Recent Ammendments in IPCC Information Technology Syllabus

Free Online Ammendment Class On topics included will be held soon.

Date and time will be updated via CCI

Probable date between 14-16 December , 2012

By : VISHAL Email : cavidyamandir@gmail.com

Chapter 1

Unit 1- Introduction to computers - Deleted

Unit 2 – Input and Output Devices - Deleted

Deleted as per latest notification

(Now only Software part is in Syllabus)

Chapter 2

There are no changes in chapter 2

Chapter 3

Some Changes As per Last updated modules in September, 2012

Communication Channel (Medium) :

1. **Unguided Media :** Unguided Transmission Media also known as Unbound Media consists of a means for the data signals to travel, but nothing to guide them along a specific path. The data signals are not bound to a cabling system/media. Examples of unguided media are Radio wave, Microwave and Infrared wave.
   - **Radio Waves:** Radio waves are an invisible form of electromagnetic radiation that varies in wavelength from around a millimeter to 100,000 km. Radio waves are most commonly used transmission media in the wireless Local Area Networks.
   - **Micro Waves:** Microwaves are radio waves with wavelengths ranging from as long as one meter to as short as one millimeter, or equivalently, with frequencies between 300 MHz (0.3 GHz) and 300 GHz. These are used for communication, radar systems, navigation etc.
   - **Infrared Waves:** Infrared light (300GHz to 400 THz) is also used in the Wireless Local Area Networks. These networks are only limited within a room, as infrared light cannot pass through the walls. Another disadvantage of infrared light is that it can easily interfere with infrared radiations generated by sun.
     Infrared light is used in industrial, scientific, and medical applications. Night-vision devices using infrared illumination allow people or animals to be observed without the observer being detected. Infrared tracking, also known as infrared homing, refers to a passive missile guidance system which uses the emission from a target of electromagnetic radiation in the infrared part of the spectrum to track it.

Network Interface Devices :

1. **Modem :** Modem stands for Modulator/ Demodulator. It is defined as an encoding as well as decoding device used in data transmission. It converts the code format of computers to the code format of communication channels for transmission and then reverse the procedure when data is received. The communication channels include telephone lines, microwave links or satellite transmission.

   In clear words, **MODEM** is a device that converts a digital computer signal into an analog telephone signal (i.e. it modulates the signal) and converts an analog telephone signal into a digital computer signal (i.e. it demodulates the signal) in a data communication system. Modem allows the communication among computers through telephone lines. One of the greatest benefits of a modem is that it provides the ability to access remote computers

   - ***Types of MODEMs :*** *MODEMs are classified on the basis of different criterias, discussed as follows :*

     a. ***External vs. Internal Modems (on the basis of place where they are installed)***

     External Modem: It is separate from the computer system and is connected to the serial port of the computer by means of a cable. It is connected to the telephone jack by another cable and can be switched off or on easily in case of any problem. The lights on the external modem inform about the status of transmission of data.

     Internal Modem: An internal modem is a circuit board (a modem card) that can be added on one of the expansion slots on the motherboard. It is installed inside a desktop or laptop computer, allowing the computer to communicate over a network with other connected computers.

     b. ***Standard vs. Intelligent Modems (on the basis of the manner in which they accept information)***

     Standard Modems: These ar the most commonly used modems which are usually operated by commands entered from a microcomputer keyboard. The functions (dialing, etc.) are controlled by a user using different command languages. Most popular language in use is developed by a company "Hayes Microcomputer Products, Inc."

     Intelligent Modems: Intelligent modems also called Advanced modems can accept new instructions and then respond to the commands while transmitting data and information. This can be done by microprocessor chips and internal Read Only Memory (ROM) contained in the modem. As such, these modems are more expensive.

     c. ***Short-Haul and Wireless Modems (on the basis of the way the signals are transmitted)***

     Short-Haul Modems: Short-haul modems also called line drivers are devices that transmit signals via cables through any COM1 port. They sometimes are called modem eliminators, because they do not require an external power source. They can send data for a distance of more than one mile. This type of modem can be used within or across several buildings in a company or a university campus.

     Wireless Modems: Wireless also known as radiofrequency modem transmit the data signals through the air instead of by using a cable. It is designed to work with cellular technology, and wireless LANs. Wireless modems are not yet perfected, but the technology is rapidly improving.

Internal	External /Standard	Intelligent

Short Haul	Wireless

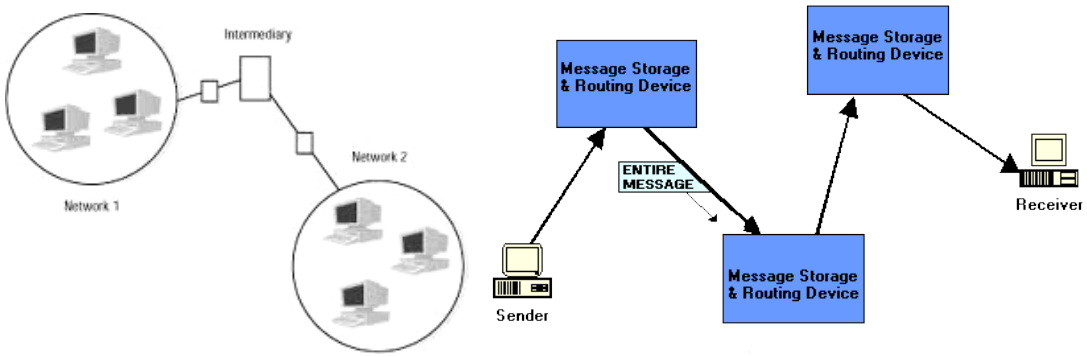
Transmission Techniques

A communication network consists of a collection of devices (or nodes) that wish to communicate and interconnect together. The primary objective is movement of information from one source to one or more destination nodes. Communication networks can be categorized based on technique of transfer into Broadcast and Switched networks.

In Broadcast networks, data is transmitted by one node to many or all of the other nodes.

In switched-communication networks, the data is transferred from source to destination and routed through the switch nodes. The way in which the nodes switch data from one link to another is referred to as a switching technique.

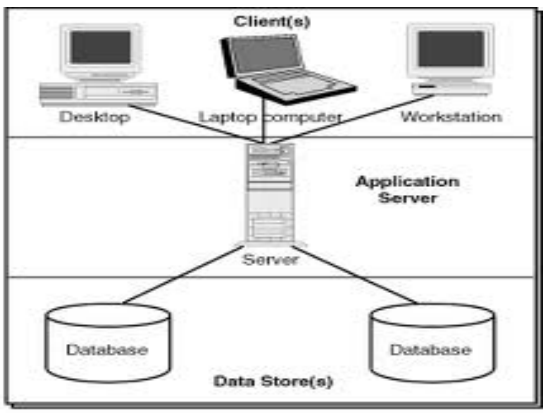
2. **Message Switch :** End-users communicate by sending message which contains the entire data to be delivered from the source to destination node. When a message is routed, intermediate switch within the network stores the entire message. If there is congestion or network resources are occupied, then inspite of discarding the traffic, the message-switched network will store and delay the traffic until sufficient resources are available for successful delivery of the message.
   There is no direct connection between the source and destination nodes. The intermediary nodes (switches) have the responsibility of conveying the received message from one node to another in the network. The process of storing all messages before retransmitting them one at a time as and when proper resources become available is often referred to as store-and-forward. It reduces the cost of transmission.
   Electronic mail (e-mail) and voice mail are examples of message switching systems. Today, message switching is used in many networks including satellite communications networks and and military networks.

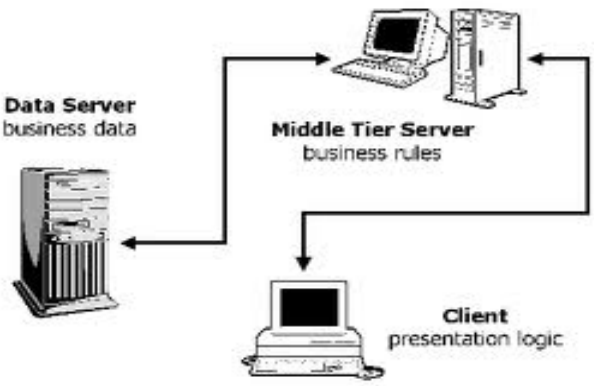


3-Tier Architecture :

Disadvantages

1. Increased need for network traffic management, server load balancing and fault tolerance.
2. Current tools are relatively immature and are more complex.
3. Maintenance tools are inadequate for maintaining server libraries which is a potential obstacle for simplifying maintenance throughout the organization





Features of Data Centers : 6-8 are new points

1. **Size :** Data Centers are characterized by the size of their operations. It can have hundred to several thousand servers. It would require a minimum area of approx. 5000 to 30000 Sq. Metres. It must have high quality construction to hold the weight of servers.
2. **Data Security :** Data Centers have maximum data security and alltime availability. They are protected from intruders with the help of firewalls & password/access rights and natural calamities like fire, flood and power failures. Security of data is also maintained by use of anti-virus software and proper backup/recovery procedures.
3. **Availability of Data :** The goal of the data center is to maximize the availability of data and to minimize downtime. Therefore, redundancy in connectivity, electrical supply and air conditioning is built in the data center.
4. **Electrical and Power systems :** Data Center has highest power availability using Uninterrupted Power supply (UPS).
5. **Physical security :** Physical security of data is maintained with the help of security guards, Biometric devices, Smart card and CCTVs.
6. **Backup Systems:** A data center should have the provision of automatically providing backup data services for all information resources. Full back up may be taken for full system restoration and off-site backup services should also be available as well.
7. **Continuous monitoring 24x7**: 24x7x365 monitoring must be there in data centers for the security of the data. Such a monitoring will be done for all the hardware including routers, switches, UPS systems and servers as well as for internet services.
8. **Environment – Cooling** : Cooling infrastructure is a significant part of a data center. The complex cooling infrastructure creates the optimal computing environment, ensuring the longevity of the servers installed within and also reduces the energy bill.

Protection Challenges and Best practice Solutions for Data Centres :

Large enterprise IT managers understand the criticality of data protection challenges and are looking for ways to mitigate the cost, risk and complexity of data protection throughout their enterprises — including data centers, disaster recovery sites etc. Some of the top challenges faced by large enterprise IT managers and the best practices for overcoming them are as follows:

1. **Control skyrocketing data growth :** Data growth is the biggest data center hardware infrastructure challenge for large enterprises. Several types of data deduplication technologies are used to reduce data storage needs by eliminating redundant data. Data deduplication also reduces the data that must be sent across a WAN for remote backups and disaster recovery.
2. **System performance and scalability :** Data Centers have to opt for the latest technology from time to time for better performance, keeping in mind that fast obsolecense of technology.
   IT managers should look ahead 3-5 years and choose a data protection "target" system that will match the performance and capacity they will need without adding new system images.
3. **Network congestion and connectivity architecture :** The new generation of servers with multicore processors demands significantly high input/output (I/O), and if these servers are virtualized, this requirement further goes up being the biggest data center infrastructure challenge. Vendors should help its customers to be strategic with their network infrastructure rather than continue to take a silo approach (confined).
4. **IT administration and staff time at premium :** IT administrators have more data to protect and more complex data protection standards to meet while staying within a limited budget. They need to invest in systems that reduce complexity and provide effective reporting.
   Minimum requirements for large enterprise data protection platforms include:
   - Automatic load balancing and tuning.
   - Automatic system monitoring.
   - Provide dashboards and reporting.
5. **Inadequate Disaster Recovery plans :** Large enterprises are using outdated backup solutions whch are particularly vulnerable to downtime and data loss in the event of a disaster.

   IT managers should consider the use of a consistent platform that enables IT staff to manage remote-office backup, deduplication and restore operations from a data center headquarters.
6. **Adopting new risk prone, cost-effective data protection technologies :** Managers have managed to protect their investment in existing technologies with limited budgets and resources. The cost and risk of migrating to a new technology competely often outweighs the potential benefits.

   IT managers should look for protection solutions that mitigate these costs and risk with features such as robust tape emulation and storage pooling.
7. **Resource balancing :** Thereis a need to strike a working balance between reduced operational budgets, increased demands on existing infrastructure, maximizing availability and the periodic upgrades required by today's technology.
   Best Solution is to host mission-critical and sensitive data with established data centers, where security concerns can be met and the technology and resources are already in place.

IDS Components

Intrusion Detection Systems are generally made up of following major components :

1. **Sensors:** These are deployed in a network or on a device to collect data. They take input from various resources, including network packets, log files, and system call traces. Input is collected, organized and then forwarded to one more analyzers.
2. **Analyzers:** Analyzers in IDS collect data forwarded by sensors and then determine if an intrusion has actually occurred. Output from analyzers should include evidence supporting the intrusion report. The analyzers may also provide recommendations and guidance on mitigation steps.
3. **User interface:** The user interface of the IDS provides the end users a view and way to interact with the system. Through the interface, the user can control and configure the system and generate reports as well.
4. **Honeypot**: In fully deployed IDS, some administrators may choose to install a "Honeypots", being system components, setup as bait for intruders. Honeypots can be used as early warning systems on an attack and data collection sources for attack analysis. Many IDS vendors maintain honeypots for research purposes and to develop new intrusion signatures

Threats and Vulnerabilities:

Threats

A threat is anything that can disrupt the operation, functioning, integrity, or availability of a network or system.
Network security threats can be categorized into four broad themes:

1. **Unstructured threats -** These originate mostly from inexperienced individuals using easily available hacking tools from the Internet. These include port-scanning tools, address-sweeping tools, and many others. Most of these kinds of probes are done more out of curiosity than with a malicious intent in mind.
2. **Structured threats -** These originate from individuals who are highly motivated and technically competent and usually understand network systems design and the vulnerabilities of those systems. They can understand as well as create hacking scripts to penetrate those network systems. Usually, these hackers are hired by organized crime, industry competitors, or state-sponsored intelligence organizations.
3. **External threats -** These originate from individuals or organizations working outside an organization, which does not have authorized access to organization's computersystems or network. They usually enter into a network from the Internet or dialup access servers.
4. **Internal threats -** These threats originate from individuals who have authorized access to the network. These users either have an account on a server or physical access to the network. An internal threat may come from a discontented former or current employee or contractor.

Vulnerabilities:

Vulnerability is an inherent weakness in the design, configuration, or implementation of a network or system that renders it susceptible to a threat.

The following facts are responsible for occurrence of vulnerabilities in the software:

1. **Software Bugs -** Software bugs are so common that users have developed techniques to work around the consequences. As such bugs that make necessary to save work every half an hour or crash the computer often are considered to be a normal part of computing. For example - buffer overflow, access validation error, input validation errors are some of the common software flaws.
2. **Timing Windows -** This problem may occur when a temporary file is exploited by an intruder to gain access to the file and use the file as a gateway for entry into the system.
3. **Insecure default configurations -** Insecure default configurations occur when vendors use known default passwords to make it easy for consumers to set up new systems. Unfortunately, most intruders know these passwords and can access systems effortlessly.
4. **Bad Protocols -** Some protocols, or the standards by which information is exchanged over the Internet, lack any security at all. For example, unsolicited commercial email, commonly referred to as "spam," is the irritating result of poor protocol programming.
5. **Trusting Untrustworthy information-** This is usually a problem that affects routers, or those computers that connect one network to another. When routers are not programmed to verify that they are receiving information from a unique/specific host only, bogus routers can gain access to systems and do damage.
6. **End users -** Generally, users of computer systems are not professionals and are not always security conscious. For example, when the number of passwords of a user increases, user may start writing them down and may keep them at a place where they are easy to find. Also saving confidential files to places where they are not properly protected.

DELETED PORTIONS :

3.8.2.1 Emergence of LANS
3.8.2.2 The concept of LAN
3.13.2 Technical details of 2 tier architecture
3.13.3 Why 3 tier architecture
3.14.4 Data centers - System Monitoring and support
3.14.6 Levaraging the best
3.14.7 Challenges faced ---- **CHANGED**
3.14.9 BCP
3.15.4 Threats and Vulnerabilities ---- **CHANGED**

Chapter 4

Some Changes As per Last updated modules in September, 2012

World Wide Web (WWW) : The World Wide Web (WWW) is most often called the Web. The Web is a network of computers all over the world that can communicate with each other using a communication standard called Hypertext Transfer protocol (http). The fundamental unit of the Web is the Web page which is defined as a text document that contains links to other Web pages, graphic and audio files, and other Internet services such as File Transfer Protocol (FTP) and E-mail.

Major components of WWW.

Major functional components of the WWW are discussed below:

1. **HTML (Hyper Text Markup Language) :** This language is used to create Web pages. HTML lets the creator of a Web page specify how text will be displayed and how to link to other Web pages, files and Internet services. These links are known as **hypertext links**, because they are activated when a user clicks on specific text or images within a Web page.
2. **HTTP :** All computers in the Web communicate with each other using a communication standard called Hypertext Transfer Protocol (HTTP). HTTP is defined as the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.
3. **URIs :** Uniform Resource Identifier (URI) is a string of characters used to identify a resource either by location, name or both. It enables interaction with resource over a network using specific protocols. URIs can be classified as names (URNs) and locators (URLs), or as both.
   - **URN :** A Uniform Resource Name (URN) is a specification of URI that identifies the resource by name ie. it functions like a person's name, and
   - **URL :** A Uniform Resource Locator (URL) is a specification of URI that defines the network location of a specific resource ie. it resembles to a person's street address. It is used to address and access individual Web pages and Internet resources. The format of a URL is: protocol/Internet address/Web page address. For example - http://www.icai.org/seminars.html
4. **Web Hardware and Software :** Web pages reside on servers that run special software that allow users to access Web pages and to activate links to other Web pages and to Internet services. Tens of thousands of Web servers are connected to the Internet. A user can directly access any Web page on one of these servers and then follow the links to other pages. This process creates a Web of links around the world and, thus, the name World Wide Web.
5. **Web client and Web Browser :** Computers reading the Web pages are called a Web Client. Web clients view the web pages with a program called a Web Browser. In other words, Software which is used in surfing of Internet is called web Browser. It is designed to enable users to access, retrieve and view documents and other resources on the Internet. The first such browser capable of displaying graphics within a Web page was Mosaic. Some of the popular browsers are Internet Explorer, Netscape Navigator, Mozilla Firefox etc. A browser fetches a Web page from a server by a request.

Search Engines : The World Wide Web (WWW) is "indexed" through the use of search engines. Search engines are programs that search documents on the web for specified keywords/text and returns a list of the documents where the keywords were found. Each search engine works in a different way. Some engines scans for information in the title or header of the document whereas others look at the bold "heading" on the page for their information. Since search engines gather information differently, each probably yields different results. Therefore, it's wise to try more than one search engine when doing Web searching. Some other popular search engines include Google (http://google.com/), Lycos (http://lycos.com/), Hot Bot (http://hotbot.com/), Yahoo (http://www.yahoo.com) etc.

Difference between Internet and WWW :

The Internet & the World Wide Web (the Web) are sometimes used interchangeably but are not same.

Internet is the hardware part - it is a collection of computer networks connected through either copper wires, fiber optic cables or wireless connections.

whereas, the World Wide Web can be termed as the software part – it is a collection of web pages connected through hyperlinks and URLs. In short, the World Wide Web is one of the services provided by the Internet. Other services over the Internet include e-mail, chat and file transfer services.

Major differences between Internet and WWW.

	Internet	***WWW***
Nature	Hardware	Software
Comprises of	Network of Computers, copper wires, fiber - optic cables & wireless networks	Files, folders & documents stored in various computers
Governed By	Internet Protocol	Hyper Text Transfer Protocol
Dependency	This is the base platform and is independent of WWW	It depends on the Internet to work

Various Protocols :

HTTP – Hyper Text Transfer Protocol:

The WWW is driven by two fundamental technologies : HTTP and HTML.

- HTTP is the Hypertext Transfer Protocol that controls how Web servers and Web browsers communicate with each other.
- HTML is the Hypertext Markup Language that defines the structure and contents of a Web page.

To retrieve a Web page, the browser sends a request to a Web server using HTTP. If we look up into the address bar of our web browser, the place where we type in the address that we have to visit, it has the prefix "http://" in front of the address.

On receiving the request, the server interprets it, sometimes using a CGI script and sends back data. This data can be just about anything, including HTML, text, images, programs, and sound.

Simple Mail Transfer Protocol :

The Simple Mail Transport Protocol (SMTP) controls the transfer of email messages on the Internet. It is a connection oriented, text-based protocol in which an e- mail sender communicates with a mail receiver by issuing command strings and supplying necessary data over a reliable data stream channel [TCP connection].

An SMTP session consists of commands originated by an SMTP client (sender) and corresponding responses from the SMTP server (receiver) so that the session is opened and session parameters are exchanged. A session may include zero or more SMTP transactions.

An SMTP transaction consists of three command/reply sequences as follows :

- MAIL command, to establish the return address.
- RCPT command, to establish a recipient of this message.
- DATA to send the message text. This is the content of the message. It consists of a message header and a message body separated by an empty line.
  DATA is actually a group of commands, and the server replies twice: once to the DATA command proper, to acknowledge that it is ready to receive the text, and the second time after the end-of-data sequence, to either accept or reject the entire message.

- **File Transfer Protocol (FTP):** The File Transfer Protocol (FTP) is used for transferring files to and from a remote host. FTP is commonly used for uploading pages to a Web site and for providing online file archives. An FTP URL has the basic form: ftp://user:pass@host/directory/file
  FTP distinguishes between text files and binary files. When transferring text files, FTP converts the line break characters. This is not desirable for binary files. FTP also allows us to append text and data to an existing file.

- **Network News Transfer Protocol (NNTP):** The Network News Transfer Protocol (NNTP) is the basis for tens of thousands of newsgroups that provide a public forum for millions of Internet users. NNTP consists of two components :
  list of newsgroups supported by a specific newsgroup server
  database of messages currently available for any particular newsgroup.

- **Common Gateway Interface (CGI):** The Common Gateway Interface is used with many Web servers to provide processing beyond the normal HTTP Web interface. CGI requests are submitted from Web browsers to Web servers. When a server receives a CGI request, it executes a script to process the request and return a result to the browser.

- **Transmission Control Protocol (TCP):** TCP corresponds to the transport layer (Layer 4) of the OSI reference model. It provides reliable transmission of data in an IP environment. TCP provides various services like stream data transfer, reliability, efficient flow control and multiplexing.

- **Internet Protocol (IP):** The Internet Protocol (IP) is a network-layer (Layer 3) protocol that contains addressing and control information that enables packets to be routed.

- **VoIP (Voice over Internet Protocol):** Voice over IP (VoIP) refers to the communication protocols, technologies, methodologies and transmission techniques involved in -
  the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. Other terms commonly associated with VoIP are IP telephony, Internet telephony etc.

- **Address Resolution Protocol (ARP):** The Address Resolution Protocol is a request and reply protocol that runs encapsulated by the line protocol. It is communicated within the boundaries of a single network, never routed across internetwork nodes. For two machines on a given network to communicate, they must know the other machine's physical (or MAC) addresses. By broadcasting Address Resolution Protocols (ARPs), a host can dynamically discover the MAC-layer address corresponding to a particular IP network-layer address.

- **Internet Control Message Protocol (ICMP):** The Internet Control Message Protocol (ICMP) is a network-layer Internet protocol that provides message packets to report errors and other information regarding IP packet processing back to the source.

- **User Datagram Protocol (UDP):** The User Datagram Protocol is another transport layer protocol that provides a connectionless method of communicating between machines. It allows us to send datagrams, packets between machines.
  UDP is simpler, but unreliable. There is no guarantee that a packet will ever reach its destination. In addition, UDP has no flow control. If we send messages too quickly, packets may be lost.

  Definition: *A datagram is an independent, self-contained message sent over the network whose arrival, arrival time, and content are not guaranteed*

- **Telnet:** Telnet is a protocol that allows us to connect to remote computers (called hosts) over a TCP/IP network (such as the Internet). A software called a telnet client (eg. Tera term, Putty) on our computer is used to make a connection to a telnet server (i.e., the remote host). Once our telnet client establishes a connection to the remote host, our client becomes a virtual terminal, allowing us to communicate with the remote host from our computer. In most cases, we will need to log into the remote host, which requires that we have an account on that system.

TYPES OF ELECTRONIC PAYMENTS :

1. **Credit Cards :** In credit card transaction the consumer presents the credit card to the merchant for the payment of dues. Merchant confirms the utility of credit card online from the consumer bank & prepares a slip for signing by the consumer. The Merchant uses this slip to collect the funds from the bank and on the next billing cycle, Consumer gets his credit card statement mentioning this purchase transaction. Credit cards can also be used for making purchases through internet.

How a credit card is processed?

Step 1 : Authorization –

The cardholder requests a purchase from the merchant. After a merchant swipes the card, the data is submitted to merchant's bank, called an acquirer, to request authorization for the sale. The acquirer then routes the request to the cardissuing bank, where it is authorized or denied based on valid credit available and on getting authorisation the merchant is allowed to process the sale.

Step 2 : Batching –

At the end of a day, the merchant reviews all the day's sales to ensure they were authorized and signed by the cardholder, stores all authorised sales in a batch and transmits them at once to the acquirer to receive payment.

Step 3 : Clearing –

After the acquirer receives the batch, it sends it through the card network and each sale is routed to the appropriate issuing bank. The issuing bank subtracts its interchange fees, which are shared with the card network, and transfers the remaining amount through the network back to the acquirer.

Step 4 : Funding –

After receiving payment from the issuer, the acquirer subtracts its discount fee and sends the remainder to the merchant. The merchant is now paid for the transaction, and the cardholder is billed.

Terms Defined

Acquirer : A bank that processes and settles a merchant's credit card transactions with the help of a card issuer.

Cardholder : The owner of a card that is used to make credit card purchases.

Card network : Visa, MasterCard or other networks that act as an intermediary between an acquirer and an issuer to authorize credit card transactions.

Discount fee : A processing fee paid by merchants to acquirers to cover the cost of processing credit cards.

Interchange fee : A charge paid by merchants to a credit card issuer and a card network as a fee for accepting credit cards. They generally range from 1 to 3 percent.

Issuer : A financial institution, bank, credit union or company that issues or helps issue cards to cardholders.

Secure Electronic Transaction (SET) Standard

When credit card is used on the Internet, added steps must be taken to provide for secure transactions and authentication of both buyer and seller. To address the growing security concerns and help growth of electronic commerce on the net, the two leading credit card brands, Visa and MasterCard, developed a common standard to process card transactions on the Internet called the Secure Electronic Transaction (SET) standard.

Objectives of SET

SET is a standard which ensure that credit card and associated payment order information travels safely and securely between the various involved parties on the Internet. SET addresses seven major business requirements :

1. Provide confidentiality of payment information and order information that is transmitted along with the payment information.
2. Ensure the integrity of all transmitted data.
3. Provide authentication that a cardholder is a legitimate user of a branded payment card account.
4. Provide authentication that a merchant can accept branded payment card transactions through its relationship with an acquiring financial institution.
5. Ensure the use of the best security practices to protect all legitimate parties in an electronic commerce transaction.
6. Create a protocol that neither depends on transport security mechanisms nor prevents their use.
7. Facilitate and encourage interoperability among software and network providers.

Cryptography :

SET principally uses **cryptography** which is defined as the science of encrypting messages, that is, converting clear text to cipher text using an algorithm, and then converting it back from cipher text to clear text using the same or another algorithm.

Secret Key Cryptography (SKC) and Public Key Cryptography (PKC) are two common encryption methods.

- In Secret key Cryptography (also called Symmetric Key Cryptography), the sender uses a single 56-bit key (also called a symmetric key) to encrypt information, and the receiver will use the same key to decrypt.
- A Public Key Cryptography (PKC), also known as Asymmetric Key Cryptography is much more secure and sophisticated encryption method which uses two keys. Any one key (it does not matter which) can be used to encrypt and the other can be used to decrypt.

Certifyng Authorities :

When two parties start communicating, each wants to be sure about the authenticity of each other's public keys. To resolve this, trusted third parties also called Certifying Authorities (CAs) are used. A Certifying Authority could be a financial institution, a government body, an international body or a card brand (such as Visa or MasterCard). A CA would create a digital document containing the entity's details and public key and then sign it. This digital document is called a Digital Certificate.

In case the sender or receiver does not know of the existence of (does not trust) the certifying authority itself, SET mandates the establishment of a hierarchy of trust. This means that the CA itself will be trusted by a parent CA, which in turn will be trusted by another CA until it goes to a root CA which is trusted by everybody.

E-Commerce Risk and Security Considerations :

Due to expansion in use of e-commerce there is a need to develop methods of ensuring its safety and effective use. There are inherent risks associated with using the Internet as a primary means of conducting business transactions and those risks must be addressed and corrected.

The different dimensions of E-commerce security are as follows :

1. ***Integrity*** **-** The ability to ensure that information being displayed on a web site or transmitted or received over the internet has not been altered in any way by an unauthorized party.
2. ***Non-repudiation*** **-** The ability to ensure that e-commerce participants do not deny (i.e. repudiate) their online actions.
3. **Authenticity -** The ability to identify the identity of a person or entity with whom we are dealing in the internet.
4. ***Confidentiality*** - The ability to ensure that messages and data are available only to those who are authorized to view them.
5. ***Privacy*** **-** The ability to control the use of information about oneself.
6. ***Availability*** **-** The ability to ensure that an e-commerce site continues to function as intended.

Additional concerns about initiating electronic commerce on the Internet must be addressed before these businesses are ready to take the "electronic push :

1. **Reliability** - The availability of the service level that the company depends upon to conduct business anytime.
2. **Scalability** – The ability to scale the Internet and individual services in order to meet the needs and expectations of all businesses.
3. **Ease of use** – The methods to be developed to promote easy access and use to all potential trading partners.
4. **Payment methods** – The evolving of an appropriate, safe and reliable payment method for electronic commerce.

Concerns about the vulnerability of the Internet :

- threat of computer viruses.
- information passed through e-mail can be intercepted bringing risk to both parties.
- information stored online are subject to tampering and possible damage.
- Financial information such as credit card numbers may be stolen and used by unauthorized parties to make illegal purchases, resulting in damage to customers and businesses alike.
- Due to data sharing, the possibility of data exposure to vendors, service providers, and trading partners is significantly increased.

DELETED PORTIONS :

1. Electronic Data Interchange
2. Transactions using Third party Verifications
3. Joint Electronic Transaction (JET)
4. Risk and Security Considerations – **CHANGED**

   General manaement Concerns – **DELETED**

Free Online Ammendment Class of above topics will be held soon.

Date and time will be updated via CCI