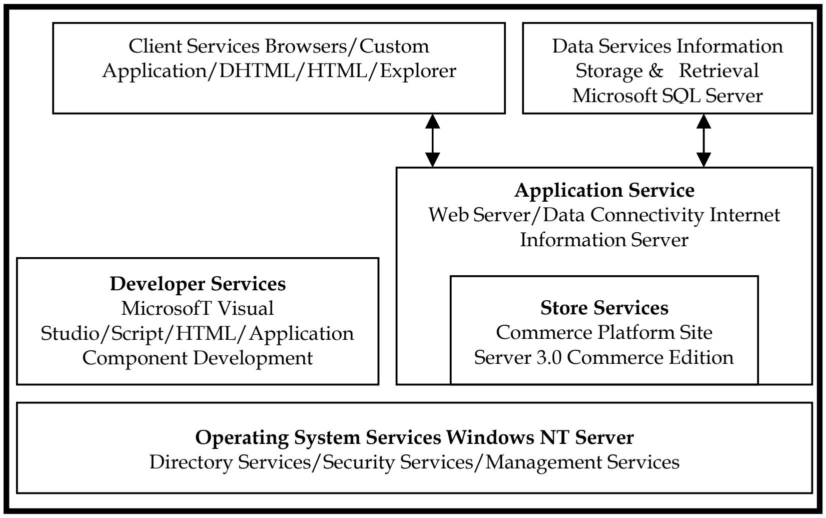

Client Services Browsers/Custom Application/DHTML/HTML/Explorer
Data Services Information Storage & Retrieval Microsoft SQL Server
Application Service
Web Server/Data Connectivity Internet Information Server
Developer Services
MicrosofT Visual Studio/Script/HTML/Application Component Development
Store Services
Commerce Platform Site Server 3.0 Commerce Edition
Operating System Services Windows NT Server
Directory Services/Security Services/Management Services

Figure 1.1 Electronic Commerce System

The common features of electronic commerce utilizing one or more above services include:

- **Payment:** Enabling credit card and other payments along with electronic fund transfers.
- **Marketing** : Publicizing products and services
- **Sales** : Generating orders for the products

- **Fulfillment:** Processing the order and delivering the product
- **Support :** Providing pre and post sale assistance to generate more sales
- **Inventory Management:** Maintaining and reporting inventory status
- **Secure Communication:** Fast, efficient , reliable communication with customers and partners

1.5 Snap Shot

- E-Commerce (EC) helps conduct traditional commerce through new ways of transferring and processing information, since it is information which is at the heart of any commercial activity.

- E-Commerce refers to the paperless exchange of business information using Electronic Data Interchange, Electronic Mail, Electronic Bulletin Boards, Electronic Funds Transfer and other network-based technologies.

- Electronic Commerce is the business environment in which information for the buying selling and transportation of goods and services moves electronically.

1.6 Brain Storm

1. What is meant by E-Commerce?

2. What are all the benefits of E-Commerce?

3. What are all the various services involved to improve E-Commerce? Explain.

Lecture 2

E-Commerce and its Types

Objectives

In this lecture you will learn the following

- What are all the various types of E-Commerce?
- About EDI
- Projects involved in E-Commerce

Coverage Plan

Lecture 2

2.1 Snap Shot

Electronic commerce solutions involve doing business online. Businesses want to harness the power of digital information to understand the needs and preferences of customers and trading partners and then deliver the products, services and information to them as quickly and with as little human interaction as possible. Companies enticed by the promise of delivering targeted, personalized, automated goods and services are engaging, exchanging order, inventory and billing information with partners, on-line banking and corporate purchasing applications that extend their enterprise to key trading partners.

2.2 Types of Electronic Commerce

Electronic commerce can be categorized into four categories:

- Business to Consumer
- Business to Business
- Consumer to Consumer
- Consumer to Business

Currently, the first two categories are the most popular models of e-commerce

Business-to-Consumer Model

In this model, commerce is conducted between a business to consumer, such as a home user on a PC. For example, to buy books or CD's on the Internet, the consumer accesses the Internet site of that particular business and makes the purchase.

Business –to-Business Model

In this model, commerce is conducted between two businesses. It includes trading goods like business subscriptions, professional services, and wholesale dealing. Sometimes, business may exit between virtual companies, neither of which may have physical existence.

Consumer-to-Consumer Model

In this model, commerce is conducted between two consumers. This can be seen in auction bidding houses. Here, commerce between a consumer who is auctioning and consumers who are bidding for it. The consumer who is auctioning decides the price of the product. The consumers, who are bidding, analyze the product and decide how much they are willing to pay for it.

Consumer-to-Business Model

In this model, commerce is conducted between a consumer and a business. In this model the goods are produced and the consumer rather than supplier dictate the price of the product. This may revolutionize the way business are conducted over the Web or even otherwise.

The following diagram displays multiple different commerce communication and solution possibilities between Business-to-Consumers (B2C) and Business-to- Businesses (B2B) . For example the arrow marked 'A' displays an instance of B2C solution where a consumer can place an order for product with a distributor and or retailer. This commerce solution can be further extended to a B2B solution as indicated by the arrows marked 'B'. Here trading information and communication between partners (in this case the partners being distributor/retailer, some corporation and suppliers) is being exchanged electronically using agreed upon protocols implemented through specific commerce solutions put in place to facilitate this interchange.

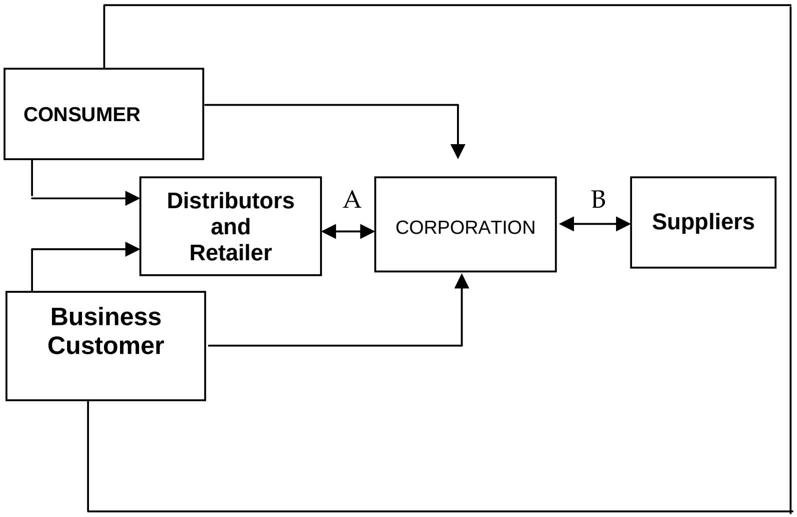


Figure 2.1 Electronic Commerce Communication.

Based on these two broad categories (B2C and B2B), the three main scenarios or service areas where companies conduct business online today are as follows:

N Direct Marketing & Selling (B2C)

N Supply Chain Integration(B2B)

N Corporate Procurement(B2B)

2.3 Direct Marketing & Selling

Selling over the Web allows businesses of all sizes to reach consumers all over the world. This requires that businesses provide consumers with an engaging shopping experience, run price promotions, cross-sell items and accept typical consumer repayment methods such as credit cards. Further, when an order is placed through organization's web site, consumers must be able to track it. Commerce solutions sell to consumers must be able to map to existing business processes, and integrate with multiple databases and/or accounting systems.

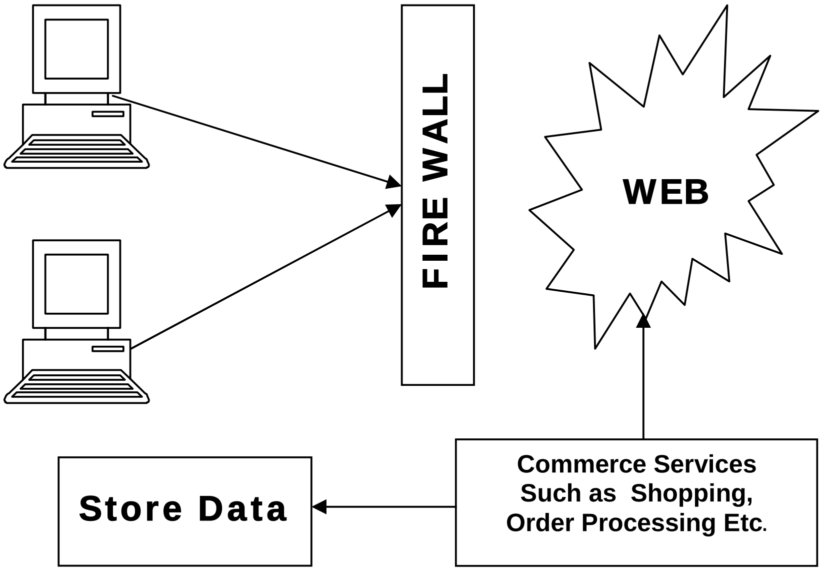
Today, more Web sites focus on direct marketing, selling, and service than on any other type of electronic commerce. Direct selling was the earliest type of electronic commerce, and has proven to be a stepping-stone to more complex commerce operations for many companies. Successes such as Amazon.com, Barnes & Noble, Dell Computer, and the introduction of e-tickets by major airlines have catalyzed the growth of this segment, proving the reach and customer acceptance of the Internet. Across consumer-targeted commerce sites, there are several keys to success:

- Marketing that creates site visibility and demand: targets customer segments with personalized offers; and generates qualified sales leads through observation and analysis of customer behavior.
- Sales-enhancing site design that allows personalized content and adaptive selling processes that do more than just list catalog items.
- Increased sales-processing capabilities that provide secure credit card authorization and payment, automated tax calculations, flexible fulfillment, and tight integration with existing back-end systems such as inventory, billing and distribution.

- Automated customer service features that generate responsive feedback to consumer inquiries: capture and track information about consumer requests; and automatically provide customized services based on personal needs and interests.

This business-to-consumer electronic commerce increases revenue by reaching the right customers more often. Targeted and automated up-selling and cross-selling are the new fundamentals of online retailing. Sites that most frequently provide the best and most appropriate products and services are rewarded with stronger customer relationships, resulting in improved loyalty and increased value.

Figure illustrates the architectural framework of a Direct Marketing & Selling.



Follow these steps to build a Direct Marketing and Selling Systems

Step 1 Dynamically built HTML pages to engage customers over the common transport.

Step2 Storage of member (customer) information for site personalization, member authentication, and the tools to manage them.

Step 3 Implementation of the "shopping basket" metaphor

Step 4 Server and Administrative security

Step 5 Customer information security

Step 6 Manage and process orders, implement business rules to transact with customers.

2.4 Supply Chain Integration

Supply Chain integration, also known as Value Chain integration, uses the low cost of the internet to highlight a tighter integration across suppliers, manufacturers, and distributors. Many of the fundamentals of building a site, extensible order processing and integration with other systems remain the same as that in the Direct Marketing & Selling scenario. But in the Supply Chain scenario, new requirements arise including authenticated log-in, generating custom catalogs for key customers and pricing and payment based on custom agreements. Suppliers need to their existing Web site or be able to “push” catalogs into another business’s systems with the ability to maintain these product catalogs when pricing and/or inventory changes.

2.5 Corporate Procurement

Businesses want to leverage the intranet and the Internet to make existing business processes more efficient .At the heart of the business model are commerce solutions that facilitate the process of purchasing low-cost, high volume goods for maintenance, repair, and operations(MRO) of a business. Labour and paper-intensive operations are converted into self-service applications where purchase approvals and business policies are enforces through automated business rules.

Approved purchase orders then need to be sent to suppliers. Corporate Procurement commerce solutions allow for transactions to be made with partnering businesses, suppliers and distributors, regardless of the data format, and data is communicated, whether it be over the Internet, an EDI VAN (Value- Added Networks), e-mail, or simply fax.

2.6 Electronic Data Interchange

The prime ingredient in Electronic Commerce is electronic communication. Electronic communication is the cornerstone of electronic commerce. It includes technologies such as electronic mail (e-mail), telecommuting, computer-to-computer FAX, video teleconferencing, electronic funds transfer (EFT) and electronic data interchange (EDI). It is one of the simplest and least expensive steps toward implementing electronic commerce. It will increase your capability to communicate with customers and other business partners.

Electronic Data Interchange (EDI) concerns the exchange of transaction data between business partners in a standardized electronic format. These standard EDI formats have been issued by the American National Standard Institute (ANSI) and are generally referred to as the X.12 standards. Many types of forms are defined, each relevant to the type of transaction that is being conducted. An application, such as order-entry or accounts payable, "translates" the internal native format of the data into offering of sexually explicity materials are just two types of socially objectionable commercial services which may involve offering electronic versions of copyrighted materials without permission or payment of royalties. The ethical, legal, and policy issues involving electronic commerce are complex and will be the subject of public debate for a long , long time.

2.7 Major projects in Electronic Communication

Many companies in several industries have experienced the benefits and realized the need to use Electronic Commerce to survive. Large Companies such as Sears, General Motors (GM), and Wal-Mart have championed electronic trading practices for their suppliers. Indeed, in some industries EDI has become a virtual necessity for doing business. Some example of the benefits of Electronic Commerce are given below.

Wal-Mart Stores, Inc In the 1980's Wal-Mart Stores, Inc., experienced explosive growth in sales, rising to number one in the U.S retail business. Despite its rapid growth, Wal-Mart's investment of half a billion dollars in computer and satellite communications networks, bar code systems, scanners, and other "quick response" equipment linking each point-of-sale terminal to distribution centers and headquarters in Bentonville, Arkansas, enabled the company to maintain high service levels and increase sales while preserving one-fourth the inventory investment. By empowering its individual stores to order directly from suppliers, even overseas, Wal-Mart stores reduced inventory restocking time from an industry average of six weeks to thirty-six hours. Moreover, by tracking every sale to see what was selling and what was not, Wal-Mart stores were better able to keep their stores well-stocked while maintaining tight inventories and low prices.

General Motors In building a brand new facility in which to manufacture its Saturn cars, General Motors developed an information infrastructure to enable Saturn and its numerous suppliers to operate as one company. Through the implementation of a production scheduling database and the use of electronic data interchange, Saturn and its suppliers reduced overhead in all organizations, increased cooperation's unwritten rule book: treat vendors as adversaries. Located in Spring Hill, Tennessee, the Saturn plant includes an online manufacturing database which is accessible by component suppliers who do not wait for GM to send a purchase order, but simply consult the car maker's production schedule, included in the database. In this process there is no paper-no purchase order and no invoice. After the parts are shipped, the vendor sends an electronic message to Saturn saying, in effect, "These are the parts we have sent you." When the box of goods arrive, the receiving clerk scans the bar code printed on it with an electronic wand, The computer can then tell the receiving clerk to what part of the plant the goods should go. The scanning also initiates payment to the vendor.

Clearinghouse for Inter Bank Payment Systems

Over the past decade, the banking and financial industries have invested heavily in automation and networking technologies to handle and process electronically an ever-increasing number of financial transactions. For example, the Clearinghouse for Inter Bank Payment Systems coordinates daily bank-to-bank transactions worth nearly $2 trillion while the nation's network of more than 75,000 Automated Teller Machines (ATMs) handles more than 6 billion transactions per year.

The Defense Medical Logistics Standard Support

The Defense Medical Logistics Standard Support (DMLSS) system has embraced Electronic Commerce concepts of business process redesign and EDI to obtain an estimated $3.2 billion savings over 12 years from an investment of $120 million. Savings come from reduced inventories and the leverage of the civilian health care supply industry to streamline DoD operations.

The U.S Customs Service

The U.S. Customs Service, one of the leaders in the federal sector for adoption of EDI, today processes 94 percent of all customs declarations electronically and collects 60 percent of all duties electronically. By moving from paper to electronic declarations, Customs reduced error rates from 17 percent to 1.7 percent, a whole order of magnitude. In addition, it save an estimated $500 million in processing costs each year while increasing annual productivity an estimated 10 percent each year.

2.8 Short Summary

- B2C - In this model, commerce is conducted between a business to consumer, such as a home user on a PC.
- B2B - In this model, commerce is conducted between two businesses.
- C2B- In this model, commerce is conducted between a consumer and a business.
- C2C- In this model, commerce is conducted between a consumer and another consumer.

2.9 Brain Storm

1. What are the various types of E-Commerce?
2. Explain each one the type of E-Commerce.
3. What do you mean by Direct Marketing & Selling?
4. What is EDI stands for?

Lecture 3

Application of E-Commerce

Objectives

In this lecture you will learn the following

- About Application of E-Commerce
- Value & Supply Chain Integration
- Examples of Today's E-Commerce Solution

Coverage Plan

Lecture 3

3.1 Snap Shot

Electronic commerce combines the advantages of computer-based processing (speed, reliability, and relatively high volumes of data) with the advantages of people-based insight (creativity, flexibility, adaptability). Electronic commerce enables people to review, analyze, add value, and sell a variety of products that are represented electronically, such as reference material, textbooks and training materials, entertainment, and software.

3.2 Applications of E-Commerce

Currently, there are three tiers in the electronic market-place, offering opportunities for companies of all sizes.

Tier 1. Electronic classified advertisements, which identify the item (or service) for sale, the price, and information necessary for contacting the seller. Electronic classifieds are analogous to print classifieds and are retrieved by the potential buyer.

Tier 2. Includes the characteristics of the first tier, but adds decision-support materials to the information available which help the user reach a purchase decision. Such marketplaces may include such information as product reviews from an industry magazine.

Tier 3. Includes the features of the first two tiers, but adds the ability to electronically match appropriate buyers and sellers. These electronic marketplaces may provide confirmation of a completed transaction through electronic or printed receipts. Automated matching technology, such as that used to trade foreign exchanges or software-based intelligent agents, are examples of technologies that can automatically match buyers and sellers.

By extension, applications of electronic commerce can include the following:

Electronic funds transfer: Extending and completing the procurement process by providing buyers with the ability to rapidly and cost-effectively make payments to sellers and shippers with less financial risk and fewer errors, while reducing paper-handling and storage requirements (this is more typical of EDI and banking networks).

Enterprise integration: Extending integration throughout a company, including other trading partners. Business process reengineering can be employed to improve communication within a company or by outsourcing to other companies and using electronic commerce like tools to manage the relationship. The result is the virtual corporation; this provides vertical integration of companies with their suppliers, as well as horizontal integration of segments of a company.

Computer-supported collaborative work. Expanding collaborative activities, such a supporting joint development of requirements, maintenance documents, and so forth, within or across companies. The intent is to remove the barriers (time, space, information complexity, etc.) that inhibit creative interactions among people. Teaming may take place at either the company or individual level, creating a just-in-time virtual resource for delivery of the right human and business resources for a job. This gives corporations the opportunity to increase chances of success, to share economic successes more broadly, and to give the customers a mix of capabilities more exactly meeting their requirements.

Government regulatory data interchange. Collecting data from and returning data to various communities to enable the government to carry out its mandated responsibilities for instance, organizations that transport hazardous materials, corporations and banking institutions that submit financial reports, and public health officials who report health statistics and epidemiological incidents.

3.3 Value Chain Integration

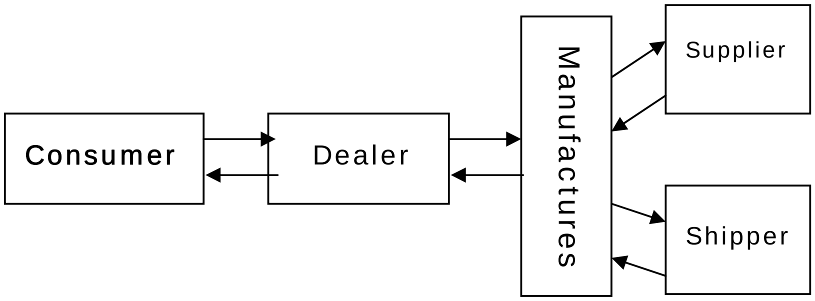
No other business model highlights the need for tight integration across suppliers, manufacturers, and distributors quite like the value chain. Delays in inventory tracking and management can ripple from the cash register all the way back to raw material production, creating inventory shortages at any stage of the value chain. The resulting out-of-stock events can mean lost business. The Internet promises to increase business efficiency by reducing reporting delays and increasing reporting accuracy. Speed is clearly the business imperative for the value chain.

Unfortunately, speed can be costly. Today, approximately 50,000 businesses exchange business documents such as orders and invoices with their trading partner through a standard communication and content protocol called Electronic Data Interchange (EDI). Most EDI implementations use leased lines or Value Added Networks the require significant integration for each trading partner. Network design, installation and administration can be costly in terms of hardware, software, and staff. In fact, these costs are the key reason that EDI is most widely deployed only in larger companies.

Moving forward, all companies will be able to take advantage of value chain integration through the low cost of the Internet. Open standards for electronic document exchange will allow all companies to become Internet trading partners and function as suppliers, consumers, or both in this business-to-business electronic commerce. This integrated trading will tighten relationships between businesses while offering them greater choices in supplier selection.

3.4 Supply Chain Integration

This case study covers where a business buyer purchases goods from a supplier. Often this is simply described as "supplier-side purchasing" by distributors, manufacturers, retail merchants, transport providers, distributors and other business buyers. The full power of electronic commerce is harnessed by creating seamless chains of materials and services that work together to supply the needs of the consumer. This helps participants plan more effectively and adapt to changing business conditions rapidly. Fig illustrates the chain that links various entities in a Supply Chain solution.



An example of how a Supply Chain Integration may work, as a case study let's use an order of new PC as a case study. The process has the following steps:

1. A customer submits an order for a new computer system through a dealer's Web site.
2. The dealer receives the order. Receipt of the order automatically generates a query to the manufacturer of the computers (case, microprocessor, memory, monitor, CPU, and so on) that make up the system.

3. Receipt of the query by the computer manufacturer automatically initiates a query to the parts inventory database of the computer manufacturer. The query results show that the computer manufacturer does not have the microprocessor in stock needed to fulfil the order. The computer manufacturer's inventory system contacts the microprocessor supplier and places an order for the necessary parts.

4. The microprocessor supplier's system informs the computer manufacturer of the earliest possible date for delivery of the microprocessor and places the order of the chip.

5. Using this date as input, the computer manufacturer calculates the date by which it could have the computers built, based on the schedule of available capacity on its manufacturing floor. Then generates a query to the shipper's computer.

6. The shipper's system checks its own transport capacity and determines that it will be able to schedule and provide delivery of the computer.

7. The computer manufacturer then confirms the order with the dealer's system.

8. Finally, the dealer sends confirmation to the consumer.

Follow these minimum steps to build a Supply Chain Integration system.

Step 1 Dynamically built HTML pages to engage customers over a common transport

Step 2 Storage of member (buyer / requisitioner) information for site personalization, member authentication, and the tools to manage them.

Step 3 Implementation of the "Purchase Requisition" metaphor similar to the virtual "shopping basket".

Step 4 Server and Administrative security.

Step 5 Customer information security.

Step 6 Manage and process orders, implement business rules to transact with customers.

Step 7 Ability to advertise other products and services and manage the process.

Step 8 Facility to store data (catalog, orders, inventory, logs, and so on) and access it dynamically.

Step 9 Management of merchandise, transactions, and the commerce system

Step 10 Tools for price promotions.

Step 11 Secure log-in and password authentication when entering a trading partner site.

Step 12 Secure exchange of business information between trading partners

Step 13 Integration with backend financial and /or inventory management systems.

Step 14 Catalog management.

Step 15 Price calculation depending on classes of accounts, purchase history, credit, territory, and so forth.

3.5 Corporate Purchasing

The Internet offers tremendous time and cost savings for corporate purchasing of low-cost, high-volume goods for maintenance, repair, and operations (MRO) activities. Typical MRO goods include office supplies such as pens and paper, office equipment and furniture, computers, and replacement parts. The Internet can transform corporate purchasing from a labor-and paperwork-intensive process into a self-service application. Company employees can order equipment on Web sites; company officials can automatically enforce purchase approval and policies through automated business rules; and suppliers can keep their catalog information centralized and up-to-date. Purchase order applications can then use the Internet to transfer the order to suppliers. In response, suppliers can ship the requested goods and invoice the company over the Internet. In addition to reduced administrative costs, Internet-based corporate purchasing can improve order-tracking accuracy; better enforce purchasing policies; provide better-customer and supplier service; reduce inventories; and give companies more power in negotiating exclusive or volume-discount contracts.

3.6 Financial and Information Services

A broad range of financial and information services are performed over the Internet today, and sites that offer them are enjoying rapid growth. These sites are popular because they help consumers, businesses of all sizes, and financial institutions distribute some of their most important information over the Internet with greater convenience and richness than is available using other channels. For example:

- **Online Banking** Consumers and small businesses can save time and money by doing their banking on the Internet. Paying bills, making transfers between accounts, and trading stocks, bonds, and mutual funds can all be performed electronically by using the Internet to connect consumers and small business with their financial institutions.

- **Online Billing** Companies that bill can achieve significant cost savings and marketing benefits through the use of Internet-based bill-delivery and receiving systems. Today, consumers receive an average of 12 bills a month by mail from retailers, credit card companies, and utilities.

- **Secure Information Distribution** To many businesses, information is their most valuable asset. While the Internet can enable businesses to reach huge new markets for that information, businesses must also safeguard that information to protect their assets. Digital Rights Management provides protection for intellectual and information property, and is a key technology for secure information distribution.

3.7 Examples of Today’s E-Commerce

The successful extensions of electronic commerce into (these) more complex areas is dependent on the integration of communications, data management, and security services into a ubiquitous, user-friendly, easily accessible electronic marketplace that encourages and enables the seamless exchange of information. The Internet, CD-ROM based catalogs, and private on-line services are the most viable media for creating on-line marketplaces at this time. Interactive TV, screen phones, and kiosks have not experienced significant market penetration in the recent past.

As an illustrative example, Cisco was planning to transact $1 billion per year by mid-1997 on its business to business Web site. Optimism for Cisco's commerce site, which can be used to purchase and configure six-figures-priced routers, has been buyed by customer reports that on-line ordering is more efficient and accurate than traditional sales methods. This site provides the following services.

- Users can select, configure, and order products and support.
- It supports predefined customer profiles that expedite orders and limit errors.
- Customers can check on the status of their orders or service requests, cutting the previous interval of 2 to 5 days.
- Users get up-to-the-minute pricing.

The company will expand the number of registered customers beyond the initial, select key accounts which were authorized to use the service. Cisco's site is the largest single site (by revenue measures) so far. The Cisco site utilizes Secure Sockets Layer (SSL) (discussed later), password association, and proprietary IP traps for security. Other select examples include the following:

Books: Amazon.com (http://www.amazon.com) offers over a million titles at discounts and lets the buyer see readers' comments on recent titles before they buy.

Travel services: USAir (http://www.usair.com) and American Airlines (http://www.americanair.com) let people sign up to receive e-mailed notices of inexpensive tickets on flights with empty seats. American also sells such seats through on-line auctions. OnLine (http://www.priceonline.com) offers a wide range of travel services and more than 5000 name-brand items at discount prices: cruises, hotel rooms, sporting goods, jewelry, china, crystal, small appliances.

Automobile specifications, delivery timetables, pricing, and even purchasing: Auto-by-Tel (http://www.autobytel.com), Dealernet (http://www.dealernet.com), and Microsoft's CarPoint (http://carpoint.msn.com) show how new cars stack up against competing models, including price and feature comparisons. Using the service is like reading through car magazines at high speed. The classifieds at Yellow Pages Online (http://www.ypo.com) allow used-car shoppers to quickly identify nearby offerings at desired ranges of price, year, model, and mileage. Auto-by-Tel (http://www.autobytel.com) matches car buyers nationwide with close-by dealers who, with lower selling costs thanks to the service, sell for less.

Flowers: 1-900-Flowers (http://www.800flowers.com) and PC Flowers (http://ww.pcgifts.ibm.com).

Computers: NecX (http://www.necx.com), CNET (http://www.cnet.com), and. pcOrder.com (http://www.pcorder.com) let corporate buyers tailor computer systems on-line to meet their needs, then compare different vendors' prices for those configurations. Onsale (http://www.onsale.com) auctions off over $1 million a week of refurbished personal computers and other consumer electronics items. Price Watch Corporation (http://www.pricewatch.com) discloses the latest street prices for various vendors' computer products in a database that it claims is updated.

EDI service: Premenos (http://www.premenos.com) and Edify (http://www.edify.com).

N **Advertising services:** Modem Media (http://www.modemmedia.com) and ada Market (http://www.adamarket.com).

N **Magazines:** Salon (http://www.salon1999.com) and Hot Wired (http://www.hotwired.com).

N **Banking and investing:** American Banking System (http://www.absbank.com), American Express (http://www.americanexpress.com), Check Free (http://www.checkfree.com), Checkpoint Software (http://www.checkfree.com), Citibank (http://www.citibank.com), Fidelity Investments (http://www.fidinv.com), Intuit (http://www.intuit.com), Mark Twain Bank (http://www.marktwain.com), and Charles Schwab (http://www.schwab.com).

N **Internet shopping malls:** CommerceNet (www.commercenet.com), Continuum (www.continuumsi.com), CyberCash (www.cybercash.com), Downtown Anywhere (www.awa.com), eShop (www.eshop.com), Internet Commerce Group (www.incog.com), Net Market (www.netmarket.com), and Open Market (www.openmarket.com).

3.8 Short Summary

- Electronic commerce enables people to review, analyze, add value, and sell a variety of products that are represented electronically, such as reference material, textbooks and training materials, entertainment, and software.

- No other business model highlights the need for tight integration across suppliers, manufacturers, and distributors quite like the value chain.

- The Internet offers tremendous time and cost savings for corporate purchasing of low-cost, high-volume goods for maintenance, repair, and operations (MRO) activities.

3.9 Brain Storm

1. Explain about the Applications of E-Commerce.
2. What is meant by Value Chain Integration?
3. What is meant by Supply Chain Integration?
4. Explain about Corporate Purchasing.
5. Explain briefly Financial & Information Services.

Lecture 4

E-Commerce Opportunities & Commercial Transactions

OBJECTIVES

In this lecture you will learn the following

- Knowing about E-Commerce Opportunities with www/Internet
- E-Commerce Tools
- Model of Commercial Transactions

Coverage Plan

Lecture 4

4.1 Snap Shot

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 sent. 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 going to be discussed here.

4.2 On-line Web selling

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

- **Toll-free or other telephone number**. 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 on line while browsing for goods.

- **Shopping clubs**. This approach requires new customer to join the club by submitting their credit card information via fax or telephone and subsequent purchase are billed to the credit card.

- **Off-line ordering and paying**. In this approach, customer sent 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.

Virtual malls This 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 my 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	http://branch.com:1080
Market Place.com	http://marketplace.com
Interactive Super Mall	http://supermall.com
Downtown Anywhere	http://awa.com
GNN Direct	http://gnn.com/gnn/gnndirect
Internet Mall	http://www.meckerweb.com:80/imall/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 $ 15000 per month to have a direct link its home page. Netscape Communication has charged $40,000 for a three-month advertisement placement on its Web site . 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, then use this demographics information to narrow cast or point cast ads to the user/consumer.

4.3 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 page that corporate 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) transactions security over the Internet.

Note, however, that even if on-line shopping increased from $540 million in 1996 to $6.6 billion in 2000 as predicted by Forrester Research, that still would not make the Web a major force in retailing, since mail-order catalog sales alone were expected to reach $75 billion in 1996.

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 "computer niks" than "communications" 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 measure, 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 types 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.

4.4 Customer service and technical support

The Internet is being used by many companies (e.g. Cisco) to provide customer service and technical support functions. Business can provide software fixes to their customers via Internet e-mail, FTP, or Web server. Providing an FTP host site can give customer easy access to a library of a company's software programs, documentation, and upgrades. FTP sites can eliminate the expense of generating floppy disks for large scale mailing to distribute software releases and upgrades. Businesses can also set up newsgroups which can act as a bulletin board system where customer can chat about the companies products. Internet e-mail can also be used to communicate problems or question to a company's customer support staff. In addition, a company can post a FAQ (frequently asked question) message about a product, with the purpose of anticipating general question that customer might have. Utilizing Internet e-mail as a way to field technical questions from customers reduces taking calls via an 800/888 telephone number (which the organization must pay for on a per minute basis). Another way for companies to offer customer support information is by publishing databases of technical information in a searchable format by using tools such as Gopher, WAIS or the Web.

Business Information research. Companies can utilize the Internet to do research on competitors and to find other business information. Gathering timely market intelligence is critical for any business. There is a plethora of information available on the Internet. Some is valuable. Other is dated. URLs can be good or no longer valid. Nonetheless the Internet can be a place to start the search. For example, EDGAR (http:// edgar.stern.nyu.edu/ EDGAR.html) is an Internet database set up by the Securities and Exchange Commission where every publicly traded company files financial results on an annual and quarterly basis. Another useful database is the State Department Travel Advisories (http: //www stolaf.edu/network/travel-advisories.html); this database provides the text of U.S Department of State reports that provide global travel information. Organizations can find data about specific companies via a search engine or by trying to open a URL that is logically given the name of the company. Most companies have servers and home pages that conform to the naming convention of http://www.company_name.com/.

Search engines. To assist companies in undertaking the kind of business research just described, search tools have emerged. Early engines have worked at finding sites and documents. These search tools may soon be expanded to help consumers comparison shop for bargains. A well known Internet search engine is Yahoo (http://www.yahoo.com/) . It provides databases on a variety of topics including arts, business and economy, computer and the Internet, education, entertainment, government, health, news, recreation, references (including libraries, dictionaries, phone books, Internet addresses, etc) regional information(by state, country, or region.) science social science, and society and culture. Users of Yahoo can also do generic searches by keyword. Another excellent search engine is Alta Vista (http://www.altavista.com)

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 user 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 news groups and mailing lists. Once a press release is posted to a 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 message a company posts on the Internet. This signature at the end of the message is typically a couple of lines about the company and represents a low key way to advertise.

4.5 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-1980's; 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 of 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.

4.6 Electronic Mail

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 multicast 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 executables and other files incorporating binary data (I, e Word for Windows files and Excel spreadsheets). A 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 data, 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 receivers 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 writs monthly newsletter covering topics of interest to the company's customers. 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.

4.7 Newsgroups

News groups 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. Newsgroups 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.

4.8 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.

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.

4.9 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 this 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.

4.10 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 users 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 document as priori. Indexing of documents allows for quick searches when users and queries to the WAIS database. Together, the index software and the WAIS database server allow users to create database 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 preceded, newer WAIS software supports further searches by allowing the user to place entire documents into the key word 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 users 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 or larger than the original document itself. WAIS servers with a large number of documents pay a premium in disk space.

4.11 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 drawing can be accessed and retrieved. Gopher also gives the user tools to locate information on specific topics from computer systems around the world. However, for the general e-commerce planner/user WWW may be better suited.

4.12 World Wide Web

The World Wide Web is the newest and most user friendly information service on the Internet WWW has the ability to incorporate FTP, WAIS Gopher e-mail and FTP applications through one user interface. Before WWW applications were available (they started to appear in the early 1990s) a user would need and FTP client to connect to an FTP archive, a WAIS client to search a WAIS server, and a Gopher client to get to a Gopher server. A Web server provides access to all of these services to enable, among other things, Web-based commerce. By creating home page on the Web, organizations are publishing their message to the world. Potential customers who stop and look can access a marketing message and use it to find out more about the company's products and services.

Web sites are referred to by their Uniform Resource Locator (URL) address which specifies and information object on the Internet such as an HTTP link or an FTP archive. All URLs indicate the type of object, a colon, then the address of the object, and any further information required. WWW documents are expressed in Hyper Text Markup Language (HTML). Web servers transfer HTML documents to each other through the Hyper Text Transfer Protocol (HTTP). Graphical Web browsers such as Netscape Navigator and Microsoft Explorer read HTML syntax and produce a point and click windowing interface for the user. HTML allows programmers to insert links which, when exercised by the user, transfer the user to another Web page on the same or on a different server. These hypertext links can bring the user to another HTML documents, a directory in an FTP archive, a Gopher server, or a WAIS database.

HTML documents give businesses the opportunity to communicate through graphics, text, sound and to link to other sites and e-mail. A company's WWW home page can be viewed as an interactive bulletin board to the world. Companies can have definitions to technical terms, allow users to access search databases of available products, provide pictures of available products in a catalog, supply sound files and picture clips, and so on to establish improved communication with customers. Home pages can also support input forms which can help companies collect user information, such as comments on a product on service which can be used to design new marketing and advertisement strategies or improve existing ones.

First generation home pages have a number of limitations. For example animation is not possible using HTML. This limitation can be overcome by languages such as Java, developed by Sun Microsystmes. An applet can be incorporated into HTML documents to provide animation. An applet is the collection of Java code that makes up an animation or other application. Applets make the World Wide Web a more effective advertising medium. For example, an applet would allow a brokerage firm to provide quotes that self update every few minutes.

Other important capabilities of the Web include directories and searching tools, these can be used to find businesses on the Internet. Yahoo, InfoSeek, and Alta Vista are some examples which were already discussed. These directories make an organization visible on the Internet the Internet is large and without visibility, a business could sit on the Web and never be noticed

4.13 Agent

Agent are becoming a useful tool for businesses and customers. An agent is a software program that is designed to automatically perform specific tasks. A customer's agent could search Web stores for the lowest price on a specific product (e.g. a book or a music CD) or check to see if certain URLs have been updated. A business might use an agent to look for competitors on the Internet. Agents are useful tools because they free organization from laborious activities, like searching the Internet. They have the potential to revolutionize the way that customers and businesses gather information.

Bargain Finder (http://bf.cstar.ac.com/bf/) is an example of an agent that searches compact disc stores on the Internet. The user enters the name of an album and Bargain Finder searches for the best price available . This agent is a limited in features, but it can be useful for a customer that wants a product at the lowest price possible.

With Web Watch

(http://www.specter.com/user/janos/spectper/webwatch.htm) a user can specify pages for the agent to monitor for changes Web Watch then will display a list of the pages and tell the user when they were last modified. Web Watch also notifies the user if the pages are no longer in existence or have changed URLs. This can be useful for businesses that wish to monitor competitors home pages. Customers could use Web Watch to monitor business pages to see if new products or information are being offered.

However, some predict that Web merchants will erect barriers to automated price comparison shopping in order to prevent their markets from being mercilessly commoditized. Sellers, for example, might offer an array of slightly different, frequently updated models through different distributors, making price comparisons almost impossible,. And anti agent systems may proliferate in 1995 when Andersen Consulting launched Bargain Finder, on-line sellers blocked it from retrieving their prices.

4.14 The Model of Commercial Transactions

This section examines some of the issues involved in electronic commerce by taking a look at what happens in the course of any commercial transaction. It focuses on the issues involved in a simple retail transaction, since virtually everyone is familiar and comfortable with this type of transaction.

Establishing Trust

Before any purchase can be made from a retail store, a customer must enter it. Most shops are open to the public, so all it takes is for a customer to walk in. However, this is not always the case: The merchant may control access to the goods it offers in several different ways. It can sell to any and all comers through an open storefront, or it can restrict its sales to a certain clientele (wholesales may sell only to resellers; exclusive merchants may do business only with referred customers). The merchant can decide which customers to give access to its merchandise and how that access is provided.

The consumer also makes choices prior to entering a store. The consumer must determine, often by just looking in a display window whether the establishment carries the product being sought out and whether the establishment is a reliable place to do business. To entice customers, the merchant may display brand names of the product carried, stickers on the door indicating payment methods accepted and sample products. Additional customer acceptance can also be gained through use of a well-known company name, by being a branch of a franchise holder of a nationally known company.

The degree to which the merchant will restrict access to its product will vary, depending on the type of business. An automobile dealer will require a driver' license before permitting a test drive; although most bookstores don't mind strangers browsing through their books, some buyers may encourage it by providing tables and comfortable chairs for such browsers. Likewise buyers may be more careful about selecting vendors of products that can affect their health or well-being (such as prescription drugs) or safety are about buying products there are relatively benign (household items or musical recordings) or inexpensive (newspapers).

The merchant and the customer each establish a level of trust in the other. The merchant trusts that the consumer is a potential purchaser, capable of selecting and paying for some product offered; the consumer trusts that the merchant may be offering the desired product and will be capable of delivering (and servicing, if necessary) that product if needed.

There are other identities issues that both buyer and seller are concerned with when first initiating contact. Many products have distribution limits. For example:

- Prescription drugs may not be dispensed to anyone without a legitimate prescription.
- Alcoholic beverages may not be sold to minors.
- Firearms and ammunition are subject to a wide range of restrictions, varying by locality.

- Tobacco products may not be sold to minors.

Establishing trust between parties in a commercial transaction that takes place across a public network is difficult. While the merchant can use judgment during in-person transactions, online transactions offer no opportunity to exercise judgment because it is difficult to correlate identities on the Internet with actual individuals. Electronic merchants cannot afford to trust everyone – or even to trust anyone.

The same goes for the consumer. There is no way to tell how long a Web page has been in existence, or whether it will be there tomorrow. Constructing a counterfeit Web page, representing as part of a large corporation, is much easier than constructing a counterfeit retail outlet, restaurant, or supermarket, and potentially more lucrative.

Online transactions require mechanisms for establishing the trust between prospective buyers and sellers. The merchant's overall presentation, on- and offline determine the consumer's level of trust. The Web page presentation content – products, descriptions pricing, and delivery – will help the consumer to make a decision.

Negotiating a Deal

Determining the item to be purchased, and the price to be charged are trivial matters in most retail stores. The buyers select the desired item, and the price is usually clearly marked either on the item itself or near its display area. In most cases, this is all that is necessary.

The validity of the merchant's offering price, as well as the exact identity of the item desired by the customer, is easy to determine in a retail store. Electronic transactions sometimes require special mechanisms to ensure that the buyer did, in fact, place an order, and that the seller did, in fact offer the product for the specified price.

Ordering products over the Internet does not offer an explicit method to reference the offering price. This problem can be solved to some extent. When more companies conduct their business online that sell similar products, by making comparison, right price of a desired product can be determined to some extent.

Payment and Settlement

At the heart of any transaction is the exchange of values, generally some standardized currency traded for some product or service. In the traditional commerce this process is straightforward: the buyer gives cash, a cheque or a credit card and receives in return the product purchased and a receipt.

Translating these actions into electronic form takes some doing. Many participants will want the entire process to be private; after all, most consumers would not announce their credit card numbers out loud in a crowded store. There are mechanisms, which allow payment information to be kept private, by encrypting it, by keeping it entirely offline, or by using third parties to settle transactions.

In the store, the transaction is completed as soon as the buyer pays for an item: The buyer can then walk away with the purchase. Over the Internet, unless the product being purchased is available digitally (information, pictures, software, or other information-based products), the buyer must trust the seller to deliver the goods. One way the consumer can avoid problems is by patronizing trusted Internet vendors; another way is to use a major credit card company that will back up the consumer in the event of a problem with a vendor.

The vendor takes a smaller risk when selling online, since credit cards can be authenticated through automated connections to settlement companies. This is similar to the authentication done in person when a clerk uses a credit card authorization terminal (“swipe box”) to verity a credit card. Both parties to an online transaction can benefit from the use of digital signatures .

Payment Vehicles and Currencies

A great deal of attention is focused on consummation of the online transaction – as it should be, since this is the point at which values are exchanged. The offline buyer has many options for transacting exchanges, of which the most common are cash, universally accepted and totally anonymous; personal check, credit, ATM card, no-questions-asked credit extension etc.

When presented in person, all these payment methods are subject to some degree of scrutiny. Merchants may examine large-denomination bills for counterfeits (or refuse to accept large bills); may accept personal checks only if the customer offers sufficient personal identification; and may verify identity and signature when accepting credit cards.

Similar mechanisms for using electronic currencies, personal checks, and credit card are available for electronic transactions. Digital currencies are being developed to allow anonymous transactions across public networks such as the Internet. Digital signature technologies permit the authentication and certification of digitally transmitted documents like personal checks. These transactions, including credit card transactions, can use special encryption methods to ensure reliability and privacy.

Products and Delivery

Merchants who sell physical items have to physically deliver them to the customer. So they need to inspire a greater level of trust in their customers; after all, those customers must wait for a delivery, and they may not be convinced that the product will arrive, until the delivery. Merchants may allay some of these fears by giving the buyer detailed delivery information (when the product will be packed and shipped, how the product is to be shipped, approximate delivery date and time).

However this problem does not occur for the digital products as they can easily be delivered electronically. Delivery of digital products online raises issues that parallel those raised by online transactions. Some vendors may want to ensure that a third party cannot eavesdrop on the product transmission and gain use of the material being sold without paying for it. Buyers want to ensure that they are getting the material they requested, from the source they requested. Everyone wants to ensure that the material received by the consumer has not been altered in any way by any third parties. These issues can be resolved using the tools that make secure and reliable transactions possible online.

4.15 Short Summary

- 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.

- Virtual malls is the combination of the home PC and the Internet is making on line services and shopping easier to implement.

- 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 is user to a limited set of commands.

- The World Wide Web is the newest and most user friendly information service on the Internet.

4.16 Brain Storm

1. What are the four ways in which Web Commerce can be undertaken over the Internet?
2. Explain Virtual malls.
3. Explain about various Tools which are involved in E-Commerce.
4. What do you mean by Agent?
5. Explain about Model of Commercial Transactions.

Lecture 5

Electronic Cash and Electronic Payments Schemes

Objectives

In this lecture you will learn the following

- How to handle the Money on the net?
- What are all the securities involved while handling money?
- Payment and Purchase order process

Coverage Plan

Lecture 5

5.1 Snap Shot

For many years the Internet was just a place to browse for information, but which 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 merchants benefit by having a convenient and immediate way of shopping and paying for merchandise. Although electronic commerce is 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.

5.2 Electronic Cash and Electronic Payment Schemes

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 of the concepts of the precursor systems. For electronic commerce to take off, 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 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 convenient means to transact on the Internet, the processes reflected in the 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.

5.3 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

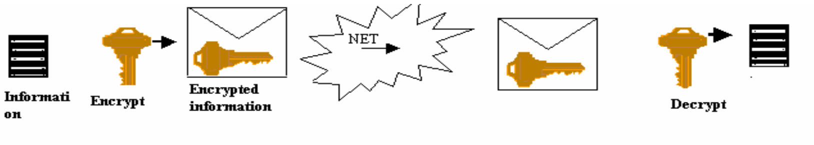
- Confidentiality of payment information
- Integrity of payment information transmitted via public networks
- Verification that an account holder is using a legitimate account
- Verification that a merchant can accept that particular account
- Interoperability across software and network providers

5.4 Confidentiality of payment information

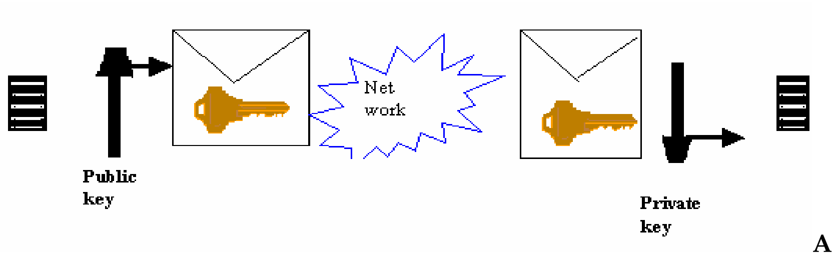
Payment information must be secure as it travels across the Internet. Without security, payment information could be picked up by hackers at the router, communication-line or host level possibly resulting in the production of counterfeit cards or fraudulent transactions. To provide security account information 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 cipher text 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). **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.

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 approaches complex from an administrative perspective. The approach of creating a 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 down loading and using the merchants 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 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.



Symmetric/Secret-key Cryptography



Asymmetric/public-key Cryptography

5.5 Payment information integrity

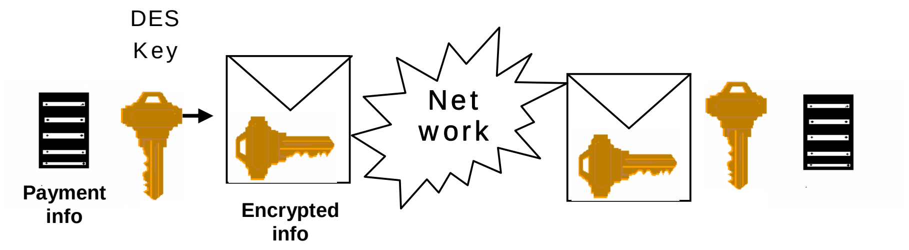
Payment information sent from consumers to merchants includes order information, personal data and payment instructions. If any piece of their information is modified, the transaction may no longer be accurate. To eliminate this possible source of error or fraud an arithmetic algorithm called hashing, 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:

N It has no secret key

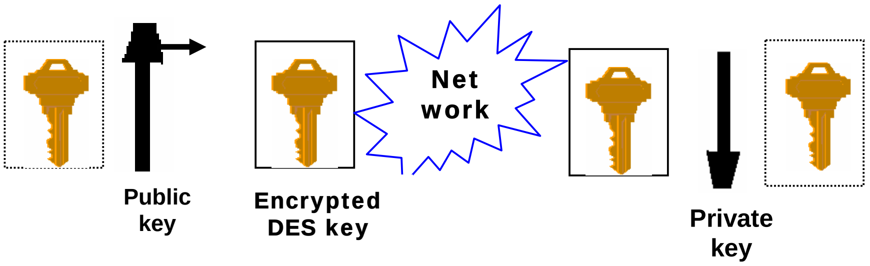
N Give a message digest, there is no way to reproduce the original information

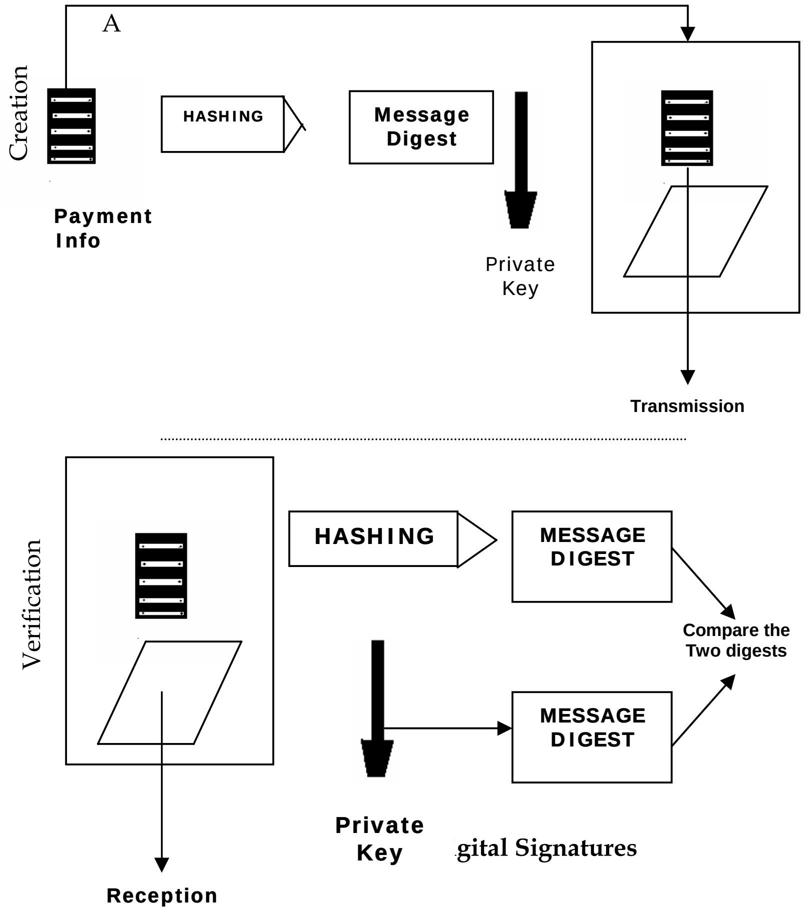
N It is impossible to hash other data with the same value.

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 receive. If the message digest does not calculate to the same value sent, the payment information is assumed to be corrupted and is therefore discarded. The hash algorithm, however is public information therefore anyone may be able to alter the data and recalculate a new "correct" message digest. To rectify this situation the message digest is encrypted using a private key of the sender. This encryption of the message digest is called a digital signature.



Secret-Key/public-key Combination





gital Signatures

Because a digital signature is created by using public key cryptograph, it is possible to identify the sender of the payment information. Since the encryption is done by private key of a public/private key pair, this means only the owner of the private key can encrypt the message digest. Therefore, if the decrypted digital signature equals the message digest calculated by the receiver, then the payment information could not have come from anyone but the owner of the private key.

Note that the roles of the public/private key pair in the digital signature process are the reverse of that used in ensuring information confidentiality. In the digital signature process, the private key is used to encrypt (sign) the information and the public key is used to decrypt (verify the signature). But how does the receiver (merchant) obtain a copy of the public key used to verify the sender's (customer's) digital signature? One way is through some secure channel directly from the customer; this method, however, is not practical. Alternatively, the customers public key could be encrypted with the payment information provide an efficient way for the merchant to verify that the payment information was sent from a particular customer. A digital signature however does not authorize a particular customer to use the monetary account information located in the payment instructions.

5.6 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 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 proceeding to transpire, however, the following is assumed:

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

5.7 Interoperability

For electronic commerce to take place, customers (account holders) must be able to communicate with any merchant. For this reasons, security and process standards must support any hardware or software platform that a customer or merchant may use and have no preference over another. Interoperability is then achieved by using a particular set of publicly announced algorithms and processes in support of electronic commerce. The rest of this discussion will assume that these algorithms and processes are in place and are being utilized

5.8 Payment and Purchase Order Process

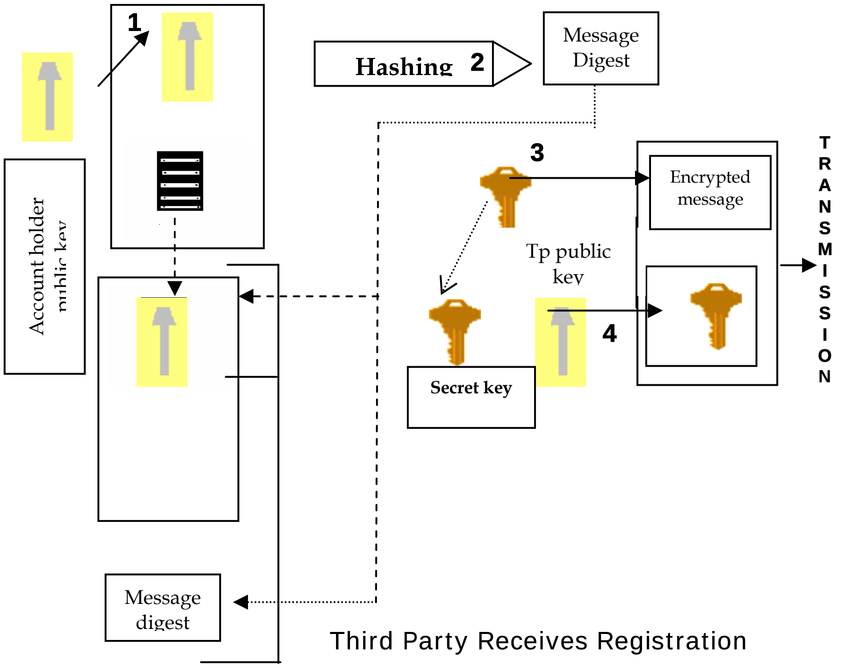
For an electronic payment to occur over the Internet, the following transactions/processes must occur

- Account holder registration
- Merchant registration
- Account holder (customer) ordering
- Payment authorization

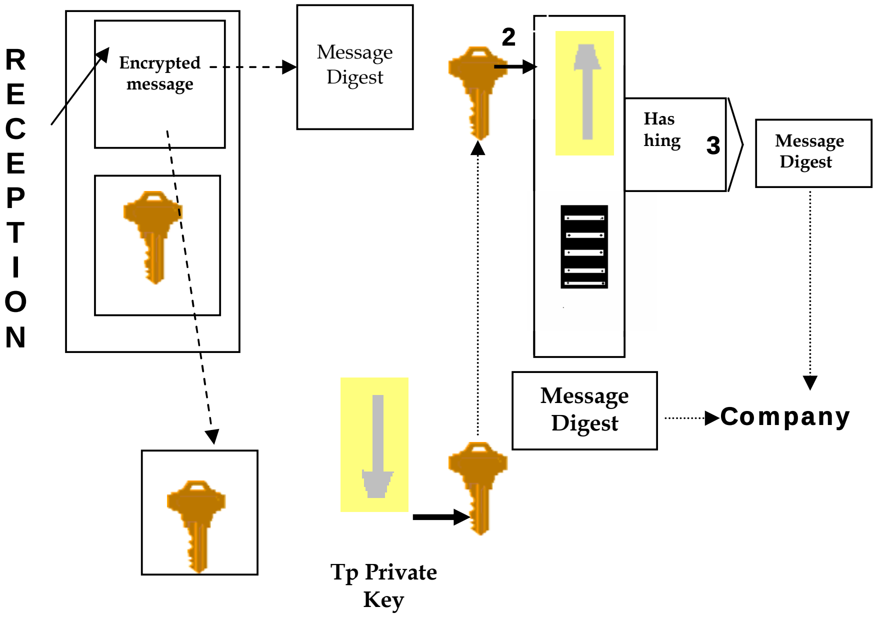
5.9 Account Holder Registration

Account holders must register with a third party (TP) that corresponds to a particular account type before they can transact with any merchant. In order to register, the account holder must have a copy of the TP's public key of the public/private key set. The manner in which the account holder receives the public key could be through various methods such as e-mail, Web-page download, disk or flash card. 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, the account holder can begin to register his or her account for Internet use. To register, the account holder will most likely be required to fill out a form requesting information such as name, address, account number, and other identifying personal information. When the form is completed, the account holder's software will do the following.

Account holder registration



Third Party Receives Registration



1. Create and attach the account holder's public key to the form
2. Generate a message digest from the information
3. Encrypt the information and message digest using a secret key
4. Encrypt the secret key using the TP's public key
5. Transmit all items to the TP

When the TP receives the account holder's request, it does the following

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 transaction.

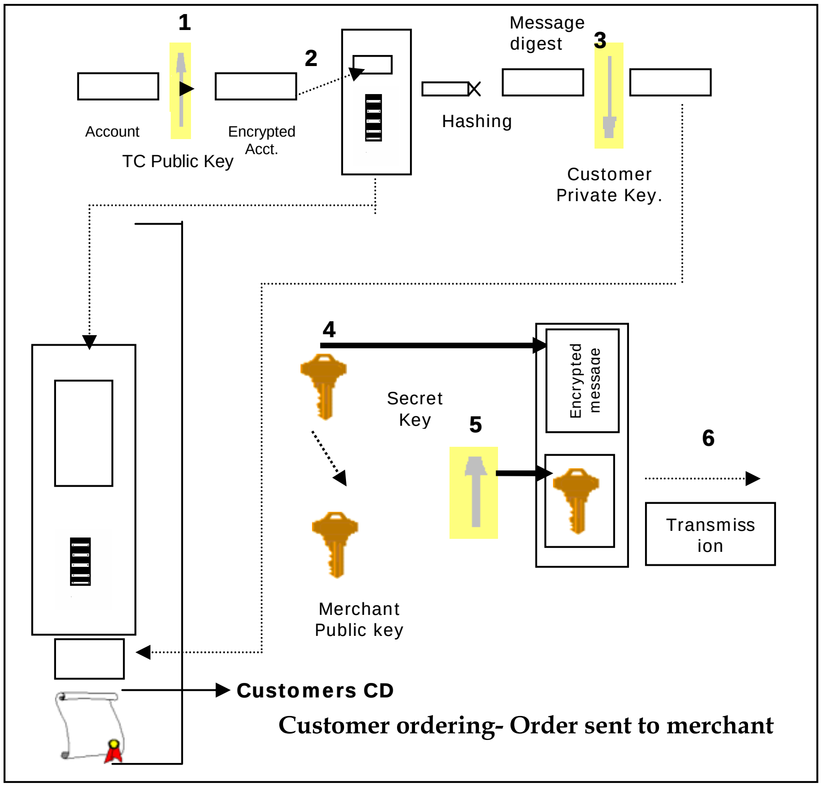
5.10 Merchant registration

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 examples if a merchant wishes to accept Visa and Master Card, that merchant may have to register with two TPs or find a TP that represents both. The merchant registrations similar to the account holder's registration process. Once merchant information is validated, certified documentation (CD) is transmitted to the merchant from the TPs . The certified documentation is then stored on the merchant's computer for future use in electronic transactions.

5.11 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 TPs public key that corresponds to the account type to be used. The order process starts when the merchants 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 CD, the customer software verifies the CD by applying the TPs public key, thus verifying the digital signature of the TP. 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 .

Account holder registration



Customer ordering- Order sent to 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.)

1. Encrypts account information with the TPs public key

2. Attaches encrypted account information to the order form

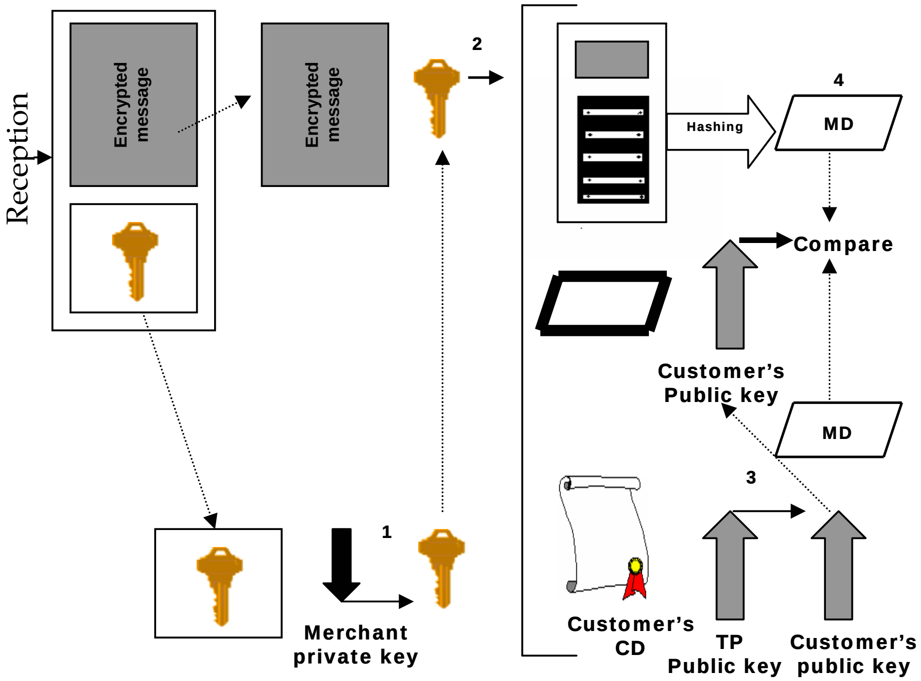
3. Creates a messages digest of the order form and digitally signs it with the customer's private key

4. Encrypts the following with the secret key order form with encrypted account information digital signature, and customer's CD

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)



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 CD using the secret key
4. Calculates the message digest from the order form and compares with the customer's decrypted messages digest

Assuming that the message digests match, the merchant continues processing the order according to its own preestablished order fulfillment processes. One part of the order process, however, will includes payments 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 received the electronic receipt is similar to the encryption and digital signature processes previously described.

5.12 Payment authorization

During the processing of an order, the merchant will need to authorize the transaction with the TP 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 TPs 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 TP payment authorization and the debit transaction tot he 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.

5.13 Short Summary

❖ 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.

❖ 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 ensure integrity the message digest is transmitted with the payment information. The receiver would than validate the message digest by recalculating it once payment information is receive.

- The roles of the public/private key pair in the digital signature process are the reverse of that used in ensuring information confidentiality.

5.14 Brain Storm

1. Explain the term Electronic Payment Schemes.
2. Briefly explain about Confidentiality of payment information.
3. How the integrity is maintained in Payment information?
4. How the Authentication has been taken place in Account Holder and Merchant?
5. What you mean by Interoperability?
6. How the registration has taken place E-Commerce?

Lecture 6

On-Line E-Cash

Objectives

In this lecture you will learn the following

- What is meant by E-Cash?
- Problems with simple E-Cash
- Preventing Double Spending

Coverage Plan

Lecture 6

6.1 Snap Shot

On-line Electronic Cash-Overview: 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 PCs hard drive or possibly by 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 using public key cryptography and digital signatures as discussed earlier. For example, the bank could give the consumer a message which 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 merchants, 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

6.2 Problems with simple electronic cash

A problem with the e-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 thorough 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.

6.3 Creating electronic cash anonymity

To allow anonymity, the bank and the consumer must collectively create the e-cash and associated serial number, whereby the bank can digitally sign and thus verify the e-cash, but not recognize it as coming from a particular consumer. To do this requires a complicated algorithm on behalf of the consumer or consumer's software. To get e-cash, the consumer chooses a random number to be used as the serial number for the e-cash. The random number is large enough so that the possibility of duplication is inconsequential. Instead of sending the generated serial number to the bank, however the consumer applies a multiplier algorithm to the serial number and sends the new multiplied serial number to the bank. The multiplier is also a randomly generated numbers.

When the bank receives the multiplied serial number, it digitally signs it with its private key and sends it back to the consumer. The bank never knows what the original serial number or the multiplier used to the create the multiplied serial number is. When the consumer receives the multiplied serial number signed by the bank, the consumer reverses the multiplier algorithm, obtaining serial number and retaining the digital signature of the bank. The retention of the bank's signature on a now unknown serial number is called a blind digital signature. The consumer now has e-cash digitally signed by the bank, but the bank will snot recognize the cash as the consumers.

Beyond the multiplier algorithm, other operations take place as the consumer withdrawal happens. Consumers must prove their identity to the bank (most likely through public-key cryptography) so that the bank can properly debit their accounts by the value of the cash. The bank also maintains a record that associates the multiplied serial number with the e-cash sent to consumers. In addition, the consumers maintain records concerning the original serial number of the e-cash and the multiplier used. The maintenance of these records are important should consumers ever wish to trace the e-cash they would have to supply to multiplier to the bank, which allows the bank to equate the multiplied Serial number to the original serial number generated by the consumer.

When a consumer uses the e-cash the receiver of the e-cash can check with the bank to make sure the serial number associated with the e-cash has not been deposited before. Although the bank will not recognize the serial number, it will remember al the e-cash that has been deposited before and alert the merchant if the money has been double spent. If the e-cash has not been deposited before, the bank can verify its own digital signature and will honor the e-cash.

6.4 Preventing double-spending

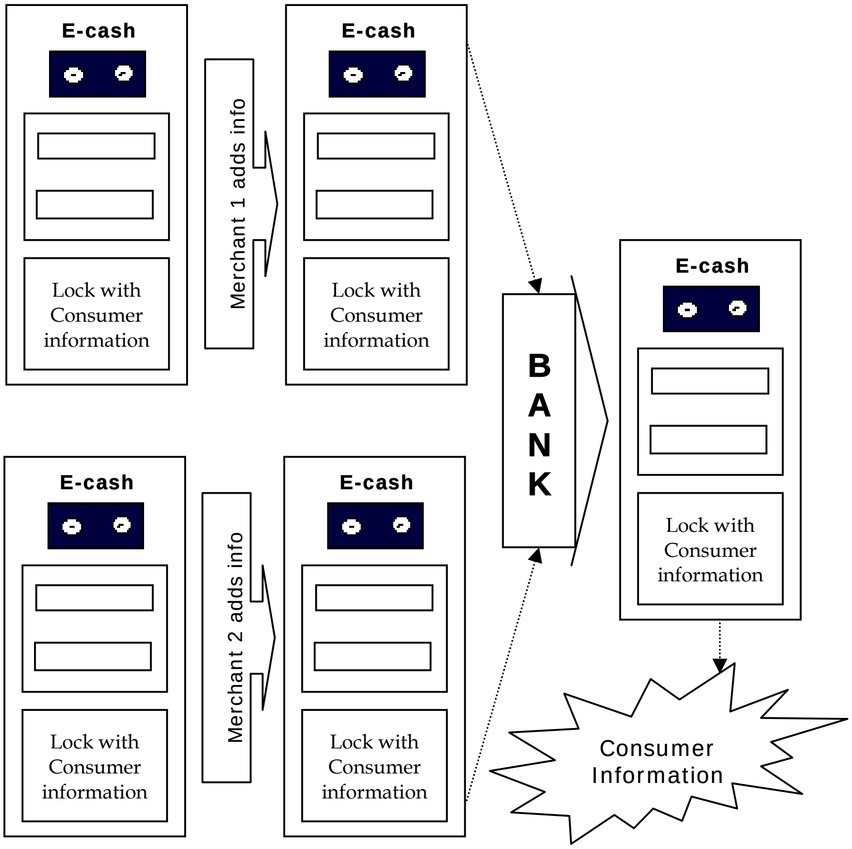
While the preceding protects the anonymity of the consumers and can identify when money has been double-spent, it still does not prevent consumers, or merchants for that matte, from double-spending.

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


E-cash
Lock with Consumer information
Merchant 1 adds info
E-cash
Lock with Consumer information
E-cash
Lock with Consumer information
Merchant 2 adds info
E-cash
Lock with Consumer information
BANK
E-cash
Lock with Consumer information
Consumer Information

Double-spending process depiction –"Simplified"

6.5 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 e-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.

6.6 Short Summary

- 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 be changed.

- To allow anonymity, the bank and the consumer must collectively create the e-cash and associated serial number, whereby the bank can digitally sign and thus verify the e-cash, but not recognize it as coming from a particular consumer.

- When the bank receives the multiplied serial number, it digitally signs it with its private key and sends it back to the consumer. The bank never knows what the original serial number or the multiplier used to the create the multiplied serial number is.

- 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.

6.7 Brain Storm

1. What is the problem in Simple E-Cash?
2. What is meant by Electronic cash Anonymity?
3. What is meant by Double Spending and how to prevent this?
4. What is meant by E-Cash Interoperability?

Lecture 7

Electronic Payment Schemes

Objectives

In this lecture you will learn the following

- What are all the various types of Payments?
- What is meant by Verigin?
- About JEPI.

Coverage Plan

Lecture 7

7.1 Snap Shot

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.

7.2 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, Cyber Cash, and GTE Corporation. Netscape Navigator was planning to include secure Courier, which encrypts data and authenticates individuals and merchants during Internet transactions

7.3 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. STT provides such enhancements as stronger authentication for 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 STT, and Spyglass was planning to build STT into its Windows, UNIX and Macintosh Web browsers and servers. The Internet Shopping Network also is implementing 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.

7.4 Checkfree

Checkfree Corporation provides on-line payment processing services to major clients, including CompuServe, 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 Version's Digital ID. Checkfree has also announced intentions to support all security methods that achieve prominence in the marketplace, e.g. SET.

Together with cyber cash (see the next section) Check free 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. The server module is integrated into a merchant's Web server. Checkfree Wallet uses public private key encryption technology from RSA Data Security and a large 768 bit key to secure sensitive payment information. The system includes CyberCash's electronic checking and support for digital cash. Checkfree Wallet users include CompuServe, Netcom On-line Communication SERvices, performance systems International, Genie, and Apple Computer's eWorld service.

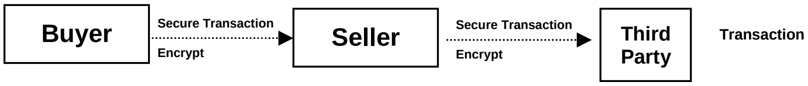
Using a system such as Wallet, a consumer can send encrypted payment information to the merchant, who then forwards the information to CyberCash's server. Only after the credit has been authorized by CyberCash over secure lines to the appropriate bank can the money in Wallet be used to complete the purchase. The concept of using a third party server to prepare credit card transactions is only one of several ways to pay for purchases done via the Internet. Alternatives include outsourcing the entire process and embedding credit card authorization tools in a Web server. For example Commerce Direct International of Issaquah, Washington, provides the back-office infrastructure necessary to safely process credit card and e-commerce transactions and manages the interfaces to financial institutions and credit card clearinghouses.

7.5 CyberCash

CyberCash (http.//www/cybercash.com) combines features from checks and cash. CyberCash is a digital cash software system 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 pertransaction. There is a one time charge to the customer to fill the coin purse and money never leaves the bank. 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. The entire process is conducted quickly and cheaply (Cybercash compares the cost per transaction to the price of a postage stamp).



Cyber Cash Electronic Transaction Process

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.

7.6 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 VeriSing's Digital ID. IBM is building support for Digital ID into its WebBrowser and Internet Connection Secure Server for AIX and OS/2. IBM also is adopting Digital ID for use in its InfoMarket publishing network and clearing house. Digital IDs provide Web servers and clients with key authentication, privacy, and nonrepudiation functions for electronic commerce.

7.7 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 be 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 transaction. 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 uses. 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's 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 wants 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.

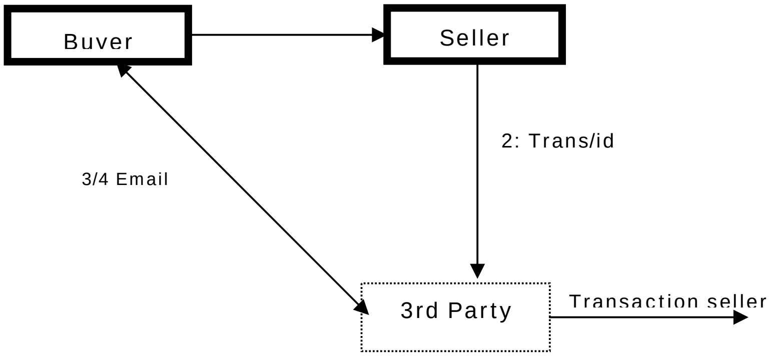
The downside of DigiCash transactions is that they are hard to trace, which does not make law enforcement officials or regulators happy, and there is no stop limit to financial risk. DigiCash is not foolproof in that it is possible for someone to steal a user's digital encryption key and use it for fraudulent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

First Virtual Holdings

First Virtual Holding is targeting individuals and small businesses that want to buy and sell on the Internet but can not 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 bills 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 exchange hands. If they do agree on the purchase, then First Virtual charges the users credit card (See.Fig)

First virtual electronic transaction process



With First Virtual, the buyer has an account with the system and receives a password in exchange for a credit card number. The password in 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 system is based on the fact that buyers can revoke each payment within a certain time.

First Virtual makes a 2 percent commission on each sale and also charges the merchants who use First Virtual a $10 registration fee. The drawbacks to this solution are mainly against the merchant because the merchant ships goods and trusts the buyer to pay for them. First Virtual, in turn, says that it will close the accounts of users who frequently return goods. Another drawback is first Virtual only supports vendors who exchange information (electronic data) with customers, it does not support merchants who sell tangible goods.

Bank America/ Lawrence Livermore Labs. Bank America and Lawrence Livermore National Laboratory created a joint pilot application to test whether the Internet can be used to securely and reliably transmit electronic messages and payments between trading partners and their banks. The electronic commerce application being tested is the transmission of financial EDI messages between Bank America and Lawrence Livermore using secured Internet electronic mail .Specifically Lawrence Livermore send Bank America a payment order via the Internet. On behalf of Lawrence Livermore, Bank America makes the payment either electronically or by check. Bank America sends acknowledgment messages back to Lawrence Livermore as electronic mail over the Internet. The electronic mail is formatted according to Internet standards already in place. All of the processing is automated, computer to computer no human intervention is required. During the pilot, Bank America and Lawrence Livermore were planning to gather data to measure the timelines, reliability, and security of using the Internet for financial EDI. (See http:// www.haas.berkeley.edu/-citm or http://www.commerce.ner)

Commerce Net. In 1993, a group of Silicon Valley entrepreneurs envisioned the Internet as a whole new model of commerce, one defined around global access, a large number of buyers and sellers, many to many interactions, and a significantly accelerated pace of procurement and development. They called this model Spontaneous Commerce. At that time, the Internet had only just begun to carry commercial traffic; the first network exchange point dedicated to the support of commercial traffic went on line in 1991. Three members of this group collaborated on a paper entitled. "CommerceNet Spontaneous electronic commerce on the Internet. The paper recommended four fixes that needed to be made before CommerceNet becomes a reality simpler access, better system for resource location, tighter communication security, and workable financial exchange mechanisms.

In April 1994, a new organization called CommerceNet backed by 20 industrial sponsors including Apple Computer, Bank of America, Pacific Bell, Wells Fargo,, and Xerox, was formed. The opening ads announced "CommerceNet makes electronic commerce over the internet a reality in Silicon Valley." This service helps businesses get on-line with starter kits and technical advice, forming working groups that would define and implement fixes for the problem previously cited, and launching and maintaining a Web site. Over the following year, solutions to most of the problems cited on the original agenda started to appear

7.8 Net Cash

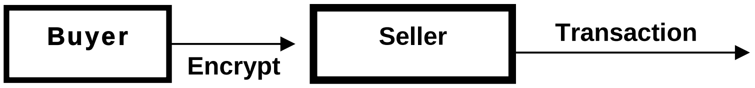
NetCash (http: / /www.netbank.com/-netcash) is the Internet's answer to traveler's checks. To use NetCash, users must enter their checking account or credit card numbers into an on-screen form and e-mail it to the NetCash system. This entitles the users to purchase electronic coupons from NetCah for their face value plus a 2 percent 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 Net Cash 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.

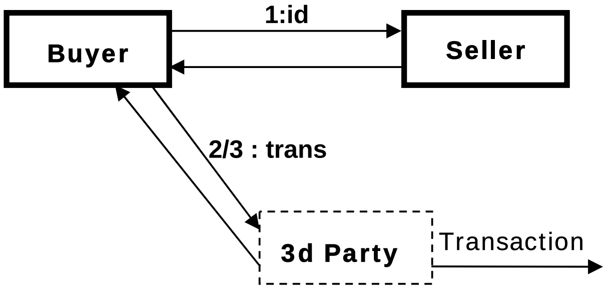
Mondex is based on smart card technology initially backed by the United Kingdom's National Westminster and Midland Banks, the electronic purse is a handheld smart card it remembers previous transactions and uses RSA cryptography. This has not proven to be successful with the majority of the risk on the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

Netmarket (http:..www.netmarket.com) receives userids and passwords over the Internet. Userid 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.

Global On-line (http://www.globeonline.fr) uses on-line challenge/response. It is based on a their party originatin agreements there fore the seller has a higher cost to enter the market. (SeeFig)



Open Market Electronic Transaction Process



Global on-line Transaction Process

7.9 Net Bill

Carnegie Mellon University's NetBill (http://www.ini.cmu.edu/NETBILL/) supports micropayment. Micropayment systems can be divided int 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 perhapes 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 bopes to pay for all costs storage, processing bandwitdth, 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 cost can be reduced significantly, customer and technical support costs remain unknown. New products naturally generate support calls, and users with money at staske 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 transaction. The prospects for any micropayment, protocol will be measured by its success at automating customer support in addition to providing security reliability, quick response time, and ease of use.

Clickshare Corportion (http”//www.clickshare.com) whichmarkets a micropayments system with the same name, has been delayed in part by resistance from one of its target mearkets: 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.

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 Emil’s site, which is hosted by the home base and then, inside emile’s site she clicks on the desired file. Emile’s server authenticates Gabrielle’s home base toke, delivers the file and sends copies of the transaction to both the home base and the account manager. Gabrielle’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 though a year earlier. Pubklishers 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. Micropayment 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 (e.g.,SET), 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 payment. VPOS is the merchant's receipt and transaction management system designed to work with a Windows NT or UNIX Web server. To connect the merchant with its bank for credit verification, VeriFone provides the VGATE Internet gateway, that uses a standard bank interchange protocol. VeriFone is also in a the process of rolling out vWallet, a payment application that lets consumers use their Web browsers, rather than propriety VeriFone software to make purchases. VWallet eventually include SET support.

Many Web server vendors have offered commerce server services for companies that want to be early adopters. These commerce servers can be installed as turnkey servers to create virtual malls or storefronts, supporting electronic commercial transactions with any customer using a Web browser. Netscape and Open Market were early suppliers of such commerce servers, largely using SSL or S-HTTP to offer security for the Web transactions. Microsoft was planning to user VeriFone's product suite for its own Merchant System, a Windows NT based commerce server. Netscape and Oracle have also announced intentions to incorporate VeriFone's VPOS system with their servers.

Analogously to the situation where individuals store more than one credit card in their classical wallet, so too, users must store more than one file for credit card information on their PCs. CyberCash, Netscape and Microsoft offer electronic wallets, that are designed to handle credit card transactions from the same central location on an end user's PC (one such wallet was described in a previous section) . The current drawback is that each company has its own version of a wallet, thereby adding to , rather than alleviating, the confusion. Other applications. (Digi Cash, for example) also can handle cash or checks; users typically set up a prepaid or automatic pay account ahead of time with a bank or other financial institution. Each wallet has its own way of handling the rest of a purchase transaction, such as price negotiation and transaction tracking, so a better way of standardizing transactions is needed. The W3C (world wide web consortium) has been working with Commerce Net on the JEPI (described later). To standardize payment negotiations, whether they use cash, checks, or credit cards.

Microtranscations and such: Other building blocks for Web commerce aer rapidly falling into place. There is interest in supporting small change transactins; these are called micropayments or micropayments. As noted,Carnegie mellon University's NetBill supports micropayments, CyberCash is also spearheading microtransaftins, Web purchases under $10 that are not practical using credit cards because of processing costs. The company's recently introduced Cyber Coin system uses encrypted digital signals in the place of real coins. A Cyber Coin hip rock band for instance, could open a Web site that would le consumers down load digitized versions of its tunes for pocket change.

7.10 Joint Electronic Payment Initiative (JEPI)

The World Wide Web Consortium (W3C)* and Commerce Net have completed the first phase of the Joint Electronic Payment Initiative (JEPI) for interoperable e-commerce systems. The two consortia of Internet vendors and developers announced a project designed to bridge electronic payment methods such as the SET specification and digital cash.

JEPI is not payment method, but it fits between shopping and paying. Besides support of SET, JEPI has two parts. The first is an extension layer called PEP (Protocol Extension Protocol) that sits on top of a Web server's basic HTTP. There is hope that the 1.2 release of HTTP will include PEP. The second part is UPP (Universal Payment Preamble) , a negotiations protocol layer that identifies appropriate payment methodology for the merchant. PEP was submitted to the IETF (Internet Engineering Task Force) in 1996 and UPP was slated for submittal by the press time. In the meantime, the W3C has already embarked on a second phase of JEPI development, which will include integration of smart cards, electronic cash, and micro payments. Some have seen JEPI as a competitor specification to SET.

Future directions

At press time, the most dominant e-cash business/technical model of all the previously mentioned systems was DigiCash. It provides security to all parties and anonymity to the buyer. As long as stop/loss can be placed in the model in the event of a major fraud, this system could do well. However, multiple models will coexist. Different models can be used for different purchases of monetary value and volume, by industry and country, based on cultural differences for the payment process.

7.11 Short Summary

- Checkfree Corporation provides on-line payment processing services to major clients, including CompuServe, Genie, Cellular One, Delphi Internet Services Corporation, and Sky-Tel.

- STT is a general purpose technology for securing financial transactions with applications beyond the Internet.

- CyberCash is a digital cash software system which is used like a money order, guaranteeing payment to the merchant before the goods are shipped.

- VeriSign is offering its digital signature technology for authenticating users as a component separate from encryption, which allows for export of stronger authentication.

7.12 Brain Storm

1. Explain about SEPP.
2. what is Microsoft's STT?
3. Give a short notes on CyberCash, Veri Sign, DigiCash.
4. What is JEPI?

Lecture 8

Security Technologies for E-Commerce

Objectives

In this lecture you will learn the following

- Cryptography – Symmetric and Public Key encryption schemes
- Digital signatures
- Digital Certificates and Certificate Authorities
- Secure Socket Layer

Coverage Plan

Lecture 8

8.1 Snap Shot

8.2 Security Threats

8.3 Cryptography

8.4 Symmetric Encryption Schemes

8.5 A Comparison of Encryption Schemes

8.6 Digital Signatures

8.7 Digital Certificate

8.8 Certificate Authorities

8.9 Secure Socket Layer

8.10 Short Summary

8.11 Brain Storm

8.1 Snap Shot

Internet is definitely an open network. When data is transmitted beyond the organizational network, it may be handled by any number of different intermediate computers (called routers) which make sure that the data is delivered to its intended destination. Data is also likely to travel across Internet backbone networks, which move vast quantities of data over large distances. This implies that the data is vulnerable at many points, including the originating computer, the local or organizational network, and some intermediate system or network out on the Internet – and the same risks exist for the network and systems on the receiving end. This reveals the fact that the Internet is unsecured. Unless Internet has some security technologies to protect the data, the advantages of electronic commerce that takes place mainly on the Internet will be nullified.

This chapter introduces the security threats to data that travel on the Internet, gives an overview of the cryptographic background needed to understand how the system works, and then discusses the principal standards currently developed to secure the Internet for electronic commerce.

8.2 Security Threats

Security is important in financial systems, whether they are based on physical or electronic transactions. In the real world everyone rely a great deal on physical security, while in the world of electronic commerce there must be an additional reliance on electronic means for protecting the data, communications, and transactions. There are two different types of security threats to the electronic data. The following table lists these threats along with security solutions.

Threat	Security Solution	Function	Technology
Data intercepted, read or modified illicitly	Encryption	Encodes data to prevent tampering	Symmetric encryption; asymmetric encryption
Users misrepresent their identity to commit fraud	Authentication	Verifies the identities of both sender and receiver	Digital signatures

Table 8.1 Some Security Threats and Solutions.

The basic requirements for conducting commerce include confidentiality, integrity, authentication, authorization, assurance, and privacy. This chapter shows how the first four requirements for electronic commerce can be solved with technology; but the last two of these requirements, assurance and privacy, depend as much on individuals and organizations acting responsibly as they do on any technological solutions. This would include adherence to laws that protect customers against fraud by merchants.

8.3 Cryptography

There are a wide variety of methods for encrypting data, from using cereal box encoder rings to using complex mathematical algorithms. It's important to understand some of the basic principles of modern encryption before looking at the mechanisms that enables to apply those principles. This section begins by illustrating a simple encryption scenario.

Take a simple phrase like "The sun is hot." The ASCII equivalent of this sentence is the following hexadecimal sequence:

```
T  h  e     s  u  n     i  s     h  o  t  .
54 68 65 20 73 75 6E 20 69 73 20 68 6F 74 2E
```

By converting the original sentence into ASCII, the data is now encrypted. Unfortunately this sort of encryption is rather easy to break because these principles are same to those underlying a cereal box decoder ring. However, the data is converted into a numeric format, and now it can be manipulated using some mathematical principles.

For this type of encryption to work, two functions are necessary:

f(x) and g(x) such that if f(x)=y, the g(y)=x

This equation must be true for all values of x that is used for encryption. The function g(x) is referred as the inverse of f(x). One example of suitable set of functions that could be used to encrypt half a bye at a time is this:

$f(x) = (3*x) \bmod 16$

$g(x) = (11*x) \bmod 16$

The asterisks in this case indicate multiplication. The "mod," short of modulus, is an arithmetic operation whose result is the remainder when the item to the left of mod is divided by the item to the right of mod. If the ASCII phrase (The sun is hot), is interpreted half a byte at a time the result looks like this:

```
                T  h  e     s  u  n     i  s     h  o  t  .
x               54 68 65 20 73 75 6E 20 69 73 20 68 6F 74 2E
f(x) = y =  FC 28 2F 60 59 5F 2A 60 2B 59 60 28 2D 5C 6A
g(y) =      54 68 65 20 73 75 6E 20 69 73 20 68 6F 74 2E
                T  h  e     s  u  n     i  s     h  o  t  .
```

The problem with this encryption scheme is that it wouldn't take a person too long to crack it with a little guessing and some simple analysis. The frequent use of the encoded value 60, for example, would probably lead the decoder to conclude that 60 represents a space. Now that he determined where the spaces are, he knows that the digit 6 represents 2 and that the digit 0 represents 0. Since the message has only a handful of two-letter words, he would have to guess just a little more to come up with the third word, is. Once he infers that 2B represents i and 59 represents s (or in more detail, that 5 represents 7, 9 represents 3, and B represents 9), then he can quickly conclude the phrase.

In the above example, the decoder used some cryptoanalysis principles, such as looking at the recurring bytes in the contents of the encoded message to determine the original phrase. If the decoder were to take the next step in the encryption process, he would determine the percentages of the recurrence of certain numbers and match these percentages against the frequency percentage of letters in every day conversation. The encoded letter that occurs most would be the letter e (which is the letter that appears the most frequently in Standard English).

This sort of encryption can significantly be made more difficult by creating a rotating effect. In the given example encryption scheme, the function

$$f(x) = (3*x) \bmod 16$$

could be considered one of many functions that follow the same format. The multiplier 3 could be replaced with a value of 7 or with any number of values. In the given example case, it's important that the number is relatively prime to 16 (that is, it shares no common factors with 16); if it is not, it won't be possible to create a proper inverse function that produces the original values. If the modules value 16 is replaced with a prime number, then all values less than the modulus will be relatively prime to it. For example, if the modulus is set to 17 instead of 16, all the following functions would create a valid encryption function:

$f(x) = (1*x) \bmod 17$
$f(x) = (2*x) \bmod 17$
$f(x) = (3*x) \bmod 17$
$f(x) = (4*x) \bmod 17$
$f(x) = (5*x) \bmod 17$
$f(x) = (6*x) \bmod 17$
$f(x) = (7*x) \bmod 17$
$f(x) = (8*x) \bmod 17$
$f(x) = (9*x) \bmod 17$
$f(x) = (10*x) \bmod 17$
$f(x) = (11*x) \bmod 17$
$f(x) = (12*x) \bmod 17$
$f(x) = (13*x) \bmod 17$
$f(x) = (14*x) \bmod 17$
$f(x) = (15*x) \bmod 17$
$f(x) = (16*x) \bmod 17$

Now the function can be referred as the following, where k can be any one of the 16 values in the above list.

$f_k(x) = (k*x) \bmod 17$

The k is referred as key to the encryption function. When the k is replaced with 3, the encryption function has the key value of 3 because it looks like this:

$f_3(x) = (3*x) \bmod 17$

It is already clear that it would be simple to decrypt a message with any of these encryption schemes. But this limitation can be overcome by changing the key value while encrypting the message. For example, while encrypting a message the original key value might be increased by 1 for every 4 bits. The example given below illustrates this. It encrypts a sequence of number 1,2,3,4,5 by starting with a key value of 3.

$f_3(x) = (3*1) \bmod 17 = 3$
$f_4(x) = (4*2) \bmod 17 = 8$
$f_5(x) = (5*3) \bmod 17 = 15$

$f_6(x)$ = (6*4) mod 17 = 7

$f_7(x)$ = (7*5) mod 17 = 1

These changes make cryptoanalytic attempts at deciphering harder, but not impossible. If the encryption scheme is applied for every bit of the input, instead of four bits, it will be more puzzling to break the scheme.

8.4 Symmetric Encryption Schemes

Symmetric encryption schemes use a single key, both to encrypt and decrypt a message. Even if the algorithm being used is known, as long as the key stays private, the message can be considered secure. In popular symmetric encryption schemes, the key is often referred to as the session key since it is usually used only for the length of the particular encryption session set up between two communicators.

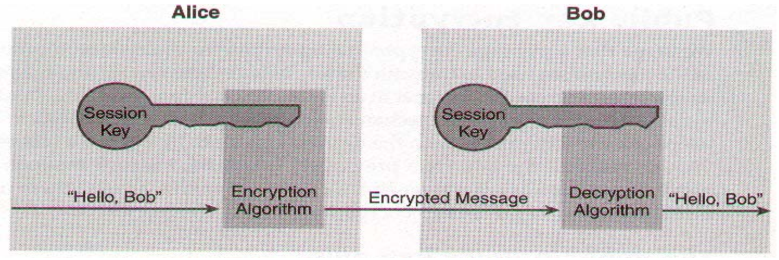


Figure 8.1 A typical symmetric encryption scheme.

One of the advantages of symmetric encryption over other forms of encryption is that it is relatively fast to encrypt and decrypt messages. There are number of symmetric encryption schemes that can be used as the basis for developing secure Web communication mechanisms.

Data Encryption Standard

Data Encryption Standard (DES) is symmetric encryption scheme that was made a United States government standard in 1977. DES is considered a block cipher because data is typically encrypted in 64-bit blocks. The key for DES is 56 bits long, which is actually considered relatively short for most encryption algorithms. However, the use of DES is rarely approved for export for foreign countries.

RC2

RC2 is another block cipher that can take variable length keys. RSA Data Security developed it, and its algorithm is confidential. RC2 was given a special status by the United States government so that export to foreign countries could be approved quickly as long as the key length was limited to 40 bits. RC2 with 128-bit key support is commonly used within the United States.

RC4

RC4 is a stream cipher also developed by RSA Data Security. Unlike block ciphers, stream ciphers encrypt a message bit by bit rather than as an entire block. RC4 is similar to RC2 in that the algorithm can be implemented with keys o various lengths. Export of RC4 has been given special approval by the United States government as along as the key length is limited to 40 bits or less.

Public Key Encryption

Message encrypted using symmetric encryption is only as secure as the mechanism used to transmit the key between the sender and the receiver. The session key can be mailed via a secure mail service, or transmitted via a previously established secure channel. But these methods are not always convenient. One way of getting around these methods is through the use of public key encryption.

The public/private key pair

Public key encryption is an asymmetric encryption mechanism that uses two different keys: a public key and a private key. Instead of using a single key known by both parties (as is the case with symmetric encryption), public key encryption uses one key to encrypt data and another key to decrypt the data. One of these keys is called a public key because it is freely available to the public. The other key (the private key) is kept secret by the owner of the key pair.

The reason public key encryption mechanism works is because they are based on a "one-way" function. A one-way function is simple to perform in one direction but difficult to perform in the opposite direction. For example, it's relatively easy to come up with two large prime numbers, but if only the product of the two prime numbers is given, then it is very difficult to factor the product back into the original two primes. Most public key encryption schemes currently in use are based on factoring large numbers into the product of two large primes.

The public and private keys for public key encryption can be used bi-directionally. For example, Mr.X can encrypt a message with his private key and it can only be decrypted with the corresponding public key. Similarly, someone who has Mr. X's public key can encrypt a message but the message can be decrypted only with Mr. X's private key. Figure 2.2 show encryption being performed in both directions by using the public and private keys.

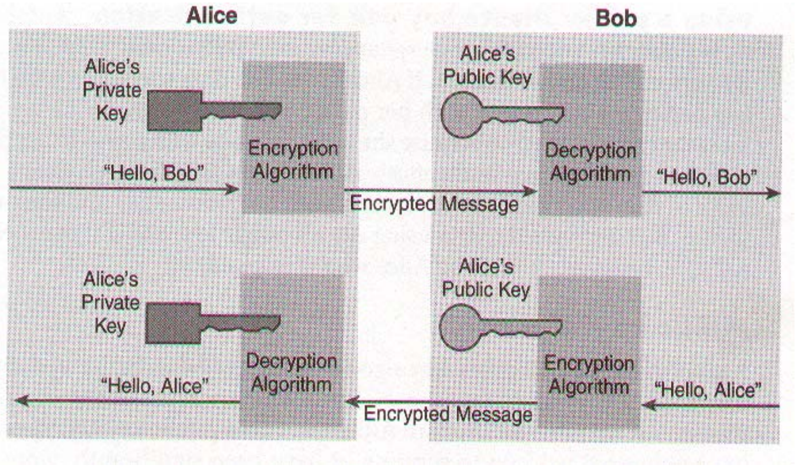


Figure 8.2 Using either the private key or the public key for encryption.

In public key encryption, the public key is well known and anyone with the public key can encrypt the message. In the top scenario in Figure 8.2, Alice should be well aware that the world knows she just said hello to Bob.

Privacy is guaranteed when encryption is performed with the public key and decryption requires the private key; in the bottom scenario of Figure 8.2, Bob is assured that his message is secure because Alice is the only person with knowledge of the private key. Anyone can grab Alice's public key, encrypt a message with it, and feel confident that Alice is the only person who can read the message.

A simple way to ensure private communication in both directions is for Bob and Alice to have their won private and public keys. When Alice sends a message to Bob, she uses Bob's public key to encrypt the data. When Bob sends a message to Alice, he uses Alice's public key. Alice knows that Bob is the only person who can read the message she has sent, and Bob can feel confident that Alice is the only person who can read the messages that he is sending.

Public key encryption schemes have some unique characteristics that make them extremely useful in other circumstances, but for encrypting and decrypting simple messages like those of Bob and Alice, public key encryption is significantly slower than symmetric encryption schemes.

Using a public/private key pair for transferring a session key

Although public encryption schemes are slower than symmetric encryption schemes, public key encryption schemes can play an important role in security even though symmetric encryption schemes.

The problem with symmetric encryption schemes is that a secure mechanism is required for transmitting the session key into the hands of the actual person to whom the information is to be sent. Public key provides this mechanism. If Bob wants to set up symmetric encryption with Alice, Bob simply generates a session key, then encrypts the session key with Alice's public key. Since Alice is the only one with knowledge of her private key, Bob knows that she is the only one who will receive the session key for performing the symmetric encryption.

Using a public/private key pair for authentication

Another capability of public key encryption that symmetric encryption doesn't offer is a mechanism for performing authentication. If Alice sends Bob data encrypted with her private key and he can decrypt it with her public key, then he knows for a fact that the message came from Alice because she is the only one with access to her private key. If all Bob wants to do is authenticate Alice, he can send her a challenge (a random piece of data) that she in turn encrypts with her private key, and if it matches his original data, he knows it must be Alice who is responding.

8.5 A Comparison of Encryption Methods

No one-encryption system is ideal for all situations. The table 8.2 illustrates some of the advantages and disadvantages of each type of encryption.

Encryption Type	Advantages	Disadvantages
Symmetric Key	• Fast • Can be easily implemented in hardware	• Both keys are the same • Difficult to distribute keys • Does not support digital signatures
Public Key	• Uses two different keys • Relatively easy to distribute keys • Provides integrity and non-reputation through digital signatures	• Slow and computationally intensive

Table 8.2 Advantages and Disadvantages of Cryptographic Systems.

Both Symmetric key and public key encryption schemes has their won advantages and disadvantages. So it can be difficult to select the appropriate algorithm for use. The general rule thumb is this – first determine how sensitive the data is, and for how long it will be sensitive and need to be protected. Once this is figured out, select an encryption algorithm and key length that will take longer to break than the length of time for which the data will be sensitive.

8.6 Digital Signatures

Using a private key for encryption is like signing a document. But using public-key cryptographic algorithms to encrypt messages is computationally slow, so cryptographers have come up with a way to quickly generate a short, unique representation of a message, called a message digest, that can be encrypted and then used as a digital signature.

Note: Despite its name, a message digest is not a condensation of the message's contents.

Some popular, fast cryptographic algorithms for generating message digest are known as one-way hash functions. A one-way hash function doesn't use a key; it's simply a formula to convert a message of any length into a single string (of fixed length) of digits called a message digest. The output of a hash function must also have two properties:

- It must be impossible to determine the original message from the digest created by the hash function.
- The hash can never create the same digest for two different messages.

A number of different has algorithms are used today. The following algorithms are accepted as Internet standards.

- MD2. This is the first of three message digest algorithms developed by Ron Rivest. It is optimized for use on 8-bit machines.
- MD4. Another digest algorithm developed by Ron Rivest. It was optimized for 32-bit machines. Although it is very fast algorithm, it has not help up to public scrutiny because it does not consistently create unique digests. MD4 should not be used as a secure mechanism.
- MD5. Also developed by Ron Rivest, MD5 is like MD4 in that it is optimized for use on 32-bit machines. MD5 fixes many of the problems of MD4, although it does so at the cost of slower performance. MD5 digests are 128 bits long.
- SHA. This is the Secure Hash Algorithm defined by the United States government. It uses similar mechanisms as MD4 but it is considerably more secure, because it generates digests of 160 bits.
- DES-DM. This is a hash function built around the DES block cipher. The blocks from DES are combined to create a fixed-length digest.

Once a message digest is ready, encrypting it with a private key creates a digital signature that can be added to the end of a document. As an example, assume that a sender, Tim, calculate a message digest for his message, encrypt the digest with his private key, and send that digital signature along with the plain-text message to Ann (See Figure 8.3).

To verify the signature, the receiver of the signed document (Ann in this case) runs the document through the same has function (which was agreed upon beforehand). She then decrypts the digital signature with the Tim's public key to see whether the result matches the document's digest. If it does, the signature is valid. If it does not, either the signature is forged or the document is corrupted in transit. In either case, the document is considered invalid.

The one problem with this approach is that the body of the message is sent as plain text, and therefore privacy is not maintained. Although this further complicates matters, a symmetric key can be used to encrypt the plain text of the message.

8.7 Digital Certificates

Using public key encryption to create digital signatures is very powerful use of an encryption scheme, but one problem still needs to be addressed if public key encryption is to be useful for securing the transmission of a session key. How can one ensure that the public key used to perform a particular task belongs to the person he thinks it belongs to? The answer is to use digital certificates and certificate authorities to distribute public keys.

Certificate A standardized document that includes a user's public key and it digitally signed by a certificate authority to prove its validity.

Certificate Authority A central authority that verifies the identity of the owner of a public key and then digitally sings the certificate used to distribute the key.

The following example illustrates why certificates and certificate authorities are essential. Suppose Bob wants to authenticate Alice by using her public key. He generates a random challenge, send it to the person claming to be Alice, and then attempt to decrypt her response with her public key. How can Bob be assured that he received Alice's public key? Suppose Charlie is trying pretend he is Alice. If Bob simply asks the sender of the message for the public key, Charlie might give Bob, his public key instead of Alice's. When Bob encrypt his data, only Charlie will be able to read it.

There must be a way of publishing public keys so that it's clear whose public key belongs to whom. One idea would be to maintain a central repository of information that would verify an individual by using standard verification mechanisms like checking a picture ID or scanning fingerprints. After verification, the central repository would add the individual's public key to its store of public keys. When a person needed the public key, he could go the central repository to get it instead of asking the unconfirmed individual for it.

The problem with a central repository of public keys, however, is that it is an inefficient mechanism of data storage on large networks. Public key quires would occur thousands, if not millions, of times per hour, and commerce could come to a standstill.

How is the public key storage problem solved? Rather than keeping public key information in a central location, the central authority digitally signs a document containing a user's public key. Alice, then can hold a copy of this signed document and pass it to anyone who wants to authenticate her identity.

Suppose Bob wants to verify that Alice is who she says she is. Bob doesn't have her public key at this point, so he asks her to provide it. Alice provides Bob with a document that both contains her public key and is digitally signed by the trusted certificate authority. Bob does have the public key of the certificate authority, which he uses to verify the document Alice gave him. Once Bob verifies the digital signature, he can trust that the document was signed by the certificate authority. The document, or certificate, would not only have Alice's public key, but it would also have several fields of unique information that lets Bob know the public key belongs to the particular Alice he's dealing with. Now he can send Alice the authentication challenge with the confidence of knowing exactly to whom the public key belongs.

To better understand what a certificate is, the following table describes the fields of information contained in a certificate.

Field	Description
Certificate Version	The version of the certificate specification that the certificate follows.
Serial Number	A unique number of every certificate signed by the certificate authority.
Signature	Specifies the hash algorithm and public key encryption scheme used to sign the certificate. The digital signature is appended to the end of the certificate.
Issuer Name	Name of the certificate authority that is signing the certificate.
Validity Period	The start and stop dates specifying when a certificate is considered valid.
Subject Name	Name of the individual whose public key is contained in the certificate. These names are universally unique.
Subject Public Key	The actual public key of the individual specified in the Subject Name field.

Table 8.3 Fields of a Certificate.

8.8 Certificate Authorities

The certificate authority is responsible for verifying all the information contained in a certificate before actually signing it. The user requesting the certificate provides the public key with his certificate request to the certificate authority. All the certificate authority has to do is verify the user and sign the certificate.

Note: Three notable certificate authorities are Verisign, Cybertrust, and Nortel.

A digital certificate can be issued in one of four classes, indicating to what degree the holder has been verified. Class 1 is the easiest to obtain because it involves the fewest checks on the user's background; only the name and e-mail address are verified. For a Class 2 certificate, the issuing authority checks a 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 in addition to the information required for a Class 2 certificate. A Class 4 certificate includes information about the individual's position within an organization, but the verification requirements for these certificates have not yet been finalized.

Once the certificate is signed by the certificate authority, the certificate can be passed freely around the world. To verify a do the following:

- Verify the validity period of the certificate is appropriate.
- Verify the digital signature of the certificate by using the certificate authority's public key.
- Verify that the certificate serial number is not on a list of revoked certificates published by the certificate authority.
- Verify that the subject name is the name of the desired individual.

There is an important point about the public key of the certificate authority. How do one can get it? How can he know that it belongs to the certificate authority he thinks it belongs to? The circular answer is. "We use certificates." Certificate authorities are supposed to be rare entities, so the act of verifying a certificate authority should be an infrequent task.

There are actually two kinds of certificate authorities – root authorities and child authorities. The difference between the two is that a root authority sings its own certificates.

The certificates with public keys for child authorities are signed by a separate certificate authority, called the parent authority. Because the parent authority itself might be a child authority for another certificate authority, verification can involve working through a complex hierarchy of certificate authorities. Certificate authorities can be verified by verifying each parent certificate authority until the top of the hierarchy is reached. At this point, the top of the hierarchy is what is called a root authority.

In addition to commercial certificate authorities (such as Verisign, Cybertrust, and Nortel), and government authorities (such as United States Postal Service), corporations can also become a certificate authority by purchasing a Certificate Server from a vendor that has been certified by a certificate authority. Such arrangements are useful when a company needs to issue digital certificates to a number of employees for doing business, either within the company, or with other companies. As more systems use digital certificates to control computer access, corporate-maintained certificate servers will become more important. In the meantime, the United States government is trying to set up the Public Key Infrastructure for certificate authorities. Figure 8.4, shows an example of a certificate authority hierarchy.

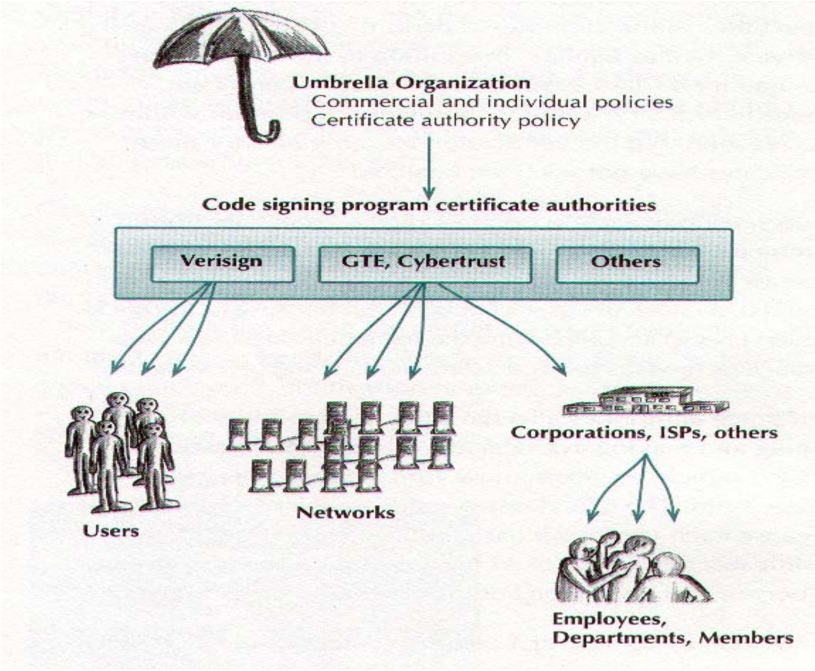

Umbrella Organization
Commercial and individual policies
Certificate authority policy
Code signing program certificate authorities
Verisign
GTE, Cybertrust
Others
Users
Networks
Corporations, ISPs, others
Employees, Departments, Members

Figure 8.4 An example of a certificate authority hierarchy.

Before a user adds a new root authority to his list of valid authorities, he needs to be very sure it came from a source that he can trust. In the best of all possible worlds, all child authorities are valid because their certificates were validated by a "higher authority." But what happens to the validity of certificates when a root authority is dishonest or its private key store has been compromised? When a root authority's private key is compromised, all certificates it signs are suspect.

One way certificate authorities avoid fraud is to maintain a Certificate Revocation List (CRL). A CRL is a list of certificate serial numbers that are no longer considered valid for reasons other than an expired validity period. For example, a certificate authority might provide a company with a CRL that includes serial numbers of certificates issued to employees who have left the company before their certificates expired.

8.9 Secure Socket Layer

So far this chapter examined symmetric encryption schemes, public key encryption schemes, authentication, digital signing, and certificates. Putting all these concepts together to create a standard mechanism for establishing a secure channel of communication is what the Secure Socket Layer (SSL) is all about. SSL provides an authentication and encrypted link through which any sort of TCP socket communication can take place. SSL provides a secure conduit for HTTP requests and responses so that sensitive information, like credit card numbers and finances can be transmitted securely across the World Wide Web.

There are two basic stages in SSL communication: the handshake stage and the data transfer stage. In the handshake stage, the secure connection is set up. As soon as algorithms are agreed upon, keys are exchanged, and the endpoints are authenticated, the data transfer stage starts. In the data transfer stage, information is passed to SSL, encrypted and decrypted, and then handed to a higher level entity. The routing of information is seamless to the higher-level application that is using SSL, as though encryption isn't being conducted at all. Figure 8.5 illustrates a typical SSL connection sequence.

SSL requires that a communication channel be established between the client and the server. Once a connection, say TCP connection is established, the SSL handshake, shown in Figure 8.5, can begin. In Figure 8.5, the first message to be sent across the underlying connection is the Client Hello message. The ' Client Hello ' message provides important information for setting up the secure channel: which version

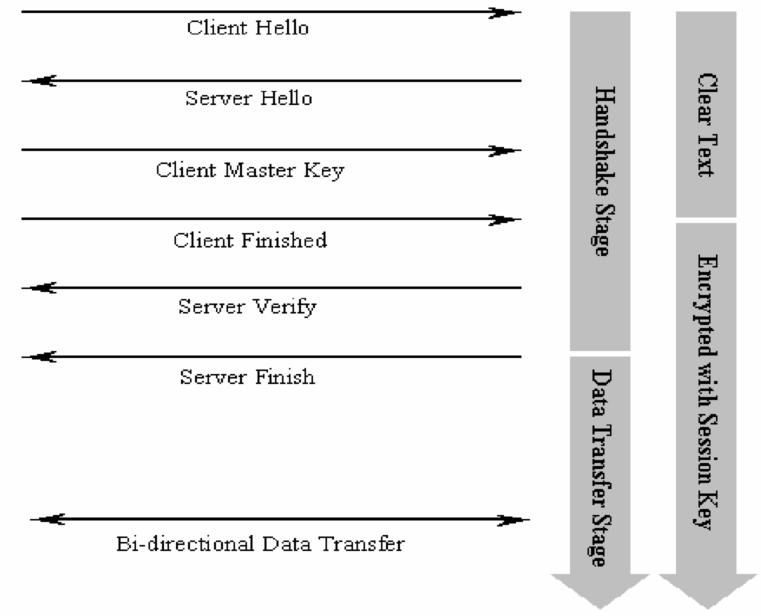


Figure 8.5 A typical SSL 2.0 session

of SSL is being used, which symmetric encryption algorithms are supported by the client, which session key sizes are supported by the client, which key exchange mechanisms can be used, and which hashing algorithms are supported. The client also sends a randomly generated challenge as part of the ' Client Hello ' message.

The server responds to the 'Client Hello' message with the 'Server Hello' message. The 'Server Hello' message responds to the client's list of supported encryption algorithms and hashes by sending a subset of algorithms that are also supported by the server. At this point, the list contains algorithms supported by both sides. The 'Server Hello' message also contains a connection ID, which servers as a challenge of the client later in the handshake process, as well as the server machine's certificate.

When the client receives the 'Server Hello' message, it verifies the server's certificate and then generates a Client Master Key message. The Client Master Key message includes the final encryption algorithms along with an appropriately generated session key, which will be used to perform symmetric encryption. The session key is actually encrypted by using the server's public key from the certificate in the 'Server Hello' message. After the Client Master Key is sent, all subsequent message are encrypted using the specified symmetric encryption algorithm and the session key indicated in the Client Master Key message.

After the client has sent the 'Client Master Key' message, it sends a Client Finished message to indicate to the server that it is ready to activate the channel. The Client Finished message includes the Connection ID sent by the server in the Server Hello message, but now the message is encrypted using the session key. This provides a degree of authentication of the client by the server.

The Server Verify message verifies that the server providing the certificate in the 'Server Hello' message is the server currently communicating. The Server Verify message contains the challenge sent in the Client Hello message, encrypted with the session key from the client Master Key message. This message is used to authenticate the server because only a machine with the server certificate's corresponding private key can decrypt the session key and use it. The client verifies that the challenge is encrypted correctly.

The Server Finish message is the server's way of indicating to the client that the server is ready to enter the data transfer stage. The encrypted Server Finish message contains a session identifier that can be used by the client later to expedite the SSL handshake process. Once the Server Finish message is sent, normal data transmission can occur. This means that the client can send its HTTP request across the secure connection and wait for the response.

In this long but simplified illustration, the server is the only portion of the connection with a certificate, meaning that the server is being authenticated but the client is not explicitly authenticated. SSL provides an optional means for authenticating clients by allowing the server to send a Request Certificate message before it sends its Server Finish message. The client must respond with its Client Certificate message, which includes the client's public key certificate along with the server's Request Certificate message digitally signed by the client. The server verifies the certificate along with the message's digital signature before sending the Server Finished message.

Once the connection enters the data transfer stage, data sent to the secure connection is broken up into messages that are both encrypted using the session key and digitally signed. The receiving end receives the encrypted message and verifies the digital signatures before attempting to decrypt the data. Having data messages signed further secures the validity of the data source and the integrity of the data.

SSL 3.0

To illustrate basic concepts, the example in Figure 8.5 shows a typical SSL 2.0 session. There have been a number of advances in secure communication since SSL 2.0 was first developed. SSL 3.0 provides greater flexibility in specifying supported encryption algorithms and parameters, so the SSL specification should remain fairly stable even if new encryption algorithms are developed. SSL 3.0 also provides a means for changing the current encryption key and algorithm on an existing secure channel.

Setting up IIS for Secure web Communication

This section looks at the details of setting up Internet Information Server so as to take advantage of its security options. First one or more certificates must be installed on the Internet Information Server to enable secure communications option.

Key Manager

Before an SSL can be established to a server, the server must have a certificate installed so that authentication and session key exchange can occur properly. Certificates are purchased from a certificate authority or can be generated using Microsoft Certificate Server. Key Manager must be run to properly install a certificate on IIS. Key Manager can be stated by several ways:

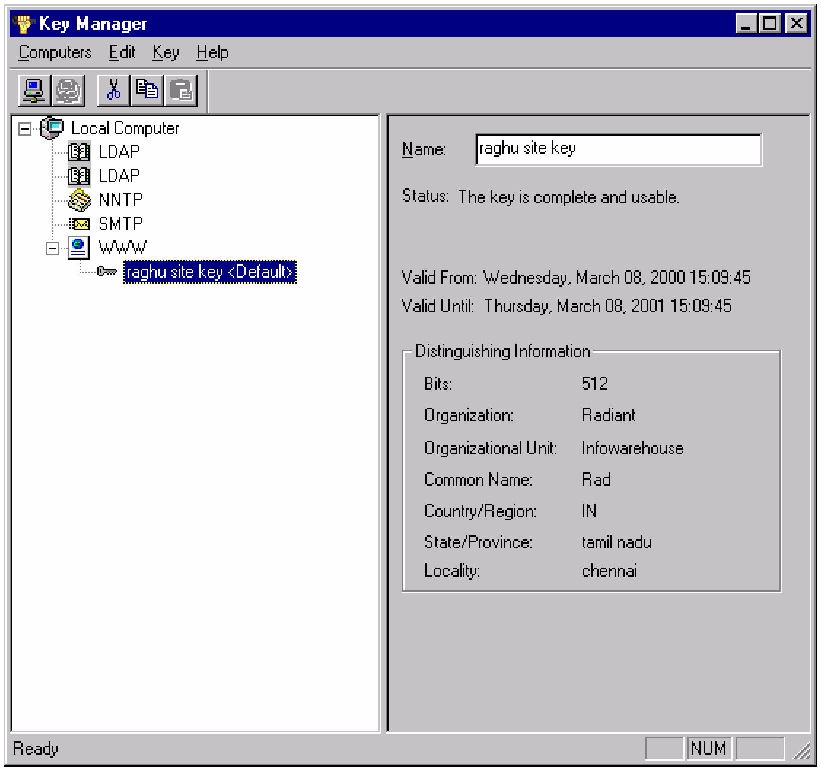
- ❖ By selecting Internet Information Server in the Scope Pane in the Management Console and then clicking its toolbar button (which shows a hand holding a key)

- ❖ By clicking the Key Manager button on the IIS Plugin's Directory Security property page.

- ❖ By running the KEYRING.EXE program located in the C:\WINNT\SYSTEM32\INETSRV directory.

Figure 8.6 shows the Key Manager application.

On the left side of the Key Manager window is a hierarchical view of an example machine and all the services for which certificates can be installed. This section focus on installing certificates for the World Wide Web service, but secure communication can be used for a number of different services. Notice in Figure 2.6 that in the left-hand pane one key is listed under the WWW icon: raghu site key . When a key is highlighted its details are displayed in the right-hand pane. Details include the key's current functional status the validity period details for the certificate, the key length, and the various components that make up the distinguished Name of the Server.



Name: raghu site key

Status: The key is complete and usable.

Valid From: Wednesday, March 08, 2000 15:09:45
Valid Until: Thursday, March 08, 2001 15:09:45

Distinguishing Information

Bits:	512
Organization:	Radiant
Organizational Unit:	Infowarehouse
Common Name:	Rad
Country/Region:	IN
State/Province:	tamil nadu
Locality:	chennai

Figure 8.6 Key Manager.

Actually a key in the Key Manager is an SSL key pair (public and private keys), which is necessary for establishing a secure communication link. The key pair is used to "negotiate" a secure SSL connection with a user's Web browser.

To create a new key

- Right click on a required service, say WWW Service and choose Create New Key.

This will start the Create New Key wizard that will guide through the process of creating a new key.

The first step is to create a request for a key. New key request can be send to a certificate authority in one of two ways. The first option is to have the wizard create a certificate request that stores the information in a text file. This file must be submitted to a certificate authority. After verification he will provide a digital certificate. This certificate must be installed in the Key Manager for its corresponding key.

The second option, which is quite convenient, is to have the wizard automatically send the request to an online authority. But this option will be enabled only if the Certificate Server is installed in the machine, where the Key Manager is running.

The wizard will prompt for a key name, a password, the key length and distinguished name fields such as organization name, organizational unit etc. to uniquely identify the server. When all these information are entered, either the request file need to be submitted to the Certificate Authority, or the request will automatically be processed, if the online option is selected in the wizard.

If the request file is submitted manually to a Certificate Authority, he will issue the certificate for the server in the form a file. After receiving this file, use Key Manager to install the certificate.

To install a certificate

- In the left-hand pane of the Key Manager, select the disabled key that corresponds to the certificate request, right-click on it, and chooses Install Key Certificate.

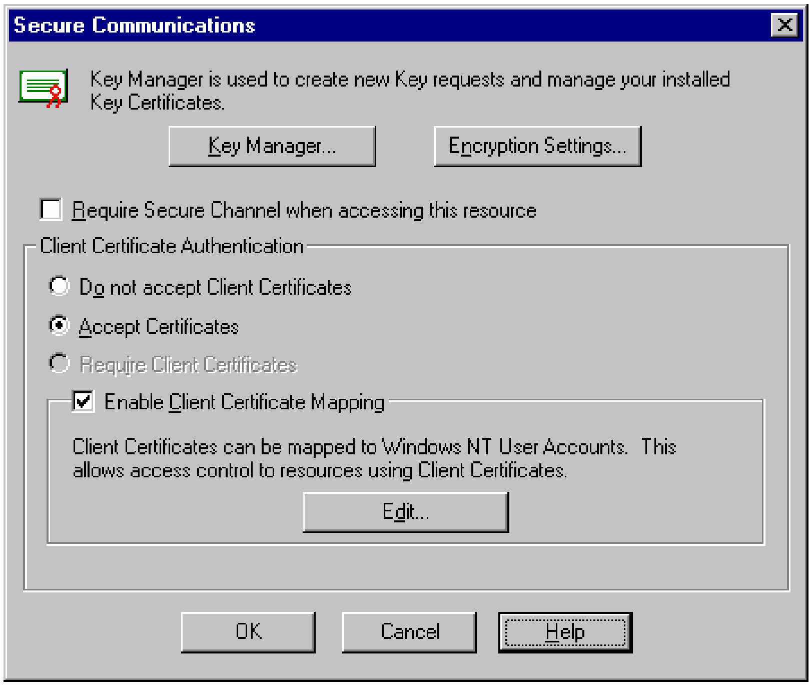
- When prompted specify the certificate file, which issued by the certificate authority and password, which is specified for the request. This will install the certificate for its corresponding key.

Note: Key Manager also enables to backup and restore server keys by using the Export and Import commands from the Key menu. Backing up the keys is a good idea because server key certificates can be relatively expensive. If a key that don’t have a backup is accidentally deleted within the Key Manager, then the only remedy is to make a another key certificate request from the certificate authority.

SSL Configuration Options in the Management Console

IIS is flexible when it comes to configuring SSL options. Home directory, virtual directories, directories and files can be configured at a fine granularity. For example, IIS lets to specify whether a particular resource will use SSL and how exactly it can be configured for the same resource.

Figure 8.7 shows the secure communications dialog box, which is accessible by clicking the Edit Secure Communications button on the Directory Security property page. For each source on a particular machine, the Secure Communications dialog box offers the gamut of options for requiring, allowing, or denying the use of SSL and client certificates. At the top of the dialog box is one button that takes back into Key Manager and an adjacent button that allows to manipulate encryption settings



Key Manager is used to create new Key requests and manage your installed Key Certificates.

□ Require Secure Channel when accessing this resource

Client Certificate Authentication

○ Do not accept Client Certificates

● Accept Certificates

○ Require Client Certificates

☑ Enable Client Certificate Mapping

Client Certificates can be mapped to Windows NT User Accounts. This allows access control to resources using Client Certificates.

Figure 8.7 Configuring secure communications.

Another option available in the Secure Communications dialog box is the Enable Client Certificate Mapping option. This option can be enabled as long as client certificates are accepted for secure communications. Choosing Edit button under the Enable Client Certificate Mapping option, displays a window that enables to map client certificates to actual Microsoft Windows NT account. So when a request comes in with a specific client's certificate, the server checks its certificate mapping list to see whether it has a valid certificate map for this particular certificate. If the server has a valid map, IIS impersonates the Windows NT account specified by the mapping when IIS executes the request. This process is similar to the way in which Windows NT impersonates a specified user when basic or NTLM authentication schemes are used, except that certificate mapping determines the account information used.

This chapter has explained about secure communication and setting up Internet Information Server to take advantage of SSL capabilities – especially that certificate are good way to ensure privacy. The cost of purchasing certificates and the lack of control in managing certificates, however, often limit their widespread use. Internet Information Server solves these and cost and controls problems by including Microsoft Certificate Server. With the help of Certificate Server, an organization can behave as a certificate authority and provide its own client (and server) certificates.

8.10 Short Summary

- Security is important in financial systems, whether they are based on physical or electronic transactions.

- Symmetric encryption schemes use a single key, both to encrypt and decrypt a message.

- One of the advantages of symmetric encryption over other forms of encryption is that it is relatively fast to encrypt and decrypt messages.

- Public key encryption is an asymmetric encryption mechanism that uses two different keys: a public key and a private key.

- Certificate A standardized document that includes a user's public key and it digitally signed by a certificate authority to prove its validity.

- Putting all encryption schemes, public key encryption schemes, authentication, digital signing, and certificates concepts together to create a standard mechanism for establishing a secure channel of communication is what the Secure Socket Layer (SSL) is all about.

8.11 Brain Storm

1. Explain about Security Threats.
2. What do you mean Cryptography in E-Commerce?
3. What is Symmetric and Asymmetric Schemes ?
4. Define the Advantage as well as Disadvantages of the above Schemes?
5. Explain about Digital Signature and Digital Certificate.

Lecture 9

Encryption Technology for E-Commerce

Objectives

In this lecture you will learn the following

- Knowing about Encryption
- About Encryption Keys
- About Conventional Encryption
- About Key Encryption

Coverage Plan

Lecture 9

9.1 Snap Shot

Earlier, we referred to one of the major security risks on LANs, which uses a multi access medium - the risk of eavesdropping. Eavesdropping can be accomplished by programming the NIU to accept packets other than those addressed to it or by physically tapping into the medium. One counter measure that, properly used, is very effective is to encrypt the data in each packet.

Encryption is the process of changing intelligible data into unintelligible data; decryption reverses the process. For most local area networks, data encryption is used only when the security threat is substantial.

9.2 Encryption

Ensuring that data is secure in a network environment is more difficult than ensuring the security of physical documents. Typically, data in a network is held in a common storage facility, and anyone authorized to use the central storage has the potential to access classified files. The best solution to this potential problem is to store the data in an encrypted form. Then any unauthorized person accessing the file would not be able to read its contents.

Encryption techniques cover a broad range, from simple encryption that guards against accidental disclosure to sophisticated methods which protect against all but the highly trained criminal with an in-depth knowledge of cryptanalysis and considerable deciphering equipment.

Most encryption schemes are based on mathematical operations that are "computationally infeasible". That is, they are based on prime numbers which are so large that even the computational power of a mainframe computer cannot break the code within a practical time period.

Two primary types of encryption exists link and end to end. Link encryption is used to many data unreadable while it is on a point- to - point link, such as between two PCs. Link encryption prevents the casual reading of data. End - to -End encryption protects data anywhere on the system.

9.3 Encryption Keys

Encryption key systems are commonly found on dial-up networks but are also available on LANs. A key is essentially a formula for coding and decoding a message. Keys are carefully distributed to authorized users. In fact, the security of the distribution channel for key often establishes the security level of a system.

Such a system of secret keys is very difficult and expensive to maintain, especially as the number of participants increases. To overcome these disadvantages, a new key called a "public key" was devised. Public keys may be published openly and they permit virtually any individual to use a personal public key to code a message and send it to another person. To decode the message, however, the receiver must use a secret key. A secret key consists of two prime numbers that are not published.

One other application of public keys is to authenticate messages. You can use your secret key to encrypt a message and send it to a second person. That person will take your public key and use it to decode the message. If your public key does decode an encoded message, presumably sent by you, then proof has been provided that you did indeed send the message. In other words, the public key is an electronic signature.

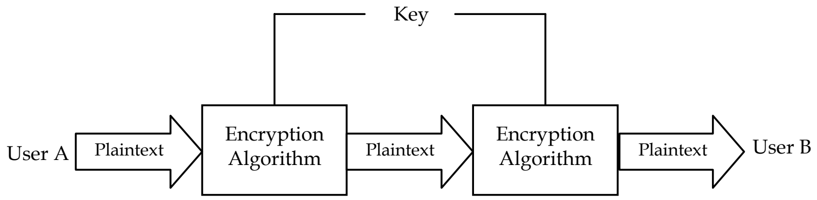
All keys are factorable and, therefore, limited in their level of security. Over the last few years, a debate has been going on about how complex a key should be. Generally, any encryption system provides file privacy against casual perusal. But encryption is an encryption system designed by IBM and adopted by the National Bureau of standards in 1977. Using an encryption system that conforms to the DES standard generally is considered sufficient protection against an authorized access. That is, most criminals and vandals would not be able to break into a communication system and stealer alter data which has been encrypted according to the DES standard. With the largest and fastest computers available today, however. Des encryption schemes probably are breakable.

A number of schemes for encryption have been proposed. In this section, we describe two techniques that are good candidates for local network use.

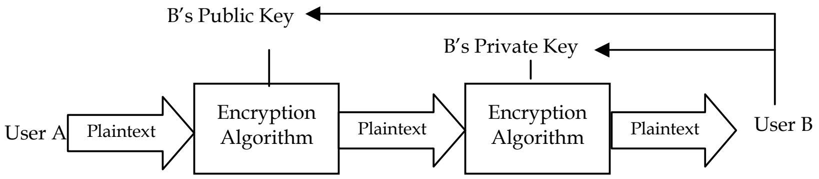
9.4 Conventional Encryption

Figure illustrates the conventional encryption process. The original intelligible message, referred to as plaintext, is converted into apparently random nonsense, referred to as cipher test. The encryption process consists of an algorithm and a key. The key is a relatively short bit string that controls the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. Changing the key radically changes the output depending on the specific key being used at the time. Changing the key radically changes the output of the algorithm.

Once the cipher text is produced, it is transmitted. Upon reception, the cipher text can be transformed back to the original plaintext by using decryption algorithm and the same key that was used for encryption.



a. Conventional Encryption



b. Pubic-Key Encryption

The security of conventional encryption depends on several factors. First, the encryption algorithm must be powerful enough to make it impractical to decrypt a message on the basis of the cipher text alone. Beyond that, the security of conventional encryption depends on the secrecy of the key, not the secrecy of the algorithm. That is, it assumed that it is impractical to decrypt a message on the basis of the cipher text plays knowledge of the encryption/decryption algorithm. In other words, we do not need to keep the algorithm secret; we only need to keep the key secret.

This feature of conventional encryption is what makes it feasible for widespread use. The fact that the algorithm need not be kept secret means that manufacturers can and have, developed low-cost chip implementations of data encryption algorithm. These chips are widely available and incorporated into a number of products. With the use of conventional encryption, the principal security problem is maintaining the secrecy of the key. This issue is addressed here.

9.5 The Data Encryption Standard

The most widely used encryption scheme is based on the data encryption standard(DES), adopted in 1977 by the National Bureau of Standards. For DES, data are encrypted in 64-bit blocks using a 56-bit key. Using the 64-bit input transformed in a series of steps involving transposition and exclusive or operations result is a 64-bit output in which each bit of output is a function of each bit of the in put and each bit of the key. At the receiver, the plain text is recovered by using the same and reversing the steps.

The DES has enjoyed wide spread use, unfortunately, it has also been the subject of much controversy as to how secure the DES is concern is in the length of the key, which some observers consider to be too short. To appreciate the nature of the controversy, let us quickly review the history of the DES.

The DES is the result of the request for proposals for al national cipher standard released by the NBS in 1973. At that time, IBM was in the final stages of a project called Lucifer to develop its own encryption capability. IBM proposed the Lucifer schemes, which was by far the best system submitted. It was , in fact so good that it considerable upset some people eat the National Security Agency (NSA), which until considerably upset some people at the National Security Agency (NSA). Which until that moment had considered itself comfortably ahead of the rest of the world in the still arcane art of cryptography. DES, as eventually adopted, was essentially the sale still arcane art of cryptography, DES, as eventually adopted, was essentially the same as Luciferm with one crucial difference; Lucifer's key size was originally 128 bits, whereas the final standard use a key of 56 bits. What is the significance of the 72 dropped bits?

There are basically two ways to break a cipher. One way is to exploit properties of whatever mathematical functions form the basis of the encryption algorithm to make a "cryptoanaltic" attack on it. It is generally assumed that DES is immune to such attacks, although the role of NSA in shaping the final DES standard leaves lingering doubts. The other way is brute force attack in which you try all possible keys in an "exhaustive search". That is, you attempt to decrypt ciphertext with every possible 56-bit key until something intelligible pops out. With only 56 bits in the DES key, there are 2X56 different keys - a number that is uncomfortably small, and becoming smaller as computers get faster.

Whatever the merits of the case, DES has flourished in recent years and is widely used, especially in financial applications. Except in areas of extreme sensitivity, the user of DES in commercial applications should not be a cause for concern by the responsible managers.

9.6 Commercial Communications Security Endorsement Programme

Although DES still has a reasonably useful life ahead of it, it is likely that non-government organizations will begin to look for replacements for what is seen as in increasingly vulnerable algorithm. The most likely replacement is a family of algorithms developed under the NSA commercial COMSEC (Communications security) Endorsement program (CCEP). CCEP is a joint NSA industry effort to produce a new generation of encryption devices that are more secure than DES, that are low-cost and that are capable of operating at high data rates. Feature of the new OCCEP algorithms are:

1. The CCEP algorithms are developed by NSA and are classified. Thus the algorithms themselves remain secret and are subject to change from time to time.

2. Industry participants will produce chip implementation of the algorithms, but the NSA maintains control over the design, fabrication and dissemination of chips.

Two types of algorithms come under the CCEP heading. Type I algorithms are designed to protect classified government information. Equipment using Type I CCEP will be available only to government agencies and their designated contractors. Type II algorithms are designed to protect sensitive but unclassified information. Type II gear is intended to replace DES gear, Unlilke the Type I modules, which will handle classified information, the Type II module is built into a computer or communication device and sold by a vendor, the customer can do with it as he or she pleases - short of exporting it overseas.

Although the purpose of developing the Type II equipment, as with the Type I equipment, was to provide a means of protecting government information, the Type II modules are available for use in non-government, private sector application. As this equipment becomes more widely available, it is likely to become more widely used, at the expense of DES.

9.7 Key Distribution

For conventional encryption to work, then two parties to an exchange must have the same key and that key must be protected from access by others. Furthermore, frequent key changes are usually desirable to limit the amount of data compromised if an attacker learns the key. Therefore, the strength of any cryptographic system rests with the key distribution technique, a term that refers to the means for delivering a key to two parties that wish to exchange data, without allowing others to see the key. Key distribution can be achieved in a number of ways. For two parties A and B.

1. A key could be selected by A and physically delivered to B.
2. A third party could select the key and physically deliver it to A and B.
3. If A and B have previously and recently used a key, one party could transmit the new key to the other, encrypted using the old key.
4. If A and B each have an encrypted connection to a third party C, C could deliver a key on the encrypted links to A and B.

Options 1 and 2 call for manual delivery of a key, which is awkward. In a distributed system, any given host or terminal may need to engage in exchange with many other hosts and terminals over time. Thus, each device needs a number of keys, supplied dynamically. The difficult with option 3 is that if an attacker ever succeeds in gaining access to one key, then all subsequent keys are revealed.

Option 4 is the most attractive and could be handled from a host facility or network control center. Figure illustrates a possible implementation. For this scheme, two kinds of keys are identified.

Session key

When two end-systems (nosts, terminals, etc) wish to communicate, they establish a logical connection. For the duration of that logical connection, all user data are encrypted with a one-time session key. At the conclusion of the session of connection, the session key is destroyed.

Permanent key : A permanent key is one used between entities for the purpose of distributing session keys.

The configuration consists of the following elements:

- **Access control center**

The access control center determines which systems are allowed to communicate with each other.

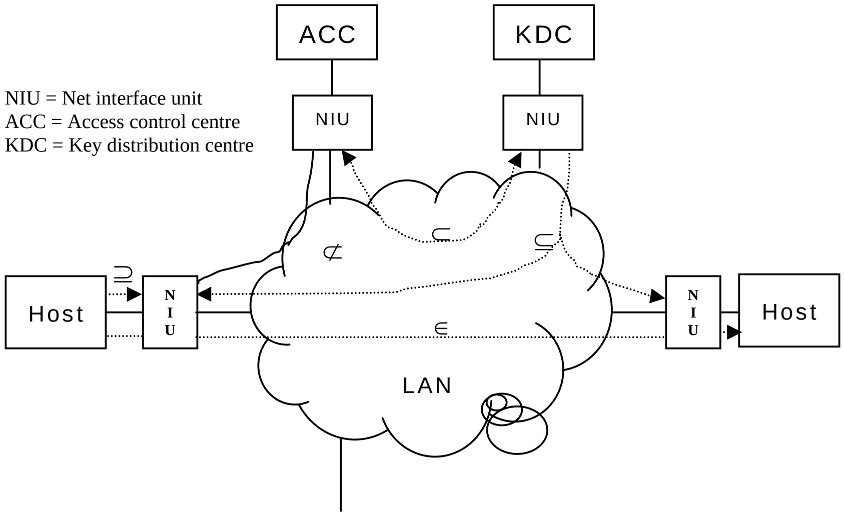
- **Key distribution center**

When permission is granted by the access control center for two systems to establishing a connection, the key distribution center provides a one-time session key for that connection.

- **Network Interface Unit**

The NIU performs end-to-end encryption and obtains session keys on behalf of its host or terminal.

The steps involved in establishing a connection are shown in fig.



1. Host sends packet requesting connection
2. NIU buffers packet, asks ACC for session key

3. ACC approves request, commands KDC
4. KDC distributes session key to both NIUs
5. Buffered packet transmitted

When one host wishes to set up a connection to another host, it transmits a connection required request packet(1). The NIU saves that packet and applies to the access control center for permission to establish the connection(2). The communication between the NIU and the access control center is encrypted using permanent key shared only by the access control center is encrypted using a permanent key shared only by the access control center and the NIU . The access control center has one such unique key for each

NIU and for the key distribution center. If the access control center approves the connection request, it sends a message to the key distribution center, asking for a session key to be generated(3). The key distribution center generated the session key and delivers it to the two appropriate NIUs. Using a unique permanent key for each NIU(4). The requesting NIU can now release the connection request packet and a connection is set up between the two end systems(5). All user data exchanged between the two end systems are encrypted by their respective NIUs using the one-time session key.

Several variations on this scheme are possible. The functions of access control and key distribution could be combined into a single-system. The separation makes the tow function clear and may provide a slightly enhanced level of security. If we wish to let any two devices communicate at will, then the access control function is not needed at all. When two devices wish to establish a connection, one of them applies to the key distribution center for a session key.

The automated key distribution approach provides the flexibility and dynamic characteristics needed to allow a number of terminal users to access a number of hosts and for the hosts to exchange data with each other. A number of LAN vendors offer some version of the scheme . It is a powerful and reasonably inexpensive means of enhancing network security.

9.8 Public Key Encryption

As we have seen, one of the major difficulties with conventional encryption schemes is the need to distribute the keys in a secure manner. A clever way around this requirement is an encryption scheme that, surprisingly, does not require key distribution. This scheme, known as public key encryption and first proposed in 1976, is illustrated in Figure 8.5b.

For conventional encryption schemes, the keys used for encryption and decryption are the same. This is not s necessary condition. Instead if is possible to develop an algorithm that used one key for encryption and a companion but different key for decryption. Furthermore, it is possible to develop algorithms such that knowledge of the encryption algorithm plus the encryption key is not sufficient to determine the decryption key. Thus the following technique will work.

1. Each end-system in a network generated a pair of keys to be used for encryption and decryption of messages that it will receive.
2. Each system publishes its encryption key by placing it in a public register or file. This is the public key. The companion key is kept private.
3. If A wished to send a message to B, it encrypts the message using B's private key.
4. When B receives the message, it decrypts it using B's private key, No other recipient can decrypt the message since only B knows B's private key.

As you can see, public-key encryption solves the key distribution problem, since there are no keys to distribute ! All participants have access to public keys and private keys are generated locally by each participant and therefore need never be distributed. As long as a system controls its private key, its incoming communications secure. At any time, a system can change its private key and public the companion public key replace its old public key.

A further refinement is needed. Since anyone can transmit a message to A using A's public key, a means is needed to prevent impostors. To develop this scheme, you need to know that public key encryption algorithms are such that the two keys can be used in either order. That is, one can encrypt with the public key and decrypt with the matching public key. Now consider the following scenario; B prepares a message and encrypts it with its own private key and then encrypts their result wit A's public key. On the other end, A first uses its private key and then uses B's public key in a double decryption. Since it was also encrypted with A's private key. it could only come from B. Since it was also encrypted with A's public key it can only be read by A. With this technique, any two stations can at any time set up a secure connection without a prior secret distribution of keys.

A main disadvantage of public-key encryption compare to conventional encryption is that algorithm for the former are much more complex. Thus, for comparable size and cost of hardware, the public-key Scheme will provide much lower throughput. One possible application of public-key encryption is to use it for the permanent key portion of Figure, with conventional keys used for sessions keys, Since there are few control messages relative to the amount of user data traffic, the reduced throughput should not be a handicap.

Table summarizes some of the important aspects of conventional and public key encryption.

Conventional Encryption	Public key encryption
Needed to work 1. The same algorithm with the same key can be used for encryption and decryption	**Needed to work** 1. One algorithm is used for encryption and decryption with a pair of keys. One for encryption and one for decryption.
2. The sender and receiver must share the algorithm and the key **Needed for security:**	2. The sender and receiver must each have one of the matched pair of keys. **Needed for security:**
1. The key must be kept secret.	1. One of the two key must be kept secret.
2. It must impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.1	2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus of the keys plus samples of ciphertext must be insufficient to determine the key

9.9 Short Summary

- Encryption techniques cover a broad range, from simple encryption that guards against accidental disclosure to sophisticated methods which protect against all but the highly trained criminal with an in-depth knowledge of cryptanalysis and considerable deciphering equipment.

- A key is essentially a formula for coding and decoding a message.

- Changing the key radically changes the output depending on the specific key being used at the time. Changing the key radically changes the output of the algorithm.

- For conventional encryption to work, then two parties to an exchange must have the same key and that key must be protected from access by others.

9.10 Brain Storm

1. Explain the concept of Encryption.
2. Explain about the Private, Public, Session Key?
3. What is meant by Conventional Encryption?

Lecture 10

Internet Working With TCP/IP

Objectives

In this lecture you will learn the following

- About TCP/IP
- About the Origin of TCP/IP
- Knowing about the Internet Architecture
- How TCP/IP works?

Coverage Plan

Lecture 10

10.1 Snap Shot

One of the problems with networks today is that there are many different protocols and network types. The hardware choices are confusing enough, but software protocol suites that run over the various types of network hardware solutions can absolutely boggle the mind. Ethernet, for instance, boasts a vast number of protocol suites such as DDCMP, LAT,MOPO,XNS,SCS,TCP/IP,VRP, NRP and a slew of other three-letter acronyms for various protocols that will solve all the problems a customer could possible have.

With in the scheme of protocols, however, some still seems to rear their ugly heads, no matter how hard the industry tries to put them down or get rid of them. One suite, Transmission control protocol/Internet protocol (TCP/IP), is such a occurrence. Every other vendor of networks will claim that their protocol is better and that TCP/IP is going away. Some will point to the decisions made by the US department of Defense(DOD) to eventually migrate to internationally recognized and standardized communications hardware and protocols, obviating the need for TCP/IP and eventually replacing it. Some view TCP/IP as a workhorse whose time has come to be put out to pasture.

Then there are the zealots-- those that think that the only communications protocol suite for use in the world is TCP?IP and all others are fluff. These folks are dangerous because they not only are vocal about TCP/IP many times they are UNIX zealots as well.

Somewhere in the middle of the two camps are those who do not know what to do with TCP/IP or, worse, do not even really understand its significance to networks. Unfortunately, these individuals are usually the managers of such diverse camps of attitudes and must make decisions on whether to us TCP/IP on project or not.

Although it is the ISO open systems protocols which have received most recent publicity, there are other well established protocol sets. Particularly on Ethernet, which have a large share of the current LAN market. Some argue that these protocols offer a better alternative to the largely untried and potentially cumbersome ISO set, but most manufacturers indicate a willingness to adopt ISO protocols at some point of time in future.

The non-ISO protocol described in this chapter illustrate different approach from the ISO protocol set to Open Systems working, TCP/IP, is a vendor independent wide area network protocol set, which has been widely used on LANs for peer-to-peer communications. Here we will examine the TCP and IP networking protocols and some implementations that have become de-facto standards in the military area as well as academic and UNIX area.

In recent years knowledge of the capabilities of transmission Control Protocol/Internet protocol (TCP/IP) has spread far in the globe. IT managers in all types of organizations have begun to research its suitability as an internetworking. TCP/IP seems to be a ready made solution to the commercial information systems requirements of intercommunication and interoperation.

In US government officials and research communities and many UNIX aficionados are already well versed in the vocabulary and configuration issues of this set of protocols. But for the newcomer to TCP/IP the existing sources of information are in many cases written by developers apparently for developers,. Most information is primarily technical with detailed descriptions of the bits, flags and fields of the protocols. But less information is given about the practical problems of implementing TCP/IP from scratch. For example in a commercial rather than a technical or research environment; here the skills and constraints may be very different. The information needed does exist, but one has to read a considerable quantity of material before finding what one needs.

10.2 Origin of TCP/IP

A comprehensive set of 'ready-made' communications protocols called TCP/IP became widely available and well known only when Berkeley software Distribution released Berkeley UNIX4.2 BSD in September 1983. This was not a coincidence; its inclusion in this release was funded by the US government. TCP/IP protocols are based on standards originally developed for the Us government and US research community. With the release of UNIx4.2BSD these communications standards emerged from the confines of the Us Department of Defense and the Us university and research networks; TCP/IP became the way to interconnect unix systems. Berkeley UNIX 4.2BSD and subsequent releases spread quickly throughout the US university and commercial communities. With UNIX achieving wide popularity as an open system the fame of TCP/IP has continued to spread. But TCP/IP is not and never has been, narrowly confined to UNIX. It was developed to allow free interchange of data among all machines independent of type, manufacturer, hardware or operating system

In the late 1980s TCP/IP received a further boost to its fortunes when sun Microsystems published the specification for Open Network Computing (ONC), often called the network file system(NFS). NFS; adds important functions to TCP/IP and is now very widely available and regarded as an integral part of the TCP/IP protocol suit. It is particularly valuable for the commercial implement or because of the simple user interfaces that it provides.

TCP/IP was developed to satisfy the need to interconnect various projects that included computer networks and also allow for the addition of dissimilar machines to the networks in a systematic and standardized manner. While it is quit true that smaller defense projects may not have warranted the use of TCP/IP for project aspects, edits from various DOD concerns such as the Undersecretary of Defense for Research and Development forced many government contractors and in house developed projects to use the suite to conform with DOD requirements.

The suite of protocols commonly referred to as TCP/IP (US Military Standards 1778 and 1777) was developed by the United Stated Department of Defense for it's a .R.P.A(Advanced Research Project Agency) network. This is a very large scale wide area network linking many major commercial, university and military establishments. The relevance of TCP/IP to LANs is two fold. First as it is a datagram based protocol, it is well suited to LAN access method particularly Ethernet. Secondly, it is particularly popular within the UNIX community, giving it a large user base many of whom wish to use LANs.

Cost effective implementations of TCP/IP are now available for all types and sizes of machines from the largest mainframe to personal computers and workstations. This has brought TCP/IP and its capabilities to the attention of a very wide audience. Computer managers and users in commercial organizations throughout the world have begun to implement TCP/IP as a way of solving the problems of inter working between machines of different manufacture.

TCP/IP provides all the facilities for two computer systems to exchange information (intercommunication), interpret it properly and present it in a format which can be understood by the local machine and its users(interoperation). NFS is now available for many different computers.

10.3 TCP/IP Communications Architecture

An interconnected set of lines and terminals allowing processing to take place in one or several locations is usually viewed as a network. A network may have several hosts interacting with multiples of terminals. To bring structure to this view of a network, the concept of network architecture is proposed; this is structured hardware and software design that supports the interconnection of a number of physical and logical components.

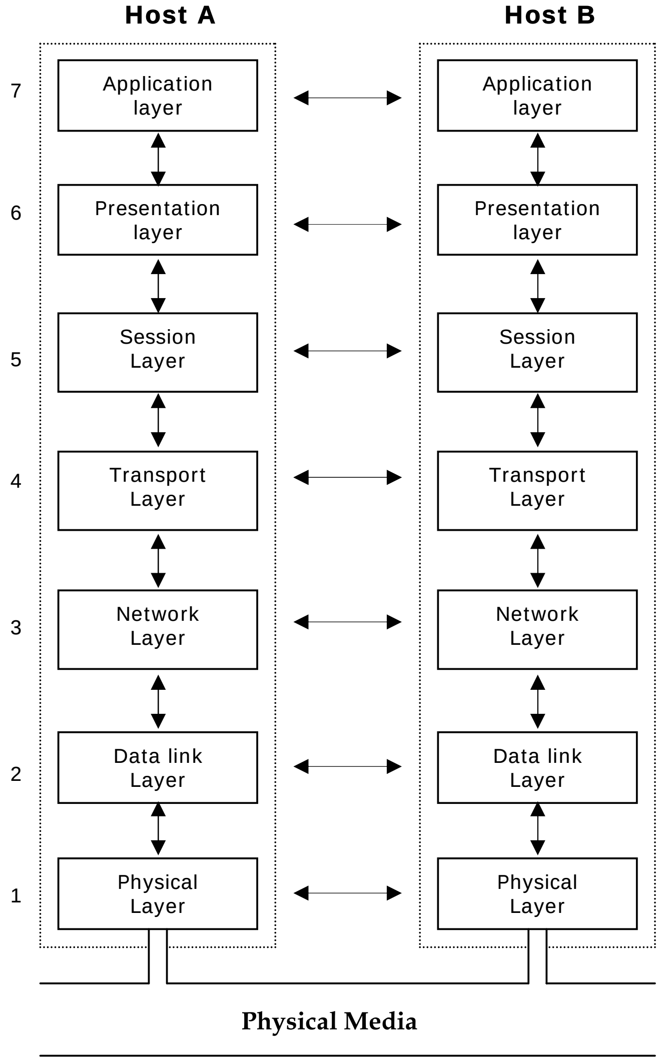
A network architecture is a way to define the set of rules to which these interconnecting elements must confer. It is now, however a definition of how the internal design is made or how the functions in the network operate or how a rule is actually implemented. A network architecture is a statement of what services need to be provided to enable the network to follow one set of rules.

In the past several years the international organization for standardization (ISO) has developed a model of network architecture called the Open Systems Interconnection (OSI) model of network architecture. The goal of this model is to promote the interconnecting of networks of all types.

The underlying principle exploited by the OSI model is layering. The idea is to create a network architecture with several layers where each layer provides certain unique functions which are not provided by any of the other layer is strictly defined. Based on some standard structuring techniques, the OSI model defines seven distinct layers, as shown in Figure each layer need only interact with the adjacent layers and has no knowledge about any other layers, as shown in Figure . Information flows down through the layers of the receiving host. Because the layers are isolated from each other by strict interfaces, information that is added by a layer in the sending host will only be used by the matching layer in the receiving host. In this sense the matching layers of the sending and receiving hosts communicate with each other in a peer-to-peer relationship as shown by the dotted lines connecting matching layers.

Application
Presentation
Session
Transport
Network
Datalink
Physical

Fig ISO/OSI Reference model



Each layer adds value to the services provided by the set of lower layers in the manner that the highest layer is offered the set of services needed to run an application distributed over several networks. Each layer provides services to the layer above requests services from the layer below. Thus the total network problem is divided into a set of smaller problems.

Intermediate networks that merely relay information from one network to another will only need to implement some of the lower three layers to act as transferal agents. Figures illustrate this principle of the OSI scheme for differing network problems.

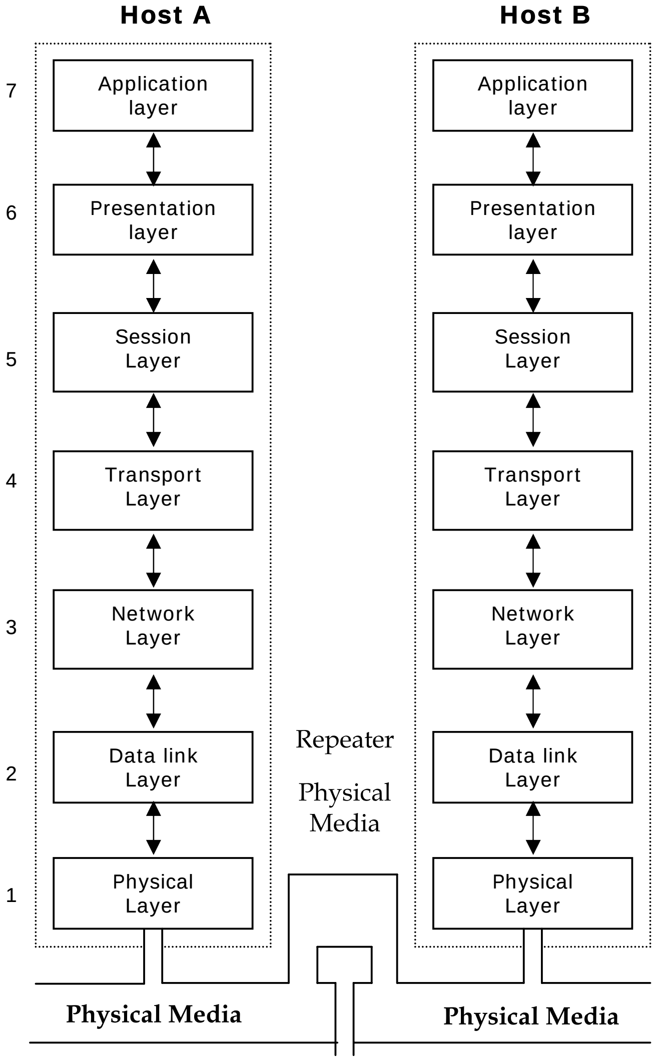


Figure How OSI model hosts communicate through repeaters

In the standard which describes the reference model, OSI standard developers state that they will exclude any details which would be implementation dependent. The result is that while the standards have been kept 'pure' many details which would aid development of viable OSI products are excluded from the standards themselves. While some should argue that OSI is more rigorous in its standardization than TCP/IP, the OSI development process Seems to have become enmeshed in procedures weighted down by the difficulties of obtaining consensus in large committees and dogged by supplier politics. By confining OSI standards to abstract definitions in a complex vocabulary, defined just for the purpose and then charging considerable sums for copies of there standards. ISO committees have, undoubtedly, if unintentionally, slowed the OSI development process and the delivery of useful conforming products.

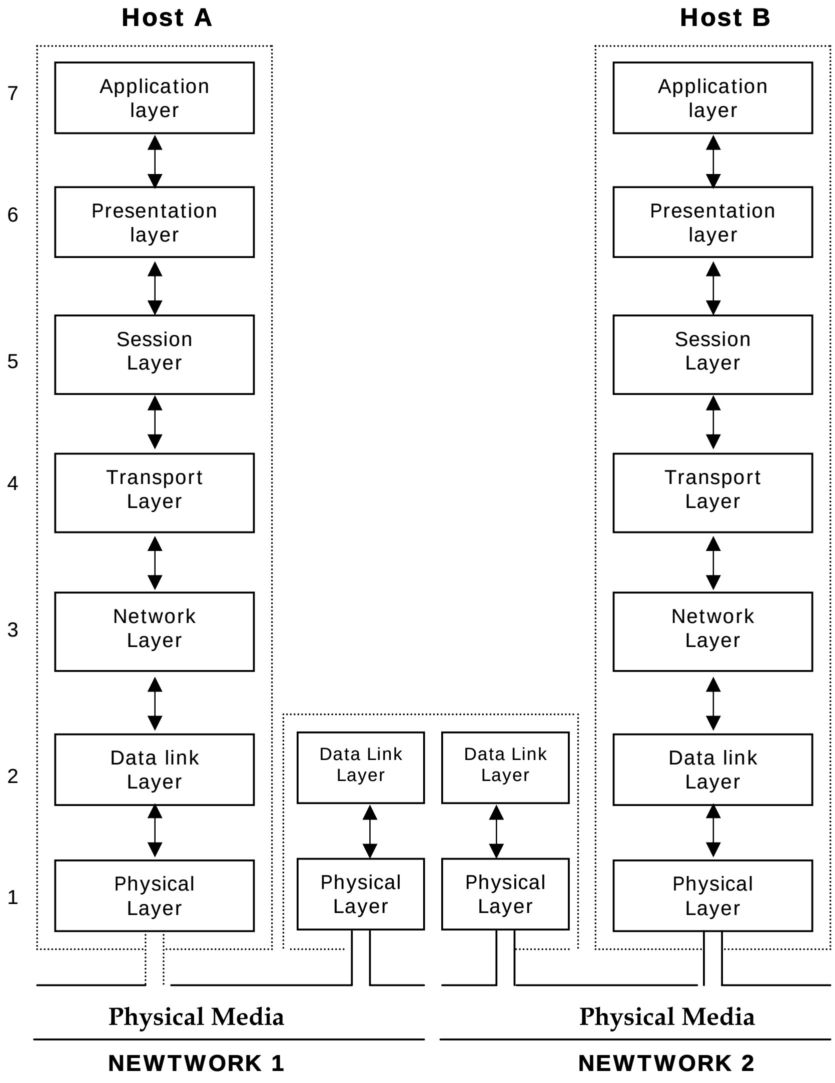


Fig How OSI model hosts communicating through bridge hosts

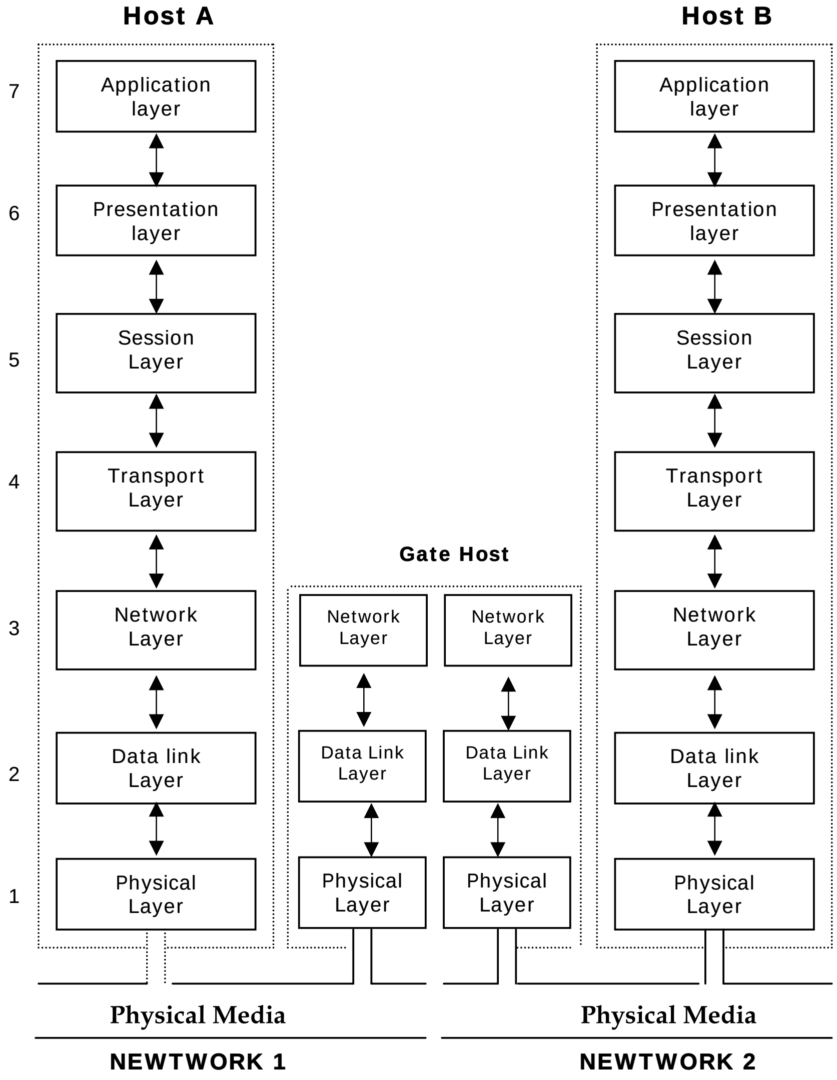


Fig How OSI model hosts communicating through gateway

With a more restricted geographic and technical scope. TCP/IP developers adopted a pragmatic approach. TCP/IP standardization was based on the request for comments(RFC) a flexible and fast standardization process using electronic mail to publish and exchange comments and ideas and to update drafts. Developers often outlined parts of a standard in a familiar computer language, usually 'C' which. While not intended to be implemented directly, gave a very good starting point for an initial implementation.

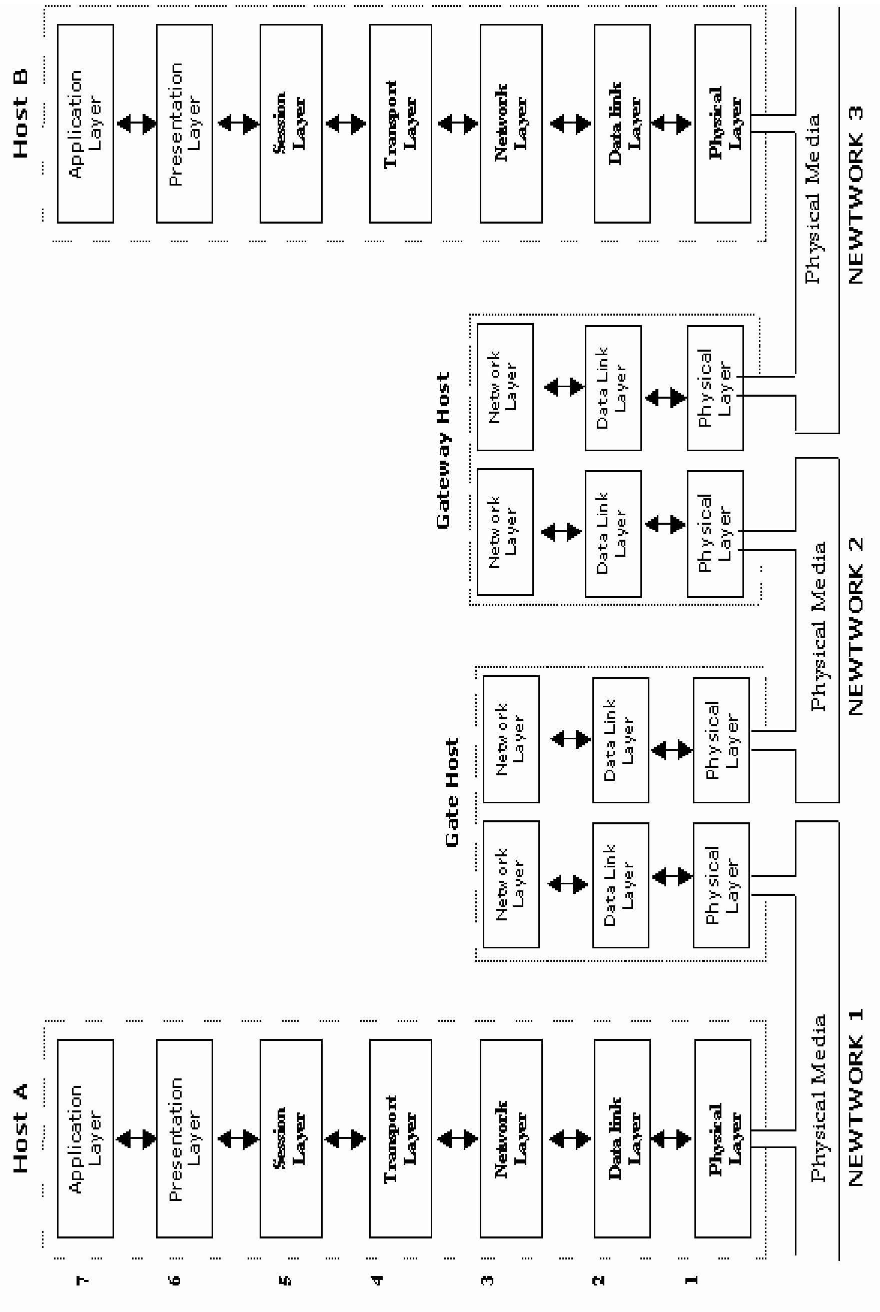
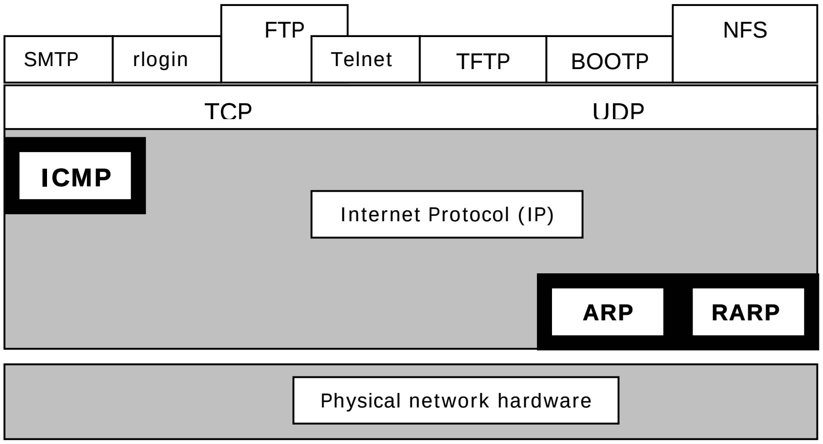


Figure How OSI model hosts communicate through routers

TCP/IP standards are freely available on-line from a number of computer systems, originally without full drawings or graphics, but today with all the quality of a laser printed, desktop-published document as postscript files. For manufacturers of communications and computing products, the contrast with OSI could not be more stark; it is just so much easier to obtain TCP/IP information than OSI. Standards were produced more quickly and they are written in a readable and comprehensible form by developers for developers.

The Us government demanded TCP/IP for all systems, there by ensuring every US government computer supplier provided it. They also funded universities to implement the standards. In the USA such publicly funded work enters the public domain and, if not of a military nature is freely available to all citizens. While it may not be used directly for commercial purposes, having a working example in 'C' source code certain assists future developments by a commercial suppliers!



ARP	Address Resolution Protocol	rlogin	remote login
Rarp	Reverse Address Resolution Protocol	FTP	File Transfer Protocol
ICMP	Internet Control Message Protocol	Telnet	remote terminal login
SMTP	Simple Mail Transfer Protocol	TFTP	Trival File Transfer Protocol
BOOTP	Boot Protocol	UDP	UserDAtagram Protocol
NFS	Network File System	TCP	Transmission Control Protocol

Figure TCP/IP Architecture

Neither OSI nor TCP/IP has been developed in isolation. There has been a considerable interchange of ideas and techniques, particularly evident in the changes in ISO since the mid-1980s with the development of the connectionless OSI suite. Now have the OSI standards been ignored by suppliers. As with TCP/IP in the USA, universities have been busy developing OSI implementations and governments have, since the mid 1980s required OSI conforming products. But this activity has not as yet created a general market demand and the same level of full developed OSI computing products, except perhaps with the notable exception of X.25 network equipment.

The 'pump priming' of TCP/IP has been more successful and has ensured, thereby, that it has moved ahead much faster than OSI. Governments and commercial organizations worldwide have waited patiently for OSI to become available and to reap the benefits of the promised flexibility of an international standard for computer communications and inter operation. In short, the development of OSI has lagged considerably behind TCP/IP, despite support from a number of governments (including since 1985, the government and department of Defense)

When it comes to breaking down communications barriers between different computer suppliers, information systems managers in commercial companies now see TCP/IP as a fully functional, proven and low-cost alternative to open systems interconnection. OSI is still immature and almost unavailable. This may change in near future but the explosive interest in TCP/IP will, on the one hand, delay OSI implementation and on the other, encourage it as larger organizations come up against some of the known fundamental limitations of TCP/IP.

As with much of the specialist vocabulary which surrounds computers and telecommunications networks, the term TCP/IP will conjure up different concepts to different readers. TCP/IP is used a s shorthand for a large set of standards with many different features and functions. The letters TCP/IP stand for two communications protocols. Transmission control protocol(TCP) and internet protocol(IP). These were developed during the late 1970s and early 1980s as the key communications protocols for the US 'Internet', the collected set of interconnected communications networks (originally comprising ARPAnet, but now including NSFnet, and NYSERnet and the Department of Defense Network among many others). Today these support the US government, Department of Defense, US military, and the university, education and commercial organizations conduct research on behalf of those bodies. (Use of the US Internet for commercial traffic between commercial organizations is not allowed.)(

TCP And IP are but two of the building blocks required for a complete communications 'architecture', but the term 'TCP/IP' is most often used as a shorthand term of the whole communications 'architecture' specified originally by the US department of Defense. This architecture is a much bigger set of standards than just TCP and IP. We shall also use TCP/IP to mean the complete architecture , except where this will cause confusion.

Communications architectures have been developed by computer manufacturers since the mid 1970s. An architecture describes three facets of communications in an abstract way which is independent of particular hardware or technology. The three aspects are:

1. Data exchange (intercommunication)
2. Data interpretation(interoperations)
3. System management.

Like the OSI reference model, communications architecture are described in layer: each layer providing its own functions but using the functions of the layer below. This layering decouples the functions of one layer from another making layered architectures flexible; their designers can respond to changes in technology and in application software without a major upheaval for existing users. The implementation and existing installations can be extended, as new, often faster techniques and technologies become available. It is important to realize that the standards do not specify the interfaces seen by computer users. Though suppliers often base their implementations on a competitor's successful product, one must expect that user interfaces will differ in major or minor ways, from supplier to supplier.

For TCP/IP, the architectural standards and the operational US Internet are controlled by the Internet Activities Board (IAB). The IAB devolves its responsibilities for development, operations and management to a number of subcommittees and work working groups which it controls and to other commercial companies specializing in communications and computing research and consultancy.

10.4 Internet Architecture

Two networks can only be connected by a computer that attaches to both of them. A physical attachment does not provide the interconnection we have in mind, because such a connection does not guarantee that the computer will cooperate with of the machines that wish to communicate. To have a viable internet, we need computers that are willing to shuffle packets from one network to another. Computers which interconnect two networks and pass packets from one to another are called internet gateways or internet routers.

Consider an example consisting of two physical networks as shown in figure. In the figure machine G connects to both network 1 and 2 . For G to act as a gateway, it must capture packets on network 1 that are bound for machines on network 2 and transfer them. Similarly G must capture packets on network 2 that are destined for machines on network 1 and transfer them.

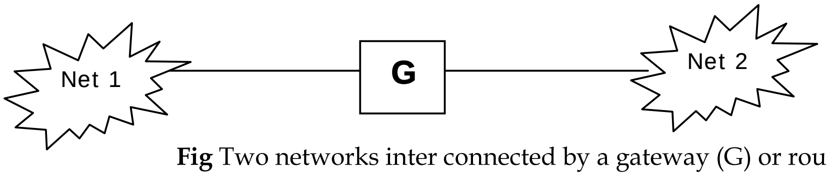


Fig Two networks inter connected by a gateway (G) or router

When internet connection become more complex, gateways need to know about the topology of the internet beyond the networks to which they connect. Figure shows an example of three networks interconnected by two gateways.

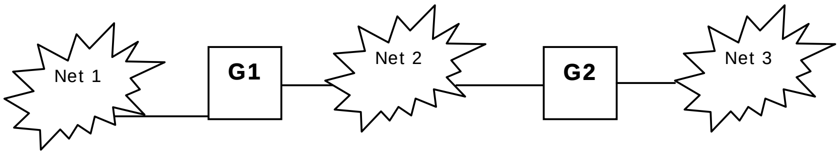


Fig Three networks interconnected by two gateways

In this example, gateway G1 must move from network 1 to network 2 all packets destined for machines on either network 2 or networks 3. As the size of the internet expands, the gateway's take of making decisions about where to send packets becomes more complex.

The idea of a gateway seems simple, but it is important because it provides a way to interconnect networks, not just machines.

❖ Note that in a TCP/IP internet, computers called gateways provide all interconnections among physical networks.

You might suspect that gateways, which must know how to route packets to their destination are large machines with enough primary or secondary memory to hold information about every machine in the internet to which they attach. However, gateways used with TCP/IP internets are usually minicomputer: they often have little or no disk storage and limited main memories. The concept of building a small internet gateway is gateways route packets based on destination network, not on distinction host.

If routing is based on networks, the amount of information that a gateway needs to keep is proportional to the number of networks in the internet, not the number of machines.

❖ Note that TCP/IP is designed to provide a universal interconnection among machines independent of the particular networks to which they attach. Thus, we want the user to view an internet as a single, virtual network to which all machines connect despite their physical connection. In addition to gateways that interconnect physical networks. Internet access software is needed on each host to allow application programs to use the internet as if it were a single, real physical network.

The advantage of providing interconnection at the network level now becomes clear. Because application programs that communicate over the internet do not know the details of underlying connections, they can be run without change on any machine. Because the details of each machine's physical network connections are hidden in the internet software, only that software needs to change when new physical connection appear or old ones disappear. It is possible to optimize routing by altering physical connections without event recompiling application programs.

A second advantage of having communication at the network level is more subtle: users do not have to understand or remember how network connect or what traffic they carry. Application programs can be written that operate independent of underlying physical connectivity. In fact, network managers are free to change interior parts of the underlying internet architecture without changing application software inmost of the computers attached to the internet.

Figure shows that gateways do not provide direct connections among all pairs of networks. It may be necessary for traffic traveling from one machine to another to pass across several intermediate networks. Thus, networks participating in the internet are analogous to highways in the Us interstate system: each net agrees to handle transit traffic in exchange for the right to send traffic though out the internet. Typical users are unaffected and unaware of extra traffic on their local network.

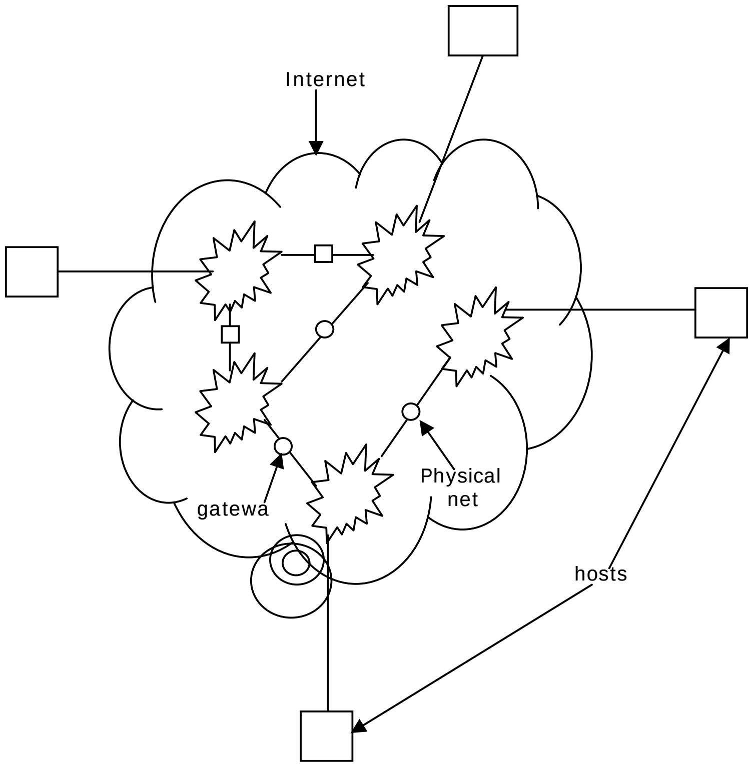


Fig The structure of physical networks and gateways that provide interconnection

It is important to understand a fundamental concept: from the internet point of view, any communication system capable of transferring packets counts as a single network, independent of its delay and throughput characteristics, maximum packet six, or geographic scale. Figure uses the same small could to depict all physical networks because TCP/IP treats them equally despite their differences.

- ❖ Note that the TCP/IP internet protocols treat all networks equally. A local area network like an Ethernet, a wide area network like the NSFNET backbone, or a point to point link between two machines each count as one network.

10.5 How TCP/IP Works?

Most networks provide some sort of connection mechanism to get from point A to point B. Other networks worry about how to get from node A on network X to node B on network Y.

If a program wishes to send information from itself on node A to another node on the same network, TCP will provide the packet sequencing, error control, and other services that are required to allow reliable end to end communications. This does not mean that IP is requires. In fact, some implementations of TCP connect directly to the network service layer and bypass IPL altogether. If, however, a program on node A on an Ethernet wished to connect to a destination program on node B on an X-25 network, internet routing function would be necessary to get data packets sent properly between the two dissimilar network services. IP would take the packet from TCP, pass it through a gateway that would provide conversion services and then send the packet to the IP layer at one remote node for delivery to the remote TCP layer and, subsequently, the destination program. A good comparison would be as follows:

a. Program A on node ALPHA wishes to connect to program B on node BETA on the same network. Program A would send a data packet to TCLP with the proper destination address. TCP would then encapsulate the data with the proper header and checksums in accordance with whatever services the program requested and pass the TCP packet to the IP layer. IP would then determine, from network directory information, that the remote node is on the same network as itself and simply pass the packet through to the network services layer for local network routing and delivery

b. Program A on node ALPHA on network X wishes to connect to program B on node BETA on network Y. In this situation, data would be handled as in case (a) above, but IP would determine that the destination is not on the local network. As a result, the IP layer in node ALPHA would determine the best route to get to the remote node and send the TCP packet to the next IP node in the path to get to the remote. IP does not care which program the source wants to connect to all it cares about is which node to send the packets to.

If nodes in the path from node ALPHA to node BETA will examine the packet to determine the destination and will forward the packet to the proper until it reaches the destination network IPL. That ILP determines that the node is on its local network and the packet is handed to the network services layer for the network on which BETA resides for delivery to node BETA.

Once the packet is received at the final destination IP. It is passed up to the TCP layer, which breaks out the packet header to figure out which program on the destination node is to receive the data. First however, the packet header is examined carefully to insure that it has arrived in the proper sequence and that there are no special handling issues that need to be serviced. Once TCP is satisfied that everything is reasonable, the data is delivered to the destination program.

While all of this seems pretty straightforward , there are some implementation issues that make all of this complex. Since TCP and IP allow many service options such as message priority, security classification, data segmentation at the TCP level , packet segmentation at the IP level and other issues that some network architectures. Such as DECnet, need not concern themselves with , there can be some considerable overhead associated with packet processing. As a result, TCP/IP performance varies significantly from network hardware to network hardware as well as from machine implementation to machine implementation.

Now that we have examined the generalized delivery mode, let us look at some of the specifics.

10.6 What TCP was Built to do?

One of the base problems that TCP was built to address is the issue of connection from a particular program on a particular node on a particular network of a remote program destination that may or may not be on the same network as the originator. As such, a method of addressing nodes needed to be developed that identified a particular program on a particular node in a particular network. A possible solution is to develop hard addresses for all entities on a particular network. While this solves the problem, it is inflexible and usually does not provide an upwardly flexible network architecture. Another problem is that some networks have their own proprietary (and sometimes bizarre)addressing scheme that must be considered as TCP/IP are above the local network addressing scheme mechanisms in the network architecture and will need to use the local mechanism that allows for delivery of packets across dissimilar network architectures.

To begin with, each program (called a PROCESS in TCP) has a unique one up address on each machine. That unique local program address is combined with a particular node address to form something called a port. The port address is further combined with the local network but each socket identifies, exactly, one specific application on a specific node on a specific network. Through this mechanism IP will get the packets to the proper node and

TCP will deliver the packet to the proper program on that node. Some nodes provide a standard process type (such as type 23 for remote log-ins) that are "known" to other network entities and that provide certain standard services. Through this mechanism. TCP provides a multiplexing capability that is essential in the efficient use of the network resource.

10.7 From one Socket to Another

As with any network two sockets that wish to connect to each other must have a mechanics, by which this happens. TCP provides this various ways. One of the more common was connections are established is via an ACTIVE/PASSIVE network OPEN. A PASSIVE OPEN is when a receptive socket declares itself to be open and available for incoming connections (this would typically be the mode used by something like a database server). A PASSIVE OPEN, however, may be set up to be FULLY SPECIFIED, which means that the socket issuing the PASSIVE OPEN tells the network exactly which socket may connect to it including security levels allowed and other related details. Another type of PASSIVER OPEN is the UNSPECIFIED PASSIVE OPEN in which the socket will accept any connection meets prescribed security and other criteria. In both types of network OPENS it is pertinent to point out that the socket OPENing the network may also declare timeout values for all data received from the originator of the connection. This allows for the expeditious handling of data as well as providing a means by which "old" messages are handled in a reasonable fashion and messages requiring special handling (in terms of time) are processed correctly.

Another type of OPEN is the ACTIVE OPEN. Unlike the PASSIVE OPEN, the ACTIVE OPEN aggressively seeks a connection to a particular socket. An ACTIVE OPEN will only be successful if there is a cooperating and corresponding PASSIVE OPEN or other ACTIVE OPEN from the destination socket.

Once a connection has been established between two sockets, data may be transferred between the sockets. TCP provides several mechanisms for data transfer, but the two most popular are segmented data transfer and PUSH mode. Segmented data transfer allows TCP to send user data in chunks across the network. As such, TCP may send the data in such a manner that allows for the best efficiency for the network being used. This means that even if the user has transferred 25 blocks of user data to TCP. TCP may not send it all at once, opting to segment the data in such a manner as to provide optimal flow of data on the network. While this technique is great for data flow issues and network congestion issue, it can be troublesome for transfers in which the data needs to get to the remote system NOW! In such cases, the user may specify the PUSH flag. A PUSH request forces TCP to send whatever has been passed from the user to TCP right away with no consideration for optimal flow control. In addition to the Push flag, the user may specify the urgency of the data being transferred to keep the remote system on its toes.

How much data is allowed to be sent from one socket to another is a function f the network and programs involved. Since TCP was developed with multiple network architectures in mind, it allows some level of line negotiation on connection and data transfer that provides for maximum buffer sizes (somewhat dynamically) and maximum buffer allocation.

10.8 TCP Sequencing

To insure that everything gets to where it is going and in the proper order. TCP provides packet sequencing services as well as error detection functions utilizing a 16-bit check sum in the TCP header area. It is also interesting to note that TCP presumes the IP layer to be unreliable and, therefor, includes a 96-bit pseudoheader infront of the actual TCP packet header that includes the sources address, destination address, protocol being used and segment size. Through the use of the pseudoheader, TCP protects itself from IP delivering the packet to the wrong place (or not at all) by misinterpreting TCP header fields. The checks min the TCP header also includes the pseudoheader bits to insure that everything is clean when it hits the remote side.

After the connection is established and all data has been transferred, the ink may be shut down via user request. This is the clean way. It is very possible that the link may also be abruptly aborted due to link drop or some catastrophic failure of the network or socket to socket linkage. TCP provides mechanisms to handle both situations. A CLOSE primitive issuance tells TCP that the user is finished with the network link and to close down the link gracefully by sending all remaining data in local buffers and notifying the remote socket that the sending user wishes to CLOSE the link. The remote TCP socket notifies the user that a CLOSE has been issued. The user may then send any remaining data and issue a CLOSE to the sender. When the sender receives the CLOSES acknowledgement from the receiver, it sends a TERMINATE to the user and the CLOSE acknowledgement from the receiver, it sends a TERMINATE to the user and notifies the remote TCP that a TERMINATE has been issued. The remote TCP socket sends a TERMINATE to the remote user and the link is closed completely.

If a network link abort occurs, for whatever reason, the ABORT primitive is sent to the remote TCP. Which tells the remote user that a TERMINATE has occurred. No more data of any kind is transmitted on the link and the link is closed immediately on both sides. Obviously, a link termination of the ABORT kind is not desirable, as data may be lost and other integrity issues may be involved.

10.9 TCP Needs not an IP

It is important to understand that TCP need not be connected to an IP, although that is frequently the case. TCP provides the essential network connection and data transfer features which a user would require to connect with a particular program on a remote system. Some companies use TCP as the protocol of choice when setting up simple direct-connect network connections (where the remote node is hard wired to the originating node) or when performing tasks such as down line system loading. In any case TCP is powerful and full featured protocol that provides reasonable network services for user data.

Many times, however, just getting the data from one socket to another may involve the connection to various types of network technologies. A TCP packet coming in from an asynchronous link may need to be routed on to an Ethernet to reach its ultimate destination. Because of the need to connect and properly route data through to its proper network and destination socket, the IP layer was developed.

10.10 Short summary

- TCP/IP a comprehensive set of 'ready-made' communications protocol.
- Any communication system capable of transferring packets counts as a single network, independent of its delay and throughput characteristics, maximum packet six, or geographic scale.
- ACTIVE OPEN aggressively seeks a connection to a particular socket.
- The advantage of providing interconnection at the network level leads to communicate over the internet do not know the details of underlying connections, they can be run without change on any machine.

- TCP And IP are but two of the building blocks required for a complete communications 'architecture'.

- A network architecture is a way to define the set of rules to which these interconnecting elements must confer.

10.11 Brain Storm

1. What is the Origin of TCP/IP?
2. Explain about TCP/IP Communication Architecture.
3. Give a short notes on Internet Architecture.
4. What is the need of TCP?

Lecture 11

Working with TCP/IP

Objectives

In this lecture you will learn the following

- About IP
- About TCP/IP Applications
- About FTP

Coverage Plan

Lecture 11

11.1 Snap shot

11.2 Gateway and IP

11.3 TCP/IP Applications

11.4 File Transfer Protocol (FTP)

11.5 Telnet

11.6 Trivial File Transfer Protocol

11.7 Simple Mail Transfer Protocol

11.8 Network File System

10.10 Short Summary

10.11 Brain Storm

11.1 Snap Shot- What is an IP?

IP is a data gram service. It basically provides rudimentary Internet routing services without any regard to the destination program. TCP formats, error control, packet sequencing, etc. Its function in life is to get the packet to the right network and eventually, to the right node. Further, IP allows for expedited routing of packets that need to get to a destination quicker than other, routine packets. In many respects, with the exception of routing priority, IP functionality is similar to Ethernet packet handling. If a packet arrives that is damaged (there is an IP checksum), the packet is discarded. What is in the data field of the packet is of no interest to IP. IP could be sending a TCP packet or some other protocol for all it cares/ As long as the proper SEND (user sending to the network) primitive fields have been filled in. IP will send the packet on its merry way. When the packet reached the remote node and the checksum figures out OK. IP sends the packet to TCP (or whatever the receptor protocol is) via DELIVER directive and all is well with the universe. If the packet gets trashed in the process of being delivered so be it . If the packets arrive out of sequence, that is not IP's problem. If a packet is missing, again . IP does not care. IP gets the data packet (usually a TCP packet) from point A on network X to point B on network Y. That is all, nothing more.

11.2 Gateway and IP

To provide the Internet work routing function, IP makes use of special nodes called gateways. A gateway, in IP terms, is a machine that allows two dissimilar networks to be connected to each other. The two networks may or may not be the same type (Ethernet, x.25, token ring, etc), as IP operates above the hardware itself and is only interested in the virtual connection function, not the physical path or hardware used. As such, there may be a need to segment large messages from the upper software layers into sizes that are applicable to the remote note work's allowances. To do this, IP will segment large messages into proper-sized chunks (such as when going from 1500 byte Ethernet packets to 128 bite X.25 packets) for the destination network and reassemble them at the remote destination IP layer before deliver to the user. If a packet gets destroyed in the segmented message and the remote IP detects the packet loss, the entire segment is killed off by the remote IP. Obviously, TCP would detect that a segment is missing and request a retransmission from the remote TCP for any missing packets. TCP has the option of forcing IP NOT to segment packets, but this is usually not implemented as it can cause routing problems where differing network technologies are concerned.

IP also provides for proper security classification of packets being sent to a remote site. If an intermediary gateway or network is not at the same security level as the transmitted packet, the packet will not be sent through that network. As a result, some strange routing of data may occur sometimes as IP must contend with the problem of expeditious routing but also the problem of security-oriented routing.

Finally, IP has some different terminology than that typically used in a network. In many networks, the concept of a "hop" is the routing of a data packet through a node on its way to its final destination point. In IP, a hop is when a data packet goes through a gateway to another network. Therefor, it is quite possible that a packet may wander through barrios nodes in a local network before it actually gets to the remote network gateway, depending, of course, upon preciously discussed variables. If the packet does not incur a route through a gateway, it, in IP terms, has not incurred a hop. If it transverses through two gateway , it would be considered to have incurred two hops on its path to the final destination. Hops, therefore, are not referred to in the same manner as many other popular communications architectures.

As can be seen, TCP and IP are not the same and may actually be implemented totally independent of each other for separate uses. More often than not, however, they are both included in many offerings from various vendors.

As can be seen, TCP and IP are not the same and may actually be implemented totally independent of each other for separate uses. More often than not, however, they are both included in many offerings from vendors.

11.3 TCP/IP Applications

In any network architecture, the protocols and transmission methods are not enough, users frequently want and need utilities that implement the protocols in the network architecture to allow file transfer, program communication, virtual terminal support and electronic, mail. Most TCP/IP implementations are the same and a few standard applications exist.

11.4 File Transfer Protocol (FTP)

File transfer facilities are usually provided for by a mechanism known as the file transfer protocol, FTP is a simple featured file-moving utility that allows a record oriented (one record at a time) transfer, a block transfer (which moves chunks of a file), or an image transfer (which does not look in any way at the file contents). Further, FTP knows about EBCDIC and ASCII and may provide some rudimentary conversion facilities BEFORE a transfer begins. As file systems are very complex and the need formulae transfer between systems is growing. FTP has evolved in some cases to special implementations that know how to convert specific file formats between certain types of machine architectures. This conversion facility is not within the defined scope of FTP, but some vendors include the conversion features anyway. Transfer a file, the user invokes the host. FTP utility, specifies file name, type, remote destination and off it goes. One interesting feature on some FTP implementation is the recovery facility. Networks, as most are well aware, will fail from time to time. In the case of failure, any transfers in process will usually have to be restarted from scratch. If the file is being transferred with FTP in block mode, It may be possible to resume the transfer at a later time by specifying which block was the last transmitted. FTP would then continue to send the file as if nothing had happened. This feature is not available on all FTP implementations and has some host and remote system software considerations involved with it , but, all in all, it is a useful feature to have when transferring very large files.

11.5 Telnet

Another popular utility is known a TELNET. TELNET is a virtual terminal facility that allows a user to connect to a remote system as if the user's terminal were hard-wired to that remote system. Virtual terminals may need to emulate a wide variety of terminals. Which may be impractical on larger, complex networks. As such, TELNET provides a basic protocol handling facility and a negotiation facility that allows for the inclusion of different types of terminal protocols and signaling mechanisms.

There are four ways of using Telnet. The terminal could be a simple 'dumb' terminal connected to a TCP/I[P terminal server with a standard communications interface A(V.24/V.28 OR EIA 232). Equally, that simple terminal could be a workstation or PC running a terminal emulator and connected to the same terminal server in the same way. A minicomputer can run Telnet software which provides the terminal server capability from with in the minicomputer. Alternatively, a PC or other workstation could run a version of TCP/IP and a terminal emulator and connect directly to a LAN.

The Telnet service was on of the first to be provided in a standard way by the TCP/IP architecture. It delivers a similar service to that provided by the switching statistical multiplexes of the early to mid-1980s which provided many companies with their first example of flexible access to information.

Telnet allows terminal or workstation users to gain access to a host system and to display host data on their screens. It is a remote terminal service; any terminal user must know how to operate the host system or host application from a terminal of that type. No attempt is made to map the user interface environments from one system to the other.

The Telnet service is most commonly used with ASCII asynchronous terminals such as the ANSI standard terminal or the DEC VT series. Most manufacturers of other terminal, types have registered them with the Internet Assigned numbers Authority (IANA) so that they can be identified to the Telnet protocol. That does not mean that a particular implementation of workstation Telnet will necessarily match the host software. Any - to -any protocol conversion is not necessarily a feature; systems which match must be carefully chosen.

The advantage of the Telnet terminal server is that it provides a low cost connection. But the interface often operates in asynchronous character-by-character mode; the terminal is strictly limited in its capabilities with little possibility of upgrading the
service in the future.

Asynchronous interfaces can involve large management overheads. Cabling for the terminals may require only three wires, but for some terminal types and uses, it could be more. A structured cabling system with centrally located terminal servers can reduce management costs. At each interface, a number of parameters must be configured- speed, parity, flow control method and type of terminal, to ensure the correct control sequences are used. Unless a single standard for these parameters can be enforced throughout the organization, by apparent cost savings can be quickly allowed up in increased management costs. This is particularly so in the larger installation, where the unit costs of supporting large numbers of terminal servers may not reduce with increasing size. Where terminal servers can be remotely configured from a central network management system, support costs may be more easily contained.

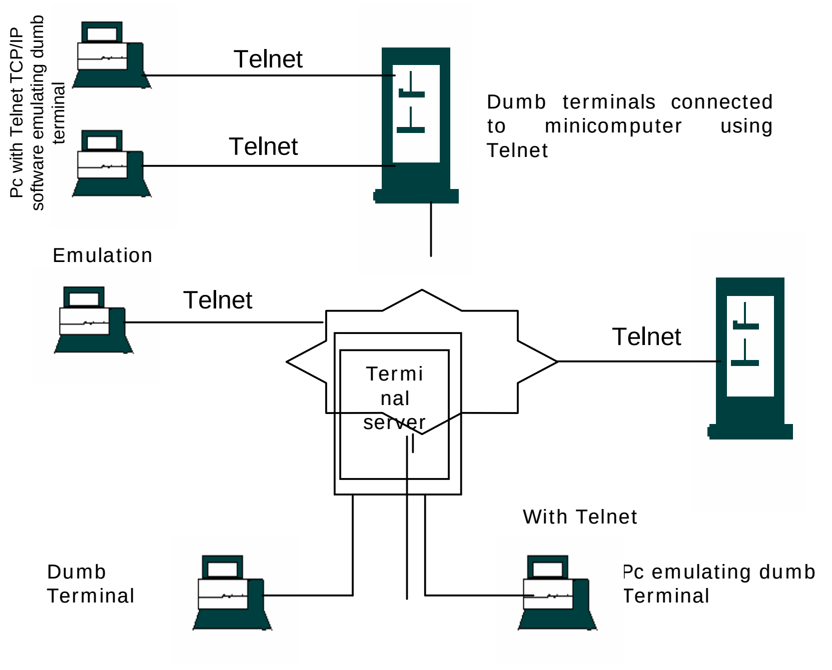

Pc with Telnet TCP/IP software emulating dumb terminal
Telnet
Telnet
Dumb terminals connected to minicomputer using Telnet
Emulation
Telnet
Terminal server
Telnet
With Telnet
Dumb Terminal
Pc emulating dumb Terminal

Figure Telnet support for terminals

11.6 Trivial file transfer protocol

The Trivial File Transfer Protocol (TFTP) is simple program with minimal facilities, designed to be implemented in permanent memory(PROM), so that diskless computers may perform their initial loading of an operating system. It is often used in conjunction with the booed protocol, It is not usual for it to be used for other purposes.

TFTP lack the security features of FTP and it is normal to disable the TFTP server on hosts which do not provide a BOOTP service.

11.7 Simple Mail Transfer Protocol

A final utility that is somewhat popular is the Simple MAIL Transfer Protocol of SMTP as it is more affectionately known. SMTP provides a mechanism by which a user can specify a destination address (or addresses if to more than one remote user), a particular path to follow (if desired) and a message. Like other electronic mail systems, SMTP provides for return receipts, forwarding of mail , and other similar features, The only odd issue has to do with the problem of the term "SIMPLE" . Having used SMTP for some years now, it is not intuitive and the routing issues can get strange. Yet, it is a useful utility and heavily used in the defense area.

Some of the organizational issues of SMTP arise because of the association of person with a particular computer. Those computers are the .MDBO/ mail servers. MDNM/ of SMTP and they must always be available to receive mail. An individual workstation or PC is unlikely to make a satisfactory mail server as its availability cannot be guaranteed. A mail server is more likely to be a prt-time task carried out by another server machine.

Building on SMTP protocols, some manufacturers have introduced the mail relay or mail store, which receives and stores mail on behalf workstation users until they access the store using as SMTP client on their workstation. A workstation can be a satisfactory generator of SMTP mail, but it is a poor and inattentive recipient.

Staff who travel must be able to access the mail system they are registered on, for that is where their mailbox resides. Alternatively, a method of mail forwarding can be devised, but such features are beyond the SMTP itself and are implementation dependent.

If mail users change location permanently, their mail addresses may change. They will have to advise all their correspondents for that change. TCP/IP standards do not include a directory services to relate people to mail addresses or for that matter to relate application servers to network addresses. Worldwide research into directory services has concentrated on perfecting and implementing the CCITT X.500 recommendations which are accepted as part of OSI. Indeed, the ULS internet is said to be the biggest trial of X.500directory services in the world. Several RFCs describe how X.500 is to be used on the internet and the adaptation needed to operate over TCP/IP PROTOCOLS.

11.8 Network file system

The network File System (NFS), as it is still commonly known, or Open Network Computing (ONC), as its create Sun Microsystems Inc, now calls its, is one of the more recent standard additions to the TCP/IP protocol suite. ONC was developed by Sun Microsystems Inc. for its high performance UNIX workstations and later released to the 'public domain' as three RFCs which describe the major protocol components. Recognizing the importance of IBM PC, Sun also developed NFS software for the IBM PC, the PC-NFS client. This allows PCs to us UNIX workstations as remote file and print servers, NFS client and server software is now available for most computer systems.

NFS provides user services familiar to any user of a proprietary resource-sharing LAN such as Net ware. LAN manager of Banyan VINES. Files, directories and peripherals on a remote NFS server are mapped to 'virtual' drives, directories or peripherals on the local system. For most purposes, these virtual drives and printers are indistinguishable from and are used identically to local resources.

On a UNIX system, each remote directory appears as an additional directory of the main local directory structure. For a PC, with PC-NFS , the remote directories appear as additional disk drives. From the perspective of the commercial information systems manager, this is ideal, for unlike other TCP/IP applications described below, most business users need no new training to use NFS; they merely have access to more information with bigger disks and better printers.

But NFS can go beyond simple resource sharing. It provides the mechanism for true distributed computing, where processing power, not just data, is shared among networked machines. These client/server applications can reduce the load on busy networks significantly.

The major management issues of NFS can be hidden from the users. These issues center on the security and mapping of user identifiers and access rights between different operating systems. NFS works in conjunction with the Network Information Services (NIS), a distributed database system for NFS security which provides for provided by Sun ; the administration of a large user population still requires careful organization. with the correct clerical procedures in place to ensure that security meet the requirements of the organization. It must not be so lax as to compromise data integrity and not so tight that no one can get work done.

NFS uses UDP transport protocol. Remote disk data transfer rates can be reduced significantly by delay, particularly in wide are links. There is at least one implementation providing the same services as NFS , which uses TCP transport. An alternative solution is to buy more servers and place them close to the users.

Where the main NFS activity is resource sharing, poor configuration options in the workstations can have a dramatic effect on network traffic. The use of print spoolers, temporary files, backup files. PC batch files and the format of the 'path' statement can all influence the traffic, a workstation generates on the network.

To make NFS completely invisible to end users, each workstation should have a script or batch file which executes the NFS 'mount' commands to make the remote resources locally available. The details of the command line can be totally hidden.

In the last, memory requirements for PC network software have left too little of the available 640k to run some of the more demanding PC applications. Some implementations of PC-NFS require in excess of 130kbytes to load a LAN card driver, the TCP/IP care software and the NGS client application. By reducing the number if file systems which may be mounted and by tuning other parameters, this figure can be reduced by a few kilobytes. A 80386 processors with large amounts of memory and the MS DOS 5.0 operating system replace older configurations and software, the PC memory sizing will be required for NFS SYSTEMS.

11.9 Short Summary

- If mail users change location permanently, their mail addresses may change.
- The Trivial File Transfer Protocol (TFTP) is simple program with minimal facilities, designed to be implemented in permanent memory(PROM).
- The advantage of the Telnet terminal server is that it provides a low cost connection.
- IP provides rudimentary Internet routing services without any regard to the destination program.

11.10 Brain Storm

1. What is an IP?
2. How does IP act as a Gateway?
3. Give short notes on FTP
4. Explain the term Telnet
5. Explain TFTP, SMTP

Lecture 12

TCP/IP Implementations

Objectives

In this lecture you will learn the following

- How is TCP/IP Implemented?
- About Finger Protocol
- About Ping

Coverage Plan

Lecture 12

12.1 Snap Shot

This chapter finished with a brief look at the X window System, another heavy user of TCP/IP. We saw that the X server manages multiple windows on a display, and handle the communication between a client and its window. Each client has its own TCP connection to the server and a single server manages all the clients for a given display.

12.2 TCP/IP Implementation

Some vendors of TCP/IP have made a cozy living out of providing their wares to defense contractors and UNIX/Ultrix shops that need to connect and communicate with their compatriots supporting TCP/IP. How the vendors have implemented TCP and IP varies greatly, which also means that features and performance vary significantly. Some vendors, such as Excel an, have chosen to implement much of the protocol suit in a controller card., effectively offloading the host from the duties of running TCP and IP programs and utilities and yet providing the necessary connectivity. This is nice as it offloads the host and mains the overall system more cost effective and less bogged down in the network mire. Other companies, such as Wollon gong, have chosen to implement TCP/IP in software on the host. This degrades the host system,. Sometimes severely, but has the advantage of being able to function as a true IP node, allowing connection to various network technologies simultaneously.

Each implementation has its benefits and drawbacks. Which one is best for a particular systems depends heavily upon cost factors, system loading expectations and how many different kinds of networks a site may be connected, some vendors have begun to introduce TCP/IP routers that allow ILP services to different types of networks by connecting the network through dedicated IP router (some times referred to as an IMP) and allowing TCP messages to be created by a particular network protocol, translated into TCP and sent to a destination node. The source node thinks that it is talking to a machine running the same protocol on the same network. In reality, the packet has been translated and set to the destination node one either the same or another network. Such routing and translation tricky is beginning to become more and more prevalent in environments where TCP and other types of networking software exist.

In the quest to TCP/IP or not TCP/IP, the bottom line is how long can it last? A few years ago it would have been said that it was a safe bet that usage of TCP/IP would last a company for some years to come. Now that the DOD no longer require the absolute use of TCP/IP opting, instead, to go with OSI, such is not a safe bet for all sites. There are enough TCP sites installed that it would be foolish and expensive to haul off and convert all sites to something else. It is also prudent to remember that the number of installed in such a way as to make protocols such as TCP/IP become a minority. Much has to do with who is buying what as to how long it will last. However, TCPL/IP will be around for a while, if to do nothing else than support current systems. As those systems cut Over to OSI, however, fewer and fewer nodes will be seen running TCP or IP in favor of OSI.

What would we do if we had to buy today? Buy TCP/IP of course. Why? Because it works and it is now. It would serve very nicely for the short term (2-4 years) and give the OSI packages some time to mature before diving in headlong. A nice side benefit is that the OSI transport service and TCP's capabilities are very similar, as are the ISO network layer routing service and the ILP services. Further, TCP/IP prescribes standardized network hardware, so OSI compliant hardware is given in many TCP/IP environments, allowing a nice migration path to OSI at a future data. If one installs OSI Compliant hardware, then conversion to OSI from TCP/IP1 IS not as traumatic as it could be.

12.3 Finger protocol

The Finger protocol returns information on one or more than one users on a specified host. It's most commonly used to see if someone is currently logged on, or to figure out someone's login name, to send them mail.

Many sites do not run a Finger server for two reasons:

i. a programming error in a earlier version of the server was one of the entry points used by the infamous internet worm of 1988.

ii. The finger protocol can reveal detailed information on users (login names, phone numbers, when they last logged in. etc.) that many administrators consider private.

The Finger server has a well-known port of 79. The client does an active open this port and sends a one-line query. The server processes the query, sends back the output, and closes the connection.

Before you can communicate with another user you must know the user's internet address. One of the commands you can use to determine the address of user is the finger command. The finger command tells you two things:

N Who is logged in at the current time
N Information about a specific user account.

For example, let's say you need to get in touch with someone at a particular host system. You think you know their user ID but you're not quite user. You can use the finger command to see if they are on line and if so you finger out what their ID might be.

FINGER <ENTER>

If the finger program is available on your system, you should see a list of users currently logged into your system.

Finger DCI <ENTER>

You can find more detailed information about an individual by following the finger Command with their ID.

The ID you use does not need to belong to a currently connected individual (dome one who is logged in): it can be any user ID recognized by your system. Using finger in this way lists the full name of the individual, how long they have been on, and other information about the user.

You can also use the finger command to find out who is logged onto other computer systems. This is done is one of two general ways. First, you can discover who is logged onto another system by including the system name is the command, as follows:

Finger @ niit.columbia.edu <ENTER>

This command tries to connect with the remote site (@niit.columbia.edu) and if successful, lists the users logged into that system. The information you get back depends on a couple of things. Primarily how the finger command functions at the remote site and whether that ’site supports the finger command being used from remote locations. Not all sites support remote fingering; if they do not, you might see a message indicating that there are no users connected or that there was an error in connecting. If remote fingering is supported, however, you will see a display similar to the one shown when you used finger on your local system.

Another way to use finger remotely is to display specific information about a user at a remote site by providing a full internet address. For instance, the following command displays specifics about a user connected to a computer at Columbia University.

```
ABC> finger smith@niit.columbia.edu ,<ENTER>
```

12.4 Whois protocol

The whois protocol is another information service. Any site can provide a who is server, the one at the InerNIC.rs.internic.net. is most commonly used. This server maintains information about all registered DNS domains and many system administrators responsible for systems connected to the Internet. Another server is provided at nic.ddn.mil, but contains information only about the MILNET. Unfortunately the information can be out of data or incomplete. RFC 954 lists I detail Whois service.

The Whois server has a well known TCP port of 43. It accepts connection requests from clients, and the client sends a one line query to the server. The server responds with whatever information is available and then closes the connection. The requests and replies are transmitted using NVT ASCII. This is almost identical to the Finger server. Although the requests and replies contain different information.

For example, if you want to connect to a computer at Arizona State University, but you don't remember the computer's Internet address, you can quickly look up that address using whois. To us the who is command, you simply use the following syntax

```
Whois  [-h host] text
```

Where host is the optional name of a particular host whois server your want to search, and text is the name, domain, or host you want to find.

As an example, let's assume you wanted to search for hosts related to Brigham Young University, in Provo, Utah. The common acronym for the school is BYU, so you figure that is a good place to start. Using this information, you can enter the following command

Whois byu <ENTER>

You can take you who is search even one step further, if you wish. For instance, let's say that the VAX system at BYU caught your interest. You could get information on this particular host in the following manner

Whois yvax.byu.edu <ENTER>

Since you entered a host name (not a domain name), who is will provide you with information about the host. This information lets you know what sort of system it is as well as who runs the system.

12.5 Gopher

Gopher is a menu driven front end to other internet resource services, such as Arched, and anonymous FTP. Gopher is one of the easiest to use, since its user interface is the same, regardless of which resource service it's using.

The use Gopher. Telnet into is.internic.net and login as gopher

12.6 Veronica

Veronica is tool used in conjunction with gopher, developed by the folks at the University of Nevada. It is basically an extension to gopher, providing a major feature (an index) that many people felt was lacking in the original product. As the number of gopher servers in the world grew, there was no comprehensive index to the information in each of the gopher servers. Basically this means that there is no easy way to quickly search all the gopher databases and extract only information that matches your particular needs. This is where veronica comes in. Veronica does nothing more than search indexes of all the tiles of documents in gopher servers around the world. Through a gopher menu choice that access veronica your can then perform a keyword search on this index. The results are returned in a form that gopher can display in its normal format.

12.7 Archie

Most of the resources used in this text were obtained using anonymous FTP. The problem is finding which FTP site has the program we want. Sometimes we don't even know the exact filename but know some keywords that probably appear in the filename.

Archie provides a directory of thousands of FTP servers across the Internet. We can access this directory by logging into an Archie server and searching for files whose name contains a specified regular expression. The output is a list of servers with matching filenames. We then use anonymous FTP to that site to fetch the file.

There are many Archie servers across the world. One starting point is to use Telnet to ds.internic.net login as archie, and execute the command servers. This provides a list of all the Archie servers, and their location.

12.8 WAIS: Wide Area Information Servers

You are already familiar with the more common searching tools available on the Internet, such as gopher and Archie. But what happens when you can't find a specific database for your research? When you have a well defined topic on which to search, you can get your work done in minimal time and error using the tools previously presented On the other hand, you may have some esoteric subject that just can't be defined in one simple word or phrase.

In a more personal sense. WAIS behaves much like a reference librarian at your public library, in that it looks for the information you request. If you provide a topic of a few descriptive keywords, any good librarian knows exactly where a certain book is located. From the vast indexes maintained in a WAIS server, WAIS also knows just where to find information based on the parameters you provide.

WAIS keeps you from the concern of where to find the data you need. Specifically the database that WAIS can access are not all located at the same diet. It would be impractical and a waste of resources to keep and maintain all the databases in one place. This would require a vast amount of storage space and computer processing, not to mention make it difficult for contributors to keep database items current.

That is where WAIS comes in. There are WAIS databases in many locations across the Internet . Each of these databases is indexed, and WAIS consults the index to satisfy your search requests. This index points to the database items (the source documents)the contain that word.

Ping

PING is a very simple protocol that uses the user data gram protocol (UDP) segment. Its principal operation is to send a message and simple wait for it to come back.

PING is so named because it is an echo protocol and uses the ICMP echo and echo-reply messages. Each machine is operating with a PING server whenever IP is active on the machine. PING is used principally by systems programmers for diagnostic and debugging purposes. It is very useful because it provides the following functions:

N The loop back ping used to verify the operation of the TCLP/IP software.

N The ping address determines if a physical network device can be addressed.

N The ping remote IP address verifies whether the network can be addressed.

N The ping remote host name verifies the operation of a server on a host.

WWW.WORLD WIDE WEB

World Wide Web lets us browse a large, worldwide set of services and documents using a tool called hypertext. As information is displayed certain keywords are highlighted and we can select more information on those keywords.

To access WWW.Telnet to info.cern.ch

12.9 X Window System

The X Window System was developed by Massachusetts Institute of Technology (MIT). Is a method of controlling an advance graphical windows interface. From the perspective of TCP/IP, the X window system is a message protocol between as X server and X client as shown in Figure .

With the x window system the boundary between user interface, which is not normally defined, and communications protocol may seem to been breached, but in face it is intact. RFC 1013 only describes the protocol between server and client. The style of the display is determined by other standards, typically the OSF/Motif display standard promoted by the open software function Inc.

This protocol is explained in RFC 1013. Copyright remains with MIT, through permission is given to distribute the RFC document as long as the copyright is acknowledged. Other aspects of the X window system, although not published as RFCs, are described in standards available from the X consortium at MIT.

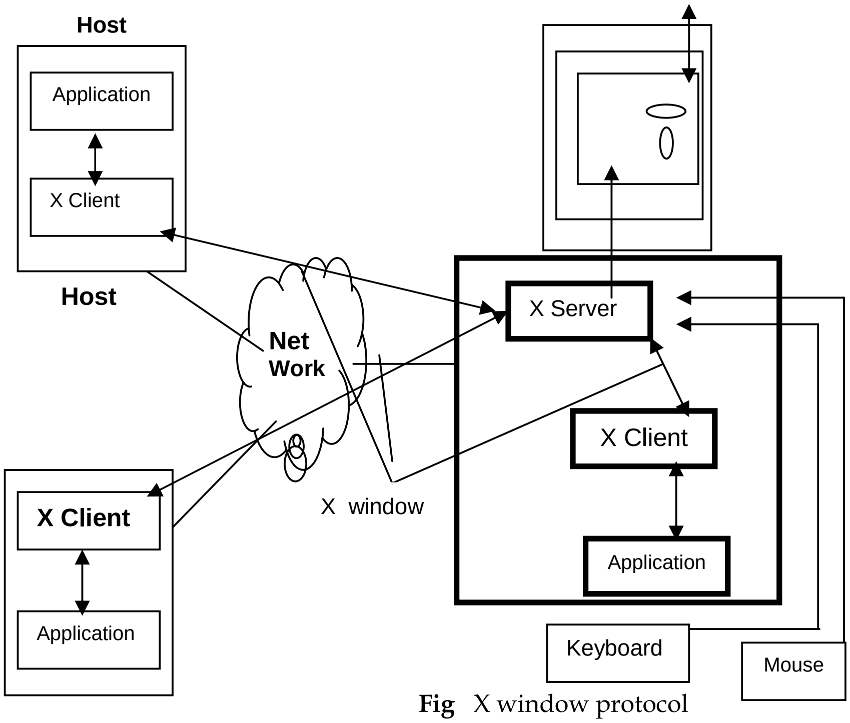


Fig X window protocol

Unlike every other reference to client and server in TCP/IP, with X window the server is normally at the user's workstation and the client, which generated the new drawing instructions, is at the application host. The X server operated the display terminal, drawing graphics objects and text in response to messages from the X client. The server must also report user actions such as keystrokes and mouse movements to any X clients that will be affected by them.

Since a window system many display output from many different applications and hosts simultaneously, each display should have a window manager, a special X client that supervises the construction of all the graphics objects on the screen as shown in Figure . It is the window manager that implements the window style, or 'look and feel' as it has been called, of the display standard (ASF/Motif, Open look or some other standard). More practically, it is the window manager that adds and controls the scroll bars, title line, move button, sizing, scaling and overlaying of windows in response to user actions. Any graphical interface with the modifications to provide the correct software interface to the X server can act as a window manager for an X window server. Microsoft windows has been adapted for this role.

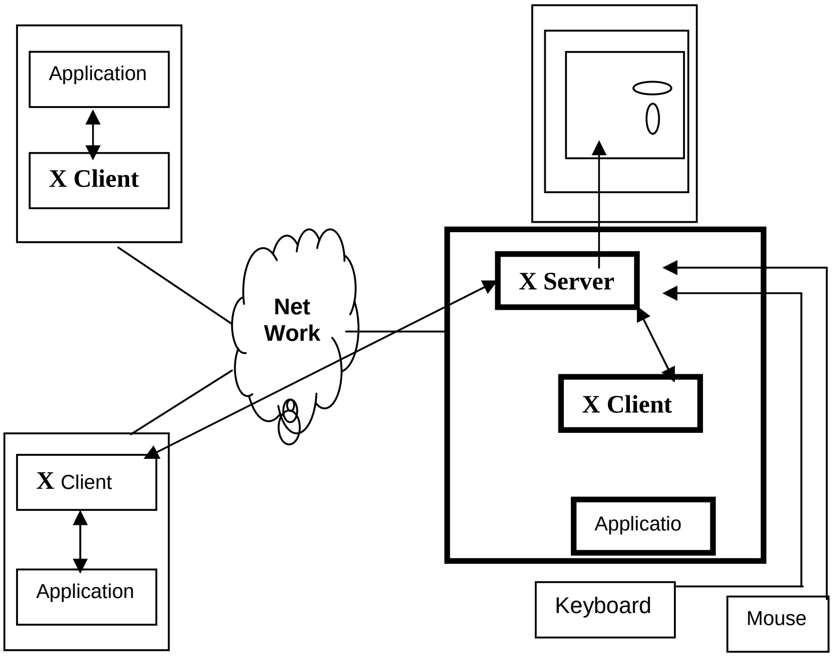


Figure The X Window Manager

12.10 The X Terminal

The X terminal is an x window display station that implements the X server, which it runs no user application (X clients) locally. All display requests are reviewed on the network connection. Extensions to the X user interface can provide for color, image support and Display PostScript among others.

Some X terminals have been adapted to operate over dial upon modem links. Since modem links are limited to 9600 bps or 144000 bps before compression, many suppliers offer some form of data compression for this type of connection. The result is s usable, if somewhat sluggish, display system provided that the dial-up link is carrying data for a single X terminal user. Where possible, higher speed lines should be used for X terminals. The increasing availability worldwide of ISDN 64 kbps dial up circuits will alleviate these restriction.

12.11 The X Window system

Graphics application, particularly when bit-mapped graphics is involved, are demanding both of processing power and of communications capacity. The communications requirements will increase if the X server and window manager are not on the same workstation. The earliest X window terminals operated with a remote, host-based window manager; the standards specifically provided for it. In this case, every user action, from a key press to a pointer (mouse) movement generates network traffic, with a large movement of the pointer potentially generating a stream of x protocol messages

The X window protocol uses TCP reliable connections between a server and its client. Each TCP data segment sent may be individually acknowledged, almost doubling the expected traffic. If the protocol is confined to a LAN segment reserved for the purpose, this traffic is uniquely to be an issue. Where X systems cross bridges or routers between LANs or more particularly cross wide area lines, the traffic generated by particularly actions should be measured for every X implementations use a local window manager, which removes a high proportion of the traffic from the network.

Tuning TCP may not improve the performance of an interactive protocol like X windows as much as a bulk transfer protocol like \FTP.

12.12 Short Summary

- TCP/IP provides reasonable network services for most applications and is extensible, well documented.

- The finger and who is are for obtaining information on user.
- Finger clients query a server, often to find someone's login name (for sending them mail) or to see if someone is currently logged in.
- The who is client normally contacts the server run by the InterNIC, looking for information on a person, institution, domain, or network number.
- The other Internet resource discovery services that we briefly described, archie, WAIS, Gopher, Veronica and WWW, help us locate files and documents across the Internet. Other resource discovery tools are currently being developed.

12.13 Brain Storm

1. How do you Implement TCP/IP?
2. Explain Finger protocol.
3. Explain Who is protocol.
4. What is meant by WAIS?
5. Write short note on X-Window system and X-Terminal.

Lecture 13

Network Security

Objectives

In this lecture you will learn the following

- Security in TCP/IP Network
- About Risk Analysis
- Passive-Active Threats
- About Security in Work Stations and Server

Coverage Plan

Lecture 13

16.1 Snap Shot

Allowing access to your hosts for only the users that you intended is the goal of security in a TCP/IP network. Once a user is logged into a system, the security within that system is all that prevents the user from accessing information that user should not be able to access. This chapter intended to deal the various levels of security in TCP/IP network.

13.2 Security in TCP/IP Network

The first level of security in a network is to make sure that all the security on the various hosts themselves in carefully policed. Unfortunately, security in UNIX hosts is based on user id and password. Thus user ids and passwords need to be very difficult to guess. The most effective method used to create truly secure systems to have user ids that are not personal names originals but computer-generated. Users will not like having user ids and passwords that are not easy to remember. But, if someone trespassed into your system that person will be able to work out user ids if it appears that some form of a person's name is being used as a user id . If you find using computer-generated user ids too difficult, you should at least force people to change their passwords regularly. Further, you should regularly use password scanning software to make sure people aren't using simple, easy to guess passwords like their name or car type.

A second level of security is to ensure that only users whom you want are even accessing your network. If your network is completely disconnected from the outside world, you only need to concentrate on the security of your individual hosts. But if you are part of the Internet community and have linked up to the outside world, you need to consider measures to isolate your network from the rest of the Internet. One method is to place a "wall" between your network and the outside networks. This mechanism is often called a firewall because a "Fire" in the outside network will not be allowed to enter attempting to access your network and exclude those addresses that are allowed. Thus, routers can be used as firewalls to filter out the network addresses that are allowed. Thus, routers can be used as firewalls to filter out the network addresses of users whom you do not want to access your system.

Another issue is security; The **rlogin** command is sometimes used in place of the **telnet** command because system administrators can set up user validation so that no password is needed for a user to log in on another host. The telnet command always requires a password to be entered. Unfortunately, this approach while convenient for users, opens a security hole on the remote system when you use it. With access to the outside world via the Internet a reality for many networks, you should not have any password less user ids . If you need to provide a guest password for a short period of time. You should create a special account for this purpose and then only assign a password when you want to provide access to that guest. By the way, user ids on most UNIX systems can be set up not to allow login on that use id at all. These user ids are normally present in the system for allowing ownership of system files.

Another issues of security involves permitting the user of anonymous file transfers. You can set up your system so that a file can be transferred between you system and another system without the user having a user id registered on your system. This is accomplished by setting up the FTP user with a special home directly for that user. Then a user can log in using the user anonymous and any password will be accepted for that user. Once logged in the anonymous user will have access to those files that are in the home directory of the anonymous user. With careful attention to the permissions on other directories, only this one directory can be made available to outside users.

13.3 LAN Security

Security for microcomputer LANs has increased in importance and more vendors are supplying LAN security systems. As end-users become more aware of the value of the vast amounts of data being accumulated and the need to protect that data, more users adopt such systems.

Newspapers carry stories almost every week about some computer network being penetrated, either for financial gain or as a prank. Most of these break-ins involve large corporate networks and wide area networks. As local area networks proliferate and tap into national and international data communication systems. These local networks will also become targets.

Companies that do sensitive work, such as those with defense contracts are often heavily involved in data security. Other companies may be aware only of the threat, but not of their own vulnerability. Most analysts agree that businesses and institutions, such as schools will have to suffer a loss through theft or vandalism before they actually establish measures to protect their data.

A computing network like any other valuable shared resources, is subject to branches of security. Such breaches can be accidental or intentional and their effects on network operations can range from harmless to irritating to devastating.

Security is a critical issue to those planning, managing or using a LAN. It is also a very complex issue. Security is a component of overall network reliability. However, reliability depends largely upon the dependability of network hardware, software and technology. In contrast, the security of a network depends almost exclusively upon the behavior of that network's authorized users, managers and their guest.

Security is best addressed as part of an overall network strategy. Security concerns must be balanced by other factors that affect the network and its users. Users and managers must therefore discover and implement methods that improve network security without infringing upon users work patterns or implying that all users are suspected violators of security.

Users have other concerns that network security methods must address as sell. User must be reassured that they can collaborate on projects and share information without being spied upon by managers or other users. Well-implemented password protection schemes can provide much of this reassurance. Managers must also demonstrate to users that procedures for tracking user work patterns on the network are used to improve security and reliability and not merely to keep a closer eye on users or their activities.

Users have other concerns that network security methods must address as well. Users must be reassured that they can collaborate on projects and share information without being spied upon by managers or other users. Well-implemented password protection schemes can provide much of this reassurance. Managers must also demonstrate to users that procedures for tracking user work patterns on the network are used to improve security and reliability and not merely to keep a closer eye on users or their activities.

Security methods must be selected with care can implemented with the full cooperation and knowledge of authorized users if security is to be assured . A first step towards these goals is a definition of network security.

LAN Security

1. Security cannot exist without a management policy.
2. LAN users should be positively identifiable before they have access to network resources.
   Prevention: passwords, passkeys authorization measures.
3. Data, hardware and software should be protected from unauthorized and /or accidental, modification, destruction, theft or disclosure.
   Prevention : locks
4. Data should be reconstruct able.
   Prevention: frequent, regular backup of files
5. Equipment must protected from fire, dirt and natural disasters.
   Prevention: smoke detector, sprinklers, air-conditioning.

13.4 What Network security Means

All the features of electromagnetic media which are desirable to a user also make this media vulnerable to theft and damage. Information stored on disk is easily copied altered and erased. As larger amount of critical data are stored in this way, the significance of the problem grows.

A stand-alone personal computers is easy to secure. You simply put your diskettes in a safe and store your computer in a locked closet. But when you attach that computer to a network of computers, security becomes more complicated. Even a "local"{ network probably will spread out through several offices, with connecting cables running in ceilings and floors and in halls and basements. A thief or vandal can tap into any one of a dozen or more spots on the network, many secluded from normal observation. But tapping into the network from some secluded spot on the cable is not usually necessary. A person can simply log-on to a convenient PC and steal or damage data at will. Unfortunately, the easier a system is to use, the easier it is to misuse.

Like any other kind of insurance, data security involves trade-off. You must weigh the cost of the potential loss against the cost of protection as well as any inconvenience the security measures may cause. The first thing to do in planning your data security program is to put a value on the data you are going to protect.

In general, a secure network is one that is resistant to disruptions caused by unauthorized network use. Such a network is designed and operated to minimize unauthorized users evade safeguards.

Network security can be defined as the protection of network resources against unauthorized disclosure, modification, utilization, restriction or destruction. Security has long been an object of concern and study for both data processing systems and communication facilities. With computer networks, these concerns are combined. And for local networks, the problems may be most acute.

Consider a full capacity local network, with direct terminal access to the network and data files and applications distributed among a variety of processors. The local net work may also provide access to and from long haul communication and be part of an internet. The complexity of the task of providing security in such an environment is clear. The subject is a broad one and encompasses physical and administrative controls as well as automated ones.

This general definition of a secure network is the foundation upon which you must build a definition that fits your work group's specific requirements and constraints. An effective definition that fits your work group's specific requirements and constraints. An effective definition requires careful assessment of needs by you, your colleagues and your managers.

13.5 Risk Analysis

Before you can realistically decide how much time and money to invest in data security, you must quantify the risk. Risk analysis has been elevated to a precise discipline. For out purposes. We should not need to examine formulas or other exact methods of quantifying every risk associated with networked data. But we can look briefly at some of the elements of risk analysis . These can help you to develop a preliminary description of your data's value and potential for loss.

First, you will want to determine two values, in rupees. For the information stored in your data system. One is the cost of re-creating the data: the other is the value of lost business if a competitor should gain access to your data.

These tow figure should be easy to obtain or at least to estimate. Many smaller companies have never considered the potential loss of their stored data. If nothing else, such an appraisal should encourage the use of data back up and the insistence on serious password security procedures.

Next, you should identify any possible threat to your data. If your data has little or no monetary value to a competitor, then there is probably little risk of theft. On the other hand, the value of your data to a competitor may be great, with the risk of theft proportionally high.

The physical volume of valuable data is another element to consider. If the volume and diversity of the data are extensive, the chance of a total loss by theft is reduced. A related calculation is the frequency of potential thefts. This figure can be difficult to predict unless you have compiled a history of losses over some period of time. Law enforcement agencies and some trade associations keep extensive records of thefts, defined by type of business, kind of penetration and value of loss. Contacting these groups may turn up sufficient data to allow you t make an intelligent prediction of rish. In addition, you should make a detailed study of any active attacks on your data so that you can estimate the cost of countering a similar attack.

Vandalism is another threat, possible more serious than theft because the frequency of vandalism is often greater. A discontented employee may decide to "get even" by destroying or altering important files. Or an act of vandalism may be done simply as a prank or game, just to see if it can be done.

After you calculate the value of your data and the types of risk, the final element in risk analysis is the data's vulnerability. Remote access is one factor that causes data to become more easily available and vulnerable. When people can access your network remotely, the potential for loss increases.

On a local basis the risk to data goes up when the network's contents are generally known. The capability to see those contents (for example, files servers and other resources) is controlled partially by the operating system and partially by the site administration.

Making a risk analysis will enable you to answer many questions about where risks are greatest and how much money and procedural inconvenience are necessary to thwart these threats. Next, you should consider steps for building a secure data network.

13.6 Types of Threats

A publication of the National Bureau of Standards identified some of the threats that have stimulated the upsurge of interest in security:

1. Organized and intentional attempts to obtain economic or market information from competitive organizations in the private sector.

2. Organized and intentional attempts to obtain economic information from government agencies.

3. Inadvertent acquisition of economic or market information.

4. Inadvertent acquisition of information about individuals.

5. International fraud through illegal access to computer data banks with emphasis, in decreasing order of importance, on acquisition of founding data economic data, law enforcement data and data about individuals

6. Government intrusion on the right of individuals.

7. Invasion of individual rights by the intelligence community.

These are examples of specific threats that an organization or an individual (or an organization on behalf of its employees) may feel the need to counter. The nature of the threat that concerns an organization will vary greatly from one set of circumstances to another. Fortunately, we can approach the problem form a different angle by looking at the generic types of threats that might be encountered.

Table 13.1 lists the types of threats that might be faced in the context of network security. The threats can be divided into the categories of passive threats and active threats (see figure 8.2).

Table 13.1 **Potential network security threats**

PASSIVE THREATS

The monitoring and / or recording of data while the data are being transmitted or a communications facility.

RELEASE OF MESSAGE CONTENTS

Attack can read the user data in messages.

TRAFFIC ANALYSILS

The attacker can read packet headers to determine the location and identity of communicating hosts . The attacker can also observe the length and frequency of messages.

ACTIVE THREATS

The unauthorized use of a device attached to a communication facility to alter transmitting data or control signals or to generate spurious data or control signals.

MESSAGE STREAM MODIFICATION

The attacker can selectively modify, delete, delay, recorder and duplicate real messages.

The attacker can also insert counterfeit messages.

DENIAL OF MESSAGE SERVICE

The attacker can destroy or delay most or all messages.

MASQUERADE

The attacker can pose as a real host or switch and communicate with another host or switch to acquire data or services.

13.7 Passive Threats

These are in the nature of eavesdropping or monitoring of the transmissions of an organization. The goal of the attacker is to obtain information that is being transmitted. Two types of threats are involved here; release of message contents and traffic analysis.

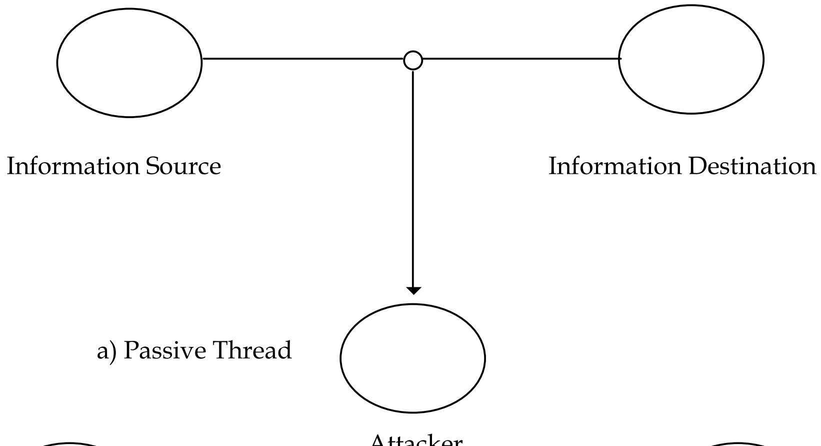
The threat of release of message contents is clearly understood by most managers. A telephone conversation, an electronic mail message or a transferred file may contain sensitive or confidential information. We would like to prevent the attacker from learning the contents of these transmission.

The second passive threat, traffic analysis is more subtitle and often less applicable. Suppose that we had a way of masking the contents of messages or other information, traffic so that an attacker, even if he or she captured message, would be unable to extract the information from the message. The common technique for doing this is encryption, discussed at length subsequently. If we had such protection in place, it might still be possible for an attacker to observe the pattern of there messages. The attacker can determine the location and identify of communicating hosts and can also be useful in guess if the nature of the communication that is taking place passive threats are very difficult to detect since they don't involve any alteration these attacks from being successful. Thus threats is on prevention and not detection.

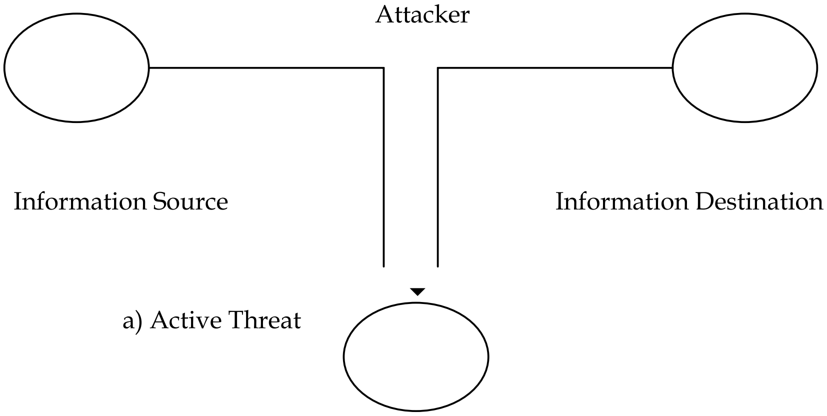
13.8 Active Threats

The second major category of threat is active threats. These involve some modification of the data stream or the creation of a false stream. We can subdivide these threats into three categories; Message – stream modification, denial of message service and masquerade.

Message – stream modification – Simply means that some portion of a legitimated message is altered, or that messages are delayed, replayed or reordered, in order to produce an unauthorized effect, for example, a message meaning "Allow J.N.Saxena to read confidential file account" is modified to mean " Allow F.G.Bansal to read confidential file accounts".



a) Passive Thread



a) Active Threat

The denial of service prevents or inhibits the normal use of management of communication facilities. This attack may have a specific target; for example, an entity may suppress all messages directed to al particular destination (e.g. the security audit service). Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

A masquerade takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other two forms of active attack. Such at attack can take place, for example, by capturing and replaying an authentication sequence.

Active threats present the opposite characteristics of passive threat. Whereas passive attacks are difficult to detect, measures are available to prevent their success. On the other hand, it is quite difficult to absolutely prevent active attacks, since this would require physical protection of all communication facilities and paths at all times. Instead, the goal with respect to active attacks is to detect these attacks and to recover from any disruption or delays caused by the attack. Because the detection has deterrent effect, this may also contribute to prevention.

13.9 Determining what secure means to you and your LAN

To arrive at a specific definition of security for your LAN, you and your colleagues must first examine your current network or network plans to identify points of vulnerability. Where points of vulnerability occur depends greatly on the work and net work use patterns of every member of your work group. An initial challenge, thus, is to determine these patterns accurately without interfering with them.

If you already have a network, your group will have to decide whether written surveys, personal interviews, software that tracks network access by user, or some other method is best for gathering this information. If you are still in the planning stages, you and your group will have to gather the same information about each independent personal computer (PC) user and use the data to hypothesis points of network vulnerability. A consultant may be helpful with this step.

Every network environment is different, with a different list of specific points of vulnerability. However, most environments have certain vulnerable points. Be sure not to overlook these areas in determining you own environment's particular potential weakness.

13.10 Securing workstations and servers

Like LANs themselves, strategies that address security begin on users desktops, with their workstations. To protect against both accidental and intentional breaches of network security, users must develop good workstation-protection habits.

One simple habit is turning o workstations when leaving for the evening or weekend, So the screens do not attract wandering eyes and hands. Keeping boot(startup) disks in a non-obvious drawer instead of on a desk or in the workstation's floppy drive also reduces the likelihood of unauthorized access via an authorized user's workstation.

Physical locks are also available for disk drive doors, keyboards and workstations or PC system units. Some of these locks impede both access and theft. LAN users in large or open-office environments should be encouraged to use these additional security measures and not to defeat them by keeping the keys in their unlocked desks.

It is important to note that in many organizations, the most serious threat to workstation security is not unauthorized users with malicious intent. A larger problem is unauthorized access to user workstations by guests or children of authorized users. These legitimate users often sit their charges in front of an absent user's workstation, to play or explore while the worker works.

This problem is most acute during off hours, when network supervision is minimal or absent. Some companies report a similar problem with after-hours office cleaning staff bringing in and playing unauthorized games on PCs connected to a network. Practices like these must be detected and discouraged to prevent serious network problems caused by well intended but untrained people.

Servers represent another point of potential vulnerability, especially if they are non-decided and also used as workstations. A single user problem on a combined workstation-server can become a network-wide problem. In addition, even a dedicated server can be mistaken for a workstation if it has a keyboard, floppy disk drive and a screen attached.

The more critical your network is to your business the more seriously you and your colleagues must work to secure your servers. Removal of the keyboard from each CP-based server is a good first step. You may also want to put warning signs on servers or to secure them behind locked doors, depending upon their configuration and susceptibility to unauthorized access.

13.11 Securing Network Password

Another point of vulnerability under direct user supervision is the passwords that allow access to the network itself, as well as to specific resources, such as particular servers, programs or files, users remember their passwords better when they choose their own, so assignment or random passwords is to be avoided in most situations. However, users must be encouraged to use a bit of creativity when selecting their passwords to make them difficult for unauthorized users to guess or discover accidentally.

You and your colleagues should choose as passwords random numbers or word combination that are not obvious, but have enough personal significance to be remembered easily. Such a password is less likely top be guessed or discovered and is amore effective security measure than a password based on your telephone number, your birthday or a loved one's name.

You and your colleagues must also implement routines for changing your passwords regularly. Some network managers automatically invalidate any passwords more than 30 days old, forcing users to select new ones at least once a month. Your network security and reliability could be enhanced simultaneously if you and your colleagues changed your personal passwords each time you made complete back u copies of your network files.

Needless to say, some users write down their passwords or store them in some electronic note file. If these users leave the notes where others can find them, all the security you and your colleagues are trying to implement can be rendered useless. Encourage your co - workers to treat their network passwords like credit card numbers or access codes for automated teller machines and to protect them with at least as much vigilance.

13.12 Securing Files and Programs

Users can also help protect against unauthorized access to network files and programs. Keep master and boot copies of programs on write protected disks and, if possible, use passwords to protect your work group's network or application software. When copies of important files are stored on easily removable media such as floppy disks or tape cartridges, restrict access to these media by using locks and keys, sign-in and sign-out lists, supervisor monitoring or other measures. These practices reduce the possibility of accidental or malicious erasure or modification of important files.

File must also be protected while they are in use on a network. Users must strive always to open and close files according to the procedures required by their network and application software. Otherwise, network file directories can become incorrect or corrupted, and larger problems can result. Most network software offers some protection against these problems, but good user habits are the best safe guards.

Some network programmes require the insertion of key disks into workstation floppy drives to qualify legitimate users for access to programmes and files. Where these disk are in use, they must be protected and not widely distributed or duplicated. The use of third-party programmes that eliminate the need for key disks must also be weighed against the increased security risk that these disks can represent.

Networks must also be protected from unauthorized programmes, such as game programmes or other personal software. Unauthorized programmes can contaminate your network with annoying or highly destructive software viruses.

You and your colleagues should avoid bringing unauthorized software into contract with your network, Whether a harmless game or out own copy of a program your work group uses, any software not supplied through your network's usual channels should be viewed as a potential source of harm to your network.

13.13 Short Summary

- Companies that do sensitive work, such as those with defense contracts are often heavily involved in data security.

- Network security can be defined as the protection of network resources against unauthorized disclosure, modification, utilization, restriction or destruction.

- PASSIVE THREATS-The monitoring and / or recording of data while the data are being transmitted or a communications facility.

- ACTIVE THREATS- The unauthorized use of a device attached to a communication facility to alter transmitting data or control signals or to generate spurious data or control signals.

13.14 Brain Storm

1. What is meant by Security?
2. Explain the term Risk Analysis.
3. What are the two Types of Threats? Explain.
4. How do you maintain the Security in Workstation and server?
5. How do you secure your files and programs?

Lecture 14

Level of Security

Objectives

In this lecture you will learn the following

- Knowing about the Various level of Securities
- Knowing About Physical Security
- Knowing about the Online Coders
- Protection against Cable Radiation

Coverage Plan

Lecture 14

14.1 Snap Shot

14.2 Levels of Security

14.3 Physical Security

14.4 Access Controls

14.5 Personal Identification

14.6 Passwords

14.7 Security in Log-in

14.8 Encryption

14.9 Online Coders

14.10 The Diskless PC

14.11 Protection Against Cable Radiation

14.12 Call-Back Security

14.13 Management level Concerns

14.14 Short Summary

14.15 Brain Storm

14.1 Snap Shot

This lecture deals about the remaining levels of Security such as online coders, Call back Security, and about the Management level concerns. There is no such thing as 100% security. With enough skill and thought time to complete the job, a perpetrator can defeat any security measure. This lecture introduce you in to the various levels of security involved in E-Commerce.

14.2 Levels of Security

Of the two security elements of skill and time, the most dependable protection is time. If you can make certain that a break-in will be a time consuming project for a thief, you have gone a long way in protecting your data. Therefore, all system are layered with not one but several security measures (see fig 14.1) for local area network the following strategies should be considered:

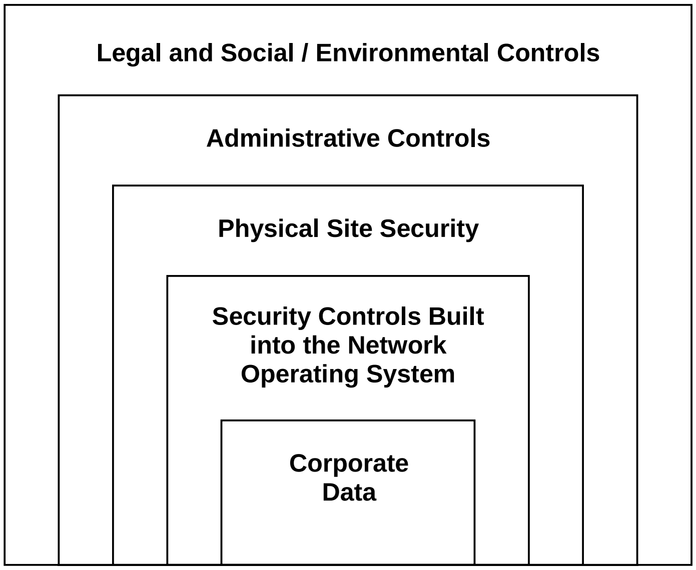

Legal and Social / Environmental Controls
Administrative Controls
Physical Site Security
Security Controls Built into the Network Operating System
Corporate Data

Figure 14.1 Layers of data security

1. Physical security
2. Access control
3. Personal ildentification
4. Encyrption
5. The diskless PC
6. Protection against cable radiation
7. Call-back security.

14.3 Physical Security

Data security can take many forms. The simplest is physical security, which may be a lock on the computer or a guard at the door. With physical security, a would-be thief must attack and defeat your security measures before becoming a threat to the data.

Locks can set up barriers from the back door to the office door to the computer it self. Key locks are now provided for IBM PC/Ats and compatible. The lock interrupts the power to the display and keyboard, while still allowing the terminal to remain on-in. This kind of physical security is available for personal computers.

An alarm system works in partnership with your physical security measures. Locking devices are designed to increase the time needed for penetration. Alarms put an effective limit on the amount of time available. Professional criminals do not run when they hear an alarm or when they think they have tripped a silent alarm. Most know precisely how much time they have before the police arrive. If they cannot get through the security system's physical barriers in the time available, then the criminals will abandon the effort.

14.4 Access Controls

The purpose of access controls is to ensure that only authorized users have access to the system and its individual resources and that access to and modification of particular potions of data is limited to authorized individual and programmes.

Figure depicts, generically, the measures taken to control access in a data processing system. They fall into two categories; first those associated with the user or group of users and, second, those associated with the data. In what follows, we elaborate on these concepts and extend them to the local networking environment.

The control of access by user is referred to an authentication. A quite common example of this one a time-sharing system is the user log-on, which requires both a user ID and a password. The system will only allows a user to login if that user's IN is known to the system and if the user knows the password associated by the system with the ID. This ID/Password system is a notoriously unreliable method of access control. Users can forget their passwords and accidentally or intentionally reveal their password. Also, the ID password file is subject to penetration attempts.

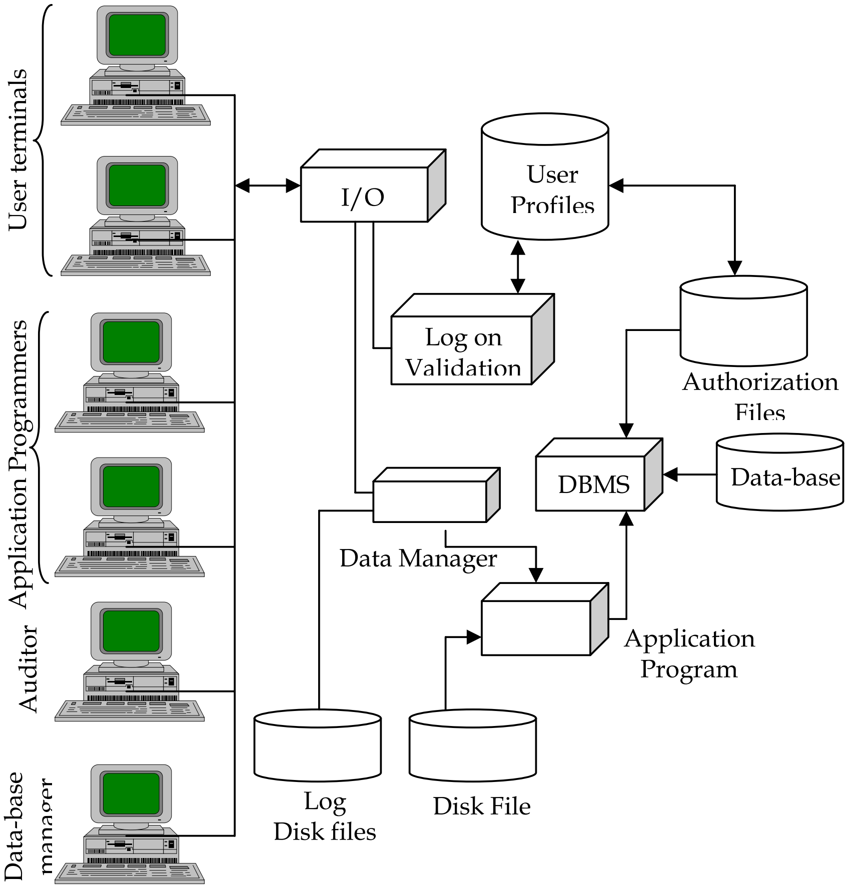


Figure Data Processing system security

No cost-effective method of overcoming this problem exists. Exotic techniques such as voice print, fingerprints and hand geometry analysis may be foolproof but are at present prohibitively expensive. Simple measures that can be taken now are to change passwords frequently and to maintain tight multiple measures of security over the ID/password directory. One additional measure that is cost effective is to associate ID's with terminals rather than users and hard wire the code into the terminal. This changes an administrative/software security problem into a physical security problem. However, if it is desirable to allow one-to-many and /or many to one relationships between users and terminals, this technique is in effective.

The problem of authentication's compounded over a multi-access medium LAN. The log-on dialogue must take place over the communication medium and eavesdropping is a potential threat. One approach to protection would be to certify that each NIU can capture only data addressed to it. This is no easy task. Another approach is to encrypt the ID/password data. User and user group authentication can be either centralized or distributed. In a centralized approach the network provides a login service. Distributed authentication treats the network as a transparent communication link and the usual login procedure is carried out by the destination host. Of course, the security concerns for multi access media must still be addressed.

In fact, in many local networks, two levels of authentication will probably be used., Individual host may provided with login facility to protect host-specific resources and application. In addition, the network as a whole may have protection to restrict network access to authorized user. This two-level facility is desirable currently for the common case, in which the local network connects disparate hosts and simply provides a convenient means of terminal-host access. Future integrated networks (in the OSI sense) may require only network-level scheme.

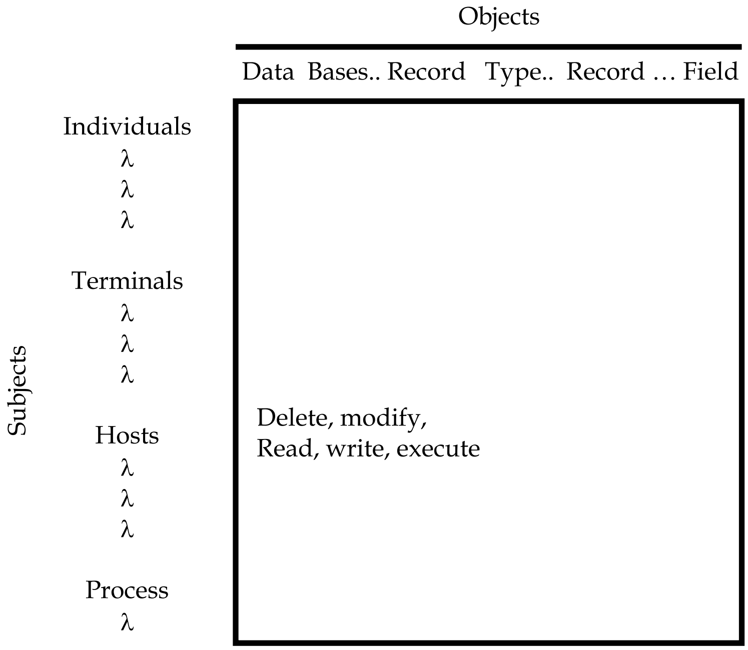
Following successful authentication, the user has been granted access to one or a set of hosts and/or processes. This is generally not sufficient for a system that includes sensitive data in its data base. Through the authentication procedure, a user can be identified together with a profile that specifies permissible operations and file accesses. The operating system can enforce rules based on the user profile. The database management system, however, must control access to specific proteins of records. For example, it may be permissible for any one in administration to obtain a list of company personnel, but only selected individuals may have access to salary information. The issue is more than just one of level of detail. Whereas the operating system may grant a user permission to access a file or use an application, following which there are each individual access attempt. That decision will depend not only on the user's identity but also on the specific parts of the record being accessed and even on the information already divulged to the user.

A general model of access control as exercised by a data base management system is that of an access matrix(see table). One axis of the table consists of identified subjects that may attempt data access. Typically, this list will consist of individual users or user groups, although access could be controlled for terminals, hosts or processes instead of or in addition to users. The other axis lists the objects that may be accessed. At the greatest level of detail, objects may be individual data fields. More aggregate groupings, such as records, record types, or even the entire data base may also be objects in the matrix indicated the access rights of that subject for that object.

In practice, an access matrix is usually sparse and is implemented by decomposition in one of the two ways. The matrix may be decomposed by columns, yielding access control lists. Thus for each object, an access control list lists users and their permitted access opportunities. Decomposition by rows yield capability tickets. A capability ticket specifies authorized objects and operations for a user. Each user has a number of tickets and may be authorized to loan or give them to others. Because tickets may be dispersed around the system, they present a greater security management problem than access control lists.

Network considerations for access control parallel those for authentication. Encryption may be needed to provide secure communications on a LAN. Typically, access control is decentralized, that is controlled by host-based data management systems. However, if a network data base server exists on a LAN, access control becomes a network service.

Table : Data base access matrix



14.5 Personal Identification

A local area network presents some additional security problems because of its dispersed nature and because many people have access to the network. Remote access through modems and telephone lines is used widely on LANs which makes dispersion essentially infinite. Dispersion thwarts one of the best types of personal identifications security systems.

On most networks the first line of security is personal identification. You physically recognize people who are authorized to be in your office, sitting at a PC. With remote access this kind of identification is impossible. Companies must rely on passwords and classified access schemes to protect their data.

Several techniques can be used to restrict access to authorized users. All these techniques are based on some kind of identification: personal, such as ID badge; key word such as a log-in name and pass word; or key number.

Badges and personal recognition may not be successful in large companies where everyone is not personally known. In a company with many employees, a counter felt badge may, infact, be all that is necessary to penetrate a security system based widely on identification.

14.6 Passwords

Password security adds no cost to the network and is potentially a useful security measure. After logging onto the network, the user must type a password. Theoretically, if users must give a password, unauthorized access is prevented. But often the password system is misused and ineffective.

Passwords usually are chosen because they are easily remembered. This, however, also makes them easily guessed. Common assignments include first name for log in name and last name or title for password. The value of passwords I further diluted when employees give their passwords to others in the organization. A password often is given out because another employee needs to read a particular file or to perform some task for an absent employee.

Password protection can be improved through both systematized procedures and more sophisticated operating system password utilities. Passwords should be assigned by a network manager, not by a network manager, not the individual. This assignment method reduces the likelihood that someone will identify the password in half a dozen guesses. Many network operating systems have a password utility that allows authorized users to change their own passwords. Such a utility should be deleted from all users directories and given only to the network supervisor.

Overtime, passwords will become generally known, particularly within a small office or department. This decaying security can be stopped by periodically issuing new passwords, say, on a monthly basis. One additional advantage of changing passwords regularly is that employees will take more seriously both the password system and the subject of security.

14.7 Security in log-in

The network operating system should be designed to thwart attempts to break into the system. For one thing, the password Should not be "echoed" back to the screen when the user types it during log-in. The number of times that a password can be attempted should be limited to no more than three tries. After that, the log-in name should be invalidated temporarily and the network supervisor notified of a failed log-in. An audit tail can also be provided to record the number of password attempts from a given user to station. The presence of the audit trail utility that monitors the password system is a deterrent in itself, especially to malicious or casual vandals.

A sophisticated thief, however, can collect log-in routines and password as they are entered often simply by tapping into the network. The network operating system cab be enhanced to make this activity more difficult for the thief. Passwords cab be encrypted at the workstation and decrypted at the central processor so that the data on the cable is unusable through a tap.

As part of security planning and implementation, an independent analyst should evaluate the security measures, even to the extent of attempting to steal or corrupt a prearranged target file.

14.8 Encryption

You already learnt about Encryption technology and how it is used to secure data in Lecture 9.

14.9 Online Coders

The easiest measure to take for LAN security is to attach an encryption device at either end of a communication link. Several companies make such devices and will modify them for specific applications. After the devices are installed, the message sent between parties will be encrypted while it on the line.

Another way to set up a system is to place an encryption box between each PC and the network. Then all the data that goes out on the network and all data stored on the hard disk will be encrypted. Ideally, the device can be modified and turned to provide the speed and security needed. If necessary, a public key system can also be built in.

To show how such a security system might work, let us suppose that we have three groups on a network; administration, accounting and sales. All the data on the network can be encrypted. The administrator can read everything, but accounting and sale can read only their respective files. Each user encrypts the data on an optional basis. With each transmission the encryption device will ask the user whether to transmit in the clear or with encryption. The administrator's device will also ask the administrator. "which key do you want admin, accounting or sales?".

14.10 The Diskless PC

The power of the PC itself is a potential security threat that should be considered. One of the advantages that the personal computer has over dumb terminals is its local storage capability. Information can be locally manipulated and stored on a PC's floppy diskettes, them transferred to the central storage. From central storage the information can be made available to other users and maintained and backed up properly.

With local storage devices, users can maintain their own back-up systems, independent of the central system. The degree of autonomy associated with a persona set of data diskettes is appealing to many users. At the same time, such autonomy creates two threats to data security.

One threat is unintentional. Because two copies of data exist, one on the central disk and only locally, the copies may be updated independently. Eventually, unique data on one version may be lost when the two "copies" are merged.

The other threat is that local disk drive permits data theft. A person with access to the network and with a local disk drive can copy large amounts of data onto floppy disks in just minutes. The data, them, can be easily hidden and removed from even reasonably secure buildings.

Most network vendors now provide the capability of booting a local PC workstation from a central server so that diskless PCs can be used on the network. Since machine require full-time networking and permit no local storage, a common reason for using diskless pcs is cost . Because diskless pcs require no local floppy controller or disk drive, the cost of workstation is reduced. But equally important is the increased security offered by a diskless PC.

Take away the disk drive and you take away the means for stealing the data. But you also reduce the power of the PC in many instances local storage is desirable so that the PC can be used as a stand alone workstation in the event of a network failure. One answer is to exchange a local floppy for a local hard disk. Then not only would the user have all the benefits of local storage, but local speed and efficiency would improve also. No ready way, however, would be available to copy or remove data.

Diskless PCs have been hampered by software problems. Many application programmes are designed to run only from a local floppy disk drive. Diagnostics and the operating system itself have usually required at least one local drive.

Increasingly, however, software vendors are providing some mechanism for their application packages to be stored on a hard disk and used in a multi user environment. A company can then make its own decisions about how to configure PCs. Probably the answer will be a variety of configurations to fit particular circumstance.

14.11 Protection Against Cable Radiation

Any time information is transmitted, even through cable, that information can potentially be intercepted by unauthorized persons. The possibility also exists that a vandal can tamper with data or destroy data files.

Several methods may be used for protecting data while it is on the cable. The first thing to do is to put the cable out of sight. This step should be taken anyway, to prevent damage to the cable and to meet building codes. Security is a secondary benefit, Install cables in protective raceways in areas where penetration is less likely.

A radio-signal that is broadcast onto the air waves can easily be intercepted and the information stolen. Such emissions, however, are not limited to broadcasted radio signals. A data cable also radiated intelligible signals, just as a transmitting antenna does. Simple intercept equipment located near the cable can pick up and record these transmissions. More sophisticated devices can intercept the signals a considerable distance from the cable.

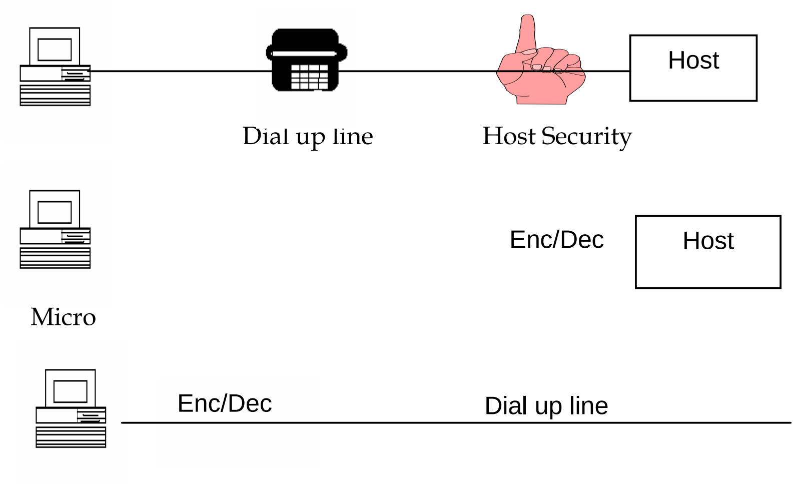
The likelihood of signal interception can be eliminated by using a shielded cable, which is a cylinder of braided copper wire that encases the intelligence-carrying wires. If one shield does not reduce emissions to satisfactory levels, more shields can be added. Frequently, cable with the necessary electrical characteristics is available in only one version. If additional shielding is needed, special shielding conduct is available that meets security standards.

Another way to eliminate the cable radiation problem entirely is by using fiber-optic cable. Fiber optic technology uses a glass fiber to carry a beam of light. Information is passed when the light is modulated. With fiber optics no signal is emitted outside the cable; therefore, data cannot be intercepted. Because fiber-optic cable is also extremely difficult to tap into physically, it is ideal for security purposes.

14.12 Call Back Security

Remote access to networks is a significant threat to data security. Remote workstations are part of many LAN environments, enabling a user to access networks remotely, log into the network, and use the system as if the user were local, securing this type of call-back security and user management are part of dial up systems and can used with remote PC-to-network traffic (see fig) with call back security, when you want to access a computer, you can call into a different number instead of calling in directly. You indicate that you want to access the network and the security device arranges for a call back to your location. In other words, the system has embedded within battery-supported memory a complete listing for every allowed user. Included in this file is a ID number that you must punch in when you want to access the file, a telephone number at which you can be reached and the hosts systems to which you are allowed access.

When a computer system can be accessed through telephone lines, security measures must be taken to protest against unauthorized access. Two ways to protect the system are call-back mechanisms and data Encryption



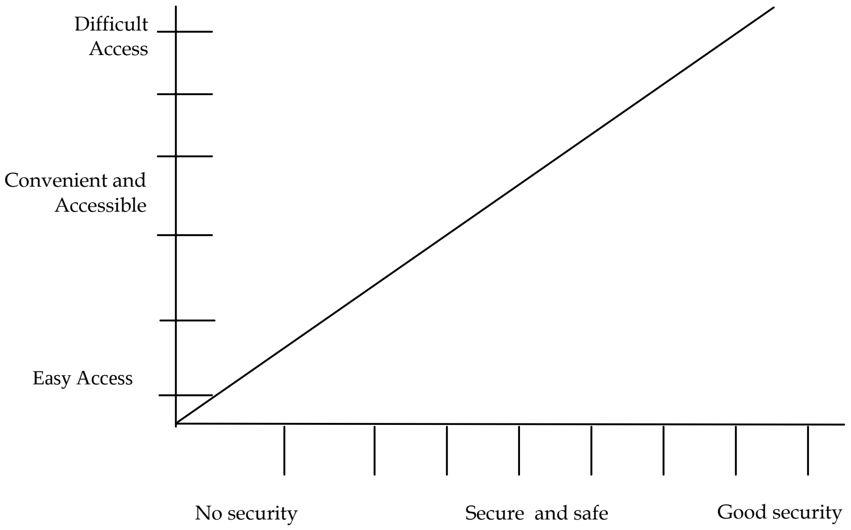
This security device also keeps track of user priorities. If all available lines are busy, the device sets up a queue based on the priority of the user. The device will inform the caller regarding queue position. When a line becomes available, the device contact the user. Therefore, the user never has to get busy signals. The device also keeps accounting information for traffic statistics and call-backs..

14.13 Management level concerns

Management have a sensitive role in network security (see figure).They must help users implement and execute measures like those discussed here and integrate these into network-wide policies that are followed rigorously. These policies also must go beyond the measures that users can implement, but without interfering with users work..

Managers of sensitive LANs need to address the possibility of their LANs being tapped like telephone lines. With relatively simple electrical devices and a little time, an interloper can tap a LAN cable with little or no immediate evidence. Some LANs can even be tapped from a distance, with devices that monitor the radio frequency emissions that almost all LANs produce. LANs that permit dial-up connections are particularly susceptive to such taps. LANs based on fiber optic cable are the most tap resistant.

Good Security usually reduces case of access to the computer. Managers must weigh the trade offs between convenience and security when implementing a specific system



Call back modems are a security measure used by many managers of dial-up LAN connections. These modems and their software accept user's calls and then instruct user to enter identifying information and to hang up. The modem then checks the user's access information and calls the user back only after the information is verified, Users who enter information that the system cannot verify are refused to access network.

Managers must also monitor connections between their LANs and other networks and computer. Managers must periodically audit access to and from network bridges, routers and other links and they must regularly update the passwords and other security measures allocated with these links. Managers may also have to help users implement more complex personal security measures as their LANs gain access to other networks and systems and security risks increase.

Managers must also implement measures that provide as much information as possible about network security and about attempted and successful breaches. Ideally, some combination of hardware, software, and physical procedures should be used to provide a near-constant audit of network access and use. This audit will not only help trace the paths of any breaches, but will aid in recovery from any problems these breaches may cause.

Software and procedures that increase accountability can be of great value to a LAN manager and to that manager's organization. Sufficient information about accountability can limit the liability of an individual, a work group or an organization, should an accidental or malicious breach of network security result in a loss of tangible assets or in a law suit for some other reason.

LAN managers are also ultimately responsible for maintaining a constant balance between security measures that are effective and security measures that interfere with users work pattern or make users feel that their every move is being monitored. The best way to maintain this balance is to involve users actively and positively is the implementation of any security measures.

Users should also be encouraged to see enhanced security as a way of protecting their own livelihoods and work environments, as well ad the assets of their enterprise. The LAN manager has primary responsibility for getting both network users and financial decision makers to see network security as s strategic benefit as well as a basic necessity.

In many cases, the best way to enhance network security is to include security bolstering procedures and tools alongside aids to other aspects of network operation and management. There are LAN software products which enhances security gracefully. These LAN packages are designed to be invisible to LAN users and can be used to control access to programme and files, to audit network software for changes, to protect networks against viruses and to facilitate rapid recovery from disk drive and server failures.

Every expert in home automobile or business security is quick to point out that there in no lock that cannot be picked, given sufficient time an inclination. The incentive behind sophisticated looks and policies that encourage and enforce their use , is there fore to make a given facility as difficult and daunting as possible to a potential thief.

Sound network security schemes must accomplish similar goals; They must deter potentially malicious users. In addition, they must encourage users to "lock" their LANs like they lock their cars and buildings. LAN security strategies must also protect networks from non-malicious accidental incursions, especially by those inexperienced with LANs.

Technology alone is inadequate to ensure security. True network security is a human issue, with responsibility divided between users and managers, just as network processing is increasingly divided between clients and servers. If viewed as a type of client-server risk management, security naturally becomes part of a larger network strategy to ensure total network reliability and to encourage users to participate actively in the protection of their vital network assets.

Network security manager must carefully and thoughtfully plane firewalls. In most cases, a network administrator will define the firewall requirements. As an Internet programmer you may implement the administrator's requirements as a custom security program. As you develop Internet based programs, you should keep network security in mind. In most cases, the network administrator will not raise security concerns until after the network has experienced a serious security breach.

14.14 Short Summary

- With physical security, a would-be thief must attack and defeat your security measures before becoming a threat to the data.
- The purpose of access controls is to ensure that only authorized users have access to the system and its individual resources and that access to and modification of particular potions of data is limited to authorized individual and programmes.
- On most networks the first line of security is personal identification.
- Password security adds no cost to the network and is potentially a useful security measure.
- The easiest measure to take for LAN security is to attach an encryption device at either end of a communication link.
- One of the advantages that the personal computer has over dumb terminals is its local storage capability.
- Every expert in home automobile or business security is quick to point out that there in no lock that cannot be picked, given sufficient time an inclination.

14.15 Brain Storm

1. What are various levels of securities ?
2. What is Physical security?
3. How the Personal Identification is Used in Security?
4. What is meant by Online Coders?
5. How do you maintain Security in PC?
6. Write about Call Back Security.

Lecture 15

Introduction to Electronic Data Interchange

Objectives

In this lecture you will learn the following

- What is EDI?
- What is the use of EDI?
- How the EDI Works?

Coverage Plan

Lecture 15

15.1 Snap Shot

In any E-Commerce systems implementation, integration between business processes within a company and across companies is very important for a successful implementation. Within a company integration needs include interfacing with legacy systems, communicating with third party products, and integrating business processes across distributed E-Commerce systems. The two most commonly deployed technologies for this type of integration are ALE (Application Link and Enabling) and EDI (Electronic Data Interchange) technologies, which make use of the popular IDoc (International Document) interface for exchanging data.

EDI provides business process integration across companies by exchanging business documents such as purchase orders, invoices, and shipment notices in electronic form, using industry standard formats such as ANSI X.12 (American National Standards Institute) and EDIFACT (Electronic Data Interchanging For Administration, Commerce and Transport).

ALE, Which is SAP's proprietary technology for integrating distributed business processes within a company, has been available in SAP since release 3.0 ALE was designed to link one SAP system to another SAP system, but the ALE architecture lent itself to being used in linking SAP systems to non-SAP systems without any modification. The flexibility of ALE technology has proliferated into several application areas, and today most third-party products use it to exchange data with SAP. ALE technology is also the basis for SAP's Business Framework architecture ,introduced in release 4.0.

The underlying architecture of the ALE and EDI technologies are quite similar. Both make use of SAP's proprietary Idoc interface, which defines the format and structure of the data that is exchanged between two systems. Although ALE and EDI are the two biggest users of the Idoc interface, this interface can also be used by any two applications that need to exchange data. For example , it can be readily used to integrate SAP with Web applications.

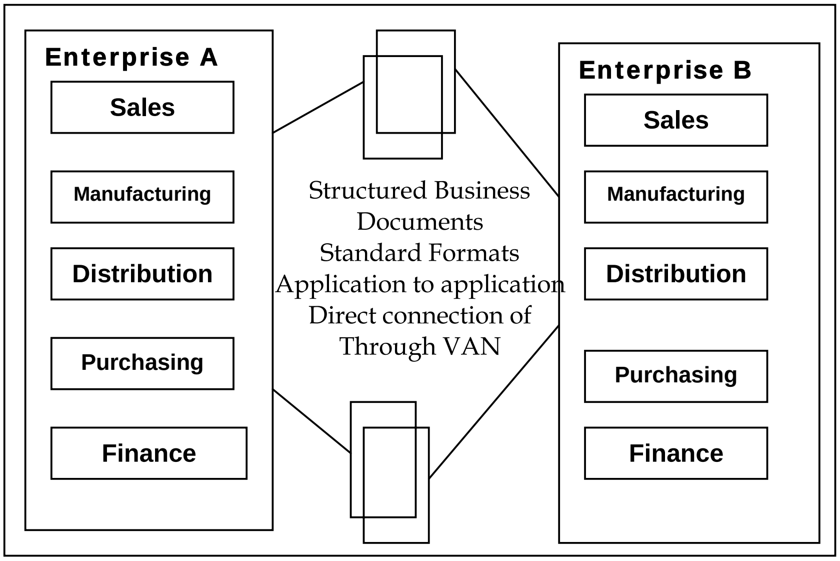
As cross-application technologies, ALE and EDI are used in various modules of SAP such as SD(Sales and Distribution) , MM (Material Management), and FI (Financials). The wide-ranging application of these technologies has created and ever-increasing need for ALE, EDI, and Idoc skills. Mastery of these skills is a necessity for anyone involved in the technical or functional side of an SAP implementation.

15.2 Electronic Data Interchange (EDI)

Traditionally, the transfer of data from one company to another has been by paper documents. This is known as a paper-based system. These documents have to be manually forwarded and entered to the destination computer.

EDI is the electronic exchange of structured business information, in standard formats, between computers. EDI eliminates the need for a paper-based system by providing an electronic link between companies. This reduces data entry tasks and improves business cycle times.

EDI is the electronic transfer of structured business documents in an organization -- internally among groups of departments or externally with its suppliers, customers and subsidiaries (See Fig). The documents likely to be used in EDI are invoices, purchase orders, shipping requests, acknowledgements and payments. EDI is quite different from generic correspondence like e-mail and involves the exchange of specific documents with management and tracking procedures designed to efficiency.



Electronic Data Interchange

In EDI information is passed electronically from one computer to another over a network without having to be read, retyped or printed. The information transferred must have a defined structure agreed between your company, and the company or group you send and receive data from.

Any company or group which uses EDI is called a trading partner. The computers that different trading partners use do not have to be from the same manufacturer.

The information that EDI handles includes, for example, purchasing orders, invoices. However, any type of business document can be sent, providing it conforms current industry, national or international format standards.

Examples of current uses of EDI include automatic teller machines (ATMs) in banks where EDI is used for transferring and withdrawing funds between different bank accounts, airline reservation systems, stock exchange transactions and car reservation systems.

15.3 Use of EDI

The data from one computer is normally not in a form suitable to be entered directly into another computer. The data may have to be arranged differently before it can be entered into another computer or some items of data may not be needed at all. With EDI, all the data is converted into an agreed standard format before it is sent over the network. The computer that receives the data can then extract the information it requires.

Using EDI implies three things:

1. Information is transferred electronically rather than on paper. This means that there is no need to enter the data manually in the destination computer.

2. Information is transferred between trading partners who have negotiated trading agreements and have formalized their data transfer system.

3. Information that is transferred complies with agreed standards for the format of the content and the transmission control mechanisms.

15.4 The Evolution of EDI

Consider a very simple business scenario. A customer who to purchase an item creates a Purchase order and then faxes or mails it to the vendor. The vendor receives the Purchase order and manually keys in a Sale Order. The vendor's system generates a confirmation date that is sent back to the customer via fax or mail. The vendor then ships the goods are shipped, the vendor invoices the customer. The customer makes the payment by check, and the vendor deposits the check in the bank. Finally, funds are transferred from the customer's account the vendor's account.

This simple scenario requires the exchange of various documents between several business partners at different times. There are some inherent problems with this scenario, in that it:

N Is Highly inefficient and laborious
N Cannot be tracked easily
N Gives no visibility into the process
N Has a very long lead time.
N Includes redundant data entry at various points

To circumvent some of the trouble spots, the business partners started exchanging data electronically via floppy disks and other storage devices, which meant that the business partners had to adopt standard formats. An ANSI committee was formed to define the standards. Ultimately, the electronic exchange of business documents in a standard format gave birth to what is now known as EDI.

EDI is not a recent invention. It has been around for more than 30 years. The transportation industry pioneered this technology and is thus responsible for its current architecture, but most industries have realized the benefits of using EDI. Today almost any industry or organization can take advantage of EDI. The retail and automotive industries are major EDI users, and the technology is used in several other large industries, including health care, government agencies, real estate, and education. In fact, EDI can be implemented not only between organizations, but also within an organization, an area that is gaining strength these days.

15.5 Benefits of the EDI Process

Implementing EDI benefits both the sender and the receiver. It is mutual effort, and its benefits are maximized by sharing information in a timely manner. The benefit include the following;

Reduced data entry errors. EDI does not involve data entry at multiple points. In the traditional system a sender creates a purchase order on their system, prints, it and then faxes or mails it to a trading partner. The receiver then re-keys the same information on their computer. The proves is prone to data entry errors. This procedure is repeated when invoicing takes place. With EDI data goes directly from one compute to another without involving a human being.

Reduced processing cycle time. The biggest advantage is the reduced processing time of the complete cycle. As soon as orders are entered into the system they can be processed on the receiving side in seconds. There is a considerable saving in the processing time of document transfer.

Availability of data in electronic form. Data from EDI is in electronic form, which makes it easy to share across the organization. For example a purchasing department can user the date to evaluate vendors, or a marketing department can use it to analyze the trends and demands of customers.

Reduced paperwork. The entire EDI process can be handled without using a single piece of paper. Some companies believe that they must have appropriate paperwork for audits and legal issues. In its paperwork reduction act, the IRS recognize the electronic form as a valid legal documents as log as the vendor or supplier can prove the origin and show complete trails on how data was generated. A company needs to have controlled processes to handle data flowing in and out. This ruling has created some tough auditing requirements but meeting them is worth the effort.

Reduced cost. Time is money. Any savings in time are directly linked to savings in money. The initial cost of an EDI setup is certainly higher as compared to the paper process, but over a long period it is very cost effective. In the long term, the overall cost of exchanging business documents in paper form can cost anywhere from $10-$15 per transaction. If the processes has to be repeated for some reason, for example if an invoice is lost, it can cost around $45. On the flip side, the average cost of an EDI transaction is close to $2.

Reduced inventories and better planning

Companies do not have to keep a safety stock for the time taken with order processing. Changes to planning schedules can be communicated instantaneously. MRP (Material

Requirement and Planning) can take into account a shipment in transit as soon as an Advance ship notice (EDI 856) transaction is received.

Standard means of communication

Because EDI enforce standards on the contents of data, uniform naming standards and field sizes have emerged. Such consistency leads to clearer communication and less ambiguity.

Better business processes

Compared to traditional methods of exchanging business documents, EDI is certainly a better way of communicating with your trading partners. Companies are willing to share information and participate in inter-organizational issues. This environment enhances supply-chain management.

Competitive advantage

In many cases, companies that have implemented EDI have an advantage over their competitors, especially when dealing with government agencies or large corporations. For example, potential vendors must use EDI to bid for certain government contacts. The procurement divisions in government agencies publish their RFPs (Request for Proposal) on the EDI network. In addition, large retailers and corporations discourage doing business with a business partner if the partner cannot send EDI transactions. The same holds true for the automotive industry. To be a certified auto-industry vendor, an organization must be able to communicate electronically. Trying to clear goods through customs is truly a nightmare if the necessary documentation is not in EDI format and has not been sent in advance.

15.6 How EDI Works ?

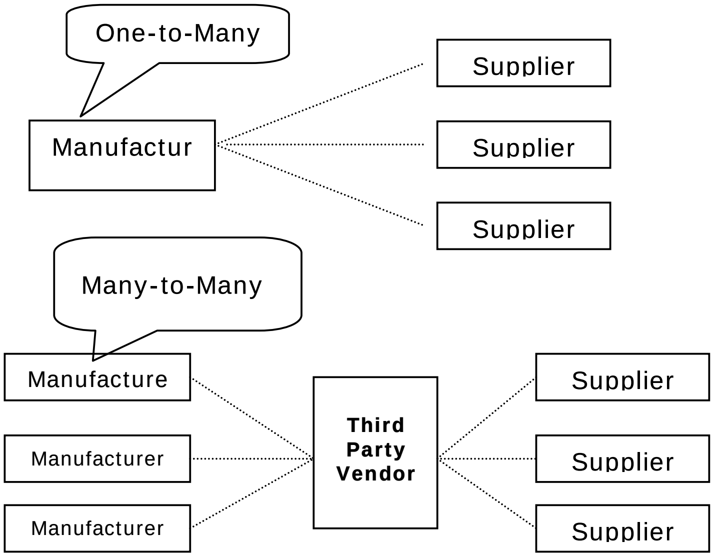
Regardless of the format chosen, companies using EDI communicate with their trading partners in one of two ways: Either they exchange data with several trading partners directly or they interact with multiple companies through a central information clearing-house (See Fig). In the latter case, all transactions are funneled through a third party’s computer system, which routes them to the appropriate receiver’s computer. This enables the sender to communicate with an unlimited number of trading partners without worrying about proprietary systems, audit trails, variable transmission speeds, and general computer compatibility.

Basically, here is how EDI works:

1. Prior to any computer work, representatives of two companies interested in exchanging data electronically meet to specify the applications in the EDI standard which they will implement.
2. Each company adds EDI programs to its computer to translate company data into standard formats for transmission, and for the reverse translation on the data it receives.

3. Then, as often as operationally required the two companies exchange data electronically in the standard formats.

Typical EDI Configuration

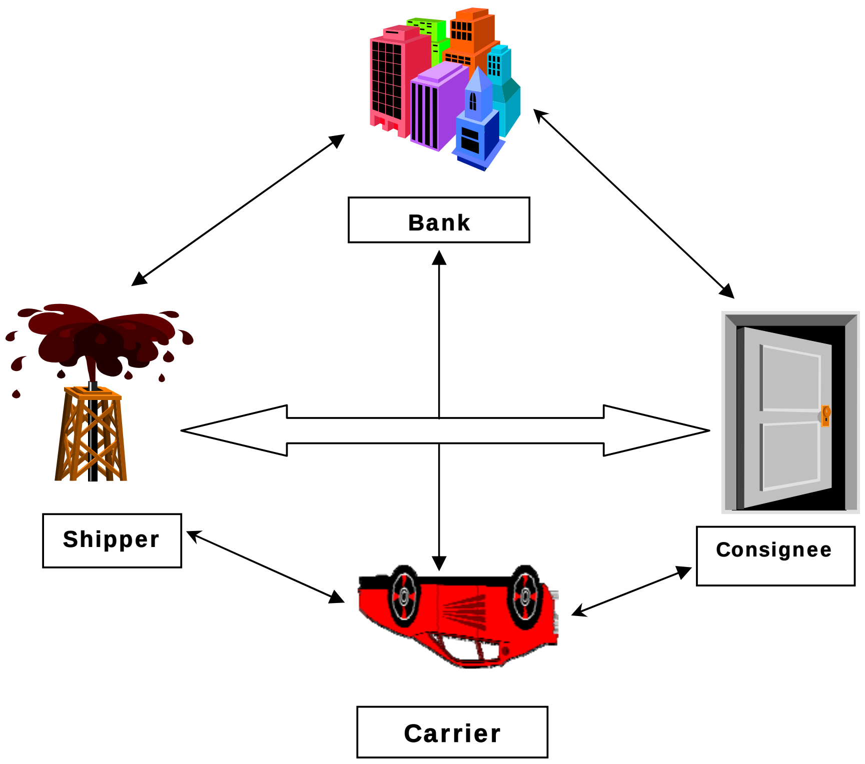


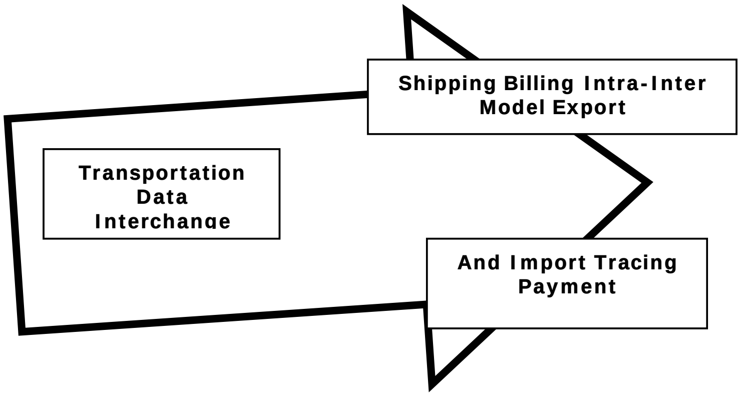
Typical EDI configurations may involve either direct communication with others (often using a proprietary system) or the use of a third-party vendor to translate and communicate messages to customers

The data transmitted originates from records in the sender's data base after the sender confirms that the receiver is an authorized recipient for such data. The sender composes a transmission formatted in the EDI standards: the 0receiver translates the formatted message to a computer record to be processed and used internally. All transmissions are checked both electronically and functionally and the protocol includes procedures for error detection and correction.

Once a company has established standardized communications with another company, it is now in a position to communicate with any other company that is also using the EDI standards.

The following figure pictures EDI in its working environment. Notice that the environment may include banks and customs as well as companies and carriers, and the environment may include banks and customs as well as companies and carriers, and the environment may be broadened as needs develop. The information flow in EDI is:




Shipping Billing Intra-Inter Model Export
Transportation Data Interchange
And Import Tracing Payment

1. A company collects data for its own operational or statistical requirements. This data is edited and added to its own data base.

2. Pertinent information is extract by the company from its data base, summarized if necessary, constructed into EDI transaction sets, and transmitted to the company or organization requiring it for valid reasons.

3. The frequency for preparing this information is determined by the operational requirements of each recipient.

4. A communications link for transmission is established according to the standard communications protocol.

5. The recipient of the information receives the transmission and checks it for its physical characteristics (parity, check character, transmission mode). Retransmission is requested if an error is detected in the physical characteristics of the transmission.

6. The receiver checks the functional characteristics of the data. A message is transmitted to the original sender to acknowledge the transmission and to identify any errors detected.

7. The receiver processes the information received according to its own internal procedures and timing requirements.

Here is how a typical EDI exchange works (our example assumes the two companies communicate directly with one another). A manufacturer writes its replenishment orders to a computer file instead of printing them. At a mutually agreed-on time, it connects this computer by telephone line, either leased or dial-up, to a processing function and then to the supplier's machine. After an initial "handshake" routine, which establishes the identities of the machines, the manufacturer's computer forwards the relevant orders to the supplier's computer.

Next, the supplier processes the orders, perhaps sending an acknowledgement to the sender. At the same time, the supplier's system generates packing notes and associated documentation for the warehouse and carrier, then produces its invoices as a computer file and forwards them to the manufacturer. The manufacturer, in turn, sends its remittance advice electronically and may even pay the bills through a bank clearing-house system.

In sophisticated applications, the EDI information flows directly into an artificial intelligence system, where the computer uses it to make business decisions.

15.7 Short Summary

N EDI provides business process integration across companies by exchanging business documents such as purchase orders, invoices, and shipment notices in electronic form, using industry standard formats.

N Implementing EDI benefits both the sender and the receiver. It is mutual effort, and its benefits are maximized by sharing information in a timely manner.

N EDI does not involve data entry at multiple points.

N Data from EDI is in electronic form, which makes it easy to share across the organization.

N The entire EDI process can be handled without using a single piece of paper.

15.7 Brain Storm

1. What are ALE & EDI?
2. How EDI differs from Traditional Approach?
3. What is the use of EDI?
4. What is the need of EDI?
5. What are all the benefits of EDI?
6. Explain How EDI works?

Lecture 16

EDI Standards

Objectives

In this lecture you will learn the following

- What is meant by EDI Standards?
- What is the Motivation?
- About Electronic Trading Networks

Coverage Plan

Lecture 16

16.1 Snap Shot

The development of new ways of doing business is often paralleled by the development of industry standards. EDI standards fall under the auspices of the American National Standards Institute(ANSI), which chartered the Accredited Standards Committee X12 (ASCX12) in 1979. The ASCX12 Committee's objective is to develop uniform standards for inter-industry electronic interchange of business transactions

16.2 EDI Standards

Briefly, the X12 data interchange standards consist of :

Transaction Set Standards: These define the procedural format and data content requirements for specified business transactions, e.g., purchase orders.

Data Dictionary and Segment Dictionary: These define the precise content for data elements and data segments used in building transaction sets.

Transaction Control Standards: These define the formats for the information required to control the data interchange.

Universal adoption of the EDI standard developed by ANSI/ASCX12 will enable all organizations desiring to conduct multi-industry transactions to use a single standard format for interchanging data. In the US alone, over 10,000 companies, in a wide range of industries, already routinely use EDI and ASCX12 standards. International standards have been established based on the X12 standards as well. These standards are called EDI for Administration Commerce and Trade (EDIFACT) and may be obtained through ANSI.

EDI standards grew from needs in transportation and payment applications and have been extended for use in other business and technical applications. For transportation, the information system parallels the physical movement of cargo and an information transaction accompanies significant events in cargo movement:

- Reservation or pick-up request
- Shipment information from shipper to carrier

- Export/import information for international shipments
- Carrier-to-carrier way bill data exchange
- Tracing information
- Freight bill data, carrier-to-payer
- Payment data

- ➢ Payer-to-bank
- ➢ Bank-to-bank
- ➢ Bank-to-payee.

Each type of information-need requires the formal definition of an EDI transaction set and establishment of user timing requirements. Although the original EDI standards included the transaction formats for transportation applications, formats for other applications are being derived by industry groups. The applications, formats for other applications are being derived by industry groups. The applications for transportation include shipment information, import/export data, interline and inter-modal data, inquiry and reply. Consolidation, repetitive pattern processing , invoicing , and payment. Other applications include order placement, commercial invoicing and payment.

For each application, major units of information are defined as 'transaction sets' which are the structure for communicating information between systems. A 'transaction set' in EDI equates to a form in a paperwork system. An application may have several different transaction sets defined. The transaction set is further defined in terms of 'segments' (or lines of information), and the segment is defined in terms of 'data elements' (the smallest information unit other than a character).

All units of information—transaction set, segment, data element – may be variable length, but the information is structured so that it may be constructed by one computer system and interpreted and processed by another. New applications and information units may be specified without impacting work previously completed.

Data movement from one system to another may be initiated in several ways:

1. Inquiry transaction set received from another system.
2. Previously established schedule
3. Exceptions (management by exception)

4. Detection of errors in data received from another system
5. Inquiry transaction set generated in response to management needs.

The interface computer program and the structure of each type of transaction set are part of the EDI standards. EDI does not address a standard which extends into a company's internal system.

EDI standards and documentation for transportation include:

- Information Structure
- System rules and procedures
- Programming guide
- Transaction set formats

Air,
Motor,
Ocean,
Rail
Segments, data elements and codes
Communications specifications.

The standards were developed by industry work groups at the Transportation Data Coordinating Committee (TDCC).

16.3 Variable-Length EDI Standards

The discussion of standards in this section is application to all variable-length standards, such as:

TDCC: The Transportation Data Coordinating Committee (TDCC) was formed to develop EDI formats for the transportation industry's four primary segments: air, motor, ocean and rail. This same organization is called EDIA (The Electronic Data Interchange Association) today.

UCS/WINS: The Uniform, Code Council (UCC) was chosen to oversee the creation and ongoing maintenance of the Uniform Communication Standard (UCS) for the grocery industry and the Warehouse Information Network Standard (WINS) for the warehousing industry.

X12: The American National Standards Institute (ANSI) formed the Accredited Standards Committee (ASC) X12 as the development and maintenance organization for a generic cross-industry EDI standard, ANSI ASC X12. The Data Interchange Standards Association (DISA) is secretariat for this standards process. The X12 standard is committed to meet the needs of all industries. TDCC, UCS, and WINS are in the process of becoming part of the ANSI ASC X12 standards.

No one industry uses all the capabilities available in the X12 standard. Instead, industries have identified subsets of the standard that their members will use. Some have given their subsets names. References to such standards as EDX(Electrical Data Exchange), EIDX (Electronic Industry Data Exchange), CIDX(Chemical Industry Data Exchange), PIDX(Petroleum Industry Data Exchange), AIAG(Automotive Industry Action Group), ICOPS (Industry Committee for Office Products Standards), VICS(Voluntary Inter-industry Communications Standard), HIBCC (Health Industry Business Communications Council), NWDA (National Wholesale Druggists Association). Etc., are actually references to industry-specific subsets of ANSI ASC X12.

EDIFACT: The EDIFACT Standard, EDI for Administration, Commerce and Transport, has been developed for international EDI.

16.4 Motivation

The methodologies for communicating business, trade, and transportation transaction data between concerned organizations in the U.S. materialized during the evolution of improved data processing and data communications technologies. Some practical events which dictated that new methodologies be employed are:

1. Cost of improved technologies become more acceptable.

2. Dynamics of modern business operations relating to time and response constraints, transaction volumes, cost of manual operations, and general growth in complexity brought about increased usage of computer and communications capabilities.

3. Corporate 'internal' operations, services, and/or functions were recognized by being dependent on information originating from 'external' organization.

4. Costs were rising for producing, storing, mailing, administering , manage handling, transcribing and otherwise responding to business information received from external sources on paper.

5. Organizations recognized the potential of EDI for becoming more operationally responsive in order to retain a competitive place in the market.

6. Transportation and transportation status information was seen to play critical roles in operating timely, reliable, efficient, and responsive business logistics systems.
7. Companies and organizations employing computer technology in the U.S represented a significant "in place" resource which could productively support EDI operations.

16.5 Cost Benefit Analysis of EDI

The demonstrated benefits of EDI include reduced inventories, reduction in purchase and payment overheads and faster reaction times. However, there is an intangible benefit of EDI that cannot be measured in percentages—improved business relationships with trading partners.

According to Price Waterhouse, the accounting firm, EDI is attractive because apart from eliminating paper and manual processing, if implemented properly it can reduce the cost of doing business by as much as five percent of net sales. A complete cost-benefit analysis of EDI should also include the value of increased market share that EDI may bring.

EDI provides many significant business benefits, including:

- Marketing competitiveness
- Administrative cost savings
- Shorter time to market
- Better quality control
- Improved corporate trading relationships.

16.6 Beyond EDI: Electronic Trading Networks

Evolving electronic trading networks will bring both opportunities and threats to users. Electronic trading networks (ETN) incorporate the functions provided by EDI, electronic mail, and other services, but go much further to electronically embrace all steps in the trade process, including the trade itself.

To qualify as an ETN, networks and services must be combined to provide a seamless and open environment for the procurement of goods and services. Thus, an ETN must transparently offer the whole range of interactive data exchange necessary for inter-firm searching and trading.

The ideal form of ETN is not a market tied to, or dominated by, one major player but a source of many enquiry with both suppliers and customers, leading to fluid, multiple contractual alliances. Ultimately, ETNs can be expected to reduce information-related costs, speed the identification and location of customers and suppliers, increase the accuracy of the match between product and service specification and buyer’s needs, and facilitate negotiation and delivery.

Interest in ETNs has it roots in research that has challenged the popular belief that information technology, for example, argues that the real benefits of using IT derive from the ways in which organizations are able to integrate information and communication technologies into their commercial structures.

The task of managers, it suggests, is to re-engineer business processes, both internally and externally, and to develop new forms and styles of organization, rather than simply to automate and support existing information systems and processes.

One way organizations can do this is by joining an ETN. These networks could be operated by network service providers, by trade association or by coalitions of users.

Membership in an ETN can lead to a redefinition of the scope of an organization. For example, access to an ETN could provide small- and medium-sized enterprises seeking to grow their businesses with a mechanism to avoid traditional vulnerabilities.

Most failures have two origins: over-reliance on core business with a dominant trading partner who withdraws, and a cash flow crisis at a time of over-trading due to failure in the arrival of funds or raw materials.

The first problem can be reduced by membership in an ETN, which provides an opportunity for a company to broaden its customer base. The second problem is avoided by an ETN institutional structure that ensures guaranteed payments and payments and delivery of materials. Moves toward the establishment of ETNs can already be observed. Initiatives include networks of customer-service terminals and shopping mall kiosks, some EDI user groups, and alliances of professional trading intermediaries such as brokers and auctioneers.

But if ETNs bring advantages, they also pose dangers. Access to such networks can alter knowledge and power balances between participants. It is difficult to assess whether the benefits of trading on ETNs will be real or illusory in the long term. Simply having access to more information needed to become involved in a trade is not a sufficient guarantee of sustained competitive advantage for users of ETN. The quality, timeliness and security of such information are key ingredients, as are all the rules governing international transactions.

The airline industry provides an example of the kind of inequity that my be created in such a system. When American Airlines introduced in the first computerized reservation system—a system that included information on both its own flights and those of other airlines—it ensured that information on its own flights was contained on the first page of information. Similarly, selective inputting of information may favor those controlling the information.

Ownership and rules for usage are also key. For example, should one organization be responsible for all the elements of an ETN? The issues here include: who operate the network infrastructure: who operates the market: who controls financial clearing and settlement: and who has the right to access and trade on the network itself?

ETNs are unlikely to bring about a perfectly competitive market. In fact, unexpected asymmetries can be expected to develop. Potential ETN participants can be threatened, for example, by the arrival of new players in previously protected markets; price competition may increase or be suppressed by new market leaders; and the traditional competitive advantages of partnerships might be eroded.

Inappropriate regulations and the growing complexity of electronic markets could well result in the proliferation of a new form of black market—a market that eludes the monitoring and accountability procedures created by national governments to a greater degree than ever before.

The challenges can be considered under four dimensions:

1. Institutional Dimension. The ETNs emerging in Europe are doing so in an environment heavily influenced by regulation. Such regulations may promote or hamper the process of building electronic trading user groups. They also affect firms decisions to shift from the use of traditional communication networks, such as telephone and fax, to advanced interactive data exchange procedures such as EDI.

2. User Dimension. The potential for ETNs to create opportunities for strengthened competitiveness through improvements in logistics is widely recognized, for example, in shipping and rail transport. But from the users perspective, the benefits of such networks are contingent on suitable procedures for electronic document certification, clear designation of responsibilities and guarantees, geographical location, firm size and resources, and network and application standards.

3. Services Dimension. Traditionally, communication in trading networks has been composed primarily of the telephone, fax and a limited number of relatively simple non-interactive data transmission services. In the 1990s, interactive services such as voice and image processing, electronic funds transfer, EDI, and multimedia applications are expected to combine with open document standards and signature authentication to support interactive data exchange among geographically dispersed and diverse trading communities.

   Some of these service have been implemented, others await commercialization, but access, interconnectivity conditions and service functionality will be critical factors in the diffusion and take-up of these services.

4. Technical Dimension. Underlying the emergence of ETNs are choices on network interface protocols, software applications, system architectures, and information storage and retrieval methods.

16.7 Short Summary

- EDI standards fall under the auspices of the American National Standards Institute(ANSI), which chartered the Accredited Standards Committee X12 (ASCX12) in 1979.

- Universal adoption of the EDI standard developed by ANSI/ASCX12 will enable all organizations desiring to conduct multi-industry transactions to use a single standard format for interchanging data.

- No one industry uses all the capabilities available in the X12 standard.

- Evolving electronic trading networks will bring both opportunities and threats to users. Electronic trading networks (ETN) incorporate the functions provided by EDI, electronic mail, and other services, but go much further to electronically embrace all steps in the trade process, including the trade itself.

16.8 Brain Storm

1. What do you mean by EDI Standards?

2. Explain-
   X-12
   EDIFACT
   TDCC
   UCS/WINS
   EIDX, PIDX, CIDX, AIAG, ICOPS, VICS, HIBCC, NWDA

3. What are the practical events for new methodologies be employed?

4. What is the cost Benefit Analysis of EDI?

5. Explain ETN?

Lecture 17

EDI Components

Objectives

In this lecture you will learn the following

- Knowing About EDI Components
- Knowing About File Types
- Knowing About EDI Services

Coverage Plan

Lecture 17

17.1 Snap Shot

A typical EDI system implements a specific set of EDI by enabling the exchange of business documents. It accepts documents from business software applications, converts the document to a standard format and sends it to another software application or trading partner.

17.2 EDI Components

EDI system converts generic EDI messages (in EDIFACT or any other EDI standard) format to RDBMS format and from RDBMS format to EDI format. There are EDI application programs for software developers to configure EDI to work with the various user application software programs. There is normally no end-user interaction with EDI—it is entirely within the background of the EDI system.

RDBMS data base contains the data to be translated into EDI format and where EDI data is to be converted (and written) to. EDI treats the application data base generically—it reads and writes to the tables and fields specified according to the message mappings created by the EDI Administration during EDI message configuration. These are done by EDI Configuration programs under the purview of EDI.

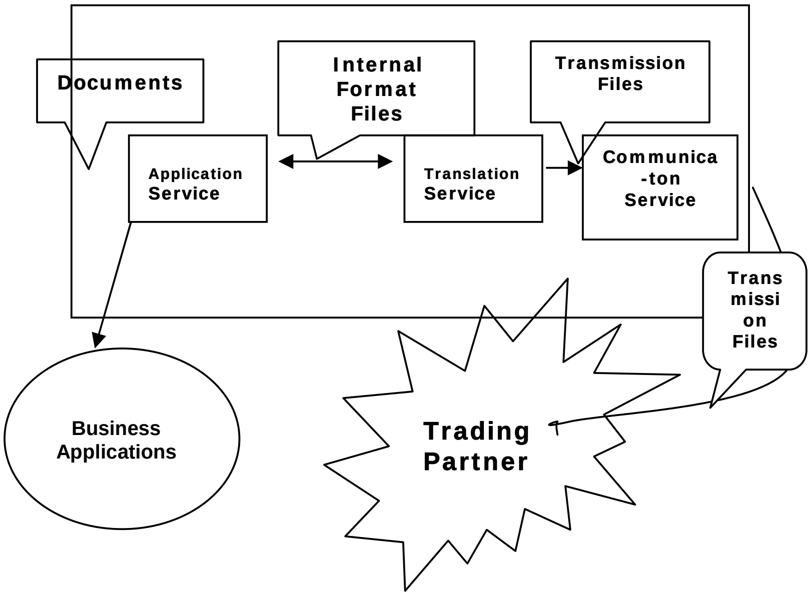
There are three main components in a EDI system:

1. Application Service – provide the means of integrating existing or new applications into the EDI system.

2. Translation Service – converts data from internal format standards to an external format and translates data from an external format to an internal format standard.

3. Communication Service- passes documents onto a network via the agreed communication protocol.

Fig shows the interaction between the three EDI service components. All these components are described in detail later.



Interaction between the DEC/EDI service Components

17.3 File Types

EDI creates the following files as a document passes through the system:

- Internal Format File (IFF)
- External Format File (EFF)
- Transmission File

Each of these files described in the following sections.

Internal Format File

An internal format file (IFF) contains a single document for a single trading partner. Internal format file is principally for EDI's own use.

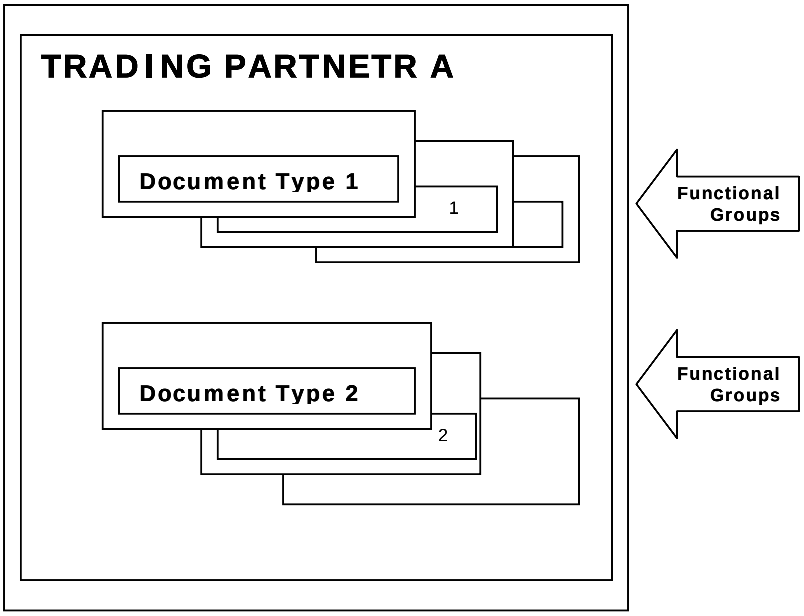
External Format File

The external format file (EFF) contains the same data as the internal format file translated into the appropriate standard document format.

Transmission File

A transmission file contains one or more documents for the same trading partner. Documents of the same type are packaged together in functional groups. The functional groups to one trading partner are packaged into an interchange set. An interchange set contains one or more functional groups of documents with the same sender and receiver. Fig is a representation of a transmission file.

Interchange Set



Transmission File

17.4 EDI Services

The three EDI services all perform different tasks. The following sections give an overview of what happens in each of three services.

Application Service

The Application service provides the link between a business application and EDI. It allows you to send document to, and receive documents from, a EDI system.
A set of callable routines is used to transfer documents from the business application into EDI. Documents destinations can be either intra-company or to external companies, i.e., trading partners.

The EDI Application Service holds each incoming and outgoing document as a single internal format file.

EDI converts the document to a standard format and sends it to the trading partner using the relevant communication protocol. A number of different standards and communication protocols are available.

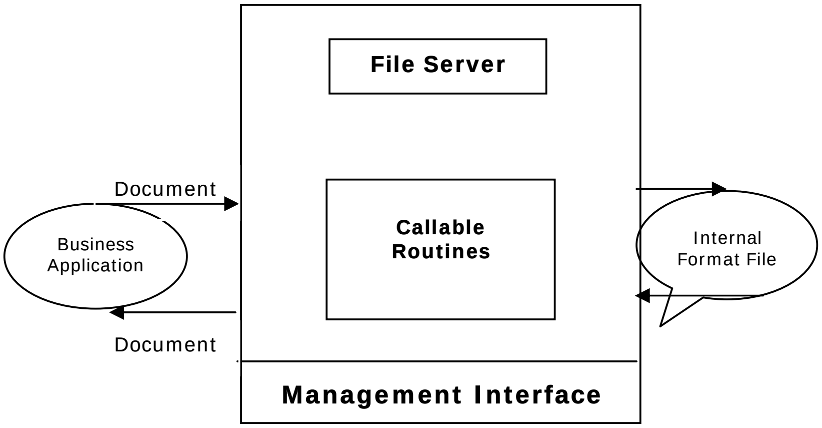
The following lists describe what happens in the Application Service:
For outgoing documents:

- The business application uses the callable routines to send a document from the business application to the Application Service. The document is now in the EDI system and is called internal format file.

- The Application Service sends the document in the internal format file to the Translation Service

For incoming documents

- The Application Service receives an internal format file from the Translation Service.



Application Service

- The Application Service makes the data in the internal format file available in database so that the business application can fetch the document from EDI. A callable interface is used to do this.

- The Application Service makes the data in the internal format file available in database so that the business application can fetch the document from EDI. A callable interface is used to do this.

Translation Service

- converts outgoing documents from an internal format file to an agreed external format.

- translates incoming documents from an external format to the EDI internal format file.

- The external document standards that a EDI system supports are EDIFACT, X12,TDCC, and ODETTE.

The following lists describe what happens in the Translation Service:

- The translation Service receives a document in the internal format file from the Application Service. It converts the internal format file to the appropriate external standard (either EDIFACT, X12, TDCC, or ODETTE). The file is now an external format file.

- The Translation Service combines one or more external format files into a transmission file.

  For incoming documents:

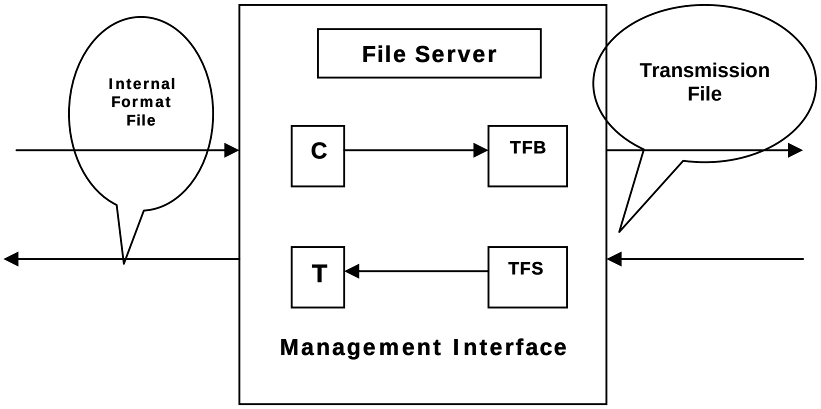
- The Translation Service receives a document in the transmission file from the Communication Service.

- Separates the transmission file to produce external format files.

- It translates each external format file which may be in an external standard (either EDIFACT, X12, TDCC, or ODETTE) to the internal format file. The file is now an internal format file.

- The Translation Service now sends the internal format file to the Application Service.

The following Fig shows the EDI Translation Service



MMMmanff

C	=	Converter
T	=	Translator
TFB	=	Transmission File Builder
TFS	=	Transmission File Splitter

(FIG)Translation Service

Communication Service

The Communication Service sends and receives transmission files to and from the trading partners either directly or by using a third-party service called a Value Added Network (VAN).

The following lists describe what happens in the Communication Service:

For outgoing documents:

The Communication Service receives a transmission file from the Translation Service. It checks the file to see which trading partner it has to be sent to.

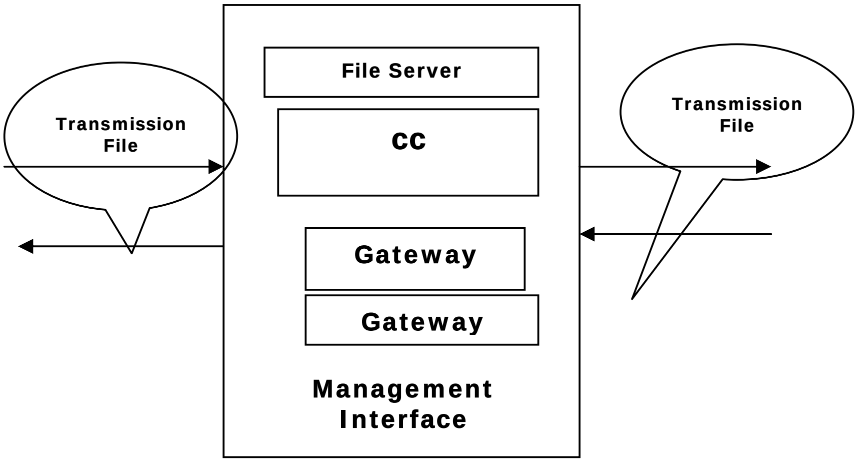
When it has identified the type of connection to be used for this trading partner it determines which gateway to use.

The Communication Service sends the transmission file to the trading partner.

For incoming documents:

- The Communication Service receives a transmission file from the trading partner. The file arrives through one of the gateways that EDI supports.
- The Communication Service sends the transmission file to the Translation Service.

The following Fig shows the EDI Communication Service



Communication Service

CC = Communication Controller
Fig Communication Service

17.5 Short Summary

- EDI system converts generic EDI messages (in EDIFACT or any other EDI standard) format to RDBMS format and from RDBMS format to EDI format.
- Application Service – provide the means of integrating existing or new applications into the EDI system.

- Translation Service – converts data from internal format standards to an external format and translates data from an external format to an internal format standard.
- Communication Service- passes documents onto a network via the agreed communication protocol.

17.6 Brain Storm

1. What are the three main Components of EDI?
2. Explain about Application Service.
3. Explain about Translation Service.
4. Explain about Communication Service.
5. What are the three File Types?

Lecture 18

EDI-Business Approach

Objectives

In this lecture you will learn the following

- Knowing About EDI Value Added Network(VAN)
- About EDI Software
- Business Approach to EDI
- Developing an EDI plan

Coverage Plan

Lecture 18

18.1 Snap Shot

In reality, most of the time EDI users will be influenced by factors other than the variations between VANS services. One of the main factors which influence most companies is an analysis of which VANS are used by their main trading partners. As stated earlier different industries tend to have developed their use of EDI around a particular VAN therefore a useful starting point is to evaluate which of your key trading partners are on which network.. It is also often the case that if your interest in EDI is being driven by a request to trade electronically with a particular customer that this organization will have developed a start up package for you with a particular network . This again will influence your decision.

If you are not influenced by either of the above factors, you can evaluate each of the VANS in turn and make up your own mind. There are differences in approach and the costs associated with joining each network and you should therefore determine which VAN best supports the needs of your organization. Your local Awareness Center will help you if need further information about VANS. In particular we hold stocks of literature, community lists and in some cases examples of the implementation documents prepared by the VANS in conjunction with their major customers.

18.2 Choosing EDI Value Added Network (VAN)

Selecting the Value Added Network (VAN) that your company will use to do business with the ABC Department is not necessarily a simple task. Neither is it as complex as some might lead you to believe. As a supplier to a large trading partner, many of the decisions fall into place for you. The larger retail trading partner, makes the tough choices regarding technology and providers. The only choice available to the supplier is often to just accept the situation.

The situation becomes more complicated when trying to trade with companies which use different VANs. In these cases, though, most of the considerations are economic: given your options, how do you connect with your trading partners in the most cost effective manner?

As we have said before, though ABC Department EC (Electronic Commerce)/EDI is different. In an effort to promote competition and reduce cost, the ABC Department connects to number of VANs it has “certified” for meeting a number of pertinent criteria. In evaluating these, you will find similar offerings from many different vendors, all of which claim to offer the best service or pricing. You may find radically different services offered. However, most the complex technical decisions (like X12 version) have already been made by your large EDI customer. Spend some time becoming familiar with your EDI needs and desires so that you may make an informed business decision.

So, in selecting a VAN for XYX Department EC/EDI, the first thing to look for in a VAN is "XYZ Department certification". VANs make EDI transactions (such as Requests for Quotation) available by downloading the information into one of your company's computers, XYZ Department-certified VANs have proven that they can relay messages between XYZ Department buyers and XYZ Department suppliers. All XYZ Department-certified VANs have access to the same set of XYZ EDI transactions so you shouldn't need to worry about which VAN has the data from specific XYZ Department installations.

Conversely, no uncertified VAN has access to those transactions, so don't even bother with one if you want to trade with the XYZ Department. That narrows the field to 20 or so.

The nest thing to recognize is that VAN selection must be tightly coupled with EDI software selection. Not all VANs work with all EDI software packages. Some VANs work only with software that they supply. Other VANs work with a specific list of EDI software package, if you have some reason to select a particular VAN (for example, you may have non ABC Department trading partners that already use that VAN) then try to pick an EDI software package that your selected VAN promises to support, if you already have an EDI software package that you desire to use (for example, you may have been using EDI in house and have integrated some EDI software package with your inventory system), then you need to see which ABC Department certified VANs support your EDI software. If you re new to EDI, and especially if the ABC Department is your only EDI trading partner, consider getting your VAN service and EDI software from the same place. Many VANs offer both VAN services and EDI software.

When you start shopping for a Value Added Network you will find a wide variety of different services offered. Some VAN accounts are very simple. You are provided with software when you get an account and pay a flat monthly fee for the service. The VAN will define a "profile" for your business that determines which XYZ Department RFQs you will receive. All you need to do is to install the software and run it whenever you want to bid on XYZ Department RFQs. Several of XYZ Department certified VANs specialize in this type of "entry level" or "turn key" EDI installation.

Other VANs will offer more complex and powerful EDI implementations. Pricing schemes may be based on the amount of data you send and receive. You may be able to change which XYZ Department RFQs you see by managing your own account on the VAN. Your VAN account may allow you to archive data on the VAN instead of on your local PC and it may work with multiple different EDI software packages, each with its own specific strength Multiple versions of the ANSI X12 EDI standard may be supported. This can be important if you have many commercial EDI trading partners, so that you can use the same EDI system with all of them.

18.3 Choosing EDI Software

Choosing EDI software for your company is similar in many respects to selecting a Value Added Network to handle your EDI transactions. A very wide range of software packages are available, ranging in price form less than $100 to thousands of dollars for multi-user, network versions. Remember that not all EDI software packages work with all VANs and that you may need to limit your choice of VANs if you select your EDI software before your VAN. Similarly, if you have already selected a VAN, your choice of EDI packages may be constrained by your VAN selection.

As we discussed earlier, the primary function of EDI software is something called "translation". Transaction is the process of converting a file in the ANSI X12 or United Nations EDIFACT standard (files intended for computer processing) into files intended for examination and reading by humans. A raw X12 data file looks like gibberish to most people. A translated X12 data file looks like a business document, a Purchase Order, for example.

You have to have translation functionality describes the ability of an EDI program to bring up data entry forms on the screen so that you can, for example, respond to an 840 (Request for Quotation) transaction by generating an 843 (Quote) transaction.

In a simple EDI implementation you will call your VAN, respond to RFQs, print reports, and manage your historical data and audit trail information all within a single software application. These "all in one" (or "plug and play") EDI software applications can be very simple to set up and use.

In a more complex EDI implementation, the functions just mentioned could be performed by separate programs. EDI data could be retrieved from your VAN(s) by a dedicated computer system using async, by-sync, X25, Internet, X..400, and /or other telecommunication standards and networks. A standalone translator could be used to process the process the EDI data. A mapping program could place the EDI data into your corporate database system. Other custom software applications could be used to generate Quotations or other EDI transactions, perhaps in an automated or semi-automated fashion. These generated Quotations or other transactions could then be translated back into ANSI X12 and delivered to your VAN by separate pieces of software. This type of EDI implementation can be expensive to set up but might prove very profitable in the long run since the human intervention in producing quotations can be reduced and since all data can be made to reside in your own corporate database systems.

The following are the major factors used to select EDI software:

Ease of upgrade:

As an EDI trading relationship matures there is likely to be a requirement for enhancement of the existing system. This may arise as a result of additional messages, changes to existing messages or standards, addition of new trading partners and their individual messaging requirements, inclusion of additional network connections or an increase in the number of business applications to be integrated.

Network connectivity:

Some EDI software packages are restrictive , since they do not allow users to be connected to all of the major EDI networks. This is the exception to the rule since most of the most popular packages have multi-network connectivity.

Multi-standards capability:

In cases where a supplier is faced with a situation in which two or more trading partners require EDI messages to be transmitted using different standards the software must be able to accommodate this need. Many Companies will not be integrating their EDI application with their in-house systems and will required a hard copy print of any incoming EDI messages. This facility must be available on the software under consideration.

18.4 Business Approach to EDI

Very often, it is difficult to quantify the effect of EDI on the day to day running of business. This is particularly true for small companies who do not handle the vast volumes of paperwork which have become such a problem for large organizations and cannot easily achieve significant savings in administrative overheads. For smaller organizations to understand the importance of EDI in a business sense, it is necessary to step back from day to day operational issues and consider the major changes in business management and operations which are taking place in all industries.

Need for Change

Organizations in both the private and public sectors are under pressure to provide a better service to their customers as cost effectively as possible. To achieve this businesses now have to work more closely with each other than they have ever done before. Partnership has become a major theme of business, underpinned with very fast and reliable methods of communication to enable business partners to function more effectively. Where these partnerships are being developed, supported by EDI, an evolution in supply chain management is taking place. At the heart of this change is the need for much closer integration of business processes throughout the supply chain. For this to take place there must also be true integration of the computer systems which support the activities of all of the organizations involved. This is the role that EDI fulfils, ensuring that information on orders, schedules, invoices etc, which supports the business relationship between customers and suppliers need only be entered once into the system. It can then flow rapidly and accurately down the supply chain to all of the parties involved in the delivery of a product or service to market.

18.5 Rationale for EDI

It is clear therefore that EDI has an important role for business today. Linked to other Information Technology and Management Strategies it can assist what is now called the Re-engineering of Business Processes. Organizations must use information to support their businesses they must also share import information with their business partners as quickly as possible. Investments have therefore been made in systems which capture reliable sales information. Distribution and Inventory management systems manage the flow of products to the consumer and EDI ensures that suppliers, whose performance is essential to this process, receive rapid notification of schedule and order requirements.

For retailers to be able to meet customer demand and back this up with rapid reordering and delivery mechanisms EDI has become essential. Automotive companies have set themselves the objective of delivering vehicles, built to order, within 4 weeks. To achieve this they need well managed communications with suppliers to ensure that components are delivered 'Just-in-Time' to the assembly line. Suppliers now realize that if they receive orders and work schedules via EDI they must process them directly through their computer systems and rapidly make the appropriate amendments to their suppler schedules for the true benefits of EDI to be realized. This means that manual processing times are cut from hours to minutes and that managers can manage by exception rather than be overwhelmed with the volume of information which flows through the system.

18.6 EDI is a Business Issue

For all of these reasons and many more, EDI is a business rather than a technical issue. The technical aspects of EDI are relatively simple. The key issue with regard to EDI is the way in which it is used in a business and operational sense. Therefore for EDI to deliver benefits to any organization

Its introduction must carry the full weight of management commitment. This is not just a commitment to the introduction of EDI in the short term but to the long term integration of EDI into the business and to the operational and procedural changes it will stimulate. To achieve these levels of commitment a strategy or plan for EDI will be necessary. This should place EDI in a context which is meaningful for each organization. It must therefore be conceived to take account of the business environment facing the company and current computer systems.

18.7 Developing an EDI Plan

If a company recognizes that is a business need to develop plans for the implementation of EDI then it is useful to devise a step-by-step approach as discussed below:

1. EDI Champion Management commitment and involvement is vital. Since management attention is focused on the day to day running of the business it will be necessary to

prepare the case for EDI so that it can be given some priority in your company. To achieve this every company needs an EDI champion. This can be anyone whether from a business or IT background. This person should then undertake preliminary investigation to begin to build the business case for EDI.

2. Business Case Initially it is useful to understand the status of EDI in your industry. The EDI Awareness Centers can help with this by providing information and useful contacts. You should then by able to form a view of the potential for EDI in your company and from whom external influences are likely to come.

The next phase of evaluation involves an internal analysis of EDI opportunities. All departments in the company should be included. Again discussions with active EDI users should provide guidance as to where benefits are to be derived. The exact scope of the benefits will vary from company to company. Some organizations feel that the fact that customers can be sure that orders will be processed on the day that they are issued is a significant benefit and greatly enhances the business relationship. Others are able to qualify the tangible benefits associated with removing paper and the re-keying of information from the business process. Most feel that the use of EDI enables them to handle greater volumes of documents without the need for additional staff. These and other EDI related benefits must be translated into each companies operational environment if justification for EDI is to be developed. It is also important not to evaluate EDI on the basis of one application e.g. orders, from one customer, Companies often find EDI difficult to justify on this basis as this does not take the full potential for EDI into consideration.

3. Management Commitment When this evaluation is complete the company will then be in possession of the facts with which to make a decision about EDI. Then management should be asked to support EDI implementation and, most importantly, the FULL integration of EDI with current systems and processes. This level of management understanding and commitments is essential to the successful use of EDI and without it the full benefits are unlikely to be obtained.

4. EDI Development and Implementation With management support it is possible to move on to a more detailed analysis of EDI applications from an Operational and Technical stand point. The result of this will be a Development Plan which clearly outlines the implementation strategy including factors which are external to the company e.g, trading partners plans and internal needs which are required to support the plan e.g, systems

developments. It is essential however that these plans are practical, that they support defined business needs and that they can be supported by the current IT capabilities of the organization.

5. Training All staff who are to be involved in the EDI project should be kept fully informed. The user department will have to be trained in both the new EDI application and the procedures which have been defined to support the application. In addition, if the company has decided to take a proactive approach in leading the introduction of EDI with its trading partners, management will have to be fully briefed so they can provide active support to the project.

6. Communication with Trading Partners Communication at the day to day operational and implementation level is important. Good supporting documentation is also essential. Any organization which is leading an EDI implementation project should be able to provide you with a comprehensive Implementation Guide. They should also be prepared to offer you some support and provide you with concise information about project time scales, live dates etc.

18.8 Short Summary

- There are differences in approach and the costs associated with joining each network and you should therefore determine which VAN best supports the needs of your organization.

- Linked to other Information Technology and Management Strategies EDI can assist what is now called the Re-engineering of Business Processes.

- Organizations in both the private and public sectors are under pressure to provide a better service to their customers as cost effectively as possible.

- Some EDI software packages are restrictive , since they do not allow users to be connected to all of the major EDI networks.

18.9 Brain Storm

1. Explain about EDI-Value Added Network.
2. What is meant by EDI Software?
3. What are all the major factors to select EDI-Software?
4. Explain about the Business Approach to EDI.
5. How to develop an EDI Plan?

Lecture 19

Enterprise Resource Planning: An Introduction

Objectives

In this lecture you will learn the following

- Knowing About Reengineering For Electronic Commerce
- Enterprise Resource Planning
- Various Characteristics & Features of ERP
- Implementation Approach of ERP
- The Future of ERP Systems

Coverage Plan

Lecture 19

19.1 Snap Shot

ERP (Enterprise Resource Planning) is an industry term for the broad set of a activities Supported by multi-module application software that help a manufacture or other business manage the important parts of its business, including product planning, parts purchasing, maintaining inventories, interacting with suppliers, providing customer service, and tracking orders. ERP can also include application modules for the finance and human resources aspects of a business. Typically, an ERP system uses or is integrated with a relational database system. In other words, ERP is a software infrastructure that helps to manage the different parts of a company of business. The aim is to improve the cooperation and interaction between al the departments such as the products planning, purchasing, manufacturing, sales and customers service department. In brief, it is the planning of the 4Ms- Man, Money, Machines and Materials. The deployment of an ERP system can involve considerable business process analysis, employee retraining , and new work procedures.

19.2 Evolution of ERP

In today's business environment, there has to be much greater interaction between the customers and manufactures. This means that, in order to produce goods tailored to customer requirements and provide faster deliveries, the enterprise must be closely linked to both suppliers and customers. In order to achieve this, improved delivery performance, decreased lead times within the enterprise and, improved efficiency and effectiveness, manufactures need to have efficient planning and control systems that enable very good synchronization and planning in all the processes of the organization. Today, however, the challenge is intense and requires a strong integration across the value chain. In the ever growing business environment the following expectations are placed on the industry:

N Aggressive Cost control initiatives

N Need to analyze costs/revenues on a product of customer basis

N Flexibility to respond to changing business requirements

N More informed management decision making

N Changes in ways of doing business

Enterprise Resource Planning is a strategic tool, which equips the enterprise with the necessary capabilities to integrate and synchronize the isolated function into streamlines business processes in order to gain a competitive edge in the dynamic business environment. Prior to 1960's, the business had to rely on the traditional ways of inventory manage4ment to ensure smooth functioning of organization. The most popularly known amongst them is EOQ (Economic Order Quantity).In his method, each item in the stock is analyzed for its ordering cost and the inventory carrying cost. A trade off is established on a phased out expected demand of one year, and this way the most economic ordering quantity can be decided. This technique in principle is a reactive way of managing inventory. In 1960's a new technique of Material Requirements Planning, popularly known as MRP, evolved. This was a proactive manner of inventory management. This technique fundamentally ex0plodes the end product demand obtained from the Master Production Schedule (MPS) for a specified product structure (which is taken from Bill of Material) into a detailed schedule of purchase orders or production orders taking into account the inventory on hand. MRP is a simple logic but the magnitude of data involved in a realistic situation makes it computationally cumbersome .If undertaken manually the entire process is highly time consuming. It therefore becomes essential to use a computer to carry out the exercise.

The effectiveness of MRP successfully demonstrated in:

N Reduction in production and delivery lead times by improving co-ordination and avoiding delays

N Reduction of inventory

N Increased efficiency, and making commitments more realistic

MRP proved to be a very good technique for managing inventory, but it did not take into account other resources of an organization.

MRP proved to be a very good technique for managing inventory, but it did not take into account other resources of an organization. In 1970's this gave birth to a modified MRP logic popularly known as Closed Loop MRP. In this technique the capacity of the organization to produce a particular product is also taken into account by incorporating a module called Capacity Requirements Planning (CRP).

Hence, a feedback loop is provided form the CRP module to VPS if there is mot enough capacity available to produce.

In 1980's, the concept of MRP-II (Manufacturing Resources Planning) is an extension of MRP to shop floor and Distribution Management activities. In early 1990's MRP-II was further extended to cover more areas like Engineering, Finance, Human Resources, Projects Management, etc., i.e., the complete gamut of activities within in business enterprise. Hence, the term ERP (Enterprise Resources Planning) was coined. In addition to system requirements, ERP addresses technology aspects like client/server distributed architecture, RDBMS, object oriented programming , etc . ERP Systems- Bandwidth ERP solutions address broad area within any business like Manufacturing ,Distribution ,Finance, Project Management. Service and Maintenance ,Transportation etc. a seamless integration is essential to provide visibility and consistency across the enterprise.

The Enterprise Resource Planning system should be sufficiently versatile to support different manufacturing environments like make-to-stock, assemble-to-order and engineer to order. The Customer Order Decoupling Point (CODP) should be flexible to allow the co-existence of these manufacturing environments within the same system. An example here could be any manufacturing company which has businesses spread over all there manufacturing environments. It is also very likely that the same product may migrate from one manufacturing environment to another during its producer life cycle.

The systems should be complete enough to support both Discrete as will as Process manufacturing scenario's. The efficiency of an enterprise depends on the quick flow of information across the complete supply chain i.e. form the customer to manufactures to supplier. This places demands on the ERP system to have rich functionally across all areas like sales, accounts receivable, engineering, planning, Inventory Management, Production, Purchase, account, payable, quality management, production, distribution Planning and external transportation. Electronic Data interchange (EDI) is an important tool in speeding up communications with trading partners.

Lots of companies are becoming global and focusing on down-sizing and decentralizing their business. A typical example here could be ABB and Northern Telecom companies, which have business spread around the globe. For these types of companies to manage their business efficiently. ERP systems need to have extensive multi-site management capabilities.

The complete financial accounting and management accounting requirements of the organization should be addressed.

It is necessary to have centralized or de-centralized accounting functions with complete flexibility to consolidate corporate information.

For companies undertaking large scale and complex ERP projects, tools should be available for cost-effective project management, project planning and project control. After-sales service should be streamlines and managed efficiently. A strong Enterprise Information System (EIS) with extensive drill down capabilities should be available for the top management to get a progress report of their organization which helps them to analyze, manage and quick decision making in the key areas.

Difficulty in getting accurate data, timely information and improper interface of the complex natured business functions have been identified as the hurdles in the growth of any business. Time and again depending upon the velocity of the growing business needs, one or the other applications (See Table) and planning systems (See Table) have been introduced into the business world for crossing there hurdles and for achieving the required growth.

Table: Evolution of Business Applications

Abbreviations	**Description**
MIS	Management Information Systems-(No Decision Support)
IIS	Integrated Information Systems-(No Decision Support)
EIS	Executive Information Systems-(Decision Support)
CIS	Corporate Information Systems-(Decision Support)
EWS	Enterprise Wide Systems-(No Decision Support Logistics are considered as a part of system)

Abbreviation	**Description**
MRP	Materials Requirement Planning
MRP II	Manufacturing Resource Planning
MRP III	Money Resources Planning

ERP	Enterprise Resources Planning

19.3 Characteristics of ERP

An ERP system is not only the integration of various organization processes. Any system has to possess few key characteristics to qualify for a true ERP solution. These features are:

a. **Flexibility**: An ERP system should be flexible to respond to the changing needs of an enterprise. The client server technology enables ERP to run across various data base back ends through Open Data Base Connectivity (ODBC).

b. **Modular & Open**: ERP system has to have an open system architecture. This means that any module can be interfaces or detached whenever required without affecting the other module. It should supply multiple hardware platforms for the companies having heterogeneous collection of systems. It must support some third party add-one also.

c. **Comprehensive**: It should be able to support variety of organizational functions and must be suitable for a wide range of business organizations.

d. **Beyond The Company**: It should mot be confined to the organizational boundaries, rather support the on-line connectivity to the other business entities of the organization.

e. **Best Business Practices**: It must have a collection of the best business processes applicable world wide.

f. **Simulation of Reality**: Last but not the least, it must simulate the reality of business processes on the computers. In no way it should have the control belong the business processes and it must be able to assign accountabilities to the users controlling the system.

19.4 Features of ERP

The major features of ERP and what ERP can do for the business system are:

N ERP facilities company-wide Integrated Information System, covering all functional areas like, manufacturing, Selling and distribution, Payables, Receivables, Inventory, accounts, Human resources, Purchases, etc.

N ERP performs core corporate activities and increases customer device and thereby augmenting the corporate image.

N ERP eliminates most of the business problems like Material shortages

N Productivity enhancements, Customer service, cash Management,

N Inventory problems, quality problems, Prompt delivery, etc.

N ERP not only addresses the current requirements of the company but also provides the opportunity o0f continually improving and refining business processes.

N ERP allows automatic introduction of latest technologies, like

N Electronic Fund Transfer (EFT), Electronic Data Interchange(EDI),

N Internet, Intranet, Video conferencing, E-Commerce, etc.

N ERP provides business intelligence tools like Decision Support

N Systems(DSS), Executive Information System (EIS), Reporting, Data

N Mining and Early Warning Systems fort enabling people to make better decisions and thus improve their business processes

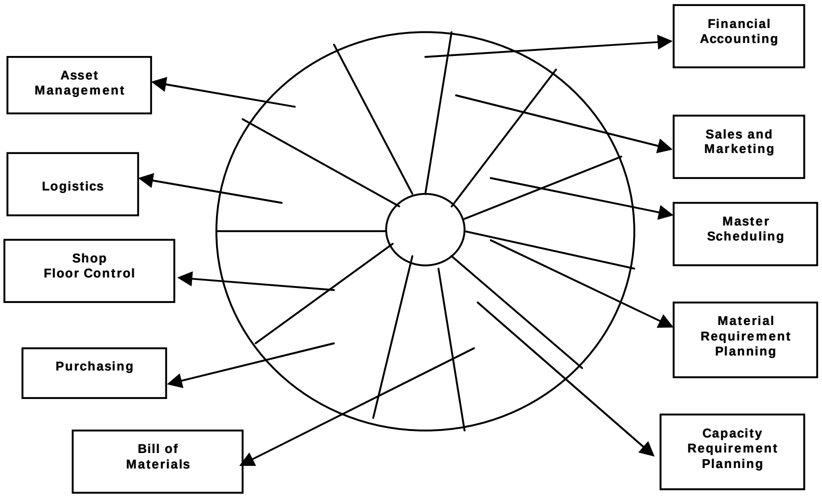
N ERP bridges the information gap across the organization.

N ERP provides for complete integration of systems not only across the departments in a company but also across the companies under the same management.

N ERP is an effective solution for better Project Management.

19.5 Components of ERP

To enable the easy handling of the system the ERP has been divided into the following core subsystem (See Figure)



N Asset Management

N Bill of Materials

N Capacity Requirements Planning

N Financial Accounting

N Logistics

N Master Scheduling

N Material Requirement Planning

N Purchasing

N Sales and Marketing

N Shop Floor control

19.6 Need of ERP

Most organizations across the world have realized that in a rapidly changing environment, it is impossible to create and maintain a custom designed software package which will cater to all their requirements and also be completely up-to-date. Realizing the requirement of the user organizations, some of the leading software companies have designed, Enterprise Resource Planning software, which will offer an integrated software solution to all the functions of an organizations such as:

N complete Integration of systems across the departments in a company as well as across the enterprise as a whole.

N Effective solution for better Project Management

N Better Customer Service

N Automatic Introduction of latest technologies

N Expertise database

19.7 ERP Vendors

There are various ERP vendors available today, who are very active in the market. Some of the companies offering renowned international ERP products include:

N SAP

N Baan

N Oracle

N Peoplesoft

N JD Edwards

N IBM

N CODA

N D & B

N Marcarn

N QAD

N SMI

N Platinum

N Software 2000

N Ramco

These vendors offer slightly differing features in their products; still the major modules are same in all of the products, SAR R/3, which is the market leader in this segment, offers the following modules:

N Financial Accounting

N Treasury

N Controlling

N Enterprise Controlling

N Investment Management

N Production Planning

N Materials Management

N Plant Maintenance & Service Management

N Quality Management

N Project System

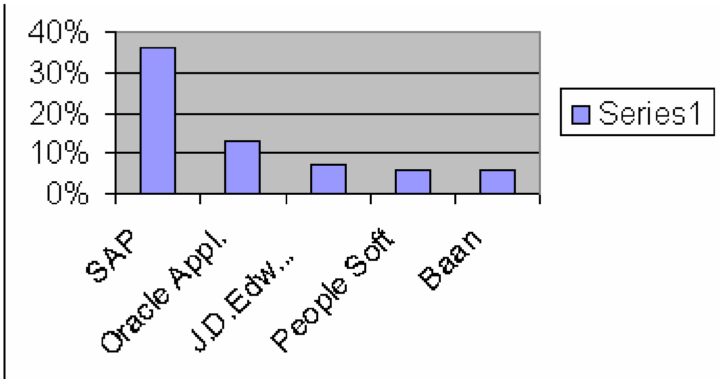
N Sales & Distribution

N Human Resources Management

N Business Information Warehouse

Today SAP is considered to be the most exhaustive ERP system. SAP R/3 Also allows the connectivity to Internet and the business through it for the mobile and distantly located users. Other vendors also provide more or less similar functionality in their bundle of product.

Today there are approximately 1,400 active R/2 installations and as impressive 15,000 R/3 installations. Currently, SAP is in the company with -and leading - several other major client/server ERP development companies Figure shows SAP's Standing in the ERP market:



Source:AMR,1997 Estimated Market

As one can see, SAP has clearly taken the lead and continues to stay in front of the pack. Its growth has been nothing short of astounding

N SAP employs more that 15,000 people.

N SAP dedicates 55 percent of its resources to customer service.

N SAP focuses 24 percent of its resources on research and development.

N SAP focuses 21 percent of its resources on sales and marketing

N SAP has offices in more that 50 countries

N SAP provides solutions for 15 major industry sectors, including oil and gas health care, automotive, and high tech and electronics.

N In financial year (FY) 1997 SAP achieved a 62 percent increase over FY96 revenues.

N In FY97, SAP R/3 sales rose 63 percent.

SAP is currently used by more than 7,500 customers in more than 90 countries with live SAP installations au more than 13,000 geographically dispersed customer sites. The list of SAP customers reads like a Wall Street "who's who" list of world market leaders. SAP customers include the following companies

N Chevron Petroleum
N Chrysler International
N Random House,Inc.
N Hewlett Packard
N Reebok
N Deutsche Bank

Today, SAP is recognized as the fourth-largest independent software supplier in the world and it ranks as the global leader in business application software.

19.8 Business Process Reengineering

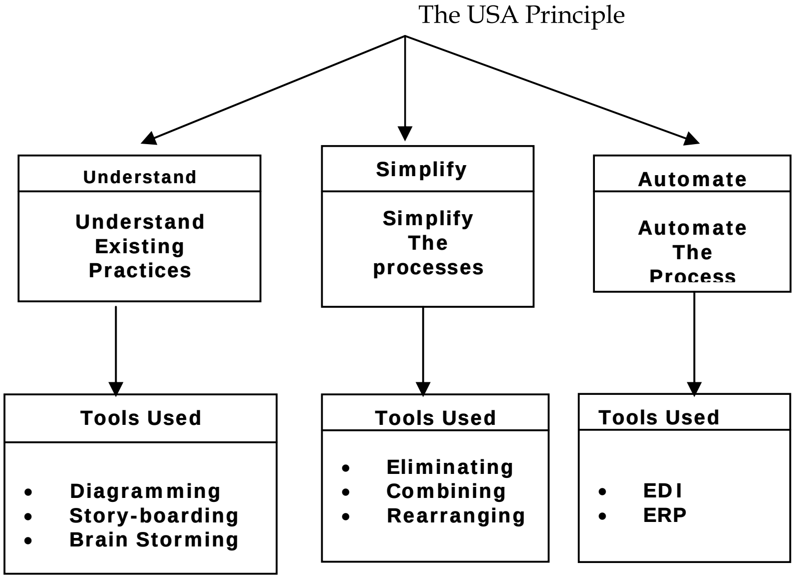
Business Process Reengineering is a pre-requisite for going ahead with a powerful planning tool, ERP. Since, ERP gets the best out of the available resources, t is very important to reengineer the business process before, during or immediately after an ERP implementation. If the business processesare not streamlined , the resource allocation will always be sub-optimal.

Reengineering also makes it smooth to drive the ERP implementation programme, because the former builds the spirit of competitiveness and adaptation of best practices. An in-depth BPR study has to be done before taking up ERP.

Business Process Reengineering brings out deficiencies of the existing system and attempts to maximize productivity through restructuring and reorganizing the human resources as well as divisions and departments in the organization. Business Process Engineering involves the following steps:

N Study the current system
N Design and develop new systems
N Define Process, organization structure and procedure
N Develop customize the software
N Train people
N Implement new system

The principle followed for BRP may be defined as USA principle (Understand , Simplify and Automate) i,e., understanding the existing practices, simplifying the processes and automate the process. Various tools used for USA principle are shown in Figure



19.9 Evaluation Criteria for ERP Packages

Once the BTP is completed the next task is to evaluate and select a suitable package for implementation. Evaluation of the right ERP package is considered as more crucial step. Evaluation and selection involves:

N Functional fit with the Company's business processes
N Degree of integration between the various component of the ERP system

N Flexibility and scalability

N Complexity, user friendless

N Quick implementation: short end ROI period

N Ability to support multi-site planning and control

N Technology: client/server capabilities, database independence, security

N Availability of regular upgrades

N Amount of customization required

N Local support infrastructure

N Availability of reference sites

N Total costs, including cost of license, training, implementation, maintenance, customization and hardware requirements.

Advantages of ERP Packages

The ERP packages have following advantages:

N Ease to use

N General purpose

N Readymade solutions for most of the problems

N Only customization required

N Integration of all functions already established

N ROI earlier than the software developed in-house

N Dependency on Human Resources eliminated

N Easy enterprise wide information sharing

N Suppliers and customers san be on-line communication

N Knowledge transfer between industries guarantees innovation

N Automatic adaptation to new technology

19.10 Implementation Approach of ERP

Implementation of an ERP package has been dome on a phased manner, Step by step method of implementing ERP System will yield a better result. The normal steps involved in implementation of an ERP are as below:

N Project Planning

N Business & Operational analysis including Gap analysis

N Business Process Reengineering(BPR)

N Installation and configuration

N Project team training

N Business Requirement mapping to software

N Module configuration

N System modification and interfaces

N Data conversion

N Custom Documentation

N End user training

N Acceptance testing

N Post implementation

The above steps are grouped and sub-divided into four major phases namely

1. Detailed discussions
2. Design & Customization
3. Implementation and
4. Production.

The phases of implementation, vis-a-vis their tasks and respective deliverables are shown in Figure

Phases	Tasks	Deliverables
Detailed Discussions	• Project Initialization • Evaluation of current Processes, business Practices, requirements • Set-up Project Organization	• Accepted norms & Conditions • Project Organization Chart • Identify work or Support Teams.
Design & Customization.	• Map Organization • Map Business Processes • Define Functions and Processes. • ERP Software Configura- tion. • Build ERP System Modifications.	• Organization Structure • Design Specification • Process Flow Diagrams • Function Model • Configuration Recording • Systems Modification
	• Create Go-Live Plan & Documentation. • Integrate Application • Test the ERP Customization	

Implementation	• Train Users • Run Trial Production • Maintain Systems	• Testing Environment Report • Customization Test Report • Implementation Report
Production		• Reconciliation Reports • Conversion Plan Execution.

Implementation of ERP solutions is one of the largest drivers of growth in the consultancy business, The introduction of a large and complex software like ERP,which enables an organization to integrate heir manufacturing, finance and marketing operations at all levels, is in itself a challenge, since it calls for technical and functional skills and a change in user mindsets, And therein comes a role of a consultant will play a major role in implementation of an ERP solution.

Assuming a situation where the client has implemented an ERP solution If the auditor is aware of ERP he can make use of the features or ERP and thereby:

N ensures that the internal controls and checks are consistently maintained.

N ensures that the provisions of Income tax or other fiscal laws are not ignored e.g., one can control the payment of cash in excess of Rs.10000 for expenses or Rs.20000 as loans and advances, EDS deductions and payment are automated etc.,

N ensures that the Accounting Standards are consistently followed across the company.

N improves the quality of the reporting.

By now, one should be knowing that the ERP is a high end sophisticated software solution that reduces the pressure and work load of the managers and provides accurate, timely information for taking appropriate business decisions. Managers with knowledge of ERP will be able to achieve their targets and goals by proper implementation of ERP system in their organization In fact managers are expected to translate the business rules and requirements for mapping them into RTP software. Managers, as representatives of the organization have to coordinate with vendors, consultants, auditors etc.,for a proper implementation of ERP package.

Today, many companies have been benefited a lot by implementing ERP packages. Sole of the benefits are listed below:

N Improved Cost Control

N Faster response and follow up on customers

N More efficient cash collection , say, material reduction in delay in payments by customers.

N Better monitoring and quicker resolution of queries

N Enables quick response to change in business operations and market conditions

N Helps to achieve competitive advantage by improving its business process

N Reduce paper documents by providing on-line formats for quickly entering and retrieving information

N Improves timeliness of information by permitting posting daily, instead of monthly

N Gives Accounts-Payable personnel increased control of invoicing and payment processing and thereby boosting their productivity and eliminating their reliance on computer personnel for there operations. Greater accuracy of information with detailed content, better presentation, fully satisfactory for the auditors.

N Improves supply-demand linkage with remote locations and branches in different countries.

N Improves information access and management throughout the enterprise Provides solution for problems like Y2K and Single Monitory (SMU) or Euro Currency.

N Provides unified customer database, usable by all applications.

N Improves International operations by supporting a variety of tax structures, invoicing schemes, multiple currencies, multiple period accounting and languages.

Today's, ERP is being implemented in almost all types of organizations irrespective of its mode and spread of operation typical list of segments where ERP systems have been implemented are Aerospace & Defense Automotive industry, Banking & Insurance Chemical & pharmaceutical industries, consumers goods, Healthcare ,High-tech & electronics

,Mechanical engineering & heavy construction, Oil& gas, project oriented manufacturing, Public administration &education, Retail Telecommunications, Utilities etc.

The BaaN approach is to conduct a concurrent Business Process Re-engineering during the ERP implementation and aim to shorten the total implementation time frame. Two scenario's can be distinguished

1. Comprehensive Implementation Scenario: Here the focus is more on business improvement than on technical improvement during the implementation. This approach is suitable when : Improvements in business in processes are required . Customization are necessary . Different alternative strategies need to be evaluated .High level of integration with other systems are required .Multiple Sites have to be implemented

2. Compact Implementation Scenario: Here the focus is on technical migration during the implementation with enhanced business improvements coming at a later stage. This approach is suitable when; Improvements in business processes are not required immediately. Change-minded organization with firm decision making process. Company operating according to common business practices. Single site has to be implemented.

Any ERP software is of no value unless it is implemented well. Implementation is expensive and normally costs 2 to 3 times the product value . While a number of products have third party consultants who implement the product , getting the support directly from the vendor is obviously better, from the perspective of a better understanding of how to implement the product to take full advantage pf its capabilities.

Given that people trained in some of there products have a good demand world-wide , it is critical to ensure stability of the implementation team to carry through the entire exercise.

Finally, the stability of the vendor , his commitment to this market and commitment to India are of vital importance. By implementing EERP solutions, and given the competitive context an ERP system would become a necessary part of infrastructure.

19.11 The Future of ERP systems

Enterprise Resource Planning is the latest high end solution, information technology has lint to business application. The ERP As solutions seek to streamline and integrate operation processes and information flows in the company to synergies the resources of an organization namely men, material, money and machine through information. Initially implementation of an ERP package was possible only for very large multinational companies and infrastructure companies due to high cost involved, ERP implementation in India is picking up very fast. Last few years have seen lot of products coming into the market and the leading companies taking initiatives to implement ERP, not most of these, implementation have not yet witness the expected results. However the expects are hopeful about the success an ERP system , Again, it is not a magic tool, which will transforms everything overnight, rather successful implementation is a long journey towards enterprise excellence.

The Internet represents the next major technology enabler which allows rapid supply chain management between multiple operations and trading partners. Most ERP systems are enhancing their products to become "internet Enabled " so that customers worldwide can have direct access to the supplier's ERP systems are building in the Workflow Management functionally which provides mechanism to manage and control the flow of work by monitoring logistic aspects like workload capacity, throughput times, work queue lengths and processing times.

Recognizing the need to go beyond the MRP-II all ERP vendors are busy adding to their product portfolio. baaN for example has already introduced concepts like ITP(intelligence Resource Planning),MTP-III(money Resources Planning) and has acquired companies for strategic technologies like Visual Product Configuration. Product Data Managing and Finite Scheduling.

19.12 Short Summary

N Enterprise Resource Planning is a strategic tool, which equips the enterprise with the necessary capabilities to integrate and synchronize the isolated function into streamlines business processes in order to gain a competitive edge in the dynamic business environment.

N For companies undertaking large scale and complex ERP projects, tools should be available for cost-effective project management, project planning and project control.

N Need for ERP- Most organizations across the world have realized that in a rapidly changing environment, it is impossible to create and maintain a custom designed software package which will cater to all their requirements and also be completely up-to-date.

19.13 Brain Storm

1. What is meant by ERP?
2. What are the Characteristics of ERP?
3. What are the Features of ERP?
4. Explain about Components of ERP?
5. What is Business Process Reengineering?
6. Explain about the Implementation Approach of ERP.

Lecture 20

Information Technology Plan for ERP System

Objectives

In this lecture you will learn the following

- Enabling Best Technology Practices
- Information Technology Assessment
- Reviewing the Information Technology Plan
- Reviewing Technology Portfolio

Coverage Plan

Lecture 20

20.1 Snap Shot

Enabling Best Technology Practices

Thinking of an ERP system without sophisticated information technology infrastructure, is not possible. It is said that, ERP is the finest expression of the inseparability of business and information technology. The incremental improvement in the information technology and the drastic reduction in prices of computers have made it possible even for the small organization to think about ERP systems. The earlier ERP systems were build only work with huge mainframe computers, The new era of PC, advent of client server technology and scalable Relational Data Base Management Systems (RDBMS) all nave contributed for the ease of deployment of ERP systems . Most of the ERP systems exploit he power of Three Tier Client Server Architecture .In a client server, environment , the serer stores the data, maintaining its integrity and consistency and processes the requests of the user from the client desktops . The load of data processing and application logic is divided between the server and the client. The three tier architecture adds a middle stratum, embodying all application logic and the business rules that are not part of the application , enforcing appropriate validation checks.

It is assumed that the companies implementing ERP solutions have multiple locations of operation and control. Hence, the online data transfer has to be dome across locations. To facilitate these transactions, the other important enabling technologies for ERP systems are Workflow, Workgroup , Groupware, Electronic Data Interchange(EDI) , Internet, Intranet, Data warehousing, etc.

Companies live or die by IT. When technology investments are perfectly aligned with business goals and work flawlessly, they imbue an enterprise with incredible Strength. But when companies fail to identify the right IT-enabled opportunities ,deploy ill-conceived systems of mismanage the overall activity. Poorly envisioned an executed IT investments become slow leaks that can burden a company while remaining almost unnoticed –until it's too late, Half of all technology projects fail to meet manager expectations. But instead of figuring out where and why a project fails, business executives sometimes use the Manager as scapegoat, loading to a revolving door at top the IT function and an underlying problem that never gets addressed.

Considering how few business initiatives today can succeed without assistance from IT, executives would be wise to become enlightened partners in the IT process and Thus help ensure its overall success. After all, allocating blame becomes irrelevant when sink or sail everybody is in the same boat.

Recognizing the need to get involved in IT decision making is one thing, but actually knowing how to do it is another. Any business executives struggle to get their brains around IT. Understandably they balk at measuring the value and performance of something so intimidatingly complex and, well, so technical. But being a good executive officer requires knowing how to leverage IT to advance business goals .And doing that will means evaluating whether IT is actually living up to its potential.

Once should also keep the following point in consideration while evaluating IT potential in your organization:

1. Customer Satisfaction
2. Enable Business Growth
3. Empower productivity
4. Innovation and learning
5. Running of IS

20.2 Customer Satisfaction

IT systems should match business objectives, Otherwise, "The systems as focused internally on things that are divorced from what really creates value". And for virtually every successful enterprise, customer satisfaction is a crucial business objective. Indeed, in come commodity-style industries, improving the customer experience offers the best and sometimes the only hope of com0petitive differentiation.

IT should enable a business to deliver a higher –quality customer experience at a lower cost to the company. While some technologies deliver highly visible forms of customer interaction, customers don't need to see technology to benefit from it-as in the case of a data warehouse that enables a company to tailor its products to customer preferences or a state-of-the art logistics system that allows an organization to deliver a product two days earlier than the competition Companies embrace the goal of improving customer satisfaction to varying degrees. If you 're in doubt about your own efforts, look outside your company to see how others do it .At the extreme end of the spectrum are companies like San Jose , Calif –based Cisco Systems Inc. The $6,.55billion Internet networking vendor is loath t6o approve a new IT project unless it directly affects the customer experience. Cisco claims that this customer-oriented approach saves it at lest $290 million dollar per year in operating, organizations competing directly with a Cisco should think hard about making customer satisfaction a priority when designing systems.

But not all customer –focused systems are good customer-focused systems. Don't fall into the trap pf creating technology systems just for the sake of having them. The last thing you want is a system that degrades customer satisfaction levels. Better not to invest in an automated customer support hotline at all, for example, if customers with unusual questions get frustrated because they can't talk to a real human . The effect that systems have on the customer experience can be measured by analyzing customer surveys or complaints logged into a help desk. If neither of these data points is available, that in itself is a red flag about your company's and is department—commitment to customer satisfaction.

20.3 Enable Business Growth

An important goal of the IS department should be to enable business growth opportunities. In a merger or acquisition, for instance, IT should clear the path for the unimpeded flow of information and operations. The integration of two companies technology systems can be the single biggest factor in a merger's success or failure/Yet all too often the IT function isn't factored into initial strategic conversations .

Beyond merely enabling already identified expansion opportunities, the Manager should also pose new ideas for growth. Managers are uniquely qualified to broaden strategic possibilities by proposing new applications of emerging technologies. In fact, information technology can help grow the business to such a degree that it becomes its own line of business. Just look at the Sabre Network, once an application to help American Airlines Inc keep track of seats, flight and reservations and now the world's largest privately owned real-time computer network. Or look at Amazon com Inc's mightly Web bookstore –which is helping to transform an entire industry.

How do you know if it is fulfilling its potential to help the business grow? First, evaluate the role IT played in the company's major growth moves in the past few years: Was the Manager present at all important conversations about strategy? Did he or she make suggestions about new ways to do things? Can the Manager articulate the long-term vision for the IS department and how it relates to the overall business strategy? Your Manager has a responsibility to communicate new developments to the executive team. If you aren't receiving such updates , you may have cause for concern because the Manager could overlook something important.

20.4 Empower Productivity

Information technology (IT) can help people do things faster, easier and better. It should empower productivity at the level of both the individual employee and the organization . Is that happening at your company?

One way to find out is by looking at internal feedback gleaned from steering committees, review boards and councils and surveys of end users. End-users surveys are good for turning up festering problems that impair employee productivity .But they also have their limits, even when users express overall satisfaction , that may not indicate a clean bill of health. " You can make customers completely satisfied and still miss new business opportunities across the enterprise .

Again, the trust measure of IT's impact on productivity is the degree of alignment between IS and business strategy . Just because the Manager provides cutting edge technology tools doesn't mean he's necessarily improving productivity. Someone can be very satisfied with the latest 'gee-whiz' technology, but they are not operating any differently and therefore the organization is not getting any value from IT. Often organization go merrily along upgrading to the latest version, but from a business standpoint (this) has a negative impact on productivity because they're making additional capital investments and may not be getting any value out of it. It's also worth noting that productivity is often retarded when have of climb the next upgrade's learning curve.

The ultimate measure of ITs impact on productivity, however, comes from your own experience. Has your behavior changed as a result of technology? Are you able to make decisions faster and easier than in the past? What sources of insight do you lack that could help you be a more effective business leader? Do you spend too much time liking for information? Does the Manager know of your frustrations, and is he responding? If the answer to any of these questions is "no", then you need to sit down with the Manager and hammer out an attack plan to turn the situation around.

20.5 Innovation and Learning

Technology alone cant's foster innovation. To flourish innovators need an open, risk-friendly corporate culture. To nurture, innovation, IT can develop tools that help employees share information and learn from others. Take a hard look at how your employees research their ideas. Is there an easier way? Can Geographically dispersed groups exchange ideas and experiences electronically? Is there a mechanism for capturing institutional knowledge? What about for obtaining and storing ideas from even the lowest-ranking employees ? The Manager should play a significant role in both articulating the new space created by technological advancements and providing employees with tools to capitalize on their creative potential.

Benchmarking against other companies is the surest way to answer this question. If competitors are beating you to market with innovations, you need to ramp up your efforts. And such IT tools as intranets, video-conferencing, electronic whiteboards and online training courses play an increasingly important role in stimulating communication and collaboration.

20.6 Running of IS

This is both the most and least important. But it's the one executives have historically concentrated on, sometimes to the detriment of more strategic assessments. At the high level senior business executives are concerned with , you should almost be able to know about the running of information systems. If your IS department is keeping up-to –date with outside developments, focusing on the customer, aligning properly with business strategy and providing tools to help employees do their jobs better and more creatively, then changes are it's operating effectively. In that case, sticking your nose in the Manager's business is unnecessary, counterproductive and potentially demoralizing.

If on the other hand ,your manager is untested or appears unable to address the first four questions, then you may want to look inside the department . A mal functioning Manager is a danger to the organization, leaving it vulnerable to looming crises like the year 2000 problem and the European Monetary Union convergence as will as to more nimble competitors. Companies that maintain inflexible systems impair their ability to keep up with rivals innovations and are as good as doomed, even when everyone else but the Manager is doing the right things.

In evaluating IS at the operational level , start with the IT budget –making sure to look at it in the most strategic light: what percentage of the IS budget is spent in furtherance of business objectives? If senior executives focus only on operational details like cost and spending ,they can draw the wrong conclusion.

20.7 Information Technology Assessment

The Information Technology(IT) plan must be more than a traditional description of technology evolution, more than an ingenious plan scripted to persuade the organizational financial decision makers to invest, The IT planning effort must move beyond the technical focus to include those issues of particular interest to the organization. A self-servicing approach to the development of an IT plan based solely on technical content is unacceptable. Unfortunately, most reports remain unread, tucked away, out of view in hope of not reminding the author of he questionable expense of the time resource expended . However a properly structured approach to the research leading up to the creation of the report can be the real value. The end result is mot necessarily the benefit it is the journey, the uncomfortable questions that are asked , and the opportunities that are uncovered that produce the lasting benefit to the organization .

The information technology assessment methodology sets out to establish two things:

i. To capture the state of deployment of information technology within the organization

ii. To rank the degree of which the organization utilizes the existing information technology if has already deployed

The first benefit in establishing these metrics is that you are abl8ia to determine the extent to which information technology is deployed throughout the organization. As you must have experience that there are probably fewer individuals who appreciate the breath of application of information technology across the organization. Knowing how widely information technology is deployed throughout an organization can elicit a strong response from senior managers who suddenly realize that without information technology, the organization would virtually come to a standstill. This reality check for senior managers must be controlled ad presented in the light of opportunity. You must leverage the fact that the organization is , to a degree, dependent on information technology. The dependence must be presented as an opportunity to further increase the positive return to the business.

The information technology assessment typically will cover the following areas:

N Organizational Structure. The IT Department will take on many forms depending on the organizational overall structure. Not only are there typical centralized and decentralized structure, there will be matrix structures inherited form the parent organization

N Service Level . The service level perception of the organization's information technology users is used to rank the effectiveness of the IT department . This must involve a service level survey ,which can take many forms.

N Budget,. The organization likely is unaware of the true cost of supporting its information technology resources. The total cost of ownership has been estimated by several industry analysts with some correlation. This study opens the door to opportunity in assigning costs directly to the appropriate business consumer of the technology

N Project Mix Primarily the assessment is used to identify projects that do not need to be part of the information technology portfolio. These projects are shown to be business initiatives and not technology initiatives.

N Technology Portfolio. This resembles a hardware and software inventory.

N The fact that your organization will conduct an information technology assessment should be communicated to the entire busies. The communication does not have to be elaborate or highly detailed . The purpose is to inform employees that the organization values its investment in information technology and that the result will be a status report used to highlight new opportunities to utilize technology even further. The communication can use any medium the organization currently utilizes. The information posting should include the following information

N A definition of the assessment

N Who or which group is leading the assessment

N The expected duration

N Any activities in which the employees may be asked to participate.

N The Expected benefits

N A date when the next communication will be made available

N A contact for further information or feedback.

The assessment is a preliminary measurement exercise. Employees become very interested in measurements because measurements can be used to rank employee performance. The old adage" what gets measured is what gets done" is both opportunity and risk for the organization. If the organization selects the right measurements, then the right things will get done.

Metrics Available for the IT Assessment

Area	Parameter
Organization	The following parameters can be used as a measure of compliance that your current organization exhibits with respect to industry standards. N Number of full-time IT personnel . An absolute measure that is sometimes skewed with the (mis) definition of full-time employees , part-time employees , contract employees and consultants. N Number of external contractors or consultants. Using this measure along with the number of full-time IT personnel will provide a more precise comparison between organizations. N Number of IT personnel as a percent or total employees . Typically used as a service metric , but in this context provides a normalized comparison between organizations of varying employee count.

N IT personnel cost as a percent IT budget . This will provide a normalized measure of the importance placed on human resources over technical resources.

N IT personnel cost as a percent of revenue. This provides a more consistent metric when comparing the human resources importance between organizations of varying revenue levels

N IT spending per total number of employees. Used occasionally ,but only within similar industries. Be cautious; the number of employees can vary dramatically between industries

N IT personnel and contractor /consultant turnover as a percent of total employee turnover . Use this parameter both alone and as compared to the rest of the organization. An improvement to this parameter is to gather turnover by reason . The turnover reason can point out various root causes, some under the control of the IT department and come with the organization.

N Shift in IT personnel capabilities. Not an absolute measure, but a classification of the skills required to perform the required technical tasks. Over time it is important to develop adequate training programs to meet the emerging technical capability demands.

Service Level

The following service level metrics can be used as a measure of Compliance that the emerging technical capability demands your current organization exhibits with respect to industry standard

N Number of information technology users per IT employee. A common metric used throughout the industry for inter-company comparisons. This metric is best used to compare organizations in similar industries. Many users on a large, mainframe-based application can be supported by relative by few support personnel, while several distinct client/server applications and fewer end users require relatively more support personnel.

N Support calls per employee and per IT employee. This can as an inter-company comparison but it primarily used as an internal measure of technical support loading

N Other support call parameters. There are dozens of support call metrics that tend to provide better internal measurements than inter-company comparisons . However, these various support call metrics can be averaged to produce an estimation of customer satisfaction.

N Satisfaction with applications. This is different than customer satisfaction. Here you develop a measure of the usefulness of the tools provided to the information technology users. This is a useful parameter, especially when considering upgrading legacy systems. It may be a surprise that the end users are quite satisfied with the benefits from the current system in place.

Budget

The following financial parameter can be used as a measure of compliance that your current organization exhibits with respect to industry standards.

N IT budget as a percent of sales. Probably the most widely used parameter when comparing IT departments between companies.

N IT versus business unit investment. A recent trend shows that IT budgets are no longer tightly controlled within the IT Department, but rather each business unit is now being allocated an IT budget. Whether the IT budget is being distributed or the business units are simply allocating more of their existing budget to IT is not entirely clear, This certainly supports the notion that as an increasingly larger portion of technology dollars are controlled outside of the IT department, it follows that the decision making on the target of those budget dollars is being shared proportionally .

N Rate of IT budget change. Certainly an indicator of your organization’s perception of the value that IT has brought to the business.

N Training as a percent of total IT budget. Particular to information technology is the increasing rate of change. Developing skills in every emerging technology is not feasible. However, the rate at which training dollars are invested can indicate the optimism an organization has towards information technology.

N IT spending per technology. A good comparison to ensure your shift in investment is correlating to the industry and ifs perception of emerging value-added technology.

Project

The following project parameters can be used as a measure of compliance that your organization exhibits with respect to industry standards.

N Project completion. An indicator of whether the IT Department is profit or delivery focused, Primarily an internal benchmark.

N Capital investment . Also considered an IT budget metric. A relative internal comparison between the dollars invested in organization capital projects versus those in the IT department.

N R&D investment .Also considered an IT budget metric. A relative internal comparison between the dollars invested in product research and development and those invested in emerging technology opportunity development.

N Barriers to completion. A good cross-industry comparison. Determines whether a specific technology or method hampers completion of projects.

N Legacy system replacement rate. An indicator of the value your organization puts in new and emerging information technology. Can be combined with the project completion and the satisfaction with applications metrics to provide a realistic comparison

N BPR related project rate. An indicator on the value your organization puts on the efficiency of the underlying business processes unit investment metric.

Technology Portfolio The following technology parameters can be used as a measure of compliance that your current organization exhibits with respect to industry standards.

N Platform distribution. A ranking of the technologies used in your organization and the market leadership those technology vendors occupy.

N Rate of growth of client/server Combined with the legacy system replacement rate, this metric is a good indicator of the risk level an organization is willing to accept.

N Package (ERP) systems. A good indicator of an organization's willingness to change its thinking from independent business units to a cross-functional model.

In the case of the information technology assessment, the measurements help produce the status report, but are more importantly used to identify opportunities in which you can leverage information technology to increase the return of business value.

The second benefit of the information technology assessment is the ability to rank your organization against industry benchmarks. In large organizations there met be internal corporate benchmarks that can also be used . Table provides a sample list of parameters that can be applied in each case.

The information technology assessment is not a trivial exercise for an organization to complete. Typically the complexity of the information technology assessment is proportional to the organization's size. It follows that a large organization may have several facilities of sites to evaluate and may have to deal with a larger number of personnel. A large organization would also be challenged to uncover true financial statistics. However, the benefit of a large organization is that the parameters can be used internally as benchmarks between business units. The comparison will be much more realistic because the underlying definition and calculation of the metrics will be similar across the organization. A small organization will have to compare its metrics strictly to external organizations, where the metric definition can vary.

A completed information status technology assessment allows the organization to produce a status report. The review of the status report should serve the entire organization. The IT status report does not have to be confined to the IT Department This is an opportunity to alert senior management to ant issues that have been identified.

20.8 Reviewing the Information Technology Plan

IT plans are short lived. Unlike a typical business plan, IT plans do not have a life cycle of four or five years. For example, a personal computer will double in processing capability in 12 months, but can be purchased at the same price as the current model. With this in mind, the IT plan must be reviewed regularly. Typically IT plans can span up to three years.

20.9 Reviewing Organization

Most organizations view the IT Department as a cost of doing business. That view is changing. As the need to carefully craft information technology solutions to support the business processes becomes an absolute necessity to compete , the IT Department is being considered an equal partner in shaping the organization's direction.

Today IT leaders are expected to be business leaders first and technologists second. The IR leader must possess the necessary business acumen to participate in the organization's management process and business planning process. The IT leader must gain the credibility of his of her management peers in order to be trusted with the delivery of the information technology portfolio. An addition to the change in the skill set of the IT leader, is the change required of the IT Department's organizational structure. The change in the IT leader's skill sit has brought change in the measurement systems placed against the department from the rest of the organization. This prompts the IT Department to realign to best meet the new measurements systems.

The organization's overall structure will have a great deal of influence over the demands placed upon the information technology organizational structure. In a large organization, the IT Department will tend to be less constrained for resources , This will allow the IT Department to focus some energy on more strategic initiatives. Whereas the small organization's IT department will likely be resource strained and will need o focus all its available energy on the tactical or operational task.

Utilizing the results of the it assessment and determining the type of organization being assessed will show the types of structures available. The intent is not to draw a completely mew organizational chart has reason to bend to accommodate the findings.

Fundamentally, there are only two structures to apply to organize the IT Department. They are the following:

i. Centralized. This structure provides tight control over all strategic, tactical, and operational technology issue advantage or the centralized organization is that it provides a clear source of direction. There is no doubt of this source. In a technical organization, a centralized structure will provide optimum definition and control of standards, policies and procedures. This can lead to a better understanding and control of expense or total cost of ownership. Further, with a single set of standards policies and procedures, the organization provides itself with some flexibility to change as the need arises.

ii. Decentralized. This structure provides loose control over all strategic, tactical, and operational technology issues. The advantage of the decentralized organization increases with overall company size Although there maybe more than one source of direction, having the input of more than a single source in a large company will provide more visibility to the needs of the 0organization. Responsiveness increases as local business units are able to react quickly to locally changing needs and requirements. Technical decisions can be averaged across the organization to provide a better overall result to he company

Unfortunately, the optimum organizational structure will exist somewhere in between, typically referred to as a hybrid organizational structure, there are several degrees of freedom that must be understood and defined. These degrees of freedom can include the following:

i. Information technology steering committee-In a large organization where some IT Department decentralization is expected, the overall information technology direction must be monitored and focused according to the business demands placed on it. A steering committee that includes technical members and key business unit members needs to be formed. There is a distinct need to provide specialized services on a particular set of technology . This could be hardware, software, networking or communications to name a few. An area of particular interest is the application support.

ii. Competency centers- The competency center is the notion of distributing responsibility over the ownership of the application process and the underlying infrastructure, The trend in this area continues to be that business units are adopting the application and that the IT Department is retaining control of the infrastructure. This is not meant as a divide and run scenario; it is intended as a partnership. IT will leverage a common infrastructure to keep the business unit from having to have the resources available to provide this service. While the business unit will invest in the process it operates and the IT Department does not have to invest in resources to learn the specific of each business units processes.

iii. Application ownership- The data center is another functional area that can be organized centrally or be decentralized out to the business units. When the data center is decentralized out to the business units consider both the positive and negatives consequences Technology consistency is more difficult to maintain. Each data center will tend to make decisions independently of the others and technology fragmentation can occur . However ,multiple data centers offer the opportunity create redundant or backup data centers. However, there must be sufficient organization control to mandate data center standards . A slight variation on the decentralized similar to the decentralized model in that there are multiple centers supporting each business unit able to act as a backup. The campus model capitalizes on the centralized model value to provide consistency in standards. Unfortunately, the campus model is limited to organizations who themselves are aligned along a camps model If an organization locates units independent of each other geographically, that the campus model reduces to the decentralized model.

iv. Hybrid model – The hybrid organization model will vary in terms of its implementation indifferent organizations. This is primarily a result of how the decentralized technical members are viewed. Should they be IT Department members who live in the business unit or members of the business unit who act as technical representatives for the IT Department.

20.10 Reviewing Service Level

The service level provided by the IT Department to the technology end users is probably the most interesting parameter to review. The service level is usually estimated by considering the effectiveness of the organization's technical support help desk. Although this is a very important metric, you must understand that there are other considerations as well.

The IT Department is interested to know how it is perceived from its customer base, the information technology end users. Do the end users view the IT Department as an operational or strategic partner? This dictates the importance the business units will place on the importance of the IT Department. Further, it is proportional to the investment the organization is willing to make in information technology in general and the IT Department specifically. This will also be concluded from the perception of how the IT Department is perceived to understand the underlying business needs and not just looking to deploy new technology. The OT Department must take a proactive approach to the underlying business needs, It is very important to understand the business that is being supported . This provides the opportunity to determine whether the business is taking full advantage of the available technology.

As part of the IT assessment, try to include an end user survey. Properly structured, replies will provide a wealth of information in a number of areas. This information will help establish some of the parameters previously discussed as well as create awareness, Further you need to get appreciation for the task at hand. End users need to understand that the IT Department is in a transition and that the final result will provide improved service level to the technology end users. In addition to service level parameters, to survey can capture data that can support cost/benefit calculations leading to identification of new service opportunities. Technology end users need more than help desks Conducting a survey is one way to accumulate statistics and to produce

A customer satisfaction benchmark. Using this benchmark, several opportunities may exist to provide increased support to the end user. For instance, the end users would surely appreciate the fact that the IT Department solicited their input the determine new service offerings.

The IT assessment will attempt to capture information that can lead to conclusions on several issues related to the end user service level. The first area to get focused feedback is those issues dealing with the end users first priority, that is, technology problem solving and support. This is usually an area where feedback is abundant. Unfortunately, it is usually negative feedback. However, it is the things dome poorly that need to be improved. The intent s to categorize the feedback and look for patterns that may point to a particular application of infrastructure element of hat may indicate additional training is needed on the part of the help desk technicians . This information could be coupled with reorganization of the help desk discussed previously.

It is useful to gauge the interest level of the end users to contribute new ideas to the improvement of the information technology portfolio. The use of comment sections provides the opportunity for improvement suggestions. Still better is a comment section that has selections identified. This helps get feedback on specific proposed initiatives and prompts the end users to think of similar needs.

The IT Department can organize itself sufficiently to develop and manage a service level agreement with the end users. There are likely to be several service level agreements in place. Earlier you learned about the concept of a competency center. The competency center could be used as a vehicle to package and deliver the services included in the end user application service level agreement. The following are various elements to consider with the competency center:

i. **Help desk** : The service level agreement will is identify the call resolution rate. That is how many calls can be responded to in a given time period and what percentage will get resolved in a given time period. The help desk calls must be tacked and documented for several reasons. The two most important reasons are to enable repeat problem identification and to support a claim of meeting the service level agreement.

ii. **Application Testing** : Regardless of whether the competency center delivers the enhancements, it should have the capability to test the enhancements in the organization’s production environment.

iii. **Customization**: The competency center is designed to serve the organization as a whole. It makes little sense to have end users responsible to outsource and project manage application enhancements.

A new release of the application must be tested prior to release into production .The competency center provides an opportunity to utilize the organization data and other unique attributes that the application vendor is unable to provide.

i. **Training**: Training can be best organized within a competency center because the application expertise is already present . An external training organization will not be as familiar with day to day operation of the application, especially if the application has been customized to the organization.

ii. **Marketing** : This is a proactive role for the competency center, The organization cannot afford to have all of its application end users responsible for monitoring new releases of the application for new feature function availability to the specific and users.

The parameters developed in the area of IT Department budget lead to the estimation of the total cost of ownership(TCO). A much touted parameter in the information technology industry, the ECO metric first arose out of the personal desktop computer. The Gartner Group lead the way with TCO studies in the early 1990's . The TCO studies were the first real attempts to consolidated the total investment an organization must make to support the desktop environment. The TCO parameter accumulate both operational expense and capital investment. The operational expense captures the cost of administration support and operation , while the capital investment includes the cost of capital in addition to the acquisition cost, To what stint direct end user costs are included tends to skew the comparison between TCO parameters between organizations.

The intent of the IT assessment in this area is to gather sufficient financial information to formulate the TCO. The IT assessment should focus on the following areas:

i. **Allocation of costs**. It is necessary to determine if a charge back policy exists. Do the end users to the technology have to pay from their departmental budgets or are the funds administered from the IT department budget ? What decision cycle or methodology does the organization use to determine whether a particular information technology investment is appropriate ? Is there a particular cost tracking mechanism in place to support the allocation of cost?

ii. **Administration costs**. This is a more difficult metric to quantify. However it is important to understand the amount of time and expense that is invested in developing partnerships and alliances with information technology vendors. The degree to which partnership are a success can be measured, in part through the use of compatible technology.

iii. **Support costs**. Several area of interest help develop an idea of support costs. Assess the use of standards , both technology standards(operating systems, network topologies and protocol and so on) and product standards (brand names, models, and so on) Also determine the extent to which product suites are used.

iv. **Purchase costs**. Determine the level to which the organization takes advantage of volume purchasing agreements or has negotiated long-term purchasing agreements.

v. **Operational costs**. Determine the mix of purchase versus leasing of technology get allocated throughout the organization ? How does the IT Department model its software licensing ? Is it a concurrent user model or a named user model?

With these parameters, the TCO model will begin to take shape. In some cases it will be a revealing exercise. The TCO is traditionally a Figure that greatly exceeds the purchase price. The purchase price typically is the only metric considered in most organizations.

With the IT assessment results , the IT Department can begin to focus the IT plan with respect to financial planning.

The IT Department budget as a percent of revenue tends to pose a dichotomy to the reviewer. If the actual fate is lower than the industry rate . then 8is can be perceived that the organization is well positioned, because if is managing to spend less than its competitor on information technology. It can also be viewed that the organization is being the industry and needs to invest more aggressively. If the actual rate is higher than the industry rate it can be interpreted that the organization is spending too much on information technology and should consider a mote conservation approach. It can also be interpreted that the organization is being aggressive with respect to its competitors.

The next most popular industry metric is the TCO. However, this parameter is still relatively new in practice. As such , it may be the first time an organization will be exposed to the TCO.

Be well prepared when using this measures in the IT budget. Although the resulting plan may be taking a very aggressive approach to controlling the newly found/ allocated costs, the shocks of tabling the ECO for the first time may present a barrier to overcome. In this section you will consider some of the ways in which the TCO parameters can be controlled.

To lower the purchase cost of technology look into preconfigured units, which in turn , drive the need for standards . If the organization can leverage many units at a standard configuration, the costs can be lowered. Look to vendors or resellers that can provide a pre-configuration service. The organization can provide standard profile or image to be installed in each unit, Typically, this is best leverage in the workstation or desktop /laptop area.

To lower support costs, look at your organization's business model. If the organization is global, then it follows that the technology vendor must provide a global support model. Attempting to provide service and support across different time zones and different geography involving different languages and cultures can be and enormous challenge. Put simply, the vendor must be where your organization is located. Of course, product quality should obviate the need for extensive support and service. Ensure the vendor implements quality practices and procedures consistent with your organization's quality expectations.

To lower operating costs, the organization must consider the rate at which it wants to refresh technology. Historically, organizations used the trickle down method to reallocate older technology, especially in the computer desktop area. An emerging trend is to consider lease arrangements over capital purchases. Some programs offer the capability to hold the expense constant while replacing the technology as the performance increases .

Another key item to consider closely is the concept of volume license agreements. Historically, the volume required excluded the majority of organization, however recent trends are clearly bringing the volume barrier to the point where most every company can participate. Be sure to clearly define the model as concurrent use and not per named user, Basically, the concurrent user model require that you license only active users, while the names use model requires that you like every end user regardless of use. This should be applied to every support (email) productivity (word processor) or production application like SAP, Baan etc.

20.11 Reviewing Project Mix

The IT Department has a portfolio of projects it must manage to completion. These projects are typically prioritized relative to the end user's persistence of getting the project delivered. However, the project list must reflect what the IT department should be doing from an organization can utilize information technology to do the following

i. Simply automate existing processes
ii. Bring together island of information
iii. Align business process
iv. Reengineer the business
v. Completely redefine the scope of the business.

The level of change the organization is promoting determines the number and type of projects the IT department must manage.

On the whole, IT Department must manage, there are three broad categories of projects.

i. Strategic. The projects are focused on the initiatives in the organization's business plan that are categorized as capital investment initiatives. These projects will help support the organization in its new form planned for in the strategic plan.

ii. Tactical. These project are those initiatives that are currently in place supporting the business in its current or near term form. A tactical project evolves from a planned strategic project or it can be an operational project that may be dealing with infrastructure.

iii. Development. These projects typically support the strategic initiatives of evolving the technical infrastructure. These projects are coupled with training and development opportunities for the IT personnel. These projects are coupled with training and development opportunities for the IT personnel. These projects will result in new infrastructure being deployed of new capabilities that can be offered to the organization.

The IT assessment will attempt to draw out information that will lead to conclusion in the project mix. There are the three categories previously defined; strategic, tactical, and development. Furthermore, you must determine whether the IT Department is leading projects that it should otherwise not be leading. In fact there is a great opportunity to ensure that the business units are taking ownership of the projects that are directly related to their business processes.

The financial parameter related to capital and R & D investment are interesting to calculate and then compare with the organization's overall rate of investment in these categories.

The IT plan must be focused to clearly define the three types of projects and the criteria to determine the type. Project ownership of each type of project must be clearly defined. The fact that all projects must be profit focused must replace the notion of delivery focused projects. This is not to say that project deadlines are not to be considered at all. Rather, timeliness and milestones are evaluators of progress and really have little to do with success.

The strategic project should have a project leader assigned who resides in the business unit that owns the project, The appropriate business unit, through its understanding of the organization's strategic direction, will likely have initiated this type of project. If the business unit is not willing to manage the project, then the project objective needs to be re-examined . If an initiative is important to a department, that department will certainly provide leadership. It is in that business unit's best interest to take control in order to determine when the project success factor has been reached.

The tactical project is one that is currently in motion to support an existing business need. As with the strategic project, the probable leader for the tactical project of from the sponsoring business unit. This does not preclude the fact that the IT Department may have a major contribution to made to the project. Tactical projects need to complete and deliver the expected benefits in the organization's neat term typically between 2 and 12 months.

The development project is typically an internal IT Department project. It is tied to strategic initiative, but is separate from the time line of the strategic project . The strategic project may not begin for up to 12 months; however the technology capabilities need to be understood and developed early and then maintained. As such, the project leader is usually from within the IT Department . The development projects should be organized to provide the majority of training that IT personnel will require. Training does not have to be a separate exercise.

20.12 Reviewing Technology Portfolio

Here you will consider the types of information technology and tools typically used and you will define a way in which to group these into manageable families. It tends to look more like an organizational structuring and in the end this may be the most efficient way to approach the technology classification The technology portfolio needs to capture several characteristic of the organization and the technology that is deployed.

From an organizational perspective, deployed application-level technology tends to follow the vertical functions within an organization . That is to say, certain applications will appear useful only in certain parts of the business. It follows from this that the hardware that supports the application will align along the same application and organizational lines As you look down into the layers of supporting technology and peer into the infrastructure, the alignment of the technology with the business is less clear. You see this trend continue: The further the technology is from the end user application, the more likely it is to be application independent. The infrastructure will begin to move from a vertical alignment to lay horizontally across the organization .

From the perspective of managing the technology, you can see that the technology alignment supports with your assumptions of the organizational alignment Previously, you learned about the requirement of business unit leadership for strategic and tactical projects. It follows that the management or ownership of the technology should follow the same orientation. The business units should own and support the applications they use in their business That is , as long as it is specific to that business unit. The challenge is then to locater technical resources is financially supported by the IT Department or is a member of the business unit. The latter or preferred but is highly dependent on the overall organizational model.

As you move away from the end used application into the infrastructure, the alignment to the business is less and the technology begins to standardize across business units. The technical resource to support the infrastructure will likely be part of the IT Department . The foal is to leverage centralized support for a standard technical infrastructure.

The following technology parameters can be used to gathered or calculated for the IT Department technology portfolio:

i. Platform distribution
ii. Rate of growth of client/server

iii. Type of computing devices used
iv. Type of production systems used
v. Type of productivity tools used
vi. Type of collaboration tools used.

The IT assessment will draw primarily on technical personnel to gather data for the infrastructure area. In some cases this can be gathered from existing hardware and software inventories. The survey should include such items as data based, collaboration, operating and network systems server hardware and communications. Business unit personnel will have valuable input in the area of production applications, protectively tools and collaboration needs.

You've reviewed the opportunity for an organization to focus the IT plan using information recovered from an assessment of the current state. There are probably hundreds of parameters that could be calculated . The success lies with those who understand what they need from the assessment in order to develop a highly focused IT plan.

20.13 Short Summary

- It is said that, ERP is the finest expression of the inseparability of business and information technology.
- Information technology (IT) can help people do things faster, easier and better. It should empower productivity at the level of both the individual employee and the organization
- The Manager should play a significant role in both articulating the new space created by technological advancements and providing employees with tools to capitalize on their creative potential.

20.14 Brain Storm

Write an essay about the conditions and terms for a good Company.

1. How do you empower the productivity?
2. What is meant by Innovation & Learning?
3. Give a notes on Information Technology Assessment.

Lecture 21

Getting Started with Active Server Pages

Objectives

In this lecture you will learn the following

- About Active Server Pages
- How Active Server Pages Really Work?
- Benefits of ASP
- How to Write ASP Scripting?
- About ASP Syntax
- About Expressions & Statements
- About Script Tags.

Coverage Plan

Lecture 21

21.1 Snap Shot

Microsoft Active Server Pages (ASP) is a serve-side scripting environment that you can use to create and run dynamic, interactive, high-performance Web server applications. When your scripts run on the server rather than on the client, your web server does all the work involved in generating the Hypertext Markup Language (HTML) pages that you send to browsers. You need not worry whether a browser can process your pages: your Web server does all the processing for it.

ASP scripts are an integral element necessary for process flow. For performance and scalability, COM components should be used to provide the functional processes within the page.

ASP is built on a scripting engine. This enables it to support multiple scripting languages such as Microsoft Visual Basic Scripting Edition (VBScript), Jscript, and PERL. Developers may create the components to interface with the scripting engine to create new scripting languages.

Server-side scripting provides the structure for ASP. Application developers use scripting to provide input to components and may use a script for simple functions and calculations.

21.2 The Evaluation of Active Server Pages

Active Server Pages is a feature of and can be used with the following Web servers:

N Microsoft Internet Information Server version 4.0 on windows NT Server

N Microsoft Peer Web Services Version 3.0 on Windows NT Workstation

N Microsoft Personal Web Server on windows 95

21.3 The Active Server pages Model

An ASP script begins to run when a browser requests an .asp file from your web server. Your Web server then calls ASP, which reads through the requested file from top to bottom, executes any commands, and sends an HTML page to the browser.

21.4 A Brief History of Hypertext

Active Server Pages (ASP) represents a significant advance in web technology. This section offers a brief history of the Web's evolution from linked static content to the dynamic, interactive environment of ASP.

Linked Static Content

The web's origins lie in linked static content, and many sites today remain static; That is, you must manually edit your HTML pages in order to change what your Web server sends to a browser. In the static model, a browser uses the Hypertext Transport Protocol (HTTP) to request an HTML file from a Web server. The server receives the request and sends an HTML page to the browser, which formats and displays the page. Although this model provides ready access to nicely formatted pages of information for your employees or potential customers, it provides only limited interaction between the user and the Web server-and the static pages must be manually edited to update their content.

Dynamic HTML

Gateway Interfaces such as Common Gateway Interface (CGI), Internet Server Application Programming Interface (ISAPI), and others can be used to add dynamic content to the web. With these interfaces, a browser can send an HTTP request for an executable application rather than for a static HTML file. The server runs the specified application. The application can read information associated with the request to determine what values were passed with request, such as those values that a user submits by filling out an HTML form. The application then parses the values for meaningful information and generates output in HTML to send to the browser. The disadvantage of gateway programs is that they are difficult to create and change. Gateway programs are not integrated into HTML files; in fact, they require an entirely different design process than do HTML files.

Note Although HTTP browsers and servers can transfer data formats other than HTML, such as Audio Video Interleaved (AVI) and Graphic Image Format (GIF), for the sake of simplicity, most of the discussion in this guide refers to content simply as HTML.

21.5 Active Server Pages

N You can use ASP to include executable scripts directly in your HTML files. HTML development and scripting development become the same process, enabling you to focus directly on the look and feel of your web site, weaving dynamic elements into your pages as appropriate. ASP applications are:

N Completely integrated with your HTML files.

N Easy to create, with no manual compiling or linking of programs required.

N Object-oriented and extensible with ActiveX server components.

This translates into tangible benefits, enabling Web providers to provide interactive business applications rather than merely publishing content. For example, a travel agency can go beyond just publishing flight schedules; it can use ASP scripting to enable customers to check available flights, compare fares, and reserve a seat on a flight.

ASP applications are easy to develop because you use ASP scripting to develop them. With ASP scripting, you can use any scripting language for which you provide the appropriate scripting engine. ASP supplies scripting engines for Microsoft Visual Basic Scripting Edition (VBScript) and Jscript. You can incorporate sophisticated functionality using ActiveX server components, formerly known as Automation servers, to process data and generate useful information.

ASP-generated content is compatible with standard Web browsers.

21.6 Benefits of ASP

The primary benefit of using ASP is the ability for a Web developer to provide dynamic content to users. The Web site can deliver content that is customized for that specific user based on user preferences, demographics, customer information, or a more basic criterion, such as whether the user’s Web browser can view content displayed in frames.

The ADO component provides standard access to multiple data sources. Internet Information Server includes drivers for Microsoft SQL Server, Microsoft Access, and Oracle databases. Using ODBC, other databases are supported.

The OLE DB further extents the ODBC standard to permit connection to various data source: Microsoft Excel files, text files, log files, Microsoft Exchange Servers, indexed sequential access method (ISAM), virtual storage access method (VSAM), AS/400, and many other sources.

The Internet Information Server administrator may choose to run all of the applications on the Web server in the same address space for scaling and efficiency. By default, Internet Information Server uses threads within the Web server's address space, instead of creating a new process for each user. The administrator can configure a single application to run in a separate memory space to assure that a problem with one application does not impact the remaining Web applications on the server. Keep in mind, however, that running applications in their own memory space requires additional memory.

ASP provides integrated state and user management. Because HTTP is a stateless protocol, the Web server does not maintain state information about the client. Creating dynamic applications requires state management, which ASP can provide. Through the use of the Application and Session Object, the state of the application is available in both Application and Secession scope. The Application object is a repository for information and objects that are available application wide. In this sense, they are global objects and data. The Session object maintains information on a per-user basis. A separate copy of the Session object is created for each user of the application.

ASP enables developers to reuse software components. Components may also be aggregated. For example, if a component provides 85 percent of the functionality required by an application, the developer may simply capitalize on the functions of that component and only code the remaining 15 percent of the functionality required.

21.7 What is an .asp File?

Active Server Pages (ASP) is built around files with the file name extension .asp. An .asp file is a text file and can contain any combination of the following:

N Text

N HTML tags

N Script commands. A script command instructs your computer to do something, such as assign a value to a variable.

It's easy to create an .asp file: Just rename any HTML file, replacing the existing .htm or .html file name extension with .asp. To make the .asp script file available to web users, save the new file in a web publishing directory (be sure that the associated virtual directory has Execute permissions enabled). When you view the file with your browser, you see the ASP processes and returns HTML, just as before. For more information about web publishing, virtual directories, and setting permissions, refer to your Microsoft web server's online documentation. ASP really begins to work for you, however, when you add scripts to your HTML.

21.8 What is a Script?

A script is a series of script commands. A script can, for example:

N Assign a value to a variable. A variable is a named storage location that can contain data, such as a value.

N Instruct the web server to send something, such as the value of a variable, to a browser. An instruction that sends a value to a browser is an output expression.

N Combine commands into procedures. A procedure is a named sequence of commands and statements that acts as a unit.

Executing a script sends the series of commands to a scripting engine, which interprets and relays them to your computer. Scripts are written in languages that have specific rules; thus, if you want to use a given scripting language, your server must run the scripting engine that understands the language. ASP provides scripting engines for the VBScript and Jscript scripting languages. Your primary scripting language—that is, the language that ASP assumes you are using if you don't specify a language—is VBScript by default.

21.9 ASP Syntax

ASP is not a scripting language; rather, ASP provides an environment that processes scripts that you incorporate into your HTML pages. To use ASP successfully, you need to learn the syntax, or rules, by which it operates.

Delimiters

HTML tags are differentiated from text by delimiters. A delimiter is a character or sequence of characters that marks the beginning or end of a unit.
In the case of HTML, these delimiters are less than (<) and greater than (>) symbols.

Similarly, ASP script commands and output expressions are differentiated from both text and HTML tags by delimiters. ASP uses the delimiters<% and %> to enclose script commands. For example, the command <% sport = "climbing" %> assigns the value climbing to the variable sport

ASP uses the delimiters <% = and %> to enclose output expressions. For example, the output expression <%= sport %> sends the value climbing (the current value of the variable) to the browser.

Single Expressions

You can include within ASP delimiters any expression valid for your primary scripting language. For example, the following line produces text ending with the current server time:
This page was last refreshed at <% = Now %>.
In this case, the Web server returns the value of the VBScript function Now to the browser along with the text.

Statements

A statement, in VBScript and other scripting languages, is a syntactically complete unit that expresses one kind of action, declaration, or definition. The conditional If… Then… Else statement that appears below is a common VBScript statement.

```
<%
If Time >= # 12:00:00 AM# And Time < #12:00: 00 PM# Then greeting = "Good Morning!"
Else
```

```
Greeting  =  “Hello!”
End If
%>
```

This statement stores either the value “Good Morning!” or the value “Hello!” in the variable greeting. It does not send any values to the client browser. The following lines send the value, in green, to the client browser:

```
<FONT COLOR = “GREEN” >
<% = Greeting %>
</FONT>
```

Thus, a user viewing this script before 12:00 noon (in the web server’s time zone) would see

Good Morning!

A user viewing the script at or after 12:00 noon would see

Hello!

Including HTML in a statement

You can include HTML text between the sections of a statement. For example, the following script, which mixes HTML within an If… Then… Else statement, produces the same result as the script in the previous section:

```
<FONT COLOR = “GREEN”>
<% If Time  > =  #12:00:00 AM#   And Time < # 12:00:00 PM# Then %>
Good Morning!
<% Else %>
Hello!
<% End If %>
</FONT>
```

If the condition us true—that is, if the time is midnight or after, and before noon—then the web server sends the HTML that follows the condition (“Good Morning”) to the browser; otherwise, it sends the HTML that follows Else (“Hello”) to the browser.

21.10 Script Tags

The statements, expressions, commands, and procedures that you use within script delimiters must be valid for your default primary scripting language. ASP is shipped with the default primary scripting language set to VBScript. However, with ASP you can use other scripting languages; just use the HTML script tags <SCRIPT> and </SCRIPT>, together with the LANGUAGE and RUNAT attributes, to enclose complete procedures written in any language for which you have the scripting engine.

For example, the following .asp file processes the Jscript procedure
My Function.

```
<HTML>
<BODY>
<% Call My function %>
</ BODY>
</HTML>

<SCRIPT RUNAT = SERVER LANGUAGE = JSCRIPT>
function My Function ()

{
    Response. Write (“My Function  Called”)
}
</SCRIPT>
```

Important

Do not include within <SCRIPT> tags any output expressions or script commands that are not part of complete procedures.

You can include procedure written in your default primary scripting language within ASP delimiters.

Including other Files

Server-side includes is a mechanism you can use to insert Information into a file prior to processing. ASP Implements only the #INCLUDE pre-processing directive of this mechanism. You can use this directive to insert the content of another file into an .asp file before ASP processes the .asp file. Use the following syntax:

<! -- # INCLUDE VIRTUAL /FILE= “file name”→

Where you must type either VIRTUAL or FILE, which are keywords that indicate the type of path you are using to include the file, and filename is the path and file name of the file you want to include.

Included files do not require a special file-name extension; however, Microsoft recommends giving included files an .inc file-name extension to distinguish them from other types of files.

Using the Virtual Keyword

Use the virtual keyword to indicate a path beginning with a virtual directory. (For information about using virtual directories, refer to your Microsoft Web server's online documentation.) For example, if a file named Footer .inc resides in a virtual directory named /Myapp, the following line would insert the contents of Footer .inc into the file containing the line:

```
< ! -- # INCLUDE VIRTUAL = "/MYAPP/FOOTER.INC" – - >
```

Using the File Keyword

Use the File keyword to indicate a relative path. A relative path begins with the directory that contains the including file. For example, if you have a file in the directory Myapp, and the file Header1.inc is in Myapp\Headers, the following line would insert Header1.inc in your file:

```
< ! -- # INCLUDE FILE = "HEADERS/HEADER1.INC"-- >
```

Note that the path to the included file, Headers/header1.inc, is relative to the including file; if the script containing this Include statement is not in the directory/Myapp, the statement would not work.

You can also use the FILE parameter with ../ syntax to include a file from a parent, or higher-level, directory if the Enable Parent Paths registry setting is 1.

Including Files : Tips and Cautions

An included file can, in turn, include other files. An .asp file can also include the same file more than once, provided that the <INCLUDE> statements do not cause a loop. For example, if the file First .asp include the file Second .inc, Second .inc must not in turn include First

.asp. Nor can a file include itself. ASP detects such loop or nesting errors, generates an error message, and stops processing the requested .asp file.

ASP includes files before executing script commands. Therefore you cannot use a script command to build the name of an included file. For example, the following script would not open the file Header1. inc because ASP attempts to execute the #Include directive before it assigns a file name to the variable name.

```
<!—This script will fail -- >
<% name (header 1 &”inc “ ) %>
<!--# include file =” <%= name %> “-- >
```

Scripts Commands and procedures must be entirely contained within the script delimiters <% and %>, the HTML tags<Script> and </Script>, or the HTML tags ,<OBJECT> and </OBJECT> . That is, you cannot open a script delimiter in an including .asp file, then close the delimiter in an included file; the script command must be a complete unit , For example the following script would not work :

```
<!—This script will fail -- >
<%
For I =1 To n
    Statements in main file
< !-- #include file =” header1.inc “-->
Next
%>
```

The following script would work:

```
<%
For I =1 to n
  Statements in main file
%>
<! -- #include file = “header1.inc “-->
<%Next %>
```

21.11 Using a Server Script to Modify a Client Script

Although ASP is used primarily to process server-side scripting , you can extend its reach by using it to generate client-side scripts that are then processed by the client browser. ASP does this by combining client-side scripts that are enclosed by HTML comments with server-side scripts that are enclosed by delimiters:

```
<SCRIPT LANGUAGE =”VBScript”>
<!—
client script
<%server script %>
client script
<%server script %>
client script
…
-->
</SCRIPT>
```

with this functionally in your scripts you can create exciting applications. For example the following script uses a databases to provide a particular client script as a result of the user’s actions .

In the following script ASP retrieves data from the database (in the case ,data pertaining to musical artists and albums and generates a subroutine for each line of data These subroutines then control what happens when a user clicks links in the page displayed in the client browser.

Note This script will not function by itself. It is sown here only to illustrate the functionality of ASP if used in conjunction with a database , server-side scripting, and client –side scripting

```
<! - - This script is incomplete -- >
<%
Set rsAlbums = Server . CreateObject (“ADODB.Recordist”)
rsAlbums .Open “SELECT Artists.*,Albums.* FROM Albums INNER                JOIN
Artists ON  Albums. ArtistID =Artists.ArtestID”, Session (“conn”),1,2
Do while rsAlbums.EOF =False
%>
<SCRIPT LANGUAGE =”VBScript”>
<!—Sub Enhanced _OnLoad( )
Enhanced.DrawBuffer = 500000
End Sub
Sub AlbumHotSpot <%=rsAlbums (“AlbimID”)%>_MouseEnter( )
```

```
AlbumName.Caption=”<%=rsAlbums(“AlbumName”)%>”
ArtistName.Caption =”<%= rsAlbums(“ArtistName”)%>”
Divider.Visible= true
End Sub
Sub AlbumHotSpot<%= tsAlbums(“AlbumID”)%>_click()
Window.Location.HRef = “details.asp ?Albumid=<%= rsAlbums (“AlbumID”)%>”
End Sub - -  >
</SCRIPT>
<%
rsAlbums.MoveNext
Loop
%>
```

Scripts of this kind can be expended to create controls that are associated with the user events .The end result is a robustly generated set of controls with dynamically generated event handlers. By writing scripts such as this , the web developer can create functions and subroutines that manipulate database information, saving time that would otherwise be used writing detailed script procedures.

21.12 Short Summary

1. Microsoft Active Server Pages (ASP) is a serve-side scripting environment that you can use to create and run dynamic, interactive, high-performance Web server applications.

2. In the static model, a browser uses the Hypertext Transport Protocol (HTTP) to request an HTML file from a Web server.

3. Gateway Interfaces such as Common Gateway Interface (CGI), Internet Server Application Programming Interface (ISAPI), and others can be used to add dynamic content to the web.

4. With ASP scripting, you can use any scripting language for which you provide the appropriate scripting engine.

5. The primary benefit of using ASP is the ability for a Web developer to provide dynamic content to users.

6. ASP is built on a scripting engine. This enables it to support multiple scripting languages such as Microsoft Visual Basic Scripting Edition (VBScript), Jscript, and PERL.

7. ASP really begins to work for you, however, when you add scripts to your HTML.

8. ASP is not a scripting language; rather, ASP provides an environment that processes scripts that you incorporate into your HTML pages.

9. Although ASP is used primarily to process server-side scripting , you can extend its reach by using it to generate client-side scripts that are then processed by the client browser.

21.13 Brain Storm

1. What do you mean by Static Model?
2. What do you mean by Dynamic Model?
3. What are the benefits of ASP?
4. What is an .asp File?
5. What is script?
6. What is meant by Delimiters?

Lecture 22

Using Scripting Languages

Objectives

In this lecture you will learn the following

- Writing Procedures with Multiple Languages
- Using VBScript and JScript
- Working with Built –In Objects
- How to send Information to users?
- How to get Information from Users?

Coverage Plan

Lecture 22

22.1 Snap Shot

Scripting languages are an intermediate stage between HTML and programming languages such as Java , C++ , and Visual Basic.HTML is generally used for formatting and linking text. Programming language are generally used for giving a series of complex instructions to computers. Scripting languages fall somewhere in between although scripting languages function more like programming languages than simple HTML docs. The primary difference between scripting languages and programming language is that the syntax and rules of scripting language are less rigid and intricate than those of programming languages. Scripting engines are the COM (Component Object Model)objects that process scripts.

22.2 Using Scripting Languages

Active Server Pages provides a host environment for scripting engines and distributes scripts within. asp files to these engines for processing For each scripting language that is used in coordination with ASP scripting the related scripting engine must be installed on the Web server. for example, VB script is the default language of Active Server Pages, so the VBScript engine resides as an COM object accessible by Active Server Pages so that it can process VBScript Scripts. Likewise , Active Server Page can pr9ovide scripting environment for a number of other scripting languages including Jscript, REXX and Perl and others .Active Server Page makes it possible for the Web developer to write complete procedures by using a variety of scripting languages without having to worry about whether a browser supports them all In fact, several scripting languages can be used within a single.. asp file. This can be done by identifying the script langrage in an HTML tag at the feigning of the script procedure

In addition, because scripts are read and processed on the server side, the client browser that requests the .asp file does not need to support scripting.

22.3 Setting the Primary Scripting Language

VBScript is the default scripting language that is used for primary scripting If you use primary scripting which uses the <% and%> delimiters, you can place any valid VBScript command inside the scripting delimiters and Active Server Pages will process the commands inside of the delimiters as VBScript. Active Server Pages makes it possible to set any scripting langrage as the primmer scripting language, You can set the primary scripting language on a page-by-page basis of for all pages on your web server.

To change the primary scripting language for all pages in all applications, you must change the value of the Default Script Language entry in the registry to that language.

The procedure for setting the primary scripting language depends on whether the chosen language supports Object.Method syntax. The procedures are detailed below

Languages That Support Object.Method Syntax

For languages that support Object. Method syntax and use parentheses to enclose parameters, such as VB Script and Jscript, you can change the primary scripting language for a single page by adding a command lime to the beginning of your .asp file .The syntax for this command is:

<%@ LANGUAGE = Scripting Language%>
where scripting Language is the primary scripting language that you want to set for that particular page.
Follow these guidelines when setting the primary scripting language for a page:

N Set the primary scripting language on the first line of the file

N Do not set the page's primary scripting language in an include file

N Place a space between @ and LANGUAGE

N Do not 0place ant elements other than @ and LANGUAGE = scripting Language between the scripting delimiters(<% and %>)

N If you do not follow these guidelines for setting the primary scripting language for a page, an error will be generated.

Languages That Do Not Support Object. Method Syntax

In order to use a language that does not support the Object.Method syntax as the primary scripting language, you must first create the Language Engines registry key with the corresponding language name sub key and values

```
HKEY_LOCAL_MACHINE \SYSTEM\Current controlSet \Services
\w3svc
\ASP
\Language Engines
\Language Name
value: Write REG_SZ : Response. Write Equiv |
value : Write Block REG_SZ: Response.Write BlockEquiv |
```

where LanguageName is the name of the chosen language, Response. Write.Equiv is the language’s equivalent of Response .write and Response.writeBlockEquiv is the language’s equivalent of Response.WriteBlock . The pope symbol (|) is an insertion used by Active Server Pages to send expressions and HTML blocks that are normally processed with Response.write and Response. WriteBlock methods. This may be dome automatically when installing additional scripting languages.

Note Some scripting languages are sensitive to white space or new line characters; may not be possible to use such languages as the primary scripting language by chang8ing the registry entries as described above An alternative to using these as primary scripting languages is to manually write HTML blocks to the browser rather than using Active Server Pages to automatically handle interleaved <% … %> script directives and HTML. Another option is to write that language’s functions within tagged script blocks (<SCRIPT>…</SCRIPT>) and call them from any other language.

Writing Procedures with Multiple Languages

An attractive feature of Active Server Pages is the capability to incorporate several scripting language procedures within a single .asp With this functionality, you can use scripting languages that have particular strengths to help you get a specific job done.

Creating Procedures

A procedure is a group of scientist commands that performs a specific task. You can define your own procedures and call them repeatedly in your scripts. Procedure definitions can appear within <SCRIPT> and </SCRIPT> tags and must follow the rules for the declared scripting language. You can also define a procedure within scripting delimiters (<% and%>) as long as it is in the same scripting language as the primary script.

You can place procedure definitions in the sane .asp file that xalls the procedures or you can put commonly used procedures in a shared .asp file and use a server-side include statement (that is ,<!-- #INCLUDE FILE=…)to include it in other .asp file that call the procedures. Alternatively you could package the functionality in an ActiveX server component.

Calling Procedures

To call procedures, include the name of the procedure in a command. For VBScript, you can also use the call keyword when calling a procedure. However if the procedure that you are calling requires arguments the argument list must be enclosed in parentheses. If you omit the Call keyword you also must omit the parentheses around the argument list, If you use Call syntax to call any built –in or user-defined function, the function's return value is discarded. If you are calling Jscript procedures from VBScript you must use parentheses after the procedures name; if the procedure has no arguments, use empty parentheses.

The following example illustrated creating and calling procedures by using two different scripting languages(VBScript and J Script)

```
<HTML>
<BODY>
<TABLE>
<% Call Echo %>
</TABLE>
<% Call PrintDate %>
</BODY>
</HTML>
 <SCRIPT LANGUAGE =VBScript RUNAT= Server>
Sub Echo
Response.write
“<TR> <TD>Name</TD>Value </TD></TR>”
Set params = Request. QueryString
For Each p in params
Response.write “<TR><TD>” & - & “ </TD></TR>” &_
Params(p) & “</TD></TR>”
Next
End Sub
</SCRIPT>
```

```
<SCRIPT LANGUAGE= Jscript RUNAT =Server>
Function PrintDate( )
{
var x
x =new Date ( )
Response.Write (x.toString( ))
}
</script>
```

Note To pass an entire array to a procedure in VBScript use the array name followed by empty parentheses ; in Jscript, use empty square brackets.

22.4 Using VBScript and Jscript

When using VBScript on the server with ASP, two VBScript features are disabled. Because Active Server Pages scripts are executed on the server the VBScript statements that present user-interface elements, InputBox and MsgBox, are not supported. The VBScript Functions CreateObject and GetObject are also not supported . Use of these statements will cause an error.

Including Comments

HTML Comments

Because the processing of all ASP scripts is done on the server side, there is no need to include HTML comment tags to hide the scripts from browsers that do not support scripting as is often dome with client-side scripts. All ASP commands are processed before contents is sent to the browser.

VBScript Comments

Basic REM and apostrophe-style comments are supported in VBScript. Unlike HTML comments, these are removed when the script is processed and are not sent to the client.

```
<%
REM This lime and the following two are comments
‘The printable function prints all
‘ the elements in an array.
Call Print Table(myarray( ))
```

```
%>
```

Important You cannot include a comment in an output expression. For example the first line that follows will work, but the second lime will not, because it begins with

```
< %=
<% I= I+1 'this increments i. This script will work %>
<%= name 'this prints the variable name. This script will fail.%>
```

Jscript Comments

The // comment characters are supported in Jscript. These characters should be used on each comment line.

```
<% Call PrintDate %>
<SCRIPT LANGUAGE =Jscript RUNAT =Server>
function PrintDate ( )
{
var x
x=new Date( )
Response. Write (x..getDate( ))
}
//This is a definition for the procedure PrintDate
//This procedure will send the current date to the client-side browser.
</SCRIPT>
```

22.5 Working with Built-in Objects

Script writers often find that they need to accomplish certain tasks in their scripts on a regular basis. For example, you might have a number of scripts all of which ultimately perform different tasks, but all of which need to get information from a user. Objects save you the labor of reinventing the wheel every time you need to perform such a common task. An object is a combination of programming and data that can be treated as a unit .To use most objects, you must first create an instance of that object. However, Active x Server Pages (ASP) includes five objects that do not require instantiation. The following table summarize these built-in-objects, the tasks they are used for and where to look for examples.

Object	Task	Examples
Request Object	Get information from a user	Getting Information from a User
Response Object	Send information to a user.	Sending Information to a User.

Server Object	Control the ASP execution environment	Working with ActiveX Server Components
Session Object	Store information about a user's session.	Developing ASP-Based Applications
Application Object	Share information among users of an application.	Developing ASP-Based Applications.

Object Syntax

The syntax by which you gain access to an object depends on the scripting language you are using. Because the default primary scripting language of ASP is VBScript, the examples that appear in this guides use VBScript Syntax ,except where noted otherwise. If you want to use another scripting language , refer to that language's documentation for the appropriate syntax to work with objects .

The Request and Responses objects contain collections. A collection is a set of related pieces of information that are accessed the same way. You can also gain access to information in a collection by using the For … Each statement. This statement is useful in debugging scripts;

Using Methods

A method is a procedure that acts on an object. The general syntax is
Object.Methods parameters. Where parameters may be a variant, data, a string, or a URL depending on the method.

Using Properties

A property is a named attributes of an object. Properties define object characteristic, such as enabled or disabled. The general syntax is Object.Property parameters. Where parameters may be a value, string, or flag depending on the property.

22.6 Getting Information from a User

Often you want to get information about a user, for example, the type if browser the user is running. You might also want to get information from a user, for example, when the user submits information in forms. The ASP Request built-in object makes getting this information easy.

The Request object gives you access to ay information that is passed with an HTTP request. This includes

N A standard set of information included in the server variable set

N A set of parameters passed with the Post method

N A set of query parameters attached to the GET method

N Cookies that are passed from a browser. Cookies allow a set of information to be associated with a user.

N Client Certificates

The Request object has five associated collections:

N Query String

N Form

N Cookies

N Server Variables

N Client Certificate

You can use the following general syntax to access the information in the Request object:

Request.CollectionName(variable)

Where Collection Name can be QueryString, Form, Cookies , ServerVariables, or ClientCertificate and variable is the name of the variable in the collection that you want to access.

You can use the following general syntax to access variables in the Request object without including the collection name:

Request (variablename)

The collections are searched in this order : QueryString, Form, Cookies, ServerVariables, ClientCertificate. The first variable that matches variablename is returned.

Note If an HTML Page might have more than one variable with the same name, make sure you include the collection name between Request and the variable name.

22.7 Getting Information from HTML Forms

An HTML form is the most frequently used medium for getting information from a web user.A form's text boxes, option buttons and check boxes, displayed on an HTML page in a browser, provide the user an easy way of submitting information. When the user clicks the Submit button, the browser sends the collected or process HTML form values in three ways:

N A static, htm file can contain a form that posts its values to an .asp file.

N An .asp file can create a form that posts information to another .asp file

N An .asp file can create a form that posts information to itself, that is, to the .asp file that contains the form

The first two methods operate in the same way as forms that interact with other gateway programs, except that, with ASP you can include commands that read and respond to user choices.

Creating an .asp filr that contains a form that posts information to itself is a slightly more complicated but very powerful means of working with forms.

Using the QueryString Collection

Although you could use the QUERY_STRING server variable to process QUERY_STRING information from a user request,ASP provides the QueryString Collection to make this information readily accessible. If the form method is POST, the QuertString collection contains all the information passed as a parameter after the question mark in the URL If the form method is GET, the QueryString collection contains all the information passed in the form

For example, when a user sends the following URL request, the Request.QueryString collection would contain two values: name and age

```
<A HREF =”myasp. Asp?name=Charles + Parker&age =30”>
```

The following script uses the Request Object to access these values.

```
Welcome, <% = Request.QueryString(“name”)%>
Your age is <% =Request.QueryString (“age”)%>
```

In this case , the following text would be sent back to the user :

Welcome, charles parker. Your age is 30.

The QueryString collection also automatically handles the case of multiple variables with the same name. When parsing a query string such as name=Andrew &name=Aaron&name=Eric, for example, ASP creates a new collection called name that in turn contains three values: Andrew,Aaron, and Eric.Each of these values is indexed by an integer, with the following results:

Reference	**Value**
Request.QueryString (“name”)(1)	Andrew
Request.QueryString(“name”)(2)	Aaron
Request.QueryString(“name”)(3)	Eric

A Collection created in this manner supports the Count property. The Count property describes how any many items a collection contains.In the example the value of Request.QueryString (“name”) is 3, because there are three separate values stored in the name collection.

If you were to use the Response.QueryString method to gain access to the variable name the output would become a comma-delimited string . In the above example, the value of Request.QueryString (“name”) would be “Andrew, Aaron, Eric”.

Using the Form Collection

The Form collection contains all the values that a user entered in a form submitted with the POST method. For example, when the user fills in and submits the following form:

```
<form action=”/scripts/submit.asp “ methods =”post”>
<p>Your first name : <input name=”firstname” size=48>
<p>What is your favorite ice cream flavor :<select name=”flavor”>
<option>Vanilla <option>Strawberry <option>Chocolate<option>Rocky Road
</select>
```

```
<p><input type= submit>
</form>
```

The following request is sent:

```
Firstname=James&flavor =Racky+Road
```

And the following script is returned by a results page (such as submit .asp):

```
Welcome,<%=Request.Form("firstname")%>
Your favorite flavor is <%=Request.Form ("flavor")%>.
```

Which would result in the following output:

The form collection treats multiple parameters with the same name in the same way that the QueryString Collection does.

Using the Server Variables Collection

The ServerVariables Collection provides information from the HTTP headers that are passed along with a user's request as well as certain Web server environment variables. You ca use this information to provide customized responses to users. This script accesses the SERVER_PORT server variable defined by the Common Gateway Interface (CGI) standard:

This HTTP request was received on TCP/IP port <%= Request ("SERVER_PORT")%>

The following script which provides content based on the user's language, access the HTTP_ACCEPT_LANGUAGE HTTP header variable <% language =Request.ServerVariable

("HTTP_ACCEPT_LANGUAGE")

```
If language ="en" Then %>
<!--#INCLUDE FILE ="myapp/Englishpage.asp"-->
<%Else %>
<!- -##INCLUDE FILE="myapp/Otherlang .asp"-->
<%End If%>
```

Posting Information to the Originating .Asp file

With ASP, you have the flexibility to define a form in an .asp file that posts its input values back to itself ; that is a form that posts values back to the .asp file that contains the form . when a user fills in and submits form values, you can use the Request object to read these values. If you receive an invalid value ,you can send a message back to the user, pointing out the problem and asking for a different value.

If the page that you send to the user contains only a message, the user must return to the page that contains the form. You can save the user this step by sending your message and defining the form again.

If you post form input messages to the same file that originally defined the form, however you can send informational messages along with the content of the form; thus, you need only define the form once.

For example, suppose you define a form the allows a user to submit an email address, and you want to verify that the information a user submits is valid according to your criteria. If the value does not contain @, it is probably incomplete. The following script in GetEmail .asp checks for this. This script is the source of the form, and it include an error message if appropriate.

```
<HTML >
<BODY>
<!—This is Get Email.asp -->
<% If Is Empty (Request(“Email”)) Then
Msg=”Please enter an email address.”
ElseIf InStr (Request(“Email”), “@”) =0Then
Msg =”Please enter an email address”&_
“in the form username@location .”
Else
Msg= “This script could process the “&_
“valid Email address now.”
End If
%>

<FORM METHOS = “POST “ ACTION =”GetEmail .asp”>
<pre>
Email : <INPUT TYPE = “TEXT “ NAME =”Email” size=30
VALUE=”<% = Request (“Email”)%>”>
<% =Msg %>
<p>
<INPUT TYPE =”SUBMIT “ VALUE=”SUBMIT”>
</PRE>
 </FORM>
</BODY>
```

```
</HTML>
```

Using the Cookies Collection with the Request Object

A cookie is a token that either a client browser sends to a Web server, of that a Web server sends to a client browser. Cookies allow a set of information to be associated with a user ASP scripts can both get and set the values of cookies by using the cookies collection . This section discusses be to gain access to cookies a browser sends to your Web Server.

To get the value of a cookie, use the Request.Cookies collection. For example, if the client HTTP request sets animal=elephant, then the following statement retrieve the value elephant.

<% =Request.Cookies (“animal”)%>

If an HTTP request sends multiple values for the same cookie, ASP creates an indexed cookie . Each value is assigned a key ; you ca retrieve a particular cookie key value by using the syntax Request.Cookies (“name”)(“key”). For example, if a client sends the following HTTP request:

Animal = elephant& elephant =African

The following script command returns the value African:
<%= Request.Cookies (“animal”) (“elephant”)%>

22.8 Sending Information to a User

You can use the ASP built-in object Response to control the information you send to a user by using the

N Response.Write method to send information directly to a browser

N Response.Redirect method to direct a user to a URL other than the requested URL

N Response.ContentType method to control the type of content you send

N Response.Cookies method to set cookie values.

N Response.Buffer bmethod to buffer information

Sending Text to a User

The Write method is the most commonly used method of the Response object . You can use the write method to send information to a user from within ASP delimiters Response.write variant

Where variant can be any data type supported by your default primary scripting language. For example, the following statement sends a greeting to the user:

```
<%
If user_has _been _here _ before Then
Response.write “<H3 ALIGN = CENTER >welcome Back to the Overview Page</H3>”
Else
Response.Write “<H3 ALIGN=CENTER >Welcome to the Overview Page </h3>”
End If
%>
```

The Response.Write method is especially useful if you want to send content back to the user from within a procedure.

You do not have to use Response.Write to send content back to the user .Content that is not within scripting delimiter is send directly to the browser, which formats and displays this content accordingly . For example, the following script produces exactly the same output as the previous script:

```
<H3 ALIGN= CENTER >
<% If user _has _ been _here _before  Then %>
Welcome Back to the Overview Page.
<% Else%>
Welcome to the Overview Page.
<% End If %>
</H3>
```

Redirecting a User to Another URL

Instead of sending content to a user, you can redirect the browser to another URL with the Redirect method.

Response.Redirect URL

For example if you want to make sure users have entered your application from a particular page, you can check to see if they have been to that page; if they have not you can send them there.

```
<%
If Not Session (“Been _to _Home_ Page”) Then
Response .Redirect”homepage.asp”
End If
%>
```

Note If you use Response.Redirect from an ,asp file after content has already been sent back to the user, an error message is generated.

Setting the HTTP Content Type

You can user the ContentType property of the Response object to set the HTTP content type strung for the content you send to a user. The general syntax is Response.ContentType =ContentType Where ContentType is a string describing the content type. For a full list of supported content types, see our Web browser documentation or the current HTTP specification. For example, if you want to send source (that is, the .asp file from which an ASP page is generated) to a browser set ContentType to text/plain:

```
<% Response.ContentType=”text/plain”%>
```

The browser then displays the page as text, rather than interpreting the page as HTML.

Using the Cookies Collection with the Response Object

A cookie is a token that either a client browser sends to a web server or a web server sends to a client browser, Cookies allow a set of information to be associated with a user. ASP scripts can both get and set the values of cookies by using the Cookies collection. This section discusses how to set the value of cookies your web server sends to a client browser

To set the value of a cookie , use Response.Cookies. If the cookie does not already exist, Response.Cookies. creates a new <%Response.Cookies ("animal") ="elephant"%>

Similarly , to set the value of a cookie key:

<%Response.Cookies (animal")("elephant")="African "%.>

If an existing cookie has key values but Response.Cookies does not specify a key name, then the existing key values are deleted . Similarly ,If an existing cookie does not have key values but Response.Cookies specifies key names and values, the existing value of the cookie is deleted and new key_value pairs are created.

Buffering Response

The default setting for buffering of all ASP pages is off. However, you can set the Buffer property of the Response object to True to process all of the script on a page before sending anything to the user:

<%Response.Buffer= True%>

You can use buffering to determine at some point in the processing of a page that you do not want to send previous content to a user. You can, instead , redirect the user to another page with the Redirect method of the Response object, or clear the buffer with the Clear method of the Response object and send different content to the user .The following example uses both of these methods.

```
<% Response .Buffer= True%>

<HTML>
<BODY>
.
.
.
<%
If Request("FName")=" " Then
Response.Clear
Response.Redirect"/aspsamp/samples/test.html"
Response.End
Else If
%>
</body>
</html>
```

when you call the Buffer methods in a script and d not call the flush method in the same script, the server will maintain deep-alive requests made by the client , The benefit of writing scripts in this manner is that server performance is improved because the server does not have to create a new connection for each client request (assuming that the server, client and any proxies al support keep–alive requests).However, a potential drawback to this approach is that buffering prevents any of the response from being displayed to the user until the server has finished all script processing for the current .asp file .For long involved scripts, the user might be forced to wait a considerable amount of time before the script is processed.

Buffering is turned off by default for all ASP pages in all applications by setting the BufferingOn registry setting to 0.

22.9 Short Summary

N The primary difference between scripting languages and programming language is that the syntax and rules of scripting language are less rigid and intricate than those of programming languages.

N VBScript is the default scripting language that is used for primary scripting .

N An attractive feature of Active Server Pages is the capability to incorporate several scripting language procedures within a single .asp

N Active x Server Pages (ASP) includes five objects that do not require instantiation.

22.10 Brain Storm

1. How do you create Procedure and call the Procedure?
2. What is meant by Built-In Objects? Explain briefly.
3. Explain the use of Request Object.
4. How do you use Query String?
5. How do you get the Information from the Users?
6. How do you send the Information to the Users?

Lecture 23

Working with ActiveX Server Components

Objectives

In this lecture you will learn the following

- How to Create an Instance of a Component
- About Retrieving Data from a Database
- Developing ASP Based Application
- Using the Session and Application Objects
- Debugging Active Server Pages Script

Coverage Plan

Lecture 23

23.1 Snap Shot-Working with ActiveX Server Components

This section provides an overview of some of the tasks you can accomplish with the ActiveX server components included with Active Server Page (ASP).

ActiveX server components, formerly known as Automation servers, are designed to run on your Web server as part of a Web-based applications. Components package common dynamic features, such as database access, so that you do not have to create and recreate these features.

Components are typically invoked from .asp files. However, you can invoke components from other sources as well, such as an ISAPI application, another server component, and other OLE –compatible languages.

Active Server Pages(ASP) includes five ActiveX server components:

N Database Access Component
N Ad Rotator Component
N Browser Capabilities component
N File Access component
N Content Linking component

23.2 Creating an Instance of a Component

You can create an instance of an ActiveX server component with a single statement. Once you have created an instance of a component, you can use the methods associated with that component, or set and read the component's properties.

The following script uses the Server.CreateObject method to create an instance of the Browser Capabilities component and assigns it to the variable bc:

```
<% Set bc= Server.CreateObject("MSWC.BrowserType")%>
```

You can also use the <OBJECT>tag to create a component instance This example creates an instance of the Ad RotatorComponent:

```
<OBJECT RUNAT =Server ID=MyAd PROGID= "MSWC.AdRotator">
</OBJECT>
```

Note Typically, you use the extended <OBJECT>tag in the Global .asa file to create session-scope or application-scope component instances.

Retrieving Data from a Database

You can use the database Access component to provide access to a database from within your Web application. You can then display the entire contents of a table, allow users to construct queries, and perform other database operations from Web pages

Displaying Advertisements on a Page

You can use the Ad rotator component to display and alternate a series of images, as well as to provide a link from the displayed image to another URL. You keep a list of advertisement in a text file; the Ad Rotator component displays them according to the statements in your data file. The following script, for example, displays an ad when a user requests a page.

```
<%Set Ad = Server.CreateObject ("MSWC,Adrotator")%>
<%=Ad.GetAdvertisement ("/ads/adrot.txt")%>
```

Such a script might produce the following HTML.

```
<A HREF=http://www.msn.com/scripts /adredir.asp?url=http://www.company .com/>
<IMG SRC="http://msnnt3web /ads /homepage /chlogo_lg.gif "
ALT="Check out the new Technology Center "
WIDTH =440 HEIGHT=60 BORDER=1>
</A>
```

Determining Browser Capability

Because of the variety of browsers and browser capabilities on the web, you may want to tailor the content you send to a browser based on the browser's capability component to do this

Reading From and Writing to Files

The File Access component uses the FileSystemObject and TextStream objects to retrieve and modify information stored in files .

Managing Page Navigation

The Content Linking component makes it easy for you to provide logical navigation through the .asp files in an application. Rather than maintaining URL references in a number of .asp files, you can specify the sequential organization of .asp files in a single , easy-to-edit text file .The following example reads the link reads the link order from a text file and creates a table of contents on a single page.

```
<%
Set NextLink =Server.CreateObject(“MSWC .NextLink”)
Count =Next.Link,GetlistCount (“/vroot /Nextlink.txt”)%>
<UL>
<% For i=1 to count%>
<li>
<a href = “<%NextLink.GetNthUrl(“/vroot /NextLink.txt”,i)%>
<%=NextLink.GetNthDescription(“/vroot/NextLink.txt”,I)%>
</a>
<%Next%>
```

23.3 Developing ASP-Based Applications

An ASP-based application consists of a virtual directory on a web server and all the folders and files within that virtual directory .For more information about virtual directories, refer to your Microsoft web server online documentation.

An application can be simple home page; it can include a number of dynamic elements, such as the custom home page of the MSNtm online service (www.msn.com); or it can consist of a complex set of interrelated pages and logic.

When you use ASP-based applications, you are able to maintain state is the ability to retain information. You can use ASP to maintain two types of state:

N Application state in which all information pertaining to an application is available to all users of an application.

N Session state, in which information is available only to a user of a specific session.

The ASP tools you use to manage state are the Session and Application built-in objects.

Using the Session and Application Objects

You can use the ASP built-in objects the Session and Application to extend the functionality of your ASP-based applications .

Use the Session object to manage information for a user when that user is using an application. A Session belongs, in effect, to a single user .The Application object is used to store common information that can shared between all users of a single ASP-based application.

Using the Global.asa file

Each ASP-based application can have one Global.asa file(The file name extension .asa stands for "Active Server Application ") This file must be stored in the root directory of the application. ASP reads a Global.asa file when:

N The Web server receives the first post-startup request for any .asp file in a given application; that is, after the Web server starts , the first request for any .asp file in an application causes ASP to read the Global .asa file for that application.

N A user who does not have a session requests an .asp file in an application.

You can include the following in a Global .asa file:

N Application –start events, session-start events, or both.

N Application-end events, session-ends events or both

Objects tags. You can use the <OBJECT>tag to create objects in a Global .asa file.

Application-Start and Session-Start Events

The application-start and session-start events are Application_OnStart and Session-OnStart ,respectively .You should include in these procedures scripts that you want to run whenever an application or session starts. If an application and a session start at the same time, ASP processes the application-starts event before if processes the session-start event .

Use the following syntax to define an application-start event:

```
<SCRIPT LANGUAGE=VBScript RUNAT=Server>
Sub Application-OnStart
'this is where you would insert script for an application-start event.
End Sub
</SCRIPT>
```

To create an instance of the Ad Rotator component whenever a session starts, you could define the following procedure:

```
<SCRIPT LANGUAGE=VBScript RUNAT=Server>
Sub Session_OnStart
Set Session ("MyAd ")=Server.CreateObject("MSWC.Adrotator")
End Sub
</SCRIPT>
```

Application-End and Session-End Events

The application-end and session-end events are Application _OnEnd and Session-OnEnd, respectively. Like the application-start and session-starts and session-starts events, these events are procedures that you include in a Global .asa file .Unlike start events end events occur only when a session or application ends; thus, you should include u them any scripts that you want to run at those times. If a session and an application end at the same time ,ASP processes the session –end event before it processes the application –end event.

Use the following syntax to define an application-end event

```
<SCRIPT LANGUAGE=VBScript  RUNAT=Server >
Sub Session_OnEnd
This is where you would insert script for a session-end event.

End Sub
</SCRIPT>
```

Use the following syntax to define an application-end event:

```
<SCRIPT LANGUAGE=VBScript RUNAT=Server >
Sub Application _OnEnd
'This is where you insert script for an application ending event.
End Sub
</SCRIPT>
```

Ending a Session

A session automatically ends if a user has not requested or refreshed a page in an application for a specified period of time .This value is 20 minutes by default. You can explicitly end a session with the Abandon method of the Session object . For example, You can provide a Quit button on a form with the ACTION parameter set to the URL of an .asp filr that contains the following command .

```
<%Session.Abandon%>
```

If , for a specific session, you want to set a timeout interval that is longer than the 20 minute default, you can set the timeout property of the Session object. For example, the following script sets a timeout interval of 30minutes.<%Session .Timeout-30%>

Note You cannot set the timeout interval to be less than the default value.

Ending an Application

An application ends when the Web server is shut down.

Managing Sessions

You can use the Session object to set objects or variables to have session scope .Scope is the extent to which a component instance , object or variable is available within Active Server Page .A variable that has session scope , then , is accessible only within that session. A session can begin in three ways:

N A new user requests a URL that identifies an .asp file in an application, and the Global .asa file for that application includes a Session_OnStart

N A user stores a value in the Session object

N A user request an .asp file in an application, and the application's Global.asa file uses the <OBJECT> tag to instantiate an object with session scope.

SessionID and Cookies

The first time a user requests an .asp file within a given application, ASP generates a SessionID , then sends a response to the user's browser to create a cookie for the SessionID. The SessionID is a number produced by a complex algorithm that identifies the user's session. The SessionID cookie is a token sent to a client browser that is not stored in the client computer's hard disk because it does not set an expiration date. Note While most browsers support cookies , some do not . If a user's browser does not support cookies , ASP does not support the Session object for that browser .The SessionID cookie is similar to a locker key in that , as the user interacts with an application during a session , ASP can store information for the user in a locker on the server . The user's SessionID cookie which it sends in the HTTP request header, enables access to this information in the way that a locker key enables access to a locker's contents. Each time that ASP receives a request for a page it checks the HTTP request header for a SessionID cookie.

Storing Variable in the Session Object

You need only reference a New variable in order to create and store the variable in the Session object. For example, the following commands store three new variables in the Session object.

```
<%
Session ("Initiated")=Now
Session("Fidelity")="Low"
Set Session("myobj")=Server.CreateObject("someobj")
%>
```

Remembering User Preferences

You can store user preference in the Session object .For example , you can allow a user to specify a text-only version of your content in the first page of the application and apply this choice on all subsequent pages that the user visits in this application.

```
<%
If Session("Fidelity ")="Low" Then %>
This is the text version of the page.
<%Else %>
This is the multimedia version of the page
<%End If%>
```

Managing Applications

You can use the Application object to set properties that are accessible to every user un an ASP –Based application.

Posting Messages to Application Users

You can use the Application object to post a message that each user of the application sees on entering the application . This section shows an example in which you define an application property called message in an Application_OnStart procedure, then enable subsequent users to modify the message .

The application-wide message is given a default value in Global.asa:

```
<SCRIPT LANGUAGE=VBScript RUNAT=Server>
Sub Application_OnStart
Application ("Message")= "This is the default message."
End Sub
</SCRIPT>
```

A.asp displays the message. Every user who requests A.asp can see the global message.

```
<HTML>
<BODY>
This is the message:<p>
<%= Application ("Message")%>
</BODY>
</HTML>
```

B.asp provides a way for a user to type a new message and submit the change.

```
<HTML>
<BODY>
```

```
<Form method =”post” action=”C.asp”>
Enter a new value for the application-wide message:<br>
<input type = “text” name=”newmsg” size=60> <p>
<input type=”submit” value =”submit”>
</form>
</BODY>
</HTML>
```

C.asp resets the global message to the value received from a user in B.asp and respects the user to A.asp to see the new value.

```
<%
If Not IsEmpty (Request,Form(“newmsg”)) Then
Application.Lock
Application (“Message”)= Request.Form(“newmsg”)
Application.Unlock
End If
Response.Redirect(“A.asp”)
%>
```

23.4 Setting Component Scope

An ASP-based application can set ActiveX server components to have application, session of page scope.

N An application-scope component instance is a single instance of a component that is created when the application starts. This instance is shared by all client requests .

N A session-scope component instances is created for each mew session in an application and released when the session ends; thus , there is one instance per active session.

N A page-scope component instance is created for the processing of a page for one client; it is available through the processing of that page; and is then released when the response is sent back to the client. A component instance has page scope by default.

You can declare component instances with session or application scope in a Global .asa file by using the <OBJECT>tag, extended with RUNAT attribute (which must be set to Server) and SCOPE attribute(which can be set to session or application)You can accomplish this by using either the registered name (PROGID) method or the registered number (CLASSID) method.

The following example uses the registered name (PROGID) method to create a session-scope instance of the Ad Rotator Component:

```
<OBJECT RUNAT=Server SCOPE=Session ID =MyAd PROGID =”MWSC.Adrotator”>
</object >
```

The following uses the registered number(CLASSID), method to create an application –scope instance of the Ad RotatorComponent:

```
<OBJECT RUNAT=Server SCOPE=Application ID =MyAd
CLASSID =”Clsid :00000293-0000-0010-8000-00A06D2EA4”> </OBJECT>
```

When you declare a session –scope or application-scope instance of a component by using the <OBJECT> tag, the variable you assign to the component goes into the session of application namespace, respectively.This means that you do not need to use the Session of Application built –in objects to access the component instance .For example, the following script command, issued from within any .asp file that is part of the Ad Rotator component declared in those examples :

```
<%=MyAd .GetAdvertisement (“addata.txt”)%>
```

You can also use the <Object>tag to create ActiveX server component instances in a particular .asp file. In this case the SCOPE attribute can be omitted or set to PAGE. All such component instance have page scope.

Using the Server.CreateObject Method

You can use the Server.CreateObject method to store an instance of a component in the Session object. The following example stores an instance of the Ad Rotator Component in the Session object.

```
<%Set Session (“MyAd ”)=Server.CreateObject(“MSWC.Adrotator”)%>
```

To display an ad, you would include the following :

```
<%set MyAd = Session(“MyAd”)%>

<%=MyAd.GetAdvertisement(“addata.txt”)%>
```

Performance Issues

ASP does not instantiate a component that you declare with the <OBJECT> tag until that components referenced by a script from an .asp file .The Server.CreateObject method instantiates the component immediately. Thus the <OBJECT> tag offers better performance than the Server.CreateObject

Method offer equivalent performance

You can use the <OBJECT> tag to store single –threaded , free-threaded or apaerment-0threaded objects in both Session and the Application objects. you can use the Server.CreateObject method to store single-threaded free-threaded and apartment-threaded objects in the Session object. However, whether you use the <OBJECT> tag or the Server.CreateObject the method , unless the object of store is marked "both "ASP treats the application or session containing this object as "single –threaded ".Thus , storing objects that are not marked "both "may have performance implications, particularly for high –volume sites.

23.5 Debugging Active Server Pages Scripts

When you write out a script both technical and syntactical accuracy are required .Inaccuracy may prevent a script from running properly and may generate error messages. The process of resolving these messages is called debugging ,Thoroughly testing your scripts and debugging them if necessary , insures that all users who visit your web site will get the intended experience rather than an error message .

Error messages are sent back as HTML with all or some the following information, depending upon the nature of the error:

N The scripting language in which the error occurred.
N The error number
N A short description of the error.
N The name of the .asp file.
N The line number where the error occurred.
N Along description of the error and a possible fix for the error.

Note Using a text editor that displays lime numbers will help you locate a line with an error in your .asp file.

Use this information to modify .asp files so that errors can be resolved. Errors of a severe nature will be sent to the Windows NT log and the Internet Information Server (IIS)log, as will as to the client browser. All other will be sent to the IIS log and client browser

Error Handling with VBScript

The On Error Resume Next Statement

If an error is encountered in your .asp file, the processing of your script stops and an error message is returned to the browser. If you want to continue processing your page even if an error is encountered , include the following line at the beginning of your .asp file:

<%On Error Resume Next%>

Note The On Error Resume Next statement is a VBScript statement; it affects only scripts written in VBScript .Using this statement within an .asp file containing Jscript will have no effect pm Jscript error debugging because JScript has no functional equivalent of resuming after an error. If you call a Jscript function from VBScript and the JScript function causes an error , an error message is returned to the browser and processing of the .asp file stops at that point.

Using the On Error Resume Next statement does not actually clear an error ; to manually cleat the error , you can use the Err.Clear method:

```
<HTML>
<HEAD>
<TITLE>Error Handling with an Error Resume Nextand Err.Cleat</TITLE>
</HEAD>
<BODY>
<%
Call DoSafeDivide(1,3)
Call DoSafeDivide(1,0)
%>
<SCRIPT LANGUAGE=”VBScript” RUNAT=Server>
        Sub DoSafeDivide(x,y)
```

```
      On Error Resume Next
       Z=x/y
       If Err.Number>0 Then
Response.Write(“Division failed: “ & x & ” / ” & y & ”<BR>)
Response.Write (“Error Source:”&Err.Source & “<BR>”)
Response.write(“Error number: “&Err.Number &”<BR.”)
Res[pmse.Write(“Error description:”&Err.Decscription&”<BR>”)
Err.Clear
Else
Response.Write (“Division succeeded: “& x & ” / ” & y & ” = ” & z & ” <br>”)
End If
End Sub
</SCRIPT>
</BODY>
</HTML>
```

The For …Each Statement

You can use the For …Each statement to iterate over a collection , thus simplifying your debugging process by returning all of the variables ot a collection in a script .For example, the following script sample uses the For …Each statement with the QueryString collection of the Request object to return all values for all keys in the QueryString collection.

```
=<br>
There are values for.<br>
Value is <b></b><br>
VBScript errors can generate a pointer which indicates the exact location of the error in the script code:
Microsoft VBScript compilation error ‘800a03f3’
Expected ‘=’
/ASPSamp/Samples /outstrem.asp, line11
Set OutStream Nothing
-----------------^
```

Error Handling with JScript

The following scripting mistakes commonly result in errors for JScript:

N Misspelling of terms

N Incorrect capitalization (JScript is case-sensitive)

N Unmatched pairs of brackets, parentheses and single and double quotation marks.

Always check for these types of errors when debugging JScript.

Debugging Forms

If you are receiving variables in the QueryString collection of the Request

Object that should be in the Form collection, make sure that the HTML <FORM> tag is setting METHOD-POST The GET method passes form variables into the QueryString collection .The POST method passes form variables into the Form collection.

23.6 Short Summary

N ActiveX server components, formerly known as Automation servers, are designed to run on your Web server as part of a Web-based applications.

N You can create an instance of an ActiveX server component with a single statement.- Server.CreateObject.

N The File Access component uses the FileSystemObject and TextStream objects to retrieve and modify information stored in files.

N An ASP-based application consists of a virtual directory on a web server and all the folders and files within that virtual directory.

N You can use the ASP built-in objects the Session and Application to extend the functionality of your ASP-based applications .

N You can use the Application object to post a message that each user of the application sees on entering the application .

23.7 Brain Storm

1. Writer short notes on Creating an Instance of a Component.
2. How do you develop ASP-Based Application using Session and Application Objects?
3. What do you mean by Component Scope?
4. How can you debugging the ASP Scripts?

Lecture 24

Understanding Microsoft Transaction Server

Objectives

In this lecture you will learn the following

- About Microsoft Transaction Server
- About Three –Tier Architecture
- About MSMQ

Coverage Plan

Lecture 24

24.1 Snap Shot

Microsoft transaction Server simplifies the application development process. With it, you can deploy scaleable server applications built from Microsoft ActiveX components. This lesson provides an overview of how Microsoft Transaction Server works.

Microsoft Transaction Server delivers the component – including transactions scalability services, connection management, and point –and –click administration that makes it possible for you to build and deploy scaleable applications. Microsoft Transaction Server uses a simple programming model. The basic pattern is always the same: the client requests a Component Object Model (COM)object running under Microsoft Transaction Server Control. This permits Microsoft Transaction Server to create an object context and associate it with the object. When the work is dome, the object either calls Set complete to indicate success or calls Set Abort to indicate rollback.

24.2 Transaction

A Transaction is a unit of work that succeeds or fails as a whole. Transaction are a way to coordinate a series of changes made to a resource or sets of resources. The most common type of transactions handle this coordination through a central point called a resource manager

These actions have what are known as ACID properties ,ACID is an acronym that stands for Atomicity, Consistency, isolation, and Durability.

N Atomicity- Either all changes happen or none happen .Atomicity refers to the fact that a single transaction has an all-or-nothing behavior. An example of this is a bank account transfer ,When you withdraw money from your checking account and deposit it into your savings account you expect the transaction to be atomic, that is, completed as a whole.

N Consistency-Actions taken as a group do not violate any integrity constrains. Consistency ensures that, in the preceding example, the deposit-withdraw pair does not violate any rules or integrity constraints ,such as transferring more than $200 on any business day, or overdrawing your checking account.

N Isolation –For actions that execute concurrently , one is either executed before or after the other , but not both. Isolation ensures that, if two people share a joint checking account and they are both moving money transaction waits for the other money transaction to be completed. If the account contains $200 ,each individual does not withdraw the only $200 at the same time.

N Durability – Changes survive failures of process, network, operating system, and others. Durability ensures that if the Automatic Teller Machine (ATM) that you are withdrawing money from experiences a power failure in the middle of the transaction, the $200 in bills that you receive is ensured to be debited from the account.

24.3 Microsoft Transaction Server Components

There are four major categories of Microsoft Transaction Server services. First, there is an Object Request Broker (ORB). When a call comes into a server and requests an object, the ORB handles this call, checks for availability, and ultimately gives the requestor an object.

Next, a Transaction Processing Monitor (TP Monitor) is, in simplest terms, an environment that inserts itself between the clients and the server resources so that it can mange transactions, mange resources, and provide load balancing and fault tolerance. The typical TP Monitor model does not acknowledge other objects. It only knows how to handle requests in the most efficient means possible.

Microsoft Transaction Server combines Object Request Brokering and TP Monitoring using the Distributed Component Object Model (DCOM) as the main element. Microsoft Transaction Server uses the Microsoft Distributed Transaction Coordinator (DTC) as the TP Monitor.

In a typical process, requests for objects come in by means of DCOM; Microsoft Transaction Server processes the requests, efficiently allocates server resources, and begins a Distributed Transaction Coordination transaction. It then returns this object to the client. The client then uses the object to perform its intended function. Microsoft Transaction Server resides between the object and the client, and monitors all client actions. By doing this, it is acting as a TP Monitor and, as result, can perform the duties of the TP Monitor. For example, it can schedule requests and pool resources during idle time. When the client is done with the object, the client releases the object which causes Microsoft Transaction Server to complete the transaction and free or pool the resources.

24.4 Three-Tier Architecture

Three-tiered applications, where the application server, client computer, and data source can be separated from each other, provides more deployment flexibility than two-tiered client/server programming, where application code is location-dependent. The three-tier architecture consists of:

N Presentation. The client application consists mostly of a graphical user interface (GUI). Services such as database connections and business services are obtained from middle-tier servers. This results in less overhead for the user, but more network traffic for the system as components are distributed among different computers.

N Business/Data Components. Middle-tier components can implement data rules or business rules. Business rules can consist of rules to keep the data structures consistent, within a specific database as well as among multiple databases. These can exist on a server computer to assist in resources sharing. They can be used to enforce business and data rules. Because they are not tied to a specific client, they can be used by all applications.

N Data Access. This is the actual database management system (DBMS) access layer. It can be accessed through the data/business rules layer, and on occasion by the GUI itself. It consists of data access components (rather than raw DBMS connections) to aid in resource sharing and to allow clients to be configured without installing libraries or drivers on each client.

No matter which kind of presentation interface is used, it is important to remember that all applications consist of the same basic pieces. A three-tier architecture is a logical architecture, and does not imply that you need to use three different computers. In other words, there is no required correspondence between the logical layers of a three-tier architecture and the physical topology of your network. How the pieces of an application are distributed may change, depending on the system requirements.

In a typical Client/Server environment it is deemed best to acquire resources early and hold them for the duration of the application. Although the amount the amount of time that these resources were in use was small in comparison to the time the resources were performance. Resource utilization was a secondary consideration.

24.5 MSMQ

Microsoft Message Queue Server (MSMQ) can act as a Microsoft Transaction Server resource manager. It permits asynchronous transport through an enterprise-wide queuing system. It enables scalability, because transaction-processing systems such as Microsoft Transaction Server do not have to depend on all resource managers being available all of the time, or the transaction response being dependent on the slowest resource manager. Messages can simply be queued for future delivery. MSMQ offers ActiveX support, dynamic routing and configuration, multiple delivery and acknowledgment options, and integration with Microsoft Windows NT Security facilities.

24.6 ASP Integration

Internet Information Server 4.0 integrates Active Server Pages (ASP) technology and Microsoft Transaction Server. The ASP technology built into Internet Information Server makes it possible to apply the client/server model to Web-based applications. This means you obtain faster responses to queries and less network traffic. ASP has been extended further to accommodate scaleable three-tier applications. Active Server pages are now based on Microsoft Transaction Server. This means ASP applications can run in separate address spaces for reliability and security. A transaction cannot span multiple ASP pages. You should make sure to group objects on one ASP page if a transaction requires objects from several transactional components.

24.7 Components of a Transaction

A component is a discrete unit of code build on ActiveX technologies that delivers a well-specified set of services through well-specified interfaces. Components provide the objects that clients request at run time.

24.8 Short Summary

- A Transaction is a unit of work that succeeds or fails as a whole.
- There are four major categories of Microsoft Transaction Server services.
- In a typical Client/Server environment it is deemed best to acquire resources early and hold them for the duration of the application.
- Microsoft Message Queue Server (MSMQ) can act as a Microsoft Transaction Server resource manager.

24.9 Brain Storm

1. Give an Overview about MTS?
2. What is meant by Transaction?
3. Explain the term ACID?
4. What is the need of Three-Tier Architecture?
5. Explain MSMQ.

℘End☙

Manonmaniam Sundaranar University

Centre for Information Technology

Tirunelveli

Syllabus for MS(IT&EC)

2.2 E-Commerce Concepts and Application Design

Lecture 1

Electronic Commerce: (An Overview)- What is E-Commerce ? - Basic E-Commerce Concepts - Various Services- Operating System Services - Developer Services - Data Services - Application Services - Store Services - Client Services

Lecture 2

Types of Electronic Commerce Solutions - B2B - B2C - Direct Marketing & Selling - Supply Chain Integration - Corporate Procurement - Major Projects in Electronic Communication

Lecture 3

Applications of Electronic Commerce – Introduction - Value Chain Integration - Supply Chain Integration - Corporate Purchasing - Financial purchasing and Information Services - Examples of Today's E - commerce

Lecture 4

E-Commerce opportunities with www/internet – E-Commerce tools - The Model of Commercial Transactions.

Lecture 5

Handling Money On the Net and Security Requirements: Confidentiality of payment information – Integrity of payment information – Account holder and merchant authentication – Interoperability. - Payment and Purchase order Process: Overview – Customer (Account holder) registration – Merchant registration – Customer Ordering – Payment Authorization.

Lecture 6

On-line E-Cash: Transaction on the Internet – Problems with simple E-Cash – Creating E-Cash Anonymity – Preventing Double spending – E-Cash Interoperability.

Lecture 7

Types of Electronic Payments: Netscape's Secure Courier E-Payment Scheme, Microsoft's STT – CheckFree – CyberCash – VeriSign - DigiCash – NetCash – OpenMarket – Global On-line – NetBill - Credit Cards – E-Checks – Joint E-Payment Initiative(JEPI).

Lecture 8

Security Technologies - Cryptography - Digital Signatures - Digital Envelops - Digital Certificates - Certificate Authorities

Lecture 9

Encryption - Encryption Keys - Conventional Encryption - The Data Encryption Standard - Commercial Communications Security Endorsement Programme - Key Distribution - Public Key Encryption

Lecture 10

Internet Working with TCP/IP - Introduction - Origin of TCP/IP - TCP/IP Communication Architecture - Internet Architecture - How TCP/IP works? - What TCP was Built to do? - From One Socket to Another - TCP Sequencing - TCP Needs Not an IP

Lecture 11

Internet Working with TCP/IP - What is an IP? - Gateways and IP - TCP/IP Applications - File Transfer Protocol(FTP) - Telnet - Trivial File Transfer Protocol - Simple Mail Transfer Protocol - Network File System

Lecture 12

TCP/IP Implementations - Finger Protocol - Whois Protocol – Gopher – Veronica – Archie - WAIS : Wide Area Information Servers – Ping - WWW:World Wide Web - X Window System - The X Terminal - The X Window System

Lecture 13

Net work Security and Firewall - Security in TCP/IP Networks - LAN Security - What Network Security Means - Risk Analysis - Types of Threats - Passive Threats Active Threats - Determining what secure means to you and your LAN - Securing workstations and servers – Securing network passwords - Securing Files and Programmes

Lecture 14

Level of Security - Physical security - Access Controls - Personal Identification – Passwords - Security in Log-In -Online coders - The Diskless Pc - Protection against Cable Radiation Call-Back Security - Management-Level Concerns

Lecture 15

Electronic Data Interchange (EDI) - Use of EDI - Evaluation of EDI Benefits of the EDI Process -How EDI Works?

Lecture 16

EDI standards - Motivation - Cost benefit Analysis of EDI - Beyond EDI : Electronic Trading Networks

Lecture 17

EDI Components - File types – Internal Format file, External format files, Transmission file - EDI Services - Application service - Translation Service - communication service

Lecture 18

Choosing EDI Value Added Network(VAN) - Choosing EDI Software - Business approach to EDI - Need for change - Rational for EDI - EDI is a business issue - Developing an EDI plan

Lecture 19

Reengineering For Electronic Commerce - Enterprise resource planning - Evaluation of ERP - Characteristics of ERP - Features of ERP - Components of ERP - Need of ERP - ERP Vendors - Business process reengineering - Evaluation Criteria for ERP packages - Implementation Approach of ERP - The Future of ERP systems

Lecture 20

Information technology plan for ERP system - Enabling Best Technology Practices - Information Technology Assessment - Reviewing the Information Technology Plan - Reviewing Organization - Reviewing Service Level - Reviewing Project Mix - Reviewing Technology portfolio

Lecture 21

Getting Started With Active Server Pages - The Evolution of Active Server Pages - Understanding How Active Server Pages Really Work-The Active Server Pages Model-A brief history of Hypertext –Linked Static Coneten- Dynamic HTML- Active Server Pages- Benefits of ASP -Writing ASP Scripts – What is na .asp file? –What is a Script?- ASP Syntax- Single Expressions-Statements-Script Tags- Including Other Files-Using a Server Script to Modify a Client Script.

Lecture 22

Using Scripting Languages- Setting the Primary Scripting Language- Writing - Procedures with Multiple Languages –Using VBScript and Jscript - Working with Built-In Objects-Object Syntax-Getting Information from a User-Getting information from HTML Forms- Sending Information to a User- Sending Text to a User-Redirecting a User To Another URL- Using the Cookies Collection with the Response Object – Buffering Response.

Lecture 23

Working with ActiveX Server Components-Creating an Instance of a Component- Retrieving Data from a Database-Displaying Advertisements on a Page- Determining Browser Capability –Reading from and Writing to Files – Managing Page Navigation –Developing ASP- Based Application – Using the Session and Application Objects- Setting Component Scope- Debugging Active Server Pages Script.

Lecture 24

Understanding Microsoft Transaction Server - Microsoft Transaction Server Components - Three-Tier Architecture – MSMQ - ASP Integration - Components of a Transaction - Component-Based Programming.

Lecture 25

Case Study

Lecture 26

Case Study

Lecture 27

Case Study

Lecture 28

Case Study

Lecture 29

Case Study

Lecture 30

Discussion

Best of Luck