Unit 8
Data communication and computer Network

Data communication is the physical transfer of data over a physical or radiator media.

Basic parts of a data communication system

- Source - Generate information to send.
- Transmitter - Convert the information for sending over the medium.
- Communication medium - The medium which is used to transmit.
- Receiver - Convert to information which was in medium compatible.
- Destination – The ultimate receiver.

Protocols

Protocols are digital rules that are used to send message among computers. This process has two parts.

1. Synchronization (SYN)
2. Acknowledgement (ACK)

Signals

Information can be transmitted over a medium by changing a physical property. There are two types of signals.

1. Analog (Continuous) signals.
2. Digital (Discreet) signals.

Analog signals

A continuous signal that changes its amplitude continuously with time.

Digital signals

A discreet signal that keep the amplitude at a constant level.

Communication Method

1. Manual Communication Methods
   Cave drawing, Messenger Birds, Arrows, etc.
2. Modern Communication Methods
   - Telephone- Transmit and receive voice over a pair of copper wires as electricity.
   - Radio/TV - Uses radio/magnetic waves to transmit audio/video signals.
   - Satellite - Uses microwave to connect between earth station.
   - Integrated Services Digital Network – Used to provide higher data rates through a telephone network for business application before ADSL.
   - Asymmetric Digital Subscriber Line (ADSL/DSL) - Uses the telephone line to transmit high speed data.
   - Code division multiple access (CDMA) - Multiple digital signals are sent over a same frequency at the same time.
   - General Packet Radio Service (GPRS) - It adds packet capability (Data) to GSM.
   - Global system for mobile communication (GSM) - It uses a subscriber identity module (SIM).

Modulation Techniques

This is the process of encoding source data into a carrier signal.

Properties of signal

1. Amplitude (A) - The strength of a wave at a given time.
2. Frequency - Is the rate at which a signal pattern repeats.
3. Wavelength - Distance between repeating units of a wave.
4. Phase - Is a definition of the position.

Two type of modulation techniques.

1. Analog signal modulation.
2. Digital signal modulation.

Analog Signal Modulation

1. Amplitude modulation (AM) - The carrier signals amplitude is changed according to variation of original signal.
2. Frequency Modulation (FM) - The carrier signals frequency is changed according to variation of modulating signal.
3. Phase Modulation (PM) - The carrier signals phase is changed according to modulating signal.

Digital Signal Modulation

1. Amplitude shift keying (ASK) - Two different amplitudes are used to represent 0 and 1.
2. Frequency shift keying (FSK) - Two or more frequencies are used to represent 0 and 1.
3. Phase shift keying (PSK) - Carrier wave is systematically shifted 0 or 180^{O} degrees at each symbol period.

Analog to Digital Modulation

Pulse code modulation (PCM) - Commonly used to convert analog signal to digital signal. PCM has following 3 phases.

1. Sampling
2. Quantizing
3. Encoding

Sampling - The voice send over the telephone falls within the limits 0.3 kHz-3.4 kHz it is generally taken as 0.4 kHz.

Quantizing - Each sample is calculated into a specific level so that it can be encoded.

Encoding - The quantized sample is then encoded using 8 bits.

Multiplexing

Multiplexing is the technique used to send multiple signal over the same medium at same time. 3 types

1. Frequency division multiplexing (FDM)
2. Time division multiplexing (TDM)
3. Code division multiplexing (CDM)

Frequency division multiplexing (FDM) - Used to divide the total bandwidth available in a communication medium into a series of non-overlapping frequency.

Time division multiplexing - Time sharing among source signals using around robin technique to send the signal over a single medium. Most used in digital telephone.

Code division multiplexing - Form of spread spectrum which narrow band signal is spread over a wider frequency band. Popularly known as CDMA.

Transmission mediums

1. Guided media (wired) - Use a physical medium
2. Radiator/Unguided media (wireless)

Guided Media

1. Twisted pair cable - Consist two insulated copper wires. Twisting reduce interference. Used for building communication and telephone networks.
    a. Unshielded twisted pair
    b. Shielded twisted pair
2. Coaxial Cable - A center conductor is shielded and out of the shield there is a braided outer conductor.
3. Fiber Optic - Transmit data based on total internal reflection.

Unguided Media

Data transmitted over air.

1. Radio transmission - Can work with or without line off sight.
2. Satellite transmission - Used to link ground station.
3. Terrestrial Microwave - Uses radio frequency to establish connection. (1GHz- 170GHz)
4. Intrawave - signals are sent from an infrared LED and received by a photo diode.

Transmission Impairments

Transmission lines get distorted due to transmission impairments. There are 3 types of impairment.

1. Attenuation
2. Distortion
3. Noise

Attenuation

- The signal becomes weaker over distance.
- Affects intelligibility of the received signal.

Distortion

- Signals changes its form or shape.
- The shape of the composite signal is therefore not the same.

Noise

Insertion of unwanted signals into the transmission signal.

- Thermal Noise - Caused by the thermal. Always present in electronic circuit and also called white noise.
- Intermodulation noise - When multiplexing different signals could mix and produce new signal.
- Crosstalk - Unwanted coupling between signals.
- Impulse noise - That may cause by lightning or electrical load variations.

Computer Networks

Two or more computing devices connected via a form of communication technology is a computer network.

Advantages

- Can share resources.
- Can establish communication facilities.
- Remote information access.
- Centralized Control.
- Expensive to establish and manage.
- If central device fail whole network is fail.
- Special skills and training required to maintain.

Connection Types

- Point-To-Point - Provides a dedicated link between two devices.
- Multipoint - Single link shared among several devices.

Classification of networks

Based on geographical distance.

- ✓ Local Area Network - Connects a set of devices in a small geographical area.
- ✓ Metropolitan Area Network - Extended over an entire city.
- ✓ Wide Area Network - Large geographical area.

Network Topologies

- ❖ Star
    - Better performance
    - Easy to maintain
    - Centralized management
    - Centralized device failed whole network is down
    - Central device is expensive.
    - Nodes are limited by central device.
- ❖ Bus
    - Less cables
    - Less expensive
    - Suitable for small networks
    - If main cable fails whole network is fail
    - Difficult to detect problem
    - Less security
- ❖ Ring
    - Data is sent only one node at a time
    - Less collusion
    - No need central device
    - Each data passes through all nodes
    - If one node fails the whole network is affected
    - Highly depends on wire
- ❖ Tree
    - Expansion is easy
    - Network divisions can be controlled easily
    - If one damaged it doesn't affect to network
    - Depends on main bus cable
    - Maintenance is difficult
    - Troubleshooting is difficult
- ❖ Mesh
    - Data can be transmitted simultaneously
    - If one cable fail it doesn't affect to network
    - High security
    - Cost is high
    - Setup and maintenance is difficult
    - Adding a computer is hard

VPN

VPN is technique used for sending data securely over internet through a tunnel.

Network Modules

1. Peer to peer – Each computer acts as both client and server.
2. Client Server Network – Provide a service is known as a server. And requester is known as a client. Server is a powerful machine that share resources with clients.

Network Commands

Ping- Check the connectivity to a device or computer.
Hostname – Shows the host name of the computer.
IPconfig – Display current network setting.
NSLookup – Looks the IP address of a domain.

ISO-OSI 7 Layer Remembering Song

All **P**eoples **S**eems **T**o **N**eed **D**ata **P**rocessing

ISO-OSI 7 Layer Architecture

Open system international model defines a 7 layers to a networking framework to implement protocols and devices.

1. Application – 7th layer provides application services for file transfer and other network software.
2. Presentation – Translating application layer data into network layer compatible data.
3. Session – Establish, manage, and terminate connection between applications.
4. Transport – Provides transparent transfer of data between systems or hosts.
5. Network – Provides switching and routing technologies. Create logical path to send data.
6. Data link – Data packets are encoded and decoded into bits.
    - Media Access Control Layer (MAC)
    - Logical link control layer (LLC)
7. Physical – Physical devices on the network.

Datagrams in 7 layers

Upper Layer Data	Application Presentation Session
Segments	Transport
Packets	Network
Frame	Data link
Bits	Physical

Addresses

3 types on addresses related to computer networks.

1. Port Address – An Interface on a computer which identifies the type of service.
2. Logical Address – The IP is an identifier for a device on the TCP/IP network.
3. Physical Address – The hardware address that uniquely identify each node of a network.

Networking Devices

- Repeater – Used to regenerate or replicate a signal. Operates in physical layer.
- Hub – Used for connecting segments or nodes. Operates in physical layer.
- Bridge – A device that connects two LAN's or two segments of same LAN. Operate in data link layer.
- Switch – Filters and forwards packets between LAN segments. Operate in data link layer.
- Router – Forwards data packets between different networks. Used to connect LAN to WAN. Operate in network layer.
- Gateway – Serves as an entrance to another network. Operates in transport and application layer.

TCP/IP Models

TCP/IP is a collection of communication protocols used to connect hosts in the internet.

TCP/IP vs OSI

<table>
<tr><td>Application</td><td rowspan="3"></td><td rowspan="3">Application</td></tr>
<tr><td>Presentation</td></tr>
<tr><td>Session</td></tr>
<tr><td>Transport</td><td></td><td>Transport</td></tr>
<tr><td>Network</td><td></td><td>Internet/Network</td></tr>
<tr><td>Data link</td><td rowspan="2"></td><td rowspan="2">Network Access</td></tr>
<tr><td>Physical</td></tr>
</table>

OSI Model Internet Model

Application layer

Defines TCP/IP protocols and how host program interface with the transport layer services to use the network.

Transport Layer

Provide communication sessions management between host computers.

Internet layer

Packages data into IP datagrams.

Network access Layer

Specifies details how data is physically sent through the network.

- A protocol is a set of rules agreed by both ends.

IEEE 802.3/Ethernet

- Station sends a link before start to transmission (Carrier Signal – CS)
- Multiple pc's access media at different time (Multiple Access - MA)
- Station monitors the medium to see if transmission is successful (Collusion Detection – CD)
- If collusion detected station stops transmission.
- Retransmit if the medium is free.

IEEE 802.5 token ring (Physical Layer)

A token ring network is a local area network (LAN) topology where nodes/stations are arranged in a ring topology.

Internet Protocol (Network Layer)

- IP format of packets are called datagrams.
- Most networks combined IP with transmission control protocol.(IP/TCP)

Transmission Control Protocol – TCP (Transport Layer)

- TCP enable to establish a connection and exchange streams of data.
- TCP guarantees the delivery of data.
- Connection is established between client and server.
- Error control and flow control can be done.
- Data transfer is reliable.

User Datagrams Protocol – UDP (Transport Layer)

- Connection less.
- Data will go through the network and reach the server.
- The server doesn't send any acknowledgement.
- Primarily used for broadcasting messages over a network.

Internet control message protocol (ICMP) (Network Layer)

ICMP is an extension to the internet protocol and it supports packets containing error control information messages.

Address Resolution Protocol (ARP) (Network Layer)

ARP is used to convert IP address into a physical address and is known as MAC address.

Application Layer Protocol

Dynamic Host Configuration Protocol (DHCP)

DHCP protocol used to assign dynamic IP addresses to a device on a network.

Domain Name Server (DNS)

An internet service that translate domain name into IP address.

TELNET

The telnet protocol is used for remote login.

File Transfer Protocol (FTP)

Protocol used for exchanging files over the internet. FTP uses TCP/IP protocol to enable data transfer.

Trivial File Transfer Protocol (TFTP)

TFTP is a file transfer protocol which is simple in nature and uses UDP than TCP and user authentication is not required.

Simple Mail Transfer Protocol (SMTP)

A protocol used to send email between servers.

Post Office Protocol v3 (POP3)

Protocol used to retrieve email from server.

Simple Network Management Protocol

A set of protocols for managing complex networks

Hyper Text Transfer Protocol (HTTP)

HTTP is protocol used by WWW. HTTP defines how messages are forwarded and transmitted. HTTP doesn't remember previous commands. S-HHTP is another version of HTTP and is used to send data securely.

Client-Server Architecture

1. Web server – Web servers are computers that deliver web pages and it has an IP address and possibly a domain name. Any computer can be turned into web server by installing server software.
2. Mail server – An email server acts as a virtual post office service and internal space is required to store emails.
3. Proxy server – A proxy server acts as an intermediary for requests from clients and checks if it can fulfill the requests itself.
    a. Improve performance by providing faster service.
    b. Filter requests for restricted websites.
4. Application server – Application server handles all application operations between users.
5. DNS server – DNS is an internet service that translate domain into IP addresses.

Leased Lines

A permanent telephone line between two points to connect geographically distance offices.

IP Addresses

- IP addresses are used to identify a computer on the network.
- Worldwide IP addresses are assigned by Internet Assigned Number Authority (IANA).
- Asia Pacific Network Information Center (APNIC) decide IP address range for Sri Lanka.
- Two versions of IP
    - IPv4 – Uses 32 binary bits separated into 4 groups each having 8 bits and the 8 bits known as an octet.

      Eg: 192.168.100.1
    - IPv6 – Uses 128 binary bits and expressed by 8 groups of hexadecimal numbers separated by columns.

      Eg: 2001:cdba:0000:0000:0000:3132:4365:fedc
- IPv6 was introduced because of the limitation of capacity in IPv4

Network ID and Host ID

The IP address consist of two sections.

1. Network ID – Defines the network within internet.
2. Host ID – Identifies the computer within the network.

IP address classes

Class	First Octet Range	Max Hosts
A	1 – 126	16 Million
B	128 – 191	64 Thousand
C	192 – 223	254
D	224 – 239	N/A
E	240 - 254	N/A

- Class D IP addresses are used for multicasting purpose.
- Class E IP addresses was set aside for experimental use and reserved for future use by IANA.

Private IP addresses

Used to identify a computer in a private network. These can be repeated within private networks.

Class	IP range
A	10.0.0.0 – 10.255.255.255
B	172.016.0.0 – 172.31.255.255
C	192.168.0.0 – 192.168.255.255

IP sub-netting

Sub-netting enables the host part of the IP address to be divided to create smaller network called subnet. Depending on the number of subnets require the network part borrows bits from host part of the IP.

- The number of subnets that is created is calculated from the following expression.

2^n-2 ("n" is the number of bits borrowed from the host side.)

Subnet Mask

The subnet mask is the network address plus the bits reserved for identifying the sub network.

The Internet

The Internet is a global, interconnected computer network in which every computer connected to it can exchange data with any other connected computer.

The Internet's History

Significant events in the history of the Internet.
1962- J.C.R. Licklitерconceives of the idea of a "Galactic network".
1969 – ARPANET goes online, connecting four computers.
1972 - Ray Tomlinson invents e-mail.
1983 - Internet protocols begin.
1989 - The World Wide Web is developed.
1994 - The first graphical Web browser is developed.
1995 - Barriers to commercial activity are lifted.

Hosts

A computer that is connected to a TCP/IP network, including the Internet. Each host has a unique IP address.

Internet Service Provider (ISP)

A company that provides Internet services, including personal and business access to the Internet. ISPs provide the following types of Internet connections

- Dial-up Connections
- Broadband Connections
- Internet Leased Lines

ISPs are connected to each other through Network Access Points (NAP)
Examples: SLT, Dialog, Etisalat, Lankacom, Suntel

Internet Backbone

The Internet consists of main cables which connect the main nodes (or segments) of the globally distributed network. Such Bus cables are known as Backbones.

Bandwidth

The amount of data that can be transmitted within a unit time. For digital devices, including the Internet, the bandwidth is usually expressed in bits per second (bps) or bytes per second.

Internet Usage

According to statistics the growth rate of the Internet users have been more than 500% from 2000 –2012.

Internet Technologies

The suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP.

During the 1980s the **TCP/IP Protocol suite** was introduced by **Winton Cerf** and **Robert Khan,** which laid the foundation to the modern Internet.

Internet Protocol

IP specifies the format of packets, also called datagrams, and the addressing scheme. IP by itself is something like the postal system. It allows you to address a package and drop it in the system, but there's no direct link between you and the recipient.

Transmission Control Protocol (TCP)

Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data (Acknowledgement) and also guarantees that packets will be delivered in the same order in which they were sent. (Synchronization)

Intranet

A network based on TCP/IP protocols (an internet) belonging to an organization, usually a corporation, accessible only by the organization's members, employees, or others with authorization. An intranet's Web sites look and act just like any other Web sites, but the firewall surrounding an intranet fends off unauthorized access.

Extranet

An intranet that is partially accessible to authorized outsiders. Whereas an intranet resides behind a firewall and is accessible only to people who are members of the same company or organization, an extranet provides various levels of accessibility to outsiders. You can access an extranet only if you have a valid username and password, and your identity determines which parts of the extranet you can view.

Routing

The process of moving a packet of data from source to destination is called routing. Routing is usually performed by a dedicated device called a router. Each intermediary computer performs routing by passing along the message to the next computer until it reaches its destination marked by the IP address. Part of this process involves analyzing a routing tabletop determine the best path at a given time. Because the traffic patterns change with time, packets may take different routes to reach the destination.

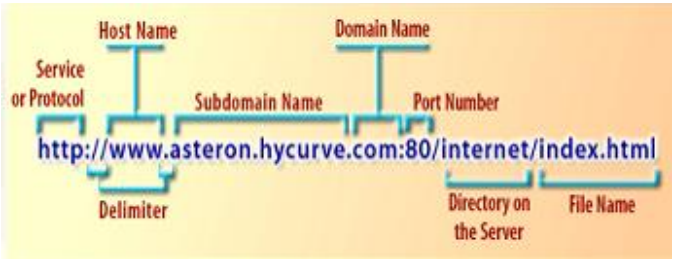
Packet switching

Introduced by **Leonard** Kleinrock. Which was later extended into a communication technique over the network by **Paul Baran**. Messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination.

Once all the packets forming a message arrive at the destination, they are recompiled into the original message. Most modern Wide Area Network (WAN) protocols, including TCP/IP, X.25, and Frame Relay, are based on packet-switching technologies. Packet switching is known as a connection-less method of communication, as opposed to the PSTN with circuit switching where connection-oriented method is used.

URLs

Uniform **R**esource **L**ocator (URL) it is the global address of documents and other resources on the World Wide Web.



Cookies and Sessions

A **Cookie** is a message given to a Web browser by a Web server. The browser stores the message in a text file. The message is then sent back to the server each time the browser requests a page from the server. The main purpose of cookies is to identify users and possibly prepare customized Web pages for them. A **Session** is a cookie that is erased when the user closes the Web browser. The session cookie is stored in temporary memory and is not retained after the browser is closed. Session cookies do not collect information from the user's computer.

IETF

Short for **I**nternet **E**ngineering **T**ask **F**orce, the main standards organization for the Internet. The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.

Services provided over the Internet

- World Wide Web
- Email
- File transferring
- Chatting
- Electronic funds transfer (EFT)
- E-commerce
- Content Streaming

WWW

A system of Internet servers that support specially formatted documents. The documents are formatted in a markup language called HTML (Hypertext Markup Language) that supports links (hyperlinks) to other documents, as well as graphics, audio, and video files. Pages containing such links are called hyper media. This means you can jump from one document to another simply by clicking on hot spots. World Wide Web is **not** synonymous with the Internet.

Web Browsers

A software application used to locate, retrieve and also display content on the World Wide Web, including Web pages, images, video and other files. As a client/server model, the browser is the client run on a computer that contacts the Web server and requests information. Many browsers offer plug-ins which extend the capabilities of a browser so it can display multimedia information (including sound and video) Mobile browsers are typically "stripped down" versions of Web browsers and offer fewer features in order to run well on mobile devices.

Services on the WWW

- Newsgroups
- Portals
- Blogs
- VoIP
- Social Networking

Newsgroups

Same as forum, an on-line discussion group. On the Internet, there are literally thousands of newsgroups covering every conceivable interest. To view and post messages to a newsgroup, you need a news reader, a program that runs on your computer and connects you to a news server on the Internet.

Eg: Google Reader
News Crawler

Portals

A Web portal or public portal refers to a Web site or service that offers a broad array of resources and services, such as e-mail, forums, search engines, and online shopping malls.
Eg: www.gov.lk

Blogs

Short for We**b log**, a blog is a Web page that serves as a publicly accessible personal journal for an individual. Typically updated daily, blogs often reflect the personality of the author.

VoIP

Short for **V**oice **o**ver **I**nternet **P**rotocol, a category of hardware and software that enables people to use the Internet as the transmission medium for telephone calls by sending voice data in packets using IP rather than by traditional circuit transmissions of the PSTN.

There are many Internet telephony applications available. Some, like Cool Talk and NetMeeting, come bundled with popular Web browsers. Others are stand-alone products. VoIP also is referred to as Internet telephony, IP telephony, or Voiceover the Internet (VOI)

W3C

Short for *World Wide Web Consortium,* an international consortium of companies involved with the Internet and the Web. The W3C was founded in 1994 by Tim Berners-Lee, the original architect of the World Wide Web. The organization's purpose is to develop open standards so that the Web evolves in a single direction rather than being splintered among competing factions.

Computer Security

Common Vulnerabilities

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privileges
- Phishing
- Port Scans

Spoofing

- A technique used to gain unauthorized access to computers by fooling network hardware and software. The intruder sends a message to a computer with a different IP address indicating that the message is coming from a trusted host.
- Newer routers and firewall arrangements can offer protection against IP spoofing

Tampering

- Also known as parameter tampering.
- A form of Web-based attack in which certain parameters in the Uniform Resource Locator (URL) or Web page form data entered by a user are changed without the user's authorization.

Repudiation

- Repudiation is the denying of a communication or data transfer between two parties. A data or message sent by one party may not be acknowledged as received by the receiving party even though the message or data has been received.

Information Disclosure

- Disclosing (revealing) sensitive information of a person or an organization without their knowledge.

Denial of Service

- Also known as DOS attacks.
- A type of attack on a network that is designed to bring the network to a congested state by flooding it with useless traffic.
- There are different types of DOS attacks such as the Ping of Death and teardrop attacks, which exploit the limitations in the TCP/IP Protocol.

Elevation of Privileges

- Bugs in certain software may enable a lower-end user to gain access to content which is usually accessible by a higher end user such as an application developer or a system administrator.

Phishing

- Misleading a user by sending emails or directing to web sites where they are asked to update personal information such as passwords, credit card or bank account numbers that the original (legitimate) organization already has.
- These websites are bogus (false) and set up only to steal the information the user enters on the page.

Port Scan

- Scanning a computer's ports to gain access to a computer through a weak point. A port is a place where information goes into and out of a computer.
- Types of port scans
    - Vanilla
    - Strobe
    - Fragmented Packets
    - UDP
    - Sweep
    - FTP Bounce
    - Stealth Scan

Types of attacks

- Hackers and Crackers
- Espionage
- Eavesdropping
- Man in the middle attacks
- IP Session Hijacking

Hackers and Crackers

- Hackers are individuals or teams that use their extensive knowledge in computing to gain unauthorized access in a sneaking manner. This is not done with a harmful purpose in mind, and they are more interested in gaining knowledge about computer systems
- Crackers are computer experts who break into security systems to cause harm and damage to computer systems.

Espionage

Also known as cyber spying, this describes the stealing of secrets stored in digital formats or on computers and IT networks.

Eg:

- Gauss (2012) in Middle East.
- Stuxnet (2010) in Iran.
- Flame (2012) in Iran.
- DuQu (2011)

Eavesdropping

- Network Eavesdropping or network sniffing is a network layer attack consisting of capturing packets from the network transmitted by others' computers and reading the data content in search of sensitive information like passwords, session tokens, or any kind of confidential information.

Man-in-the-middle attack

- Abbreviated as MITM, a man-in-the-middle attack is an active Internet attack where the person attacking attempts to intercept, read or alter information moving between two computers.
- MITM attacks are associated with 802.11 (WLAN) security, as well as with wired communication systems.

IP Session Hijacking

- A security attack on a user session over a protected network. There are two types of session hijacking.
    - ❖ IP Spoofing
    - ❖ Man in the middle attacks
- This is possible because the authentication takes place at the beginning of communication. Once the connection is established, an intruder can send packets and issue commands to the two ends pretending to be authentic commands.

Types of Malware

- Short for malicious software, malware refers to software designed specifically to damage or disrupt a system
- There are several types of malware
    - ❖ Viruses
    - ❖ Hoaxes
    - ❖ Worms
    - ❖ Trojans
    - ❖ Blended Threats
    - ❖ Spams
    - ❖ Spyware

Virus

- A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels.
- Viruses cannot be spread without a human action.
- The damages done can vary depending on the type of virus.

Hoaxes

- In e-mail terms, a hoax is a message which is written to purposely spread fear, uncertainty and doubt. In some cases websites may be attached to prove these false claims.

Worms

- Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action.
- Since worms spread in masses, networks and web servers can be congested and may result in DOS.
- Some advanced types of worms create tunnels in security so that outsiders can gain remote access to a computer system (Eg: Blaster).

Trojans

- The Trojan horse, at first glance will appear to be useful software but will actually do damage once installed or run on your computer.
- Trojans are also known to create a backdoor on a computer system that gives malicious users access to the system.
- Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate.

Blended Threats

- A blended threat is a more sophisticated attack that bundles some of the worst aspects of viruses, worms,
- Trojan horses and malicious code into one single threat.
- Blended threats are considered to be the worst risk to security since the inception of viruses, as most blended threats also require no human intervention to propagate

Spams

Spam is unsolicited (unwanted) emails. Most often these are electronic junk mail or unwanted newsgroup postings or sometimes emails advertising for some product sent to a mailing list or newsgroup.

Spyware

- Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes.
- Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet

Security precautions: Physical Security

- Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution.
- This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism.
- Protection from attackers and natural disasters multiple locks, fencing, walls, fireproof safes, and water sprinklers
- Surveillance and notification systems lighting, heat sensors, smoke detectors, intrusion detectors, alarms, and cameras apprehend attackers and recover quickly.

Security precautions: Software Security

- Encryption
- Antivirus Software
- Firewalls and Proxy servers
- Patches and Updates
- Authentication
- Access Control
- Disable unused Interfaces
- Honeypots and Sugarcanes.

Encryption

- The translation of data into a secret code
- To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.
    - ❖ Plain text - Unencrypted data
    - ❖ Cipher text - Encrypted data
- Uses two types of keys
    - ❖ Public key - known to everyone
    - ❖ Private key - known only to the recipient

Antivirus Software

- An antivirus program is a utility, which scans hard disk drives for viruses, worms and Trojan horses and removes, fixes or isolates any threats that are found.
- Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses.

Firewalls

- A firewall is a system designed to prevent unauthorized access to or from a private network.
- All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.
- Firewalls can be hardware or software

Proxy Servers

- A server that sits between a Web browser, and web server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server.
- Proxy servers can also be used to filter requests. For example, a company might use a proxy server to prevent its employees from accessing a specific set of Web sites.

Patches and Updates

- When a software has a bug or a loophole which can become a security threat, a fix called a patch is released by the software company.
- A patch is an actual piece of object code that is inserted into (patched into) an executable program.
- Updates of programs will have bug fixes and patches and are usually available over the internet for free.

Authentication

- The process of identifying an individual, usually based on a username and password.
- In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity.
- Authentication only ensures that the individual is who he or she claims to be.

Access Control/Authorization

- Refers to mechanisms and policies that restrict access to computer resources. Usually this is done by maintaining a list called the ACL.
- The ACL (access control list), is a set of data that informs a computer's operating system which permissions, or access rights, that each user or group has to a specific system object.
- Each object has a unique security attribute that identifies which users have access to such as read, write or execute.

Disabling unused interfaces

- These interfaces refer to the services provided by routers.
- By default, routers come with a lot of services pre-enabled. Which may create a path for intruders to get in to the system.
- It is necessary to disable these unused interfaces by the system administrator to ensure the security.

Honey pots & sugarcanes

- An Internet-attached server that acts as a trap, attracting in possible hackers in order to study their activities and monitor how they are able to break into a system.
- Honeypots are designed to imitate systems that an intruder would like to break into but limit the intruder from having access to an entire network.
- A honeypot that tricks as an open proxy is known as a sugarcane.