MAR GREGORIOS COLLEGE OF ARTS & SCIENCE

Block No.8, College Road, Mogappair West, Chennai – 37

Affiliated to the University of Madras
Approved by the Government of Tamil Nadu
An ISO 9001:2015 Certified Institution

DEPARTMENT OF COMPUTER APPLICATION

SUBJECT NAME: E-COMMERCE

SUBJECT CODE: SEZ6B

SEMESTER: VI

PREPARED BY: PROF. J.SUMITHRA DEVI

Title of the Course/ Paper	**E-COMMERCE**		
Elective	**III Year & SixthSemester**	Credit: 4	
Objective ofthe course	This course gives an exposure to the Electronic Commerce		
Course outline	Unit-1: Electronic Commerce and Opportunities : Background The Electronic Commerce Environment – Electronic Marketplace Technologies – Modes of Electronic Commerce: Overview : Electronic Data Interchange.		
	Unit-2:. Approaches to Safe Electronic Commerce . Overview – Secure Transport Protocols – Secure Transaction – Secure Electronic Payment Protocol(SEPP) – Secure Electronic Transaction (SET)		
	Unit-3:. Certificates for Authentication – Security on Web Servers – Payment Schemes: Internet Monetary Payment and Security Requirements- Payment and purchase order process – Online electronic cash.		
	Unit-4:.Internet / Intranet Security Issues and Solutions : The Need for Computer Security – Specific Intruder Approaches – Security Strategies- Security Tools – Encryption – Enterprise Networking and Access to the Internet Antivirus Programs.- Security Teams		
	Unit-5: MasterCard/Visa Secure Electronic Transaction : Introduction –Business Requirements – Concepts – payment Processing. E-mail and secure e-mail technologies for Electronic Commerce: Introduction _ The Means of Distribution – A model for Message Handling- MIME, S/MIME, MOSS , MIME and Related Facilities for EDI over the Internet.		

Recommended Texts:

Daniel Minoli & Emma Minoli, “Web Commerce Technology Handbook”. TataMcGraw Hill – 1999.

Reference Book:

1.K.Bajaj & D Nag , “E-Commerce”, Tata McGraw Hill – 1999.2.Mamta Bhusry – “E-Commerce”

UNIT-I

E Commerce Environment and Opportunities

Background

- Internet change the way of business.
- In the past few years, access to the internet has been increasing 8% per month.
- Business have been looking for ways to increase their profit and market share since antiquity.
- The development of money was one of the key milestones.
- More recently, paper money came into use, as the transaction of large amounts of coins became inconvenient.
- Even more recently, plastic money has become popular, further enhancing buyer's and seller's convenience.
- During the past century, the telegraph, the telephone, fax and electronic mail have provided faster, cheaper and more reliable ways of communicating business information within and between commercial entities.
- The search for more efficient ways of doing business is now driving another revolution in the conduct of business and in our concept of money. Thisrevolution is known as electronic commerce, which is any purchasing or sellingthrough an electronic medium.
- Electronic commerce is the symbiotic integrations of communications, data management and security capabilities to allow business applications within different organizations to automatically exchange information related to the saleof goods and services.
- Security mechanism authenticate the source of information, guarantee the integrity of the information received ,prevent disclosure of the information to inappropriate users and document that the information was received by the intended recipient.
- Existing standards, technology and the systems for Electronic Data Interchange (EDI) enables fast ,accurate and compact exchange of basic formalized businesstransaction between different automated information system ,EDI requires rigid agreements about the structure and meaning of data.
- Electronic payment methods and smart cards can make the process of buying and selling quicker, easier and more convenient, for merchants and consumers alike.
- An advanced national electronic commerce capability will be comprised of interconnected communications network, advanced computer hardware and software tools and services established business transaction and interoperabilitystandards, accepted security and privacy provisions and suitable administrative practices.
- This infrastructure will enable companies to rapidly, flexibly and securely exchange and more important use information to drive their business processes.

Basic Web Commerce Concepts

- Consumers are now being offered the opportunity to shop electronically or shopover the internet.
- The World Wide Web is one of the more prominent applications supported bythe Internet.
- The idea of doing business electronically is not a product of 1990's;however ithas recently gained popularity among entrepreneurs and business executives ,since the launch of the so-called information superhighway ,formally known asthe National Information Infrastructure (NII) and the recent use of th Internet,asmeasured by users.
- ECommerce encompasses several methods of connecting buyers and sellers including advertising, product demonstration, catalogs and directories.
- Web commerce is one of the battery of on-line services that consumers may ultimately be

interested in.

- Electronic Commerce in general and Web Commerce in particular different from traditional commerce in the way of information is exchanged and processed.
- Traditionally, information has been exchanged through direct, person-to-person contact or through the use of the telephone or mail system.
- In electronic commerce information are conveyed via a communication network, a computer system or some other electronic media.
- Electronic Commerce pulls together a gamut of business support services, including inter-organizational e-mail, on-line directories, trading support systems for commodities, products, customized products, and custom-built goods and services; ordering and logistic support systems; settlement support systems;and management information and statistical reporting systems.
- Electronic Commerce includes electronic marketing as a subdiscipline.
- The defining characteristic of electronic marketing is interactivity,where a marketer establishes two-way communication with a customer in what is called an asynchronous domain.
- An electronic market place therefore is the digital environment or locale where a marketer presents these promotional messages and where a potential buyer canpurchase a marketer's products or services and request more information.
- The following list the principle opportunities available through web commerce are
  - Usage fees paid to internet providers.
  - Content fees paid for information downloading.
  - Advertising fees.
  - Transaction processing fees.
- The following list the objectives of electronic commerce
  - Exchange procurement informations such assolicitations,offers,contracts,purchase orders,invoices, payments and other contractual documents, electronically between the privatesector and the federal government to the maximum extent practical.
  - Provide businesses, including small, disadvantaged and women owned businesses with greater access to federal procurement opportunities.
  - Ensure that potential suppliers are provided simplified access to the federal government's electronic commerce system.
  - Employ nationally and internationally recognized data formats that serve to broaden and ease the electronic interchange of data.
  - Use agency and industry systems and netwoks to enable the government and potential suppliers to exchange information and access federal procurement data.
- The following assumptions about electronic commerce are advanced by industry.
  - New media technologies will become an integral part of cosumer homes and business offices.
  - Marketers will continue to spend resources on their electronic marketing efforts.
  - On-line services will continue to contribute as the largest percentage of electronic marketplace transactions until the turn of the century.
  - Within the on-line industry segment ,transaction revenues generated by business-to-business on-line services will outspace consumer on-line services in the near-term future.
  - The Internet's share of the electronic marketplace will grow more rapidly over the next five years than any other media,as security standards are put in place.
  - The fraction of electronic marketplace sales generated by other means such as kiosks,

CD-ROM’s ,and screen phones will remain fairly static through the turn of the century.

The Electronic Commerce Environment The Virtual Corporation

- Electronic Commerce is the essence of the virtual corporation:it allows the organization to leverage information and communication resources with all its constituencies ,including employees,customers,bankers,governmentagencies,suppliers,advertisement agencies,and the public.
- Successful companies for turn-of-the-centuary environments
  - Organizational structures of the past:vertical corporations where every function was performed in house.
  - Organizational structure of late 1980’s:horizontally integrated enterpriseswhere core competencies were performed in house and the rest was outsourced.
  - Organizational structure of late 1990’s:corporations are moving towardbeing fully integrated and virtual.
    =>Aim at making all business functions world-class in order to enhancevalue.
    =>Access to all world’s best of breeds, skills, knowledge and resources.
    =>Use combination of insourcing and outsourcing to create best of breedend-to-end solutions.
    =>Overcome distance and time barriers.
    =>The future is a network centric model where the corporation is thenetwork paradigm is supreme.
    =>Connectivity and bandwidth are becoming cheaper and easy to secure.

- **Figure represents IT evolution**

- Network may be comprised of

(1) a traditional enterprise network - The physical foundation of corporation communication

(2) an intranet-overlay on enterprise network which is a way to build uniformapplication on client and server

(3) the internet-the enterprise network par excellence

(4) specialized networks-other inter- company network sometimes called asextranets

(5) international extension-synthesis of communication facilities calledomninet.

- Internet technology like TCP/IP, HTTP,HTML,browsers,servers can be usedfor both internal nad external applications.

The Electronic Marketers

- Electronic Marketers are defined as companies that market their products andservices to other businesses or consumers through private online network s , commercial online services such as Prodigy and America online(AOL),the internet,CD-ROMs ,interactive TV and web TV and floppy disk media.
- E_Commerce frees retailers and consumers from many store constraints.
- A website can deliver products quickly or in a few days;a retail store can deliver products within a few hours or within a few days.

The catalyst of E_commerce and web commerce

- The growth and impact of PC was not as strong in view of some observers.
- The PC changed society and its penetration experienced a high growth rate for years but in recent times the internet is experiencing rampant growth in the range of 50 to 100 percent a year.
- WWW is one of the well-known application of the internet.
- Press-time studies indicate that
    - □ 90% of people using web services do so to browse or explore.
    - □ 70% search for other information.
    - □ 60%search for information on companies/organizations.
    - □ 55% search for information on products and services.
    - □ 13% purchase products and services.
    - □ 15%forpersonaluse.
    - □ 10% for academic usage.
- Internet today defined in terms of size and reach, is the largest ,most used datanetwork of all.
- There are three components of internet today
    - □ (1)A multitude of access/deliver sub networks all over the country.
    - □ (2)A dozen or so national interconnected backbones
    - □ (3)Thousands of private and/or institutional networks.
- Access services are provided by Internet Service Providers (ISP) whilebackbones are provided by Network Service Providers (NSP).
- The key to the internet’s potential is its ability to interactively communicateinformation.

Available communication apparatus

- E-Commerce clearly depends on the availability of reliable, inexpensive andubiquitous connectivity.
- **The Electronic Commerce Environment – Broad View**
- In this context there are five relevant elements
    - □ Organization’s own networks which house appropriate information usually beyond the organization’s firewall apparatus.
    - □ The public switched telephone network. This is generally constituted of Local Exchange Carrier (LEC) and competitive LEC’s (CLEC)at local level and a multitude of Interexchange Carriers(IXC) at national backbone level.
    - □ The internet consist of ISP and NSP provides a large inter-enterprise infrastructure.
    - □ Online networks such as AOL which utilize their own communication and information facilities. They can beaccessed bydial-up or private lines andnow have access to the internet.
    - □ Specialized industry networks, such as those to support EDI.

Application of electronic/web commerce

- E_Commerce combines the advantages of computer based processing like speed,reliability,and relatively high volumes of data with the advantages of people based insight like creativity,flexibility,adaptability.
- E_Commerce enables to review,analyse,add value and sell a variety of products that are represented electronically such as reference material,text books and training materials,entertainment and softwares.
- There are three tiers in th electronic marketplace offering opportunities for companies of all types.

□ Tier 1 : Electronic classified advertisements, which identify the item for sale, the price and information necessary for contacting the seller.

□ Tier 2 : Includes the characteristics of the first tier but adds decision support materials to the information available which helps the user reach a purchase decision.

□ Tier 3 : Include the features of the first two tiers but adds the ability to electronically match appropriate buyers and sellers.

- ➢ Applications of electronic commerce includes the following

□ EDI:-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.

□ Enterprise Integration:-Extending integration throughout a company including other trading partners.This results in virtual corporation provides vertical integration of company with suppl,ier and horizontal integration of company.

□ Computer Supported Collaborative Work:-Expanding collaborative activities such as supporting joint development of requirements, maintenance documents and so forth within or across companies.

□ Government Regulatory Data Interchanges:-Collecting data from various communities to enable the government to carry out its mandated responsibilities.

- ➢ Other select examples include the following

□ Books:-www.amazon.com

□ Travel Services:-www.usair.com

□ Automobile Specifications:-www.autobytel.com

□ Flowers:-www.800flowers.com

□ Computers:-www.cnet.com

□ EDI Services:-www.premenos.com

□ Advertising Services:-www.modemmedia.com

□ Magazines:-www.salon1999.com

□ Banking and investing:-www.americanexpress.com

□ Internet Shopping Malls:-www.commercenet.com

Benefits of electronic/web commerce

- ➢ The benefits of electronic commerce includes the following

□ Reduced cost to buyers from increased competition in procurements,as more suppliers are able to compete in an electronically open marketplace.

□ Reduced cost to suppliers by electronically accessing on-line data bases of bid opportunities by on-line abilities to submit bids and by on-line review of awards.

□ Reduced errors,time and overhead costs in information processing by eliminating requirements for reentering data.

□ Reduced inventories as the demand for goods and services are electronically linked through just in-line inventory and integrated manufacturing techniques.

□ Increased access to real-time inventory information, faster fulfillment of orders, and lower costs due to the elimination of paperwork.

□ Creation of new markets through the ability to easily and cheaply reach potential customers.

□ Improved market analysis.

□ Rapid information access.

□ Rapid interpersonal communications.

□ Cost-effective document transfer.

Elements of successful electronic marketplace

- The capabilities required for internet/web commerce are as follows
  - □ Enable buyers to inquire about products, review products and service information, place orders, authorize payments and receive both goods and services on-line.
  - □ Enable sellers to advertise products, receive orders, collect payments, deliver goods electronically and provide ongoing customer support.
  - □ Enable financial organizations to serve as intermediaries,that accept payment authorization make payment to sellers and notify buyersthat transactions arecomplete.
  - □ Enable seller to notify logistics organizations electronically as to where and when to deliver physical goods/merchandise.
- The following qualities characterize in the view of industry experts,successful marketplace.
  - □ Utilizes an exizting customer base.
  - □ Makes an existing marketplace more effective.
  - □ Brings together communities.
  - □ Is easily accessible, has window distribution.
  - □ Offers decision support information.
  - □ Ability to close the sale.
- Two trends impact this market
  - □ The ease of supporting the electronic delivery of information.
  - □ The difficulty for existing computer distribution channels of handling the gamut of computer products from both new and existing marketers.

Security issues and approaches related to Web Commerce

- Many of the concerns about e_commerce developments ,particularly over open networks deal with the risk of possible fraud, security infractions, counterfeiting and with consumer privacy issues.
- Issues relate to

  (1) Secure payments via e_cash.

  (2) Confidentiality and authentication of financial transactions.

  (3)General confidentiality in the transfer of any document.
- Encryption refer to the encoding of data so that it can only be decoded only by the intended recipient who knows the key.
- Each key performs a one-way transformation of data—what one encrypt and other can decrypt.
- The issues relating to security are
  - □ Secure Payments

    *E_Cash can be thought of as the minting of electronic moneyor tokens.

    *In electronic schemes,buyers and sellers trade electronic value tokens which are issued or backed by third party,be it an established bank or a new institution.

    *An article in the Nov26,1994, issue of The Economist foresaw potential for privately issued electronic currencies to compete with or supplant official state currencies ,with no legalized exchange rate into legal tender,other than what themarket dictates.

    *The effects of a system failure in an electronic cash scheme are much harder to anticipate,system failure could also occur through many means not the least of which is insufficient funds to back up the new electronic money.
  - □ Secure Transactions

    *Agreements on standard Internet Payment systems were getting closer at press time.

    *During 1996,IBM/Master card and Microsoft/Visa respectively agreed on a single industry standard for conducting credit card transactions over the internet.

*The issue has been which technology to use,Microsoft’s Secure Transaction Technology(STT) or IBM’s SEPP;the breakthrough came when the four companies agreed to use SET based on SEPP work.

*SEPP is a protocol originally developed by Master card ;IBM,Netscape,GTE, and cybercash have also signed to further develop the protocol specification.

*The development of electronic commerce is at a critical juncture at this time for the following reasons

=>Consumer demand for secure access to electronic shopping and otherservice is high.

=>Merchants seek simple ,cost effective methods for conducting electronic transactions.

=>Financial institutions look for a level playing field for softwaresuppliers tgo ensure quality products at competitive prices.

=>Payment card brands must be able to differentiate electronic commercetransactions without significant impact to the existing infrastructure.

*Master card International published a new draft of secure electronic transactions in August 1996.It consists of three books namely

=>Book 1:-Bussiness specification

=>Book 2:-Technical specification

=>Book 3:-Formal Protocol Definition

*The solution is based on establishing a trusted link between the internet anda traditional banking entity.Three services are available

=>credit card ,electronic cheque,and electronic coin which are the counter parts to credit card ,check,and low-denomination cash payments.

*Other efforts include but are not limited to the following

=>The internet society launched an initiative called the Internet Mercantile Protocol(IMP) to develop set of standards and practices in support of electronic commerce.

=>Master card and Visa both have electronic commerce projects based onsmart cards.

□ Message Transfer Confidentiality and Authentication

*Basic issues of secure payments ,there are several fundamental technologies being developed to secure transaction(confidentiality)of any kind of internet/intranet-resident information .

*Two different protocols have been developed for enhanced web security:S_HTTP(Secure Hyper Text Transfer Protocol) and SSL(Secure Socket Layer).

□ S-HTTP

*S_HTTP is an extension of HTTP that provides a variety of security enhancements for the web.

*Message protection is provided in three ways:Signature,authentication andencryption.

*Any messages can use any combination of these three methods.

*Authentication is performed using digital certificates issued by certificationauthorities.

*Encryption makes data transferred over the network unintelligible tointruders and eavesdroppers.

*S-HTTP provides independently applicable security services for transaction confidentiality,authenticity/integrity and nonreputability of origin.

*Digital Signature provide two benefits

=>first,they verify that data transferred over the network was not changeden route.

=>second,they provide nonrepudation where the receiver of data canprove to a third party that the sender really send the data.

*S-HTTP is flexible in that it allows each application to configure the level of security required.

*A transmission from client-to-server or server-to-client can be signed ,encrypted, both or neither.

*S-HTTP provides a secure communication mechanism between an HTTP client/server.
*The protocol provides symmetric capabilities to both client and server while preserving the transaction model and implementation characteristics of HTTP.
*Several cryptographic message format standards may be incorporated intoS-HTTP clients na d servers.

*A secure HTTP message consists of a request or status line followed by a series of headers followed by an encapsulated content.

□ SSL

*SSL is a transport layer security technique that can be applied to HTTP as well as to other TCP/IP based protocols.
*The SSL protocol is designed to provide privacy between two communicating applications ,for example client and server.

*SSL provides authentication,encryption and data verification.
*The protocol is designed to authenticate the server and optionally the client but encryption and data verification are mandatory with SSL.

*The SSL protocol is actually composed of two protocols .
*Layered on top of some reliable transport protocol,is the SSL encapsulation of all transmitted and received data,including the SSL Handshake protocol,which is used to establish security parameters.
The advantages of the SSL protocol is that it is application-protocol- independent.
*A higher level application protocol (HTTP,FTP,Telnet)can run transparently on top of the SSL protocol.
*All of the application protocol data is transmitted encrypted,ensuring privacy.
*SSL is a cryptosystem that works at the protocol level and provides authentication,encryption and data integrity.

*SSL requires a reliable transport protocol such as TCP.
*Security process begins when the client sends a request to connect to the server.

*The server transmits a digital certificate to the client.
The client authenticates the server by decrptying the digital signature that iswith the digital certificate.
*The client generates a session key and encrypts it using the server's publickey from the certificate.
*The server receives the session key and uses it to encrypt and decrypt thedata.
*SSL uses message authentication codes to ensure the data transferredbetween client and server has not been tampered with.

*If any of these steps fails,the connection between client and server is closed

□ Comparison of S-HTTP and SSL

S-HTTP	SSL
Application level protocol	Transport level protocol
Digital signature available	No Digital signature
Able to work with firewall	Hides firewall
Flexible to configure security	Not Flexible
Expensive	Low Expense compared to S-HTTP

Size of the electronic marketplace

- Some estimates that the potential market for electronic commerce could be aslarge as $500 billion per year,although the current figures are much smaller.
- Revenue was generated from several potential media – business on-line ,consumer on-line ,Internet ,CD-ROM,Kiosks,screen phones and interactivetelevision.
- Electronic Marketplace Transaction By Media (in $ millions)

Elements	1996 Estimate	Market Share %
Bussiness on-line	324	60
Consumer on-line	161	30
Internet	32	6
CD-ROM	15	3
Kiosks	5	1
Screen Phone	3	0
Interactive Television	0	0
Total	$540	100

- Bussiness on-line which includes such services as Data Transmission Network (DTN)services and AutoInfo,represented the largest percentage of electronic transactions at press time.
- The second marketplace segment is Consumer on-line which includes CompuServe’s Electronic Mall and other services delivered through proprietarynetworks.
- The third largest ,the Internet is just beginning to generate transactional revenueas of press time.

Electronic Marketplace Technologies

- Each of the possible electronic commerce media identified in the previous section has distinct advantages and disadvantages that limit or improve its potential in creating an effective electronic marketplace

Electronic Data Interchange

- EDI is the well defined business transactions in a computer processable format.
- EDI provides a collection of standard message formats to exchange data betweenorganizations computers via any electronic service.
- EDI covers traditional business facets as inquiries,planning,purchasing,acknowledgements,pricing,order status,scheduling,test results,shipping and receiving ,invoices ,payments and financial and business reporting .
- Additional standards cover interchange of data relating to security, administrative data,trading partne rinformation, specifications, contracts, production data,distributionand salesactivities.

On-line networks and services

- On-line services provides access to information, entertainment, communications and transaction services.
- This term refers to networks by companies such as America Online,CompuServe,and prodigy.
- The public switched-telephone network is the typical distribution system ;cable networks,satellite,wireless networks,and the unused portion of FM radio and broadcast TV signals may also be used.
- It also includes other specialized networks.
- The on-line environment presents challenges as well as opportunities to a varietyof marketers.

- This method has not become a widely accepted way of supporting electronic commerce.
- The main advantages of on-line networks is their ability to offer timelyupdated information,communication capabilities such as electronic mail,bulletin boards and real time chat and supplementation of core materials with limited multimedia.
- Another advantage is that private on-line networks are more secure than the Internet,and therefore can support on-line credit card purchases.
- Other advantages of the mall approach include lower prices ,since cost to build the storefronts are shared among a group of marketers.
- The drawback is that individual storefronts can prove to be more expensive.

The Internet:Web Commerce

- The fastest growing part of the internet at this time is the world wide web.
- Users may purchase information that interest them by using a browser,such as Netscape Navigator or Microsoft Explorer and exercising the links embedded in the parent document recursively under their current consideration.
- The Internet offers an extensive and demographically attractive potential audience ,especially for business-to-bissiness marketers.
- With its large and quickly growing audience ,the Internet provides a variety of mechanism to access information and transfer information including WWW ,electronic newsletters, Gopher, File Transfer Protocol(FTP) and Wide Area Information Server(WAIS).
- Spam is the term used to describe a company that posts unwelcomingadvertising messages to as many newsgroup as it can.
- The market will explode within the next to 5 to 10 years
- Press time salary ranges are as follows
  - □ Intranet Researcher:$25 to $40,000.
  - □ HTML Programmer:$35 to $65,000.
  - □ Content Specialist:$27 to $60,000
  - □ Web Designer:$42 to $75,000
  - □ WebMaster:$46 to $77,000

CD-ROMs and hybrids

- The multimedia and storage capabilities of CD-ROMs and the growth in the penetration of CD-ROM drives in both business and home PCs are the reasons why business-to-business and consumer marketers sought to use the CD-ROM as a marketing vehicle in the recent past.
- CD-ROMs can store large amounts(650 MB or more) of data in text and/or graphical form.
- CD-ROM provides the ability to add sound,photos and full-motion video to a marketing interaction beyond what is offered by the online medium over the telecommunication link.
- Because of their cost-effectiveness,CD-ROM catalogs,with the products of either one or multiple marketers have become popular.
- There are number of advantages to the CD-ROM medium over online and the internet.
- First,CD-ROMs can store a large amount of data, making them a portable medium for storing large databases of products as well as for storing multimediamaterial.
- Secondly,because CD-ROMs are standalone entities ,they can more conspicuously stand out from the large amounts of information already on-line and especially on the internet.
- CD-ROM based commerce however has a number of disadvantages.
- Consumers at large are still relatively unfamiliar with PC technology for buying goods and services compared to the use of other home appliances,such as the telephone and television.

- The CD-ROM is also limited by the fact that it is a time-static medium,meaningonce the disk is pressed,the information it contains cannot be updated.
- A typical software CD-ROM catalog carries between 30 and 150 software programs in encrypted form ,which means that users can sample the software before they make a purchase.

Screen Phones

- Screen Phones are similar to regular telephones but have advanced features suchas credit card readers small screen phones and keypads that can be used for a variety of interactive ,transactional and informational services.
- Typical services include home banking,home shopping and electronic white pages.
- This technology is used more commonly in Europe Where consumers can get up-to-date information on many things from a list of specialty restaurants to traininformation.
- The screen phone’s primary advantage for electronic commerce is that it is basedon a device that consumers are familiar with and are comfortable using.
- Their future is uncertain, especially if low-cost entry devices become popular.

Kiosks

- Kiosks are displays used to provide merchandise information in a remotelocation such as retail store or a shopping mall.
- Kiosks employ a variety of technologies to deliver multimedia marketing information.
- Most kiosks allow the consumer to order products directly from the unit by usinga magnetic credit card reader,touch screen or keypad.
- Kiosks’ primary advantages are their large storage storage capacityand multimedia capabilities including full-motion video,sound,graphicsand text.
- Kiosks have not proven to be an effective medium to support transaction basedinteractions.
- Multimedia kiosks can cost anywhere from $10,000 and $50,000 per unit.

Interactive Television and Video Dial Tone

- The television is a ubiquitous electronic home appliance.
- Interactive Television enables consumers to view advertising about specific products and place orders through the television screen using a remote control and a special set-up box attached to the cable television line into the home.
- Interactive Television is delivered via braosdband networks and can support the highest quality multimedia marketing and advertising information of any other medium.
- Creating digital advertising and shopping services for interactive television hasproven costly for marketers.
- One of the advantage of interactive TV would be narrowcasting of advertisements to the subscribers based on their viewing habits.
- It will probably take atleast five years into the next decade before there will bemuch video dial tone penetration on the part of the RBOCs.
- At the same time,the cable TV companies are upgrading their networks tosupport more interactive services including internet access.

WebTV

- A new technology called WebTV by some and intercasting by others was seeingdeployment at press time.
- This approach is yet another vehicle for electronic commerce.
- Intercasting is a technology developed by Intel that intertwines WWW pages with TV broadcasts.

- Television signals contains pauses,called vertical blanking intervals(VBI)to allow for the electron beam that creates the picture in the cathode ray tube(CRT)to move from the bottom of CRT to the top of CRT.
- The only new component needed to make this work is an intercast chip to decodethe broadcast webpages.
- Decoder boxes now cost about $300 ,it should be realized however that the VBIinformation is one way only:it is a receive mechanism.,
- The received web pages would typically contain background information aboutthe broadcast.
- It appears that initially this service will be targeted at residential customers.

Interactive Banking

- Many banks are offering another form of electronic commerce known asinteractive banking.
- This generally refers to methods that allow their customers to conduct some oftheir bank business over the phone or with the PC.
- Using a Touch-Tone Telephone customers can check their account balances,paybills,order statements and so forth.
- Home banking has been offered for over a decade with mixed results.
- The near-term future of home banking is unclear at this time.
- Banks without branches are now available on internet.

Modes Of Electronic Commerce

Overview

Electronic commerce

- Commerce is the interchange of goods and services especially on a large scale.
- Over the centuries and decades ,trading has continued to become no longer done face-to-face,but are conducted over a telephone or via mail ,with the exchange of new plastic money.
- Traditionally money is typically backed by the federal government and most typically comes in paper form.
- There are other forms of money and payments that have been introduced in the last century:checks,credit cards,and other forms of payment orders.
- Factors that impact the way commerce has matured relate to the increase in the speed and scope of communication in both actual movement of people and merchandise.
- Financial service activities such as home banking,brokerage,insurance and bill paying will be generally available in the near future.
- The major difference between the way in which the electronic commercehas been conducted until now and the way it is now proposed to operate relates to aparadigm shift:moving from using a closed private network ,in which two partieshave previously established some type of agreement,to utilizing an open publicnetwork such as internet,without any prior knowledge of the buyer.
- The internet and the ancillary e-commerce software allow transactions betweenparties that do not previously known each other.
- Electronic information can be delivered cheaply because there is no need for packing,trucks,warehouses;subscribers simply pay the cost to access the market.
- The largest cost components of merchandise are not the costs of raw goods but of the purchasing,shipping,receiving,and the inventory processes.

- The electronic commerce transactional models vary between proposedofferings,each having a different level of attractionor detraction depending on the industry and level of acceptable risk.
- Financial risk has increased in recent years due to changes in payment and the forward rate at which items are purchased.
- One of the key question pertaining to risk is how can two or more unknown parties exchange money over an open ,unsecured network without a highpotential for fraud.

Some Open Issues

- There are traditional concerns about credit card fraud and blank embezzlement.
- The potential for high-volume fraud and automated fraud is greater in e-commerce with the introduction of public network computerized transactions.
- Protecting intellectual property rights becomes a problem when digital duplication is easy and fast ,leading to the proliferation of pirated copies.
- Methods to ensure that cardholder's payments are safely made ,that merchant's information is retained as confidential,and that banks maintain a high degree of security over protected funds are issues that must be addressed and solved.
- Mechanisms to pay for goods and services to on-line merchants and the introduction of new products and services add an additional degree of financial risk to sending financial information across public networks.
- The confidential transmission of data,authentication of the parties involved and ensuring the integrity of order data and payment instructions for goods and services are all components of the new electronic business model.
- Some open issues related ti e-commerce

Taxation	When a merchant collects sales tax ,which rateshould the customer be charged.
Customs	The ability to purchase and import certain types of information goods might be subject to customsregulations.
Regulation	Government bodies,regulators enforce restrictionswhich invade privacy or hinder security
Fraud	When e-cash is fully deployed ,What are the legal protections?
Security	Authentication,nonrepudiation,accountability,andphysical delivery are all handled differently under the e-commerce approaches now in place.

Electronic Data Interchange

- EDI is defined as the interorganization exchange of documents in standardizedelectronic form directly between computer applications.
- EDI can be thought of as the replacement of paper-based purchase orders withelectronic equivalents.
- Example for paper exchanging
  - Documents originate in the sender's computer.
  - Print them in forms.
  - Sent via mail or fax.
  - Receivers are forced to reenter the information.

- Disadvantages are
  - Slow
  - Inefficient
  - Error prone
- Example for EDI exchange
  - The business documents are moved electronically from the sender's computer application to the receiver's application.
  - Besides application-to-application communication ,ideally one wants dataina standard format so that users do not have to deal with each other's internal data formats.
- Goals of EDI
  - Goal is to enable easy and inexpensive communication of structured information throughout the corporate community.
  - EDI can facilitate integration among dispersed organizations.
  - EDI goal is to reduce the amount of data capture and transcription ;this results in a decreased incidence of errors ,reduced time spent on exception handling and fewer data cause delays in the business process.
  - Benefits can be secured in inventory management ,tramsport and distribution,administration,and cash management.
  - In addition,faster handling of transactions results in increased cash flow.
  - The early applications of EDI were undertaken in the United States.
  - In 1968,the United States Transportation Data Coordinating Committee(TDCC) was formed to coordinate the development of translation rule among four existing sets of industry-specific standards.
  - A significant move toward standardization was realized with the X12 standards of the American National Standards Institute(ANSI),which gradually extended and replaced those created by the TDCC.
  - At the same time,the U.K Department of customs and excise was developing standards for documents used in international trade.
  - These were later extended by the United Nations Economic Commission for Europe(UNECE) into what became known as the General purpose trade data interchange(GTDI) standards.
  - Harmonization between the two different sets of standardized documents has been addressed with the formation of a United Nations Joint Europeanand North American working party (UN-JEDI),which began the development of the EDI for administration,commerce,and transport(EDIFACT) document translation standards.
  - Today,EDI messages are coded in a standard data format governed by X12 and EDIFACT specifications.
  - The key aspects of EDI are as follows:

    □ The utilization of an electronic transmission medium rather thanhe transfer of physical storage media such as paper,magnetic tapes and disks.

    □ Use of structured ,formatted messages based upon agreed standards.

- □ Relatively fast delivery of electronic documents from sender to receiver.
- □ Direct communication between applications.

EDI’s Benefits

- ➢ Business can secure many benefits when utilizing EDI.
- ➢ Investment will be necessary in order to achieve lower costs,and planning and control is needed to ensure that the savings are actually realized.
- ➢ Cost savings arise in relation to the preparation,postage,and handling of mainstream transactions or in secondary but expensive areas such as the preparation and dispatch of applications for approval by a regulatory authority or other reporting functions.
- ➢ The major benefits is the elimination of rekeying the data.
- ➢ The receiver needs not reenter the information from a paper form;keypunchingerrors are avoided and the accuracy of the data increases.
- ➢ EDI also eliminates other paper-handling tasks.
- ➢ Benefits can arise from reduced exceptions handling.
- ➢ With EDI ,data need to be captured only once.
- ➢ With EDI,organizations exchange business documents more quickly ,resultingin a shorter business cycle.
- ➢ EDI can positively impact customer service factors,such as the incidence oferrors and the timeliness of deliveries.

Status

- ➢ The technologies underlying EDI have matured and the economies of EDI applications have improved to the point that an increasing number of organizations are seeing opportunities for cost savings,improved service andcompetitive advantage.
- ➢ EDI has been growing in the recent past,although the penetration is still low.
- ➢ Roll-out cost factors include the following
  - Reaching a legal agreement between the parties regarding responsibilities and dispute settlement.
  - Building and installing the EDI system.
  - Modifying and interfacing with the existing computer system.
  - Obtaining network services.
  - Testing and installation.
  - Reengineering internal processes with the goal of taking full advantages of the technology.
  - Training.

System Approach

- ➢ There are a number of ways in which computers can be set up to support EDI.
- ➢ A single dedicated PC can be used as the company’s link to the outside world.
- ➢ Types of software packages that would make up an EDI terminal on a PC includethe folloeing:
  - Application Software

- Message Translator
- Routing Manager
- Communication Handler

- Using a PC with a dial-up modem is an easy way to start using EDI.
- Software is available that provides all the necessary EDI functions,such as the communications protocol and the EDI message translator.
- The function of the routing manager may be included in the software so that communication links are established automatically whenever a data exchange isrequired.
- Client/Server systems can also be utilized :one computer handles EDI communications,while another supports the applications which create the information to send or use the information which is received.
- It is possible to print the messages so that the information can be handled as if it had been received on paper.

Communication Approach

- Although dial-up is an entry-level mode approach to using this technology,sophisticated applications of EDI require a more elaborate communication infrastructure.
- The VAN networks used by companies in a conventional EDI environment are limited in functiontionality and scope.
- There are only a small number of companies one can reach and interact with.
- The VAN market has been growing at an annual rate of 12 percent per year.
- The original definition of a VAN (Virtual Area Network) was a telecommunications network,primarily for data,which processed or transformed data and information in some manner,and thereby provided services beyond simple transport of information.
- Carriers have covered most major markets of the world in order to service themultinational corporation.
- The companies that provide VAN services include IBM,British Telecom Tymnet,CompuServe,EDS and GE Information Services.
- VAN-based EDI and electronic commerce in the past has not been based on interoperability and open communication system.
- Users have not been satisfied with VAN providers making it possible to send EDI messages from one network to another and are worried that the VANs are not expending enough effort on the set up phase with other users.
- Pricing VAN services is not a trivial task,because as technology changes ,the balance of power between users and service providers changes.
- VANs were forced in the early 1990s to abandon volume-sensitive pricing in the United States,as organizations started to build private networks.

- Making the transition has been more difficult in overseas markets because PPTs(post,telegrapg,and telephones)control the VANs in particular and the telecommunications market in general.

- VAN has also responded to competition by adding services including supportfor
  - TCP/IP-Protocol for internet
  - SNA-Protocol for mainframe and minicomputers.
  - IPX-Used only for LAN multimedia services.

- The Federal Electronic Commerce Action Team has led the way in showing how interoperability of VANs can be simulated by providing a gonernment-built system which interfaces to many VANs so that government generated Requests For Quatotions(REQ)can be equally distributed to many networks.

- This means less pressure toward interoperable netwoks.

UNIT-II

Approaches to Safe Electronic Commerce

Overview

- Business activity grows on the Internet, security is becoming an important consideration.
- Security relates to three general cases
  - Secure file / information transfers.
  - Secure transactions.
  - Secure enterprise networks, when used to support web commerce.
- Computer security has several fundamental goals
  - Privacy:-Keep private documents private , using encryption, passwordsand access-control systems.
  - Integrity:-Data and applications should be safe from modification withoutthe owner's consent.
  - Authentication:-Ensure that the people using the computer are theauthorized users of that system.
  - Availability:-The end system (host) and data should be available whenneeded by the authorized user..
- Secure Commerce Requirements

Requirement	Description
Content Security	The ability to send information across the internet in a manner in which unauthorized entities are not able to read the contents.
Signature	The ability to specifically identifythe entities associated with the information.Things may be signed are contents, messages etc..
Content Integrity	The ability to identify modificationto the covered information.
Nonrepudiation of Origin	The ability to identify who sent the information originally versus which intermediary forwarded it.
Nonrepudiation of Receipt	The ability to identify that the information was received by the final addressed destination in a manner that cannot be repudiated.
Nonrepudiation of Delivery	The ability to identify whether the information was delivered to an appropriate intermediary in a manner if cannot repudiate.

Key Management	The functionality necessary to create,distribute,revoke,and manage the public/private keys.

Secure Transport Protocols

- The Secure Socket Layer system from Netscape Communications and theSecure Hyper Text Transfer protocol from CommerceNet offer secure means oftransferring information through the internetand the WorldWideWeb.
- SSL and S-HTTP allows the client and servers to execute all encryption and decryption of web transactions automatically and transparently to the end user.
- SSL works at the transport layer and it is simpler than S-HTTP which works at the application layer and support more services.

Secure Hypertext Transfer Protocol (SHTTP)

SHTTP extends the HTTP internet protocol with public key encryption, authentication, and digital signature over the internet. Secure HTTP supports multiplesecurity mechanism, providing security to the end-users. SHTTP works by negotiating encryption scheme types used between the client and the server.

Secure Electronic Transaction

It is a secure protocol developed by MasterCard and Visa in collaboration. Theoretically, it is the best security protocol. It has the following components −

- **Card Holder's Digital Wallet Software** − Digital Wallet allows the card holder to make secure purchases online via point and click interface.
- **Merchant Software** − This software helps merchants to communicate with potential customers and financial institutions in a secure manner.
- **Payment Gateway Server Software** − Payment gateway provides automatic and standard payment process. It supports the process for merchant's certificaterequest.
- **Certificate Authority Software** − This software is used by financial institutions to issue digital certificates to card holders and merchants, and to enable them to register their account agreements for secure electronic commerce.

S-HTTP

- S-HTTP is a secure extension of HTTP developed by CommerceNet Consortium.
- S-HTTP offers security techniques and encryption with RSA(Rivest Shamir's Adlemen)methods along with other payment protocol.
- S-Http supports end-to-end secure transcations by incorporating cryptographic enhancements to be used for data transfer at the application level.
- S-HTTP incorporates public-key cryptography from RSA data security in addition to supporting traditional shared secret password and Kerberos-based security systems.
- The RSA data security ciphers used by S-HTTP utilize two keys;files encrypted by one can only be decrypted by application of the other key.
- A company generates a pair of these keys publishes one and retains the other.

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

SSL

- The Secure Socket Layer protocol developed Netscape Communications is asecurity protocol that provides privacy over the internet.
- The protocol allows the client/server applications to communicate in a waythatthe data transmissions cannot be altered or disclosed.
- Servers are always authenticated and clients are optionally authenticated.
- The technology has support for key exchange algorithms and hardware tokens.
- The strength of SSL is that it is a application-independent.
- HTTP, Telnet and FTP can be placed on top of SSL transparently.
- SSL provides channel security (privacy and authentication) through encryptionand reliability through a message integrity check (secure hash functions).
- SSL uses a three-part process
    - First, information is encrypted to prevent unauthorized disclosure.
    - Second,the information is authenticated to make sure that the informationis being sent and received by the correct party.
    - Finally, SSL provides message integrity to prevent the information frombeing altered during interchanges between the source and sink.
- SSL depends on RSA encryption for exchange of the session key and client/server authentication and for various other cryptographic algorithms.
- SSL requires the merchant to use the Netscape server software and the buyer touse the Netscape browser software.
- SSL becomes more widely deployed and implemented, this restriction shouldgo away.
- Netscape has also developed Secure Courier, which uses SSL to allow financialdata to be transmitted in a secure digital envelop.

Alternatives

- The good news is that the SSL and S-HTTP standards are converging into a single standard which will accommodate both protocols making the use of encrypted credit card transactions even easier to implement.
- A related capability is a certification authority to authenticate the public keyson which the RSA system relies.
- The goal is to assure users that a public key that seems to be associated with acompany actually is and is not a spurious key.
- The authority requires applicants to prove their identity .

- Those passing the test are issued a certificate in which the applicant's publickey is encrypted the authority's private key.
- An alternative to internet on-line credit card transactions is the use of digitalcash.
- Digital cash is a system by which on-line shoppers trade real dollars for internetcredits to pay for goods and services.
- Digital coins can easily be stolen or faked,which reduces the risk for both thebuyer and seller.

Secure Transactions

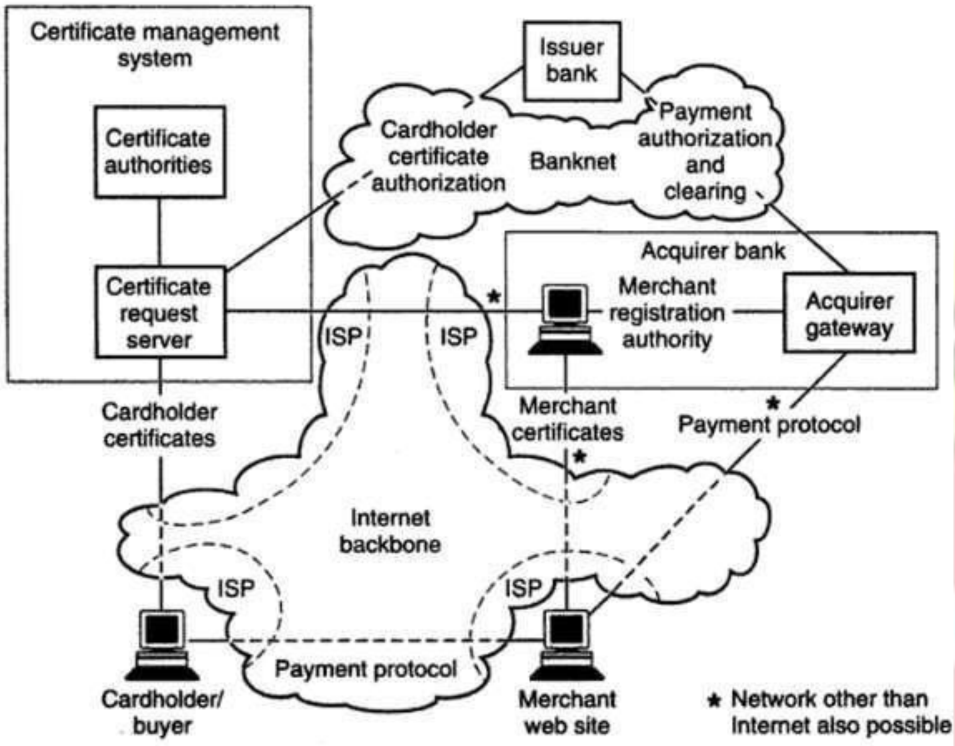
- Three methods have evolved in the recent past.
- Netscape Communications Corporation and Microsoft Corporation have promoted their respective payment protocols and installed them in World WideWeb browsers and servers.
  1. SEPP has been championed by MasterCard and Netscape and by the other supporters ;the American National Standards Institute(ANSI) is fast-trackingSEPP as a standard for the industry.
  2. STT was developed jointly by Visa and Microsoft as a method to secure bank card transactions over open networks.STT uses cryptography to secure confidential information transfer ,ensure payment integrity, andauthenticate both merchants and cardholders.Confidentiality of information is ensured by the message encryption ;payment information integrity is ensured by the use of digital signatures;cardholder account authentication is ensured by the use of digital signatures and card holder credentials;merchant authentication is ensured by the use of digital signatures and merchant credentials;and interoperability is ensured by the use of specific protocols and formats.
  3. At this juncture,it appears that SET will become the industry de factostandard.SET has emerged recently as a convergenceof the previous standards and has a lot in common with SEPP.SET is expected to be rapidly incorporated into industrial-strength "merchantware" already available from Netscape,Microsoft,IBM,and other software sellers.
- This approach is attractive because there is no prearranged relationship necessary between vendors and customers in order for business transactions to take place.
- Advantages of NetBill business model are that it simplifies authentication , single statement billing, and access to account information.
- The disadvantages concern network and processing bottlenecks and privacy concern.

Secure Electronic Payment Protocol

- IBM,Netscape,GTE,CyberCash, and MasterCard have cooperatively developed SEPP-an open ,vendor-neutral,nonproprietary,license free specification for securing on-line transactions.
- There are several major business requirements addressed by SEPP:
  - To enable confidentiality of payment information.
  - To ensure integrity of all payment data transmitted.
  - To provide authentication that the cardholder is the legitimate owner of card account.
  - To provide authentication that a merchant can accept Master card branded card payments with an acquiring member financial institution.
- SEPP is the electronic equivalent of the paper charge slip,signature,and submission process.
- SEPP takes input from the negotiation process and causes the payment to happenvia a three way communication among the card holder,merchant,acquirer.

- SEPP only addresses the payment process;privacy of nonfinancial data is not addressed in the SEPP protocol-hence ,it is suggested that all SEPP communications be protected with encryption at a lower layer,such with Netscape's SSL.
- Negitiation and delivery are also left to other protocols.
- SEPP features have been folded into SET. SEPP

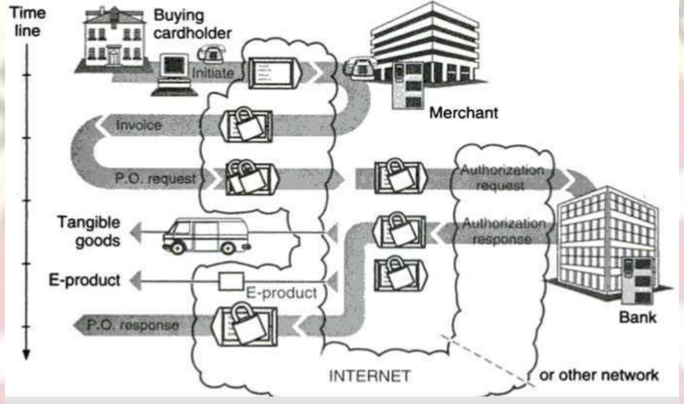
Process



- SEPP assumes that the cardholder and merchant have been communicating in order to negotiate terms of a purchase and generate an order.
- These process may be conducted via a WWW browser;alternatively,this operation may be performed through the use of electronic mail,via the users's review of a paper or CD-ROM catalog or other mechanisms.
- SEPP id designed to support transaction activity exchanged in both interactive(online)and noninteractive(offline)modes.
- The SEPP system is composed of a collection of elements involved in electronic commerce are

  - Cardholder:-This is an authorized holder of a bankcard supported by an issuer and registered to perform electronic commerce.
  - Merchant:-This is a merchant of goods and services and e-products who accepts payment for them electronically and may provide selling services and/or electronic delivery of items for sale.
  - Acquirer:-This is a financial institution that supports merchants by providing service for processing credit-card-based transactions.
  - Certificate Management System:-This is an agent of one or more bankcard associations that provides for the creation and distribution of electronic certificates for merchants,acquirers,and cardholders.
  - Banknet:-This represents the existing network which interfaces acquirers,issuers and the certificate management system.

- Messages for SEPP-compliant processing of payment transactions like
  - Purchase Order Request
  - Authorization Request
  - Authorization Response
  - Purchase Order Inquiry
  - Purchase Order Inquiry Response
- Additional messages for on-line customer are
  - Initiate
  - Invoice
  - Purchase Order Response(with Purchase Order Status)



- Messages for off-line transactions or transactions sent to merchant not on-line with the acquirer is
  - Purchase Order Response(acknowledgement without authorization).
- Simplified SEPP Process
  - The buying cardholder begins the transaction by sending the merchant an Initiate message.
  - The merchant responds with an Invoice message containing information used by the buying cardholder to validate the goods and service and the transaction information.
  - The buying cardholder then prepares a purchase order request which contains goods and service order validation information and the buying cardholder's payment instructions which are encrypted in a manner so as to only be decrypted by the acquirer.
  - The merchant receives the purchase order request, formats an authorization request and sends it to the acquirer.
  - The authorization request contains the confidential cardholder payment instructions.
  - The acquirer processes the authorization request.
  - The acquirer then responds to the merchant with an authorization response.
  - The merchant will respond to the buying cardholder with a purchase orderresponse ,if a purchase order response message was not previously sent.
  - At a later time,the buying cardholder may initiate a purchase order inquiryto which the merchant will respond with a purchase order inquiry response.
- The process of shopping is merchant-specific.
- The process of transaction capture,clearing and settlement,of the transaction is defined by

the relationship between the merchant and acquirer.

- The merchant sends a authorization request to the acquirer.The acquirer performs the following tasks
  - Authenticates the merchants.
  - Verifies the acquirer /merchant relationship.
  - Decrypts the payment instructions from the buying cardholder.
  - Validates that the buying cardholder certificate matches the accountnumber used in the purchase.
  - Validates consistency between merchant’s authorization request and thecardholders payment instruction data.
  - Formats a standard authorization request to the issuer and receive theresponse.
  - Responds to the merchant with a validated authorization request response.

SEPP Architecture

- This provides the buying cardholders with the flexibility to shop and conductnegotiations with the merchant system offering items for sale.
- The workstation may support all three stages of the electronic commerce processdescribed in the previous sections.
- Two designs of cardholder workstations are supported.
- Functions added to traditional WWW browsers to support electronic payments include encryption and decryption of payment data,certificate management and authentication and support for electronic payment protocols.
- To obtain certificate ,the buying cardholder’s PC software interfaces with the certificate request server in the certificate management system.
- The certificate management system generates the certificates needed to identify the buying cardholder.
- The interface to the certificate request server is based in HTTP interactions;the certificate server includes a WWW server to which the buying cardholder interfaces.
- Structure of SEPP
- The buying cardholder’s second and primary interface is with the merchant system.
- This interface supports the buying cardholder’s segments of the payment protocol ,which enables the buying cardholder to initiate payment ,perform inquiries,and receive order acknowledgment and status.
- This interface supports encrypted data sent to the merchant that is only capable of being decrypted by the merchant’s acquirer.
- This ensures that the buying cardholder is dealing with a valid merchant.
- The merchant computer system is based on a web server that provides aconvenient interface with the buying cardholder for the support of the electronicpayments.
- The merchant also interfaces with the merchant registration authority in the acquirer bank.
- This is the interface through which a merchant requests and receives its public certificates to support the electronic commerce security functions.
- The merchant needs to support SEPP protocols for the capture and authorizationof electronic commerce transactions initiated by the buying cardholder.
- The SEPP acquirer consists of a traditional acquirer with the addition of an acquirer gateway and a merchant registration authority.
- The acquirer gateway is a system that provides electronic commerce services to the merchants in support of the acquirer and interface with the acquirer to support the authorization and capture of transactions.

- The acquirer receives certificates from the off-line certificate authority.
- The merchant registration authority is a workstation located at the acquirer bankthat enables the acquirer to securely receive,validate and forward merchant certificate requests to the certificate management system and to receive back certificates.
- The certificate management system consists of computer system providing certificate authorities to support trusted ,reliable,certificate granting service to cardholders,merchants and acquirers.
- Banknet is the existing financial network through which acquirers obtain authorization for payment from issuers.
- It is also used in SEPP for cardholder certificate authorization between the certificate request server and the issuers.

UNIT III

Certificates for authentication:

A digital certificate is a foodproof was of identifying both consumers, and merchants.

The digital certificate acts like a network version of a driver‟s license- it is not credit, bat used in conjunction with any number of credit mechanisms, it verifies the users identity.

Digital certificates, which are issued by certificates authorities such as VeriSign and cyber trust, include the holder‟s name, the name of the certificates authority a public key for cryptographic use and a time limit for the use of the certificates.

The certificates typically includes a class, which indicates to what degree it has been verified.

For example, VeriSign digital certificates come in three classes. Nortel also offers digital certificates as part of its ensure Internet security software.

Both Hewlett – Packard Company and IBM have announced their intentions to use Entrust with their electronic commerce and security products. One of the issues affecting the industry, however, is interoperability. The document certification practice statement issued by VeriSign proposes interoperability approaches, but the outcome was unknown at press time.

Security on web servers and enterprise networks:

There are two general techniques are available

- Host security consideration
- Enterprise network security

Host based security capabilities - these are means by which each and every computer on the system in mode (more) impregnable.

Security watchdog system which guard the set of internal interconnected systems, communication between the internal world must be funneled through, these system. These watchdog systems that deal with security within an organizations own enterprisenetworks are called firewalls.

A firewall allows a business to specify the level of access that will be afforded to networks users. In general, both methods are required.

An internet site can set up an anonymous FTP site that allows any outside user to accessfiles at the site (anonymous FTP is very useful to companies that wish to place documentation in the public domain; it also can be used to allow users to download software). This could be as a start alone system which is updated only by off-line means (eg., load a diskette),or by a physically separate post (eg, consoleport); or, it could be a system outside the firewall (but still residing on the overall organization‟s networks) called a bastion. The firewall comes into play if the FTP system located onthe organization‟s networks, for case of updating.

Host security considerations:

Host security is a discipline that goes back to the 1960‟s main frame were perhaps endowed with more rigorous security capabilities than their successors. Naturally ,security comes at a price including the following.

The Financial resource spent in acquiring the constituent element such as packet filtersproxy server log hosts ,vulnerability detection tools, smart cards ,and so on.

The staff time spent configuring these tools identifying and correcting security holes and training the users about the new tools.

Venues to host infraction:

In a stand alone host environment ,host access can be restricted to logging in at the console through the serial port card or over a restricted dialup line in a network environment a web server, for example access is typically available from a variety of sources. Individual accessing information on the organization host(Web/HTTP)

- Individual accessing the organization host transparently(e.g., NFS,NIS)
- Individual interrogating the organization host(e.g., via ping, finger, dig,nslookup)
- Individual running programs on the organization host(rsh , x)
- Individual taking and leaving things (mail,UUCP,FTP,rcp)
- Individual understanding networks logins(rlogin,Telnet)

The majority of communication utilities in host were designed in the 1970 and 1980 without a high regard for security at a time the goal way easy network access. Anyonewith administrative powers can reconfigure a host‟s IP address and create specific accounts in order to masquerade as another host and user on the network.

Host Based security tools include the following:

- Monitoring and logging tools
- Filtering Tools
- Vulnerability detection tools

Web security concerns include the following

- Server side security which involves protecting hosts running the WWW serversthemselves
- Client side security which relates to security issues involved in requestingWWW service.
- Confidentiality which aims at guaranteeing the privacy of information
- transmitted across the network between clients and servers.

Some basic precautions for the server are the follows

- The http demon server should be executable only by root and is to be typicallyinvoked only at execution time.
- All files and directories in the server directory structure should be owed by root.
- Do not allow user to install scripts in this directory
- Remove all ability for remote logins such as rlogin or telnet
- Remove all nonessential compiler and programming tools that might be used byattackers to create or run programs on the server.

Enterprise Network Security:

A firewall (also called a secure Internet Gateway) supports communication based security to screen out undesired communication which can cause havoc on the host. Host based security is a critical element of overall computer security although isdoes not scale easily, nonetheless it must be employed. Ideally an administrator use allavailable tools including host security and communication gateway security. It is like having two lacks on a door both methods should be used for increased assurance.

The firewall deployment in the enterprise network must support the following capabilities:

- All traffic between the inside and outside must transmit through the firewall.
- Only authorized traffic based on the security policy is allowed transit the firewallitself must be immune to penetration .
- Firewalls act as a single focus for the security policy of the organization and support advanced authentication techniques such as smart card and one time password.
- Firewall are typically configured to filter traffic based on one of two design policies.
- Permit unless specifically denied this is weaker because it is impossible to be aware of all the numbers network utilities you may need to protect against specifically this approach does not protect against new internet utilities.
- Deny unless specifically permitted this is stranger because the administrator canstart off with a blank permit list and add only those function that are explicitly required.
- There are some variation in firewall architecture which modulated both the security level as the cost and complexity of the hardware.

There are two categories of firewall

IP and or TC/UDP datagram(packet)filters(including screening routers)which parse/filter traffic based on some combination of IP host and Network address ,IP protocol ,Port number, and possibly other values.

Application layer protocol gateways (also known as proxy server) which are intermediately hosts that accept incoming request for communication services and make the appropriate calls on the client behalf.

Electronic Payment and Electronic payment schemes:

E-Cash is a form of an electronic payment system where a certain amount of money isstored on a client’s device and made accessible for online transaction.

Stored-value card – A card with a certain amount of money that can be used to performthe transaction in the issuer store.

Internet Monetary payment and security Requirement:

For consumer and merchant to be able to trust one another, Prevent transmitted payment information from being tampered with and complete transaction with any valid party, the following issues need to be addressed:

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

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 as the router communication line or host level possibly resulting in the production of counterfeit card or fraudulent transaction.

There are two encryption methods used symmetric cryptography and asymmetric cryptography.

Symmetric cryptography or more commonly called secret key cryptography, usethe same key to encrypt and decrypt a message. A commonly used secret key algorithm is the Data Encryption Standard (DES) Asymmetric cryptography or public key cryptography, use two distinct keys: public key and a private key. This allows multiplesenders to receiver who uses the private key to decrypted it .The assurance of securityis dependent on the receiver protecting the private key.

For merchants to use secret key cryptography, they would each have to administer individuals secret key to all their customer and provide these keys through some secure channel .This channel complex from an administrative perspective. This process ,the customer generate a random number used to encrypt payment information using DES. The DES encrypted payment information and the encrypted DES key are then transmitted to the merchant. To decrypt the payment information the merchant first decrypt the DES key then use the DES key to decrypt the payment information . **payment information Integrity** Payment information sent from consumer to merchants includes order information, personal dataand payment instruction .The information is modified ,the transaction may no longer be accurate. To eliminate this possible source of error or fraud , an, arithmetic algorithm called hashing. The hash algorithm generates a value that is unique to the payment information to be transferred.

A helpful way to view a hash algorithm is as a one way public cipher ,in that It has no secret key Given a message digest there is no way to reproduce the original information.

- It is impossible to hash other data with the same value.
- To ensure the integrity the message digest is transmitted with the paymentinformation.
- The receiver would then validate the message digest by recalculating it oncepayment information is received.
- If the message digest does not calculate the same value sent the paymentinformation is assumed to be corrupted and is therefore discarded.
- To rectify the situation the message digest is encrypt using a private key of thesender (customer).This encryption of a message digest is called a digital

  signature.

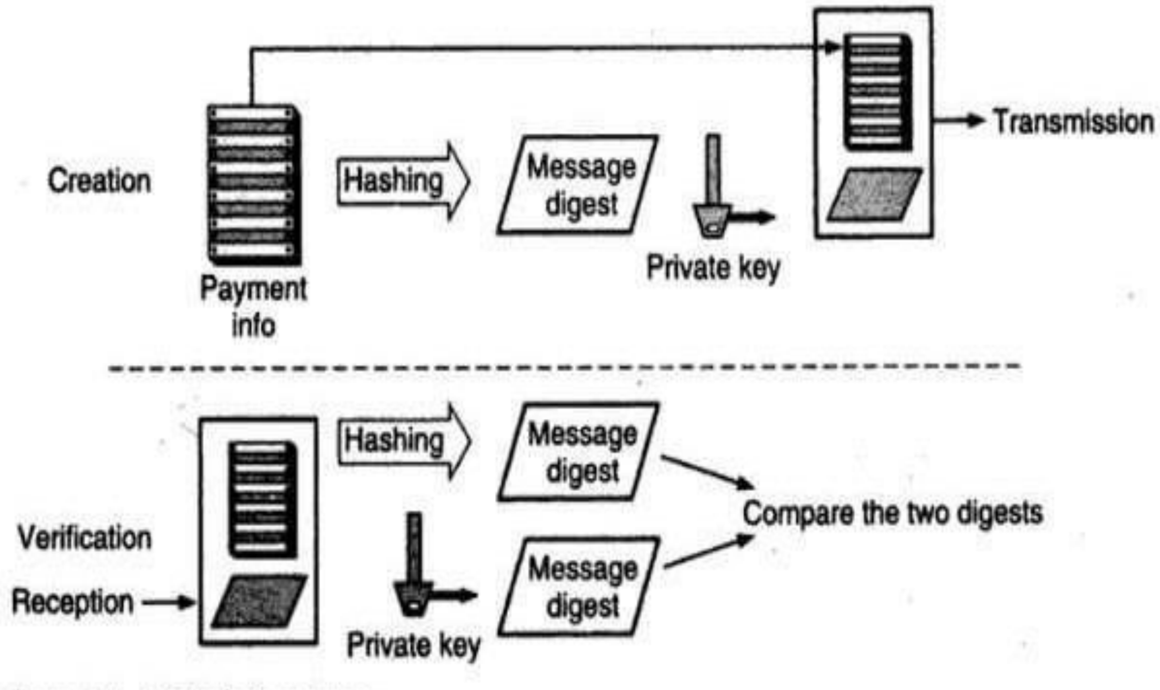


Figure 4.4 Digital signatures.

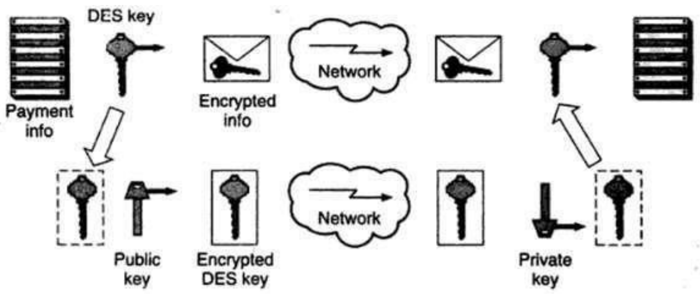


Figure 4.3 Secret-key/public-key combination.

A digital signature is created by using public key cryptography, it is possible to identify the sender of the payment information .The encryption is done by using the private key of a public /private key pair this means only the owner of that private key can encryptthe message digest. 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. A digital signature however ,does not authorize a particular customer to use the monetary account information located in the payment.

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. A way to secure this link is by use of a trusted third party who could validate the public key and account of the customer this third party could be one of many organization ,depending upon the type of account used. For example if a credit card account were used the third party could be one of the major credit card companies ;if a checking account were used ,the third party could be the federal clearinghouse or some other

financial institution. Merchants would then decrypt the public key of the customer and ,by definition of public key cryptography ,validate the public key and account of thecustomer. For the preceding to transpire ,however, the following is assumed.

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

Interoperability:

For electronic commerce to take place ,customer must be able to communicate with any merchant. Interoperability is then achieved by using a particular set of publicly announced algorithm and process in support of electronic commerce.

Payment and purchase order process:

Overview:

For an electronic payment to occur over the internet the following transaction/processmust occur.

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

Account holder registration :

Account holder 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. To register the account holder will most likely be required to fill out a from requesting information such as name, address, account number, and other identifying personal information when the form is completed the account holder software will do the following.
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 key4.Transmit
all times 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 digest

The certified documentation is then encrypted using a secret key which is in turn encrypted with the account holder‟s public key. The certified documentation is then verified by the account holder by using the public key of the TP, thus checking the digital signature.the account holder‟s software for future use in electronic commerce transaction.

Merchant registration:
Merchant must register with TPs that correspond to particular account type that they wish to honor before transacting business with customer who share the same account types. For example if a merchant wishes to accept visa and MasterCard ,that merchant may have to register with two TPs or find a TP that represent both The merchant registration is similar to the account holder‟s registration process.

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 form is completed ,that customer software does thefollowing

- Encrypts account informationwith the TP‟s public key.
- Attaches encrypted account information to the order form
- Creates a message digest of the order form and digitally signs it with the
- customer‟s private key.
- Encrypts the following with the secret key order form ,digital signature, and
- customer‟s.
- Encrypts secret key with the merchant‟s public key from the merchant CD.
- Transmits the secret key encrypted message and encrypted secret key to theMerchant.

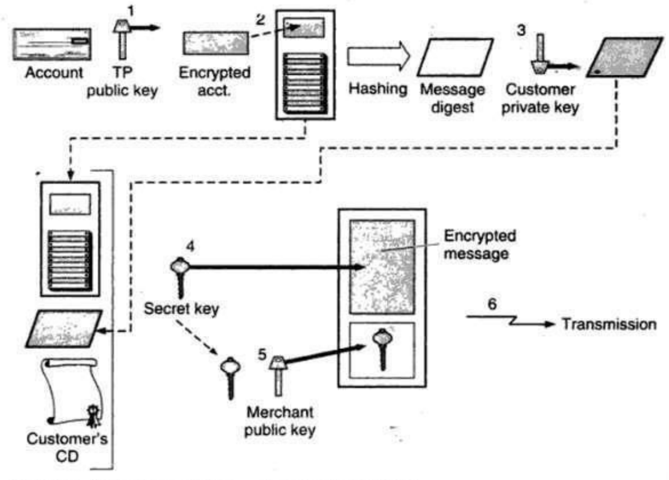


Figure 4.7 Customer ordering—order sent to merchant.

When the merchant's software receives the order, it does the authorization:

The processing of an order, the merchant will need a authorize (clear) the transaction with the TP responsible for that particular account. The authorization assures the merchant that the necessary funds or credit limit is available to cover the cost of the order. The merchant has no access to the customer account information since itwas encrypted using the TP‟s public key thus it is required that this information be sent tothe TP so that the merchant can receive payment authorization from the TP and that the proper customer account is debited for the transaction.

Merchants CD

Specific order information such as amount to be authorized order , number, date. Customers ID

Customers account information After verifying the merchant , customer, and account information the TP would then analyze the amount to be authorized.

On-Line Electronic cash:

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. The e-cash is then stored on a PCs hard drive or possibly a PCMCIA card for later use. These transaction could all be done using public key cryptography and digital signatures as discussed easily.

Problem with simple electronic cash:

A problem with the e-cash example just discussed is that double spending cannot be attacked or prevent since all cash would look the same. 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 frustrate the nature of privacy associated with real cash.

Creating electronic cash anonymity:

To allow anonymity the bank and the customer must collectively create the e-cash andassociate 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 get e-cash the consumer choose a random number to be used as the serial number for the e-cash.

Preventing double spending:
While the preceding process protects the anonymity of the consumer and can identify when money has been double spent,it still does not prevent consumer ,or merchant forthat matter ,from double spending. To create a process to identify double spender but one that keep the anonymity of lawful individuals requires the use of tamperproof software and complex cryptography algorithms. The software prevents double spending by encrypting an individuals identity by using a random secret key generatedfor each piece of e-cash.

E-cash Interoperability:

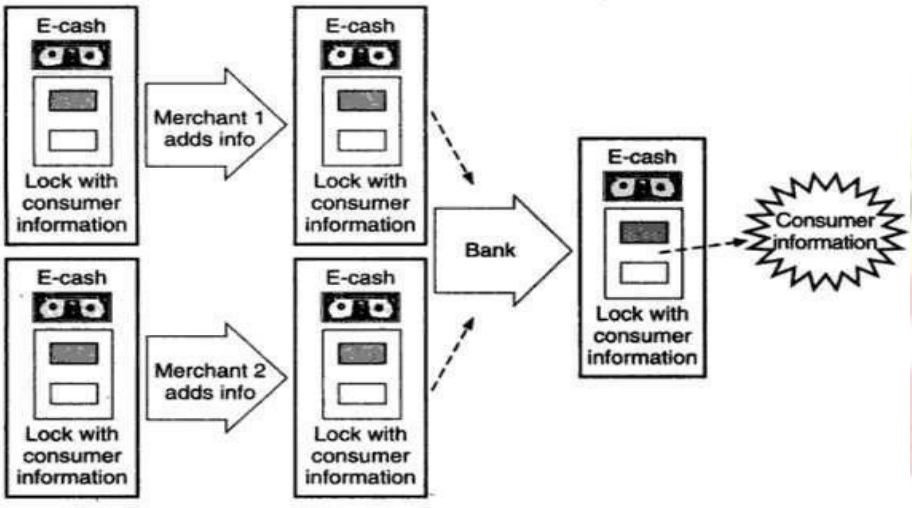

E-cash
Lock with consumer information
Merchant 1 adds info
E-cash
Lock with consumer information
E-cash
Lock with consumer information
Merchant 2 adds info
E-cash
Lock with consumer information
Bank
E-cash
Lock with consumer information
Consumer information

Figure 4.9 Double-spending process depiction—"simplified."

Consumer must be able to transact with any merchant or bank .Hence process and security standard must exit for all hardware and software used in e-cash transaction. Interoperability can only be achieved by adherence to algorithm and process in supporte- cash-initiate commerce

Electronic payment scheme:

The leading commercial electronic payment schemes that have been proposed in the past few years and the companies using them . Netscape.Netscape secure courier electronic payment scheme which has been selected by intuit for secure payment between users of its quicken home banking program and bank use SEPP. Microsoft: Microsoft STT is similar to SEEP/SET in that it provides digital signature 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. Check free: check freecorporation provides online payment processing service to major clients

To major clients, including CompuServe, Genie, Cellular one, Delphi Internet servicecorporation and Sky-Tel. check free has also announced intension to support all security methods that achieve prominence inn the marketplace. e.g., SET. **CyberCash:**

CyberCash combines features from checks and CyberCash is a digital cash software system which is usedlike a money order guaranteeing payment to the merchant before the goods shifting. CyberCash wants a micropayment capabilities of 5 to 20 cents pre transaction.

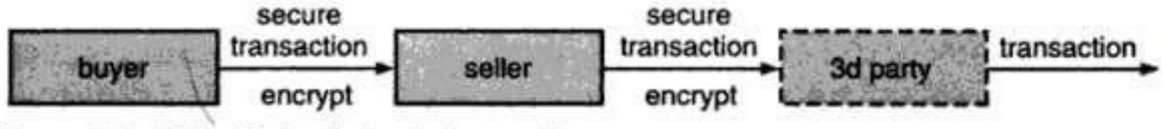


Figure 4.10 CyberCash electronic transaction process.

VeriSign:

VeriSign is offering its digital signature technology for authenticating as a componentseparated from encryption which allows for export of stronger authentication.IBM is building support for digital ID into its web browser and internet connection secure server for AIX and OS/2.

DigiCash:

DigiCash is a software company whose products allow users to purchase goods over the internet without using accredit card. The threat of privacy loss(where expenses canbe easily traced) gave rice to the idea of anonymous e-cash ,an electronic store of cashreplacement funds which can be loaded into a smart card for electronic purchase.

First virtual holding:It‟s targeting individuals and small business that want to buy and sell on the internet but cannot afford an extensive on-line infrastructure. A first virtual e-mail account and first virtual hosting system to track and record the transfer of information ,products , and payment for accounting and billing purpose ,consumer and merchant can buy and sell goods on the internet without sensitive information such as credit card number moving across the network. All sensitive information is deliveredby telephone.

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 seller many to many interaction and a significantly accelerated pace of procurement and development they called this model Spontaneous commerce.

Netcash :

Netcash is the internet answer to traveler‟s check. To use Netcash user must enter their checking account or credit card numbers into an on screen form and e-mail it to the Netcash.

Other approach: This section lists a few other approaches that have appearedin the recent past.

Mondexis based on smart cardtechnology initially backed by the united kingdom‟s West minster and midland Banks. The electronic purse is a handled smart card it remembers previous transaction and use RSA cryptography. Openmarket handles credit card transaction via web servers but it was planning to provide support for debit cards checking account and corporate purchase order. Global online use on-line challenge/response. It is based on a third party originating agreements therefore the seller has a higher cost to enter the market.

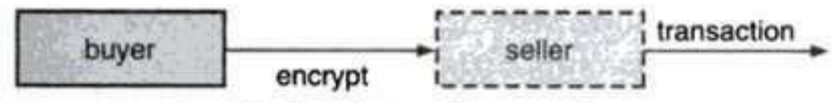


Figure 4.12 OpenMarket electronic transaction process.

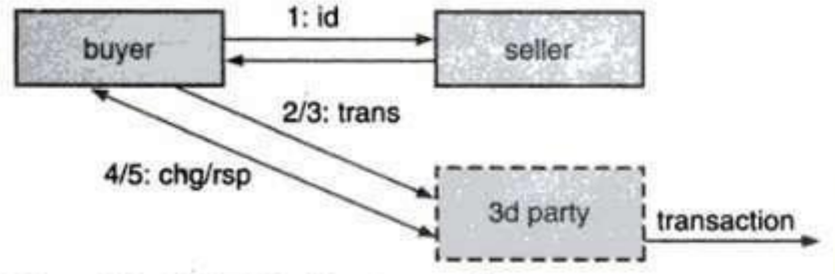


Figure 4.13 Global On-line transaction process.

Wallet and such:

Even in the absence of standards(e.g., SET) vendors have been developing system to handle sales over the internet and companies willing to accept that the products are not interoperable can support business before standard become widely deployed.

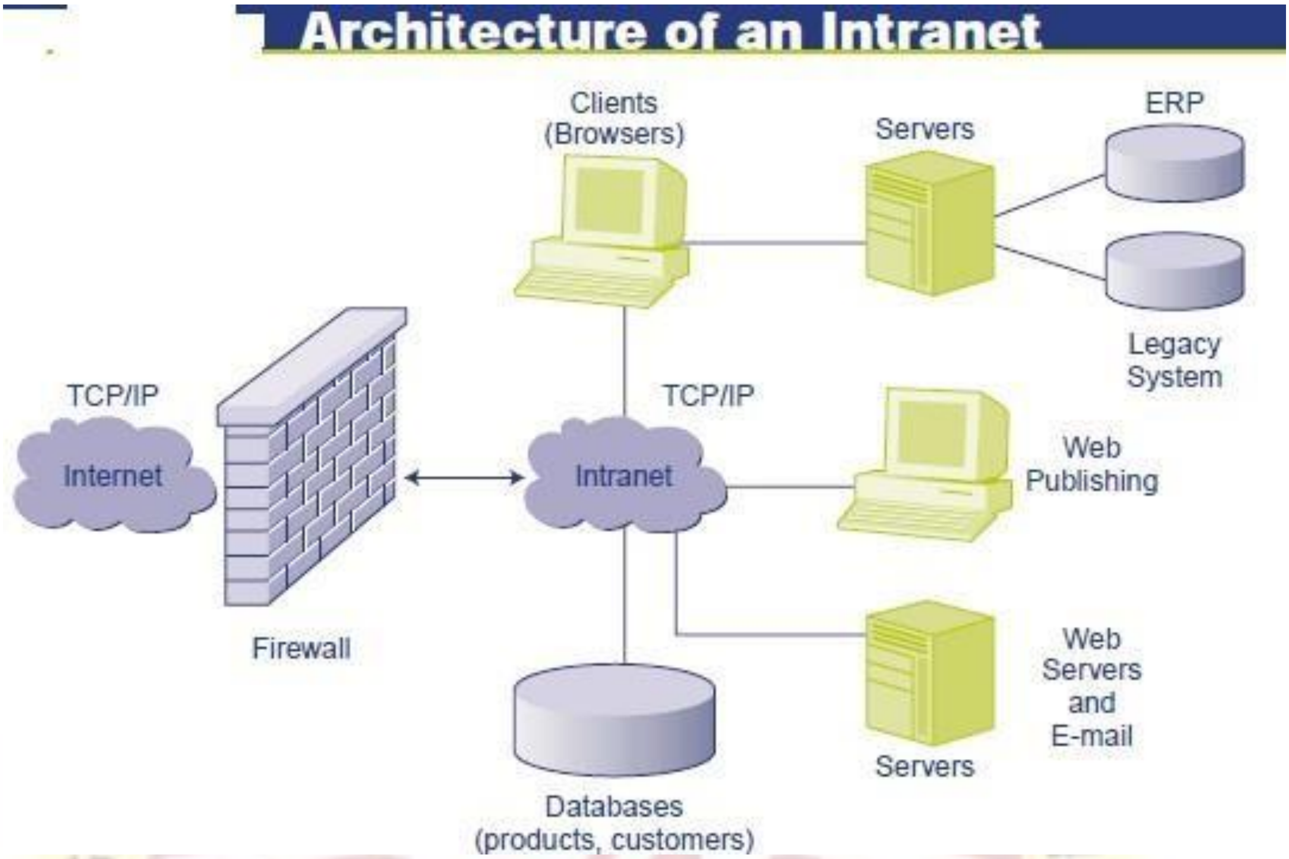
UNIT IV

Intranet

Intranet Software:

Intranet Software enables an organization to securely share it's information or operations with it's members. It enables the efficient use and more importantly reuse of an organization's gathered business knowledge and intelligence, which increases productivity and knowledge transfer in any organization. Increasingly, extranets are also coming into use, where external partners, customers can also interact with an organization. E.g. ERP software that provides a centralized repository of information for massive amount of transaction and details generated daily.

The cost of converting an existing client-server network to an intranet is relatively low, especially when a company is already using the Internet.



Applications of Intranet:

The most popular intranet application is obviously:

1. Inter-office e-mail, this capability allows the employees of a company to communicate with each other swiftly and easily. If the intranet has access to the Internet, e-mail can be accessed through the Internet connection. If the intranet is running without the Internet, special e-mail software packages can be bought and installed so that employees can take advantage of its many benefits.
2. An intranet has many other different applications that can be utilized by a company.These include the Web publishing of corporate documents, Web forms, and Web-to- database links that allow users to access information.

3. Newsletters, information on benefits, job listings and classifieds, libraries, stock quotes, maps, historical data, catalogs, price lists, information on competitors' products, and customer service data are just a few examples of these types of applications.

Generic Functions of Intranet:

Major generic functions that intranet can provide are:

Corporate/ department/ individual WebPages: Access the web- pages of corporate,departments and individual.

Database access: Web- based database.

Search engines and directories: It assists the keyword- based search.

Interactive communication: chatting, audio and videoconference.

Document distribution and workflow: web- based download and routing of documents.

Groupware: E-mail and bulletin board.

Telephony: intranet is the perfect conduit for computer-based telephony.

Extranet: linking geographically dispersed branches, customers and suppliers to authorized sections of intranets creates happiest customers, more efficient suppliers, and reduced staff cost.

Security is an essential part of any transaction that takes place over the internet. Customers will lose his/her faith in e-business if its security is compromised. Following are the essential requirements for safe e-payments/transactions −

- **Confidentiality** − Information should not be accessible to an unauthorized person. It should not be intercepted during the transmission.
- **Integrity** − Information should not be altered during its transmission over the network.
- **Availability** − Information should be available wherever and whenever required within a time limit specified.
- **Authenticity** − There should be a mechanism to authenticate a user before giving him/her an access to the required information.
- **Non-Repudiability** − It is the protection against the denial of order or denial of payment. Once a sender sends a message, the sender should not be able to deny sending the message. Similarly, the recipient of message should not be able to deny the receipt.
- **Encryption** − Information should be encrypted and decrypted only by an authorized user.
- **Auditability** − Data should be recorded in such a way that it can be audited for integrity requirements.

Measures to ensure Security

Major security measures are following −

- **Encryption** − It is a very effective and practical way to safeguard the data being transmitted over the network. Sender of the information encrypts the data using a secret code and only the specified receiver can decrypt the data using the sameor a different secret code.
- **Digital Signature** − Digital signature ensures the authenticity of the information. A digital signature is an e-signature authenticated through encryption and password.
- **Security Certificates** − Security certificate is a unique digital id used to verify the identity of an individual website or user.

Security Protocols in Internet

Secure Socket Layer (SSL)

It is the most commonly used protocol and is widely used across the industry. It meets following security requirements −

- Authentication
- Encryption
- Integrity
- Non-reputability

It consists of protocols that safeguard people who engage in online selling and buying of goods and services. You need to gain your customers' trust by putting in place eCommerce security basics. Such basics include:

- Privacy
- Integrity
- Authentication
- Non-repudiation

1. Privacy

Privacy includes preventing any activity that will lead to the sharing of customers' data with unauthorized third parties. Apart from the online seller that a customer has chosen, no one else should access their personal information and account details.

A breach of confidentiality occurs when sellers let others have access to such information. An online business should put in place at least a necessary minimum of anti-virus, firewall, encryption, and other data protection.

2. Integrity

Integrity is another crucial concept of eCommerce Security. It means ensuring that any information that customers have shared online remains unaltered. The principle statesthat the online business is utilizing the customers' information as given, without changing anything. Altering any part of the data causes the buyer to lose confidence inthe security and integrity of the online enterprise.

3. Authentication

The principle of authentication in eCommerce security requires that both the seller and the buyer should be real. They should be who they say they are. The business should prove that it is real, deals with genuine items or services, and delivers what it promises.The clients should also give their proof of identity to make the seller feel secure about the online transactions. It is possible to ensure authentication and identification.

4. Non-repudiation

Repudiation means denial. Therefore, Non-repudiation is a legal principle that instructsplayers not to deny their actions in a transaction. The business and the buyer should follow through on the transaction part that they initiated. Non-repudiation gives eCommerce security another layer. It confirms that the communication that occurred between the two players indeed reached the recipients. Therefore, a party in that particular transaction cannot deny a signature, email, or a purchase.

While growth in eCommerce has improved online transactions, it has attracted the attention of the bad players in equal measures

The eCommerce world experiences about 32.4% of all attacks. 50% of small eCommerce store owners are lamenting that the attacks are becoming severe. Furthermore, the reports show that 29% of traffic accessing a website consists of malicious requests.

Such attacks have contributed to significant losses in financials, market shares, and reputation. Almost 60% of small eCommerce stores that experience cybercrimes don't survive more than six months.

Therefore, it is very crucial to put in place water-tight security measures and hire a robustteam. It will ensure you run your business without worrying about closing down due tocybercriminals.

Common Ecommerce Security Issues

1. Lack of trust in the privacy and eCommercesecurity

Businesses that run eCommerce operations experience several security risks, such as:

- **Counterfeit sites**– hackers can easily create fake versions of legitimate websites without incurring any costs. Therefore, the affected company may suffer severe damage to its reputations and valuations.
- **Malicious alterations to websites**– some fraudsters change the content of a website. Their goal is usually to either divert traffic to a competing website or destroy the affected company's reputation.
- **Theft of clients' data**– The eCommerce industry is full of cases where criminals have stolen the personal information of customers, such as addresses and creditcard details.
- **Damages to networks of computers**– attackers may damage a company's online store using worm or virusesattacks.
- **Denial of service**– some hackers prevent legit users from using the online store, causing a reduction in its functioning.
- **Fraudulent access to sensitive data**– attackers can get intellectual property andsteal, destroy, or change it to suit their maliciousgoals.

2. Malware, viruses, and online frauds

these issues cause losses in finances, market shares, and reputations. Additionally, the clients may open criminal charges against the company. Hackers can use worms, viruses, trojan horses, and other malicious programs to infect computers and computers in many different ways. Worms and viruses invade the systems, multiply, and spread. Some hackers may hide Trojan horses in fake software, and start infections once the users download the software. These fraudulent programs may:

- hijack the systems of computers
- erase all data
- block data access
- forward malicious links to clients and other computers in the network.

3. Uncertainty and complexity in online transactions

Online buyers face uncertainty and complexity during critical transaction activities. Such activities include payment, dispute resolution, and delivery. During those points,they are likely to fall into the hands of fraudsters.

Businesses have improved their transparency levels, such as clearly stating the point ofcontact when a problem occurs. However, such measures often fail to disclose fully the collection and usage of personal data.

1. Use Multi-Layer Security

It is helpful to employ various security layers to fortify your security. A Content Delivery Network (CDN) that is widespread can block DDoS threats and infectious incoming traffic. They use machine learning to keep malicious traffic at bay.

A two-factor authentification is a good example. After the user enters the login information, they instantly receive an SMS or email for further actions. By implementing this step, it blocks fraudsters as they will require more than just usernames and passwords to access the legit users' accounts. However, hacking can still occur evenif an MFA is in place.

2. Get Secure Server Layer (SSL) Certificates

One of the primary benefits of SSL Certificates is to encrypt sensitive data shared acrossthe internet. It ensures that the information reaches only the intended person. It is a verycrucial step because all data sent will pass through multiple computers before the destination server receives it.

If SSL certificate encryption is absent, any electronic device between the sender and the server can access sensitive details. Hackers can thus take advantage of your exposed passwords, usernames, credit card numbers, and other information. Therefore, the SSL certificate will come to your aid by making the data unreadable to unintendedusers.

2. Use solid-rock Firewalls

Use effective e-commerce software and plugins to bar untrusted networks and regulatethe inflow and outflow of website traffic. They should provide selective permeability,only permitting trusted traffic to go through.

You can trust the Astra firewall to stop Spam, XSS, CSRF, malware, SQLi, and manyother attacks on your website. It ensures that the only traffic that accesses your eCommerce store consists of the real users. Moreover, we have specialized WAF solutions for WordPress, Magento, Opencart, Prestashop, Drupal, Joomla, and custommade PHP sites.

In a nutshell, the Astra firewall protection from:

- OWASP top 10 threats
- Protection from bad bots.
- Spam protection.
- Protection against 100+ types of attacks.

3. Anti-Malware Software

Your electronic devices, computer systems, and web system need a program or softwarethat detects and block malicious software, otherwise known as malware. Such protective software is called Anti-malware software. An effective anti-malware should render allthe hidden malware on your website. One such scanner is the Astra Malware Scanner. It scans your web system for all malicious software round the clock and is at your disposal It also lets you automate yourscans with its “Schedule a Scan” feature. You can schedule the scans daily, weekly, monthly or fortnightly.

Types of Security Attacks

- **Passive Attack**
- **Active Attack**

- **Passive Attack:** In Passive attack a network intruder intercepts data travelling throughthe network. A passive attack monitors unencrypted traffic. Passive attacks include traffic analysis, monitoring of unprotected communications, capturing authentication information such as passwords.

Types of Passive Attacks:

a) **Wire Tapping or Telephone Tapping**: Telephone tapping is the monitoring of telephone and internet conversations by a third party. Passive wire tapping monitors orrecords the traffic.

b) **Port Scanner**: A port scan can be defined as an attack that sends client requests to a range of server port addresses on a host, with a goal of finding an active port and exploiting a known vulnerability of that service.

c) **Idle Scan**: The idle scan is a TCP port scan method that consists of sending spoofedpackets to a computer to find out what services are available. This is accomplishedby impersonating another computer called a “zombie” and observing the behavior of the “zombie” system.

- **Active Attack**: In active attacks intruder initiates commands to disrupt the network’s normal operation. In an active attack, the attacker tries to bypass or break into securedsystems. This can be done through viruses or worms. Active attacks include attempts to break protection features to introduce malicious code, and to steal or modify information.

Types of Active Attacks

a) **Denial-of-service Attack (Dos)**: Denial of service attack is an attempt to make a machine or network resources unavailable to its intended users. It generally consists ofefforts to temporarily or indefinitely interrupt or suspend services of a host connectedto the Internet. One common method of attack involves saturating the target machine with external communication requests, so much so that it cannot respond to legitimate traffic or responds so quickly as to be rendered essentially unavailable. Such attacks usually lead to a server overload.

b) **Spoofing attack**: A spoofing attack is when a malicious party impersonates anotherdevice or user on a network in order to launch attacks against network hosts , steal data, spread malware or bypass access controls.

c) **Man-in-the-middle attack**: The man-in-the middle is a form of active eves droppingin which the attacker makes independent connections with the victims & relays messages between them, making them believe that they are talking directly to each other over a private connection, while in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the twovictims & inject new ones.

d) **SQL injection**: Sql injection is a code injection technique, used to attack data drivenapplications, in which malicious SQL statements are inserted into an entry field for execution.

Difference between Computer Virus and Computer Worm

Sno.	Computer Virus	Computer Worm
1.	It cannot be controlled remotely.	It can be controlled remotely.
2.	It deletes, modifies the files and alsochange the location of file.	It only monopolies the CPU & memory.
3.	It is slower than worm	Worm is faster than virus.
4.	The virus is the program code that attaches itself to application program and when application program run it runs along with it.	The worm is code that replicate itself in order to consume resources to bring it down.

Firewall

- Firewall is software or hardware based network security system that controls the incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed through or not, based on a rule set.
- A firewall establishes a human barrier between a trusted, secure internal network & another network that is not assumed to be secure and trusted.
- Many personal computer operating systems include software-based firewalls to protectagainst threats from the public Internet. Many routers that pass data between networkscontain firewall components and conversely many firewalls can perform basic routingfunctions.

Types of Firewall

- Network Layer or Packet Filters Firewall
- Application Layer Firewall
- Proxy Firewall
- Unified Threat Management(UTM)

Network Layer or Packet Filters Firewalls

Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set.

A simple router is the traditional network layer firewall, since it is not able to make particularly complicated decisions about what a packet is actually taking to or where it actually came from. Modern network layer firewalls have become increasingly more sophisticated & now maintain internal information about the state of connections passing through them at any time.

Application Layer Firewalls

Application layer firewalls work on the application level of the TCP/IP stack, and mayintercept all packets traveling to or from an application. They block other packets (usually dropping them without acknowledgement to the sender).

On inspecting all packets for proper content, firewalls can restrict or prevent outright the spread of networked computer worms and Trojans.

Proxy Firewalls

Proxy firewalls offer more security than other types of firewalls. Unlike application layer firewalls which allow or block network packets from passing to and from a protected network, traffic does not flow through proxy. Instead computers establish a connection to the proxy which serves as an intermediary and initiate a network connection on behalf of the request. This prevents direct connections between systems on either side of the firewall and makes it harder for an attacker to discover where the network is, because they will never receive packets created directly by their target system.

Unified Threat Management

A product category called unified threat management (UTM) has emerged. These device promise integration, convenience & protection from pretty much every threat out there and are especially valuable to small & medium-sized businesses.

Unified Threat Management is a firewall appliance that not only guards against intrusion but performs content filtering, spam filtering, intrusion detection & anti-virusduties traditionally handled by multiple systems. These devices are assigned to combat all levels of malicious activity on the computer network.

Smart Cards

- A smart card is a plastic card about the size of a credit card, with an embedded microchip that can be loaded with data.
- Smart cards are made of plastics generally polyvinyl chloride.
- Smart cards can provide identification, authentication, data storage & application processing.
- A smart card contains more information than a magnetic strip card and it can be programmed for different applications.
- Smart cards within the next five years will be the industry standard in debit and credit cards. As the major high street banks and finance houses are now investing in the changeover to smart card technology.
- You may use a smart card to:-
- Establish your identity when logging on to an Internet access provider or to an online bank.
- Pay for parking at parking meters or to get on subways, trains or buses. Give
- hospitals or doctors personal data without filling out a form.
- Make small purchases at electronic stores on the web.

Advantages of Smart Cards:

Greater Reliability

- Storage Capacity is increased up to 100 times.Smart
- cards are multifunctional.
- The anticipated working life of a smart card is ten years compared to that of a magneticstrip card.

4. Electronic Cheques

The electronic cheques are modeled on paper cheques, except that they are initialted electronically.

They use digital signatures for signing and endorsing and require the use of digital certificates to authenticate the payer, the payer's bank and bank account.

Electronic checks allow merchants to convert paper check payments made by customers to electronic payments that are processed through the Automated Clearing House (ACH).

How Electronic Cheques work:

When you receive a paper cheque payment from your customer , you will run the cheque through an electronic scanner system supplied by your merchant service provider. This virtual terminal captures the customer's banking information and payment amount written on the cheque. The information is transferred electronically via the Federal Reserve Bank's ACH Network, which takes the funds from your customer's account & deposits them to yours.

Once the cheque has been processed & approved, the virtual terminal will instantly print a receipt for the customer to sign & keep.

Benefits of Electronic Cheques:

- Secure and quick settlement of financial obligations. Fast
- cheque processing
- Very low transaction cost.

Electronic or Digital Cash

A system that allows a person to pay for goods or services by transmitting a number from one computer to another.

Like the serial numbers on real dollar bills, the digital cash numbers are unique. Eachone is issued by a bank & represents a specified sum of money.

Digital Cash combines computerized convenience with security and privacy that improve upon paper cash. Cash is still the dominant form of payment as: The consumerstill mistrusts the banks. The non-cash transactions are inefficiently cleared. In addition, due to negative real interests rates on bank deposits.

Digital cash is based on cryptographic systems called "Digital Signatures" similar to the signatures used by banks on paper cheques to authenticate a customer.

Some qualities of cash:

a. Cash is a legal tender i.e. payee is obligatory to take it.
b. It is negotiable i.e. can be given or traded to someone else.
c. It is a bearer instrument i.e. possession is proof of ownership.
d. It can be held & used by anyone, even those without a bank certificate.
e. It places no risk on part of acceptor.

The following are the limitations of Debit and Credit Cards:

i. They are identification cards owned by the issuer & restricted to one user i.e.cannot be given away.
ii. They are not legal tender
iii. Their usage requires an account relationship and authorization system.

Properties of Digital Cash

- Must have a monetary value: It must be backed by cash (currency), bank authorized credit or a bank certified cashier’s check.
- Must be interoperable or exchangeable: as payment for other digital cash, paper cash, goods or services, lines of credit, bank notes or obligations, electronic benefit transfersand the like.
- Must be storable and retrievable: Cash could be stored on a remote computer’s memory, in smart cards, or on other easily transported standard or special purpose devices. Remote storage or retrieval would allow users to exchange digital cash from home or office or while traveling.

6. Debit Cards

A debit card is a plastic payment card that provides the cardholder electronic access tohis or her bank account at a financial institution.

Types of Debit Card Systems: Online

- Debit or Pin Debit Offline Debit or
- Signature Debit

Online Debit System: Online debit system requires electronic authorization of every transaction and the debits are reflected in the user’s account immediately. The transaction may be secured with the personal identification number (PIN) authentication system.

Offline Debit System: Offline debit system may be subject to a daily limit. Transactions conducted with offline debit cards, require 2-3 days to be reflected on user’s account balances.

Advantages of Debit Cards: There is

- no need to carry cash

- It is quick and less complicated than using a cheque.It can be
- used for withdrawals of cash.
- It can be issued to any individual without assessing credit worthiness.
- Its holders can have a record of the transactions in his bank statement which willenable him to plan and control the expenditure.

7. Electronic Wallet/Purse

A digital/electronic wallet refers to an electronic device that allows an individual to make electronic commerce transactions. This can include purchasing items on-line with a computer or using a smartphone to purchase something at a store.

Increasingly, digital wallets are being made not just for basic financial transactions but to also authenticate the holder's credentials. For example, a digital-wallet couldpotentially verify the age of the buyer to the store while purchasing alcohol.

It is useful to approach the term "digital wallet" not as a singular technology but as three major parts: the system (the electronic infrastructure) and the application (the software that operates on top) and the device (the individual portion).

An individual’s bank account can also be linked to the digital wallet. They might also have their driver’s license, health card, loyalty card(s) and other ID documents stored on the phone. The credentials can be passed to a merchant’s terminal wirelessly via near field communication (NFC). Certain sources are speculating that these Smartphone “digital wallets” will eventually replace physical wallets.

A digital wallet has both a software and information component. The software providessecurity and encryption for the personal information and for the actual transaction.

Typically, digital wallets are stored on the client side and are easily self-maintained and fully compatible with most e-commerce Web sites. A server-side digital wallet, also known as a thin wallet, is one that an organization creates for and about you and maintains on its servers. Server-side digital wallets are gaining popularity among major retailers due to the security, efficiency, and added utility it provides to the end- user, which increases their enjoyment of their overall purchase.

Advantages of Electronic Payment System

- **Decreasing Technology cost**

The technology used in the networks is decreasing day by day, which is evident from the fact that computers are now dirt cheap and Internet is becoming free almost everywhere in the world.

- **Reduced operational and processing cost**

Due to reduced technology cost the processing cost of various commerce activities become very less. A very simple reason to prove this is the fact that in electronic transactions we save both paper and time.

- **Increasing online commerce**:

The above two factors have lead many institutions to go online and many others are following them.

Drawbacks or Risks in Electronic Payment System

Electronic payment is a popular method of making payments globally. It involves sending money from bank to bank instantly -- regardless of the distance involved. Suchpayment systems use Internet technology, where information is relayed through networked computers from one bank to another. Electronic payment systems are popular because of their convenience. However, they also may pose serious risks to consumers and financial institutions.

- **Tax Evasion**

Businesses are required by law to provide records of their financial transactions to thegovernment so that their tax compliance can be verified. Electronic payment howevercan frustrate the efforts of tax collection. Unless a business discloses the various electronic payments it has made or received over the tax period, the government may not know the truth, which could cause tax evasion.

- **Fraud**

Electronic payment systems are prone to fraud. The payment is done usually after keying in a password and sometimes answering security questions. There is no way ofverifying the true identity of the maker of the transaction. As long as the password and security questions are correct, the system assumes you are the right person. If this information falls into the possession of fraudsters, then they can defraud you of your money.

- **Impulse Buying**

Electronic payment systems encourage impulse buying, especially online. You are likely to make a decision to purchase an item you find on sale online, even though youhad not planned to buy it, just because it will cost you just a click to buy it through your credit card. Impulse buying leads to disorganized budgets and is one of the disadvantages of electronic payment systems.

- **Payment Conflict**

Payment conflicts often arise because the payments are not done manually but by an automated system that can cause errors. This is especially common when payment is done on a regular basis to many recipients. If you do not check your pay slip at the endof every pay period, for instance, then you might end up with a conflict due to these technical glitches, or anomalies.

UNIT V
MASTER CARD/VISA SECUREELECTRONIC TRANSACTION

In august 1996, Master card and visa agreed to jointly develop the Secure ElectronicTransaction (SET) Specification.

Internet:

The internet is changing the way we access and purchase information, communicate and pay for services, and acquire and pay for goods. Financial service such as bill payment, brokerage insurance and home banking are now or soon will be available over the internet. Any organization can become a global publisher by establishing an information site on the Internet's World Wide Web.

World Wide Web:

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

Role of payment systems

Payment system and their financial institution will play a significant role byestablishing
open specification for payment card transaction that:

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

Use of payment card products

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

Purpose of Secure Electronic Transaction

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

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

These specificationwill enable greater payment card acceptance, with a level ofsecurity that will encourage consumers and business to make wider use of payment card products in this emerging markets.

The primary motivation for the bankcard association to provide specification for securepayments are:

- To have the bankcard community take a leadership position in establishing secure payment specification and , in the process, avoid any cost associated with future reconciliation of implemented approaches,
- To respect and preserve the relationship between merchants and Acquires and between cardholders and Issuers,
- To facilitate rapid development of the marketplace,
- To respond quickly to the needs of the financial services market and,
- To protect the integrity of bankcards brands.

Payment security: The objectives of payment security are to:

- Provide authentication of cardholders, merchants and acquires
- Provide confidentiality of payment data,
- Preserve the integrity of payment data, and
- Define the algorithms and protocol necessary for these security services.

Interoperability:

The objectives interoperability are to:

- Clearly define detailed information to ensure that applications developed by onevendor will interoperate with application developed by other vendors,
- Create and support an open payment card standard,
- Define exportable technology throughout, in order to encourage globally interoperable software,
- Build on existing standards where practical,
- Ensure compatibility with and acceptance by appropriate standards bodies, and
- Allow for implementation on any combination of hardware and software platforms such as power pc, Intel, Spare, UNIX, MS-DOS,OS/2,windows and Macintosh. Marketacceptance:

The objectives of market acceptance are to:

- Achieve global acceptance, via ease of implementation and minimal impact onmerchant and cardholder and users,
- Allow for “bolt-on” implementation of the payment protocol to existing clientapplication,
- Minimize change to the relationship between acquires and merchants, andcardholders and issuers,
- Allow for minimum impact to existin g merchants acquire and payment systemapplication and infrastructure, and
- Provide and efficient protocol view from the financial institution perspective.

Business Requirements

Introduction

This section introduce the business requirements for secure payment processing usingpayment card products over both public networks (such as the Internet)and private networks.

Security issues noncompetitive: Security issues regarding electronic commerce mustbe viewed as noncompetitive in the interest of financial institution, merchants and cardholders Seven business requirements

There are seven major business requirements addressed by set:

1. Provide confidentiality of payment information and enable confidentiality of orderinformation that is transmitted along with the payment information.
2. Ensure integrity for all transmitted data.
3. Provide authentication that a cardholder is a legitimate user of a branded paymentcard account.
4. Provide authentication that a merchant can accept branded payment cardtransactions through its relationship with an acquiring financial institution.
5. Ensure the use of the best security practices and system design techniques to protectall legitimate parties of an electronic commerce transaction.
6. Ensure the creation of a protocol that i s neither dependent on transport securitymechanisms nor prevents their use.
7. Facilitate and encourage interoperability across software and network providers.Features.

Features of the specification :

These requirements are addressed by the following of these specification:

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

Confidentiality of information:

To facilitate and encourage electronic commerce using payment card products, it willbe necessary to assure cardholders that their payment information is safe and accessible only by the intended recipient

Online shopping: In today online shopping environment , payment instruction containing account information are often transmitted from cardholders to merchants over open networks with little or no security precautions.

Fraud : while it is possible to obtain account information in other environment, t her isa heightened concern about the case of doing so with public network transactions. This concern reflects the potential for high volume fraud, automated fraud (such as using filters on all messages out of a data stream), and the potential for “mischievous” fraud”that appears to be characteristic of some hackers. Confidentiality is ensured by the useof message encryption Integrity of data: The specification must guarantee that message content is not altered during the transmission between originator and recipient. Payment information, sent form cardholders to merchants include order information, personal data and payment instructions if any component is altered in transit, the transaction will not be processed accurately. Payment information integrity is ensured by the use of digital signatures. Cardholder account authentication: Merchants need a way to verify that a cardholder is a legitimate user of a valid branded payment card

account number. A mechanism that uses technology to link a cardholder to specific payment card account number will reduce the incidence of fraud and therefore the overall cost of payment processing. These specification define the mechanism to verifythat a cardh older is a legitimate user of a valid payment card account number. Cardholder account authentication is ensured by the use of digital signatures and cardholders certificates. Merchant authentication: The specification must provide a way for cardholders to confirm that a merchant has a relationship with a financial institution allowing it to accept payment cards. Cardholders also need to be able to identify merchants with whom they can securely conduct electronic commerce.

Merchants authentication is ensured by the use of digital signatures and merchants certificates. Interoperability : The specification must be applicable on a variety of hardware and software platforms and must include no preference for one over another. Any cardholder with compliant software must be able to communicate with any merchants software that also meets the defined standard. Interoperability is ensured bythe use of specific protocols and message formats Scope Use of payment cards The SET specification address a portion of the message protocols that are necessary for electronic commerce. It specifically address those parts of the protocols that use or impact the use of payment cards. Electronic shopping experience The electronic shopping experience can be divided into several distinct stages. Even though these stages have been described as occurring in a specific order, variations are possible ; many such variations are describe later in these specification.

With in the scope The following are within the scope of these specifications

- Application of cryptographic algorithms (such as RSA and DES)
- Certificate message and object formats
- Purchase message and object formats
- Authorization message and object formats
- Capture message and object formats
- Message protocols between participants Outside the scope The following are outsidethe scope of the set specifications
- Message protocols for offers, shopping, delivery of goods, etc
- Operational issues such as the criteria set by individual financial institution for theissuance of cardholder and merchants certificates
- Screen formats including the content, presentation and layout of order ent ry formsas defined by each merchant
- General payments beyond the domain of payment cards
- Security of data on cardholder, merchants, and payment gateway systems includingprotection from viruses, Trojan horse programs, an hackers

Payment system participants\Payment system participants

Interaction of participants

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

Cardholder

In the electronic commerce environment, consumers and corporate purchasers interact with the merchants form personal computers. A cardholder uses a payment card that has been issued by an Issuer. SET ensure that the interactions the cardholder has with a merchant keep the payment card account information confidential.

Issuer

An issuer is the financial institution that establishes an account for a cardholder and issues the payment card. The issuer guarantees payment for authorized transaction using the payment card in accordance with payment card brand regulation and local legislation.

Merchant

A merchant offers goods for sale or provides services in exchange for payment. SET allows a merchant to offer electronic interactions that cardholders can use securely. A merchant that accepts payment cards must have a relationship with an Acquirer.

Acquirer

An acquirer is the financial institution that establishes an account with a merchant andprocess payment card authorizations and payments.

Payment gateway

A payment gateway is a device operated by an Acquirer or a designated third party that processes merchant payment messages(including payment instruction form cardholders)

Brand

Financial institution have founded bankcard association that protect and advertise the brand, establish and enforce rules for use and acceptance of their bankcards, and provide networks to interconnect the financial institutions. Order brands are owned by financial services companies the advertise the brand and establish and enforce rules for use and acceptance of their payment cards. These brands combine the roles of Issuer an Acquire in interactions with cardholders and merchants.

Third parties

Issuers and Acquires sometimes choose to assign the processing of payment card transaction to third party processor, this documents does not distinguish between the financial institution and the processor of the transaction.

Cryptography

Protection of sensitive Cryptography has been used for centuries to protect sensitive information as it transmitted from one location to another in a cryptographic system ina message encrypted using a key. Secret key cryptography also known as symmetric cryptography, uses the same key to encrypt and decrypt the message. Public key cryptography, also known as asymmetric key cryptography uses two key: one key to encrypt the message and the other key to decrypt the message. The two keys are mathematically related such the data encrypted with either jey can only be decrypted using the other.

Encryption

Relation of keys

When two key users want to exchange messages securely, each transmits one component of their key pair, designated the public key, to the other and keeps secret key the other component , designated the private key. Use of symmetric key ,SET willrely on cryptography to ensure message confidentially to SET, message data will initially be encrypted using randomly generated symmetric encryption key.

Digital signature

Relationship of keys

Because of the mathematically relationship between the public and private keys, data encrypted with either key can only be decrypted with the other . this allows the sender of a message to encrypt it using the sender private key. Any recipient can determine that the message came from the sender by decrypting the message using the sender’s public key . When combined with message digests, encryption using the private key allows users to digitally sign message. A message digest is a value generated for a message for document that is unique to that message.

Certificates

Authentication is further strengthened by the use of certificates

Need for authentication

Before two parties use public key cryptography to conduct business each wants to be sure that the other party is authenticated. Before Bob accepts a message with Alice`s digital signature, be wants to be sure that the public key belongs to Alice and not to someone masquerading as Alice on an open network

Need for trusted third party

An alternative to secure transmission of the key is to use a trusted third arty to authentication that the public key belongs to Alice. SET authentication: The means that a financial institution uses to authenticate a cardholder or merchant is not defined by these specifications. each payment card brand and financial institution will select an appropriate method.

Payment processing Transaction

It describes the flow of transaction as they are processed by various systems

- Cardholders registration
- Merchant registration
- Payment authorization
- Payment request
- Payment capture

Other transaction

The following additional transaction are part of these specification

- Certificate query
- Purchase inquiry
- Purchase notification
- Sale transaction
- Authorization reversal
- Capture reversal
- Credit
- Credit reversal

Certificate authority function

- Receive registration requests
- Process and approve/decline requests and
- Issue certificate

E-MAIL AND SECURE E—MAIL TECHNOLOGIES FOR ELECTRONIC COMMERCE

E-mail is the use of electronic messaging technologies to allow computer users to communicate with each other for a variety of purposes. An electronic message can consist of a single text line: of a multimedia document encompassing text, video, and sound; or some other document. E-mail supports messaging, return receipts, and the ability to attach pertinent ancillary files to the basic message. E-mail allows one to transmit messages and other files to people located either down the hallway, or, usingthe Internet, around the world. In order to send Internet mail, one needs to obtain an account with an Internet Service Provider or an on-line service (i.e., America Online, Prodigy, and so forth) and know the address of the recipient. The ISP provides an Internet address to the subscriber that allows the individual to receive Internet mail. Compani ies are using the Internet to pursue business opportunities in three areas; electronic collaboration, information distribution and access, and electronic commerce. Message can be sent to multiple parties simultaneously and nearly instantaneously without having to retype each individual letter or memo. Someone receiving a message may forward the message to another destination with or without comment. Mail can be sorted in order to determine what to read immediately and whatto read later. Message can be filed electronically for future reference. There are simplified procedure for responding to mail sent by others. Mail can be accessed andsent from anywhere around the world. This feature becomes even more prevalent in today’s working society because of telecommuting. Many companies find telecommuting attractive because they save on benefits and overhead or office space as part of the virtual corporation discussed in Chap.1 Multiple copies can be sent in different formats. Messages can be sent electronically to another mailbox, a telex terminal, another fax machine, by mailgram or cablegram, or all at once. Attachments of all kinds can (generally) be included.

How does the e-mail works:

The first architecture is commonly referred as a file-based system. in this architecture

,the mail clients creates a file containing the message header, text , and pointers to attachments and posts it to a directory on a post office server. next, message transport software, usually hosted on another pc ,uses TCP/IP transport capabilities to route message from post office to post office ,as needed. The recipient’s e-mail client periodically polls the local post office server’s directory and notifies the user when new mail arrives. The second example is more popular client/server architecture here

,the first step involves the e-mail client workstation creating a real-time session with an e-mail server and using a remote proceeds call(RPC) to request an `IDID that will be used to label the message envelope.

Delivery date: This lines shows the date and time the message was received in the mailbox

Return Path: This line shows the reply the address of the original sender

Received: Every entry in the header starting with received represents a computer/gateway that has transferred the message also referred to as a hop. if there are two many hops, the message will be bounced or returned, to the original sender. A message will also bounce if the person is no longer found at that mail system.

Date: This lines shows the date and time the message left the sender. This will vary by several seconds or minutes from the delivery date line. From: This line specifies the full name and email address of the original sender.

Message ID: This line serves as a unique identifier of each mail message. It includes the name of the machine sending the message ,the date , time and file name.

To: Each person receiving the message will appear on the line if there is more than one address, the addresses will be separated by a comma.

For example , an internet address is denise,_derkacs@merck.com.the user name is denise_derkacs. The domain is merk.com.

.edu for educational institutions

.gov for federal governmental officers are organization

.org for any other address that does not fall into a previous identifiers _usually non profit organization

Address outside the united state will append a two letter country identifier, such as .ca

MIME:MULTIPURPOSE INTERNET MAIL EXTENSIONSBASIC CONCEPT

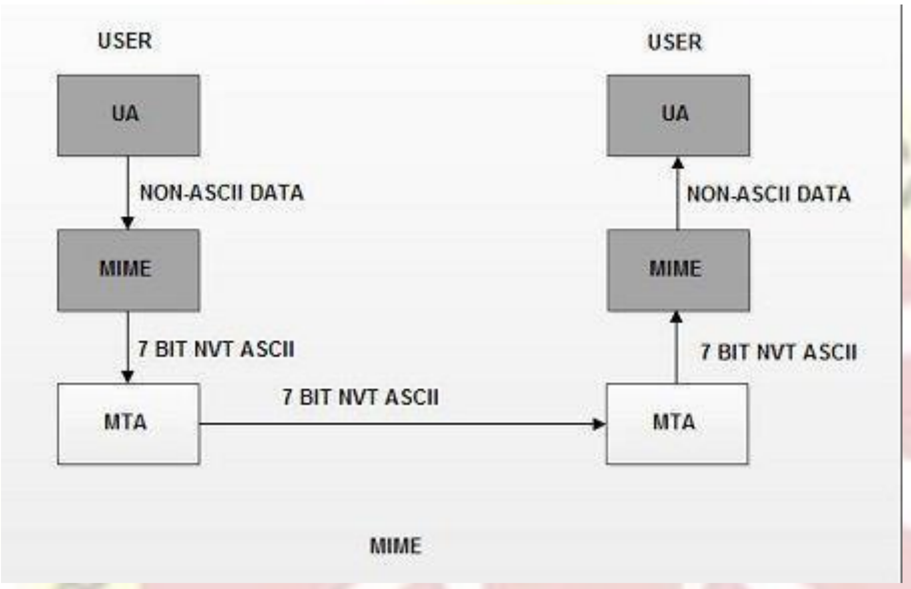
Multipurpose internet mail extensions(MIME)RFC-1521 provides internet e-mail support for messages containing formatted text, sound images, video, and attachments

- Common way in which files are sent as e-mail on the internet.
- Content type are 1. Primary type----indicates general content of the material 2. Subtype indicates the specific format.
- Five basic primary mime content types of text , image, audio, video, and application
- Composite MIME content types
- Message: one can send the message inside another message, labeling it message/rfc822. A mime mailer can label each segment or part of the message as message/partial. The recipients mail software can re assemble the message automatically.
- Multipart: allows more than one piece of MIME to be included in a message.
- MIME encoding
- Uses many different encoding methods , depending on the file type it is sending .
- Content _transfer_encoding header on each message corresponding to the type ofdecoding the recipient needs to perform.
- Mime software adopts the general philosophy of trying to work with existing nonMIME software as much as it possibly can.
- Users an encoding called base 64 for pure binary files.

MIME :

It is a Standard for attaching non-text files to an internet mail message, such as animation, graphics, hypertext files, sound files, spreadsheets. MIME standard converts (encodes) non-text files into text that is normally unreadable and then, at the other end, reconverts (decodes) the files to their original form. A more secure version is called secure MIME (S/MIME).

MIME stands for *(**Multipurpose Internet Mail Extensions**)*. It is widely used internet standard for coding binary files to send them as e-mail attachments overthe internet. MIME allows an E-mail message to contain a non-ASCII file such as a video image or a sound and it provides a mechanism to transfer a non text characters to text characters.



The MIME specification includes the following elements:

1. **Message header fields**. Five message header fields are defined. These fields provide information about the body of the message.

2. **Content formats**. A number of content formats are defined, thus standardizing representations that support multimedia electronic mail.

3. **Transfer encoding**. Transfer encoding are defined that enable the conversion of any content format into a form that is protected from alteration by the mail system. **Multipurpose Internet Mail Extensions (MIME)** five additional extensions to SMTP messages, supports multipart messages with more two parts, and allows the encoding of 8-bit binary data such as image files so that they can be using SMTP. The encoding method for translation binary information used by MIME, Base64 Encoding,essentially provides a mechanism for translating non text information into text characters. The MIME extensions are implemented as fields in the e-mail message header.

These fields are the following: Content type, Content transfer encoding method, MMEversion number Content ID (optional), Content description (optional).

MIME Header

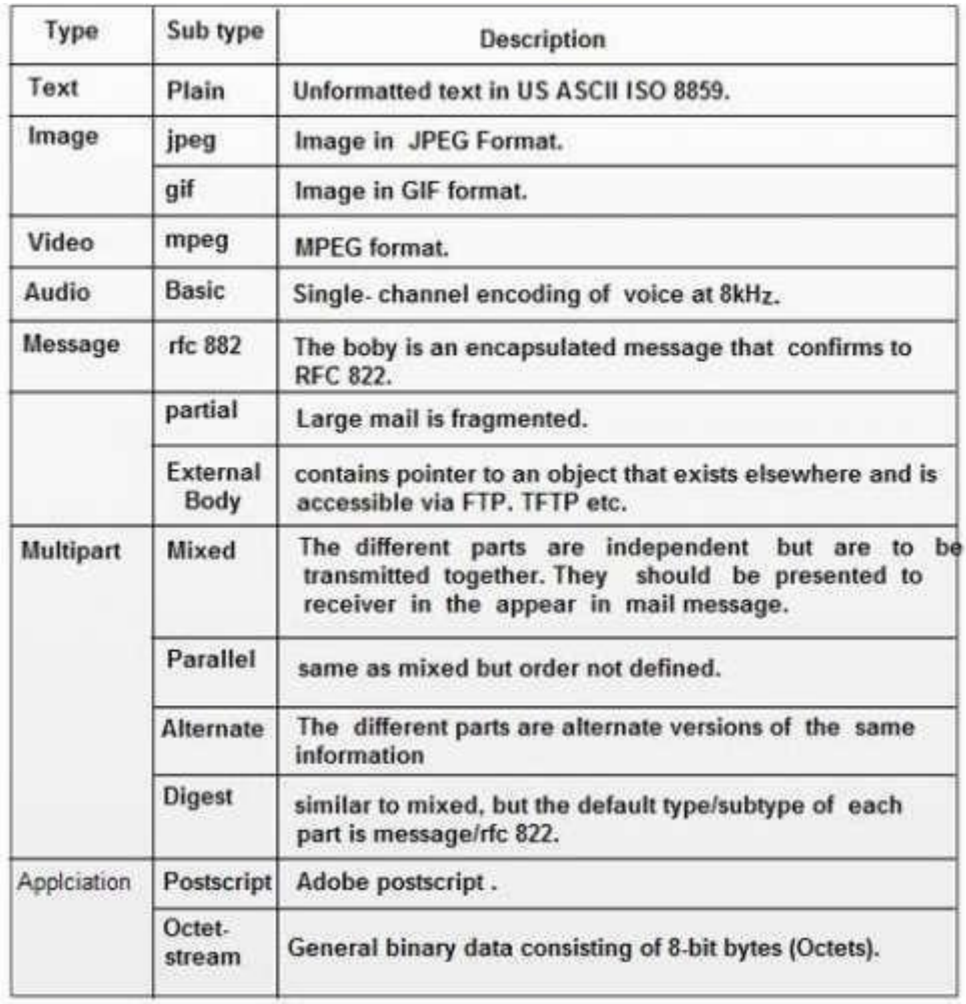
The five header fields defined in MIME are as follows:

1. **MIME-version**. It indicates the MIME version being used. The current version is It is represented as : MIME-version: 1.1.

2. **Content-type**. It describes the type and subtype of the data in the body of the message. The content type and content subtype are separated by slash. This field describes how the object in the body is to be interpreted. The default value is plaintext in US ASCII. Content type field is represented as:

Context-type: <type/subtype; parameters>

There are seven different types and fourteen sub-types of content. The various contenttype are listed in the table below:

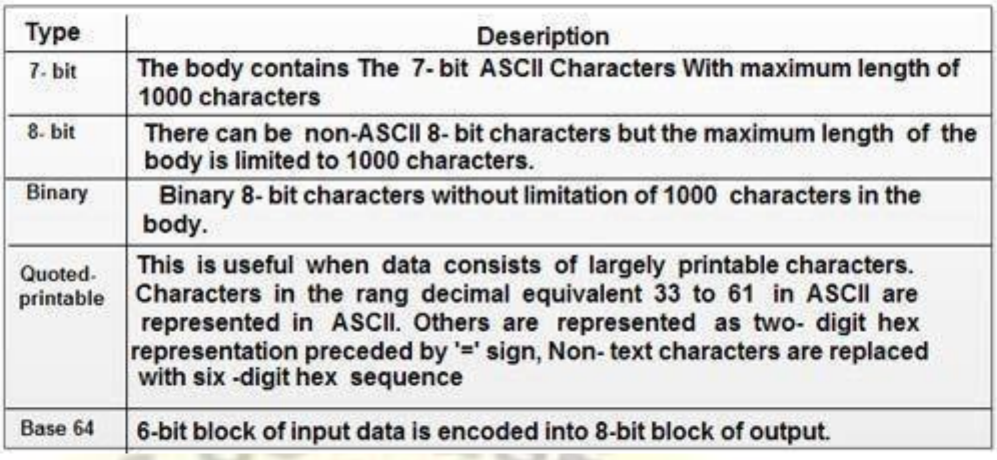


Type	Sub type	Description
Text	Plain	Unformatted text in US ASCII ISO 8859.
Image	jpeg	Image in JPEG Format.
	gif	Image in GIF format.
Video	mpeg	MPEG format.
Audio	Basic	Single- channel encoding of voice at 8kHz.
Message	rfc 882	The boby is an encapsulated message that confirms to RFC 822.
	partial	Large mail is fragmented.
	External Body	contains pointer to an object that exists elsewhere and is accessible via FTP. TFTP etc.
Multipart	Mixed	The different parts are independent but are to be transmitted together. They should be presented to receiver in the appear in mail message.
	Parallel	same as mixed but order not defined.
	Alternate	The different parts are alternate versions of the same information
	Digest	similar to mixed, but the default type/subtype of each part is message/rfc 822.
Applciation	Postscript	Adobe postscript .
	Octet-stream	General binary data consisting of 8-bit bytes (Octets).

3. Content-transfer encoding. It describes how the object within the body has been encoded to US ASCII to make it acceptable for mail transfer. Thus it specifies the method used to encode the message into 0s and 1s for transport. The content transfer encoding field is represented as :

Content-transfer-encoding : <type>

The various encoding methods used are given in the table below:



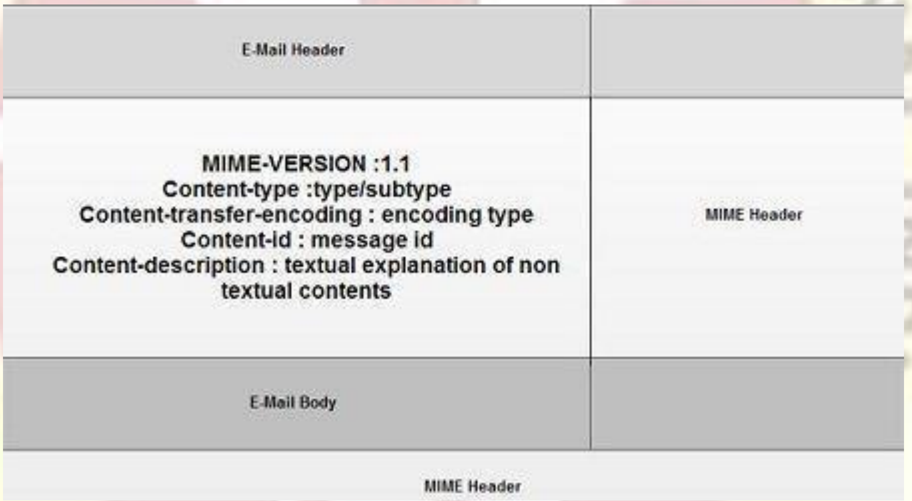
Type	Deseription
7- bit	The body contains The 7- bit ASCII Characters With maximum length of 1000 characters
8- bit	There can be non-ASCII 8- bit characters but the maximum length of the body is limited to 1000 characters.
Binary	Binary 8- bit characters without limitation of 1000 characters in the body.
Quoted-printable	This is useful when data consists of largely printable characters. Characters in the rang decimal equivalent 33 to 61 in ASCII are represented in ASCII. Others are represented as two- digit hex representation preceded by '=' sign, Non- text characters are replaced with six -digit hex sequence
Base 64	6-bit block of input data is encoded into 8-bit block of output.

4. Content-Id. It is used to uniquely identify the MIME entities in multiple contexts i.e. it uniquely identifies the whole message in a multiple message environment. This fieldis represented as:

Content-id : id = <content-id>

5. Content-description. It is a plaintext description of the object within the body; It specifies whether the body is image, audio or video. This field is represented as: **Content-description: <description>**

The various fields in the MIME header are



MIME-VERSION :1.1
Content-type :type/subtype
Content-transfer-encoding : encoding type
Content-Id : message id
Content-description : textual explanation of non textual contents

S / MIME

S/MIME stands for Secure Multipurpose Internet Mail Extension.S/MIME is a secure e-mail standard.

Working of S/MIME

S/MIME approach is similar to PGP. It also uses public key cryptography, symmetric key cryptography, hash functions, and digital signatures. It provides similar security services as PGP for e-mail communication.

The most common symmetric ciphers used in S/MIME are RC2 and TripleDES. The usual public key method is RSA, and the hashing algorithm is SHA-1 or MD5.

S/MIME specifies the additional MIME type, such as “application/pkcs7-mime”, for data enveloping after encrypting.

The whole MIME entity is encrypted and packed into an object. S/MIME has standardized cryptographic message formats.

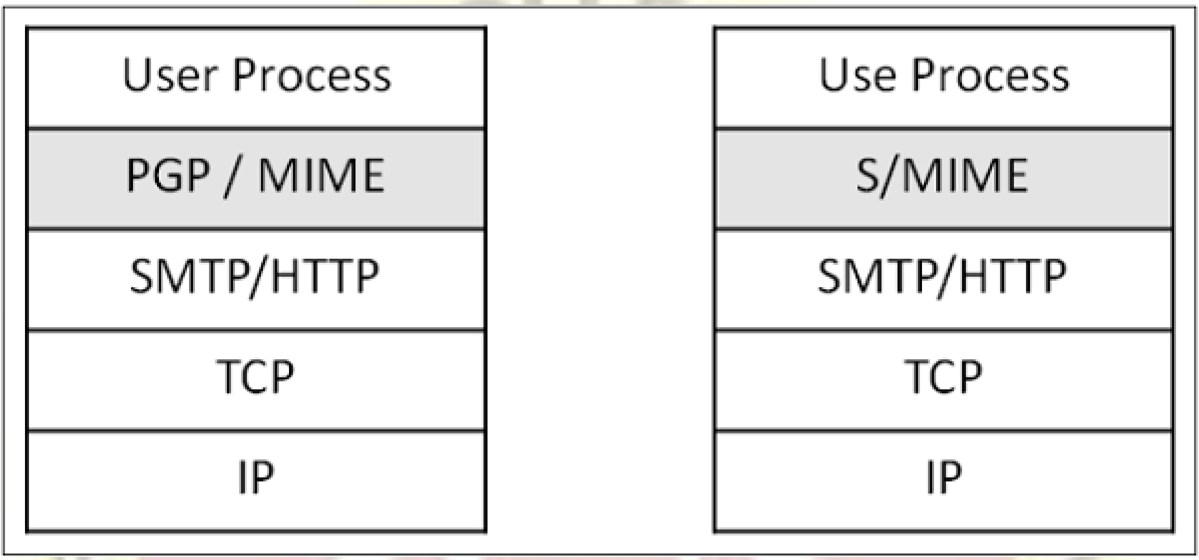
MIME is extended with some keywords to identify the encrypted and/or signed partsin the message.

S/MIME relies on X.509 certificates for public key distribution.

Employability of S/MIME

Due to the requirement of a certificate from certification authority for implementation,not all users can take advantage of S/MIME, as some may wish to encrypt a message,with a public/private key pair. For example, without the involvement or administrativeoverhead of certificates.

Implementation layer in network architecture for PGP and S/MIME schemes is shown in the following image. Both these schemes provide application level security of for e-mail communication.



For e-mail security over Internet, where mails are exchanged with new unknown usersvery often, S/MIME is considered as a good option.

S/MIME stands for Secure Multipurpose Internet Mail Extension. S/MIME is a secure e-mail standard.

S/MIME is employed to encrypt MIME data—emails in simple terms. S/MIME, basedon Public Key Infrastructure or Asymmetric Encryption, facilitates email security by using encryption, authentication, and integrity.

Working of S/MIME

S/MIME approach is similar to PGP. It also uses public key cryptography, symmetrickey cryptography, hash functions, and digital signatures.

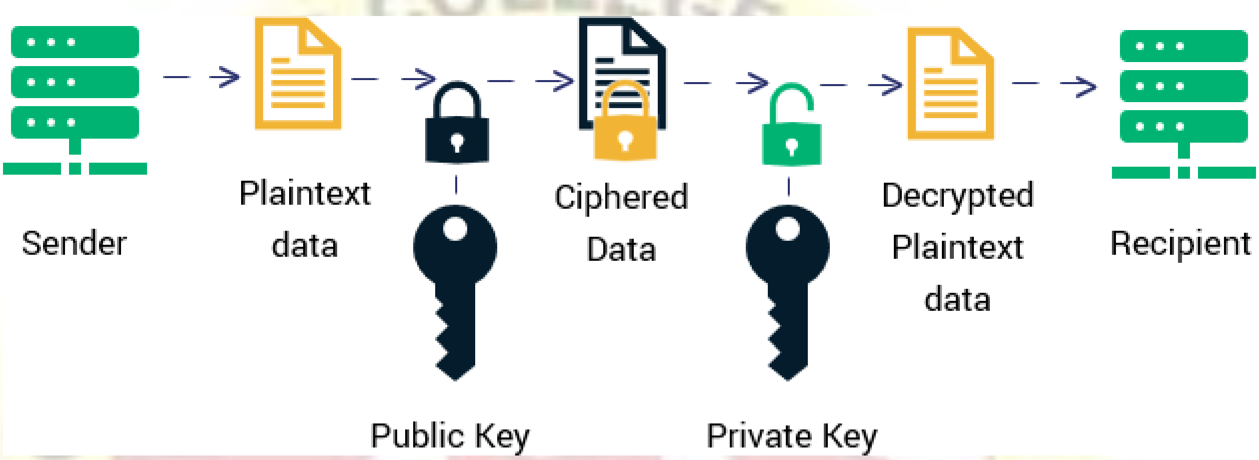
The most common symmetric ciphers used in S/MIME are RC2 and Triple DES. The usual public key method is RSA, and the hashing algorithm is SHA-1 or MD5. S/MIME specifies the additional MIME type, such as “application/pkcs7-mime”, fordata enveloping after encrypting. The whole MIME entity is encrypted and packed into an object.S/MIME has standardized cryptographic message formats.

MIME is extended with some keywords to identify the encrypted and/or signed parts in the message.

S/MIME relies on X.509 certificates for public key distribution

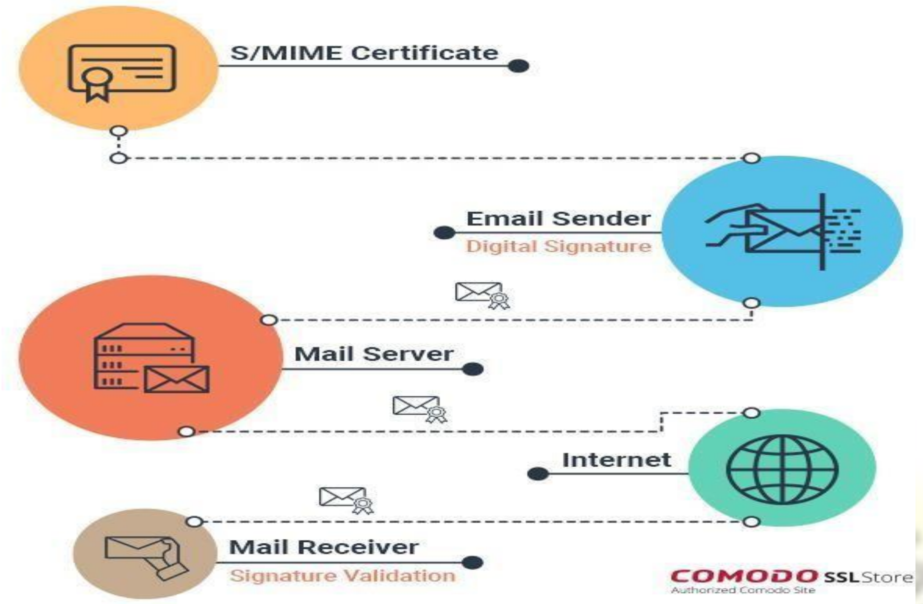
S/MIME certificate are based on asymmetric encryption. That's why they involve twodistinct keys – a public key and a private key. The public key and private key come ina pair, one public key can only have one private key and vice versa. This is because they're mathematically related to each other, the public key is actually derived from the private key.

The graphic below illustrates how asymmetric encryption works to encrypt and decryptplaintext information.

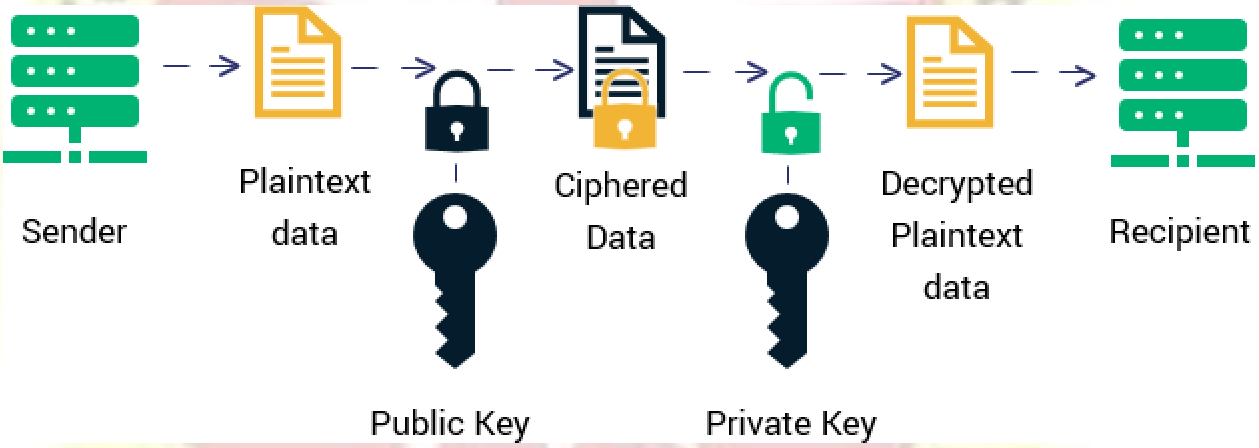


The way this works is as follows:

- A digital signature is associated with two keys, a private key, and a public key.
- Authentication is done using the public key, whereas the private key is used togenerate the signature itself.
- The public key is sent along with every protected email message to assert theidentity of the sender.
- The private key, on the other hand, generates and applies the unique digitalsignature to each email.
- Signatures verify that the message is unaltered and not tampered by an unauthorized third-party



The graphic below illustrates how asymmetric encryption works to encrypt and decrypt plaintext information.



The way this works is as follows:

- A digital signature is associated with two keys, a private key, and a public key.
- Authentication is done using the public key, whereas the private key is used to generate the signature itself.
- The public key is sent along with every protected email message to assert the identity of the sender.
- The private key, on the other hand, generates and applies the unique digital signatureto each email. Signatures verify that the message is unaltered and not tampered by an unauthorized third-party.

S/MIME (Secure / Multipurpose Internet Mail Extension)

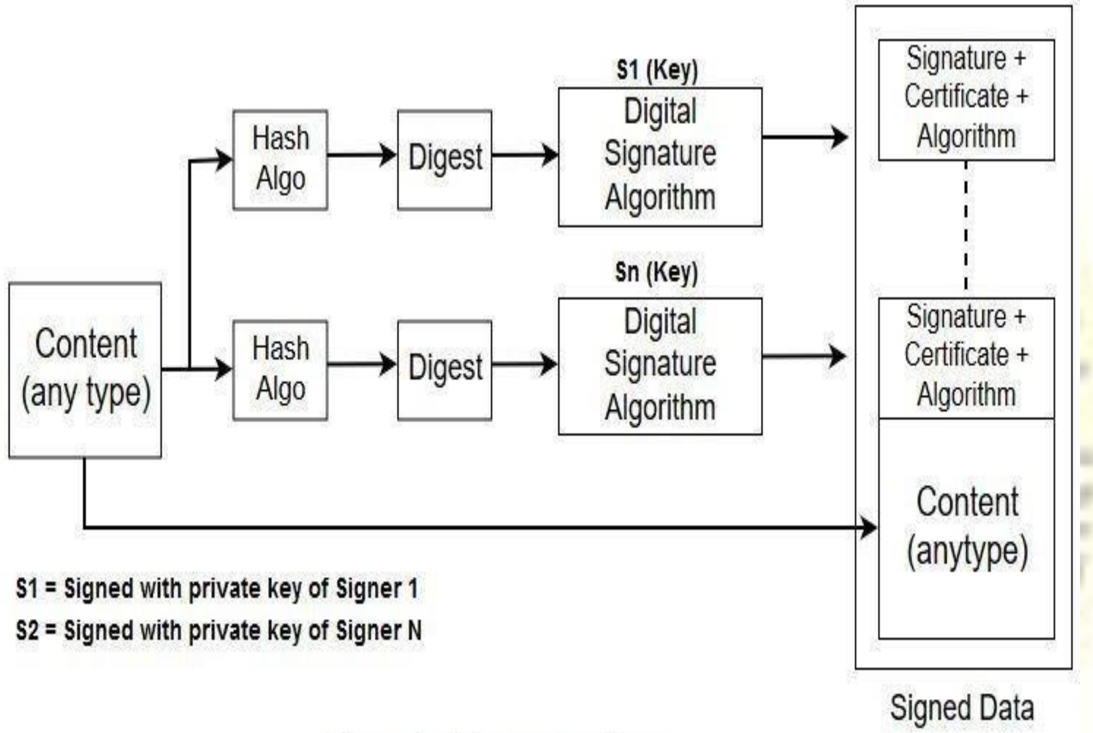
- It is enhancement of MIME protocol. -SI MIME adds some new content types to include security service to the MIME. All these new types include the parameter " application / pkcs7-mime", in which 'pkcs' defines "Public Key cryptography Specification"

Cryptographic Message Syntax (cms)

- S/MIME has defined CMS, the syntax in each case defined the exact encoding scheme for each content type. following content type describe the type of message & different sub types that are created from the messages.

a.Data content types: - This is an arbitrary string. The object created is called Data. b.Signed- Data content type: - This type provides only integrity of data. It contains anytype & zero or more signature values. The encoded result is called signed data. figurebelow shows the process of creating an object of this type. following are the steps in the process

1. for each signer ,a message digest is created from the content using a specific header algorithm chosen by that signer.
2. Each message digest is signal with the private key of the signs.
3. The content signature values , certificates are then collected to create the 'signed dataobject'.

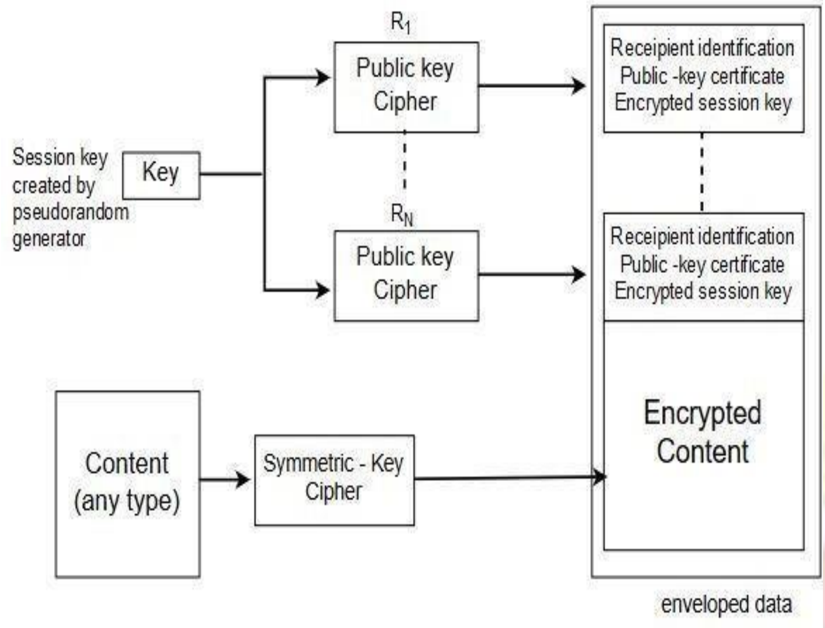

S1 (Key)
Hash Algo
Digest
Digital Signature Algorithm
Sn (Key)
Content (any type)
Hash Algo
Digest
Digital Signature Algorithm
Signature + Certificate + Algorithm
Signature + Certificate + Algorithm
Content (anytype)
Signed Data
S1 = Signed with private key of Signer 1
S2 = Signed with private key of Signer N

Signed - data content type

c. Enveloped -Data content type :

This type is used to provide privacy for the message. It contains any type & zero or more encrypted keys & certificated. The encoded result is an object called enveloped data . Below figure shows the process of creating an object of this type.

1. A pseudorandom session key is created for the symmetric key algorithm to beused.
2. For each recipient, a copy of the session key is encrypted with the public key of each recipient.
3. The content is encrypted using the defined Algorithm & created session key.
4. The encrypted contents, encrypted session keys, algorithm used & certificate are encoded using radix.



Enveloped data content type

d. Encrypted data type content type :

This type is used to create an encrypted session of any content type. This is similar to the enveloped data content type, the encrypted data content type has no recipient. It can be used to store the encrypted data instead of transmitting it. The process is very simple , the user employs any key & any algorithm to encrypt the content. The encrypted content is stored without including the key or the algorithm.The object created is called encrypted data.

e. Authenticated -Data content type: This type is used to provide authentication of the data. The object is called authenticated Data. figure below shows the process.

1. using a pseudorandom generator, a MAC key is generated for each recipient. 2.The MAC key is encrypted with the public key of the recipient.
1. A MAC is created for the content.4.The content MAC, algorithms & other information are collected together to for the authenticated Data object.

Key Management. 1. The key management in S/MIME is a combination of key management used by X.509 & PGP. S/MIME uses public-key certificates signed by the certificate authorities defined by X.509. However, the user is responsible to maintain the web of trust to verify the signature as defined by PGP.

Applications of S/MIME :- It is predicted that S/MIME will become the industry choice to provide security for commercial email.

*****