



SURESH
GYAN VIHAR
UNIVERSITY
Accredited by NAAC with 'A+' Grade

Bachelor of Computer Application

(B.C.A.)

E-Commerce Concepts
Semester-II

Author- Anshu Vyas

SURESH GYAN VIHAR UNIVERSITY
Centre for Distance and Online Education
Mahal, Jagatpura, Jaipur-302025

EDITORIAL BOARD (CDOE, SGVU)

Dr (Prof.) T.K. Jain
Director, CDOE, SGVU

Dr. Dev Brat Gupta
*Associate Professor (SILS) & Academic
Head, CDOE, SGVU*

Ms. Hemlalata Dharendra
Assistant Professor, CDOE, SGVU

Ms. Kapila Bishnoi
Assistant Professor, CDOE, SGVU

Dr. Manish Dwivedi
*Associate Professor & Dy, Director,
CDOE, SGVU*

Mr. Manvendra Narayan Mishra
*Assistant Professor (Deptt. of Mathematics)
SGVU*

Ms. Shreya Mathur
Assistant Professor, CDOE, SGVU

Mr. Ashphaq Ahmad
Assistant Professor, CDOE, SGVU

Published by:

S. B. Prakashan Pvt. Ltd.

WZ-6, Lajwanti Garden, New Delhi: 110046

Tel.: (011) 28520627 | Ph.: 9205476295

Email: info@sbprakashan.com | Web.: www.sbprakashan.com

© SGVU

All rights reserved.

No part of this book may be reproduced or copied in any form or by any means (graphic, electronic or mechanical, including photocopying, recording, taping, or information retrieval system) or reproduced on any disc, tape, perforated media or other information storage device, etc., without the written permission of the publishers.

Every effort has been made to avoid errors or omissions in the publication. In spite of this, some errors might have crept in. Any mistake, error or discrepancy noted may be brought to our notice and it shall be taken care of in the next edition. It is notified that neither the publishers nor the author or seller will be responsible for any damage or loss of any kind, in any manner, therefrom.

For binding mistakes, misprints or for missing pages, etc., the publishers' liability is limited to replacement within one month of purchase by similar edition. All expenses in this connection are to be borne by the purchaser.

Designed & Graphic by : S. B. Prakashan Pvt. Ltd.

Printed at :

Syllabus

e-Commerce Concepts

Learning Objectives

- Students will learn the basic aspects of information technology and occurrence of E-commerce.
- Will be able to understand the functioning of market in online mode, related threats, advantages, etc.
- Will be able to understand the difference in conventional marketing and E-Marketing.
- Will be able to learn about the ethics in the field of E-commerce.

Unit 1

Overview of developments in Information Technology and Defining E-Commerce: The scope of E commerce, Electronic Market, Electronic Data Interchange, Internet Commerce, Benefits and limitations of E-Commerce, Produce a generic framework for E-Commerce, Architectural framework of Electronic Commerce, Web based E Commerce Architecture.

Unit 2

Traditional retailing and e retailing, Benefits of e retailing, Key success factors, Models of e retailing, Features of e retailing. E services: Categories of e-services, Web-enabled services, matchmaking services, Information-selling on the web, e entertainment, Auctions and other specialized services. Business to Business Electronic Commerce.

Unit 3

Benefits of EDI, EDI technology, EDI standards, EDI communications, EDI Implementation, EDI Agreements, EDI Security. Electronic Payment Systems, Need of Electronic Payment System: Study and examine the use of Electronic Payment system and the protocols used, Study Electronic Fund Transfer and secure electronic transaction protocol for credit card payment. Digital economy: Identify the methods of payments on the net – Electronic Cash, cheques and credit cards on the Internet.

Unit 4

Virus, Cyber Crime Network Security: Encryption, Protecting Web server with a Firewall, Firewall and the Security Policy, Network Firewalls and Application Firewalls, Proxy Server.

Unit 5

Understanding Ethical, Social and Political issues in E-Commerce: A model for Organizing the issues, Basic Ethical Concepts, Analyzing Ethical Dilemmas, Candidate Ethical principles Privacy and Information Rights: Information collected at E-Commerce Websites, The Concept of Privacy,

Legal protections Intellectual Property Rights: Types of Intellectual Property protection, Governance.

References

- Elias. M. Awad, " Electronic Commerce", Prentice-Hall of India Pvt Ltd.
- RaviKalakota, Andrew B. Whinston, "Electronic Commerce-A Manager's guide", Addison-Wesley.
- Efraim Turban, Jae Lee, David King, H.Michael Chung, "Electronic Commerce–A ManagerialPerspective", Addison-Wesley.
- Elias M Award, "Electronic Commerce from Vision to Fulfilment", 3rd Edition, PHI.
- Judy Strauss, Adel El-Ansary, Raymond Frost, "E-Marketing", 3REdition, Pearson Education.

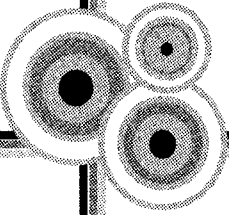
Contents

1.	Introduction to Electronic Commerce	30
1.	E-Commerce	1-1
2.	Main Activities of E-Commerce	1-2
3.	Goals of E-Commerce	1-3
4.	Technical Components of E-Commerce	1-4
5.	Functions of E-Commerce	1-7
6.	Advantages and Disadvantages of E-Commerce	1-7
7.	Scope of E-Commerce	1-11
8.	Electronic Commerce Applications	1-12
9.	Electronic-Business	1-18
10.	E-Commerce v/s E-Business	1-20
2.	Building Own Website	26
1.	Introduction	2-1
2.	What does a Website do?	2-1
3.	Reasons to Build a Website	2-3
4.	Benefits of Having a Website	2-4
5.	Bandwidth Requirements	2-6
6.	Cost of Building a Website	2-8
7.	Time Consumed	2-11
8.	Reach or Accessibility of Website	2-12
9.	Register a Domain Name	2-15
10.	Web Promotion	2-17
11.	Banner Exchange	2-19
12.	Shopping Bots	2-22
13.	Target E-mails	2-23
3.	Internet and Extranet	31
1.	Internet	3-2
2.	Tools and Services of Internet	3-4
3.	Hardware and Software for Internet	3-5
4.	Advantages and Disadvantages of Internet	3-7
5.	Intranet	3-8
6.	Software of Intranet	3-9
7.	Intranet Security	3-10
8.	Planning and Creating an Intranet	3-11
9.	Advantages and Disadvantages of Intranets	3-12
10.	Features of Intranet	3-14
11.	Components of Intranet Information Technology Structure	3-15
12.	Extranet	3-17
13.	Applications of Extranet	3-17
14.	Advantages and Disadvantages of Extranet	3-20
15.	Internet versus Intranets	3-20
16.	Extranet Versus Intranet	3-22
17.	Development of Intranet	3-22
	Electronic Payment System	36
1.	Introduction	4-1
2.	Requirements for Electronic Payment System	4-2

3.	Characteristics of Electronic Payment System	4-2
4.	Traditional Payment System	4-3
5.	Process of Electronic Payment System	4-3
6.	Types of Electronic Payment Systems	4-5
7.	E-Payment Tools	4-10
8.	Electronic Funds Transfer	4-21
9.	Payment Cards	4-23
10.	Micropayment and Other Payment Systems	4-25
11.	Electronic Bill or Paperless Bill Presentment and Payment	4-26
12.	Need of E-payment	4-28
13.	Payment Considerations	4-28
14.	Using Payment Service Providers	4-29
15.	Value Exchange System	4-31
16.	Modern/ Mobile Payment of Cash	4-31
5.	Technology Solution	26
1.	Introduction	5-1
2.	Protecting Internet Communications	5-2
3.	Encryption	5-3
4.	Symmetric-Key Encryption	5-9
5.	Public Key Encryption	5-11
6.	Public Key Encryption using Digital Signatures	5-14
7.	Digital Envelopes	5-18
8.	Digital Certificates	5-21
9.	Limitations to Encryption Solutions	5-23
6.	E-com Security	26
1.	Introduction	6-1
2.	E-Commerce Security Environment	6-2
3.	Security Threats in E-commerce Environment	6-4
4.	Malicious Code and Unwanted Programs	6-5
5.	Phishing and Identity Theft	6-7
6.	Hacking and Cyber Vandalism	6-11
7.	Credit Card Fraud/Theft	6-13
8.	Spoofing	6-16
9.	Denial of Service (DOS)	6-18
10.	Distributed Denial-of-Service Attack (DDoS)	6-23

* * *

INTRODUCTION TO ELECTRONIC COMMERCE



1. E-Commerce

Computerization has increased and triggered major changes in the organization of work. Re-engineering of paper work is done to gain the benefit of doing business electronically. Businesses are implementing E-commerce to meet the demand of a crucial and increasingly competitive world.

Electronic commerce, commonly known as E-commerce refers to a wide range of online business activities for products and services. It also pertains to *“any form of business transaction in which the parties interact electronically rather than by physical exchanges or direct physical contact.”* E-commerce is related with buying and selling over the Internet, or conducting any transaction involving the transfer of ownership or rights to use goods or services through a media of computer network.

Definition

“E-commerce is the use of electronic communications and digital information processing technology in business transactions to create, transform, and redefine relationships for value creation between or among organizations, and between organizations and individuals”.

Electronic commerce is the process of buying and selling products and services on Internet and other computer networks.

The spread of the Internet has increased the amount of trade conducted electronically. A wide variety of E-commerce is encouraging innovations in electronic funds transfer, supply chain management, Internet marketing, online transaction processing, Electronic Data Interchange (EDI), inventory management systems, and automated data collection systems. E-commerce normally uses the World Wide Web for the transaction lifecycle, also it includes a wider range of technologies such as E-mail.

E-commerce is conducted completely electronically for virtual items like access to premium content on a website, but most electronic commerce involves the transportation of physical items. Online retailers are known as E-tailers and online retail is known as E-tail. More or less all big retailers have electronic commerce presence on the World Wide Web.

E-commerce comprises:

- i. E-tailing or 'virtual storefronts' on websites with online catalogs, sometimes gathered into a 'virtual mall'.
- ii. The gathering and use of demographic data through Web contacts.
- iii. Electronic Data Interchange (EDI), the business-to-business exchange of data.
- iv. E-mail and fax used as media for reaching prospective and established customers.
- v. Business-to-business buying and selling
- vi. The security of business transactions

Electronic commerce use telecommunications and data processing technology to advance the quality of transactions between business partners. E-commerce has improved the organizational competence by leveraging data processing, database storage, and data communications technologies. Existing network facilities saves labour costs and reduces the paper storage and handling facilities. It facilitates companies to be more effective in improving the quality of standard goods and services and to offer a variety of new services. The global marketplace has become larger and wider than ever, the reason being the expansion of E-commerce activity.

2. Main Activities of E-Commerce

The nine essential activities of E-commerce:

- i. Access control and security
- ii. Profiling and personalizing
- iii. Search management
- iv. Content management
- v. Catalog management
- vi. Payment
- vii. Workflow management
- viii. Event notification
- ix. Collaboration and trading

The nine essential activities of E-commerce consist of:

- i. **Access control and security:** E-commerce processes establish mutual trust and secure access between the parties in an E-commerce transaction by authenticating users, authorizing access, and enforcing security features.
- ii. **Profiling and personalization:** Profiling processes gather data on an individual and the website performance and preferences, and build electronic profiles of the characteristics and inclinations. User profiles are developed using profiling

tools such as user registration, cookie files, website behavior tracking software, and user feedback.

- iii. **Search management:** Efficient and effective search processes provide a top E-commerce website capability that helps customers find the specific product or service they want to evaluate or buy.
- iv. **Content and catalog management:** Content management software helps E-commerce companies develop, generate, deliver, update, and archive text data, and multimedia information at E-commerce websites. Generating and managing catalog content is a major subset of content management.

Content and catalog management has expanded to include product configuration processes that support Web-based customer self service and the mass customization of a company's products. Configuration software helps online customers to select the best possible set of product features that can be included in a finished product.

- v. **Payment:** The digital financial payment helps E-commerce companies for transaction involving currency transfer between two or more parties.
- vi. **Workflow management:** E-business workflow systems help employees electronically collaborate to achieve structured work tasks within knowledge E-based business processes. Workflow management in both E-business and E-commerce depends on workflow software which contains software models of the business processes to be accomplished. The workflow model expresses the predefined sets of business rules, roles of stakeholders, authorization requirements, routing alternatives, databases used, and sequence of tasks required for each E-commerce process.
- vii. **Event notification:** Many E-commerce applications are event-driven systems that respond to a huge number of events. Event notification processes play an important role in E-commerce systems, since customers, suppliers, employees, and other stakeholders must be notified of all events that might affect their status in a transaction.
- viii. **Collaboration and trading:** This processes support the vital collaboration arrangements and trading services needed by customers, suppliers, and other stakeholders to accomplish E-commerce transactions.

3. Goals of E-Commerce

- i. **To facilitate the globalization of business:** E-commerce facilitates the globalization of business by providing some economical access to distant markets and by supporting new opportunities for firms to increase economies by distributing their products internationally.

Number of business
2
 quotes

Oct. 2012 – 15M

What is E-commerce?
 Explain goals of
 E-commerce along with
 its advantages and
 disadvantages.

Apr. 2013 – 4M

Write a short note:
 Goals of E-commerce.

- ii. **To provide purchasing opportunities for the buyer:** As E-commerce increases sales opportunities for the seller, it also increases purchasing opportunities for buyer.
- iii. **To reduce staffing cost:** As in E-commerce, the selling and purchasing process is online, the amount of interaction with the staff is minimized.
- iv. **Market based expansion:** An E-commerce is open to an entirely new group of users, which include employees, customers, suppliers and way business partners. It opens new markets, enabling to reach new customers.

It also enables easier and faster for organization to do business with existing customer base.

- v. **To increase profits:** With E-commerce, companies reach more and more customers where physical commerce cannot reach. Also applications provide business solutions that improve the quality of goods and services, increase the speed of service delivery, and reduce the cost of business operations, thus increasing profits.
- vi. **Increased customer service and loyalty:** E-commerce enables a company to be open for business wherever a customer needs it. Tracking customer satisfaction, requesting more customer feedback, and presenting custom solutions for the clients are just some of the opportunities that E-commerce offers.
- vii. **Increase speed and accuracy:** E-commerce sees the speed and accuracy with which business can exchange information, which reduces cost on both sides of transactions. It is available 24 hours a day and 7 days a week.
- viii. **Reduction of paper storage:** Ordering, invoicing and customer support, to network-based system can also reduce the paperwork involved in business-to-business transactions.
- ix. **Increased response times:** In E-commerce, the interaction with the system takes place in real time and therefore allows customer or bidder to respond more quickly and thus reduces the time of discussion between them as in traditional commerce.

4. Technical Components of E-Commerce

► Integrated Services Digital Network (ISDN)

ISDN, stands for Integrated Services Digital Network, is a system of digital phone connections. This system allows voice and data to be transmitted simultaneously across the world using end-to-end digital connectivity.

ISDN telephones provide a much clearer voice signal and dialing is much faster. PCs equipped with a TA card can connect to the Internet, or another PC, in a fraction of a second.

Data transmission is faster than the best modems (64 or 128 Kbits/s). ISDN is available as basic rate (equivalent to the capacity of two phone lines or 128 Kbits/s) for domestic or small office use, which gives an aggregate bandwidth of over 2 Mbits/s. It is used to connect a remote office to a main office computer network so that an executive can work remotely but have all the benefits of being in the main office.

However, one of the drawbacks to using ISDN is that it is still essentially a dial-up service, and each channel is charged at normal telephone rates. So using both channels becomes quite expensive.

► **Broadband**

Broadband refers to telecommunication in which a wide band of frequencies is available to transmit information.

Broadband services are based on a number of transmission technologies:

- i. **DSL (Digital Subscriber Line) services** that make use of existing telephony infrastructure.
- ii. **Cable Modem services**, that make use of cable TV infrastructure.
- iii. **Metropolitan Area Ethernet services**, that generally require the installation of new cable infrastructure, often based on fiber optic cabling, although some variants of this technology make use of DSL technology.
 - a. **ADSL:** The most common DSL service available is the ADSL service in which the 'A' is 'Asymmetric'. It means that the data transfer rates in both the directions are not same. The transmission rate from the subscriber to the Internet is lower than that in the reverse order. The data rates available with ADSL, and in fact the actual availability of ADSL, depends critically on the distance between the subscriber and the nearest digital telephone exchange, and also on the number of subscribers that are using the service.
 - b. **Cable Modems:** The Cable Modem services presented by the cable TV companies are only available in those areas which are already served by a cable TV network. The data transmission rates available with these services are comparable to ADSL. With both ADSL and Cable Modem services, it is a simple matter to connect the cable modem or the ADSL filter into an existing LAN, allowing the external Internet connection to be accessed by all of the PCs connected to the LAN.
 - c. **Metropolitan Area Ethernet Services:** Metropolitan Area Ethernet services provide significantly higher data transmission rates. This allows data rates of up to 10

Number of Questions
2

Oct. 2012 – 4M

Write short note:

Technical Components of E-commerce

Apr. 2012 – 10M

What do you mean by E-commerce? Explain different technical components of E-commerce.

Gigabits/second to be achieved between the customer location and the service provider. This is used in order to allow a large company that was spread across a number of sites to interconnect their LANs, making them appear like one single LAN from the point of view of the users.

► Leased Lines

Telecom operators have diverse choices for permanent connections for data transmission. These include ISDN, connections available from 'network providers', companies which have private network capacity who lease some or all of their capacity from telecoms companies. Leased lines is used to connect LANs into a WAN (*for example*, head office to a branch) or for teleconferencing.

► Wireless Networking

Wireless network refers to a computer network that is wireless, and is related with a telecommunications network whose interconnections between nodes are implemented without the use of wires. Wireless telecommunications networks are executed with remote information transmission system that uses electromagnetic waves, such as radio waves, for the carrier and this implementation usually takes place at the physical level or 'layer' of the network

Two relatively new networking technologies are:

- i. 802.11 Wireless LANs, known as 'Wi-Fi'
 - ii. Bluetooth.
- i. **Wireless LAN:** A wireless LAN provides a wireless connection between a computer system and the LAN, via a wireless access point. The data transmission rates that can be achieved are comparatively low to 10 Megabits/second Ethernet LAN, but are ample for connecting the average PC or laptop to a LAN. Wireless access points have an Ethernet port that allows them to be connected to a conventional wired LAN backbone, but for small business use, it is possible to network a number of PCs together using only a wireless access point. The range of transmission is variable, depending on the construction of the building that it is used in. It covers distances of up to 100 meters under the right conditions.
- ii. **Bluetooth:** Bluetooth is an open wireless technology used for exchanging data over short distances using short wavelength radio transmissions from fixed and mobile devices, creating personal area networks (PANs) with high levels of security. It is used to connect a palmtop computer to a host PC, or to connect a hands free kit to a mobile phone. The transmission range for Bluetooth is significantly shorter as less power is needed to drive the radios in Bluetooth devices.

5. Functions of E-Commerce

► Customer's View

From a customer's view, the function of an electronic-commerce system is to enable the customer to locate and purchase a desired product or service over the Internet when, he or she wants it. Its function is no more or less than providing a virtual store.

► Merchant's View

From a merchant's view, the key function of an electronic commerce system is to generate higher revenues than the merchant would attain without the system. For this the electronic commerce system utilizes existing data and business processes. All of the processes are same that the merchant has in place to support an in-store or catalog purchase for electronic items like product information, inventory systems, customer service, and transaction capabilities, along with credit authorization, tax computation, financial settlement, and shipping.

Additional functions of an electronic commerce system, is to help redefine and enhance an enterprise's brand strength, customer-service capability, and supply-chain effectiveness.

Number of business solutions

1

Apr.2011 – 10M

What do you mean by E-Commerce? Elaborate on the functions of E-commerce.

6. Advantages and Disadvantages of E-Commerce

Advantages

The advantages of E-commerce are basically to increase sales and decrease costs through the use of electronically media. The greatest and the most important advantage of E-commerce is that it enables a business concern or individual to reach the global market. It accommodates the demands of both the national and the international market. With the help of electronic commerce, even small enterprises can access the global market for selling and purchasing products and services. Even time restrictions are non-existent while conducting businesses, as E-commerce empowers one to execute business transactions 24 × 7. This in turn significantly increases sales and profit. Electronic

commerce provides the customers an opportunity to look for cheaper and quality products. With the help of E-commerce, consumers can easily research on a specific product and even find out the original manufacturer to purchase a product at a much cheaper price than that charged by the wholesaler. Shopping online is usually more convenient and time saving than conventional shopping. Also the reviews posted by other customers about the products purchased from a particular E-commerce site are very helpful to make purchasing decisions.

For business concerns, E-commerce significantly cuts down the cost associated with marketing, customer care, processing, and information storage and inventory management. It reduces the time period involved with business process re-engineering, customization of products to meet the demand of particular customers, increasing productivity and customer care services. Electronic commerce reduces the burden of infrastructure to conduct businesses and thereby raises the amount of funds available for profitable investment. It also enables efficient customer care services. On the other hand, it collects and manages information related to customer behavior, which in turn helps to develop and adopt an efficient marketing and promotional strategy.

► **Advantages to Organizations**

Through the Internet, E-commerce offers a wide range of choices and higher levels of customer information and details for individuals to search and compare. Some build-to-order companies provide a competitive advantage by inexpensive customization of products and services.

E-commerce helps organizations to decrease costs in creating, processing, distributing, storing and retrieving information. The communication and advertising costs lower down by sending E-mails and using online advertising channels.

E-commerce has extended trading hours, i.e., 24 hours a day, 7 days a week in 365 days. It provides the up-to-date company material, current inventories, improved customer service, better customer's communication, increased operating and trading flexibility.

► **Advantages to Consumers**

For customers, the advantages are the buying process, product research, evaluation and execution. E-commerce provides customers with a platform to search for product information through global markets with a wider range of choices, which makes comparison and evaluation easier and more efficient. With the ubiquity (omnipresence) in accessing the Internet, consumers are able to search for shops or perform other transactions anytime in almost any location. Cheaper goods and services are the benefits for consumers who purchase online. Delivery time and costs are saved by buyers when they purchase digital goods and services.

► **Advantages to Society**

As individuals work and do their purchasing from home rather than travelling around, this helps in traffic and air pollution control. The service and products are available which were unavailable in the

past, opportunities and higher education services are more achievable for students. Non-profit organizations, including government services, have benefited from E-commerce by the online payment system which supports the payment of tax refunds and pensions quickly and securely. Public services such as health care, education, and public social service also benefit from E-commerce. Rural doctors and nurses can access professional information and the latest health care technologies. E-commerce makes products and services easily available without geographic limitations.

E-commerce offers buyers maximum convenience. They visit the websites of multiple vendors round-the clock a day to compare prices and make purchases, without having to leave their homes or offices from around the globe. Consumers can immediately obtain a product or service, like an electronic book, a music file, or computer software, by downloading it over the Internet.

For sellers, E-commerce helps in cost effectiveness and expands their markets. Building, staffing, or maintaining a physical store or print and distribution of mail order catalogs are not required. Automated order tracking and billing systems cut additional labour costs. The products are sold over the global Internet; sellers have the potential to market their products or services globally and are not limited by the physical location of a store. Internet technologies also permit sellers to track the interests and preferences of their customers with the customer's permission and then use this information to build an ongoing relationship with the customer by customizing products and services to meet their needs.

► **100% Business Uptime**

E-commerce systems are available to people 24 hours a day, 7 days a week and 365 days a year. They never take a break or close down for the day or take public holidays.

► **Global Access**

E-commerce system is accessible by anyone across the World Wide Web. Any person or business having just an Internet connection can access E-commerce systems.

► **Quick Response Time**

Transaction is handled over the Internet instantaneously without high response times, most of the times much faster than offline systems. Messages are delivered to the end of the globe at the snap of a finger, enabling quick commerce.

► **Cost Efficiency**

E-commerce is very cost efficient and economical. General costs of running a business otherwise are far higher than that operated with the help of technology and E-commerce. Staffing, middlemen, overhead costs, etc. can be reduced drastically, making business handling and administration much more easy by the electronic transaction procedures.

Disadvantages of E-Commerce

Electronic commerce has some limitations which has restricted the number of people to use this. One disadvantage of E-commerce is that a number of people are still not aware of the Internet, either due to lack of knowledge or trust. A large number of people do not use the Internet for financial transaction. Many refuse to trust the authenticity of completely unfriendly business transactions. Many people are suspicious regarding the requirement to disclose personal and private information for security concerns.

Another disadvantage of E-commerce is that it is not suitable for perishable commodities like food items. People prefer to shop in the conventional way than to use E-commerce for purchasing food products. The time period required for delivering physical products is quite extensive. A lot of phone calls and E-mails may be required to get the desired products. Returning the product and getting a refund can be even more troublesome and time consuming than purchasing.

► Delivery Time

Physical goods take more time to reach than shopping done in the local store. Delivery times may range anywhere from a day to even a month. Moreover, perishable goods cannot be shipped over such a long delivery time as they tend to get destroyed during transit.

► Hesitancy

Most customers and businesses are hesitant to do transactions online. Some people are familiarized to shop with family and friends and hang out at malls and big outlets, which is not available on the Internet.

Online furniture businesses have failed for the most part because customers want to test the comfort of an expensive item such as a sofa before they purchase it. Many people also consider shopping a social experience. Consumers also need to be at peace that credit card transactions are secure and that their privacy is respected.

► Online Safety

Online safety is a critical factor that most people consider before even thinking of performing commercial transactions. Customers and businesses should be assured of privacy implications, confidentiality, and security. An amount of trust has to be developed before starting or involving into transactions.

► Other Drawbacks

One of the biggest drawbacks of E-commerce is that many people are not satisfied with the virtual experience of trading and buying products lying possibly thousands of miles away just by sea.

picture. International trade, import/export and global sourcing all involve great geographical distances spanning over continents or nations, and this lack of physical proximity turns out to be a disadvantage sometimes. For many people E-commerce is not about big international trade, import/export or global sourcing but simply about enjoying shopping over the net. Sometimes the electronic experience does not satisfy their social or holiday needs, hence they distance themselves away from the concept of E-commerce. From the seller's point of view, E-commerce does not offer a direct face-to-face proximity with the probable customer and therefore things may not work out the way they would have done otherwise. However many times international trade, import/export and global sourcing does require personal interaction for a couple of times before things can later be carried out via E-commerce. Therefore in such cases, E-commerce tends to act as an extension of the trader for carrying out activities related to international trade, import/export and global sourcing rather than as an alternative for it.

For many products it is not possible to check them online for their effectiveness in terms of customer satisfaction parameters.

7. Scope of E-Commerce

- i. Marketing, sales and sales promotion
- ii. Pre-sales, subcontracts, supply
- iii. Financing and insurance
- iv. Commercial transactions: ordering, delivery, payment
- v. Product service and maintenance
- vi. Co-operative product development
- vii. Distributed co-operative working
- viii. Use of public and private services
- ix. Business-to-administrations (*For example, customs, etc*)
- x. Transport and logistics
- xi. Public procurement
- xii. Automatic trading of digital goods
- xiii. Accounting
- xiv. Dispute resolution

8. Electronic Commerce Applications

Number of questions asked
1

Oct. 2011 – 10M

What is E-commerce?
Brief its applications.

Electronic commerce is doing business online. It is about using the control of digital information to understand the needs and preferences of each customer and each partner; to customize products and services for them; and then to deliver the products and services as quickly as possible. Personalized, automated services offer business the potential to increase revenues, lower costs, and establish and strengthen customer and partner relationships.

To achieve these benefits, many companies engage in electronic commerce for direct marketing, selling, and customer service, online banking and billing; secure distribution of information, value chain trading, and corporate purchasing.

Business communicates with customers and partners through channels. The Internet is one of the latest and, for many purposes, the best business communications channel. It is fast, reasonably reliable, inexpensive, and universally accessible. It reaches virtually every business and more than 100 million consumers. Joint online business is electronic commerce. The four main areas or application where companies conduct business online today are:

Four main applications where companies conduct business online today are

- i. **Direct marketing and selling:** It is the practice of delivering promotional messages directly to potential customers on an individual basis as instead of a mass medium. Many websites focus on direct marketing, selling, and service than on any other type of electronic commerce. Direct selling was the earliest type of electronic commerce, and has proven to be a stepping-stone for many companies. Business-to-consumer electronic commerce increases revenue by reaching the right customers. Targeted and automated up selling and cross selling are new fundamentals of online retailing.
- Sites that most frequently provide the best and most appropriate products and services are rewarded with stronger customer relationships, resulting in improved loyalty and increased value.
- ii. **Online Banking and billing:** It is a service offered by banks that allows account holders to access their account data via the Internet. To minimize the risk of fraud, online banking is enabled through a secure server, which grants the individual a private access to his or her bank account. Online banking is designed to streamline banking chores that otherwise require considerable time and effort. Online banking facilitates direct access to account details, enables transfer of funds, allows for multiple bills payments, and performs an array of other transactions. Online banking is available 24 hours, seven days a week, regardless of the bank's working hours. Online billing is the electronic delivery and presentation of financial statements, bills, invoices, and related information sent by a company to its customers.

Companies can achieve significant cost savings and marketing benefits through the use of Internet-based bill delivery and receiving systems.

- iii. **Secure Distribution of information:** To many businesses, information is their most valuable asset. Although the Internet can enable businesses to reach huge new markets for that information, businesses must also safeguard that information to protect their assets. Digital Rights Management provides protection for intellectual and information property, and is a key technology for secure information distribution.
- iv. **Value chain integration:** It is the process in which multiple enterprises within a shared market cooperatively plan, implement, and manage (electronically and physically) the flow of goods, services, and information from point of origin to point of consumption. It is done in such a manner that it increases customer-perceived value and optimizes the efficiency of the chain, creating competitive advantage for all stakeholders involved.

Delays in inventory tracking and management move from the cash register all the way back to raw material production, creating inventory shortages at any stage of the value chain. The resulting out-of-stock event means lost business. The Internet assures to increase business efficiency by reducing reporting delays and increasing reporting accuracy. Speed is clearly the business element crucial for the value chain. But the speed is costly.

- v. **Supply chain integration:** Supply chain integration uses the low cost of the Internet to highlight a tighter integration across suppliers, manufactures, and distributors. Many of the fundamentals of building a site, extensible order processing and integration with other systems remain the same as that in the direct marketing and selling scenario. But in the supply chain circumstances, new requirements arise including authenticated login, generating custom catalogs for key customers and pricing and payment based on custom agreements. Suppliers need to be able to provide their catalogs into another business's systems, with the ability to maintain these product catalogs when pricing and/or inventory changes.
- vi. **Corporate procurement:** Business influences the Intranet and the Internet to make existing business processes more efficient. At the heart of this business model are commerce solutions that facilitate that processes of purchasing low-cost, high volume goods for Maintenance, Repair and Operations (MRO) of a business. Labour and paper intensive operations are reconverted into self-service applications where purchase approvals and business policies are enforced through automated business rules.

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

Some other common applications of electronic commerce are:

- i. E-mail
- ii. Enterprise content management
- iii. Instant messaging
- iv. Newsgroups
- v. Online shopping and order tracking
- vi. Online banking
- vii. Online office suites
- viii. Domestic and international payment systems
- ix. Shopping cart software
- x. Teleconferencing
- xi. Electronic tickets

8.1 · Benefits of E-Commerce

E-commerce offers a competitive advantage. The market for E-commerce is growing; more consumers and businesses gain Internet access and transaction processing technologies improve security.

The benefits of E-commerce to a small business may include capabilities to:

- i. Extend the range of sales territory
- ii. Streamline communication to suppliers and clients
- iii. Expand reach to new clients
- iv. Improve service to existing clients
- v. Reduce paperwork and time spent on correspondence
- vi. Track customer satisfaction
- vii. Expedite billing
- viii. Improve collaboration on work projects
- ix. Expand markets beyond geographical, national boundaries
- x. Leverage legacy data
- xi. Improve inventory control, order processing
- xii. Establish position in emerging E-commerce marketplace
- xiii. Lower costs of overhead
- xiv. Realize economies of scale by increasing sales volume to new markets

- xv. Monitor competition and industry trends
- xvi. Improve or expand product lines - locate new suppliers, products that could be included in catalog.

The benefits to organizations are as follows:

- i. Electronic commerce expands the marketplace to national and international markets. With minimal capital outlay, a company can easily and quickly locate more customers, the best suppliers, and the most suitable business partners worldwide.
- ii. Electronic commerce decreases the cost of creating, processing, distributing, storing, and retrieving paper-based information.
- iii. Capability for creating highly specialized businesses.
- iv. Electronic commerce allows reduced inventories and overhead by facilitating 'pull'-type supply chain management. In a pull-type system, the process starts from customer orders and uses just-in-time manufacturing.
- v. The pull-type processing enables expensive customization of products and services, which provides competitive advantage to its implementers.
- vi. Electronic commerce reduces the time between the outlay of capital and the receipt of products and services.
- vii. Electronic commerce initiates business processes re-engineering projects. By changing processes, productivity of salespeople, knowledge of workers and administrators can increase by 100 percent or more.
- viii. Electronic commerce lowers telecommunications cost-the Internet is much cheaper than VANs.
- ix. Other benefits include improved image, improved customer service, newfound business partners, simplified processes, compressed cycle and delivery time, increased productivity, eliminating paper, expediting access to information, reduced transportation costs, and increased flexibility.

The benefits of EC to consumers are as follows:

- i. Electronic commerce enables customers to shop or do other transactions 24 hours a day, all year round, from almost any location.
- ii. Electronic commerce provides customers with more choices; they can select less expensive products and services by allowing them to shop in many places and conduct quick comparisons.
- iii. In some cases, especially with digitized products, electronic commerce allows quick delivery.
- iv. Customers can receive relevant and detailed information in seconds, rather than days or weeks.
- v. Electronic commerce makes it possible to participate in virtual auctions.
- vi. Electronic commerce allows customers to interact with other customers in electronic communities and exchange ideas as well as share experiences.
- vii. Electronic commerce facilitates competition, which results in substantial discounts.

The benefits of E-commerce to society are as follows:

- i. Electronic commerce enables more individuals to work at home and to do less travelling for shopping, resulting in less traffic on the roads and lower air pollution.
- ii. Electronic commerce allows merchandise to be sold at lower prices, so less wealthy people can buy more and increase their standard of living.
- iii. Electronic commerce enables people in rural areas to enjoy products and services that otherwise are not available to them. This includes opportunities to learn and earn college degrees
- iv. Electronic commerce facilitates delivery of public services, such as health care, education, and distribution of government social services at a reduced cost and/or improved quality. Health-care services, *for example*, can reach patients in rural areas.
- v. Expands markets from local to global.
- vi. Reduces costs with telecommunications and physical maintenance.
- vii. Minimizes resources used for storing physical receipts.
- viii. Instant product updates, including descriptions and pricing.
- ix. 24-hour store visibility to anyone with an Internet connection.
- x. Large portals enable large product bases, manufacturers and prices.
- xi. Search utilities far surpasses the speed used to find products through catalogs.
- xii. Encourages competition between small and large online retailers.

8.2 Limitations of E-Commerce

The limitations of E-Commerce can be grouped into technical and non-technical categories:

► Technical Limitations of E-commerce

- i. There is a lack of system security, reliability, standards, and some communication protocols.
- ii. There is insufficient telecommunication bandwidth.
- iii. The software development tools are still evolving and changing rapidly.
- iv. It is difficult to integrate the Internet and EC software with some existing applications and databases.
- v. Vendors may need special Web servers and other infrastructures, in addition to the network servers.
- vi. Some electronic commerce software may not fit with some hardware, or may be incompatible with some operating systems or other components.

► Non-technical Limitations

- i. **Cost and justification:** The cost of developing electronic commerce in-house can be very high, and mistakes due to lack of experience may result in delays. There are many opportunities for outsourcing, but where and how to do it is not a simple issue. Furthermore, to justify the system one must deal with some intangible benefits which are difficult to quantify.
- ii. **Security and privacy:** These issues are especially important in the B2C area, especially security issues which are perceived to be more serious than they really are when appropriate encryption is used. Privacy measures are constantly improved. Yet, the customers perceive these issues as very important, and, the E-commerce industry has a very long and difficult task of convincing customers that online transactions and privacy are, in fact, very secure.
- iii. Lack of trust and user resistance customers do not trust an unknown faceless seller, paperless transactions, and electronic money. So to switch from physical to virtual stores may be difficult.
- iv. Lack of touch and feel online. Some customers like to touch items such as clothes and like to know exactly what they are buying.
- v. Many legal issues are as yet unresolved, and government regulations and standards are not defined enough for many circumstances.
- vi. Electronic commerce, as a regulation, is still evolving and changing rapidly. Many people are looking for a stable area before they enter into it.
- vii. There are not enough support services. Copyright clearance centers for E-commerce transactions do not exist, and high-quality evaluators, or qualified E-commerce tax experts, are rare.
- viii. In most applications there are not yet enough sellers and buyers for profitable E-commerce operations.
- ix. Electronic commerce results in a breakdown of human relationships.
- x. Accessibility to the Internet is still expensive and / or inconvenient for many potential customers.
- xi. Credit card security is a serious issue if susceptible.
- xii. Costs involved with bandwidth and other computer and server costs.
- xiii. Extensive database and technical knowledge and experience is required.
- xiv. Customers are uneasy about online credit card orders.
- xv. Constantly changing technology may leave slow businesses behind.
- xvi. Some customers need instant satisfaction, and shipment time interrupts that satisfaction.
- xvii. Search utilities far surpass the speed used to find products through catalogs.
- xviii. Encourages competition between small and large online retailers.

9. Electronic-Business

Definition: As per **United States Census Bureau**, E-business is defined as “*any process that a business organization conducts over a computer mediated network. Business organizations include any for profit, governmental, non-profit entity. Their processes include production, customer, and internal or management-focused business processes.*” E-business is the process of conducting business electronically or over the Internet.

IBM defines E-business as “any activity that connects critical business systems directly to their critical constituencies (customers, employees, vendors and suppliers) via intranets, extranets and over the World Wide Web”.

E-business is a large-scale concept that refers to the numerous ways in which companies are taking advantage of the worldwide connectivity offered by the Internet and other computer networks. This focuses on the ideas and processes involved in starting an E-business or in adding E-business functions to an existing business. E-business facilitates a customer to conduct business anytime, anywhere and from any place over a distribution channel. It helps to get a continuous dialogue between business and the customer, just as if both were talking face-to-face. E-business is more than having a website for the business. Accessing internet to provide information about the company, products, supplies, using appropriate project management software, etc. have made the administrative, operational activities more efficient. The term E-business is broader, referring to the transformation of fundamental business processes through the use of Internet technologies. It refers to the way internal business processes and communication with suppliers etc. is carried out through computer networks. E-business is the electronic exchange of information between two or more parties. Specific activities include: customer relationship, order processing, distribution and procurement. E-business includes E-commerce, but adopts a broader perspective with prominence on key internal business processes. These processes include marketing, finance, human resource management, operations, production and risk management.

► Significance

E-business is the security of online business information, business activities. With the development of E-business, some new problems appeared. They are a challenge to the traditional commercial mode, honesty and the evaluation method. It's difficult for traditional credit factors and evaluation method to cover E-business and thus one needs an in-depth analysis and study of the characteristics, background, influence and impact of the issues. Based on the practice of international E-business development, E-business honesty includes the truthfulness confirmation of personal identity, protection for relevant (private) information, security from individual or enterprise, honesty of business behavior, and the handling of possible disputes. Honesty and ability evaluations of

individuals and enterprises not only include these factors, but also include government support and participation, legal support, service environment of relevant honesty and evaluation standard, and people's understanding of E-business honesty.

► **Electronic-business Opportunities**

- i. **Selling goods online:** Electronic commerce is one subset of E-business. It involves buying and selling hard goods, electronic goods or services over the Internet. Selling goods online is probably the simplest way one can start an E-business. Depending on the business plan, one can put up an online store for a very small investment or one can spend millions.
- ii. **Service companies:** The Internet can be used for a lot more than just selling products. Companies are now moving toward service-oriented models, using the Internet as a delivery vehicle to provide services to consumers and other businesses. The services include those that weren't possible before the Internet revolution and the technology accompanying it. There are a variety of services that can be offered using the Internet as a conduit. One can offer online data backup, be an ASP or provide a unified online message center. ISPs fall into the category of E-commerce services as well.
- iii. **Distance learning:** In the old days, when a company wanted to train its employees, it had to send them to an off-site location, pay for accommodations, and lose a day or two of productivity for each employee. Now it's possible for employees to get training on demand, right at the desktop, delivered via the Internet. Becoming a part of this training delivery vehicle can be lucrative.
- iv. **Telecommunications:** Since deregulation, telecommunications has blossomed, and the competitive marketplace has opened up. There are plenty of opportunities for the Internet entrepreneur here, from simply selling telecom equipment and services to becoming a link in an Internet telephony network. Internet telephony, a new type of technology that allows placing long distance calls over the Internet at very low cost, is an area with lots of potential for service-oriented companies. Tremendous opportunities exist in establishing the infrastructure required for Internet telephony and in reselling long distance minutes.
- v. **Information and content provider:** The World Wide Web has turned publishing, giving the opportunity to create a publication without having to invest in printing presses, ink or paper.

► **Advantages of E-business**

E-business along with helping a company in increasing its growth, productivity, making its consumers, is also helpful in the following ways:

- i. Analyzing the market potential for the company
- ii. Its prominent competitors

- iii. Plans for improving its business, products, services
- iv. It creates awareness in the society for understanding the technology and accessing it
- v. Access to global market and information
- vi. Better decision making
- vii. Cost effectiveness and increased productivity
- viii. Quicker and easier communications
- ix. Strengthened marketing capabilities and reach
- x. Access to broader information through research
- xi. Reducing the cost of doing business by lowering transaction costs and increasing efficient methods for payment, such as using online banking and reducing stationery and postage costs
- xii. The opportunity to adopt new business models and develop tailored customer support.

► Limitations

It also has a few disadvantages:

- i. Cost inflexibility
- ii. High marketing/Advertising expenses
- iii. Liquid market place
- iv. High cost of doing business
- v. Middlemen may be required

10. E-Commerce v/s E-Business

E-business and E-commerce are the ways of doing business online but the terms are not interchangeable, which refer to different degrees of a similar practice. E-commerce refers to the area of online business transactions, while E-business describes web-based practices that a business integrates into a variety of its functions.

- i. **Technology:** Both E-business and E-commerce rely on the Internet to accomplish their goals. Business owners set up E-business and E-commerce systems through desktop and mobile devices, using basic concepts of data management and security, including servers, system management and legacy systems.

- ii. **Appearance:** E-commerce focuses on appearance much more than E-business. E-commerce is primarily concerned with transactions, not only with customers but also with online suppliers and distributors. E-business applications strive to give a good idea of their company, promoting the values they use to market their business. As a result, E-commerce is much more concerned with user interface and advertising than E-business.
- iii. **Business models:** E-commerce requires a new or additional business model to govern online sales and services. This new model must include different methods of advertising, system management, security, marketing and the costs involved in maintaining an online website for business transactions. E-business, use E-commerce strategies, tends to affect the existing business model more thoroughly, reinventing older processes.
- iv. **Internal management:** While E-commerce is concerned more with the outside functions and appearance of the business, E-business is concerned with the inner workings of the company itself. E-business works to apply online solutions to payroll, human resources, internal data management and other systems that customer may not see but affects every part of the business.
- v. **Advantages:** The advantages of E-commerce are mostly market-oriented. It allows businesses to reach markets which they could not access before and show a new, up-to-date face for the company that may attract potential customers. The main advantage of E-business, on the other hand, is efficiency. While E-business strategies take longer to incorporate and are often more expensive, they create a more fluid, dynamic and efficient business model than before, increasing overall profits and growth.

10.1 Categories of E-Commerce

In terms of transaction categories, E-commerce falls into the following categories:

► Business-to-Business (B2B)

Business-to-business involves electronic transactions among and between businesses. This technology has been around for many years through EDI and Electronic Funds Transfer (EFT).

Business-to-business is the selling between companies, wholesale rather than retail. Efficient use of capital demands small inventories,

which involves expecting demand, and so maintaining detailed information flows between all parties involved in complex manufacturing processes.

Number of questions asked
1

Apr. 2013 – 15M

Define E-Commerce.
Explain different types of E-commerce.

Number of questions asked
1

Oct. 2012 – 4M

Write short note: B2B

Business-to-business involves widening the circle of suppliers for safety and competition, and of centralizing control for records and discounts. Pricing is based on quantity of order and is often negotiable. This system offers services in areas of procurement, supply-chain management, and collaborative product development. Partners achieve build-to-order capability through connectivity among the key lines of business and throughout an individual company's supply chain.

Business-to-business E-commerce is an important part of any online business. Leaving aside the simple transfer of funds, many businesses need some combination of:

- i. Creditworthiness assessment
- ii. Guarantee of quality and delivery of goods (escrow services)
- iii. Safeguards against fraud
- iv. Fast collection of funds, with ability to vary the collection period
- v. Reporting approval of sale, invoicing, delivery, payment
- vi. Procedures to handle disputes
- vii. Information of all types like corporate, technical, identity etc. are required. Building has to be interchanged across the scattered divisions of large companies, and new ideas cultivated, assessed and disseminated. Speed is vital, as are improved communication, collaboration, and customer understanding. All these requirements are handled by Internet and software has been developed to meet the challenge like customer relationship management, enterprise resource planning, online auction, supply chain management, etc.

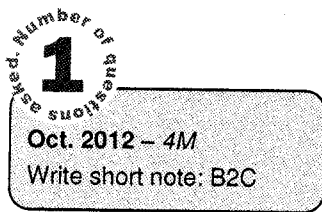
► Business-to-Consumer (B2C)

In business-to-consumer E-commerce, businesses sell directly to consumers. It is the businesses selling to the general public typically through catalogs utilizing shopping cart software. Doing business online doesn't require a huge investment by retailers, reason being developments in template-based online stores which are based on packaged applications that are delivered over the Internet.

All online stores require the functions: catalogs, order baskets, payment processing, content management and member management.

It makes sense for those components to be created once and shared by all stores, with each store effectively 'renting' its own copy of the applications.

The one area where it's important for online stores to differentiate is their look and feel, and naturally retailers feel very strongly about their business branding. So the ability to create a unique 'skin' for each site is an important part of a template-based E-store offering.



Using the latest Internet application technology, individual sites can be created within minutes of the retailer selecting a template and supplying graphics such as logos. Typically, retailers will pay only a modest monthly rental charge and retailers require no specialist hardware or software, other than internet access.

Anyone who wants to sell products and services over the Internet, or who wants customers to be able to research their purchases on the Internet, should consider an online store.

A website should be a standard part of the promotional and advertising mix for every business, along with other tools such as Yellow Pages, newspaper advertising and signage.

Advantages of Business-to-consumer E-commerce

Business-to-consumer E-commerce has the following advantages:

- i. Shopping can be faster and more convenient
- ii. Offerings and prices can change instantaneously
- iii. Call centers can be integrated with the website
- iv. Broadband telecommunications will enhance the buying experience

► Challenges faced by Business-to-consumer E-commerce

The two main challenges faced by business-to-consumer E-commerce are building traffic and sustaining customer loyalty. Due to the winner-take-all nature of the business-to-consumer structure, many smaller firms find it difficult to enter a market and remain competitive. In addition, online shoppers are very price-sensitive and are easily attracted to competitors, so acquiring and keeping new customers is difficult.

► Consumer-to-Consumer (C2C)

Consumer-to-consumer involves the electronically-facilitated transactions between consumers through some third party. A common example is the online auction, in which a consumer posts an item for sale and other consumers bid to purchase it; the third party generally charges a flat fee or commission. The sites are only intermediaries, just there to match consumers. They do not have to check quality of the products being offered.

The consumer-to-consumer category involves business transactions among individuals using the Internet and web technologies. Using consumer-to-consumer, consumers sell directly to other consumers. This is done through classified ads or by advertising, individuals sell services or products on the Web or through auction sites. Using these websites, consumers are able to sell a wide variety of products to each other. Consumer-to-consumer E-commerce configuration offers catalogs,

auctions, and escrow services. Consumers are also able to advertise their products and services in organizational intranets and sell them to other employees. The introduction of the new economy has helped to create a very individualistic and independent society. Consumers are no longer totally reliant on corporations and are increasingly looking to conduct their own business transactions. As a result, many individuals established online organizations that encouraged and assisted commerce between consumers.

There are many sites offering free classifieds, auctions, and forums where individuals can buy and sell, thanks to online payment systems where people can send and receive money online with ease.

► **Consumer-to-Business (C2B)**

Consumer-to-business E-commerce involves individuals selling to businesses. This may include a service or product that a consumer is willing to sell. In other cases an individual may seek sellers of a product and service. Individuals offer certain prices for specific products and services. A consumer posts his project with a set budget online and within hours companies review the consumer's requirements and bid on the project. The consumer reviews the bids and selects the company that will complete the project. It empowers consumers around the world by providing the meeting ground and platform for such transactions.

► **Business-to-Government (B2G)**

Governments, as national administrators, play a significant role in guiding, administrating and adjusting economy. The advent of E-commerce age put forward the new request to the original functions of governments. Governments should administrate E-market effectively and render better service to enterprises and the public by E-government on the one hand. Governments, as the 'big clients' in the economy should take the lead to adopt E-commerce and offer efficient path through electronic tender invitation for government procurement on the other hand.

Following requirements to Business-to-Government are necessary:

- i. **Commodity spot market:** Gather, classify, and summarize the information of the wholesale article and the retail article efficiently by making use of E-commerce form for macro analysis in many aspects.
 - a. Steer the structure of commodity production in case of 'market being out of order'.
 - b. Control the capacity and circulation of ineffective articles.
 - c. Crack down the production and distribution of counterfeit and shoddy products.
- ii. **Second-hand market:** As for the second-hand market, governments should learn the overall condition timely by electronic network. What kind of second hand are of high exchange rate, what kind of second hand are of the low exchange rate, what belongs to the normal

commodities trading range, what article should follow the special commodities trading policy. *For example*, when dealing with cultural relic, governments should play an active role in leading people to trade accurately, reasonably and legally because article condition of cultural relic is more complicated than stock-in-trade.

- iii. **Commodity market in the future:** It is necessary for governments to monitor commodity market in the future, because it is incomprehensive to consider commodity production only from the perspective of customers, manufactures and circulation. For instance, excessive consumption of raw materials and resources and environmental pollution has to be considered from the perspective of the national collective interests. Moreover, governments are responsible for putting forward requirements of commodity favourable for the interests of people and the nation.
- iv. **Commodity purchasing:** Government, as a big client (community), should make use of E-commerce to purchase commodity, which is of high-efficiency and low-cost on the one hand, standard, open, just and fair on the other hand. Thus, it should lead enterprises in production and circulation fields to manufacture and sell commodities efficiently and economically by adopting E-commerce.

Governments undertake large numbers of social, economic, cultural and service functions, and as 'visible hands' in particular, they play a significant role in coordinating market economy and keeping markets from being out of order. In the age of E-commerce, the governmental supervision is definitely to change when enterprises apply E-commerce to produce and operate, bank realizes the finance electronicization, and customers carry out online shopping.

E-commerce age is an information-based and digital age. Governments always play an important part in guiding, managing and adjusting economies. In the new age, it is required that governments adopt the modern means to manage the economies, and specify E-commerce market so as to sustain the healthy and continuous development of national economy. Governmental functions can be carried out online, that is the forming of E-government which will become an important component of E-commerce supporting environment.

► **Government-to-Government (G2G)**

Governmental E-commerce requirements in social production and commercial activities can be divided into the following categories: participation, statistics, service, leading of production, circulation, consumption, etc. Original national information system is mostly made up of national, provincial (municipal), local (municipal) organic statistics systems or multilevel statistics bureaus. The statistics system is mainly aims at serving state-owned economy and enterprises with urban and rural survey teams attached to statistics bureaus as organizational guarantee to set up the foundation for macro decision making by collecting, processing, disposing data of industrial and agricultural production. But along with the advance of 'two fundamental transformations' in the country, the intensification of opening up to the outside world and reforms, the transfer of the initiative of market

economy from manufacture to circulation, the original statistics system lags behind, because the methods of plan rather than actual measurement, part rather than whole, sampling rather than overall situation investigation is adopted. Therefore, data obtained are low in authenticity, high in error and hysteretic and it is difficult to obtain real time objective information and make real time adjustment, which becomes more and more prominent. Accordingly, it is necessary and extremely urgent to collect and process macro production data and help in macro pre-decision making by means of E-commerce.

E-commerce of administrations is to carry out the administration, service and internal administration etc. effectively on computer network by making use of the information and communication technology and to establish an assembly of organic service systems between administrations, society and the public.

In general, the targets of the E-government mainly are embodied in the following five aspects:

- i. Computerization, network and information of each government sector are beneficial to improve governmental efficiency, service and supervision. The E-government positively boosts the streamline of government organs and business simplification with the help of information technologies.
- ii. Administrations serve economy actively rather than passively, for which enterprises and citizens can have the knowledge of, and master governmental guideline and policies and services without the restriction of time and space.
- iii. Supply the public with excellent and diversified services by making use of network and information system built up by governments. The network covers all government sectors. The E-government supplies simple diversified services by making use of the unified information resources and modern technology, such as voice and Internet etc.
- iv. Advance the whole social informatization, the process primarily by which information technologies, such as the world-wide web and other communication technologies, have transformed economic and social relations to such an extent that cultural and economic barriers are minimized by government informatization. Display the application of the hi-tech to the community, enables the whole society to enjoy the facility of the information network, and practically boosts the social informatization.
- v. Create E-commerce supporting environments to suit the development of digital economy and to guide, layout and supervise E-commerce activities. In E-government, online virtual administration is built up to carry out online E-government by means of Internet, a fast, cheap and vivid communication method. The establishment of E-government will boost its supervision and application functions and public service by making use of advanced electronic tools.

► **Consumer-to-Administration (i.e., C2G = Consumer to Government)**

Consumer E-commerce administration means individual E-commerce activities. This kind of E-commerce activity has not really formed yet.

However, in some developed countries, such as in Australia, the government's tax body has been through the designation of private tax, or financial accounting firm to use electronic means for individual tax returns. Although such activities have not yet reached the true electronic filing, but it already has the consumer E-commerce executive body shape. The government is business to consumer, business-to-executive body of the E-commerce development on the community's personal implementing a more comprehensive electronic service. Various government departments to the community services provided by the taxpayer, such as the payment of social welfare and so on, in the future will be conducted online.

► **Business-to-Administration (B2A)**

Business-to-the executive body of the E-commerce refers to business and government agencies to conduct E-commerce activities. *For example*, the government will purchase the details of the announcement on the Internet, by way of online auction bidding, companies have to tender through electronic means.

This approach is currently in an initial pilot phase, but may be developed very quickly, because the government can establish its image in this way, through an exemplary promotional role. In addition, the government can implement E-commerce business management as regards administrative matters, such as government payments of import and export licenses, to use E-commerce to carry out statistical work, businesses can apply through the online payment of taxes and tax rebates.

► **Peer-to-Peer (P2P)**

Peer-to-peer (P2P) technology employs a network to put individuals in direct contact with each other. A simple telephone call to a friend, then, could be considered a form of peer-to-peer. In modern idiom, however, peer-to-peer refers almost exclusively to computer-based systems of sharing information directly with others via the Internet. Peer-to-peer technology has its roots in locally-based hardware arrangements in which each individual system shares certain identical features and capabilities. In the Internet age, peer-to-peer refers usually to specific applications rather than hardware arrangements.

The peer-to-peer network architecture eliminates the direct top-down relationship between clients and their servers in to link each connected individual as a peer, avoiding the centrality of traditional networks by placing the focal points at each individual computer. Users in a peer-to-peer network

can pool their resources, sharing each other's files, storage systems, and applications, thereby paving the way for extensive collaboration and efficient information sharing.

► **Business-to- Persons (B2P)**

In 'Business-to-persons' (B2P), where the word 'persons' means those who are freelancers, employees of various institutions, individuals engaged in self-employment, etc. It is the result of social networking platforms that give new power to the customer and the communities of interest that form around them. The astronomical growth and evolution of platforms such as ibibo, Facebook and MySpace reflects the B2P model. Social networks are now being leveraged by sales executives to understand the networks of prospects and leads, and customers in the realm of B2P marketing and sales. Social networks facilitate and automate vast interactions, connections and networks of people by enabling collaboration with colleagues, clients and suppliers anywhere and at anytime. This new paradigm completely eliminates the need for travel. The impact of these far-reaching social networks on business is becoming clearer every day as millions of consumers, partners, suppliers and businesses discuss and share their brand experiences.

According to *Mohan Sawhney of Northwestern's Kellogg School of Business and author of The Global Brain*, "*Social Customers are driving Innovation, they are empowered and collaborative, they are drivers and initiators of effective innovation and are increasingly viewed as a strategic asset to companies. Today's customer is looking for a personalized experience and relationship, demanding solutions rather than products.*" People are calling for greater transparency and accountability in a way that no company, government or even an individual can escape. This is facilitated by the emergence of a 24-hour global cycle of news, information and dialogue, accessible online anywhere and anytime known as B2P.

Summary

1. Electronic commerce refers to business activities conducted using electronic data transmission via the Internet and the World Wide Web.
2. **Features of E-commerce**
 - a. Ubiquity
 - b. Global Reach
 - c. Universal Standards
 - d. Richness
 - e. Interactivity
 - f. Information Density
 - g. Personalization / Customization
3. **Advantages**
 - a. Global market all day
 - b. Can access simply and browse naturally, with no technology related difficulties
 - c. Customers can compare prices easily
 - d. Save time and money finding and purchasing goods
 - e. Meet the consumer's purchasing needs within the framework of a satisfying process
 - f. Feedback can be immediate
 - g. Changing information can be available quickly
 - h. Ability to gather customer information, analyze, and react to it
 - i. New and traditional approaches to generating revenue
 - j. Manufacturers can buy and sell directly, avoiding the cost of the middleman
4. **Disadvantages**
 - a. Inability to sell some products (*For example*, high cost jewellery and perishable foods)
 - b. The newness and evolution of the current technology
 - c. Many products require a large number of people for purchase to be viable
 - d. High capital investment
5. **E-commerce Categories**
 - a. Business to Consumer (or B2C) E-commerce
 - b. Business to Business (or B2B) E-commerce
 - c. Consumer-to-Consumer (or C2C) E-commerce
 - d. Business-to-Government (or B2G) E-commerce
 - e. Consumer-to-Business (or C2B) E-commerce
 - f. Government-to-Government (or G2G) E-commerce
 - g. Business-to-Administration (or B2A) E-commerce
 - h. Consumer-to-Administration (or C2A) E-commerce
 - i. Peer-to-Peer (or P2P) E-commerce
 - j. Business-to-Persons(B2P) E-commerce
6. **E-commerce Application**
 - a. Direct marketing and selling
 - b. Online banking and billing
 - c. Secure distribution of information
 - d. Value chain trading and corporate purchasing



PU Questions

[Apr.2013 – 15M]

1. Define E-Commerce. Explain different types of E-Commerce.

[Apr.2013 – 15M]

2. Write short note: Goals of E-commerce

[Oct.2012 – 15M]

3. What is E-Commerce? Explain goals of E-Commerce along with its advantages and disadvantages.

[Oct.2012 – 4M]

4. Write short notes:

i. B2B, B2C

ii. Technical Components of E-Commerce

[Apr.2012 – 10M]

5. What do you mean by E-Commerce? Explain different technical components of E-Commerce.

[Oct.2011 – 10M]

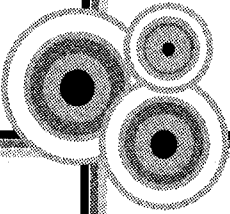
6. What is E-Commerce? Brief its applications.

[Apr.2011 – 10M]

7. What do you mean by E-Commerce? Elaborate on the functions of E-Commerce.


VISION

BUILDING OWN WEBSITE



1. Introduction

The newly introduced software has made it much easier to develop a professional website. The main work in building a website is creative and not to that extent technical, as the software would build up the site but would not provide any help for colour selection and layout.

2. What does a Website do?

A website serves several purposes:

- i. It presents your information, image and product on the Internet. In a very real sense, a website is your 'Internet Business Card'.
- ii. It helps people to find you when they search the web for related information.
- iii. It establishes credibility for your company or organization.

Internet is one of the venues other than TV and radio for information and marketing. Businesses and organizations distribute information over the Internet at a very low cost as compared to traditional channels of communication.

Website is the cost-effective way to advertise. Website is useful for:

- i. Business to provide a corporate presence on the Internet
- ii. For established service practice
- iii. For political candidates, to provide the voters with information about the candidates position, statements, etc.

Website Features

Features of Website

- i. **Store:** A storefront is the place on Internet which allows selling products on the website. If the business comprises of commercial products, books and journals, an online store lets the customers purchase material through the website.
- ii. **Content management system:** A website content manager allows changing the contents of the website without the help of webmaster. A good content manager is very easy to use.
- iii. **Blog:** A blog is a discussion forum where one can post their comments and others can post comments in response. A blog allows people to read the material anytime.
- iv. **Bulletin board:** Bulletin boards or forums were in existence long before blogs. They are generally more structured than blogs - a bulletin board can have many sub-forums, each dedicated to a specific issue or location. *For example*, a bulletin board could have a forum for each individual state.
- v. **Photo gallery:** A photo gallery allows the webmaster to post the photos on the website, along with captions and additional information which may be useful for business to grow.
- vi. **E-mail campaign manager:** An e-mail campaign manager allows composing the newsletters or product announcement and even allows sending them to the customers. The e-mail contains the brand logo.
- vii. **Audio:** If required owner can include audio or musical performances on website.
- viii. **Video:** Video presentations, product announcements, press conferences, or videos of performances can be added to the website.

3. Reasons to Build a Website

Web serves information for all types. Thus one can build a website to provide the information. One can build a site, even with no programming experience and reach more people than ever before.

► Availability

Information regarding an individual can be accessed at any time of the day from a website as some people surf the Web during regular daytime hours while some surf at night. The website provides the visitors information about the owner immediately. Websites have now become the easiest way to provide the information about the launch of a new product without notifying people personally as they can view all the information, on the site.

► Internet Showcase

Showcase of work via website proves to be a valuable tool in the marketing field. As a real estate agent can upload the pictures of the available properties, an artist can have a digital portfolio of all the art pieces. Through website address, the work or person can be immediately accessed.

► Credibility

Credibility is essential for an establishment and website is a support for the same. The certificates provided to a business are important as they serve as a point of view of customers. Thus one can publish links of reputed organization or the awards won on the website. Having a Web address and custom e-mail proves that one has spent time on developing business goals and objectives.

► Marketing

Promotion through website can be done 24×7 which includes images or text or both. Internet advertising is significantly lower in cost than traditional marketing methods, such as newspaper advertisements or direct mail. More importantly, one can now reach people in all parts of the world via Internet advertising.

► Networking

Networking is important for all kinds of objective. With a website, one can build a forum and connect with those who share similar interests and benefit from the information. One can find others in the same field and create relationships in order to share tips and ideas or solve problems. Further, one can cross-link with other related organizations so that visitors have multiple avenues of finding individuals on the Web.

Number of questions asked
2

Oct. 2012 – 15M

Brief about WWW.
Explain reasons for building own website.

Apr. 2011 – 15M

Define website. Explain the reasons for building own website.

4. Benefits of Having a Website

Number of Researches
1
suot

Apr.2013 – 15M

Explain benefits of building own website and different ways of promoting the website.

Some of the goals that can be achieved by launching a website include the following:

- i. **Far cheaper and much more flexible than print advertising:** The Internet is extremely different from print advertising as it is cheap, the advertisement is accessible for a longer period of time, the content can be changed without having to ask someone to do it and one can potentially reach a wider audience.
- ii. **Market expansion:** The Internet has allowed businesses to be accessible virtually from any part of world as it breaks through the geographical barriers.
- iii. **Diversify revenue streams:** A website is a medium for representation of the company as well as it is a form of media from which everybody can acquire information. Companies provide complimentary services along with their business. *For example*, a catering company along with their normal course of businesses provides complimentary services such as event coordinators, electronic equipment, rental companies, etc.
- iv. **24 × 7 × 365:** Website services are provided 24 × 7 × 365 in spite of public holidays or particular trading hours or Time to close shop. Websites provide information anytime and anywhere (virtually).
- v. **Offer convenience:** In the midst of a busy schedule it has become difficult to research on a product, and look for or ask someone for information on a product. It is better to surf the website on the Internet. The customer can visit the website with ease of comfort and privacy without waiting in a long queue.
- vi. **Add value and satisfaction:** As each customer is attended to individually, it ultimately adds value to the product offer and customer. Thus customer experiences a higher level of satisfaction. The extra service provided on the Internet also adds value and helps the customer to remember the website.
- vii. **Standardize sales performance:** Going by the past results which has worked and the approach which have been favourable for the business and those which have not, one can produce the vital field and use it with the website, so that one can use it on every customer. Thus there is need to train the sales personnel.
- viii. **Improve credibility:** A website gives an opportunity to tell the customers what is the business about and why the website deserve their trust and confidence. In fact, many people use the Internet for pre-purchase research so that they can determine for themselves whether a particular supplier or brand is worthy of their support. The Internet also allows for Viral Marketing (It refers to marketing techniques that use pre-existing social networks to create an

increase in brand awareness or to achieve other marketing objectives through self-replicating viral processes, analogous to the spread of virus or computer viruses.) where the website visitors spread positive word-of-mouth information about the business - the customers do the marketing.

- ix. **Promote the Brick N Mortar presence:** In a city or place where one has come for the first time, one finds it difficult to reach a particular place or the market. One can publish what they call a dummy map on the website, which shows directions and landmarks graphically and thus the customer can reach the place without any problem. One might advertise a promotion on the website encouraging the visitor to visit the Brick N. Mortar premises like 'At a branch near you!' Because a website is flexible, one can change the content as one likes. Individual can change contact details instantly and lower the risk of losing customers when moving to a new location.
- x. **Growth opportunity:** A website serves as a great place to contact potential investors, to show them what the company is about, what it has achieved and what it can achieve in future.
- xi. **Two-way communicative marketing:** Customers can quickly and easily give feedback on the product and/or marketing approach.
- xii. **Cheap market research:** One can use features on the website such as visitor polls, online surveys and the website statistics to find out what the customers like more and how they feel about certain aspects of business to determine how one can improve the product and the way one can do business.
- xiii. **Increases awareness of products/services:** A website provides the opportunity to publish who, what, where, when and why of the business in a powerful and effective manner. How many potential customers might be persuaded if they could learn a little more about individual and the company, and products, etc., without having to call up or taking the time out to meet with one in person? A website makes it easy for customers to learn more about the business at their own pace.
- xiv. **Build branding:** Build brand awareness by having a website on all other marketing material one uses. If the brochures, website, business cards, advertisements, posters, etc. have the same look and feel, it increases brand awareness.
- xv. **Enhance the image:** A website can help to establish a credible, professional image, instilling a level of trust with the customer and their purchasing confidence will follow suit. The website can reflect the spirit and vision of oneself and the company. The Internet also offers the opportunity for a small business to portray itself as a big business. How will the business be perceived on the web?
- xvi. **Create a competitive edge:** If the customers can't find one online, they will find the competitors. With more and more companies making a web presence, the companies that lose business to their competitors will most likely be those who fail to represent themselves on the Internet. If a potential customer can leisurely browse the company information online but cannot find the competitors' information, one's company has definitely an additional edge.

- xvii. **Open new channels of communication with staff, partners and suppliers:** Intranet websites are an easy way to provide the employees with a way to get information they need to perform their duties in one centralized location. One can post benefits information, changes in staff, esteem for hard work, a place for their schedules, and much more. One can put as much or as little information as one wants on the site and make them give a password to access the information that needs to be kept private.

5. Bandwidth Requirements

► Concept of Bandwidth

Definition: *Bandwidth refers to the amount of the data transferred to the visitor's computer from the web space. In other words, bandwidth refers to the amount of data transferred through the network wire in a specific period of time.* The bandwidth for a hosting service is calculated on monthly basis. The web hosting service providers pay huge amount for the broadband connection. Bandwidth is a measure of available or consumed data communication resources expressed in bit/s or multiples of it (kbit/s, Mbit/s etc). The word bandwidth may also refer to consumed bandwidth, corresponding to achieved throughput or good put, i.e., the average data rate of successful data transfer through a communication path. This sense applies to expressions such as bandwidth shaping, bandwidth management, bandwidth throttling, bandwidth cap, bandwidth allocation (*for example*, bandwidth allocation protocol and dynamic bandwidth allocation), etc. An explanation to this usage is that digital bandwidth of a bit stream is proportional to the average consumed signal bandwidth in Hertz (the average spectral bandwidth of the analog signal representing the bit stream) during a studied time interval.

Digital bandwidth may also refer to Average Bit Rate (ABR) after multimedia data compression (source coding), defined as the total amount of data divided by the playback time.

► Bandwidth in Web Hosting

In website hosting, the term 'bandwidth' is used to describe the amount of data transferred to or from the website or server within a prescribed period of time, *for example*, bandwidth consumption accumulated over a month measured in Gigabyte per month. The more accurate phrase used for this meaning of a maximum amount of data transfer each month or given period is monthly data transfer.

Analogy or the similarities between the two individuals are:

- i. Rented Water Tank = web-server that hosts website
- ii. Water company = hosting company where web-server resides
- iii. Water = files, data, images, etc, that comprise website
- iv. Pipe = the Internet
- v. Quantity of water delivered = bandwidth consumption

There's a pipe that delivers water from rented water tank to the home. As one requests for water, the water company delivers it to the individual. All the while, they are keeping track of how much water was delivered to the customer, during a billing cycle. One has a contract with the water company in which they agree to charge a fixed amount per billing cycle, provided one does not request more water than the allowable quantity, as defined in the contract. If one does request more water, they will not deny but will incur additional charges for the extra water requested / delivered.

Web pages typically equate to a small quantity of water and images, videos, PDFs, and other similar media can potentially equate to large quantities of water being delivered by the water company. The accumulated total can grow rather quickly, especially when a website is popular.

Internet connection bandwidths

The following list shows the maximum bandwidth of the Internet access:

- i. 56 kbit/s: Modem / Dialup
- ii. 1.5 Mbit/s: ADSL Lite
- iii. 1.544 Mbit/s: T1
- iv. 10 Mbit/s: Ethernet
- v. 11 Mbit/s: Wireless 802.11b
- vi. 44.736 Mbit/s: T3
- vii. 54 Mbit/s: Wireless-G 802.11g
- viii. 100 Mbit/s: Fast Ethernet
- ix. 155 Mbit/s: OC3
- x. 300 Mbit/s: Wireless-N 802.11n
- xi. 622 Mbit/s: OC12
- xii. 1000 Mbit/s: Gigabit Ethernet
- xiii. 2.5 Gbit/s: OC48
- xiv. 9.6 Gbit/s: OC192
- xv. 10 Gbit/s: 10 Gigabit Ethernet
- xvi. 100 Gbit/s: 100 Gigabit Ethernet

5.1 Ideal Bandwidth Requirement for Website

Before one plans to buy a web hosting service, research must be done regarding the bandwidth. Having a high bandwidth is not always the correct decision. High bandwidth comes with high fees, this must be kept in mind while buying the web hosting service. Moreover, the actual usage is not that much.

Number of questions asked
1

Oct. 2011 – 15M

What are the reasons for building own website?
What are the bandwidth requirements for the same?

► Calculation of Bandwidth

Calculating the actual bandwidth required for the web hosting service is very simple. The formula is total size of the web pages in the site \times monthly traffic volume = required bandwidth.

For example, one has 5 web pages in the website and the average size of the web pages is 70 KB. That means, the total size of the web pages in the site is $70 \times 5 = 350$ KB. Now, if the expected traffic volume is 3000 per month, required bandwidth should be $350 \times 3000 = 2.1$ GB per month. This is the simplest formula for calculating web hosting bandwidth. It is not necessary that all the viewers will see the 5 pages. And if the site provides the download it should be also kept in mind while calculating the bandwidth. Like if music files or video files are to be downloaded, then sufficient amount of bandwidth support should be there. If PDF files are to be downloaded, it requires more than 1GB bandwidth. The.php pages require more bandwidth than html pages.

One should properly manage the bandwidth size. For that website components should be in order, web pages size should be kept minimum. This provides cost effective website and even the website loading is also fast, which proves to be a plus point with respect to customer. One must use small size pictures rather than heavy images and even multiple file download should be avoided.

6. Cost of Building a Website

To determine the exact cost of a website is a tough job. Website can be built by:

- Hiring a couple of college kids to put together a low-budget site, or
- Hiring a professional firm

Web developers provide a code HTML and they also help to decide what information to place on site, create graphics, logos and other marketing collateral, connect the site to databases and E-commerce systems, add multimedia and other types of content.

It is not necessary to build a world-class site that will get millions of hits a day, for that one has to spend a lot. It can be made with just few mount (i.e., a physical location in the partition used as a root file system).

6.1 Factors Affecting Website Cost

The cost of designing a website is a function of a number of factors, including:

- i. The amount (and quality) of artwork and graphic design to create the site

- ii. The number of website pages
- iii. The volume and complexity of content or 'copy'
- iv. Features that are to be incorporated into the website, such as a store and content management.
- v. The number of images and photos
- vi. Stock-art and photo purchase and royalty costs
- vii. The quantity (and quality) of charts, graphs, icons and special images that need to be created
- viii. Audio and video editing and preparation
- ix. Incorporation of Flash (scalable animation)
- x. The experience and competency of the website designer

To understand the work involved in the web development and to find the exact cost, it is acceptable to ask the designer to help quantify the factors affecting the website cost.

A website is developed on the basis of either a fixed bid or as a time and materials bid where work is billed at an hourly rate and extra costs. A fixed bid is usually used, when the precise size and scope of the project is known in advance. A time and materials bid is more appropriate when the website is in the ongoing work stage.

A website can be constructed either from pre-constructed 'canned' templates, or it can be custom-designed as per the requirements. Templates initially are the cheapest way to go for entry-level websites, but templates are often problematic as for browser incompatibility, poor internal html code, and lack of extensibility. It is recommended to create a solid, basic, website, or a unique, custom website designed to the specifications. As with any marketing material, the preliminary cost of quality design may be higher, but the ultimate return on investment may be significantly greater.

It is important to determine the relative size and quality of intended website, as this will greatly facilitate obtaining an accurate and appropriate proposal of cost. More experienced, competent and 'higher-end' web designers are costlier but the quality of the resulting website will increase.

6.2 Ancillary Website Implementation Costs

In addition to website design costs, extra costs will be incurred known as ancillary cost. They are as follows:

- i. **Domain registration cost:** Domain registration costs approximately ₹ 425 per year.
- ii. **Hosting cost:** It approximately costs from ₹ 999 to ₹ 1999 per month to host a website. The cost depends on the complexity of the website, the quality and reliability of the services, the amount of support required, and the amount of support provided by the hosting company.

- iii. **Merchant account:** A merchant account is a credit relationship with a bank that allows to process credit cards. Costs vary widely, it depends on one time transaction or per month transaction or the credit card transaction amount. It may vary from ₹ 40,000 to ₹ 3000 and even the charges vary for the transaction in national or international markets.
- iv. **Credit card processing:** E-commerce allows selling products online and accepting payment via credit cards. Various services charge varying rates to process credit card transactions. In addition, if one has a comprehensive store with a merchant account, back-end scripting or programming will almost certainly be required on the website.
- v. **E-mail campaign management:** An E-mail campaign management system allows to easily sending e-mail 'blasts' to clients, customers and supporters.
- vi. **Website development cost:** Websites are hardly ever motionless creations. Indeed, the advantage of a website is that one can change and improve it over a period of time. Maintenance cost is typically bid by a webmaster at an hourly rate, or monthly or yearly basis.

The cost of building a website can be cheap or expensive as one wants it to be. There are many ways to create a website through which one can determine how much to spend.

There are many ways to create website through which one can determine how much to spend

- i. Self-building a website
 - ii. Professional firms building the website
 - iii. Hosting
 - iv. Domain space
 - v. Advice on cutting costs
- i. **Self-building a website:** The cost of creating a website includes money spent on programming software. Any version of Dreamweaver, Flash or Microsoft Publisher can cost anywhere from ₹ 6,000 to ₹ 30,000.
 - ii. **Professional firms building the website:** Costs to have a professional firm build the site can run anywhere from ₹ 3999 to ₹ 30,000, depending on the firm or individual.
 - iii. **Hosting:** Hosting is putting the raw data (everything that was programmed and built) onto a secure server. Depending on the complexity of the site and its features, one can spend anywhere from ₹ 499 to ₹ 58999 to host alone.
- iv. **Domain space:** Domain space needs to be renewed annually, or every two years. Expect to pay anywhere from ₹ 4,999 to ₹ 11,000.
 - v. **Advice on cutting costs:** If one has the matter, images or photos one wants to use for the website, they should be submitted to the firm which builds the website. This helps in to reducing the cost.

7. Time Consumed

The time consumption depends upon the type of website and the reason for which it is built. This can only be calculated via assumptions like:

- i. 10 pages of content
- ii. A simple graphic banner
- iii. A standard 2 section layout (body and right navigation panel)

The above is a standard website.

Another important factor is the knowledge of website technologies. Since one is interested in knowing how long it takes to create a website it is safe to assume that one has very little experience or one has never created a website before. This estimate assumes that one's experience is as follows:

- i. Very basic understanding of HTML
- ii. No understanding of CSS
- iii. Little or no experience creating graphics (Photoshop)
- iv. Little or no experience using website creation software (Dreamweaver)

There are 3 major parts to creating a website:

- i. **Content:** The words that will fill the webpage.
- ii. **Website itself:** The layout and navigation between pages.
- iii. **Graphics:** Logos and eye pleasing graphical icons.

Initial work of website development is to prepare the content of website. For that one should write the content on a word document. This could take approximately 10 hours or 1 hour per page, which depends upon the writing skill and speed of the creator, otherwise time can exceed from 1 hour per page to 10 hours per page.

Next job is to create the website layout. For that one has to learn how to use website creation software and how Cascading Style Sheet (CSS) works. Creating the website layout is a simple task. Just one has to create a template page, choose some colours and fonts. It is simple, but time consuming as it needs adjustments and is a twisted job. The general layout takes around 8 hours. While preparing the layout everything should be aligned and the colour contrast should be pleasant along with the centered logo. This takes around 24 hours to 28 hours.

Time required to create a website:

- i. Creating content: 20 hours.
- ii. Learning to use Website Creation Software and CSS: 12 hours.
- iii. Creating website layout and basic graphical logo: 28 hours.

Total hours: 60 hours

8. Reach or Accessibility of Website

Accessibility means making site available to as broad a range of visitors as possible. For a website to be accessible means that it is coded well, it is easy to navigate, and works in everyone's browser.

Tools to make website accessible:

- i. **Learn to use the 'alt' attribute for each visual feature on page:** This tag is used to show alternative text in case the images have been disabled to save on bandwidth or the connection is too slow to load images. Good tags should define the image they stand for in the shortest way possible without losing any meaning. They are read by screen reading software, thus it should be concise and to the point. All visual features have descriptive text on mouse hover. That is, if one places the cursor over any visual feature, a small coloured pop-up window appears containing precise descriptive text of the visual feature.
- ii. **Use link text that describes the destination:** Normally, even visitors of normal ability do not read the entire content of a page that allegedly contains the solution to the problem they are searching for. Instead they skim through looking for the link to the answer. Links such as click here and follow this link should be avoided as they are not descriptive of the destination they are linking to. Not unless one reads their context, they are not likely to communicate the fact that they are the answer to the visitor's search. Instead, use short descriptive text such as visit home page or learn more about the gadget. This allows the visitor to go directly to what they want instead of wasting time reading lines and lines of lip-service to something they already know. Take a peek at open office website to see what proper links should look like. They not only lead to where one probably wants to go but also unobtrusively suggest better destination with more useful information based on the searched keywords.
- iii. **On diction and readability:** The words used must be simple enough to efficiently pass the information but not too simple to appear childish. Avoid irrelevant information, stick to the content. Unless it's a personal website, avoid talking about oneself. Visitors want answers to their problems and even though one is the inventor of the award-winning solution, talk less about oneself and more about the product or service. Use correct grammar and spell check before posting it on the site. If there are abbreviations or technical jargon, remember to include a glossary to help readers understand the content. If there content covers several pages, provide a succinct summary covering the main points and a table of content to save the readers from going through irrelevant text. The table of content should preferably consist of placeholders or links to the position of that topic in the page. The text should be in a legible font. San-serif fonts are considered the best for body text as they are rendered well by all browsers. Using the right font that is in tune with the theme of the content is not only enticing but also ensures easy comprehension and even enjoyment when reading. Use different fonts or colour for links so that they stand out in the descriptive text. This is convenient for skimmers of content to get what they want. Keep paragraphs brief to keep the reader engrossed and interested in what you have to say. To this end keep the word count per sentence at 75 words. The white space

between lines should preferably be less than half the font height used. Never fully justify text to avoid 'rivers of white': large irregular white spaces forming patterns throughout the page.

- iv. **Provide text version of all audio and video content:** It is not uncommon to find a website that uses audio to convey the entire content it has to offer. This is disadvantageous for those short on hearing or with slow Internet connections. Provide a mechanism to have the content in visual or text format by either transcribing audio content and posting it on the same page or captioning video files. One could also describe briefly the theme of the video to save the viewer from watching irrelevant content. Use a buffering system that downloads the video in the background and plays the downloaded content simultaneously. One could also provide different formats for video or audio that compromise on either quality or size. Youtube.com *for example*, provides both .flv and .mp4 file formats for viewership. Flash files are smaller but low on quality while MP4 files are high in quality but large in size. This caters adequately for different bandwidths.
- v. **Use a site map, search mechanism and place holders:** On an average, websites have several hundreds if not thousands of pages. Each has some form of information that is of interest to different viewers. To save the viewers from wading blindly through the pages looking for keywords, include both a site map outlining the main topics covered in each page and each title should be a link referencing that part of the website. Alternatively or additionally integrate a search mechanism for the users to search for keywords that will conveniently lead them to the pages they are interested in. One could also use open source tools such as Google Search that offer customized search engine capabilities for the users. On proper navigation usability take a look at the site that allows moving from one page to the next in one fluid and logical process. All the information is available at the click of a link within the pages of the site.
- vi. **Organize the page and remain consistent:** Most websites have different features for the viewer to choose from. This may fall under categories like related ads, past articles, content updates, registration and support. This should be organized under headings or separated into tables that have different colours and backgrounds for readability. Ads and site map goes to the periphery of the page leaving the center of focus for product information or the main content. The top is reserved for a banner proclaiming the website and maybe some ads. Whatever the structure one opts for, one should stick to it throughout the website. Viewers take time to learn the structure and if it keeps changing, they soon lose interest. Preferably, keep some aspects of the page constant. With a brief glance, a visitor can take in everything without any browsing required. For further navigation, a clean and clear menu is available on the left of the page which is separated cleverly from the rest of the content.
- vii. **Ensure the webpage is versatile:** A versatile page is one that can be read by most, if not all browsers and can be easily formatted to be viewed on handheld devices such as mobile phones. Include support for change of sizes for the visually handicapped. Text and images should remain recognizable whether minimized or increased in size or quality. Allow the disabling of images and ensure that content is comprehensible with and without the images.

- viii. **Refrain from distractive features:** Most developers assume animations, pop-ups, flashing text or other visually grabbing features are good for passing the information across. Most people are easily disoriented by these distractions and chances of going back to what they were reading are next to none. Highlight whatever one wants the visitor to consider viewing, for instance, using a different font, colour or put it in bold, underline or italicize. Whatever effect used should not be exaggerated or over used to avoid losing the effect. Websites such as 'recyclenow' have put the finger on the right balance between too much clashing colours for emphasis without it proving to be a distraction to the visitor.
- ix. **Provide some control mechanism over the website for the user:** When a user feels in charge of the pages, they are likely to stay longer and get interested in what one has to offer. For instance, use indicators for the viewer to see where they are in the web site and a means to easily go to another area or go back. Integrate the ability to cancel, reverse, confirm or altogether stop an important action. Generate error messages where appropriate instead of taking the user back to the home page by default without alerting them as to the nature of the error encountered, however genuine it is. Else the visitor becomes frustrated and may not wish to come back even though the product is what they want.
- x. **Test the website for usable accessibility:** It requires one to set the following settings in browser and reload the page:
- i. Disable images
 - ii. Disable JavaScript support
 - iii. Disable style sheets
 - iv. Increase text size
 - v. Set custom browser font and style or any other than the default settings

Now reloading of page can be done and it is watched whether the page is still legible without much effort. One has to see:

Is the content understandable?

Are the alternative image tags visible and do they make sense in context to the rest of the content in the page? Try navigating throughout the page without the mouse.

Are all links visited using the tab key? Try accessing the page on a data enabled phone.

Are the main contents and all links visible? Once the website has been subjected to these tests and passed with commendations, then one is ready to launch the website onto the rest of the world.

9. Register a Domain Name

Registering the website is the first job before building the website. A domain name like t: 'yourdomain.com'.

The domain name represents the URL, i.e., Uniform Resource Locator (or permanent web address) of the website. Therefore, when anyone types in 'yourdomain.com' or 'www.yourdomain.com', they will see the individual's website.

Registration of the domain name is done through a domain name registrar or hosting provider. The preferred domain name availability is checked, if available then it can be registered online. Registration of domain name is done annually. It can be registered in advance even as it can be set for 'auto - renew'.

Number of questions asked
1

Apr. 2011 - 15M

Elaborate on domain name. Describe procedure for registering a domain name.

9.1 How to Register a Domain Name?

A domain name is essentially the website's name without the term *www*. Registration for domain name is done for a period from one to ten years, with options for renewal. It costs approximately ₹ 425 (lowest) per year to register a domain. While the process of registration is on, the webmaster keeps an eye and if needed will help out for pitfalls along the way.

The domain name(s) should be such that it reflects the company's name or organizational purpose. *For example*, if business is of advertising via bidding, a domain name of advertiser.com would be good, but a name of bidadvertiser.com is better. There may be a situation like the common domains have already been registered. So the next step should be to search for the available domain name which should be similar to what one thought before. But keep in mind that name should be easier and shorter. Use of dashes should be avoided as it is hard to learn or remember and difficult to explain to people. One to three words placed together are usually better than using dashes.

There are a number of top rank domains, including com, org, us, net, info, biz, and various country names like in, uk etc. If one has a commercial business, one will go for registering the com variation of domain name and probably the newer biz variant. A non-profit organization, or even an individual, will prefer registering the org version and quite possibly the com and us variant (for US-based organizations).

Number of questions asked
1

Apr. 2012 - 15M

Explain in detail how a Domain name is registered. Brief about Cost, Time and Reach factors for building own

Several variants of top-level domains (like com and org) are registered because:

- i. It is difficult to remember whether the domain name is org or com. If registered for both, it would be beneficial, since both will take people to the website.
- ii. The competitor (whether in a competing business, organization, or political opposition) could register the popular com, org, net, us or info variants, if available, and set up a disinformation website of the main website.
- iii. Domain resellers or 'scalpers' register the available variants and then offer to sell them to the original for hundreds or thousands of rupees.

9.2 Which Domain Name Registrars to Use?

One should register the domain and host the website in the country, one is doing business in. This ensures that one will stay to applicable rules in that country and one can use the correct top level domain registrar for that country. There are a large number of domain registrars, and one need to be very selective when choosing a domain registrar. Here are a few drawbacks:

- i. It is difficult to register the domain name in one's name, under one's ownership. One should not register the domain name under the name of the owner. It will create difficulty in transferring the domain name to another registrar in future.
- ii. The domain name should be registered with correct information. Every domain name has four types of contact information: administrative (the domain owner), registrant, technical, and billing. As per current rules, to retain the domain name one should provide the correct information. As the information becomes public, it is important to first take the permission from the parties before entering the information and making it publically available.
- iii. It is difficult to lock the domain name while registering it.
- iv. If one registers a domain name as part of a bundled package from an ISP, it will be relatively costlier.
- v. There are small company registrar who subcontracts their registration and support to large registrars, such as Go Daddy - who offer these support services to many such resellers. It is more difficult to deal with the small company directly, when of problems arise.
- vi. Quite a few domain registrars charge very high prices. The market rate for domain registration is approximately ₹ 425 per year, which varies depending on the top level domain.
- vii. Some domain registrars won't make it easy to transfer the domain to a different registrar with more competitive prices or better service.
- viii. Another problem is when loses the user code and password for access to an existing domain name at a domain name registry. The procedure to prove that one is the true owner is complex, and takes weeks to resolve. It usually involves a minimum faxing in a copy of the drivers' license on the letterhead.

10. Web Promotion

One of the biggest problems that small businesses today are facing is how to get more traffic, customers and sales to their sites. There are many effective strategies that help to increase the ranks on search engines, thereby increasing website's potential visitors and customers.

This is done by using linking strategies, submitting site to directories and industries that are specific to the business and writing keyword rich content in a subtle manner that links to site and which other online businesses can use in their newsletters. Blogging on business sites and press releases also helps in advertising, and works surprisingly when it comes to the visibility of the website.

Advertisement of website can be done by embossing the website's URL on stationery, cards, and other copy. Developing a free service, such as a periodic marketing report or contest will help the website in its advertising efforts. Some other traditional methods of advertising such as newspapers, flyers and billboards also work. Though expensive, they effectively target a specific audience in the local area.

Starting a newsletter proves to be a good tool to advertise the website. One can offer a free report or product on the site in exchange for e-mail addresses. One can then use these e-mail addresses to send the newsletter embedded. Such e-mail strategies are effective and generate a fair amount of Internet traffic on the website.

Sharing traffic with other similar sites is another way to promote the website. For instance, find another site with similar products and services, request to share the e-mail list with them and offer a percentage of the profits - this method is very effective, is free and works to the benefit of both parties.

Some other strategies that can be used to promote your website are:

- i. Site promotion on forums and blogs
- ii. Having online contests
- iii. Requesting visitors to bookmark the website
- iv. Advertisement exchanging with related businesses
- v. Planning marketing techniques
- vi. Paid advertising (very effective)
- vii. Purchasing advertisement space in Newsletters
- viii. Starting an affiliate program
- ix. Product listings on auction and shopping sites

Number of pages
1
pages

Oct. 2011 –5M

Write short note on: Web promotion

10.1 Need for Website Promotion

The rapidly-growing overabundance of websites means that there is tough competition for search engine visibility across a common set of keywords and keyword phrases. *For example*, a recent Google search for 'wedding dance bands in India' returned approximately 2,83,000 results, and a search for 'plumber' returned approximately 71,70,000 results. Thus, to have the result of one's website in the top ten, one should have a unique business or organization. Otherwise people would not be able to find the website.

► How to Promote Your Website?

There are a number of ways that can attract people to the website:

1. Put the website URL (*for example*, www.ElbelConsultingServices.com) on the business cards, letterhead, envelopes and invoices. Leave off the "http://" part. It's okay to capitalize letters.
2. Place the website on all marketing and advertising material.
3. E-mail an announcement to customers, supporters, and friends (but avoid sending bulk spam). ECS offers quality e-mail campaign management.
4. Send out a press release, possibly using a service like PR Web Direct. For search engine visibility of the site, avoid using many keywords related to the site in order to keep the archived press release from competing with the site. (ECS is experienced at writing newsworthy and relevant press releases).
5. Announce the website on the voice mail.
6. Place it in the e-mail signature.
7. Include it on the checks.
8. List it in trade association and organization directories.
9. Add the site to the Yellow Pages listing to increase credibility and direct people to the website.
10. List with local Chamber of Commerce.
11. List with the Better Business Bureau.
12. Fax your clients about the new site.
13. Tell friends, family, and others at work about the website.
14. Distribute flyers and business cards.
15. Take out bus stop advertising.
16. Send out a postal mailing to customers and supporters telling them about the website.
17. Promote website in trade journals and newsletters.

18. Take out an advertisement in the local paper to promote your company or organization and your website.
19. Encourage others to link to your website. This can include customers, suppliers, advertisers, supporters, friends, etc.
20. Mutually exchange links with organizations and similar businesses, who do not compete with you.
21. Make sure webmaster makes website search engine friendly. See 'How do I get high search engine visibility?'
22. Make sure webmaster submits website to the main search engines and directories (but don't fall for services that claim to submit the site to thousands of search engines).
23. Consider paid placement with website directories, such as DMOZ and Yahoo.
24. Consider pay per click (PPC) search engine advertising, such as with Google AdWords.
25. Write product reviews at Amazon and on shopping sites. Be sure to include a link to your website.
26. Write articles and make eZine posts with useful content that links to your website. Include keywords related to your website. This will help generate interested and qualified traffic to the website, eZines include: GoArticles, eZineArticles, iSnare and others.
27. Write forum and blog posts with useful content that links back to website.
28. Create a blog, keep it current with quality content, and promote it on blog directories.
29. Write a subject matter expert page at squidoo.
30. Promote your site on various social media.
31. Engage in 'social marketing'.
32. Evaluate list builders such as Get Subscribers (but don't send spam e-mail).
33. Place it on company-owned cars and trucks.

11. Banner Exchange

These are the advertisement boxes that appear on websites nearly everywhere you go. They ask you to buy things or encourage one to click, so that one will go and visit another person's site. It's all about getting the eyeballs to the site.

Number of questions asked
1

Apr. 13 – 5M

Write short notes on:
Banner Exchange

11.1 What is a Banner Ad?

A 'banner ad' gets its name from one of the first graphical advertisements found on the Internet. It is called a banner because the dimensions of the advertisement were made a standard 468×60 , which is an elongated rectangular advertisement that looks just like a banner.

Now, advertisements have expanded to include stretched out vertical advertisements, known as 'tower ads' and simple large square button advertisements, while some sites create rectangular small button advertisements to promote their site. These are rarely exchanged in an advertisement exchange program.

Google and others have pioneered text-based advertisements that show no graphics at all. This AdWords program has become very popular, especially because it is the only way one can advertise the site on Google.

11.2 What is a Banner Exchange?

A banner exchange is a site where many website owners contribute advertising to share among them. The owners offer to display other site owner's advertisements on their site in exchange for displaying their own advertisement on another site.

As website owner's honesty is not certain, so the banner exchange program has enforced the rule that advertisement **MUST** be displayed on another person's site when one display on one's site. Without a banner exchange program, there would be no way to enforce this rule and to keep the statistics of display of advertisement or the conversion time. Worse still, one wouldn't be able to have any accurate statistics such as how often the advertisement was displayed or about the 'conversion rate', that means how many times people clicked on the advertisement.

11.3 Nomenclature

► Impressions

This is the number of times one's banner ads are displayed on someone else's site. The statistics is summed to include all of the sites ad which was shown during a given time period. One impression is counted whenever a page is loaded that displays advertisement.

► Exchange Ratio

This ratio explains how many advertisements one must display on their own website, before the advertisement will be shown on someone else's site. The industry standard is to show advertisements at a ratio of 2:1. Orvado is seeking to revolutionize the industry by offering a 1:1 exchange ratio.

► Clickthroughs

This indicates the number of people interested in advertisement and clicked on advertisement to visit the site. This is a measure of the success of banner ad. When measured against the total number of impressions, it gives an idea of how successful the advertisement was in attracting visitors.

► Clickthrough Rate

This is a percentage value that is computed by dividing the total number of clickthroughs by the total number of impressions. So if one had 3 clickthroughs on 100 impressions, the clickthrough rate would be 3%. This is a standardized measure of the success of banner ad.

11.4 Managing Advertisement Campaigns

The banner exchange networks provide with a web-based control panel that allows one to manage all the banner ads and view statistics about the banners. The website tracks the statistics through the 'web server log'. Using a log analyzer, one can generate reports about the visitors to the site.

The control panel is a menu-driven area and is password protected which only valid banner exchange members can access. One can add new banners to the account or one could add banners to a new campaign. Usually, the banner exchange network will need to review the banners as they must be a decent banner.

Banners are uploaded to the banner exchange network so that they can be served to other users. This is done to manage statistics and ensure that each banner is shown in accordance with the banner ratio. It has to be ensured that the banner is not exchanged with an unchecked banner.

One has to submit own website which hosts the banner. The process includes a HTML code on website which has to be displayed on banner before it has to be activated on banner exchange. Then the exchange network reviews the web pages and site and ensures that it is acceptable.

Lastly, the control panel will show statistics on how many banner ads were shown on Website and also the statistics for 'impressions', 'clickthroughs', and 'clickthrough rate' (CTR.)

12. Shopping Bots

Number of searches
1
swatches

Oct. 2012 – 5M

Write short notes on:
Shopping Bots

Shopping bots are price comparison sites on the World Wide Web that automatically search the inventory of several different online merchants, to find the lowest prices for consumers. These sites rank products by price and allow the shoppers to link directly to an online merchant's site for actual purchase. Many shopping bots also include links to product reviews from evaluation sites.

One of the most popular shopping bots *pricegrabber.com* gathers the offerings of more than 2,000 retailers. Users can either search for a specific product by keyword or browse several product categories including apparel, books, consumer electronics, movies, and wireless products. Searches result in a listing of products that can be sorted by various criteria including price, merchant ratings, and manufacturers. To change the way information is sorted, shoppers can simply click on a different category heading. Shoppers who reach a decision about which item they wish to purchase begin the transaction by clicking the 'buy' button located beside each product. They then are routed to the Website selling the item, where they can complete their purchase. *Pricegrabber.com* offers its shopping bot service free to users. The site makes money via banner bar advertising. The icons for members who are permanent appear in BOLD or the permanent members appear larger in the search results offerings in comparison to the icons for merchants who are not members.

Another leading shopping bot is *PriceSCAN*, which offers a wider selection of products than *pricegrabber.com* because it includes offers from merchants without Websites. The site's databases are changed frequently as new information pulled from catalogs, print advertisements, and faxes from the merchants themselves is added daily. The bots rely solely on banner bar advertising as a source of revenue.

Other than *mySimon.com*, *pricegrabber.com* and *PriceSCAN*, some shopping bots require payment from each merchant they list. As per the November 2000 issue of *Searcher*, "the reality is that most shopping bots make money by collecting listing fees from the merchants who sell through them. Merchants who pay more get higher rankings from the bots, and sometimes they can shut out competitors altogether". For example, the entire category of 'Books' on the Lycos shopping site searches only the Barnes and Noble site with absolutely no way to compare prices. For the most recognized electronic merchants, the Yahoo! shopping bot is the best option as it limits its searches to leading online merchants.

Some of the shopping bots merchandise in some special products or merchandise in particular product. For example, *IQShopping* searches the inventories of online home electronics and video game vendors, as well as traditional brick and mortar retailers selling the same wares. *BookFinder.com* searches Amazon, *Antiqbook*, Barnes and Noble, *Bibliofind*, and other online book retailers, and gives a combined database of roughly 15 million books—to find the cheapest book prices for shoppers. CNET's shopping bot focuses on computers and other types of consumer electronics, including wireless devices.

13. Target E-mails

Targeted e-mail advertising is a very professional and cost effective way to do e-mail marketing. To reach the right group of people which require that particular product, target e-mail marketing is the best option. Targeted e-mail advertising is a cost effective method of advertising. It is quite modern as well as up-to-date. Hundreds of thousands of people have used targeted email advertising to market and grow their businesses. A lot of these people have been able to make millions of money from targeted e-mail advertising. Targeted e-mail marketing allows creating a targeted creative advertisement message or newsletter that lets the recipient know that the advertisement is targeted specifically to them. This increases the response rate or sign-up rate. And this high response really leaves a lot of opportunity open for doing big business.

13.1 Benefits of Using Targeted E-mail Advertising

Targeted e-mail advertising allows to market product or service to the specific customer rather than send e-mails to people all over and reach a much lower response rate. The targeted e-mail allows arranging service or product more efficiently; since one already knows that he / she will be placing it for the right people.

Targeted e-mail advertising favours a cost effective marketing, since one can send out a smaller amount of e-mail blast and get higher response. It also allows putting together an advertisement that refers to the local group, a specific group of people that want to reach. It can also be called as niche marketing.

Targeted e-mail advertising is a more favourable form of advertising. Recipients tend to have no problem with a targeted advertisement. *For example*, if an accountant receives a targeted advertisement offering, a new accounting software that is more recent and time efficient, he/she will be more interested in reading or looking through it rather than getting irritated or trying to unsubscribe. The advertisement is especially liked if the advertisement says something in the subject that states that it is being sent to accountants. Another example is if a cardiologist receives an advertisement about a new technology of heart surgery equipments. The doctor will most likely be interested in the advertisement rather than trying to unsubscribe or complain about receiving that targeted e-mail advertisement.

So target e-mail advertising is a very valuable form of e-mail advertising, and easily allows one to make lots of profits if it goes to the right company and if the right ad message is put.

13.2 How it Works?

The way targeted e-mail advertising works is easy and at the same time more professional than ordinary group e-mail blasts. Firstly, it is necessary to find a company that has many targeted e-mail lists which they are eager to use to do target e-mail marketing. Then the advertisement should be creative and simple. After advertisement message/ Newsletter is ready. One will then prefer the group of people, to whom e-mail is targeted from their website. One can prefer either by profession or location.

The next thing will be to place an order for a specified number of targets on their website. Advertisement will then be sent out to that group of people and will be provided with real-time stats report. One will then start receiving traffic and sales from the targeted e-mail advertising that they executed for.

13.3 How to Organize a Targeted E-mail?

Once, one has decided on a target e-mail which one wishes to pursue, then decide on the group of people one wishes to target, *for example*, student groups can be defined by:

- i. Degree discipline (Department and / or course)
- ii. Nationality
- iii. Year of study
- iv. Level of student (undergraduate, masters or research)

As a general rule, these student group definitions can be mixed together, *for example*, final year Physics, Mechanical Engineering and Computing undergraduates from France and Germany.

13.4 Processing a Targeted E-mail

- i. As soon as one agrees to the quote and proceeds with the target e-mail, one will require the text that an individual wants to send to the target group, either a Word document or plain e-mail text.
- ii. Once the target e-mail is received by the Careers Advisory Service, this can be processed and sent to the target group.

- iii. Once the target e-mail has been completed, an invoice is sent for the agreed amount. To aid the invoicing process, one will require either a Purchase Order Number or Confirmation Letter the company letter-head authorizing the target e-mail and invoicing thereafter.

Summary

Website: A set of interconnected web pages, usually including a homepage, generally located on the same server, and prepared and maintained as a collection of information by a person, group, or organization.

Create the content: When one has selected the publishing platform and thought of the website design one can go back to the paper sketch and start creating the content.

Bandwidth required: Since bandwidth is a significant determinant of hosting plan prices, one should take time to determine just how much is right for one's site.

Website cost: The cost of a website can vary greatly, depending upon the site's features, needed Internet marketing services, aesthetic qualities, the design firm, advertising agency, or freelancer creating the Web design.

Website Reach/Accessibility: Accessibility means that it is coded well, it is easy to navigate, and it works in everyone's browser.

Web promotion: Every time one can and one should advertise the site, just about anywhere and everywhere.

Types of promotion:

- i. Target e-mail
- ii. Shopping bots
- iii. Banner exchange



PU Questions

[Apr.2013 – 15M]

[Apr.2013 – 5M]

[Oct.2012 – 15M]

[Oct.2012 – 5M]

[Apr.2012 – 15M]

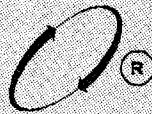
[Oct.2011 – 15M]

[Oct.2011 – 5M]

[Apr.2011 – 15M]

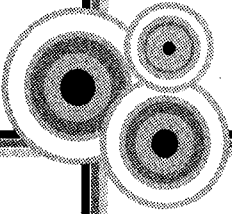
[Apr.2011 – 15M]

1. Explain benefits of building own website and different ways of promoting the website.
2. Write short notes on: Banner Exchange
3. Brief about WWW. Explain reasons for building own website
4. Write short notes on: Shopping Bots
5. Explain in detail how a Domain is registered? Brief about Cost, Time and Reach factors for building own Website.
6. What are the reasons for building own website? What are the bandwidth requirements for the same?
7. Write short note on: Web promotion
8. Define website. Explain the reasons for building own website.
9. Elaborate on domain name. Describe procedure for registering a domain name.



VISION

INTERNET AND EXTRANET



1. Internet

Internet is a global network of computers that can be server or client that exchanges information. It is defined as a 'network of networks' which can be linked through copper wires, wireless connections, and other technologies. Internet includes millions of private and public, academic, business, and government networks either local or global. It is the world-wide network of computers accessible to anyone who knows their Internet Protocol (IP) address.

IP address is a unique set of numbers that defines the computer's location. Before the named computer can be accessed, the name needs to be translated into an IP address. Thus, browser access a Domain Name Server (DNS) computer to lookup the name and return an IP address - or issue an error message to indicate that the name was not found. Once browser has the IP address it can access the remote computer.

It refers to outward-facing systems, with little or no connection to any other internal systems. Internet sites have rapidly evolved from inter-organization ecommerce systems to become a general-purpose broadcast medium for sharing data, e-commerce, corporate marketing material, etc.

This refers to the global system involving organizations of all categories, types, and size. It is a global collection of interconnected network of computers. It is made up of millions of computers

linked together around the world in such a way that information can be sent from any computer to any other 24 hours a day, 7 days a week. The computers can be in homes, schools, universities, government departments, or businesses small and large. The computers can be dumb terminals, personal computers, servers or workstations on a school or a company network. The Internet is often described as “a network of networks” because all the smaller networks of organizations are linked together into one giant network called the Internet. All computers are pretty much equal once connected to the Internet; the only difference is the speed of the connection which is dependent on the Internet Service Provider, processing power of PC, Modem or the LAN Card. The internet has developed a very strong community base where information, software and expert advice are freely shared and for this reason users have developed a very strong protective stance on freedom of speech, freedom from commercial interests, netiquette and unsuitable material on the web.

2. Tools and Services of Internet

Following are the tools and services of internet:

- i. Electronics mail
- ii. File transfer protocol
- iii. Telnet
- iv. Internet Relay Chat (IRC)
- v. Instant messengers
- vi. The World Wide Web
- vii. Remote accesses
- viii. Streaming media
- ix. Voices and video conferencing
- x. E-commerce

- i. **Electronic mail:** One of the very useful things about the Internet is that it allows exchanging electronic message (e-mail) across the world instantly. E-mail is a popular way of communication of electronic matter. An email program allows the users to create messages and send them to other users. One can e-mail to friend or to a researcher or to anyone for getting a piece of information. E-mail is mainly used for sending electronic piece of text. Through, e-mail one can be in direct touch with many of friends and colleagues.
- ii. **File Transfer Protocol (FTP):** Internet provides access to all kinds of information. However, files and data are scattered all over the Internet in large and small archives. Some of these may contain text; some may contain pictures or sounds, or computer programs. There exists a standard tool on Internet for transferring copies of files.

This program is called FTP, i.e., file transfer protocol. FTP can be used to copy any file from one Internet host to other. However, for such transfer one need an account on a remote host. The FTP program will make a connection with the remote host, which will allow browsing the directories and specifying files at the remote server. One can transfer the copy and then look at it, once it is available on own computer when transferred. What happens if one does not have an account on a remote Internet host? In such cases anonymous FTP recognizes a special account name called anonymous. Thus, by using anonymous FTP one can access public archives on the Internet and copy a file from there. Some of the common programs such as WinZip are used to compress a file before using FTP. The basic advantage of using these

compressed files is that these files require less storage space, and less time to transmit from one computer to another computer on Internet.

- iii. **Telnet:** Telnet is a program that allows an Internet host or a client computer to become a terminal of another host on the Internet. FTP opens a connection solely for transfer of files and allows becoming a user on a remote machine. One can run the computer programs at remote host, browse the database or perform any desired operation of the remote machine using this facility. Thus, Telnet provides a direct access to various services on Internet. Some of these services are available on the host, but Telnet is especially useful when these services are not available on the host. *For example*, if one wants to use graphical interfaces designed by other users, then Telnet allow accessing their hosts and using their new interfaces. Similarly, whenever someone creates a useful service on their host, Telnet allows accessing this valuable information resource. This tool is especially useful for accessing public services such as library OPAC, the databases available on the remote machine, etc. There are many databases available on the Internet. There are many Internet services yet to be created. Every year better means of accessing the treasures of the Internet are appearing in which Telnet is the key for accessing.
- iv. **Internet Relay Chat (IRC):** IRC stands for Internet Relay Chat. IRC may be one of the most addictive services available on the Internet, and often draws people into spending several hours a day on it. It is essentially a tool for chatting with other groups of people on various topics through key-board and an application. It gives people all over the world the ability to talk (type) to one another in real time. There are hundreds of thousands of users on IRC at any one time, although they are distributed across server networks and many thousands of discussion channels. This is a protocol that is the original means of chatting through the actual Internet. There are several IRC networks that exist, where users can log into any IRC server and chat with anyone on the network directly or in a 'channel' (also known as a 'chat room').
- v. **Instant messengers:** They are helpful to chat/send messages personally in an instantaneous manner, if the person is online or else one can leave the messages offline too, if the person is not connected. There are different interfaces for each language, one can communicate with others using ICQ, AOL, MSN, and Yahoo message systems. It also includes shared calendar and chat groups.
- vi. **The World Wide Web:** The World Wide Web is a huge set of interlinked documents, images and other resources, linked by hyperlinks and URLs. These hyperlinks and URLs allow the web servers and other machines that store originals, and cached copies, of these resources to deliver them as required using HTTP (Hypertext Transfer Protocol). HTTP is only one of the communication protocols used on the Internet. Web services also use HTTP to allow software systems to communicate in order to share and exchange business logic and data. Software products that can access the resources of the Web are correctly termed user agents. In normal use, web browsers, such as Internet Explorer and Firefox, access web pages and allow users to navigate from one to another via hyperlinks. Web documents may contain almost any combination of computer data including graphics, sounds, text, video, multimedia and interactive content including games, office applications and scientific demonstrations. Using

the Web, it is also easier than ever before for individuals and organizations to publish ideas and information to an extremely large audience.

- vii. **Remote accesses:** The Internet allows computer users to connect to other computers and information stores easily, wherever they may be across the world. They may do this with or without the use of security, authentication and encryption technologies, depending on the requirements. This is encouraging new ways of working from home, collaboration and information sharing in many industries. An accountant sitting at home can audit the books of a company based in another country, on a server situated in a third country that is remotely maintained by IT specialists in a fourth. An office worker away from his desk, perhaps on the other side of the world on a business trip or a holiday, can open a remote desktop session into his normal office PC using a secure Virtual Private Network (VPN) connection via the Internet. This gives the worker complete access to all of his or her normal files and data, including e-mail and other applications, while away from the office.
- viii. **Streaming media:** Many existing radio and television broadcasters provide Internet 'feeds' of their live audio and video streams (*for example*, the BBC). They may also allow time-shift viewing or listening such as preview, classic clips and listen again features. These providers have been joined by a range of pure Internet 'broadcasters' who never had on-air licenses. This means that an Internet-connected device, such as a computer or something more specific, can be used to access on-line media in much the same way as was previously possible only with a television or radio receiver.
- ix. **Voices and video conferencing:** With this one can see and hear each other over the net. This can be done through net meeting which is an inbuilt application in the Windows package.
- x. **E-commerce:** The word E-commerce means electronic commerce, with this one can trade over the net, i.e., one can purchase and sell goods over the internet, through various websites like amazon.com, etc.

3. Hardware and Software for Internet

A variety of hardware and software are used to make Internet functional, like:

- i. **Modem:** Modem is a device that enables computers to communicate through phone lines. Modem can be divided into two parts: MO, i.e., modulator and DEM, i.e., demodulator. Modem may be internal or external. Modulator converts digital signals to analog signals, whereas a demodulator performs the opposite function, i.e., it converts the analog signals to digital signals. Speed of modem is measured in bits per seconds. Higher the bps faster is the modem. Modem is available in range from 9.6 to 56 kbps.

When one starts internet, the modem communicates to the modem of Internet Service Provider (ISP).

- ii. **Computer:** In addition to modem one need a client capable of handling multiple data types. The client may be a mobile, laptop or a personal computer which is capable of handling the different data types like integers, floats and strings etc.
- iii. **Software:** Two types of software are required to enable PC as an Internet PC.
 - a. Communication software to establish TCP/IP connection to the server. An internet under TCP/IP operates like single networks connecting many computers of any size and type.
 - b. Client software for browsing, e-mail, news such as Microsoft Outlook for e-mails, Firefox, Internet Explorer, Google Chrome, Opera etc., for web browsing and Collabra for being updated with latest news.

4. Advantages and Disadvantages of Internet

Advantages

1. **Communication:** The primary target of internet has always been the communication. And internet has excelled beyond the expectations. Innovations are going on to make it faster, more reliable. By the advent of computer's Internet, earth has reduced and has attained the form of a global village.

Now, communication can be done in a fraction of second with a person who is sitting in the other part of the world. Today for better communication, one can avail the facilities of e-mail; one can chat for hours with loved ones. There are a number of messenger services. With the help of such services, it has become very easy to establish a kind of global friendship where one can share thoughts, can explore other cultures of different ethnicity.

2. **Information:** Information is probably the biggest advantage internet is offering. The Internet is a virtual treasure trove of information. Any kind of information on any topic under the sun is available on the Internet. The search engines like Google, yahoo is at service on the Internet. One can almost find any type of data on almost any kind of subject that one is looking for. There is a huge amount of information available on the internet for just about every subject known to man, ranging from government law and services, trade fairs and conferences, market information, new ideas and technical support, the list is endless.

Students and children are among the top users who surf the Internet for research. Today, it is almost required that students should use the Internet for research for the purpose of gathering resources. Teachers have started giving assignments that require research on the Internet. Almost every coming day, researches on medical issues become much easier to locate. Numerous web sites available on the net are offering loads of information for people to research diseases and talk to doctors online at sites.

3. **Entertainment:** Entertainment is another popular reason why many people prefer to surf the Internet. In fact, media of internet has become quite successful in trapping multifaceted entertainment factor. Downloading games, visiting chat rooms or just surfing the Web are some of the uses people have discovered. There are numerous games that may be downloaded from the Internet for free. The industry of online gaming has tasted dramatic and phenomenal attention by game lovers. Chat rooms are popular because users can meet new and interesting people. In fact, the Internet has been successfully used by people to find lifelong partners. When people surf the Web, there are numerous things that can be found. Music, hobbies, news and more can be found and shared on the Internet.
4. **Services:** Many services are now provided on the internet such as online banking, job seeking, purchasing tickets for favorite movies, guidance services on array of topics engulfing every aspect of life, and hotel reservations. Often these services are not available off-line and cost more.
5. **E-Commerce:** E-commerce is the concept used for any type of commercial strategy, or business deals that involves the transfer of information across the globe via Internet. It has become a phenomenon associated with any kind of shopping, almost anything. It has got a real amazing and wide range of products from household needs, technology to entertainment.

Disadvantages

1. **Theft of Personal information:** If one uses the Internet, one may be facing grave danger as the personal information such as name, address, credit card number, etc. can be accessed by other culprits to make the problems worse.
2. **Spamming:** Spamming refers to sending unwanted e-mails in bulk, which provide no purpose and needlessly obstruct the entire system. Such illegal activities can be very frustrating, and so instead of just ignoring it, one should make an effort to try and stop these activities so that using the Internet can become that much safer.
3. **Virus threat:** Virus is nothing but a program which disrupts the normal functioning of computer systems. Computers attached to internet are more prone to virus attacks and they can end up into crashing whole hard disk, causing considerable headache.
4. **Pornography:** This is perhaps the biggest threat related to children's healthy mental life a very serious issue concerning the Internet. There are thousands of pornographic sites on the Internet that can be easily found and can be a detrimental factor to letting children use the Internet.

5. Intranet

The term Intranet is derived from two words, 'Intra' which means within and 'net' which means group of interconnected computers. Intranet is a group of interconnected computer within an organization or company that uses Internet standards like Hyper Text Transfer Protocol (HTTP), Hyper Text Markup Language (HTML), Transmission Control Protocol (TCP), Internet Protocol (IP) and internet software's like web server and web browser to share information.

An Intranet is a private computer network that uses Internet protocols and network connectivity to securely share any part of an organization's information or operational systems with its employees. Sometimes the term refers only to the organization's internal website, but often it is a more extensive part of the organization's computer infrastructure. Private websites are also an important component and focal point of internal communication and collaboration.

In short, an intranet is private network, similar to the Internet and using the same protocols and technology, contained within an enterprise or not-for-profit organization. Widely referred to as the home page of the internal website, the intranet also includes many inter-linked Local Area Networks (LANs), desktop computers, websites and portals, and email system.

It may consist of many interlinked Local Area Networks and also use leased lines in the Wide Area Network. Typically, an intranet includes connections through one or more gateway computers to the outside Internet. The main purpose of an intranet is to share information within the organization and computing resources among employees. An intranet can also be used to facilitate working in groups and for teleconferences. The Intranet is a Web-based architecture used for managing internal information. Intranet is an organization's internal information system that uses Internet tools, protocols, and technology. Intranets take the same features that make a World Wide Web useful minus geographic and time barriers, integrating multiple information services into a single interface, interactive multimedia application, etc. and bring them into the office. Typically, larger organizations allow users within their intranet to access the public Internet through firewall servers that have the ability to screen messages in both directions so that company security is maintained. A firewall is a computer or several computers that sit between network and the greater Internet. Using filtering and specialized routing, as well as rules one decide upon, firewalls keep out people who don't have permission to access resources internally. With tunneling, companies can send private messages through the public network, using the public network with special encryption/decryption and other security safeguards to connect one part of their intranet to another. In some ways, the word 'Intranet', this logically combines the concepts in 'internal internet between business sites'. Internal Web servers, FTP archives, newsgroups, and other resources become the way the employees get their work done.

Number of Questions
1

Apr. 2012 – 5M

Write a short note on:
Intranet

► Intranet over Internet

The technologies used in Intranet and Internet may be same but the main difference between them is that the information shared in intranet can be access only by authorized persons especially members or employees of the organization or company where as in internet the information is shared worldwide with any public user to explain in simple terms, intranet is private, within the organization while internet is public available for global access requirement. Thus, Intranet is like a private Internet.

► Intranet over Extranet

Intranets differ from extranets in that the former are generally restricted to employees of the organization while extranets may also be accessed by customers, suppliers, or other approved parties. Extranets extend a private network onto the Internet with special provisions for access, authorization and authentication.

6. Software of Intranet

The components or software used in Intranet are:

The components or software used in Intranet are:

- i. **TCP**
 - ii. **IP**
 - iii. **Web Server**
 - iv. **Web Browser**
- i. **Transmission Control Protocol:** It helps in breaking the message or file into smaller packets that can be transmitted to the receiving end where another Transmission Control Protocol reassemble the packets and convert it into original message. Each gateway computer on the network checks this address to see where to forward the message. Even though some packets from the same message are routed differently than others, they'll be reassembled at the destination.
 - ii. **Internet Protocol:** The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet. When one sends or receives data, the message gets divided into little chunks called packets. Then it handles the address part each packet so that they can reach to their right destination.
 - iii. **Web Server:** A Web server is a program that, using the client/server model and the World Wide Web's Hypertext Transfer Protocol (HTTP), serves the files that form Web pages to Web users (whose computers contain HTTP clients that forward their requests). Every computer on the Internet that contains a Web site must have a Web server program. Two leading Web servers are Apache, the most widely-installed Web server, and Microsoft's

Internet Information Server (IIS). Other Web servers include Novell's Web Server for users of its NetWare operating system Web Browser.

- iv. **Web Browser:** The word 'browser' seems to have originated prior to the Web as a generic term for user interfaces that one browse text files online. A Web browser is a client program that uses HTTP (Hypertext Transfer Protocol) to make requests of Web servers throughout the Internet on behalf of the browser user.

Internet explorer is the most commonly used browser, having won the so-called browser wars between IE and Netscape. Other browsers include:

- a. Firefox, which was developed from Mozilla (the open source version of Netscape).
- b. Safari, a browser for Apple computers (at this writing, the third most popular browser).
- c. Lynx, a text-only browser for UNIX shell and VMS users.
- d. Opera, a fast and stable browser that's compatible with most relatively operating systems.

7. Intranet Security

A company can prevent unwanted intrusion or access into their Intranet network through two security levels:

► Internal Level

This level helps in preventing employee of the organization to misuse their company's confidential information. It can be done by Public Key Security. It has two parts:

- i. **Encryption:** Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people. Simple ciphers include the substitution of letters for numbers, the rotation of letters in the alphabet, and the 'scrambling' of voice signals by inverting the sideband frequencies. More complex ciphers work according to sophisticated computer algorithms that rearrange the data bits in digital signals. In order to easily recover the contents of an encrypted signal, the correct decryption key is required.
- ii. **Digital certificates:** A digital certificate is an electronic 'credit card' that establishes credentials when doing business or other transactions on the Web. It is issued by a Certification Authority (CA). It contains name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

► External Level

In an organization, intranet network is connected with internet connection then the next issue is regarding the protection of its confidential information from public internet user.

This is done through using firewall. The term firewall is originated from the firefighting because in firefighting the firefighter use Firewall as a barrier which helps in preventing the spread of fire. Firewall is a security device or software which is located between company's internal and external network, i.e., between Intranet and Internet. A firewall is a set of related programs, located at a network gateway server, which protects the resources of a private network from users from other networks. An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to. It needs to be regularly upgraded from time to time to check the latest potential security problems.

8. Planning and Creating an Intranet

Most organizations devote considerable resources into the planning and implementation of their intranet as it is of strategic importance to the organization's success. Some of the planning would include topics such as:

- i. The purpose and goals of the intranet.
- ii. Persons or departments responsible for implementation and management.
- iii. Implementation schedules and phase-out of existing systems.
- iv. Defining and implementing security of the intranet.
- v. How they'll ensure to keep it within legal boundaries and other constraints.
- vi. Level of interactivity desired.
- vii. Is the input of new data and updating of existing data to be centrally controlled or devolved?

These are in addition to the hardware and software decisions, participation issues and features to be supported.

The actual implementation includes steps as:

- i. User involvement to identify users' information needs.
- ii. Setting up web server with the appropriate hardware and software.
- iii. Setting up web server access using a TCP/IP network.
- iv. Installing required user applications on computers.
- v. Creation of document framework for the content to be hosted
- vi. User involvement in testing and promoting use of intranet.

9. Advantages and Disadvantages of Intranets

► Advantages of Intranet

- i. **Workforce productivity:** Intranets help users to locate and view information faster and use applications relevant to their roles and responsibilities. With the help of a web browser interface, users can access data held in any database the organization wants to make available, anytime which is subjected to security provisions, i.e., from anywhere within the company workstations, increasing employee's ability to perform their jobs faster, more accurately, and with confidence that they have the right information. It also helps to improve the services provided to the users.
- ii. **Time:** With intranets, organizations can make more information available to employees on a 'pull' basis rather than being cascaded indiscriminately by emails.
- iii. **Communication:** Intranets can serve as powerful tools for communication within an organization, vertically and horizontally. From a communications standpoint, intranets are useful to communicate strategic initiatives that have a global reach throughout the organization. The type of information that can easily be conveyed is the purpose of the initiative and what the initiative is aiming to achieve, who is driving the initiative, results achieved to date, and who to speak to for more information. By providing this information on the intranet, staff has the opportunity to keep up-to-date with the strategic focus of the organization.
- iv. **Web publishing:** An Intranet is an excellent platform for publishing information internally. It is easily deployable, as the ubiquitous Web browser is available for virtually every operating system. It allows 'cumbersome' corporate knowledge to be maintained and easily accessed throughout the company using hypermedia and Web technologies. Because each business unit can update the online copy of a document, the most recent version is always available to employees using the intranet.
- v. **Business operations and management:** Intranets are also being used as a platform for developing and deploying applications to support business operations and decisions across the inter-networked enterprise.
- vi. **Cost-effective:** Most organizations have already established TCP/IP networks, and the incremental infrastructure cost of adding Web servers to the network is well within even departmental-level budgets. Users view information and data via web-browser rather than maintaining physical documents such as procedure manuals, internal phone list and requisition forms.
- vii. **Promote common corporate culture:** Every user is viewing the same information within the Intranet.

Advantages of Intranet

- i. Workforce Productivity
- ii. Time
- iii. Communication
- iv. Web Publishing
- v. Business operations and management
- vi. Cost effective
- vii. Promote common corporate culture
- viii. Enhance collaboration
- ix. Cross-platform capability
- x. Low maintenance
- xi. Scalability
- xii. Easy software distribution

- viii. **Enhance collaboration:** With information easily accessible by all authorized users, teamwork is enabled.
- ix. **Cross-platform capability:** Standards-compliant web browsers are available for Windows, Mac, and UNIX.
- x. **Low maintenance:** It is relatively easy and affordable to add new information or to update existing information and make it instantly available.
- xi. **Scalability:** Corporations will be able to deliver information systems on the least expensive computing platforms available and to scale their computing resources upward or downward as condition shift.
- xii. **Easy software distribution:** Once PC users are equipped with Web browsers, new Web sites or pages with new information can be added without incurring the expense of locating users, sending them updated client software, and supporting them through the upgrade process.

► Disadvantages of Intranet

- i. **Collaborative applications for Intranet are not as powerful as those offered by traditional groupware:** For instance, Intranet includes no built-in data replication or directory services for remote users, while groupware packages such as Lotus notes do.
- ii. **Short-term risk:** There are limited tools for linking an Intranet server to database or other back-end mainframe-based applications. Programming standards for the Web, such as Common Gateway Interface (CGI) and Java are fairly new and just maturing.
- iii. **Less back-end integration:** With Intranets, firms have to set up and maintain separate applications such as E-mail and Web servers, instead of using one unified system as with groupware.

10. Features of Intranet

Features of Intranet

- i. Shared access to documents
- ii. Controlled access
- iii. Flexible organization
- iv. Events calendar, scheduler
- v. Message boards
- vi. Address book
- vii. Intranet search engine
- viii. Task management
- ix. Customizable interface
- x. Individualization

- i. **Shared access to documents:** This is the universal function among leading corporate intranet software. Documents should be saved in a standard file format so that all employees can open files without having compatibility issues. Many intranets allow links to outside Web sites. The Web contains a excess of useful business tools and it makes sense to make them as readily accessible as possible. Employees are sure to save time when resources such as phone directories, travel reservation sites and shipping vendors are only a click away.

- ii. **Controlled access:** Intranets should be password protected. Human resource records, corporate communications and other proprietary information should be carefully guarded from intruders. Strict security policies should be set bearing in mind that former or current employees are potential trespassers.

A sophisticated intranet allow for different levels of access. Top-level executives might have exclusive access while most other employees will be excluded from viewing confidential accounting and HR information. However, mid-level managers may need access to department level accounting and HR records. Controlled access also makes an intranet more flexible and greatly widens the range of uses.

- iii. **Flexible organization:** Intranet should be organized in a logical and precise manner. To do this effectively one need to be able to control how the content in intranet is classified.

The ability to add sub-departments will give the option to organize content in an easily searchable hierarchical fashion. This type of organization will allow to accurately establishing security parameters.

- iv. **Events calendar, scheduler:** A centralized scheduling system ensures that everyone stays on the same page. It allows meetings and events to be scheduled from a company, department and team level, when such meetings are posted all affected personal will be notified. Additionally, if the intranet is set up with appropriate controlled access, it's possible to give individuals the flexibility to schedule their own meetings and tasks.

- v. **Message boards:** Message boards allow employees to express frustrations and workout solutions. This unique forum promotes the sharing of ideas that may not occur in face-to-face discussions. It also fosters communications between departments and peer groups that might not otherwise communicate. Having these discussions on the intranet, rather than on outside service, keeps discussions focused and positive.

- vi. **Address book:** A comprehensive list of client, vendor and employee contact information makes a great addition to a company intranet. Not only is it easier to search through than its paper counterpart, it's also faster and less expensive to update.

With the right technology, an address book can become an important communication tool. Batch email functionality can be implemented so that mass emails can be sent based on search criteria. Furthermore, messages could be sent to wireless devices, such as PDAs or cell phones.

- vii. **Intranet search engine:** No matter how well things are organized, sometimes a key word search is the fastest way to find something. An Intranet Search Engine is a text field where one type in a key work and click "search." The intranet will be scanned and a list of matching results will appear within a couple of seconds.

The search function should be easily accessible, ideally available from every page on the intranet. A search field and button take up less space than a pinky finger on the screen. So, non-obtrusive yet convenient placement is a cinch.

- viii. **Task management:** Managers can add tasks for their direct reports to complete. Employees can check for new tasks and prioritization by checking their list on the intranet each day. Tasks can easily be reassigned or reprioritized by the manager by simply changing the employee or the date associated with the task.
- ix. **Customizable interface:** Another common feature of many intranet systems is that the interface is customizable. This often means that colors can be modified, a logo can be uploaded and the company name can be displayed. It may seem like a minor feature, but it's actually an important branding tool. It's the difference between handing out plain white T-shirts to employees and handing out t-shirts emblazoned with a bright company logo.
- x. **Individualization:** Intranets should ideally conform to the individual user. The idea is that intranets should be comfortable and convenient for a variety of employees with a varying range of responsibilities. Our company intranet includes a couple of slick features that achieve this end.

11. Components of Intranet Information Technology Structure

Depending on the size and needs of business, an intranet can consist of little more than email service and file sharing or can include full-fledged document management and videoconferencing. Regardless, all intranets are made up of the same basic parts:

Components of Intranet Information Technology Structure are as follows:

- i. The Network
- ii. File sharing
- iii. Communication
- iv. Group collaboration
- v. Internet access
- vi. Security

- i. **The network:** Modern intranets use a foundation of common Internet technologies, such as Point-to-Point Protocol (PPP) and Transmission Control Protocol/Internet Protocol (TCP/IP). Intranet software should support the Internet standards. Increasingly, intranet applications are designed to be viewed and used through a common Web browser.
- ii. **File sharing:** File sharing allows to store electronic documents in public folders so other people can see them and modify them. More advanced intranets allow to create folders that can be opened only by certain groups of people, such as members of the accounting or sales departments.

While it's easiest to share files between the same types of computers one can buy software that lets dissimilar machines share files as well.

- iii. **Communication:** Email is the most common form of communication on an intranet, but some companies add other options, such as discussion groups accessed via a Web browser, instant messaging to chat with clients, and/or videoconferencing. It's also possible to run an internal Web server so workers can post personal Web sites for other employees to view.
- iv. **Group collaboration:** By combining several tools on an intranet, groups can share calendars, take part in 'virtual workspaces' that contain public messages and files, and log into private chat areas dedicated to specific business projects. These group collaboration features are ideal if one have employees in several branch offices, which need to work together on a project.
- v. **Internet access:** It's not mandatory, but many companies also use their intranets to provide Web access for employees. Since the base technologies are the same, it's generally quite easy. Some all-in-one intranet servers come with built-in support for sharing a connection to an Internet service provider.
- vi. **Security:** An intranet is generally intended for employees only when one doesn't want the rest of the world reading everything on it, so security is a big issue, especially if one also use intranet to connect to the Internet. A firewall is software or hardware, or both, designed to prevent unauthorized access to intranet by blocking outside connections. Of course, employees who spend too much time looking at sports or pornography sites will hurt business, too. Proxy servers and network monitoring tools help make sure that employees use the Web for real work by blocking unauthorized sites or tracking where people browse.

12. Extranet

An extranet is a type of inter-organizational information system. Extranets enable people who are located outside a company to work together with company's internally located employees'. The main goal of extranet is to foster collaboration between business partners. An extranet is open to selected suppliers, customers and other business partners who access it through the internet. It is closed to the general public. It is a private network that uses the Internet protocol and the public telecommunication system to securely share part of an organization's information or operations with its branches (located within the same city or outside), partners, users, customers, suppliers or contacts. An extranet can be viewed as part of an organization's intranet that is extended to users outside the organization. An extranet requires security and privacy. These require firewall server management, the issuance and use of digital certificates or similar means of user authentication, encryption of messages, and the use of Virtual Private Networks (VPN) that tunnel through the public network.

Number of questions asked
1

Apr.2013 – 5M

Write a short note on:
Extranet

As businesses continue to use open Internet technologies to improve communication with customers and partners, they can gain many competitive advantages along the way - in product development, cost savings, marketing, distribution, and leveraging their partnerships. And, perhaps, most important of all, they can strengthen their business relationships.

Extranet is an intranet for outside authorized users using same internet technologies. The outside users are trusted partners of the organization who have access to information of their interest and concern.

Extranet is actually an Intranet that is partially accessible to authorized outsiders. The actual server resides behind a firewall. The firewall helps to control access between the Intranet and Internet permitting access to the Intranet only to people who are suitably authorized. The level of access can be set to different levels for individuals or groups of outside users. The access can be based on a username and password or an IP address.

When intranet crosses the logical boundary of the organization and provides secured access to selected data and information of the organization the intranet becomes extranet.

An extranet is a private network that uses Internet protocols, network connectivity, and possibly the public telecommunication system to securely share part of an organization's information or operations with suppliers, vendors, partners, customers or other businesses. An extranet can be viewed as part of a company's intranet that is extended to users outside the company. It has also been described as a 'state of mind' in which the Internet is perceived as a way to do business with a pre approved set of other company's business-to-business (B2B), in isolation from all other Internet users. In contrast, business-to-consumer (B2C) involves known server of one or more companies, communicating with previously unknown consumer users.

An extranet can be an intranet mapped onto the public Internet or some other transmission system not accessible to the general public, but is managed by more than one company's administrator. An intranet is a VPN under the control of a single company's administrator. 'Extranet' is a useful term to describe selective access to intranet systems granted to suppliers, customers, or other companies. Such access does not involve tunneling, but rather simply an authentication mechanism to a web server. In this sense, an 'extranet' designates the 'private part' of a website, where 'registered users' can navigate, enabled by authentication mechanisms on a 'login page'.

An extranet requires security. These can include firewalls, server management, the issuance and use of digital certificates or similar means of user authentication, encryption of messages, and the use of Virtual Private Networks (VPNs) that tunnel through the public network.

13. Applications of Extranet

- i. **Improved quality:** Computer to computer communication reduces errors in data entry.
- ii. **Lower communication and travel costs:** Using internet one can save 50% or more on communication costs and can reduce travel and physical meeting costs.
- iii. **Lower administrative and other overhead costs:** Automation of order entry and other routine processes saves time and resulting costs.
- iv. **Fewer help-desk employees needed:** Extranets automate inquiry systems: customers dial into databases to find information.
- v. **Faster process and information flow:** By using extranets information can flow across the supply chain rapidly, even when several tiers of suppliers are involved. Expedited processes can reduce design and production costs.
- vi. **Reduction in paper work and delivery of accurate information in timely manner:** Publishing information electronically for customers and business partners eliminates paper work and assures that information is current.
- vii. **Improved order entry and customer service:** Many companies use extranets to simplify and improved the customer order entry process as well as customer service and client relationship.
- viii. **Better communication:** Just in time information delivery and collaborative activities improve communications among business partners and / or customers.
- ix. **Overall improvement in business effectiveness:** Use of extranets enhances business opportunities, makes better use of legacy systems, promotes more effective marketing and sales and makes available training on demand.

14. Advantages and Disadvantages of Extranet

Advantages of Extranet

An organization can use provisions of the Intranet to create systems with an idea to build them for improving employee productivity, sharing data, or updating human resources information. Then they would build other applications for use outside the organization - either products for their customers or products to let the company communicate better with their vendors. So in addition to internal company networks, or intranets, that are behind the firewall, companies are building external networks called 'extranets' that reach out to people who may physically work outside the firewall

but who are an important part of the business strategy, product-delivery system, or customer-support apparatus. The organizations can use an extranet to:

- i. Exchange large volumes of multimedia data using Electronic Data Interchange (EDI).
- ii. Share office information, library, circulars, etc., at all the locations. Collaborate with other organisations on joint development efforts.
- iii. Jointly develop and use training programmes with other organizations.
- iv. Provide or access services provided by one organization to a group of other organizations.
- v. Share news of common interest exclusively with partner organizations.

An extranet is not the only method of connecting an organization to distant locations of the same organization but also to similar organizations, their employees, researchers, etc. to other businesses. An extranet offers an organization the same benefits that an intranet offers, while also delivering the benefits of being linked to the outside world. Some of the specific advantages of an extranet include the following:

Advantages of extranet are as follows:

- i. Ubiquity of access
 - ii. Open standards
 - iii. Less time and money
 - iv. System vulnerability
 - v. Insufficient support
 - vi. Coordination
 - vii. Feedback
 - viii. Customer satisfaction
 - ix. Cost reduction
 - x. Expediting communication
- i. **Ubiquity of access:** One advantage of the Internet is that it is becoming increasingly acceptable to any existing contractor or subcontractor. One doesn't need to make sure the operating system is the same, or that one is using the same type of database. "An extranet is an effective way for organizations to communicate without having to agree to buy all similar systems so the cost of enabling goes way down".
 - ii. **Open standards:** Another advantage of an extranet is the Internet's open standards. Regardless of what equipment different companies own, it's unlikely they buy their equipment from the same vendor. The extranet eliminates many compatibility problems.
- iii. **Less time and money:** Lastly, and most importantly, an extranet can save a corporation money and time. The intranet and extranets are being popularly used for communication application like audio and video conferencing, net meetings, net shows, collaborative multimedia computing, etc.
 - iv. **System vulnerability:** A system that runs over the Internet is more vulnerable than a proprietary one, and no one has yet come up with a foolproof, end-to-end security plan. Also, the type of information transmitted over extranets-financial data, specs for new products-makes the network an appealing target for hackers.
 - v. **Insufficient support:** Another concern with extranets, which also holds true for intranets, is that of quality of service.

The real significance of extranet is that it is the first non-proprietary technical tool that can support rapid evolution of electronic commerce. On a perhaps more fundamental level, the extranet is also likely to redefine the business evolution of a conventional corporation into

“the knowledge factory”. It will radically change the way private and public sector organizations would conduct their business in the new Internet-driven global economy.

- vi. **Coordination:** An extranet allows for improved coordination among participating partners. This usually includes suppliers, distributors, and customers. Critical information from one partner can be made available so that another partner can make a decision without delay. *For example*, a manufacturer can coordinate its production by checking the inventory status of a customer.
- vii. **Feedback:** An extranet enables an organization to receive instant feedback from its customers and other business partners. It gives the consumers an opportunity to express their views about products or services before those products or services are even introduced to the market.
- viii. **Customer satisfaction:** An extranet links the customer to an organization. This provides the customer with more information about products and services and the organization in general. This also makes ordering products or services as easy as a click of the mouse. Expediting B2B e-commerce is definitely one of the greatest benefits of an extranet.
- ix. **Cost reduction:** An extranet can reduce inventory costs by providing timely information to the participants of a supply-chain program. An extranet application allows distributors throughout the world to submit purchase orders. By doing this, the company increases the efficiency of the operation significantly. It also expedites the delivery of goods and services.
- x. **Expediting communication:** Extranets increase the efficiency and effectiveness of communications among business partners by linking intranets for immediate access to critical information. A traveling salesperson can receive the latest product information from his or her hotel room before going to a sales meeting. A car dealer can provide the latest information to a customer on a new model without making several phone calls and going through different brochures and sales manuals.

► Disadvantages of Extranet

- i. Extranets can be expensive to implement and maintain within an organization, if hosted internally instead of via an ASP.
- ii. Security of extranets can be a big concern when dealing with valuable information. System access needs to be carefully controlled to avoid sensitive information falling into the wrong hands.
- iii. Extranets can reduce personal contact (face-to-face meetings) with customers and business partners. This could cause a lack of connections made between people and a company, which hurts the business when it comes to loyalty of its business partners and customers.
- iv. People who are illiterate and don't have any technology knowledge can feel some problem that how to use it.
- v. Face to face contact is impossible, thus one cannot meet personally any customer or dealer.
- vi. As eye contract is impossible, so one cannot judge that who is using our information is reliable or not. It is possible that he or she can misuse our secrets or our information.

- vii. Small business or small corporate cannot bear this technology's cost as it can increase their expenses.
- viii. Business competitors or the business enemies can misuse the secrets information.
- ix. It reduces the number of employment.
- x. There are many places, where the technology is not developed so it could not work there.

15. Internet versus Intranets

The Internet is a public network. Any user can access the Internet assuming the user has an account with an Internet Service Provider (ISP). The Internet is a worldwide network, whereas intranets are private and are not necessarily connected to the World Wide Web (WWW). Intranets are connected to a specific company network, and the users are usually the company's employees.

An intranet is separated from the Internet through a firewall (or several firewalls). Intranets usually have higher throughput and performance than the Internet and are generally more secure than the Internet.

The two have a lot in common. They both use the same network technology, TCP/IP, and they both use browsers such as Microsoft Internet Explorer or Netscape Navigator. They both use documents in HTML and XML formats, and both are capable of carrying documents in multimedia format. Also, they both use the Java programming language for developing applications.

16. Extranet Versus Intranet

3
Number of Questions asked.

Oct. 2012 – 15M

Explain Internet Concept.
Differentiate between
Intranet and Extranet

Oct. 2011 – 10M

Define Internet.
Differentiate between
Intranet and Extranet.

Apr. 2011 – 5M

Write short note on:
Intranet Vs Extranet.

An extranet is a private network that uses Internet protocols, network connectivity, and possibly the public telecommunication system to securely share part of an organization's information or operations with suppliers, vendors, partners, customers or other businesses. An extranet can be viewed as part of a company's Intranet that is extended to users outside the company (*for example*, normally over the Internet). It has also been described as a "state of mind" in which the Internet is perceived as a way to do business with a preapproved set of other companies business-to-business (B2B), in isolation from all other Internet users. In contrast, business-to-consumer (B2C) involves known server(s) of one or more companies, communicating with previously unknown consumer users.

Briefly, an extranet can be understood as a private intranet mapped onto the Internet or some other transmission system not accessible to the general public, but is managed by more than one company's administrator(s). *For example*, military networks of different security levels may map onto a common military radio transmission system that never connects to the Internet. Any private network mapped onto a public one is a Virtual Private Network (VPN). In contrast, an intranet is a VPN under the control of a single company's administrator(s).

An argument has been made that "extranet" is just a buzzword for describing what institutions have been doing for decades, that is, interconnecting to each other to create private networks for sharing information. One of the differences that characterized an extranet, however, is that its interconnections are over a shared network rather than through dedicated physical lines. With respect to Internet Protocol networks, RFC 4364 states "If all the sites in a VPN are owned by the same enterprise, the VPN is a corporate intranet. If the various sites in a VPN are owned by different enterprises, the VPN is an extranet. A site can be in more than one VPN, *for example*, in an intranet and several extranets. We regard both intranets and extranets as VPNs. In general, when we use the term VPN we will not be distinguishing between intranets and extranets. Even if this argument is valid, the term 'extranet' is still applied and can be used to eliminate the use of the above description."

It is important to note that in the quote above from RFC 4364, the term 'site' refers to a distinct networked environment. Two 'sites' connected to each other across the public Internet backbone comprise a VPN. The term 'site' does not mean 'website'. Further, 'intranet' also refers to just the web-connected portions of a 'site'. Thus, a small company in a single building can have an "intranet," but to have a VPN, they would need to provide tunneled access to that network for geographically distributed employees.

Similarly, for smaller, geographically united organizations, 'extranet' is a useful term to describe selective access to intranet systems granted to suppliers, customers, or other companies. Such access does not involve tunneling, but rather simply an authentication mechanism to a web server. In this sense, an 'extranet' designates the 'private part' of a website, where 'registered users' can navigate, enabled by authentication mechanisms on a 'login page'.

An extranet requires security and privacy. These can include firewalls, server management, the issuance and use of digital certificates or similar means of user authentication, encryption of messages, and the use of Virtual Private Networks (VPNs) that tunnel through the public network.

Many technical specifications describe methods of implementing extranets, but often never explicitly define an extranet. RFC 3547 provides requirements for remote access to extranets. RFC 2709 discusses extranet implementation using IPSec and advanced Network Address Translation (NAT).

17. Development of Intranet

Developing an intranet or extranet is similar to developing other e-commerce applications. This means that a formal life-cycle should be followed. The following phases are used to develop an intranet:

- i. Establishing goals and problem definition
- ii. Cost and benefit analysis
- iii. Formation of the task force
- iv. Construction of a prototype
- v. Assessing the security and privacy issues
- vi. Tool selection
- vii. Implementation
- viii. Post implementation audit and intranet site marketing

► Establishing Goals and Problem Definition

Prior to the implementation of an intranet, similar to other information systems projects, an organization must set goals for the project. What the organization is trying to achieve should be specified as precisely as possible. Establishing goals will enable a prospective organization to measure the degree of success or failure at a later date. The goals might include improving communications among the functional areas for better advertising campaigns, supporting sales activities, creating an organization wide platform for e-commerce activities, improving inventory control, and so forth. Several methods can be used to develop an intranet for an organization. An intranet can start small and grow. A company can try out an intranet pilot project to publish a limited amount of information, *for example*, personnel policies, on a single platform and measure the results. If the pilot is successful then additional content can be added and more departments and organizational units can participate.

During the problem-definition phase for building an intranet site, a likely area for deployment must be identified. The information flow and the needs within the organization must be identified. An area that has appeal to a broad user group should be chosen. This can be done by examining the company's newsletter, human resources procedural handbooks, employee benefits handbook, and competitive sales information. The next step is to identify the content source or authors who will be responsible for the intelligence behind the information and for delivering it. Some of this information may already be available in written or electronic forms; in other cases the entire content may have to be developed from scratch. To identify where the information resides is always a challenging task.

► Costs and Benefit Analysis

Most organizations already have some kind of communications infrastructure in place. When this is the case, additional costs are minimal. However, if the infrastructure is not in place, this will be a major cost. In most cases the benefits that an effective intranet provides outweigh its costs. An intranet can serve as a dynamic platform for collecting and disseminating critical information throughout the organization. This may improve the efficiency and effectiveness of the employees, and it may also improve morale. An intranet can support many activities that in turn support an effective e-commerce program by creating an open platform for functional areas within the organization. An intranet is a critical component of an extranet that makes B2B e-commerce a reality.

Intranet technology can help employees reduce paper reports and unnecessary information. In a typical office, duplicated documents are floating all around. With an intranet only one copy, for example, a training manual, can be posted on the web server, and anybody interested can access the document electronically. Intranet technology allows different individuals to create and maintain relevant information and then make it available to all interested parties.

One of the most important benefits of an intranet is its ability to shift the control of information flow from the information creators to the information consumers. Intranet technology enhances information access by individual users from their desktops. This information may be standard forms, reports, minutes of meetings, new advertising campaigns, or the company mission statement, to name but a few. The information transfers can also include the dissemination of training manuals and educational documents. Traditionally, organizations have spent significant time and money to train and educate their employees on new products, software, and e-commerce policies and procedures. With intranet technology, information can be found efficiently and distributed on demand, which will lead to changing the traditional education and training model. If the appropriate infrastructure is in place, current information content can be found and accessed when and where it is needed. As a result, an intranet can reduce both the time needed for training and the amount of information an employee is required to absorb at once. The intranet is based on “pull technology” through which employees and interested parties extract (pull) exactly what they need when and where they need it. This is the opposite of the traditional ‘push’ technology in which information is delivered (pushed) despite not being asked for or requested. Although push technology is useful for applications, such as memo and policy distribution, this technology may significantly increase the network load. Too often workers are overloaded by information they cannot absorb. Intranets can even reduce the flow of e-mail throughout the organization. *For example*, instead of sending an e-mail to all employees, the president of the company can post a message on the president’s page and the employees can read it if they need to.

► Formation of the Task Force

Similar to the development of other information systems, the development of an intranet should include a task force. The task force creates broad support for this new technology and provides an

opportunity for the involved parties to express their views. The participants of the task force should include representatives from the following departments and user groups:

- i. User groups (including finance, accounting, marketing, manufacturing, and personnel)
- ii. Top management
- iii. Hardware group
- iv. Software group
- v. Legal department
- vi. Graphics or art department

Each group should express its views and needs regarding intranet development. The representatives from the user groups are the most important participants of the task force. Their views must be carefully considered. The representative from top management needs to provide encouragement and financial support. Hardware and software specialists provide technical advice regarding the proper implementation and utilization of the system. They also help with the technical aspects and security issues. The legal department should provide advice regarding legal issues, copyrights, and privacy problems. If such a department does not exist in a particular organization, an external consultant should be hired. The representative from the graphics or art department should provide advice regarding the look, feel, and aesthetics of the intranet site. Users will better receive a more professional-looking site. If such a department does not exist in a particular organization, an external consultant should be hired.

► Construction of a Prototype

Pilot implementation

As with other information systems, the development of an intranet site should start small or be implemented as a pilot project, then be introduced to the entire organization. Organizations must determine whether information should be made available via a web server, e-mail, or through some other means. Many companies find that building Web interfaces to legacy information systems is a key application. With tools such as Purveyor's Data Wizard and HTML Transit, end users can build simple point-and-click access to legacy information systems without programming, making information available to nontechnical users through their Web browsers. Key database applications including access to customer records, product information, and technical problem tracking are good exercises for the pilot project. Typically, organizations begin a pilot with existing content delivered via paper. It is important, for the sake of the pilot, to choose a candidate by which both the costs and results can be tracked and measured accurately. A company usually can directly measure the cost of duplicating and distributing copies of its employee benefits manual. When this traditional process is moved to an intranet site, the savings in direct costs can be taken directly to the bottom line, and the incremental costs of managing the content on the intranet server can be calculated and justified. However, the costs of informal information publishing, such as a memo or table that provides a competitive product analysis, may not be directly measurable. In many organizations, these

competitive tables are developed and distributed by staff people rather than production departments, and the direct costs are buried in other overhead expenses. Therefore, the move from traditional paper based information flow to an intranet may not result in direct measurable cost savings. Once the value of intranet technology has been established through such a pilot, it can be expanded into other departments and functions. In addition, access to other legacy information systems can be provided, so that employees can search and update customer databases, check 401 K balances, vacation days, or register for training classes. This pilot project should provide the entire organization with a better understanding of the usefulness of this powerful technology. It also provides the design team with opportunities to resolve problems before a full-scale implementation takes place.

► **Assessing the Security and Privacy Issues**

The development of intranets brings up certain organizational challenges, including security and privacy issues. Security can be defined as providing access for authorized personnel to the organizational information. A security system protects data resources, the second most important resource (after human resources) in an organization. In the case of intranets, these authorized accesses are given to the users of the organizational intranet. At the same time a comprehensive security system must deny access to all others. Web servers allow system administrators to limit access rights by specific IP addresses for individual pages. This capability would potentially allow system administrators to set access to financial records or personnel files only for the workstations of authorized staff. Security may include encryption at several levels. Web servers offer encryption for communications between the server and browser, effectively scrambling the message and preventing its interception. Encryption may also play a major role if the intranet application spans multiple organizations or locations. Firewalls can provide comprehensive security measures, protecting an intranet from unauthorized users outside of the organization who try to access the system. Many companies require employees to use personal identification numbers and passwords that limit access to their information.

E-mail confirmation sent automatically after any transaction can also guard against tampering. Firewalls are among the most effective security measures for intranets. Firewalls are a combination of hardware and software systems that protect one part of a network from another, or protect an internal network from the outside world. A firewall can determine who will cross a network boundary. The organization can further control security by restricting file and directory level access using standard user privileges. Hackers and other computer criminals are the most serious threat to intranet security. A hacker may break into a corporate intranet just for fun or for a challenge. A cracker, who is sometimes an expert retained by a competitor to wreak havoc on a company's intranet, is another outside threat. In addition to outside threats, there is an increasing trend toward security breaches initiated by current and former employees. It is estimated that insiders commit more than 70% of security threats. This makes the job of security protection a challenging one. Intranet applications can either assist in maintaining an employee's privacy, or they can have the potential to invade his or her privacy if the designer is not careful. Privacy can be enhanced by the use of intranet applications for delivering sensitive information in an anonymous manner.

For example, new raises or an overseas assignment can be delivered confidentially to the employee workstation. While the interoffice mail staff may pick through a document when they deliver a memo that is marked confidential, an intranet server treats all pages without similar bias or prejudgment. Employees can feel free to review the employee assistance program information at their desktops. They may browse information on maternity leave or sabbatical programs without fear of raising concerns of their supervisors or of personnel representatives. However, in a loosely secured network, all of this information and much more can get into the hands of unauthorized personnel. For these reasons, security issues and measures must be taken seriously.

► Tool Selection

Numerous basic intranet-publishing tools are available. Web servers, for instance, are available for a variety of platforms found in a typical organization, including Windows 3.1, Windows 95/98, Windows NT, Windows 2000, Macintosh, NetWare, VMS, UNIX, OS/2, and many others. An increasing number of tools enable the user to create HTML documents for intranet applications. Many software programs allow documents to be saved in HTML format, and tools are entering the market that allows large-scale migration of content from traditional word-processing format to HTML format. Database tools such as Microsoft Access and Borland Paradox are available for developing comprehensive data tables to be used as part of the intranet contents. These tools allow nontechnical users to continue to create content in their familiar application and to transfer this content to the server without having to manipulate each file or document.

Sophisticated users can also create HTML documents manually through any text editor. Organizations can also use Java to develop software applications that can run on any computer. Java is an object-oriented programming language similar to Visual BASIC or C and can deliver the software functionality for a specific task as a small applet downloaded from a network. An applet is a small program that can be sent along with a web page to a user. They are usually interactive and perform different tasks on a web page. As a recent programming concept, Object-Oriented Programming (OOP) is organized around 'objects' rather than 'actions.' It emphasizes the manipulation of objects rather than the logic that manipulates these objects. In an OOP environment, first all the objects are identified and then their relationships established. Java can run on any computer and operating system. It can run on a Personal Digital Assistant (PDA), a subnotebook, or a mainframe. The operating systems include Windows, UNIX, and Macintosh OS. To run Java applets, a computer needs a Java Virtual Machine (JVM). The JVM is a small program embedded in the web browsers that enables the computer to run Java applications. *For example*, a JVM is incorporated into Netscape's web browser software. Java programs are coded into byte code (computer source code) in applets or applications that are downloaded and run through the Java Virtual Machine. JavaScript scripts are a text source code in web pages that are interpreted by the browser as the page is used. The JVM runs the byte code and executes the Java applet instructions one-by-one and then performs the commands. Java capabilities allow the web server to pass information taken from HTML pages to programs that run outside of the server.

► Implementation

There are three main activities during the implementation phase of intranet development:

- i. **Build the infrastructure:** This includes the interconnection of nodes (devices attached to a network such as workstations and PCs) and installing the software and browsers.
- ii. **Choose and set up the network operating system (NOS):** This may include one of the popular operating systems, such as Windows NT, Windows 2000, Novell NetWare, IBM OS/2, Macintosh OS, and so forth.
- iii. **Overlay the intranet onto the NOS:** This involves installing TCP/IP and browsers such as Microsoft Internet Explorer or Netscape Navigator, and so forth. Intranets usually will run on a LAN in a client-server environment using the TCP/IP protocol.

► Post Implementation Audit and Intranet Site Marketing

Similar to other information systems projects, an intranet site has to be revised for improvement. Because the information needs of decision makers are constantly changing, and hardware and software technologies are improving, an intranet site could be constantly improved in order to better respond to the needs of key decision makers. New hardware and software technologies should improve the flexibility and ease of use of the intranet site, and they should always be integrated to the existing system.

An intranet has been introduced and the initial results are positive. This last phase can assist the organization by significantly enhancing the efficiency and effectiveness of this new decision-making vehicle. The goal of selling an intranet site or application is to encourage all employees to use the site as a central communications tool. The company should focus on educating its employees on how an intranet will help them do their jobs better. In other words, intranet site marketing should educate employees and show them how this new tool can make them more efficient and effective. There are four parts of a good marketing plan or a good post implementation audit program:

- i. **Involve top management:** Top executives and senior managers are among the most important groups of people who can make or break any information systems project, including the introduction of an intranet. These individuals can provide both encouragement and support regarding the success of the intranet program. If these people use e-mail, *for example*, everybody else will start using e-mail. CEO and Senior-Level Executives should be instructed on how to use the intranet site.

Four phase are involved in good marketing plan

- i. Involve top management
- ii. Create awareness
- iii. Provide ongoing education
- iv. Introduce new features by active user participation

The importance of the intranet must be explained to them. The benefits of using the intranet have to be focused on their needs.

Some of the specific benefits of an intranet for executives may include the following:

- a. An efficient and effective way to communicate.
- b. An effective way to control the operation of the organization at all levels.
- c. A good way to keep in touch with the organization's operations while traveling.
- d. A foundation for conducting B2B e-commerce.

However, the complexity and technical operations of the intranet should be deemphasized for the executives. The executives do not have to know how this technology works. They should be instructed how to navigate through the applications on the intranet, which may include sending their reports or organizational notices using e-mail.

ii. Enhance awareness: Employees have to be told that the site or application is available. Effective awareness campaigns should focus on the benefits of this new tool. Introducing the intranet as being similar to other technology applications may create resistance. The resistance can be expressed in a number of ways. Some employees may be skeptical; others will view the new tool as the latest toy; still others might complain that the new tool is one more thing added to their already overburdened workload. Ongoing education, encouraging active user participation, and including employees in the task force team should minimize these resistance issues. The existence of the site and its benefits should be advertised. Here are some methods for getting the word out:

- a. Announce important events through the site.
- b. Have the site featured in the company magazine and/or newsletter.
- c. Have the site's availability mentioned in staff meetings.
- d. Place a banner in the cafeteria and in other meeting places.
- e. Put a flyer in all employee mailboxes.
- f. Send an e-mail message to all employees.
- g. Set up meetings with division managers and supervisors.
- h. Conduct training programs to introduce the site's features.

iii. Provide ongoing education: The role of education and ongoing education in improving system acceptance is well documented throughout the information systems literature. The organization not only provides traditional education with an instructor, lectures, and slides, they also provide CD-ROM-based education. They provide private tutorial on a one-on-one basis for employees who need this kind of personal attention. They have been very successful in introducing all types of information systems applications to a broad group of users with minimal technical background. The intranet itself is a great training tool that the organization can use for future projects and applications. Generally speaking, education and training depends on company size and the location of employees. For a single-location company, a member of the information system staff can visit departmental meetings and present the site. Users should be grouped and taught how to use a browser and how to navigate through the company's web site. A brief document explaining the intranet site should be passed out to all employees. The document should highlight the type of information that can be obtained from

the site. Companies that have offices located throughout a large region should implement training through the intranet from its headquarters. Training should be short, simple, and to the point.

- iv. **Introduce new features by active user participation:** As the intranet grows, different departments will put their information on the company's web site. As mentioned earlier, there are readily available Web publishing programs that enable employees to create their own web pages without knowing HTML programming syntax. One such package is Microsoft Front-Page. Most organizations now have one or more Web masters who assist employees in publishing their own web pages. The organization should distribute formal policies and procedures for publishing and maintaining Web materials.

Guidelines such as the following may be helpful:

- a. Use the established company style guide.
- b. Create documents that are grammatically correct and are in Standard English.
- c. Develop materials that are appropriate for viewing by the entire organization.
- d. If access to the information is restricted, a user ID and password protection should be used.
- e. The information published must be legal and also should not be copy protected. In the case of copyrighted materials, the written permission of the copyright holder must be obtained.

17.1 Role of Intranet in B2B Application

B2B enterprises should have efficient internal marketing systems that enable them to service their strategic partners. An intranet is much more than an internal website. An effective intranet solution dramatically improves information sharing, collaboration and business process management throughout an organisation.

Number of Questions
1
suot

Apr.2013 – 15M

What is Internet? Explain role of Intranet in B2B applications?

Key areas where organizations need to focus:

- **Governance:** defining the project sponsor, determining the strategy.
- **Branding:** ensuring the intranet reinforces core brand values and identity.
- **Technology:** building the solution to integrate with existing infrastructure.
- **People:** engaging users as administrators and content contributors.
- **Content:** striking a balance between business and social information.

However, to ensure that intranet is successful, it must be planned carefully. A successful intranet or portal results from good planning and a strategic approach to implementing a solution that delivers real business benefits.

Defining the target audiences and identifying efficiency improvements, cost and time-savings and ways to enhance productivity that help the user perform day-to-day tasks will all contribute to the success of the system and will ensure user adoption. Even as the solution itself might hold a wealth of business information, i.e., from a simple contacts database, to campaign planning tools, sales materials or financial information, only the information useful to an individual's role is displayed.

Intranet in B2B has basically been built to deliver sales and to also help Sage get its new branding to its internal audience and its business partners. The system is a managed intranet that one host but is also effectively nine different releases of the system.

Intranet is a powerful tool to enable business to operate more efficiently, especially in the area of partner management. Moving marketing assets to an intranet and then giving partners access to these via an extranet can make good commercial sense. Cost still remains an issue for smaller organisations, but even if one is running a micro-business, a portal can help to punch well above the weight when it comes to marketing the goods or services.

One of the key issues that organisations need to consider is how the digital assets are actually going to be used. It's great having a static repository of images and collateral, but users often need more functionality. Implementing an intranet portal can offer business a huge advantage in that servicing customers and partners becomes much more streamlined.

The intranet is the product of an overall information management strategy. Information comes in many forms; structured such as images, movies, and documents, PDFs, etc. and unstructured, such as emails. The storage, management and control of this information is what sits behind truly successful intranets and extranets as they both form just two of the ways that a business chooses to make information accessible to different audiences.

Intranet is a very new way for organisations to communicate with customers and also a very new way for customers to communicate with their suppliers. It is sometimes very difficult to predict exactly what customers want, and even when one ask them they often say 'functionality', which (when delivered) is not really useful to them.

Using an intranet portal to support marketing activities makes commercial sense only if one approaches the construction and development of portal with care. If one clearly define how the intranet will operate, who will have access and who will maintain its systems, it will become a superb asset. Rolling out an intranet can help to manage the partners by giving them more access to the business. This closer relationship will result in long-term loyalty that the business can build upon.

Summary

1. Internet is a global network of computers that can be server or client that exchanges information.
2. Services and Tools
 - a. Electronic Mail
 - b. File Transfer Protocol (FTP)
 - c. Telnet
 - d. Internet Relay Chat (IRC)
 - e. Instant Messengers
 - f. The World Wide Web
 - g. Remote Accesses
 - h. Streaming Media
 - i. Voices and Video Conferencing
 - j. E-Commerce
3. Hardware and Software: a. Modem b. Computer
4. Advantages:
 - a. Communication
 - b. Information
 - c. Entertainment
 - d. Services e. E-Commerce
5. Disadvantages
 - a. Theft of Personal Information
 - b. Spamming
 - c. Virus threat
 - d. Pornography
6. Intranet is derived from two words, 'Intra' which means within and 'net' which means group of interconnected computers.
7. Software of Intranet
 - a. TCP
 - b. IP
 - c. Web Server
 - d. Web Browser
8. Advantages of Intranet
 - a. Workforce Productivity
 - b. Time
 - c. Communication
 - d. Web Publishing
 - e. Business Operations and Management
 - f. Cost-Effective
 - g. Promote Common Corporate Culture
 - h. Enhance Collaboration
 - i. Cross-Platform Capability
 - j. Low Maintenance
 - k. Scalability
 - k. Easy Software Distribution
9. Disadvantages of Intranet
 - a. Collaborative applications for Intranet are not as powerful as those offered by traditional groupware
 - b. Short-Term Risk
 - c. Less Back-End Integration
10. Features of Intranet
 - a. Shared Access to Documents
 - b. Controlled Access
 - c. Flexible Organization
 - d. Events Calendar, Scheduler
 - e. Message boards
 - f. Address Book
 - g. Intranet Search Engine
 - h. Task Management
 - i. Customizable Interface
 - j. Individualization
11. Elements or components of intranet information structure
 - a. The Network
 - b. File Sharing
 - c. Communication
 - d. Group Collaboration
 - e. Internet Access
 - f. Security
12. An extranet is a private network that uses Internet protocols, network connectivity, and possibly the public telecommunication system to securely share part of an organization's information or operations with suppliers, vendors, partners, customers or other businesses.
13. Development of Intranet
 - a. Establishing goals and problem definition
 - b. Cost and benefit analysis
 - c. Formation of the task force
 - d. Construction of a prototype
 - e. Assessing the security and privacy issues
 - f. Tool selection
 - h. Implementation
 - g. Post implementation audit and intranet site marketing



PU Questions

[Apr.2013 – 15M]

[Apr.2013 – 5M]

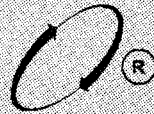
[Oct.2012 – 5M]

[Apr.2012 – 5M]

[Oct.2011 – 10M]

[Apr.2011 – 5M]

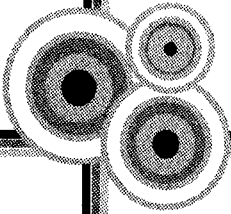
1. What is Internet? Explain role of Intranet in B2B applications?
2. Write a short note on: Extranet
3. Explain Internet Concept. Differentiate between Intranet and Extranet.
4. Write a short note on: Intranet
5. Define Internet. Differentiate between Intranet and Extranet.
6. Write short note on: Intranet Vs Extranet.



VISION

Chapter 4

ELECTRONIC PAYMENT SYSTEM



1 Introduction

Payment is an integral part of mercantile process and electronic payment system is an integral part of e-commerce. The emergence of e-commerce has created new financial needs that in many cases cannot be effectively fulfilled by traditional payment systems. For instance, new types of purchasing relationships-such as auction between individuals online-have resulted in the need for peer-to-peer payment methods that allows individuals to e-mail payments to the other individual. Virtually all interested parties are exploring various types of electronic payment system and issues surrounding electronic payment system and digital currency. Some of the electronic payment systems are simply electronic version of existing payment systems such as cheques and credit cards, while, others are based on the digital currency technology and have the potential for definitive impact on today's financial and monetary system. There has been a fundamental change in the financial sector because of the innovations in electronic payment system.

2. Requirements for Electronic Payment System

Electronic payment system is the alternative to the coin or paper based cash payment system to make it easy for the user to make payment for their purchased goods or services over the network or Internet and in absence of the physical (entity) presence. Initially, cheque in bank payment systems were used to serve the purpose of the same, but now in the era of Internet and E-commerce, paying securely over the Internet is an important task for the electronic payment system. Currently, credit cards are also in use for making payments over the network, but still users are in doubt about the security of their money because of an increase in frauds which ultimately causes loss of money, either of users, merchants or participating banks.

Present electronic payment system are too far from ideal payment system because of the higher transaction cost, more fraudulent activities, and involvement of multiple parties. The process lacks users, acceptance, proper application plans and incompatible standards/specifications. A good payment system should satisfy the user's acceptance as well as the merchants on a mass scale.

Present electronic payment system can be divided in two groups: electronic cash and credit/debit system or token based and account based system. Tokens or electronic cash are like the physical cash which represent the value and credit/debit or account based system does not carry value but a message to transfer value.

3. Characteristics of Electronic Payment System

Characteristics of electronic payment system are looked at from various points of view like technology, user, market and more.

Characteristics of Electronic payment system:

- i. Applicability
- ii. Easy-to-use
- iii. Security
- iv. Reliability
- v. Trust
- vi. Scalability

- i. **Applicability:** Acceptance of the user where he/she can use the method to buy goods or services.
- ii. **Easy-to-use:** The system should not complex, particularly in the Indian context, a user from a remote area should also be able to use the system.
- iii. **Security:** Security is concerned with enforceability of the value (money). Creation, modification and over spending of the value (money) should be protected. Integrity of the value as well as authorization for value should be spent by the concerned user only.

- iv. **Reliability:** Smooth running of the system.
- v. **Trust:** Degree of the confidence that the money and the personal information are safe.
- vi. **Scalability:** System should be scalable by timely changes in the underlying infrastructure.

4. Traditional Payment System

A traditional process of payment and settlement involves a buyer-to-seller transfer of cash or payment information. The actual settlement of payment takes place in the financial processing network. A cash payment requires a buyer's withdrawals from his/her bank account, a transfer of cash to the seller, and the seller's deposit of payment to his/her account. Non-cash payment mechanisms are settled by adjusting, i.e., crediting and debiting the appropriate accounts between banks based on payment information conveyed via cheque or credit cards. Cash moves from the buyers 'bank to sellers' bank through face-to-face exchange in the market. If a buyer uses a non-cash method of payment, then the payment information rather than cash flows from the buyer to the seller. Ultimately, payments are settled between the banks concerned, who adjust accounts based on payment information.

5. Process of Electronic Payment System

Electronic payment systems have been in operations since 1960s and have been expanding rapidly as well as growing in complexity. After the development of conventional payment system, EFT based payment system came into existence. It was first electronic based payment system, which does not depend on a central processing intermediary. An electronic fund transfer is a financial application of Electronic Data Interchange (EDI), which sends credit card numbers or electronic cheques via secured private networks between banks and major corporations. To use EFT to clear payments and settle accounts, an online payment service will need to add capabilities to process orders, accounts and receipts. The nature of digital currency or electronic money mirrors that of paper money as a means of payment. As such, digital currency payment systems have the same advantages as paper currency payment, namely anonymity and convenience. As in other electronic payment systems, here too security during the transaction and storage is a concern, although from a different perspective, for digital currency systems double spending, counterfeiting, and storage become critical issues whereas snooping and the issue of liability is important for the notational funds transfer. However, as a private monetary system, digital currency has wide ranging impact on money and monetary system with implications extending far beyond more transactional efficiency.

► Process

- i. **Marketing:** Marketing is not a new term, to sell anything companies have to market it. But to use the Internet, as a medium of marketing is new as the bandwidth is still limited so no commercials can be shown as on T.V. Internet marketing has a different approach. We market things on the net by showing small banner ads that any who surfs the net is familiar with. Also web sites like Amazon pay other websites if someone from their website comes to Amazon's website by clicking on a banner ad or a link. The whole business on the web is sticky. The term refers to the fact that the customer has to be sold a product and also the website should be so attractive that the customer keeps coming back to it for further buying. This is done by sending attractive offer mails and referrals.
- ii. **Customer/visitor:** Here, we have to make a distinction between the types of commerce websites. There actually exists three broad types of commerce websites:
 - a. *Business to Consumer (B2C):* These websites provide business to consumer. These are micro-payment based websites. They have to be attractive and should be able to show the products properly. As an example, you may visit www.fabmart.com and www.firstandsecond.com to see the feel of a Business to Consumer (B2C) site.
 - b. *Business to Business (B2B):* These are websites that provide business to the business, that is their function is similar to the stock exchanges, i.e., they are meeting points for a buyer and a seller. These do not focus on content but rather on service. Functions of such websites are online order processing, tender filling, tracking of orders, etc.
 - c. *Auction sites:* These are sites that let you auction or sell something online, it may be an old motorcycle or bed or books. To see this site, go to www.ebay.com.
- iii. **Website visit:** Once a user visits a website, the site begins tracking him/her, by presenting him/her with products based on his/her preference. Some means of doing this are cookies, registration forms, surveys, etc.
- iv. **Product browsing:** A user will typically browse through departments and then various products, he/she may be attracted to by showing blinking new offers and other discounts.
- v. **Shopping basket:** Shopping basket is a term taken straight from regular shopping, as in a store the user adds the items of need to a basket. The online store also implements a shopping basket, in which we can keep on adding items of our need.
- vi. **Checkout:** Once we have added all items we need the basket. The website lists all the items that we intend to purchase, we also have to fill in all the billing related information here. We enter the credit card numbers here. Other things such as gift wrapping, etc. are also specified here.
- vii. **Tax and shipping:** Once it has been decided where the product has to go and who is going to pay for it, we now decide on various taxes and shipping routes the product may take. These become very challenging, especially in international order as countries have different taxes and shipping rates.

- viii. **Payment:** This is the most important part of purchasing online. The user is presented with a list of all the items purchased, and a total of the payments he has to make. Then he has to decide on the mode of payment, whether by credit card or cash on delivery, etc.
- ix. **Receipt:** Once an order has been placed and confirmed, we may want to place a copy of the order with the user. This may be done either by snail mail or e-mail.
- x. **Process order:** At this stage the consumer leaves the picture, we now begin to check the credit card number and other data. This may be done online or offline, then the product is made and prepared for shipping to the customer.
- xi. **Fulfill order:** Once the order has been processed, it has to be fulfilled duly. Even though 90% of the transactions are online but the product has to reach the consumer physically and in good shape.
- xii. **Ship order:** Once we have processed the order fully it is ready to be sent to the consumer, it is then shipped to the consumer.

6. Types of Electronic Payment Systems

With the growing complexities in e-commerce transactions, different electronic payment systems have been invented. The grouping can be made on the basis of what information is being transferred online. There are six types of electronic payment systems:

- i. PC-Banking
- ii. Credit Cards
- iii. Electronic Cheques (i-cheques)
- iv. Micro Payment
- v. Smart Cards
- vi. E-Cash

It can be further classified into three types of electronic payment systems:

- i. Digital Token based electronic payment systems
- ii. Smart Card based electronic payment system
- iii. Credit based electronic payment systems

Electronic payment system can be broadly grouped into:

- i. Online Credit Card Payment System
- ii. Electronic Cheque System
- iii. Electronic Cash System
- iv. Smart Card based Electronic Payment System

Number of questions asked **3**

Oct.2012 – 15M

What are the different types of Electronic Payment System? Describe any three types.

Oct.2011 – 15M

What is EPS? Explain in detail various types of EPSs.

Apr.2011 – 15M

Enlist various types of electronic payment systems. Explain the process of electronic payment system with example.

6.1 Online Credit Card Payment System

It searches to extend the functionality of existing credit cards for use as online shopping payment tools. This payment system has been widely accepted by consumers and merchants throughout the world, and by far the most popular method of payment, especially in the retail markets. This form of payment system has several advantages, which were never available through the traditional modes of payment. Some of the most important are, privacy, integrity, compatibility, good transaction efficiency, acceptability, convenience, mobility, low financial risk and anonymity. Added to all these, to avoid the complexity associated with the digital cash or electronic-cheques, consumers and vendors are also looking at credit card payments on the Internet, as one of possible time-tested alternatives. But, this payment system has raised several problems before the consumers and merchants. Online credit card payment seeks to address several limitations of online credit card payments for merchants including lack of authentication, repudiation of charges and credit card frauds. It also seeks to address consumer fears about using credit card such as having to reveal credit information at multiple sites and repeatedly having to communicate sensitive information over the Internet. Basic process of online credit card payment system is very simple. If consumers want to purchase a product or service, they simply send their credit card details to the service provider concerned and the credit card organization will handle this payment like any other.

6.2 Electronic Cheque Payment System

Electronic cheques address the electronic needs of millions of businesses, which today exchange traditional paper cheques with the other vendors, consumers and government. The e-cheque method working is same as conventional paper cheque. An account holder will issue an electronic document that contains the name of the financial institution, the payer's account number, the name of payee and amount of cheque. Most of the information is in uncoded form. Like a paper cheques, e-cheques also bear the digital equivalent of signature, a computed number that authenticates the cheque from the owner of the account. Digital chequing payment system seeks to extend the functionality of existing chequing accounts for use as online shopping payment tools. Electronic cheque system has many advantages:

- i. They do not require consumers to reveal account information to other individuals when setting an auction.
- ii. They do not require consumers to continually send sensitive financial information over the web.
- iii. They are less expensive than credit cards.
- iv. They are much faster than paper based traditional cheque. But, this system of payment also has several disadvantages.

The disadvantage of electronic cheque system includes their relatively high fixed costs, their limited use only in virtual world and the fact that they can protect the user's anonymity. Therefore, it is not very suitable for retail transactions by consumers, although useful for the government and Business to Business (B2B) operations, because the latter transactions do not require anonymity, and the amount of transactions is generally large enough to cover fixed processing cost. The process of electronic cheque system can be described using the following steps.

- Step 1:** A purchaser fills a purchase order form, attaches a payment advice, signs it with his private key, attaches his public key certificate, encrypts it using his private key and sends it to the vendor.
- Step 2:** The vendor decrypts the information using his private key, checks the purchaser's certificates, signature and cheque, attaches his deposit slip, and endorses the deposit attaching his public key certificates. This is encrypted and sent to his bank.
- Step 3:** The vendor's bank checks the signatures and certificates and sends the cheque for clearance. The banks and clearing houses normally have a private secure data network.
- Step 4:** When the cheque is cleared, the amount is credited to the vendors account and a credit advice is sent to him.
- Step 5:** The purchaser gets a consolidated debit advice periodically. E-cheque provides a security rich Internet payment option for businesses and offers an easy entry into electronic commerce without a significant investment in new technologies or legal systems.

6.3 Electronic Cash Payment System

Electronic cash combines computerized convenience with security and privacy, which is an improvement on paper cash. Its versatility opens up a host of new markets and applications. E-cash is an electronic or digital form of value storage and value exchange that have limited convertibility into other forms of value and require intermediaries to convert. E-cash presents some characteristics like monetary value, storability and irretrievability, interoperability and security. All these characteristics make it a more attractive payment system over the Internet. Added to these, this payment system offers numerous advantages like authority, privacy, good acceptability, low transactions cost, convenience and good anonymity. But, this system of payment also has many limitations like poor mobility, poor transaction efficiency and high financial risk, as people are solely responsible for lost or stolen cash.

E-cash structure: E-cash structure could be identified as a string of bits that represents certain values such as reference number and digital signature, which could be used for the security purpose to prevent forgery and criminal use. It adds a digital watermark to e-cash structure to protect it from illegal copy and forgery activities further, the model modified the structure of the reference number to support tractability. Still there are certain concerns to be addressed for an electronic cash system.

For example, who has the right to issue electronic cash? Can every bank issue its own money? If so, how do you prevent fraud? And who will monitor the banking operations to protect consumers? Many of these concepts relate to the legal and banking regulatory aspects. However, all these issues are beyond the scope of the study and therefore, cannot be included here. But, these issues must be addressed before establishing a complete e-cash based payment system.

6.4 Smart Card based Electronic Payment System

Smart cards are credit card sized plastic cards with the memory chips and in some cases, with microprocessors embedded in them so as to serve as storage devices for much greater information than credit cards and with inbuilt transaction processing capability.

This card also contains some kinds of an encrypted key that is compared to a secret key contained in the user's processor. Some smart cards have provision to allow users to enter a Personal Identification Number (PIN) code. Owing to their considerable flexibility, they have been used for a wide range of functions like highway toll payment, as prepaid telephone cards and as stored value debit cards. However, with the recent emergence of e-commerce, these devices are increasingly being viewed as a particularly appropriate method to execute online payment system with considerably greater level of security than credit cards.

6.5 Payment Types

► Cash (Bills and Change)

There are a variety of ways to pay for purchases, and cash is one of the most common and familiar. Both paper money (of varying denominations) and coins are included under the larger category of 'cash'. While cash has the advantage of being immediate, it is not the most secure form of payment. If it is lost or destroyed, that money is essentially gone. There is no recourse to recoup those losses. If one has a torn bill and are unsure whether it is still usable, check with the nearest bank. Cash is used exclusively at physical retailers, shops. There is no way to use cash for online purchases.

► Debit Card

A debit card is an increasingly popular way to pay, for both online and retailer purchases. It looks exactly like a credit card, but it functions in a different manner. Unlike a credit card, paying with a debit card takes the money directly out of your account. In this way, it is almost exactly like writing a personal cheque, but without all the hassle of filling a cheque.

► **Credit Card**

A credit card is one of the most popular ways to make purchases which are more expensive than everyday purchases, although they can be used on purchases of any amount. Credit cards look exactly like debit cards, and using them is sometimes referred to as paying with 'plastic'. Rather than paying for the item right away, paying with a credit card temporarily defers bill. At the end of each month, one will receive a credit card statement with an itemized list of all the purchases. Therefore, rather than paying the retailer directly, one will pay off bill to the credit card company. If one doesn't pay the entire balance of the bill, the company is authorized to charge interest on remaining balance. Credit cards can be used for both online purchases and at retailer's outlets.

► **Gift Certificate**

A gift certificate is a less common form of payment, but they are increasingly becoming a popular gift. Thus, they are increasingly becoming a popular form of payment. Gift certificates come in several forms, but they are essentially prepaid certificates with a certain amount of money added to that certificate. They can be purchased from one particular store, several stores, or any participating store. They come in plastic card form, paper form, or electronic form. Depending on the type of gift certificate, they can be redeemed at physical retailers, online retailers, or both.

► **Money Order**

A money order is not currently one of the most common forms of payment, but there has been an increase in its use. They are a lot like a personal cheque but without the possibility of 'bouncing'. A cheque bounces when somebody writes a cheque without having any money in his/her account to cover the expense. When the recipient tries to cash the check, it 'bounces'. The recipient cannot get the money if this happens. It is one of the largest liabilities about personal cheque, and money orders nullify some of that liability. A money order is purchased with cash up front, so there is no worry about it bouncing. It is, however, more secure to send through the mail than cash. They are easily redeemed for cash at any post office.

► **Web Certificate**

A web certificate is a relatively new form of payment. Basically, it can be understood as a gift certificate redeemable at just about any retailer, online or otherwise. It is like cash in its versatility, but it is more secure to send and spend. A web certificate will basically function like any debit card, in that it has a unique number to identify the card, and it can be used for both online purchases and purchases from physical retailers. Web certificates can be used anywhere Mastercard or other major credit cards are accepted. Web certificates can either be given as gifts or you can load money on a card for yourself to eliminate the hassle of using cash or cheques.

► **Personal Cheque**

The personal cheque is a form of payment that is dwindling in popularity with the advent of debit cards and online money accounts. However, it is still one of the major ways to pay for purchases at retailers' outlets. Personal cheques are ordered along with your account. They are essentially paper forms one fills out and gives to the physical retailer. The retailer turns in the cheque to their bank, the bank processes the transaction, and a few days later the money is deducted from the account. However, as stated, with the increasing trend towards fast payment, cheques are seen as timely and somewhat outdated. They cannot be used to make online purchases.

► **Foreign Currency**

Foreign currency is exactly like any other form of cash. However, if one is trying to make purchases outside of the country, there are a few things to keep in mind. The exchange rates will be different between countries. The exchange rates change constantly. Before one makes purchases at physical retailers' outlets currency will have to be converted into the currency of the country one is visiting. Cash can be converted at the local bank.

7. E-Payment Tools

Online financial service is a part of E-commerce, which has already been provided all over the world. Online financial service includes online purchase, home banking, personal financing, online investment and online insurance. These financial services are characterized by timely electronic payment and settlement through online payment tools. In its broad sense, online payment is a kind of money exchange occurring on line. The online payment is developed on the basis of paying means, such as credit card, E-cheque, digital cash and intelligent card, which may be extensively accepted by customers, businessmen and banks. Since the payment is carried out online, the payment information is subject to hacker attack, so the security of payment tools has to be guaranteed. E-payment is a vital part of E-commerce. The advantage of E-commerce, compared with that of traditional commerce is becoming the driving force that stimulates more and more vendors and people to make online purchase and other consumptions. But how to securely perform transactions online are the top priority people have to consider when they decide an online transaction.

7.1 Intelligent Card

The structure of an intelligent card primarily includes three parts:

- i. The program generator that establishes the intelligent card. In the process of developing intelligent card, the program generator is used primarily to initialize the card and create all the personal data.
- ii. The agent to process the operating system of intelligent card, which includes the accessories to the interface between intelligent card OS and its applications. This agent is highly transplantable, which enables it to be integrated on chip card reader or PC and C/S systems.
- iii. The agent of application interface of intelligent card. The agent is the interface between application and intelligent card. It provides help for management of different intelligent cards and independent interface for applications.

The intelligent card, into which the embedded microchip is installed, can store and process data. The value contained in the card is protected by Personal Identity Number (PIN), so only the user can have access to it. Multifunctional intelligent card with high-performance CPU embedded and independent OS installed can have its functions configured as a PC. This intelligent card also has 'self explosion' function, if intruder wants to open the card to access the information illegally, the content of the card will disappear. The working process of intelligent card is firstly, start the browser on a machine such as PC or a terminal telephone, secondly, use the IC card to login onto the website of the user's bank through the card reader installed on a PC, and IC card will automatically inform the bank the user's account number, and the password along with all the encrypted information. Then user can transfer fund from the IC card to the vendor's account, or transfer fund from his bank account to the card. In e-commerce transaction, the application of IC card is similar to the actual transaction process. The only difference is that after the user chooses the commodity on the computer, he would enter the password and the account number of the online store to complete the transaction process.

IC card generally stores the following kinds of information:

- i. The user's identity
- ii. Absolute location of the user
- iii. Relative location of the user and his geographical location in relation to other apparatus
- iv. Particular environmental parameters, such as light, noise, heat and humidity
- v. User's physiological status and other biological statistical information
- vi. Specialized timing parameter, such as the frequency of a certain event or the time that it takes for the user to complete a certain action
- vii. Specialized movement parameters, such as velocity, acceleration, physical stance and tracking information
- viii. Information of currency that the user holds

The application range of IC card covers:

- i. E-payment, such as paying a telephone bill, substituting of credit card.
- ii. Digital identification, such as control over access to the chambers or a system, like computers or Point of Sale (POS).
- iii. Digital storage, as is applied to realize real-time storing and retrieving of data, like case history, tracking information or authentication information.

For users, IC card provides a convenient method. It eliminates disadvantages that application systems may cause to the users, and it can 'memorize' some information for the user and provide the information on behalf of the user. The application itself can also be configured according to the need of a certain user, who should not be asked to learn and adapt to the application. Using IC card means that one does not need to remember PIN or password, for instance, to make a call, withdraw money, or make payments. It is of a great advantage. IC card reduces the probability of cash payment and being defrauded, and offers excellent secrecy as a result. Users do not need to carry a lot of cash with them to accomplish all that can be dealt with a credit card, and it enables higher confidentiality than credit cards do. Therefore, it plays the most significant role in the online payment system.

IC card as an online payment tool has the following standards:

- i. Open card framework standard. This is a standard based on network computer supported by different software companies.
- ii. Java Card API standard.

7.2 E-cheque

E-cheque is a form of e-payment that transfers money from one account to another through the network connecting users and banks. Most e-cheques use public key or PIN instead of hand-written signature. The transaction cost of e-cheque is low, and banks could provide standardized capital information for vendors that take part in e-commerce, thus it is one of the most efficient payment means. Using e-cheque to pay, clients can send the e-cheque to the vendor's e-mail box.

At the same time the e-payment notification will be sent to the bank, which then transfers the money to the vendor's account. This process takes only a few seconds.

Still, a there is problem of how to authenticate the e-cheque and the user? So there should be a specialized authority to make authentication. Meanwhile, this institution should authenticate the identity and credit of the vendors like CA.

E-cheque transaction can be divided into the following steps:

- i. Client and vendor agree to use e-cheque payment.
- ii. Client sends the e-cheque to the vendor and a payment notification to the bank.

- iii. The vendor has the e-cheque authenticated through the CA, and then encashes the cheque after that.
- iv. The bank verifies the cheque through the CA, and then makes fund transfer or encash the cheque after verification.

Although e-cheque could greatly reduce the cost of processing, people still take prudent alternatives to online cheques. The extension of e-cheque still has a long way to go.

7.3 E-wallet

E-wallet is a commonly used payment tool in e-commerce. It is a new type of wallet to pay small purchases. The Mondex e-wallet developed by the National-Westminster Bank was the first e-wallet system in the world, and first introduced in Swindon, the 'British Silicon Valley' in July, 1995. Initially, it was not well-known until it made a breakthrough in Swindon, and it was widely used in supermarkets, bars, jewellery stores, pet stores, restaurants, parking lots, food stores, telephone booths and buses. The use of e-wallet is quite simple, and all that one need to do is to insert the Mondex card into the terminal. When a transaction is completed, the card reader will deduct the expense of this transaction from the Mondex card. In addition, Mondex card has most of the properties of ready money, such as a measure of commodity, saving, exchange and payment. The money on one card can be transferred to another card through a special terminal. Moreover, once the money in the card is depleted, or the card is stolen or lost, the value of Mondex card cannot be recovered, namely, the cardholder has to be responsible for the card. Some cards can be used by others who happen to access them, while others written with password are only used by the cardholder, and it is safer than cash. When Mondex card is damaged, the cardholder can declare to the issuer, and he/she will be given a replacement card by the issuer after verification. Terminal payment of Mondex card is only the early application of e-wallet, which looks very similar to the intelligent card. E-wallet has taken no physical form and turned into a real virtual wallet. Online purchase using E-wallet needs to take place in the e-wallet service system. In e-commerce, the software is generally free of charge. The user can use the e-wallet software from the system server connected with his bank account, or other software on the Internet through an encrypted means. Two primary e-wallet service systems in the world are Visa Cash and Mondex, other systems include MasterCard Cash.

The clients of E-wallet usually have to open accounts at banks. When using E-wallet, the client has to install the software connecting to the server of E-commerce, and input the data of various E-money and E-card to the service system. If the client needs to pay by credit card such as Visa Card or Mondex Card when the transaction is being processed, all that he has to do is to click the corresponding item or icon. This method is called click-payment. Only E-currency can be stored in E-wallet, namely E-cash, E-change, electronic credit card, online currency, and digital currency. All these E-payment tools support click-payment. The management module set up in E-commerce

service system for E-money and E-wallet is called E-wallet administration. Clients could use it to change password or check the bank account. The service system also contains transaction recorder, through which the clients could know the commodities and the amount they have bought. They can also print the query result.

Online purchase using e-wallet usually includes the following steps:

- i. The client uses a browser to search the commodities on the vendor's website, and chooses the ones that he would like to buy.
- ii. The client fills out order forms, including item list, prices, total price, freight charge and tax.
- iii. Order forms can be transmitted electronically, or created by the client's software. Some online shops allow the clients to bargain with vendors.
- iv. After confirmation, the client chooses to pay by e-wallet. One can install the e-wallet to the system, click the corresponding item or icon of the wallet, and then the wallet is open. In that case, he has to enter his password and confirm the wallet before he can pay by a credit card chosen from the wallet.
- v. The server of e-commerce will encrypt the credit card number and send it to the corresponding bank, meanwhile the store will receive the encrypted order, and then the store adds the order and returns it to the server. The credit card number is invisible to the store, and the store has no access to the money in it. After the server verifies the validity of the client, it will send the verification to the credit card company and the commercial bank. There will be data exchange about payment and financial data between the credit card company and the bank. The credit card company will process the request and resend it to the bank for confirmation with authorization made meanwhile; the bank will confirm and authorize it before sending it back to the credit card company.
- vi. If the bank denies the request, it means that the client's card is underfunded or overdraft. After the denial, the client can re-open the e-wallet to access another credit card and repeat the above mentioned operations.
- vii. If the bank has verified the credit card and given authorization, the store can then make delivery. Meanwhile, the store will keep all the data generated in the whole transaction, and send a copy of them to the client.
- viii. After the transaction is complete, the store will deliver the commodity to the client according to the order form that the client previously provided.

Although there are several processes of identity verification, bank authorization, and financial data exchange involved in this process, all these are completed in a very short time. Actually, it only takes 5 to 20 seconds from filling the order form to receiving the electronic receipt. This kind of purchase is simple and fast.

Moreover, the whole process is secure. During the process, the client can use any browser to browse and check the information. Since the information in the client's credit card is invisible, it is secure and reliable when the transaction is processed. In addition, it is guaranteed that the client will not be defrauded by the store because of the secure means of e-commerce.

In short, this purchase procedure has completely changed the traditional face-to-face purchase pattern, and it is a highly efficient and secure process that is quite different from the traditional way.

E-wallet is much better than other types of e-currency that emerged in the past several years.

Salient features of e-wallet are:

- i. More than 40 years of data retention.
- ii. Firewall encrypted security logic.
- iii. Compatible with many supporting hardware.
- iv. No separate card reader is required to access our card.
- v. Polarity reversal indicator is pre-built in our card.
- vi. Reusability of our card is unlimited.
- vii. Multiple card features are incorporated in the same card.
- viii. The random word generator unit generates a random word which replaces the password (correct password) in the buffers and other terminals with a random word after the transaction is over. Hence, it is almost impossible to replicate the behaviour of the ASIC and, thereby, obtain the encryption key or algorithm used.
- ix. *Chip security power management:* This unit protects the card (ASIC) against over voltage or under voltage and over frequency or under frequency of the clock signals given for operation.
- x. *Access control:* Access control unit protects the on-chip memory. It provides address and data bus scrambling and detects any non-standard attempt to acquire memory access.
- xi. *Flash ROM/ROM:* Flash ROM stores the instruction set for the microcontroller unit, the necessary monitor routine programs and the application code. Here the flash ROM is used because there are 32 available instructions sets for different applications. But only one instruction set is used. If another instruction set is used the card can be used for only the specific application.
- xii. *EEPROM:* EEPROM is used to store the processed data, i.e., the balance amount in the card. This part is of commercial importance as it holds the monetary information of the card. Also the EEPROM sends the data to be read for establishing transaction.
- xiii. *RAM:* It provides the workspace for both the microcontroller unit and the crypto co-processor. It's where the actual comparison of the stored password (original password) and the given password for transaction to takes place. Only if the given password is the actual password, the access is given to view the details of the card, deposition and withdrawal are allowed.
- xiv. *Serial interface:* It has six valid pins-CS-chip select, CLK-external clock, DI-data input, DO-data input, VOC-voltage input GND-ground. Actually, a parallel printer port is used for interface of the card with PC. But only the six required pins of the printer ports are activated. Thus the advantages of parallel and serial communication are utilized. There is no need for a separate USB.
- xv. *RF interface:* This unit provides establishment of transaction using Blue tooth technology, which is our future enhancement. External complexities are less.

- xvi. *Internal 16 bit address/data bus:* This provides communication between different units inside ASIC chip. This ASIC chip is built satisfying ISO 7816 standards.

► Operation

- i. Once the card is given the power supply all the units are activated.
- ii. The password is sought and the password is sent. The first bit is chip select then the start bit, two opcode bits, 6-address bits and 16 data bits. The dedicated embedded microcontroller looks after this process.
- iii. Then the given password is sent to the RAM work space.
- iv. The password (original password) after decryption by the crypto processor is sent to the RAM.
- v. Here the passwords are compared by the microcontroller. Only if the both the passwords are correct, the access control unit brings the flash ROM, EEPROM units of low impedance state.
- vi. Otherwise the units are kept in high impedance state.
- vii. The on-chip security power management unit provides the correct voltage and correct frequency (CLK signal) for functioning of the ASIC.
- viii. If the password is correct, then the microcontroller fetches the instructions from the instruction set in the FLASH ROM.
- ix. The balance amount can be fetched from the EEPROM, through the D0 pin of the serial interface.
- x. After the transaction is over, the balance amount is stored in the EEPROM through D1 pin of the serial interface.
- xi. Once the transaction is over, the random word generator generates a random word and sends it to the terminal ends and other buffers where the original password is present. This protects the original password from being hacked. Thus, the ASIC is designed for effective transaction with proper security to the customers.

► Features of E-wallet

- i.. Refillable
- ii. Infinite lifetime
- iii. Current balance can be stored and read
- iv. User authentication is provided
- v. Universal access
- vi. Maximum possible cash
- vii. Cannot be duplicated

Advantages of E-wallet

Ease of use

- i. Withdraw or deposit value by telephone
- ii. Pay the exact amount, no fiddling for change
- iii. No signature required
- iv. Immediate payment
- v. In the future, access points may include mobile phones

Accessibility and Convenience

- i. Cash machines and telephones give more access points to funds in bank account.
- ii. Available 24 hours/365 days.
- iii. Cash machines and telephones cannot run out of electronic cash.

Flexibility

- i. Transfer value by telephone.
- ii. Pay person-to-person.
- iii. For low or high values.
- iv. Multi-currency capability.
- v. No age limit, so suitable for all in the family.

Safety and Control

- i. Spend only what one has.
- ii. Read balance.
- iii. Load value at home.
- iv. Keep track of what one has spent and where.
- v. Customer is traceable if a lost card is found.

7.4 E-cash

E-cheque, e-draft, e-wallet and credit card offers great convenience of online payments during e-commerce, but all these cannot take the place of cash, for they all have the audit trailing function. Using these payment tools will reveal where the money goes. So there may be possibility of leaking privacy. Sometimes the client hopes to pay online, just like paying cash in real life in order to avoid trailing and privacy leakage. So e-cash comes into being.

E-cash is a kind of currency that exists in the form of digits. It transforms the cash amount to a series of encrypted numbers, representing the currency value by the serial numbers. After the client opens

2
No. of questions asked

Apr. 13, 12 – 5M

Write short note on:
E-cash.

an account and deposits money in the bank that provides e-cash service, he will be able to go shopping in stores that accept e-cash. When the client dials into online bank using a password and PIN to identify himself, and downloads packages of small-valued e-coins, e-cash comes into effect. Then, these e-cash are stored in the client's hardware until he uses them to do online shopping. In order to guarantee the transaction security, each coin is assigned a random serial number and this number is hidden in an encrypted envelope. In this way, nobody will know who withdraws or uses the e-cash. Such a shopping mode can conceal the buyer's identity, so it is popular with people who have privacy concerns.

The payment process using e-cash includes four steps:

- Step 1:** The client opens an account in the bank that issues e-cash, and buys e-cash certificates with the money deposited in the cash server account. Then the e-cash gets value, and is divided into packages of 'coins', which can be circulated in the commercial world.
- Step 2:** The client withdraws a certain amount of e-cash, usually less than 100 from the bank with the terminal software and stores it on the hard disk.
- Step 3:** The client bargains with the vendor that accepts e-cash, fills the order form and uses e-cash to pay for the commodities purchased.
- Step 4:** The vendor and the bank make settlement, and the bank will pay the money to the vendor.

E-cash has the following features:

- i. The banks and vendors should have authorization agreements.
- ii. The client, vendor and bank, all have to use the e-cash software.
- iii. The bank takes charge of the fund transfer between client and vendor.
- iv. Identity verification is completed by e-cash itself. Digital signature is used when the bank issues e-cash. The vendor sends e-cash to the bank in each transaction, and the bank verifies the validity of e-cash issued by the bank.
- v. Anonymousness.
- vi. It has the features of cash, subject to operations like withdrawing, depositing, transfer, and therefore it is suitable for small transactions.

However, e-cash payment also has some problems: a number of vendors are willing to accept E-cash, but only a few of the banks provide e-cash service; high cost, high requirements for both hardware and software, a large database is needed to store the completed transactions and E-cash serial numbers to avoid repeated payment, currency exchange problems, etc. Since E-coin is still based on traditional currency system. International trades have to use specific exchange software, which means a big risk. If the hard disk of the client is damaged, then E-cash stored on it is lost and cannot be recovered, which is a risk many consumers are not willing to bear. Another bigger concern is the existence of counterfeited e-cash. With some technologies, it is possible that the receiver of E-cash, even the issuer, will not be able to test the counterfeited E-cash. Although complicated security means lowest probability of counterfeited E-cash, the probability cannot be ignored for it

may bring rather high rewards. Once counterfeited E-cash is successful, the price that issuers and some of the clients have to pay will be disastrous. Despite various problems, the use of E-cash is still on the rise.

► **Electronic Cash Issues**

- i. E-cash must allow spending only once
- ii. Must be anonymous, just like regular currency
 - a. Safeguards must be in place to prevent counterfeiting
 - b. Must be independent and freely transferable regardless of nationality or storage mechanism
- iii. Divisibility and convenience
- iv. Complex transaction (checking with Bank)
 - Atomicity problem

► **Security**

Security is of extreme importance when dealing with monetary transactions. Faith in the security of the medium of exchange, whether paper or digital, is essential for the economy to function.

There are several aspects to security when dealing with E-cash. The first issue is the security of the transaction. How does one know that the E-cash is valid? Encryption and special serial numbers are supposed to allow the issuing bank to verify (quickly) the authenticity of E-cash. These methods are susceptible to hackers, just as paper currency can be counterfeited. However, promoters of E-cash point out that the encryption methods used for electronic money are the same as those used to protect nuclear weapon systems. The encryption security has to also extend to the smartcard chips to ensure that they are tamper resistant. While it is feasible that a system wide breach could occur, it is highly unlikely. Just as the Federal Government keeps a step ahead of the counterfeiters, cryptography stays a step ahead of hackers.

Physical security of the e-cash is also a concern. If a hard drive crashes, or a smartcard is lost, the e-cash is lost. It is just as if one lost a paper currency filled wallet. The industry is still developing rules/mechanisms for dealing with such losses, but for the most part, e-cash is being treated as paper cash in terms of physical security. Companies are making some exceptions when it comes to a software/hardware failure, but these are supposed to be rare. To help customers get used to this concept, most companies are limiting e-cash wallets to \$500, reflecting the primary use of e-cash for low value transactions. There is a benefit to e-cash in the area of theft, however. A mugger or pickpocket would not be able to make use of another's smartcard without the appropriate password. Merchants should also lose less cash to employee theft, since the electronic cash will be inaccessible (or, at a minimum, traceable).

The ultimate area of security is faith in the currency. This, however, would still be the responsibility of the Federal Government on a systematic basis.

Essentially, the e-cash is merely a representation of hard currency in deposit at banks. Thus, faith in the system should not falter.

► **E-Cash Privacy**

Transactions involving paper currency are difficult to trace. If digital money is to replace paper currency, it must retain certain aspects of this quality.

As information technologies expand, privacy becomes an issue of greater concern. People are realizing that with every credit card transaction, corporate databases are becoming larger and larger. By using paper currency, people are able to exclude themselves from these databases. Therefore, for e-cash to be effective, it must maintain this privacy function.

DigiCash claims it has developed a system that provides privacy for the user without sacrificing on security of the receiver. If a system is completely private, the merchant has no way of verifying the validity of the electronic money. The user would also be unable to have a receipt for the transaction. However, DigiCash utilizes a one-sided signature. Basically, the user keeps record of payments made, but the merchant only receives enough information to allow his bank to verify the authenticity of the e-cash.

This signature process is also supposed to deter the criminal element of cash transactions. Since a record of the transaction is created and kept (by the payee), extortion, bribes, or other illegal transactions should occur less frequently.

► **E-Cash Regulation**

A new medium of exchange presents new challenges to existing laws. Largely, the laws and systems used to regulate paper currency are insufficient to govern digital money.

The legal challenges of e-cash entail concerns over taxes and currency issuers. In addition, consumer liability from bank cards will also have to be addressed (currently \$50 for credit cards). E-cash removes the intermediary from currency transactions, but this also removes much of the regulation of the currency in the current system.

The more daunting legal problem is controlling a potential explosion of private currencies. Large institutions that are handling many transactions may issue electronic money in their own currency. The currency would not be backed by the full faith of the United States, but by the full faith of the institution. This is not a problem with paper currency, but until the legal system catches up with the digital world, it may present a problem with cyber cash.

► **Advantages of E-Money**

i. **Online Electronic Money**

- a. *Anonymity and un-traceability can be maintained:* User Id's are kept highly confidential.

- b. *No issues regarding 'Double spending'*: Real-time checking of all transactions makes the possibility of multiple expenditures negligible.
- c. *No requirement of additional secure hardware*: Existing Point of Sale (POS) hardware can be updated and used.

ii. Offline Electronic Money

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

► Disadvantages of E-Money

i. Online electronic money

- a. *Communication overheads*: Security and anonymity cost become a bottleneck of the system. This can happen at times during real-time verifications.
- b. *Massive databases*: The bank will have to maintain a detailed and confidential database.
- c. *Synchronization*: The bank needs to synchronize its server every time transaction is made. It would be almost impractical to maintain.

ii. Offline electronic money

- a. *Prevention may not be immediate*: Double spending may not be prevented effectively and immediately.
- b. *Implementation expenditure*: The required additional hardware is quite costly to install.

8. Electronic Funds Transfer

Electronic Funds Transfer (EFT) is one of the oldest EPSs and is used for transferring money from one bank account directly to another without any paper money changing hands. EFT is the foundation of the cashless and chequeless society where cheque, stamps, envelopes, and paper bills are eliminated.

The most popular application of EFT is the direct deposit option used by millions of workers in the United States. Instead of receiving a pay cheque and depositing it into an account, the money is deposited to an account electronically.

Number of questions asked
1

Apr.2012 – 15M

Explain concept of Electronic Fund Transfer. Brief about different types of Electronic Payment System.

Customers, companies, and government agencies use EFT for all kinds of applications. EFT is considered to be a safe, reliable, and a convenient way to conduct business. Direct deposit is used for payroll, travel, and expense reimbursements, annuities and pensions, dividends, and government payments such as Social Security and veteran's benefits. Other types of EFT are frequently used for bill payments, retail purchases, Internet purchases, corporate payments, and treasury management, and for the disbursement of food stamps and other government cash assistance.

In broad terms, EFT refers to any transfer of funds initiated through an electronic terminal, including credit card, ATM, Fedwire, and Point-of-Sale (POS) transactions. It is used for both credit transfers, such as payroll payments, and for debit transfers, such as mortgage payments. Many utility companies and sports clubs also use EFT. The advantages of EFT include the following:

- i. Reduced administrative costs
- ii. Increased efficiency
 - Simplified book keeping
- iii. Enhanced security

At present, acceptance of this system has not been widespread. (Please note that acceptability of payment methods varies between countries.) Banks process EFT transactions through the Automated Clearing House (ACH) network. For electronic payments, funds are transferred electronically from one bank account to the billing company's bank, usually within 24 hours of the scheduled payment date.

Another common application of EFT is for money transfer among banks and other financial institutions. When a customer pays for goods and services by cheques, the merchant collects these cheques (assuming the cheques are accepted) and sends them to its bank. The bank credits the merchant account and then sends these cheques to the clearing department. The clearing department separates the cheques by banks and transfers them to a clearing house. At this point, banks transfer cheques among themselves. The customer's bank eventually receives the cheque and debits the customer account. In some cases these cheques are sent back to the customer, which marks the end of the process. If there are not sufficient funds in the customer's account, then the cheque is sent back to the merchant bank. The merchant must pay for the fee involved in the non-sufficient funds process and has to settle this with the customer or write it off as a bad cheque. The U.S. government monitors EFT compliance through Regulation E of the Federal Reserve Board, which implements the Electronic Funds Transfer Act (EFTA). Regulation E governs financial transactions with EPSs, specifically with regard to disclosure of information, consumer liability, error resolution, record retention, and receipts at electronic terminals.

9. Payment Cards

Payment cards are the most popular instrument for electronic payment transactions and they include the following:

Payments of cards are done in the following way:

- i. Credit Cards
- ii. Debit Cards
- iii. Charge cards
- iv. Smart cards

► Credit Cards

There are two types of credit cards in the market today:

- i. Those issued by credit card companies (*for example*, MasterCard and Visa) and major banks (*for example*, Wells Fargo and Bank of America).
- ii. Those issued by departmental stores (*for example*, May Company), and oil companies (*for example*, Chevron).

Because businesses benefit tremendously from these company cards and they are cheaper to operate, they are widely issued to and used by a broad range of customers. Businesses offer incentives to entice customers to open an account and receive one of these cards.

Credit cards are issued based on the customer's credit history, income level, and total wealth. The credit limit ranges from a few thousand rupees to several lakhs of rupees. The customer uses these cards to purchase goods and services or obtain cash from the participating financial institutions. The customer is supposed to pay his or her debts during the payment period; otherwise interest will accrue.

Two limitations of credit cards are their unsuitability for very small or very large payments. It is not cost-justified to use a credit card for small payments. Also, due to security issues, these cards have a limit and cannot be used for excessively large transactions.

► Debit Cards

Debit cards function similar to cheques, in that the charges will be deducted from the customer's chequeing account. The real advantage for the merchant is the speed at which the merchant collects these charges. The advantage for the customer is the ease of use and convenience. They also keep the customer under his or her budget because they do not allow the customer to go beyond his or her means.

► Charge Cards

Charge cards are similar to credit cards except they have no revolving credit line, so the balance must be paid off every month. Credit, debit, and charge card methods of payments have been successfully utilized in the pre-Internet era, and they are often used in the e-commerce world as well. Some of the reasons for their popularity in the e-commerce world are their availability (most customers own one of these cards), ease of use, and acceptance by most customers.

To use these cards as an online payment system, a well-defined process is followed:

- i. A customer using his or her browser clicks on a product on the merchant's website and adds it to an electronic shopping cart.
- ii. The customer provides the shipping instructions and credit card information.
- iii. The detailed payment information is displayed for the customer to review. A transmission technology known as Secure Sockets Layer (SSL) protects the payment and shipping information while it is in transit.
- iv. This encrypted information is transmitted to the merchant's commerce site.
- v. The server software adds the merchant identification to the information transmitted.
- vi. The secure payment request is transmitted over the Web to the merchant bank.
- vii. The merchant bank transmits this information to the customer's bank for authorization.
- viii. The customer's bank sends approval for payment to the merchant's bank, and if approved, the process is terminated and the merchandise shipped. This entire process (not including shipment) takes less than 30 seconds.

► Smart Cards

A smart card is about the size of a credit card, made of plastic with an embedded microprocessor chip that holds important financial and personal information. The microprocessor chip is loaded with the relevant information and periodically recharged.

Smart cards are broadly classified into two groups: contact and contactless. A contact smart card must be inserted into a special card reader to be read and updated. This type of smart card contains a microprocessor chip that makes contact with electrical connectors to transfer the data. A contactless smart card can be read from a short distance using radio frequency. This type of smart card also contains a microprocessor chip and an antenna that allows data to be transmitted to a special card reader without any physical contact. This type of smart card is useful for people who are moving in vehicles or on foot. They are used for collecting payment for highway tolls, bus fares, train fares, parking, and admission fees to movies, theaters, plays, ferry crossings, and so forth. The microprocessor chip can process different types of information, and therefore, various industries use them in different ways. Smart cards can accommodate a variety of applications that allow the customer to make purchases from a credit account, debit account, or stored value on the card. These cards can even have multiple applications operating at the same time. *For example*, the customer could have a frequent flyer program working on the same card as the customer debit or credit account. This enables the customer to earn points in his or her favourite program. Other services allow the customer to participate in frequency or loyalty programs with merchants, including storing hotel reservation preferences on the smart card.

Several computer manufacturers are developing keyboards that include smart card slots that can be read like bank credit cards. A smart card can be programmed for different applications. Some cards contain programming and data to support multiple applications, and some can be updated with new applications after they are issued. Smart cards can be designed to be inserted into a slot and read by a

special reader or be read at a distance, such as at a toll booth. Smart cards can be disposable or rechargeable. A popular example of a disposable smart card is the one issued by telephone companies. After using the pre-specified amount, the card can be discarded.

Some of the advantages of smart cards include the following:

- i. Cannot be easily duplicated
- ii. Can store many types of information
- iii. Convenience (portable and do not occupy much space)
- iv. Could include high security
- v. Low cost to issuers and users
- vi. High accuracy of information

Lack of universal standards for their design and utilization and low consumer acceptance are among the disadvantages of smart cards. However, these disadvantages would be resolved in the near future with smart use of card applications expected to increase.

10. Micropayment and Other Payment Systems

Micropayments are used for small payments on the Web. Some experts predict that this type of payment will grow substantially for purchasing digital products on the Web. The process is similar to e-wallet technology where the customer transfers some money into the wallet on his or her desktop and then pays for digital products by using this wallet. Using micropayment, one will be able to pay for these digital products on the Web. There are many vendors involved in micropayments systems. It provides universal acceptance and offers comprehensive security. This micropayment system can be used for billing by banks and financial institutions, telecommunications, Internet Service Providers (ISPs), content providers (offering games, entertainment, reference information, archives, reviews, and consumer information), service providers (offering fax, e-mail, or phone services over the Web), and by premium search engines and specialized databases.

Qpass sells content from publishers such as *The Wall Street Journal* Interactive Edition on a short-term or per-article basis.

Cybergold allows users to purchase digital content such as software, video files, and MP3-based songs.

Flooz is an online gift currency sent by e-mail. The recipient spends Flooz, just like money, at the online store of their choice.

ClickCharge assists customers to download a wallet and prepay for a block of micropurchases by credit card.

Trintech offers NetWallet and ezCard, which provide customers with simple and secure e-commerce payment instruments. It does not require buyers to download a wallet, it bills micropayments to the consumer's ISP account.

Millicent is a micropayment system implemented by Digital Equipment Corporation (now merged with Compaq), started in 1999 in Japan, with wallets starting at 1000 yen and payments as small as 5 yen (approximately 2.5 Rupees)

The AuricWeb system allows ISPs to document online transactions along with other user statistics.

CyBank adapts telephone-billing models. It uses prepaid cards and metered charges to Internet purchases.

Electronic gifts are one way of sending electronic currency or gift certificates from one individual to another. Electronic gifts are similar to regular gifts, only that they are transferred on the Web from the sender to the receiver. Electronic gifts are available from just about all major online stores, and their acceptance is on the rise. Paid for by credit card, they are usually non-transferable. Flooz, PayPal, and E-moneymail are examples of electronic gifts. PayPal and E-moneymail transfer funds to a recipient chosen by the sender. To use PayPal and E-moneymail, the user is supposed to open an account. Also, PayPal charges a service fee. These options are only practical for transferring a small amount of money without the recipient using or obtaining a credit card.

Clickshare is another popular micropayment system. Using Clickshare, the customer can purchase information, music, video, software, and other digital corporation (now merged with compaq), started in 1999 in Japan.

The AuricWeb system allows ISPs to document online transactions along with other user statistics.

CyBank adapts telephone-billing models. It uses prepaid cards and metered charges to Internet purchases.

Beenz, E-gold, and Mypoints are other examples of currency used in the e-commerce world.

11. Electronic Bill or Paperless Bill Presentment and Payment

1
Based. Number of sessions

Oct. 2011 – 5M

Write short note on:
Paperless bill

Electronic Bill Presentment and Payment (EBPP), is a fairly new technique that allows consumers to view and pay bills electronically. There are a significant number of bills that consumers pay on a regular basis, which include power bills, water, oil, Internet, phone service, mortgages, car payments, etc. EBPP systems send bills from service providers to individual consumers via the Internet.

The system also enables payments to be made by consumers, given that the amount that appears on the e-bill is correct. Banks in Canada have been offering these on-line payment services for some time now, and are growing in popularity.

This service is in addition to the original EBPP method of a direct withdrawal from a bank account through a bank such as Scotiabank.

The biggest difference between EBPP systems and the traditional method of bill payment is that of technology. Rather than receiving a bill through the mail, writing out and sending a cheque, consumers receive their bills in an e-mail, or are prompted to visit a website to view and pay their bills.

Three broad models of EBPP have emerged. These are:

- i. **Consolidation:** Where numerous bills for any one recipient are made available at one Website, most commonly the recipient's bank. In some countries, such as Australia, New Zealand and Canada, the postal service also operates a consolidation service. The actual task of consolidation is sometimes performed by a third party and fed to the websites where consumers receive the bills. The principal attraction of consolidation is that consumers can receive and pay numerous bills at one location, thus minimizing the number of login IDs and passwords they must remember and maintain.
- ii. **Biller direct:** Here, the bills produced by an organization are made available through that organization's Website. This model works well if the recipient has reasons to visit the biller's website other than to receive their bills. In the freight industry, *for example*, customers will visit a carrier's website to track items in transit, so it is reasonably convenient to receive and pay freight bills at the same site.
- iii. **Direct e-mail delivery:** Here the bills are emailed to the customer's inbox. This model most closely imitates the analog postal service. It is convenient, because almost everyone has an E-mail address and the customer has to do nothing except use e-mail in order to receive a bill. E-mail delivery is proving especially popular in the Business to Business (B2B) market in many countries.

Major providers of outsourced bill production services have developed facilities to process bills through consolidation, biller direct and e-mail delivery services, thus enabling major billers to have all their bills, paper and electronic, processed through one service. Niche service providers in many countries provide one or two of these models, but generally do not integrate with paper bill production.

12. Need of E-payment

Electronic Payment is a financial exchange that takes place online between buyers and sellers. The content of this exchange is usually some form of digital financial instrument (such as encrypted credit card numbers, electronic cheques or digital cash) that is backed by a bank or an intermediary, or by a legal tender. The various factors that have led the financial institutions to make use of electronic payments are:

- i. **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.
- ii. **Reduced operational and processing cost:** Due to reduced technology cost, the processing cost of various commerce activities becomes very less. A very simple reason to prove this is the fact that in electronic transactions, both paper and time are saved.
- iii. **Increasing online commerce:** The above two factors have led many institutions to go online and many others are following them. E-commerce with EDI, this was primarily for large business houses not for the common man. Many new technologies, innovations have led to use of E-commerce for the common man also.
- iv. **Affecting the consumers:** Credit cards, Debit Cards, Automated Teller Machines (ATM), stored value cards, E-Banking.
- v. **Enabling online commerce:** Digital Cash, E-Cash, Smart cards (or Electronic Purse) and encrypted Credit cards.
- vi. **Affecting companies:** The payment mechanisms that a bank provides to a company have changed drastically. The company can now directly deposit money into its employee's bank account. These transfers are done through Automated Transfer Houses.

13. Payment Considerations

One will need to support multiple electronic payment system options, which might include credit cards, electronic cheques, automatic balance transfers, and debit cards. Electronic fund transfers are the most prevalent transactions in the Business to Business (B2B) world, but some business customers prefer to pay by other means. In addition, whatever payment methods one accepts, one will need to integrate those services with own A/R system.

Payment processing is made even more complicated by the number of parties that can be involved. *For example*, accepting credit card payments means interacting with the credit card companies or a third party like CyberCash. Accepting an electronic fund transfer means the processing will pass from the customer's financial institution to the automated clearing house network for settlement.

And, if one syndicates bill presentment to multiple sites, one must work with multiple consolidators, portals, and Consumer Service Providers (CSPs) to get paid. If one is a biller, this means the payment service chosen must be able to integrate with the many channels that may be involved in processing payments.

Although accepting electronic payments usually means getting money faster, one should realize that most electronic payment system mechanisms are neither real time nor online. The network and credit-card infrastructures are batch-processing-intensive. No matter which service provider one chooses, some level of integration or customization will be required for it to be able to accept batch-payment data transfers from external parties.

Another key concern is security. Be sure to choose a vendor with a sound approach for encrypting its data transfers. Related to this is the data-center infrastructure the payment provider offers. The payment vendor should have clearly documented backup and recovery procedures, and should ensure high levels of availability, reliability, and performance through its Service-Level Agreements (SLAs). The payment vendor should provide one with reporting or audit-trail data for internal analysis, ideally accessible through a web-based administration interface.

Finally, standards compliance is becoming more important. *For example*, XML will play a critical role as a standard format for billing data, making it easier for trading partners to ingest such data into their own backend systems.

In addition, emerging standards for financial transactions, such as Open Financial Exchange (OFX) and Interactive Financial Exchange (IFX), will also play a role. OFX, created by CheckFree, Intuit, and Microsoft, defines a means for financial-services companies to exchange financial data over the Internet. IFX is a similar initiative designed specifically for online bill presentment and payment.

All these standards will play a role in providing an alternative to EDI, an expensive approach to electronic commerce that to date has been implemented only by very large companies with many trading partners and a strict Business to Business (B2B) focus. Of the three, XML has the most momentum, thanks to the general push for more standard methods of Business to Business (B2B) integration. OFX and IFX are in the medium adopter stage.

14. Using Payment Service Providers

Choosing the right payment service provider can relieve a lot of tension about of handling payments and interacting with so many different parties. In addition, some payment processors offer a bevy of value-added services that make their packages compelling to billers. *For example*, some payment processors also offer services as diverse as presentment, customer enrollment, validation, reporting, and even financing and cash-management services.

Of course, these capabilities come at a cost. Different payment processors offer different pricing models. Some processors charge a percentage of the dollar value of the transaction. Others charge a

flat fee for every transaction, regardless of the dollar volume. Still others charge based on volume or the number of bills converted or presented.

In most cases, the biller swallows the costs of online billing, just as in traditional billing operations. Although customers of the consumer-focused consolidator sites have shown a willingness to pay for online billing, they are not likely to pay more than it would cost to mail in their payments. In the Business to Business (B2B) world, some customers may be willing to bear some of the costs of e-billing by paying for things like financial services, but the model is still untested.

So, when it comes to picking a payment service, what are your options? As previously mentioned, there exists three major classes of payment services that organizations can use as part of their EBPP deployments: biller focused, commerce focused, and payer focused.

In the biller-focused area, CheckFree is the leader. The company processes 49 million electronic payments per month, has an infrastructure that can handle massive volumes, and has been active in forming partnerships and making strategic acquisitions. CheckFree offers sound capabilities and services beyond payment, including consolidation and presentment.

But, competitors are poised to chip away at CheckFree's lead. It offers an electronic-lockbox service as part of its offering. This approach makes especially good sense for small and midsize companies that want to get their lockbox and online payment services in an integrated package. Its foray into online billing could make the company a formidable player, as it has a strong customer base with financial institutions, particularly in the Midwest.

In the commerce-focused area, the major players include CyberCash, CyberSource, and VeriSign. All three provide good payment services, with support for a wide variety of different payment types. CyberSource has the edge in terms of its breadth of payment services, with offerings for fraud screening, tax calculation, distribution control, and fulfillment management. VeriSign has the advantage in terms of secure transfer services. In addition to payment, the company offers services for secure messaging, PKI, certificate processing, and other site trust services that payment-only vendors lack.

In the payer-focused area, most people immediately think of sites like PayPlace.com and ProPay.com. Although such sites provide a nifty solution for applications such as online auction payments or letting a group of people settle a vacation tab, they are not appropriate for more sophisticated online billing, especially in the B2B arena.

But, two vendors that come from this space, X.com and PayByCheck.com, are now adapting their solutions for billers. Both services make it simple for billers to set up accounts and simply include a link to the service providers' site, where customers make their payments online. X.com has released a new premium package of its PayPal service in which the payment funds are swept from the biller's PayPal account automatically through the network and into the biller's external bank account on a scheduled basis. PayByCheck.com is pursuing a similar strategy, but the company lags PayPal in terms of market momentum and customer base.

15. Value Exchange System

► Barter System

Barter System is that system in which goods are exchanged for goods. In ancient times, when money was not invented trade as a whole was on barter system. This was possible only in a simple economy but after the development of economy, direct exchange of goods without the use of money, was not without defects. There were various defects in this system. These were the following:

- i. **Double coincidence of wants:** Exchange can take place between two persons only if each possesses the goods which the other wants, *for example*, if a weaver needs shoes and he has cloth to offer in exchange he should not only find a cobbler who makes shoes, but find such cobbler who needs cloth and is prepared to give shoes in exchange for it. In this case, it was difficult to find such a person.
- ii. **Absence of standard value:** Under barter system there was no measure of value. Even if two persons met together who wanted each other's goods, they could not find a satisfactory equilibrium price. Under such conditions, one party had to suffer.
- iii. **Indivisibility of commodities:** It was difficult to divide a commodity without loss in its value, *for example*, a man who wants to purchase cloth equal to half the value of his cow and other commodities for the rest half value of cow, he could not divide his cow.
- iv. **Absence of store of value:** Wealth cannot be easily stored for future use in the form of commodities, because they perish in the long run. In the modern economy barter system cannot succeed. Money is indispensable for large scale production. The functions of money are the same which were defects in barter system. Its functions in modern economy are:
 - a. Money is a matter of functions.
 - b. A medium, a measure, a standard and store.

16. Modern/ Mobile Payment of Cash

Mobile payment is a new and rapidly-developing alternative payment method. Instead of paying with cheque or credit cards, a consumer can use a mobile phone to pay for a wide range of services and digital or hard goods such as:

- Music, videos, ringtones, online game subscription or items, wallpapers and other digital goods.
- Transportation fare (bus, subway or train), parking meters and other services
- Books, magazines, tickets and other hard goods.

There are four primary models for mobile payments:

- Premium SMS based transactional payments
- Direct Mobile Billing
- Mobile web payments (WAP)
- Contactless NFC (Near Field Communication)

16.1 Premium SMS based Transactional Payments

The consumer sends a payment request via an SMS text message to a short code and a premium charge is applied to their phone bill or their mobile wallet. The merchant involved is informed of the payment made and can then release the paid for goods.

Since a trusted delivery address has typically not been given these goods, it is most frequently digital with the merchant replying using a Multimedia Messaging Service to deliver the purchased music, ringtones, wallpapers, etc.

A Multimedia Messaging Service can also deliver bar codes which can then be scanned for confirmation of payment by a merchant. This is used as an electronic ticket for access to cinemas and events or to collect hard goods.

Transactional payments have been overtaken by other mobile payment methods such as mobile web payments (WAP), mobile payment client and Direct Mobile Billing for a number of reasons:

- Poor reliability:** Transactional payments can easily fail as messages get lost.
- Slow speed:** Sending messages can be slow and it can take hours for a merchant to get receipt of payment. Consumers do not want to be kept waiting more than a few seconds.
- Security:** The SMS/USSD encryption ends in the radio interface, then the message is a plaintext.
- High cost:** There are many high costs associated with this method of payment. The cost of setting up short codes and paying for the delivery of media via a Multimedia Messaging Service and the resulting customer support costs to account for the number of messages that get lost or are delayed.
- Low payout rates:** Operators also see high costs in running and supporting transactional payments which results in payout rates to the merchant being as low as 30%.
- Low follow-on sales:** Once the payment message has been sent and the goods received, there is little else the consumer can do. It is difficult for them to remember where something was purchased or how to buy it again. This also makes it difficult to tell a friend about a purchase.

16.2 Direct Mobile Billing

The consumer uses the mobile billing option during checkout at an e-commerce site—such as an online gaming site—to make a payment. After two-factor authentication involving a PIN and One-Time-Password, the consumer's mobile account is charged for the purchase. It is a true alternative payment method that does not require the use of credit/debit cards or pre-registration at an online payment solution such as PayPal, thus bypassing banks and credit card companies altogether. This type of mobile payment method, which is extremely prevalent and popular in Asia, provides the following benefits:

- i. **Security:** Two-factor authentication and a risk management engine prevent fraud.
- ii. **Convenience:** No pre-registration and no new mobile software is required.
- iii. **Easy:** It's just another option during the checkout process.
- iv. **Fast:** Most transactions are completed in less than 10 seconds.
- v. **Proven:** 70% of all digital content purchased online in some parts of Asia uses the Direct Mobile Billing method.

16.3 Mobile Web Payments (WAP)

The consumer uses web pages displayed or additional applications downloaded and installed on the mobile phone to make a payment. It uses Wireless Application Protocol (WAP) as underlying technology and thus inherits all the advantages and disadvantages of WAP. However, using a familiar web payment model gives a number of proven benefits:

- i. **Follow-on sales** where the mobile web payment can lead back to a store or to other goods the consumer may like. These pages have a URL and can be bookmarked making it easy to re-visit or share with friends.
- ii. **High customer satisfaction** from quick and predictable payments.
- iii. **Ease-of-use** from a familiar set of online payment pages.

Mobile web payment methods are now being mandated by a number of mobile network operators. A number of different actual payment mechanisms can be used behind a consistent set of web pages.

► Direct Operator Billing

A direct connection to the operator billing platform requires integration with the operator, but provides a number of benefits:

- i. **Simplicity:** The operators already have a billing relationship with the consumers, the payment will be added to their bill.
- ii. **Instantaneous payments** giving the highest customer satisfaction.
- iii. **Accurate responses** showing success and reasons for failure (no money *for example*).
- iv. **Security** to protect payment details and consumer identity.
- v. **Best conversion rates** from a single click-to-buy and no need to enter any further payment details.
- vi. **Reduced customer support costs** for merchants, since customers will complain to the operator.

It has, however a drawback, the payout rate will be much lower than with other payment providers.

► **Credit Card**

A simple mobile web payment system can also include a credit card payment flow allowing a consumer to enter their card details to make purchases. This process is familiar but any entry of details on a mobile phone is known to reduce the success rate (conversion) of payments.

In addition, if the payment vendor can automatically and securely identify customers, then card details can be recalled for future purchases turning credit card payments into simple single click-to-buy, giving higher conversion rates for additional purchases.

► **Online Wallets**

Online companies like PayPal, Amazon Payments and Google Checkout also have mobile options. Here is the process:

First Payment

- User registers, inputs his phone number, the provider sends him a SMS with a PIN.
- User enters the received PIN, authenticating the number.
- User inputs his credit card info (or another payment method) if necessary. (Not necessary if account already existing) and validates payments.

Subsequent payments

- The user re-enters his PIN to authenticate

Requesting a PIN is known to lower the success rate (conversion) for payments. These systems can be integrated with directly or can be combined with operator and credit card payments through a unified mobile web payment platform.

16.4 Contactless Near Field Communication

Near Field Communication (NFC) is used mostly in paying for purchases made in physical stores or transportation services. A consumer using a special mobile phone equipped with a smartcard, waves his/her phone near a reader module. Most transactions do not require authentication, but some require authentication using PIN, before transaction is completed. The payment could be deducted from pre-paid account or charged to mobile or bank account directly.

Summary

1. Electronic Payment System: The availability of appropriate e-payment method is a crucial element of e-business.
2. Requirements for E-payments
 - a. Atomicity: Money is not lost or created during a transfer
 - b. Good atomicity: Money and goods are exchanged atomically
 - c. Non-repudiation:
 1. No party can deny its role in the transaction
 2. Digital signatures
3. Process

a. Marketing	b. Customer/Visitor
c. WebSite Visit	d. Product Browsing
e. Shopping Basket	f. Checkout
g. Tax and Shipping	h. Payment
i. Receipt	j. Process Order
k. Fulfill Order	l. Ship Order
4. Electronic payment system can be broadly be grouped into:
 - a. Online Credit Card Payment System
 - b. Electronic Cheque System
 - c. Electronic Cash System and
 - d. Smart Card based Electronic Payment System
5. E-Payment Tool

a. Intelligent Card	b. E-Cash
c. E-Wallet	d. E-Cheque
6. Electronic Fund Transfer: EFT is the foundation of the cashless and chequeless society where cheques, stamps, envelopes, and paper bills are eliminated.
7. Payment Card


a. Credit Card	b. Debit Card
c. Charge Card	d. Smart Card
8. Need of Payment
 - a. Decreasing Technology cost
 - b. Reduced Operational and Processing Cost
 - c. Increasing Online Commerce
 - d. Affecting the Consumers
 - e. Enabling Online Commerce
 - f. Affecting Companies
9. Problem in E-Payment

a. Lack of Convenience	b. Lack of Security
c. Lack of Coverage	d. Lack of Eligibility
e. Lack of Support for Micro-Transactions	



PU Questions

- [Apr.2013 – 15M]** 1. Explain the process of electronic payment system. Brief its advantages and disadvantages.
- [Apr.2013 – 5M]** 2. Write short note on: E-cash.
- [Oct.2012 – 15M]** 3. What are the different types of Electronic Payment System? Describe any three types.
- [Apr.2012 – 15M]** 4. Explain concept of Electronic Fund Transfer. Brief about different types of Electronic Payment System.
- [Apr.2012 – 5M]** 5. Write short note on: E-cash
- [Oct.2011 – 15M]** 6. What is EPS? Explain in detail various types of EPSs.
- [Oct.2011 – 5M]** 7. Write short note on: Paperless bill
- [Apr.2011 – 15M]** 8. Enlist various types of electronic payment systems. Explain the process of electronic payment system with example.


VISION



Chapter 5
**TECHNOLOGY
SOLUTION**

1. Introduction

Internet is a means of connecting a computer to any other computer anywhere in the world, via dedicated routers and servers. When two computers are connected over the Internet, they can send and receive all kinds of information such as text, graphics, voice, video, and computer programs.

► E-commerce

E-commerce is the use of the Internet and e-mail to buy, sell and market products. A website can be used to provide information about the product/business, or provide a place where sales can be made.

E-commerce is a new way of conducting, managing and executing business transactions using computer and telecommunications networks. As awareness of the Internet throughout the commercial world and general public increases, competitiveness will force lower entry barriers, continued rapid innovation and expansion of markets.

The real key to making use of electronic commerce over the Internet a normal, everyday business activity is the convergence of the telecommunications, content/media and software industries.

E-commerce is expected to improve the productivity and competitiveness of participating businesses by an unprecedented access to an on-line global market place with millions of customers and thousands of products and services.

► **The Role of the Internet in Business Communication**

The role of the Internet in business communication is varied and has come to be of great importance. It can be used to increase effective communication both internally and externally. Use of the Internet can make it easier to connect with others quickly and more often, in addition to exchanging a wide array of media types. It can be used to communicate purchase information to vendors and helps customers to ask questions. The factors that make the role of the Internet in business communication important can also cause conflict, depending on the way the medium is used.

E-mail is one of the most popular uses of the Internet in business communication. It is widely used for both internal and external communications. E-mail enables users to communicate with each other at any hour and from several locations. It can also be an effective way to keep track of requests, conversations, and other important data as it provides a record of what was communicated.

One of the most significant internal uses of the Internet in business communication is the intranet site. This is a website that is only available to the members of a particular organization. It typically serves as both a sort of community bulletin board and a place to access forms, information, and other resources that are necessary or helpful for employees. Most intranet sites are password protected and some even have sections which are only available to certain groups of employees.

An important method of external use of the Internet in business communication is the website. This can be an effective method of communicating with customers, vendors, and business partners. A website can be a sales tool, a resource, or the means by which business can be conducted. It can be used for asking and answering questions; providing updates; and giving readers a detailed picture of a product, service, or organization.

Some roles of the Internet in business communication are less positive. Though the speed with which communications can be sent over the Internet can be useful, it can also lead to complications. This can include errors in documents which are sent so quickly that they cannot be corrected in time to avoid a costly mistake. Another common problem is with e-mail, which can easily be sent to the wrong party or group. Miscommunication in e-mail can lead to minor and major conflicts, which results in wastage of time, money, and resources.

2. Protecting Internet Communications

Anyone with an access to a wire or a computer containing your communications, or within the range of your wireless signal, can intercept your Internet communications with cheap and readily available equipment and software.

Lawyers call this 'wiretapping', while Internet techies call it 'packet sniffing' or 'traffic sniffing'.

The major security threats in today's world are hackers and crackers. The hackers are able to use various software's to break the security of networks and most of Internet transactions.

These security crackers can make fake IDs and credit card numbers or even hack a system to exploit the data. The most crucial targets are credit cards and business-related transactions.

Other than hackers, the presence of worms, viruses, spyware and Trojan horse pose threats security.

Solution:

- i. It is important for online users to scan files and folders for viruses and worms before downloading data and games.
- ii. Try to avoid using evasive passwords for system.
- iii. Update the patches and softwares.
- iv. Keep changing username and passwords of your system, e-mail IDs, and network computers.
- v. Install strong anti-virus softwares which would not allow the worms and viruses to reside in the system.
- vi. Try to use strong authentication tools and firewall for security of the system.

The other ways of protecting Internet Communications are as follows:

- i. Symmetric Key Encryption
- ii. Public key Encryption
- iii. Digital signatures
- iv. Digital Envelopes
- v. Digital Certificates

3. Encryption

Maintaining privacy in our personal communications is something everyone desires. Encryption is a means to achieve that privacy. It was invented for that purpose.

Encryption is the process of using an algorithm to transform information so as to make it unreadable for unauthorized users.

Encryption is a way to enhance the security of a message or file by scrambling the contents so that it can be read only by someone who has the right encryption key to unscramble it.

For example, if you purchase something from a website, the information for the transaction (such as your address, phone number, and credit card number) is usually encrypted to help keep it safe. Use encryption when you want a strong level of protection for your information.

Encryption is a method of converting an original message of a regular text into encoded text. The text is encrypted by means of an algorithm (type of formula).

If information is encrypted, there would be a low probability that anyone other than the receiving party who has the key to the code or access to another confidential process would be able to decrypt (translate) the text and convert it into plain, comprehensible text.

Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

Encryption is the process of changing information in such a way as to make it unreadable by anyone except those possessing special knowledge (usually referred to as a 'key') that allows them to change the information back to its original, readable form.

The use of encryption/decryption is as old as the art of communication.

In war time, a cipher, often incorrectly called a code, can be employed to keep the enemy from obtaining the contents of transmissions.

Simple ciphers include the substitution of letters for numbers, the rotation of letters in the alphabet, and the 'scrambling' of voice signals by inverting the side_band frequencies.

More complex ciphers work according to sophisticated computer algorithms that rearrange the data bits in digital signals.

In order to easily recover the contents of an encrypted signal, the correct decryption key is required.

The key is an algorithm that undoes the work of the encryption algorithm.

Alternatively, a computer can be used in an attempt to break the cipher. The more complex the encryption algorithm, the more difficult it becomes to eavesdrop on the communications without access to the key.

In recent years, a controversy has arisen over so-called strong encryption. This refers to ciphers that are essentially unbreakable without the decryption keys. While most companies and their customers view it as a means of keeping secrets and minimizing fraud, some governments view strong encryption as a potential vehicle by which terrorists might evade authorities.

These governments want to set up a key-escrow arrangement.

This means everyone who uses a cipher would be required to provide the government with a copy of the key. Decryption keys would be stored in a supposedly secure place, used only by authorities, and used only if backed up by a court order. Opponents of this scheme argue that criminals could hack

into the key-escrow database and illegally obtain, steal, or alter the keys. Supporters claim that while this is a possibility, implementing the key escrow scheme would be better than doing nothing to prevent criminals from freely using encryption/decryption.

When we use the Internet, we're not always just clicking around and passively taking in information, such as reading news articles or blog posts -- a great deal of our time online involves sending others our own information. Ordering something over the Internet, whether it's a book, a CD or anything else from an online vendor, or signing up for an online account, requires entering in a good deal of sensitive personal information.

A typical transaction might include not only our names, e-mail addresses, physical address and phone number, but also passwords and Personal Identification Numbers (PINs).

The incredible growth of the Internet has excited businesses and consumers alike with its promise of changing the way we live and work. It's extremely easy to buy and sell goods all over the world while sitting in front of a laptop. But security is a major concern on the Internet, especially when you're using it to send sensitive information between parties.

Let's face it, there's a whole lot of information that we don't want other people to see, such as:

- i. Credit-card information
- ii. Social Security numbers
- iii. Private correspondence
- iv. Personal details
- v. Sensitive company information
- vi. Bank-account information

Information security is provided on computers and over the Internet by a variety of methods. A simple but straightforward security method is to only keep sensitive information on removable storage media like portable flash memory drives or external hard drives. But the most popular forms of security rely on encryption, the process of encoding information in such a way that only the person (or computer) with the key can decode it.

3.1 Need of Encryption

Encryption is important because it allows you to securely protect data that you don't want anyone else to have access to.

Businesses use it to protect corporate secrets, government's use it to secure classified information, and many individuals use it to protect personal information to guard against things like identity theft.

Intelligence agencies uses encryption to securely protect folder contents, which could contain e-mails, chat histories, tax information, credit card numbers, or any other sensitive information.

This way, even if your computer is stolen that data is safe.

i. Securing information: Encryption can provide a means of securing information.

As more and more information is stored on computers or communicated via computers, the need to ensure that this information is safe from tampering becomes more relevant.

Any thoughts with respect to your own personal information (i.e., medical records, tax records, credit history, employment history, etc.) may bring to mind an area in which you DO want, need or expect privacy.

Encryption is seen by many people as a necessary step for commerce on the Internet to succeed. Without confidence that net transactions are secure, people are unwilling to trust a site enough to transact any sort of business with it. Encryption may give consumers the confidence they need to do internet business.

ii. Authentication: Encryption can also provide a means of 'message authentication'.

The sender's own secret key can be used to encrypt a message thereby signing it.

This creates a digital signature of a message.

This proves that the sender was the true originator of the message, and that the message has not been subsequently altered by anyone else, because the sender alone possesses the secret key that made that signature.

This prevents fake of that signed message, and prevents the sender from denying the signature.

iii. E-mail security: E-mail is certainly not secure. While you may believe that the use of a password makes your business private, you should be aware that sending information without encryption has been likened to sending postcards through the mail.

Your message is totally open to interception by anyone along the way. You may believe that personal e-mail is not incriminating and does not contain content that you must keep secret, and you may be right. But there are many common situations, where users have a lawful need for security, both to protect that information and to ensure that the information is not tampered with. Consumers placing orders with credit cards via the Internet, journalists protecting their sources, therapists protecting client files, businesses communicating trade secrets to foreign branches, ATM transactions, political dissenters, or whistle-blowers -- all are examples of why encryption may be needed for e-mail or data files, and why it might be necessary to create a secure environment through its use.

iv. Wireless communications security: Encryption/decryption is especially important in wireless communications. This is because wireless circuits are easier to tap than their hard-wired counterparts. Nevertheless, encryption/decryption is a good idea when carrying out

any kind of sensitive transaction, such as a credit-card purchase online, or the discussion of a company secret between different departments in the organization. The stronger the cipher -- that is, the harder it is for unauthorized people to break it -- the better, in general. However, as the strength of encryption/decryption increases, so does the cost.

3.2 Benefits of Encryption

Encryption has changed drastically over the years, from a military solution to widespread public use. Whether it's hardware or software-based, this method is fast, easy-to-use and most important, secure. Here are some of the key benefits this solution offers:

Benefits of Encryption

- i. Peace of Mind
- ii. Identity theft prevention
- iii. Power
- iv. Flexibility
- v. Transparency

- i. **Peace of mind:** If your computer gets lost or stolen, still you will have the peace of mind knowing that your data is totally secure, unreadable and protected against unauthorised access.
- ii. **Identity theft prevention:** Identity theft remains one of the highest priorities for fraudsters today. Encrypting your computer ensures that your identity is protected in the event of it being lost or stolen. The survey from the Identity Theft Resource Center found that:
 - Only 15% of victims find out about the theft through proactive action taken by a business.
 - The average time spent by victims resolving the problem is about 330 hours.
 - 73% of respondents indicated the crime involved the thief acquiring a credit card.
 - The emotional impact is similar to that of victims of violent crimes.
- iii. **Power:** Encryption is based on global standards, able to moderate potential corruption without flaw. Many solutions are large enough to ensure that an entire organization is in full compliance with security policies. Data encryption allows a corporation to achieve military-level security with easy and affordable solutions.
- iv. **Flexibility:** Encryption can protect your sensitive information whether it's stored on a desktop or laptop computer, a PDA, removable storage media, an e-mail server or even the corporate network. This allows you to securely access important data from the office, on the road or at home. If the device is lost or stolen, the information will be protected by the data encryption mechanism.
- v. **Transparency:** It wouldn't be a good idea to employ any security measure that negatively impacts business. An efficient data encryption solution enables business to flow at a normal pace, silently securing crucial data in the background. Some of the best options are those running effectively without the user even being aware of it.

There are many benefits of data encryption as this solution provides solid protection in the event of a security violation. Not only does it offer peace of mind, it also frees up resources normally used by your perimeter defenses. Every security measure set in place is important yet inefficient if confidential data itself is not protected.

3.3 Security Encryption System

Computer encryption is based on the science of cryptography, which has been used as long as humans have wanted to keep information secret.

Before the digital age, the biggest users of cryptography were governments, particularly for military purposes.

The Greek historian *Plutarch* wrote, *for example*, about Spartan generals who sent and received sensitive messages using a scytale, a thin cylinder made out of wood. The general would wrap a piece of parchment around the scytale and write his message along its length. When someone removed the paper from the cylinder, the writing appeared to be a jumble of nonsense. But if the other general receiving the parchment had a scytale of similar size, he could wrap the paper around it and easily read the intended message.

The Greeks had used ciphers, specific codes that involve substitutions or transpositions of letters and numbers.

As long as both generals had the correct cipher, they could decode any message the other sent. To make the message more difficult to decipher, they could arrange the letters inside the grid in any combination.

Most forms of cryptography in use these days rely on computers, simply because a human-based code is too easy for a computer to crack.

Ciphers are also better known today as **algorithms**, which are the guides for encryption -- they provide a way in which to craft a message and give a certain range of possible combinations.

A **key**, on the other hand, helps a person or computer *figure* out the one possibility on a given occasion.

Computer encryption systems generally belong to one of the two categories:

- i. Symmetric-key encryption
- ii. Public-key encryption

4. Symmetric-Key Encryption

The symmetric setting considers two parties who share a key and will use this key to imbue communicated data with various security attributes. The main security goals are privacy and authenticity of the communicated data.

Secure data transmission coding schemes (such as the Data Encryption Standard) which uses only one digital key in both encoding and decoding a message.

Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.

Symmetric encryption is an encryption algorithm where the same key is used for both encryption and decryption. The key must be kept secret, and is shared by the sender and recipient.

Symmetric encryption is a form of computerized cryptography using a singular encryption key to guise an electronic message. Its data conversion uses a mathematical algorithm along with a secret key, which results in the inability to make sense out of a message.

Symmetric encryption is a two-way algorithm because the mathematical algorithm is reversed when decrypting the message along with using the same secret key.

Think of it like this:

You create a coded message to send to a friend in which each letter is substituted with the letter that is two down from it in the alphabet. So 'A' becomes 'C,' and 'B' becomes 'D'.

You have already told a trusted friend that the code is 'Shift by 2'. Your friend gets the message and decodes it. Anyone else who sees the message will see only nonsense.

The same goes for computers, but, of course, the keys are usually much longer. The first major symmetric algorithm developed for computers in the United States was the Data Encryption Standard (DES), approved for use in the 1970s. The DES uses a 56-bit key.

Because computers have become increasingly faster since the '70s, security experts no longer consider DES secure -- although a 56-bit key offers more than 70 quadrillion possible combinations (70,000,000,000,000,000), an attack of brute force (simply trying every possible combination in order to find the right key) could easily decipher encrypted data in a short while.

DES has since been replaced by the Advanced Encryption Standard (AES), which uses 128-, 192- or 256-bit keys. Most people believe that AES will be a sufficient encryption standard for a long time coming: A 128-bit key, for instance, can have more than

300,000,000,000,000,000,000,000,000,000 key combinations.

Symmetric encryption also referred to as conventional encryption or single key encryption was the only type of encryption in use prior to the development of public-key encryption in 1976.

The symmetric encryption scheme has five ingredients:

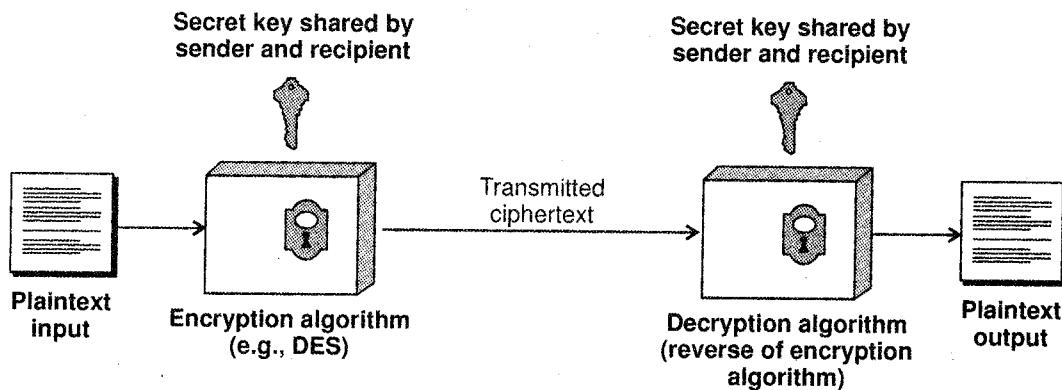


Figure 5.1: Model of Symmetric Encryption

- i. **Plaintext:** This is the original intelligible message or data that is fed to the algorithm as input.
- ii. **Encryption algorithm:** The encryption algorithm performs various substitutions and permutations on the plaintext.
- iii. **Secret key:** The secret key is also input to the encryption algorithm. The exact substitutions and permutations performed depend on the key used, and the algorithm will produce a different output depending on the specific key being used at the time.
- iv. **Cipher text:** This is the scrambled message produced as output. It depends on the plaintext and the key. The cipher text is an apparently random stream of data, as it stands, is unintelligible.
- v. **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key and produces the original plaintext.

There are two requirements for a symmetric key cryptosystem:

- i. We assume it is impractical to decrypt a message on the basis of the cipher text plus knowledge of the encryption/decryption algorithm. In other words, we do not need to keep the algorithm secret; we need to keep only the key secret.
- ii. Sender and the receiver must have obtained copies of the secret key in a secure manner and must keep the key secure. If someone can discover the key and knows the algorithm, all communications using this key is readable.

5. Public Key Encryption

One of the weaknesses some point out about symmetric key encryption is that two users attempting to communicate with each other need a secure way to do so; otherwise, an attacker can easily take the necessary data from the stream.

Public-key on the other hand, introduces another concept involving key pairs:

One for encrypting, the other for decrypting.

This concept is very clever and attractive, and provides a number of advantages over symmetric-key:

- Simplified key distribution
- Digital Signature
- Long-term encryption

However, it is important to note that symmetric-key still plays a major role in the implementation of a Public-key Infrastructure.

In November 1976, a paper published in the journal IEEE Transactions on Information Theory, titled 'New Directions in Cryptography,' addressed this problem and offered a solution: public-key encryption.

Public-key encryption also called asymmetric encryption involves a pair of keys—a public key and a private key—associated with an entity that needs to authenticate its identity electronically or to sign or encrypt data.

Public-key encryption uses two different keys simultaneously -- a combination of a private key and a public key. The private key is known only to your computer, while the public key is given by your computer to any computer that wants to communicate securely with it.

To decode an encrypted message, a computer must use the public key, provided by the originating computer, and its own private key.

Although a message sent from one computer to another won't be secure since the public key used for encryption is published and available to anyone, anyone who picks it up can't read it without the private key. The key pair is based on prime numbers of long length. This makes the system extremely secure, because there is essentially an infinite number of prime numbers available, meaning there are nearly infinite possibilities for keys.

Each public key is published, and the corresponding private key is kept secret.

Data encrypted with your public key can be decrypted only with your private key.

Following figure shows a simplified view of the way public-key encryption works:

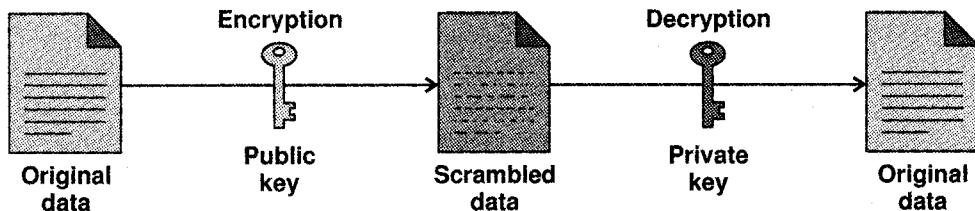


Figure 5.2

In general, to send encrypted data to someone, you encrypt the data with that person's public key, and the person receiving the encrypted data decrypts it with the corresponding private key.

Compared with symmetric-key encryption, public-key encryption requires more computation and is, therefore, not always appropriate for large amount of data.

However, it's possible to use public-key encryption to send a symmetric key, which can then be used to encrypt additional data. This is the approach used by the SSL (Secure Sockets Layer) protocol.

As it happens, the reverse of the scheme shown in figure also works:

Data encrypted with your private key can be decrypted only with your public key. This would not be a desirable way to encrypt sensitive data, however, because it means that anyone with your public key, which is by definition published, could decrypt the data.

Nevertheless, private-key encryption is useful, because it means you can use your private key to sign data with your digital signature—an important requirement for electronic commerce and other commercial applications of cryptography.

Client software such as Communicator can then use your public key to confirm that the message was signed with your private key and that it hasn't been tampered with since being signed.

The Public Key is what its name suggests - Public. It is made available to everyone via a publicly accessible repository or directory. On the other hand, the Private Key must remain confidential with its respective owner.

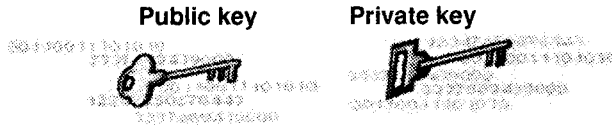


Figure 5.3

Because the key pair is mathematically related, whatever is encrypted with a Public Key may only be decrypted by its corresponding Private Key and vice versa.

Encryption and Decryption: Encryption is a mechanism by which a message is transformed so that only the sender and recipient can see. For instance, suppose that Alice wants to send a private message to Bob.

To do so, she first needs Bob's public-key; since everybody can see his public-key, Bob can send it over the network in the clear without any concerns. Once Alice has Bob's public-key, she encrypts the message using Bob's public-key and sends it to Bob. Bob receives Alice's message and, using his private-key, decrypts it.

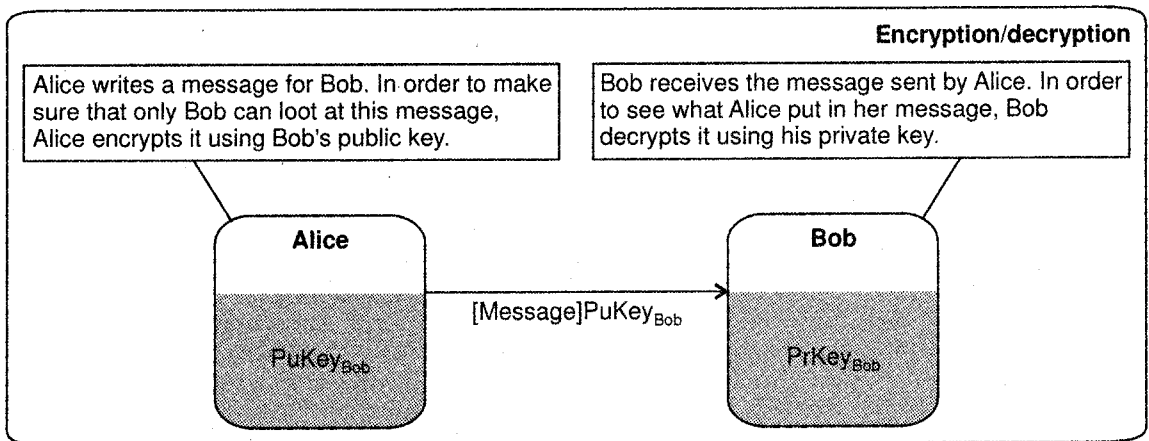


Figure 5.4: Encryption/Decryption principles

6. Public Key Encryption using Digital Signatures

Digital signature is a mechanism by which a message is authenticated, i.e., proving that a message is effectively coming from a given sender, much like a signature on a paper document.

For instance, suppose that Alice wants to digitally sign a message to Bob.

To do so, she uses her private-key to encrypt the message; she then sends the message along with her public-key (typically, the public key is attached to the signed message).

Since Alice's public-key is the only key that can decrypt that message, a successful decryption constitutes a Digital Signature Verification, meaning that there is no doubt that it is Alice's private key that encrypted the message.

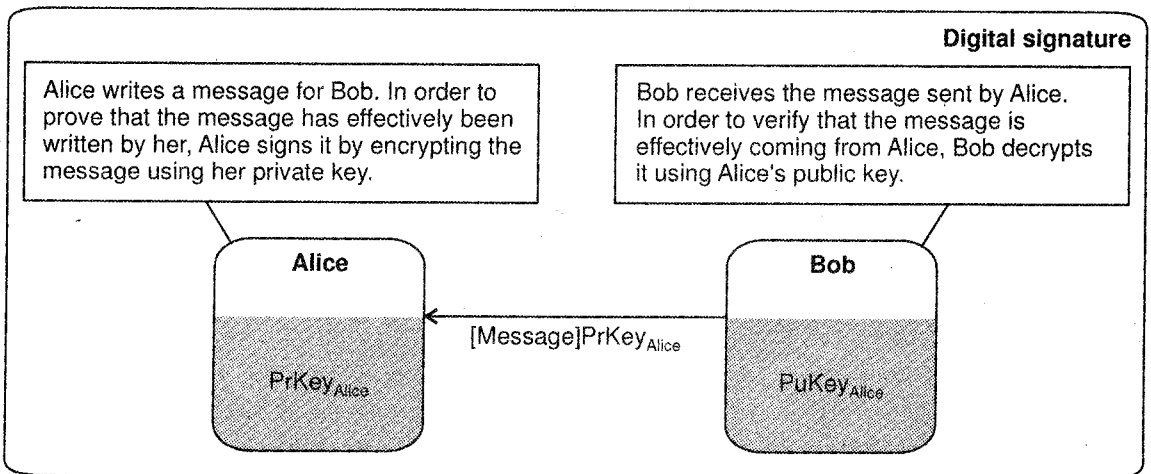


Figure 5.5: Digital signature

For Digital signature, another technique used is called hashing. Hashing produces a message digest that is a small and a unique representation (a bit like a sophisticated checksum) of the complete message. Hashing algorithms are a one-way encryption, i.e., it is impossible to derive the message from the digest.

The main reasons for producing a message digest are:

- i. The message integrity being sent is preserved; any message alteration will immediately be detected.

- ii. The digital signature will be applied to the digest, which is usually considerably smaller than the message itself.
- iii. Hashing algorithms are much faster than any encryption algorithm (asymmetric or symmetric).

The following sections explain what really happens when encrypting and signing a message on one hand, and when decrypting a message and verifying its signature on the other hand.

► Steps for signing and encrypting a message

Figure below shows the set of operations required when Alice wants to send a signed and encrypted message to Bob.

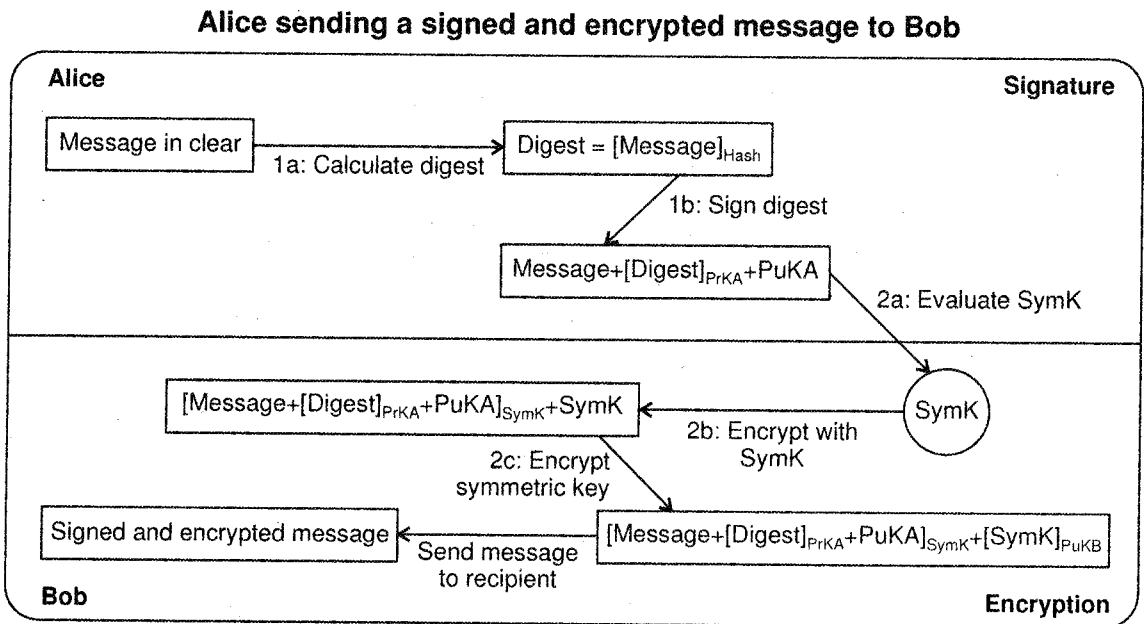


Figure 5.6

Legend	
PrKA	Alice's Private Key
PuKA	Alice's Public Key
PuKB	Bob's Public Key
SymK	One time symmetric key
Hash	Hashing algorithm

- i. **Message signature:** Digital signature includes two steps:
- Message digests evaluation.* The main purpose for evaluating a digest is to ensure that the message is kept unaltered; this is called message integrity.
 - Digest signature.* A signature is in fact an encryption using the issuer's (Alice in this case) private-key. Included in the signature is also the hashing algorithm name used by the issuer.

The issuer's public-key is also appended to the signature. Doing so lets anyone decrypt and verify the signature using the issuer's public-key and hashing algorithm. Given the properties of public-key encryption and hashing algorithms, the recipient has proof that:

- The issuer's private-key has encrypted the digest.
 - The message is protected against any alteration.
- ii. **Message encryption:** Encryption includes the following three steps:
- Creation of a onetime symmetric encryption/decryption key:* Remember that encryption and decryption algorithms using asymmetric-keys are too slow to be used for long messages; symmetric-key algorithms are very efficient and are therefore used.
 - Message encryption:* The whole message (the message itself and the signature) is encrypted using SymK, the symmetric-key evaluated above.
 - Symmetric-key encryption:* SymK is also used by the recipient to decrypt the message. SymK must therefore be available to the recipient (Bob) only. The way to hide the Symk from everybody except the recipient is to encrypt it using the recipient's public-key. Since SymK is a small piece of information compared to a message (that could be very long), the performance penalty associated with the relative inefficiency of asymmetric-key algorithms is acceptable.

One interesting point to mention is that if Alice wants to send the same message to more than one recipient, say Bob and John for instance, the only additional operation to be performed is to repeat 'step 2c' for John. Hence, the message that both Bob and John would receive would look like:

[Message+ [Digest] PrKA+PuKA]SymK+ [SymK] PuKB+ [SymK] PuKJ.

Notice that the exact same SymK will be used by Bob and John to decrypt the message.

► **Steps for Decrypting and verifying the signature of a message**

Figure below shows the set of operations required when Bob wants to decrypt and verify the message sent by Alice.

Bob decrypting and verifying message sent by Alice

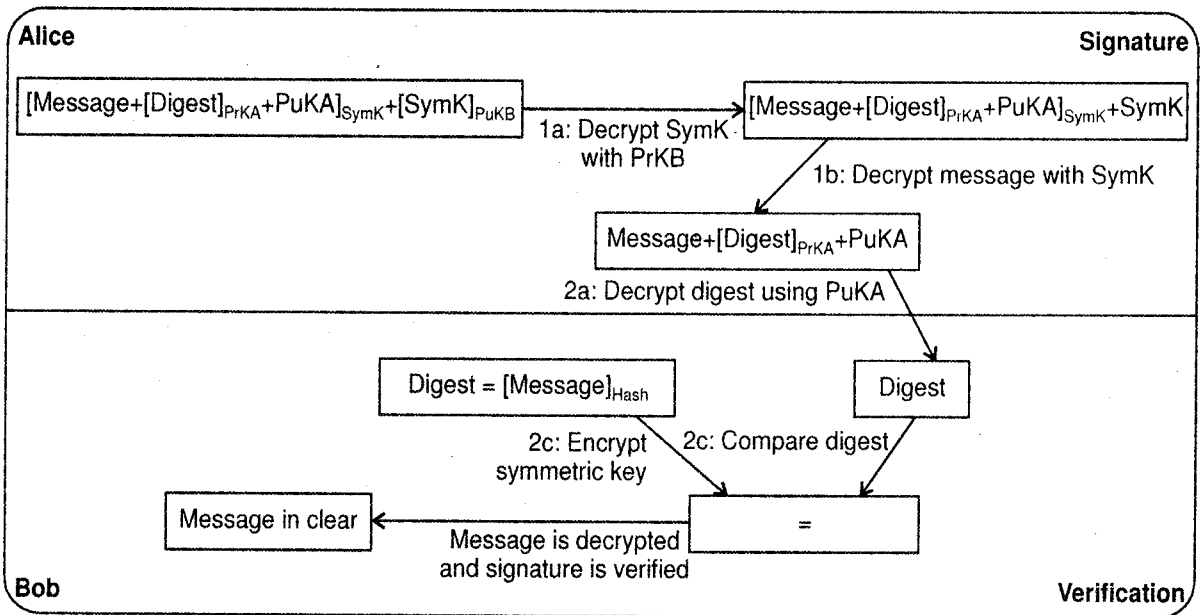


Figure 5.7

Legend	
PrKA	Alice's Private Key
PuKA	Alice's Public Key
PuKB	Bob's Public Key
SymK	One time symmetric key
Hash	Hashing algorithm

- i. **Message decryption:** The decryption includes the following steps:
- Symmetric-key decryption:* The one-time symmetric-key has been used to encrypt the message. This key (SymK) has been encrypted using the recipient's (Bob) public-key. Only Bob can decrypt SymK and use it to decrypt the message.
 - Message decryption.* The message (which includes the message itself and the signature) is decrypted using SymK.

- ii. **Signature verification:** The signature verification includes the following 3 steps:
- a. *Message digests decryption.* The digest has been encrypted using the issuer's (Alice) private-key. The digest is now decrypted using the issuer's public-key included in the message.
 - b. *Digest evaluation:* Since hashing is a one-way process, i.e., the message cannot be derived from the digest itself, the recipient must re-evaluate the digest using the exact same hashing algorithm the issuer used.
 - c. *Digests comparison:* The digest decrypted in (a) and the digest evaluated in (b) are compared. If there is a match, the signature has been verified, and the recipient can accept the message as coming unaltered from the issuer. If there is a mismatch this could mean that:
 - The message has not been signed by the issuer or
 - The message has been altered.
 - In both cases, the message should be rejected.

Public-key cryptography facilitates the following tasks:

- i. Encryption and decryption allows two communicating parties to disguise information they send to each other. The sender encrypts, or scrambles, information before sending it. The receiver decrypts, or unscrambles, the information after receiving it. While in transit, the encrypted information is unintelligible to an intruder.
- ii. Tamper detection allows the recipient of information to verify that it has not been modified in transit. Any attempt to modify data or substitute a false message for a legitimate one will be detected.
- iii. Authentication allows the recipient of information to determine its origin-that is; to confirm the sender's identity.
- iv. No repudiation prevents the sender of information from claiming at a later date that the information was never sent.

7. Digital Envelopes

A *digital envelope* (encryption) is the electronic equivalent of putting your message into a sealed envelope to provide privacy and resistance from tampering.

A type of security that uses two layers of encryption to protect a message. First, the message itself is encoded using symmetric encryption, and then the key to decode the message is encrypted using

public-key encryption. This technique overcomes one of the problems of public-key encryption, which is that it is slower than symmetric encryption. As only the key is protected with public-key encryption, there is very little overhead.

A digital envelope is a secure electronic data container that is used to protect a message through encryption and data authentication. A digital envelope allows users to encrypt data with the speed of secret key encryption and the convenience and security of public key encryption.

Rivest, Shamir and Adleman (RSA) Public-Key Cryptography Standard (PKCS) governs the application of cryptography to data for digital envelopes and digital signatures.

A digital envelope is also known as a digital wrapper.

A digital envelope uses two layers for encryption:

Secret (symmetric) key and public key encryption. Secret key encryption is used for message encoding and decoding. Public key encryption is used to send a secret key to a receiving party over a network. This technique does not require plain text communication.

Either of the following methods may be used to create a digital envelope:

- i. Secret key encryption algorithms, such as *Rijndael* or *Twofish*, for message encryption.
- ii. Public key encryption algorithm from RSA for secret key encryption with a receiver's public key.

A digital envelope may be decrypted by using a receiver's private key to decrypt a secret key, or by using a secret key to decrypt encrypted data.

An *example* of a digital envelope is Pretty Good Privacy (PGP) - popular data cryptography software that also provides cryptographic privacy and data communication authentication.

7.1 Creating a Digital Envelope

► Purpose

You use a digital envelope to protect a digital document from being visible to anyone other than the intended recipient.

The following are possible reasons for using digital envelopes:

- i. Sending confidential data or documents across (possibly) insecure communication lines.
- ii. Storing confidential data or documents (*for example*, companies internal reports).

► Prerequisites

To create a digital envelope, you need access to the intended recipient's public key. How to obtain access to the public key depends on the public-key infrastructure of your organization.

You also need the digital document that you want to protect.

► Process Flow

As an end user, you generally indicate that you want to 'create an envelope' for a document and the system does the rest.

The following figure shows what happens when you create a digital envelope:

Creating a Digital Envelope

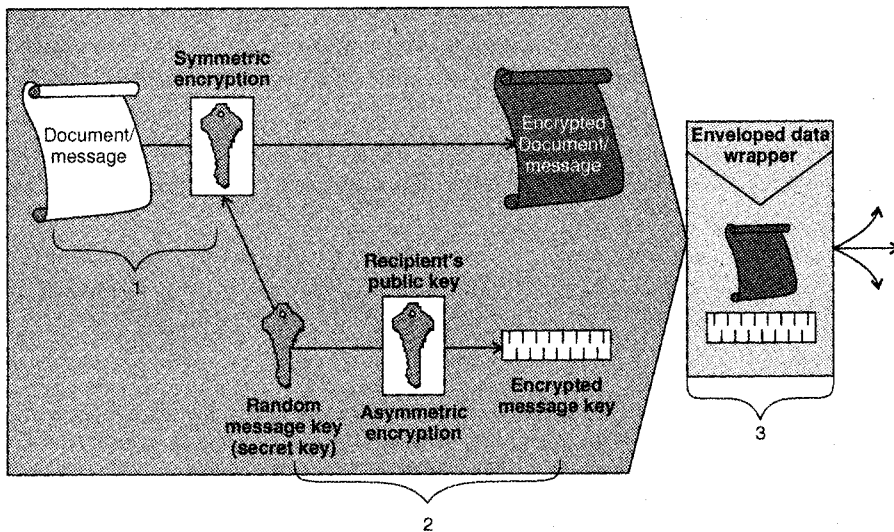


Figure 5.8

The following explains what happens at each step:

- The message is encrypted using symmetric encryption. Typically, a newly generated random message key (secret key) is used for the encryption.
- Symmetric encryption means that the same key is used for both encryption and decryption (a secret key). Anyone wanting to decrypt the message needs access to this key.
- To transfer the secret key between the parties, the secret key is encrypted using the recipient's public key.
- The encrypted document and the encrypted message key are packed together in a single data packet to save or send to the intended recipient.

8. Digital Certificates

Digital certificates: To implement public key encryption on a large scale, such as a secure Web server might need, requires a different approach. This is where digital certificates come in.

A digital certificate is essentially a bit of information that says the Web server is trusted by an independent source known as a **Certificate Authority**.

The Certificate Authority acts as the middleman that both computers trust. It confirms that each computer is in fact who they say they are and then provides the public keys of each computer to the other.

Digital certificate is a pair of files on computer that User can use to create the digital equivalent of handwritten signatures and sealed envelopes.

Each pair of files is divided into two parts: the public key and the private key.

The public key is the portion that is shared; the private key is the portion that only the user should have access to.

User's computer and programs understand how to share only the public portion of keys so that others can see them, while still keeping User private keys secure.

For example:

When sending an e-mail message, you can digitally sign the message by attaching your digital certificate. Once they receive the message, recipients can verify that it came from you by viewing the small attachment on the e-mail, which contains your public key information.

This protects you from people who might try to 'spoof' an e-mail that looks like it came from you but is really sent from a different e-mail account.

You can also use digital certificates to electronically sign documents. This is one reason why it is extremely important to protect the private key portions of your certificate files and never share them.

You could be legally bound to something, and it would be extremely difficult to prove that it wasn't you who digitally signed the message.

When you encrypt a message, you create the equivalent of a sealed envelope so that only you and the recipient can see the message. Normally, when you send an e-mail message, it is the electronic equivalent of a postcard—anyone who has access to the network between you and the recipient can potentially read that postcard.

With the encryption offered by the digital certificates, you can avoid this problem.

In the case of encryption, you use the recipient's public key to encrypt the message. Only the recipient has the private key that allows the message to be decoded.

8.1 What is a Certificate?

A certificate is a piece of information that proves the identity of a public-key's owner. Like a passport, a certificate provides recognized proof of a person's (or entity) identity. Certificates are signed and delivered securely by a trusted third party entity called a Certificate Authority (CA).

A certificate contains among other things:

- i. The CA's identity
- ii. The owner's identity
- iii. The owner's public-key
- iv. The certificate expiry date
- v. The CA's signature of that certificate
- vi. Other information

With a certificate instead of a public-key, a recipient can now verify a few things about the issuer to make sure that the certificate is valid and belongs to the person claiming its ownership:

- i. Compare the owner's identity
- ii. Verify that the certificate is still valid
- iii. Verify that the certificate has been signed by a trusted CA
- iv. Verify the issuer's certificate signature, hence making sure it has not been altered.

Certificates are signed by a CA, which means that they cannot be altered. In turn, the CA signature can be verified using that CA's certificate.

8.2 Benefits of Digital Certificates

There are several benefits of using digital certificates:

- i. Send signed e-mail messages. This ensures the recipients that the message came from the User and not someone pretending to be a user.
- ii. Encrypt the contents of e-mail messages and attachments, protecting them from being read by online intruders. Only user intended recipient can decrypt them.
- iii. Encrypt files and/or folders on user's computer. This is helpful for lost or stolen mobile devices and laptops because thieves would need to know password to access any of the encrypted files or folders.
- iv. Streamline business processes by allowing people to use digital certificates to electronically sign documents or approve something at a given stage of the process.

9. Limitations to Encryption Solutions

Some of the reasons why people may not choose to encrypt their data is because of the disadvantages that encryption has. Some of these are the complexity of computer encryption, the usually high cost, the ability for it to be easily changed and its inability to organize the data that has been encoded.

Even though the data doesn't need to be protected anymore because of the encryption, but still puts a lot of pressure on IT employees because then their top priority becomes protecting the key to the encryption. This is because if the key is lost then the data is no longer protected.

Another disadvantage is that not only is it very expensive to encrypt and decrypt power but it also takes a lot of processing, energy and computer power as well. This means that even though data is protected the overall performance of the computer could drop.

The other disadvantage is that encryption won't prevent hackers or viruses and it also may make it difficult to use the encrypted file as some restrictions may have been placed on it.

► Disadvantages of Symmetric Key Encryption

- i. **Need for secure channel for secret key exchange:** Sharing the secret key in the beginning is a problem in symmetric key encryption. It has to be exchanged in a way that ensures it remains a secret.
- ii. **Too many keys:** A new shared key has to be generated for communication with every different party. This creates a problem with managing and ensuring the security of all these keys.
- iii. **Origin and authenticity of message cannot be guaranteed:** Since both sender and receiver use the same key, messages cannot be verified to have come from a particular user. This may be a problem if there is a dispute.

► Disadvantages of Public Key Encryption

- i. **Public keys should/must be authenticated:** No one can be absolutely sure that a public key belongs to the person it specifies and so everyone must verify that their public keys belong to them.
- ii. **Slow:** Public key encryption is slow compared to symmetric encryption. Not feasible for use in decrypting bulk messages.
- iii. **Uses up more computer resources:** It requires a lot more computer supplies compared to single-key encryption.

- iv. **Widespread security compromise is possible:** If an attacker determines a person's private key, his or her entire messages can be read.
- v. **Loss of private key may be irreparable:** The loss of a private key means that all received messages cannot be decrypted.

► **Disadvantages of Digital Signatures**

Just like all other electronic products, digital signatures have some disadvantages. These include:

- i. **Expiry:** Digital signatures, like all technological products, are highly dependent on the technology it is based on. In this era of fast technological advancements, many of these technological products have a short shelf life.
- ii. **Certificates:** In order to effectively use digital signatures, both senders and recipients may have to buy digital certificates at a cost from trusted certification authorities.
- iii. **Software:** To work with digital certificates, senders and recipients have to buy verification software at a cost.
- iv. **Law:** In some states and countries, laws regarding cyber and technology-based issues are weak or even non-existent. Trading in such jurisdictions becomes very risky for those who use digitally signed electronic documents.
- v. **Compatibility:** There are many different digital signature standards and most of them are incompatible with each other and this complicates the sharing of digitally signed documents.
- vi. **Cost:** Digital signatures, even some of the simpler ones, come at a cost. You must have the necessary software to encode the signatures, and if you're using hardware so that customers can sign physically, then the cost goes up even further. Digital signatures are an additional cost that should be weighed against their potential security benefits.
- vii. **Training and Troubleshooting:** If your employees aren't tech savvy or simply aren't sure how to use a digital signature, then you'll have to spend time training them about how the signature process works. This will take them away from their jobs, costing you money. Additionally, as with all computer-related applications, sooner or later there will be a problem in the system and you'll need someone to troubleshoot. If none of your employees can find and fix the problem, you'll have to hire someone else to do it.

Summary

1. E-commerce is a new way of conducting, managing and executing business transactions using computer and telecommunications networks.
2. **Encryption** is a way to enhance the security of a message or file by scrambling the contents so that it can be read only by someone who has the right encryption key to unscramble it.
3. Computer encryption is based on the science of **cryptography**, which has been used since the time humans wanted to keep information secret.
4. Symmetric Encryption is an Encryption algorithm where the same key is used for both Encryption and Decryption. The key must be kept secret, and is shared by the message sender and recipient.
5. Public-key encryption, also called asymmetric encryption, involves a pair of keys-a public key and a private key-associated with an entity that needs to authenticate its identity electronically or to sign or encrypt data.
6. Public-key encryption uses two different keys at once -- a combination of a private key and a public key. The private key is known only to your computer, while the public key is given by your computer to any computer that wants to communicate securely with it.
7. A *digital envelope* (encryption) is the electronic equivalent of putting your message into a sealed envelope to provide privacy and resistance from tampering.
8. A digital certificate is essentially a bit of information that says the Web server is trusted by an independent source known as a **Certificate Authority**.

The Certificate Authority acts as the middleman that both computers trust. It confirms that each computer is, in fact, who they say they are and then provides the public keys of each computer to the other.
9. Digital certificate is a pair of files on computer that User can use to create the digital equivalent of handwritten signatures and sealed envelopes.

EXERCISE

A] Short answers.

[Each 5 M]

1. Write short notes on:
 - i. Digital Envelopes
 - ii. Public Key Encryption
 - iii. Symmetric-key encryption
 - iv. Benefits of Encryption
 - v. Certificate Authority

B] Long answers.**[Each 10 M]**

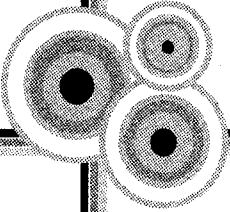
1. 'The Certificate Authority acts as the middleman that both sender and receiver trusts'. Comment. Explain the concept of Digital Certificate.
2. Give limitations of Encryption solutions.

C] Descriptive questions.**[Each 15 M]**

1. What is meant by Encryption? Describe Symmetric-key encryption and Public-key encryption.
2. Explain in detail various ways of protecting Internet Communications.
3. Explain in detail Public Key Encryption using digital signatures.



E-COM SECURITY



1. Introduction

E-commerce isn't just increasing, it's evolving. The exponential rate of e-commerce growth has far surpassed mainstream security measures set in place to properly regulate online commerce and prevent consumer identity fraud.

Every time a new e-commerce innovation is released, a new security risk is posed for consumers.

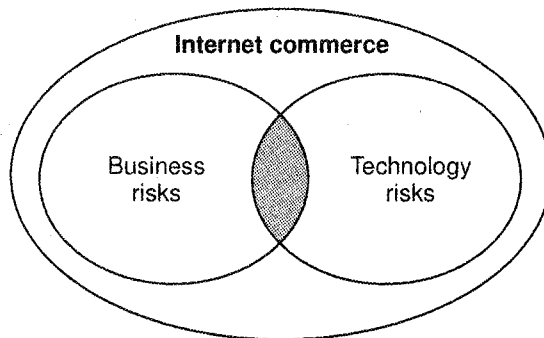


Figure 6.1

E-commerce sales is expected to grow more than 12 % in 2013 and e-commerce sales worldwide is projected to hit \$1.298 trillion this year. The burden of determining how to transact safely online has fallen hardest on the individual consumer.

Today's consumer is confronted daily by a number of different online commerce opportunities, choices, and decisions, none of which were available 20 years ago.

E-commerce is gaining momentum and acceptance, previously, risky online activity such as banking is now considered safe and reliable. Yet, popular methods used to access sensitive information online present serious security risks.

Most consumers too easily accept terms and conditions without a second thought, compromising online anonymity and privacy.

Although online commerce does present security risks, the consumer benefits of e-commerce far outnumber than those of in-store shopping.

After all, while driving to the mall there could be a risk of a car accident; swiping a credit card at checkout places us at a risk of credit card skimming. There will always be risks, but the e-commerce world will evolve rapidly.

2. E-Commerce Security Environment

E-commerce refers to the exchange of goods and services over the Internet. All major retail brands have an online presence, and many brands have no associated bricks and mortar presence. However, e-commerce also applies to business-to-business transactions, *for example*, between manufacturers and suppliers or distributors.

In the online retail space, there are a number of models that retailers can adopt. Traditionally, the Web presence has been kept distinct from the bricks and mortar presence, so transactions were limited to buying online and delivering the goods or services. The online presence is also important for researching on product that a customer can purchase later from the store. Recently, there has been a trend towards multi-channel retail, allowing new models such as purchasing online and picking up from the store.

E-commerce systems are also relevant for the services industry. *For example*, online banking and brokerage services allow customers to retrieve bank statements online, transfer funds, pay credit card bills, apply for and receive approval for a new mortgage, buy and sell securities, and get financial guidance and information.

2.1 Security has the Following Dimensions

- i. **Confidentiality:** It allows only authorized parties to read protected information. *For example*, if the postman reads your mail, this is a breach of your privacy.
- ii. **Integrity:** It ensures that information being displayed on a Website or transmitted/received over the Internet has not been altered in any way by an unauthorized party. It ensures that data remains as it is from the sender to the receiver. If someone has added an extra bill to the envelope, which contained your credit card bill, he has violated the integrity of the mail.
- iii. **Availability:** It ensures you have access and are authorized to resources. If the post office destroys your mail or the postman takes one year to deliver your mail, he has impacted the availability of your mail.
- iv. **Nonrepudiation:** It ensures that e-commerce participants do not deny (repudiate) online actions.
- v. **Authenticity:** The identity of a person or entity with whom you are dealing on the Internet is identified.
- vi. **Privacy:** It ensures control over the use of information a customer provides about himself or herself to the merchant.

2.2 Security Features

While security features do not guarantee a secure system, they are necessary to build a secure system. Security features have four categories:

- i. **Authentication:** Verifies who you say you are. It enforces that you are the only one allowed to logon to your Internet banking account.
- ii. **Authorization:** Allows only you to manipulate your resources in specific ways. This prevents you from increasing the balance of your account or deleting a bill.
- iii. **Encryption:** Deals with information hiding. It ensures you cannot spy on others during Internet banking transactions.
- iv. **Auditing:** Keeps a record of operations. Merchants use auditing to prove that you bought specific merchandise.

3. Security Threats in E-commerce Environment

In a typical e-commerce experience, a shopper proceeds to a Website to browse a catalog and make a purchase.

This simple activity illustrates the four major players in e-commerce security.

One player is the shopper who uses his browser to locate the site. The site is usually operated by a merchant, also a player, whose business is to sell merchandise to make a profit.

As the merchant's business is selling goods and services, not building software, he usually purchases most of the software to run his site from third-party software vendors.

The software vendor is the last of the three legitimate players.

The attacker is the player whose goal is to exploit the other three players for illegitimate gains.

Following *figure* illustrates the players in a shopping experience.

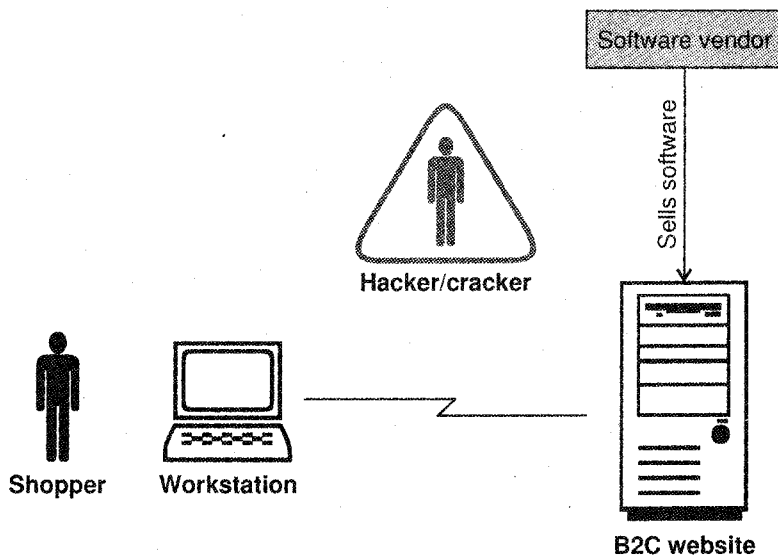


Figure 6.2

A threat is a possible attack against a system. It does not necessarily mean that the system is vulnerable to the attack.

Vulnerability is a weakness in the system, but it is not necessarily known by the attacker.

For example, only you know that you have left your front door unlocked. Vulnerabilities exist at entry and exit points in the system. In a house, the vulnerable points are the doors and windows. When the burglar threatens to break into your house and finds the vulnerability of the unlocked door, he is exploiting the assets in the house.

3.1 Points the Attacker can Target

The vulnerability of a system exists at the entry and exit points within the system. Several points that the attacker can target with e-commerce system are:

- i. Shopper
- ii. Shopper's computer
- iii. Network connection between shopper and Website's server
- iv. Website's server
- v. Software vendor

Most Common Security Threats in the E-commerce Environment:

- i. Malicious code (viruses, Trojans)
- ii. Unwanted programs (spyware, browser parasites)
- iii. Phishing/identity theft
- iv. Credit card fraud/theft
- v. Dos attacks
- vi. Insider attacks

4. Malicious Code and Unwanted Programs

Malicious code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system.

Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan horses, backdoors, and malicious active content.

A **computer virus** is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are man-made. A simple virus that can make a copy of itself over and over again is relatively easy to

produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

Since 1987, when a virus infected ARPANET, a large network used by the Defence Department and many universities, many anti-virus programs have become available. These programs periodically check your computer system for the best-known types of viruses.

A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs. These are designed to spread from computer to computer.

Trojan horse is a destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

The term comes from the Greek story of the Trojan War, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

4.1 Unwanted Programs

It is a program that may be unwanted, despite the possibility that users consented to download it.

It includes spyware, adware, and dialers, and is often downloaded in conjunction with a program that the user wants.

- i. **Spyware:** It is a software whose function includes the transmission of personal information to a third party without the user's knowledge and explicit consent.
- ii. **Adware:** It is a software whose primary function is to make revenue through advertising targeted at the person using the computer on which it is installed.
This revenue can be made by the vendor or partners of the vendor. This does not imply that any personal information is captured or transmitted as part of the software functioning, though that may be the case.
- iii. **Password crackers:** It is a software designed to allow a legitimate user or administrator to recover lost or forgotten passwords from accounts or data files.
When placed in the hands of an attacker, these same tools allow access to confidential information and represent a security and privacy threat.

- iv. **Backdoors:** These are programs that allow a third party attacker to access and, to some degree, control a machine remotely. Backdoors are largely Trojans and are dealt with correctly by most anti-virus products.
- v. **Dialers:** It is the software that redirects Internet connections to a party other than the users, default ISP for the purpose of securing additional connection charges for a content provider, vendor, or other third party.

Preventing malicious code and unwanted programs:

It should be one of the top security priorities for any e-commerce business.

- i. Make sure to install anti-virus programs, anti-spyware programs and firewalls on all computers and ensure that they are up-to-date and used properly at all times.
- ii. Make sure that all programs are in their most current version, including the programs listed above as well as any other operating systems and software.

5. Phishing and Identity Theft

Phishing refers to the act of obtaining victims' sensitive information by posing as trusted companies and organizations. It is usually carried out through spoofed e-mails and spoofed websites that urgently ask for various types of information. There are many potential threats, and identity theft is among the worst of them.

Phishing is a scam and a form of identity theft. It is used by a cyber-thief to steal your good name and credit rating. The term phishing is a clever variation on the word 'fishing.' The idea of the scam is that a bait is thrown out with the hopes that someone will be tempted into biting it.

Phishing is the method used to steal personal information through spamming or other deceptive means. There are a number of different phishing techniques used to obtain personal information from users. As technology becomes more advanced, the phishing techniques being used are also more advanced. To prevent Internet phishing, users should have knowledge of various types of phishing techniques and they should also be aware of anti-phishing techniques to protect themselves from getting phished.

5.1 Phishing Techniques

- i. **Web Based Delivery:** Web based delivery is one of the most sophisticated phishing techniques. Also known as 'man-in-the-middle', the hacker is located in between the original

Phishing Techniques are as follows:

- i. Web based Delivery
 - ii. Instant Messaging
 - iii. Trojan Hosts
 - iv. Link Manipulation
 - v. Key Loggers
 - vi. Session Hacking
 - vii. System Reconfiguration
 - viii. Content Injection
 - ix. Phishing through Search Engines
 - x. Phone Phishing
 - xi. Malware Phishing
 - xii. Malware Phishing
- website and the phishing system. The phisher traces details during a transaction between the legitimate website and the user. As the user continues to pass information, it is gathered by the phishers, without the user knowing about it.
- ii. Instant Messaging:** Instant messaging is the method in which the user receives a message with a link directing him/her to a fake phishing website which has the same look and feel as the legitimate website.
- If the user doesn't look at the URL, it may be difficult to tell the difference between the fake and legitimate websites. Then, the user is asked to provide personal information on the page.
- iii. Trojan Hosts:** Trojan hosts are invisible hackers trying to log into your user account to collect credentials through the local machine. The acquired information is then transmitted to phishers.
- iv. Link Manipulation:** Link manipulation is the technique in which the phisher sends a link to a website. When the user clicks on the deceptive link, it opens up the phisher's website instead of the website mentioned in the link. One of the anti-phishing techniques used to prevent link manipulation is to move the mouse over the link to view the actual address.
- v. Key Loggers:** Key loggers refer to the malware used to identify inputs from the keyboard. The information is sent to the hackers who will decipher passwords and other types of information. To prevent key loggers from accessing personal information, secure websites provide options to use mouse click to make entries through the virtual keyboard.
- vi. Session Hacking:** In session hacking, the phisher exploits the web session control mechanism to steal information from the user. In a simple session, hacking procedure known as session sniffing, the phisher can use a sniffer to intercept relevant information so that he or she can access the Web server illegally.
- vii. System Reconfiguration:** Phishers may send a message whereby the user is asked to reconfigure the settings of the computer. The message may come from a web address which resembles a reliable source.
- viii. Content Injection:** Content injection is the technique where the phisher changes a part of the content on the page of a reliable website. This is done to mislead the user to go to a page outside the legitimate website where the user is asked to enter personal information.
- ix. Phishing through Search Engines:** Some phishing scams involve search engines where the user is directed to products sites which may offer low cost products or services. When the user tries to buy the product by entering the credit card details, it's collected by the phishing site. There are many fake bank websites offering credit cards or loans to users at a low rate but they are actually phishing sites.

- x. **Phone Phishing:** In phone phishing, the phisher makes phone calls to the user and asks the user to dial a number. The purpose is to get personal information of the bank account through the phone. Phone phishing is mostly done with a fake caller ID.
- xi. **Malware Phishing:** Phishing scams involving malware require it to be run on the user's computer. The malware is usually attached to the e-mail sent to the user by the phishers. Once you click on the link, the malware will start functioning. Sometimes, the malware may also be attached to download files.

Phishers take advantage of the vulnerability of web security services to gain sensitive information which is used for fraudulent purposes.

- xii. **E-mail Phishing Scams:** A spoofed e-mail message is often the cornerstone of any well-executed phishing scam. From the earliest days of phishing, fraudulent e-mail messages have been used to catch Internet users unawares.

To this very day, major online entities like PayPal and eBay have to grapple with the problem of e-mail phishing. Several online banks have been targeted as well.

► **What is E-mail Phishing?**

E-mail phishing refers to the act of creating and sending fraudulent or spoofed e-mails with the goal of obtaining sensitive financial and personal information.

Under such schemes, e-mails are designed to look exactly like the ones that are sent by legitimate companies. Sophisticated phishing attacks use the e-mail addresses of people who are registered to use certain services.

When people receive e-mails that are supposed to be from those companies, they are more likely to trust them. Spoofed e-mails often contain links that lead to spoofed websites, where various methods are used to request and collect a person's financial and personal information. Forms are occasionally found within the e-mails.

► **Why E-mail Phishing Works**

Considering how long e-mail phishing has been used, it may seem odd that it continues to work. It isn't because people are foolish; it is because these e-mails are very well done.

Phishers know precisely how to design spoofed e-mails to look like their legitimate counterparts. By throwing in some urgent language, phishers dramatically increase their chances of success. Busy people scan such e-mails, trust them and click on their links because they look almost exactly like the real thing.

► **Signs of E-mail Phishing**

- i. There are many signs of a phishing e-mail.
- ii. The first thing that a User should look at is the greeting.

- iii. Does it use actual name, or does it have a generic greeting?
- iv. Look closely at the e-mail's header. What is the sender's e-mail address? These addresses are usually carefully designed to look authentic. By taking a very close look at them, though, a User can usually see inconsistencies and things that don't make sense. If possible, compare the sender's e-mail address to that of previous messages from the same company. If it's a phishing e-mail, the User will notice things that don't add up.

Examples of Successful E-mail Phishing

Many successful e-mail phishing attacks have been carried out in the past, which is why they continue to be used to this day.

Prominent examples include eBay phishing scams and PayPal phishing scams. Both companies were prime targets of e-mail phishing campaigns in the past.

eBay and PayPal users receive messages that look legitimate. The messages typically urge them to verify their account information or to update their credit card numbers. People often fall for these tactics because they are afraid of losing access to these important services. Both companies now offer extensive information on ways to avoid such phishing scams on their websites.

► **How to avoid E-mail Phishing?**

There is no simple way to completely avoid e-mail phishing attacks. The easiest way to avoid these scams is by never clicking on links that are included in e-mail messages. Make it a policy to always type in the URL of the site that you need to access manually. Upon arriving on the site, you will be able to confirm whether or not the message that you received was legitimate. If it's a spoofed e-mail, find out where to send it – most companies like to know about the scams that are going on out there.

How to Avoid Phishing?

- i. **Keep Informed about phishing techniques:** New phishing scams are being developed all the time. If you remain unaware about these new phishing techniques, you could inadvertently fall prey to one. Keep your self updated about new phishing scams. By finding out about them as early as possible, you will be at a much lower risk of getting trapped by one.
- ii. **Keep link clicking to a minimum:** It's fine to click on links when you're on trusted sites. Clicking on links that appear in random e-mails and instant messages, however, isn't such a smart move. Hyperlinks are commonly used to lead unsuspecting Internet users to phishing websites. Hover over links that you are unsure of before clicking on them. Do they lead where they are supposed to lead?
- iii. **Install an anti-phishing toolbar:** Most popular Internet browsers can be customized with anti-phishing toolbars.

- iv. **Verify a site's security:** When conducting online transactions, look for a sign that the site is secure, such as a lock icon on the browser's status bar or a 'https:' URL.
- v. **Check in with Your Online Accounts** regularly to ensure that no unauthorized transactions have been made.
- vi. **Keep Your Browser Up-to-Date:** Latest version of browser will be compatible for latest versions of websites.
- vii. **Use Firewalls:** Firewall is designed to prevent unauthorized access to or from a private network. It helps screen out hackers, viruses, and worms that try to reach your computer through the internet.
- viii. **Be Wary of Pop-Ups:** Pop-up windows often masquerade as legitimate components of a website. All too often, though, they are phishing attempts. Many popular browsers allow you to block pop-ups; you can allow them on a case-by-case basis. If one manages to slip through the cracks, don't click on the 'cancel' button; such buttons often lead to phishing sites. Instead, click the small 'x' in the upper corner of the window.
- ix. **Never give out personal information:** You never know who may gain access to your e-mail account.
- x. **Use Anti-virus software** and update it regularly to ensure that you are blocking new viruses and spyware.

6. Hacking and Cyber Vandalism

Cyber vandalism is a form of vandalism that is carried out, or committed, using a computer, and against electronic information. Specific cyber vandalism crimes include defacement of a website and denial of service attacks. Attacks of social media pages is also considered cyber vandalism, although content of social media updates may also contribute to cyber terrorism charges. There is a very fine line, in some cases between the two, so hackers and other cyber deviants should be wary of who they mess with, and what is said when they vandalize government websites.

Web vandalism is characterized by website defacement and/or denial-of-service attacks.

Website defacement is the most common form of web vandalism.

Website defacement is a major threat to many internet-enabled businesses. It negatively affects the public image of the company. Companies may suffer from loss of customers.

How does website defacement work?

- i. Find a username (e.g., by posing as an administrator and calling an employee; administrator information can be retrieved from database)
- ii. Retrieve the password for that username
- iii. Obtain administrative privileges
- iv. Begin defacing the website (and install a backdoor)

How to defend against website defacement?

- i. Avoid using the server as a client (e.g., web browser)
- ii. Remove buffer overflow vulnerabilities in your programs
- iii. Use a different user other than root for managing the website contents
- iv. Enable access logs
- v. Update

Hacker: Hacker is a term used by some to mean 'a clever programmer' and by others, especially those in popular media, to mean 'someone who tries to break into computer systems'.

1. Eric Raymond, compiler of The New Hacker's Dictionary, defines a hacker as a clever programmer. A 'good hack' is a clever solution to a programming problem and 'hacking' is the act of doing it. Raymond lists five possible characteristics that qualify one as a hacker, which we paraphrase here:
 - i. A person who enjoys learning details of a programming language or system.
 - ii. A person who enjoys actually doing the programming rather than just theorizing about it.
 - iii. A person capable of appreciating someone else's hacking.
 - iv. A person who picks up programming quickly.
 - v. A person who is an expert at a particular programming language or system.

Raymond disapproves the use of this term for someone who attempts to crack someone else's system or otherwise uses programming or expert knowledge to act maliciously. He prefers the term cracker for this meaning.

2. The term hacker is used in popular media to describe someone who attempts to break into computer systems. Typically, this kind of hacker would be a proficient programmer or engineer with sufficient technical knowledge to understand the weak points in a security system.

Hacking: Computer hacking is when someone modifies computer hardware or software in a way that alters the creator's original intent.

It refers to the hobby/profession of working with computers. It also refers to breaking into computer systems.

People who hack computers are known as hackers.

Hackers are usually real technology buffs who enjoy learning all they can about computers and how they work. Hackers think that what they do is like an art form.

They usually have expert-level skills in one specific program.

For most hackers, hacking gives them the opportunity to use their problem-solving skills and a chance to show off their abilities. Most of them do not wish to harm others.

7. Credit Card Fraud/Theft

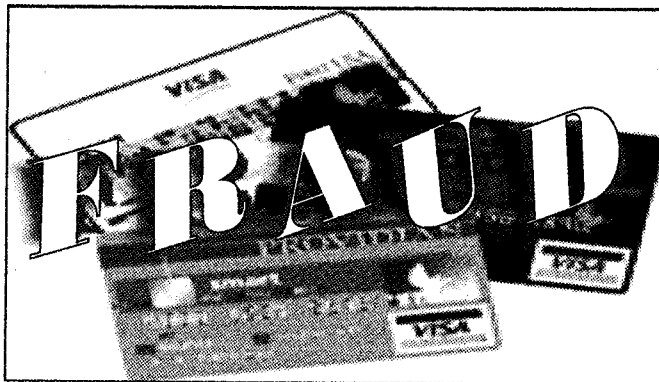


Figure 6.3

The popularity of online shopping is growing day by day. Due to a rapid advancement in the electronic commerce technology, the use of credit cards has dramatically increased.

As credit card becomes the most popular mode of payment for both online as well as regular purchase, cases of fraud associated with it are also rising.

Definition: The fraudulent use of a credit card account through the theft of the account holder's card number, card details and personal information, through a wide variety of methods in order to perform unauthorized transactions from the compromised account.

As the number of credit card users rises world-wide, the opportunities for attackers to steal credit card details and, subsequently, commit fraud are also increasing.

Credit-card-based purchases can be categorized into two types:

- i. Physical card
- ii. Virtual card

In a physical-card-based purchase, the cardholder presents his card physically to a merchant for making a payment.

To carry out fraudulent transactions in this kind of purchase, an attacker has to steal the credit card. If the cardholder does not realize the loss of card, it can lead to a substantial financial loss to the credit card company.

In the virtual card-based purchase, only some important information about a card (card number, expiration date, secure code) is required to make the payment.

Such purchases are normally done on the Internet or over the telephone. To commit fraud in these types of purchases, a fraudster simply needs to know the card details.

Most of the time, the genuine cardholder is not aware that someone else has seen or stolen his card information.

Credit card fraud is identity theft in its most simple and common form. It can happen when pre-approved credit card offers fall into the wrong hands.

All a person has to do is get these out of your mailbox (or trash can) and mail them in with a change of address request and start spending. Someone can even apply for a credit card in your name if they have the right information. You won't know a thing about it until the credit card company tracks you down and demands payment for the purchases 'you' have made.

With a person's name, social security number and date of birth, someone can get loans, access the person's existing bank accounts, open new bank accounts, lease or buy cars, get insurance, etc. Think about the things you throw in the trash. Take a look at some of the information on that seemingly unimportant piece of paper:

- i. Your full name
- ii. Your address
- iii. Your social security number
- iv. Your complete bank account number (if you have direct deposit)
- v. Your employer and its address
- vi. Your rate of pay

Now, think about the types of information you have to provide in order to get a credit card or a loan or lease a car. There is very little additional information that is needed in order to get that loan. It

would not have been that difficult to 'create' those documents using someone else's social security number, bank account numbers and other personal information.

► Credit Card Fraud Protection Tips

- i. Keep an eye on your credit card every time you use it, and make sure you get it back as quickly as possible. Try not to let your credit card out of your sight whenever possible.
- ii. Be very careful to whom you give your credit card. Don't give out your account number over the phone unless you initiate the call and you know the company is reputable. Never give your credit card information out when you receive a phone call. (*For example*, if you're told there has been a 'computer problem' and the caller needs you to verify information.) Legitimate companies don't call you to ask for a credit card number over the phone.
- iii. Never respond to e-mails that request you to provide your credit card information via e-mail -- and don't ever respond to emails that ask you to go to a website to verify personal (and credit card) information. These are called 'phishing' scams.
- iv. Never provide your credit card information on a website that is not a secure site.
- v. Sign your credit cards as soon as you receive them.
- vi. Shred all credit card applications you receive.
- vii. Don't write your PIN number on your credit card -- or have it anywhere near your credit card (in the event that your wallet gets stolen).
- viii. Never leave your credit cards or receipts lying around.
- ix. Keep a list in a secure place with all of your account numbers and expiration dates, as well as the phone number and address of each bank that has issued you a credit card. Keep this list updated each time you get a new credit card.
- x. Only carry around credit cards that you absolutely need. Don't carry around extra credit cards that you rarely use.
- xi. Always void and destroy incorrect receipts.
- xii. Never sign a blank credit card receipt. Carefully draw a line through blank portions of the receipt where additional charges could be fraudulently added.
- xiii. Never write your credit card account number in a public place (such as on a postcard or so that it shows through the envelope payment window).
- xiv. Ideally, it's a good idea to carry your credit cards separately from your wallet -- perhaps in a zippered compartment or a small pouch.
- xv. Never lend a credit card to anyone else.

8. Spoofing

The word 'spoof' means to hoax, trick, or deceive. Therefore, in the IT world, spoofing refers to tricking or deceiving computer systems or other computer users. This is typically done by hiding one's identity or faking the identity of another user on the Internet.

Spoofing is the action of making something look like something that it is not in order to gain unauthorized access to a user's private information.

The idea of spoofing originated in the 1980s with the discovery of a security hole in the TCP protocol. Today spoofing exists in various forms namely IP, URL and E-mail spoofing.

Spoofing is the creation of TCP/IP packets using somebody else's IP address. Routers use the 'destination IP' address in order to forward packets through the Internet, but ignore the 'source IP' address. That address is only used by the destination machine when it responds back to the source.

Spoofing is also used as a network management technique to reduce traffic.

For example, most LAN protocols send out packets periodically to monitor the status of the network. LANs generally have enough bandwidth to easily absorb these network management packets.

When computers are connected to the LAN over Wide-Area Network (WAN) connections, however, this added traffic can become a problem. Not only can it strain the bandwidth limits of the WAN connection, but it can also be expensive because many WAN connections incur fees only when they are transmitting data. To reduce this problem, routers and other network devices can be programmed to *spoof* replies from the remote nodes. Rather than sending the packets to the remote nodes and waiting for a reply, the devices generate their own *spoofed* replies.

Spoofing can take place on the Internet in several different ways.

One common method is through e-mail. E-mail spoofing involves sending messages from a bogus e-mail address or faking the e-mail address of another user. Fortunately, most e-mail servers have security features that prevent unauthorized users from sending messages. However, spammers often send spam messages from their own SMTP, which allows them to use fake e-mail addresses. Therefore, it is possible to receive e-mail from an address that is not the actual address of the person sending the message.

Another way spoofing takes place on the Internet via IP spoofing. This involves masking the IP address of a certain computer system. By hiding or faking a computer's IP address, it is difficult for other systems to determine where the computer is transmitting data from. Because IP spoofing makes it difficult to track the source of a transmission, it is often used in denial-of-service attacks that overload a server. This may cause the server to either crash or become unresponsive to legitimate requests. Fortunately, software security systems have been developed that can identify denial-of-service attacks and block their transmissions.

Finally, spoofing can be done by simply faking an identity, such as an online username. *For example*, when posting on a Web discussion board, a user may pretend he is the representative for a certain company, when he actually has no association with the organization. In online chat rooms, users may fake their age, gender, and location.

While the Internet is a great place to communicate with others, it can also be an easy place to fake an identity.

Types of Spoofing

- i. IP Spoofing
- ii. URL Spoofing
- iii. E-mail Spoofing

8.1 Types of Spoofing

- i. **IP Spoofing:** Internet Protocol (IP) is the protocol used for transmitting messages over the Internet; it is a network protocol operating at layer 3 of the OSI model.

IP spoofing is the act of manipulating the headers in a transmitted message to mask a hackers true identity so that the message could appear as though it is from a trusted source.

The hacker manipulates the packet by using tools to modify the 'source address' field. The source address is the IP address of the sender of the message. Therefore, once an intruder forges this address and the destination server opens up a connection, then numerous attacks can take place.

Attacks

- a. *Man-in-the-Middle attack:* In a Man-in-the-Middle attack, the message sent to a recipient is intercepted by a third-party which manipulates the packets and resends it own message.
- b. *Denial of Service (DoS) Attack:* A DoS attack is when an attacker floods a system with more packets than its resources can handle. This then causes the system to overload and shut down. The source address is spoofed making it difficult to track from where the attacks are taking place.

Solutions

IP spoofing can be prevented by monitoring packets using network monitoring software. A filtering router could also be installed, on the router an ACL (Access Control List) is needed to block private addresses on your downstream interface. On the upstream interface source address originating outside of the IP valid range will be blocked from sending spoofed information.

- ii. **URL Spoofing:** URL spoofing occurs when one website appears as if it is another. The URL that is displayed is not the real URL of the site, therefore the information is sent to a hidden web address.

Attacks

Intrusion: URL spoofing is sometimes used to direct a user to a fraudulent site and by giving the site the same look and feel as the original site the user attempts to login with a username and password. The hacker collects the username and password, then displays a password error and directs the user to the legitimate site.

Using this technique the hacker could create a series of fake websites and steal a user's private information unknowingly.

Solutions

Security patches are released by web browsers which add the feature of revealing the 'true' URL of a site in the web browser. It is important to check if your internet browser is vulnerable to perform the necessary updates.

- iii. **E-mail Spoofing:** Email spoofing is the act of altering the header of an e-mail so that the e-mail appears to be sent from someone else.

Attacks

- Cause confusion or discredit a person
- Social Engineering (phishing)
- Hide identity of the sender (spamming)

Recognize spoofed e-mail

Check the content of the e-mail:

- Is the content weird in some way, or really unexpected from the sender?
- Does it contain a form?
- Does it request to either confirm or update login or any kind of information?
- Check the header of the e-mail

9. Denial of Service (DOS)

A Denial of Service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have.

In a distributed denial-of-service, large numbers of compromised systems (sometimes called a bot net) attack a single target.

Although a DoS attack does not usually result in the theft of information or other security loss, it can cost the target person or company a great deal of time and money.

Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services.

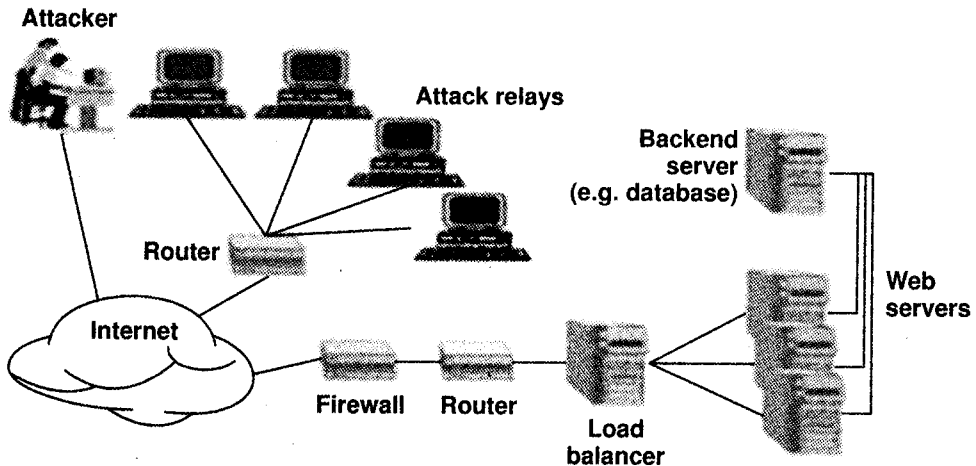


Figure 6.4

A denial of service attack can also destroy programming and files in affected computer systems. In some cases, DoS attacks have forced Websites accessed by millions of people to temporarily cease operation.

Examples of Denial of Service attacks launched against web applications include:

- Attempts to 'flood' web applications, thereby preventing legitimate user traffic
- Attempts to disrupt service to a specific system or person, e.g., blocking user access by repeated invalid login attempts resulting in the account's suspension
- Jamming the application-database connection by crafting CPU-intensive SQL queries

9.1 Risks Associated with Denial of Service Attacks

Denials of Service attacks are centered around the concept that by overloading a target's resources, the system will ultimately crash. In the case of a DoS attack against a web application, the software is overloaded by the attack and the application fails to serve web pages properly. To crash a web server running an application, a DoS threat attacks the following services:

- i. Network bandwidth
- ii. Server memory
- iii. Application exception handling mechanism

- iv. CPU usage
- v. Hard disk space
- vi. Database space
- vii. Database connection pool

In the past, Denial of Service attacks were thought to be a tool used by hacktivists as a form of protest. However, recent attacks have shown that Denial of Service attacks can also be a way for cyber criminals to profit.

By not proactively working to prevent DoS attacks, you leave your site vulnerable to:

- i. **Extortion:** Attackers threaten to continue disrupting service until payment is received.
- ii. **Sabotage:** Competing businesses attack websites to build a stronger market share.
- iii. **Brand damage:** Sites that are attacked find that their reputation is hurt by lack of uptime or the perception that the site is not secure.
- iv. **Financial losses:** Sites that are attacked are prevented from doing business online. The result is often a loss in sales revenue or advertising revenue.
- v. **Other attacks:** Information gathered from a successful Denial of Service attack can be used later to further attack a website. Additionally, other vulnerabilities may be used to launch a DoS attack providing the attacker with access to more than they had originally intended.

► How does an attacker launch a Denial of Service attack?

There are many different ways through which an attacker can launch a Denial of Service attack. They range from simply unplugging a server from the network (if they have physical access) to coordinating large armies of zombie computers to launch a large-scale distributed attack against their target using:

- i. Buffer overflows in the application functions.
- ii. Malformed data to raise unexpected exceptions.
- iii. Exploited race conditions in multi-threaded systems.
- iv. Heavy-duty SQL queries via web forms and 'spamming' them with requests, e.g., inserting % characters within search query fields.
- v. SQL Injection attacks executing recursive CPU-intensive queries.
- vi. The end users' web browsers to overload the application with parallel requests via persistent / reflected Cross-Site Scripting attacks.
- vii. Overly-complex regular expressions within search queries.
- viii. Excessively large files uploaded to the server.

There are several types of denial-of-service events.

- i. An exploitation of a vulnerability that causes a service or server to crash.
- ii. A flood of traffic that clogs up portions of a network.
- iii. A flood of specialized traffic that uses up resources on a service or server and causes it to go really slow.

While any activity that causes a service or server to crash is quite potent, the most common and most damaging attacks are types two and three, since they do not require an underlying vulnerability in a service or server in order to be successful.

Even if a system is fully patched, its ability to perform transactions can be negatively impacted or stopped by a type two or type three DoS attack. Type three attacks include methods such as the Ping Flood and the SYN Flood. Denial-of-service attacks that are generated by many computers operating in concert are called distributed denial-of-service (DDoS) attacks.

Common forms of Denial of Service attacks are:

Buffer Overflow Attacks

The most common kind of DoS attack is simply to send more traffic to a network address than anticipated by programmers who planned its data buffers. The attacker may be aware that the target system has a weakness that can be exploited or the attacker may simply try the attack, in case it might work. A few of the better-known attacks based on the buffer characteristics of a program or system include:

- i. Sending e-mail messages that have attachments with 256-character file names to Netscape and Microsoft mail programs.
- ii. Sending oversized Internet Control Message Protocol (ICMP) packets (this is also known as the Packet Internet or Inter-Network Groper (PING) of death).
- iii. Sending to a user of the Pine e-mail program a message with a "From" address larger than 256 characters.

SYN Attack

When a session is initiated between the Transport Control Program (TCP) client and server in a network, a very small buffer space exists to handle the usually rapid 'hand-shaking' exchange of messages that sets up the session. The session-establishing packets include a SYN field that identifies the sequence in the message exchange. An attacker can send a number of connection requests very rapidly and then fail to respond to the reply. This leaves the first packet in the buffer so that other, legitimate connection requests can't be accommodated. Although the packet in the buffer is dropped after a certain period of time without a reply, the effect of many of these bogus connection requests is to make it difficult for legitimate requests for a session to get established. In

Common forms of Denial Service attacks are:

- i. Buffer Overflow Attacks
- ii. SYN Attack
- iii. Teardrop Attack
- iv. Smurf Attack
- v. Viruses
- vi. Physical Infrastructure Attacks

general, this problem depends on the operating system providing correct settings or allowing the network administrator to tune the size of the buffer and the timeout period.

Teardrop Attack

This type of denial of service attack exploits the way that the Internet Protocol (IP) requires a packet that is too large for the next router to handle to be divided into fragments. The fragment packet identifies an offset in the beginning of the first packet that enables the entire packet to be reassembled by the receiving system. In the teardrop attack, the attacker's IP puts a confusing offset value in the second or later fragment. If the receiving operating system does not have a plan for this situation, it can cause the system to crash.

Smurf Attack

In this attack, the perpetrator sends an IP ping (or 'echo my message back to me') request to a receiving site. The ping packet specifies that it be broadcast to a number of hosts within the receiving site's local network. The packet also indicates that the request is from another site, the target site that is to receive the denial of service. (Sending a packet with someone else's return address in it is called spoofing the return address.) The result will be lots of ping replies flooding back to the innocent, spoofed host. If the flood is great enough, the spoofed host will no longer be able to receive or distinguish real traffic.

Viruses

Computer viruses, which replicate across a network in various ways, can be viewed as denial-of-service attacks where the victim is not usually specifically targeted but simply a host unlucky enough to get the virus.

Physical Infrastructure Attacks

Here, someone may simply snip a fiber optic cable. This kind of attack is usually mitigated by the fact that traffic can sometimes quickly be rerouted.

► The Need to Avoid Denial of Service Attacks

Denial of Service attacks is often random when they are launched against small and medium sized websites. When a website is attacked that does not fall into the category of a high profile target (large corporation, government site, or activist site), the reason usually falls within one or more of the following categories:

- i. **Grudge:** An unscrupulous competitor or disgruntled former business partner or employee may wish to cripple a business's Website for the purpose of financial gain or revenge.
- ii. **Name confusion:** The Website's name may closely resemble one used by a well-known enterprise or personality.

- iii. **Easy target:** Most mega-corporations have already installed anti-DoS safeguards - such as security technologies and extra server and connectivity power - on their sites. Smaller businesses, with fewer resources at their disposal, are tempting targets for DoS attackers, especially those looking to hone their skills.
- iv. **Bad luck:** Sometimes there's no apparent reason for a DoS attack. An attacker may simply pick a business's domain at random, or because they like the sound of its name or the way it looks. Attackers, by nature, can be highly irrational.

10. Distributed Denial-of-Service Attack (DDoS)

A Distributed Denial-of-Service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system is legitimate users.

In a typical DDoS attack, the assailant begins by exploiting vulnerability in one computer system and making it the DDoS master. The attack master, also known as the bot master, identifies and infects other vulnerable systems with malware. Eventually, the assailant instructs the controlled machines to launch an attack against a specified target.

There are two types of DDoS attacks:

- i. A network-centric attack which overloads a service by using up bandwidth
- ii. An application-layer attack which overloads a service or database with application calls.

The inundation of packets to the target causes a denial of service. While the media tends to focus on the target of a DDoS attack as the victim, in reality there are many victims in a DDoS attack -- the final target and as well the systems controlled by the intruder. Although the owners of co-opted computers are typically unaware that their computers have been compromised, they are nevertheless likely to suffer a degradation of service and not work well.

A computer under the control of an intruder is known as a zombie or bot. A group of co-opted computers is known as a botnet or a zombie army. Both Kaspersky Labs and Symantec have identified bot nets -- not spam, viruses, or worms -- as the biggest threat to Internet security.

In a distributed denial-of-service (DDoS) attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. He or she could then force your computer to send huge amounts of data to a website or send spam to particular e-mail addresses. The attack is 'distributed' because the attacker is using multiple computers, including yours, to launch the denial-of-service attack.

► How do you avoid being part of the problem?

Unfortunately, there are no effective ways to prevent being the victim of a DoS or DDoS attack, but there are steps you can take to reduce the likelihood that an attacker will use your computer to attack other computers:

- i. Install and maintain anti-virus software.
- ii. Install a firewall, and configure it to restrict traffic coming into and leaving your computer.
- iii. Follow good security practices for distributing your e-mail address
- iv. Applying e-mail filters may help you manage unwanted traffic.

► How do you know if an attack is happening?

Not all disruptions to service are the result of a denial-of-service attack. There may be technical problems with a particular network, or system administrators may be engaged in maintenance-work. However, the following signs *could* indicate a DoS or DDoS attack:

- i. Unusually slow network performance (opening files or accessing websites).
- ii. Unavailability of a particular website.
- iii. Inability to access any website.
- iv. Dramatic increase in the amount of spam you receive in your account.

► What do you do if you think you are experiencing an attack?

Even if you do correctly identify a DoS or DDoS attack, it is unlikely that you will be able to determine the actual target or source of the attack. Contact the appropriate technical professionals for assistance.

- i. If you notice that you cannot access your own files or reach any external websites from your work computer, contact your network administrators. This may indicate that your computer or your organization's network is being attacked.
- ii. If you are having a similar experience on your home computer, consider contacting your Internet Service Provider (ISP). If there is a problem, the ISP might be able to advise you on an appropriate course of action.

► Prevention of DoS and DDoS attacks

There are ways of preventing many forms of DoS attacks:

- i. **Determine the type of attack:** Analyze log files to determine that an attack is occurring and what is its nature.

- ii. **Prepare to change domain-name servers:** Go into the domain settings for your domain and set the TTL ('time to live') for your domain down to 300 seconds or less. This is a key preparatory step in the event you determine you need to move your site or re-route your traffic through a third party proxy server. A TTL of 300 seconds means that servers around the world would refresh your site's content every 300 seconds, which is very fast.
- iii. **Solicit help:** Get specialists from your server hosting company involved as quickly as possible to help analyze and protect against the attack.
- iv. **Determine if your site is the target:** If you are in a shared server environment, hopefully your provider has a good communication system to keep you informed. If the attack is network-wide, there is not much you can do. Do what you can to understand the attack and assess your options of moving forward. Find out if the attack is targeted toward your site or some other network resource.
- v. **Establish firewall settings:** If the attack is in the thousands of connections per hour, you might be able to combat it at the server level or firewall level. Installing some server modules or adding some firewall rules could be enough to keep your site hobbling along throughout the attack.
- vi. **Use professionals for large attacks:** If the attack is more at the level of hundreds of thousands or millions of connections per hour, you likely need to consider a third-party service. A Google search for 'DDoS mitigation' will present you with several options. Most of these solutions take the form of a proxy server that filters all traffic before it reaches your server. One of these services can often be configured within an hour. DDoS mitigation services can run in the thousands of dollars per incident. But they are typically quite effective at thwarting high-volume attacks.
- vii. **Monitor closely:** Once you have a protection in place, monitor the traffic and attack for changes. A protective layer in front of the website does not stop the attack from occurring; it just shields your site from the damaging traffic. In many cases the attack will subside in hours or days and you can eventually restore your server to its normal state of operation.
- viii. **Remember you customers:** Consider how to best communicate with your customers. Following up immediately with an explanation of the outage and a special 'attack coupon special' — or some other creative offering — can be a good way to restore customer faith.
- ix. **Review afterwards:** A DDoS attack can be traumatic. Once you have recovered technologically and emotionally, and while the attack is still fresh in your mind, review how the attack was carried out, how you and your support team responded, and what steps you would do differently in the event of another attack.

Summary

1. E-commerce is gaining momentum and acceptance; previously risky online activity such as banking is now considered safe and reliable. Yet, popular methods used to access sensitive information online present serious security risks.
2. Security has dimensions like Confidentiality, Integrity, Availability, Nonrepudiation, Authenticity, and Privacy.
3. Phishing is the method used to steal personal information through spamming or other deceptive means. There are a number of different phishing techniques used to obtain personal information from users. As technology becomes more advanced, the phishing techniques being used are also more advanced.
4. Cyber vandalism is a form of vandalism that is carried out, or committed, using a computer, against electronic information. Specific cyber vandalism crimes include defacement of a website and denial of service attacks.
5. **Spoofing** is the creation of TCP/IP packets using somebody else's IP address. Routers use the "destination IP" address in order to forward packets through the Internet, but ignore the "source IP" address. That address is only used by the destination machine when it responds back to the source.
6. A denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have.
7. In a distributed denial-of-service, large numbers of compromised systems (sometimes called a bot net) attack a single target.

EXERCISE

A. Short answers.

[Each 5 M]

1. Write short notes on:
 - a. Hacking and Cyber Vandalism
 - b. Unwanted Programs
 - c. Malicious Code

B. Long answers.

[Each 10 M]

1. Explain Security Threats in E-commerce Environment.

C. Descriptive questions.

[Each 15 M]

1. What is meant by Spoofing? Describe various types of spoofing.
2. Explain in detail the concept of credit card fraudulence.
3. Explain in detail the concept of Phishing techniques.

Suggestive Readings:

1. Au, Y.A. & Kauffman, R.J. (2007). The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application, *Electronic Commerce Research and Applications*
2. Engel-Flechsig, S. 2001. Securing the new global economy, *Mobile Commerce World*.
3. Tiwari, R., and Buse, S. 2007. *The Mobile Commerce Prospects: A strategic analysis of opportunities in the banking sector (PDF)*. Hamburg: Hamburg University Press.
4. Pandey, S. (2013, April 23). *Airtel Money*. (G. S. Sambhy, Interviewer) Mumbai, Maharashtra, India.
5. Pousttchi, K., Schiessler, M., & Wiedemann, D. G. (2007). *Analyzing the Elements of the Business Model for Mobile Payment Service Provision, Management of Mobile Business*.
6. Jaiswal, S. 2003. *Doing Business on the Internet: E – Commerce*. New Delhi: Galgotia Publications.
7. Joseph, P. T. 2004. *E-Commerce: An Indian Perspective*, 3rd edition. New Delhi: PHI Learning Pvt. Ltd.
8. Minoli, Daniel and Emma Minoli. 1998. *Web Commerce Technology Handbook*. New York: McGraw-Hill Osborne Media.
9. Agarwala, Kamlesh N., Amit Lal and Deeksha Agarwala. 2002. *Business on the Net: An Introduction to the ‘Whats’ and ‘Hows’ of e-commerce*. New Delhi: Macmillan Publishers India.
10. Bajaj, Kamlesh K. and Debjani Nag. 2005. *E-Commerce*. New Delhi: Tata McGraw-Hill Education.
11. Schneider, Gary P. 2008. *Electronic Commerce*, 8th edition. New Delhi: Cengage Learning