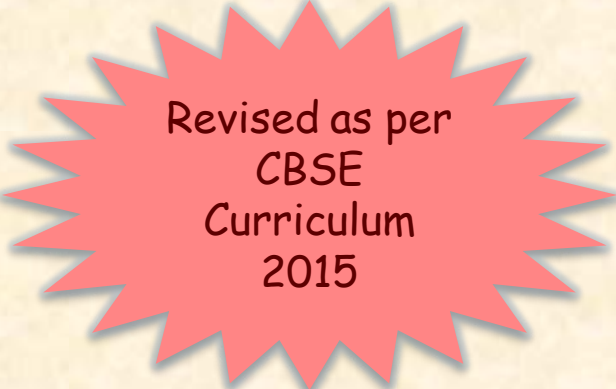


Chapter 2:

Software Concepts

Informatics Practices
Class XI (CBSE Board)



Revised as per
CBSE
Curriculum
2015

"Open Teaching-Learning Material"



Visit www.ip4you.blogspot.com for more....

Authored By:- Rajesh Kumar Mishra, PGT (Comp.Sc.)
Kendriya Vidyalaya Upper Camp, Dehradun (Uttarakhand)
e-mail : rkmalld@gmail.com

Learning Objectives

In this presentation, you will learn about-

- ❑ Hardware & Software
 - ❑ Types of Software
 - ❑ System Software
 - ❑ Application Software
 - ❑ Relationship between Hardware, Software & User
 - ❑ Introduction to System Security
 - ❑ Security Threats
 - ❑ Security Tools
 - ❑ Cyber Crime & Cyber law
 - ❑ Social Networking
-

Hardware and Software

- ❑ The **physical (tangible) components** of a computer like Monitor, Keyboard, CPU etc. are called Hardware.
- ❑ **Software** represents a set of programs that **governs the operation of a computer** and make the hardware functional.
- ❑ Hardware alone can not work unless we have some instructions for its working. The relation between hardware and software is similar to body and soul i.e. a body (hardware) is nothing without soul (software).



Types of Software

A computer software can be divided into two categories depending upon their uses and role.

❑ System Software:

The software that controls internal operation of computer is called **System Software**.

- It helps to read data/instructions from Input device.
- Process and displays result on the output devices.
- Controls all devices attached to computer system.

Example : Operating System, Compilers, Interpreters etc.

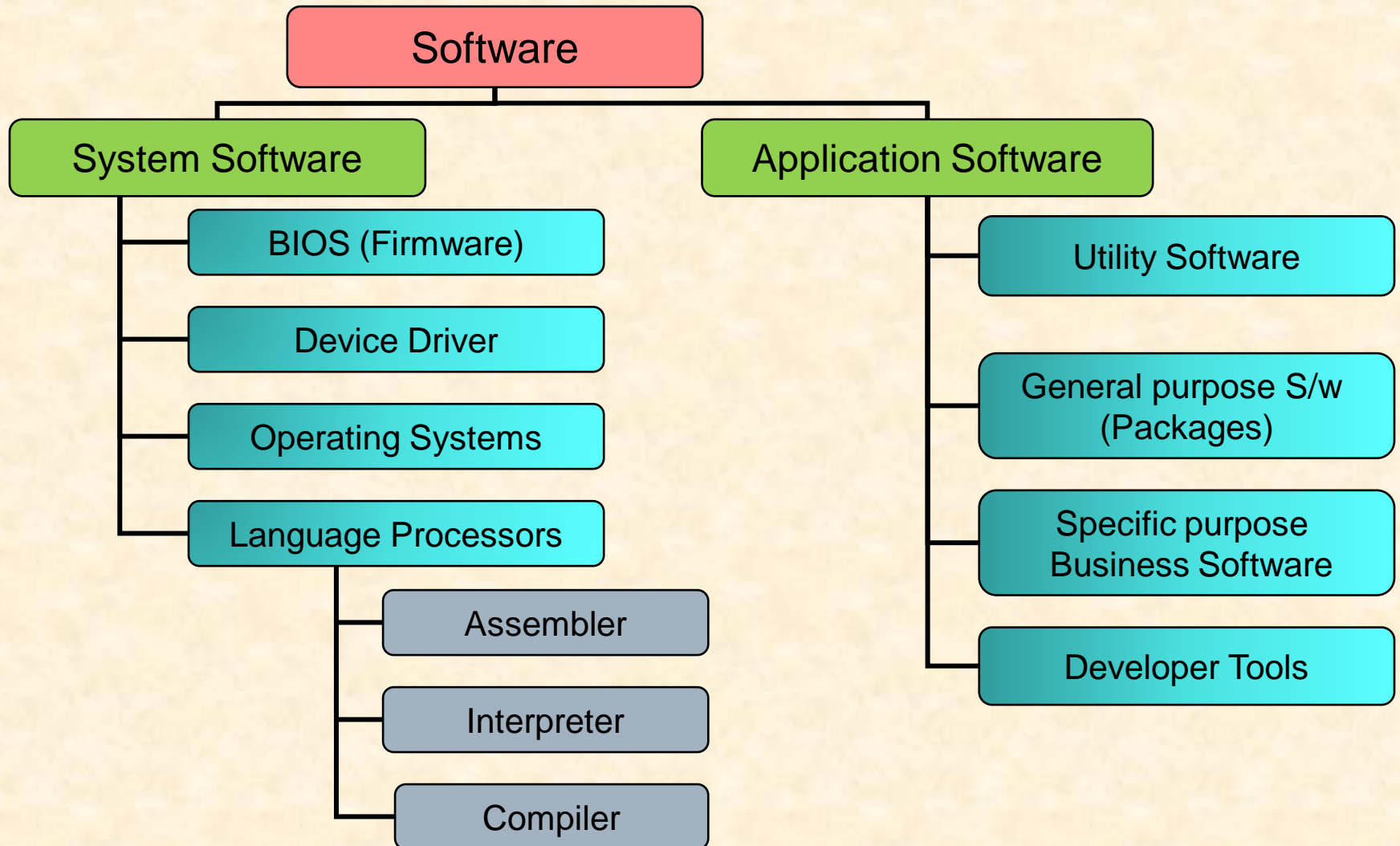
❑ Application Software:

The software that carry out operations for a specified application is called **Application Software**.

It helps to perform only one specific job like Library Management, Railway Reservation or Word Processing etc.

Example: MS Word, MS Excel, Utility Software etc.

Types of Software



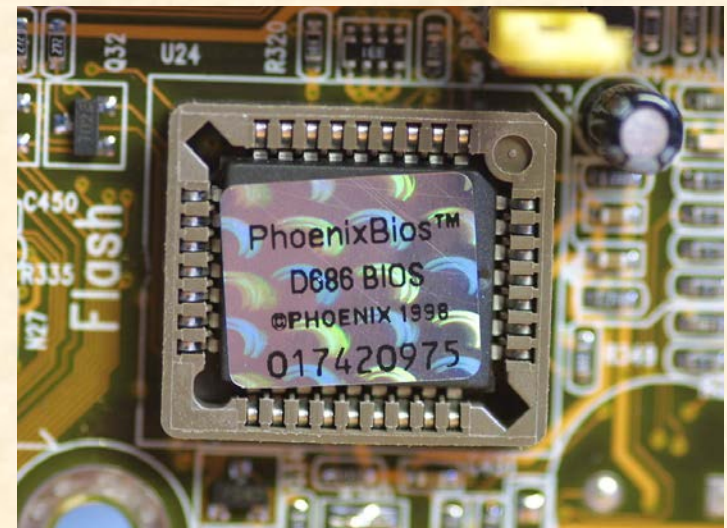
BIOS (Basic Input-Output System)

BIOS is a small, firmware (provided by the manufacturer) that controls various I/O devices (peripherals) attached to computer.

The main function of BIOS are-

- It perform **POST** (Power On Self Test) function i.e. initial checking and initializing system devices like RAM, Hard disk and other I/O devices, when computer is powered on.
- It starts **Booting** process i.e. loads Operating System from Secondary memory (Hard disk) to Primary memory (RAM).

BIOS program is provided by the computer manufacturer (Firmware) in a small Chip called BIOS chip attached to Mother Board.



Device Driver Program

A Device Driver is a system software that acts as an interface between the Device and the User or Operating System.

Some devices like Printer, Scanner, Web Camera etc. come with their own driver software given in CDs. These Drivers to be installed in the PC for proper working of the device.

Most of the small devices like Keyboard, Mouse, Pen Drive, CD Drive etc. are Plug & Play, because their Driver programs are already installed with Operating System.

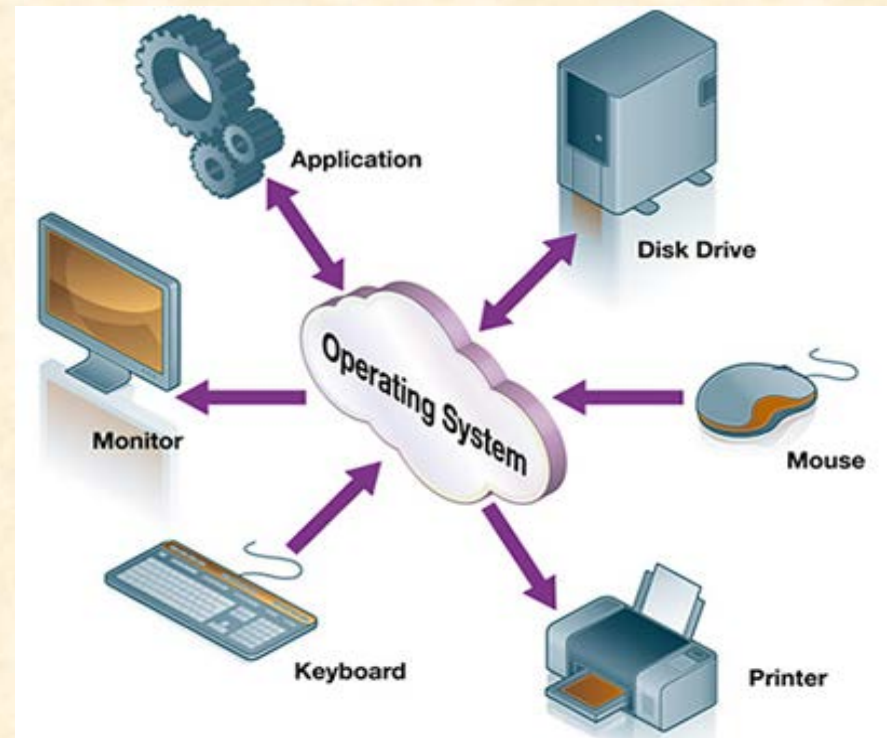


Operating System

An Operating System (**OS**) is a system program that controls and coordinates the operations of a computer system.

Operating system is also called **Resource Manager** and acts as an **Interface** between user and machine (hardware)

Example: Microsoft Windows, Mac OS, Solaris, Android, Linux, Ubuntu, Apple's i-Phone OS etc.



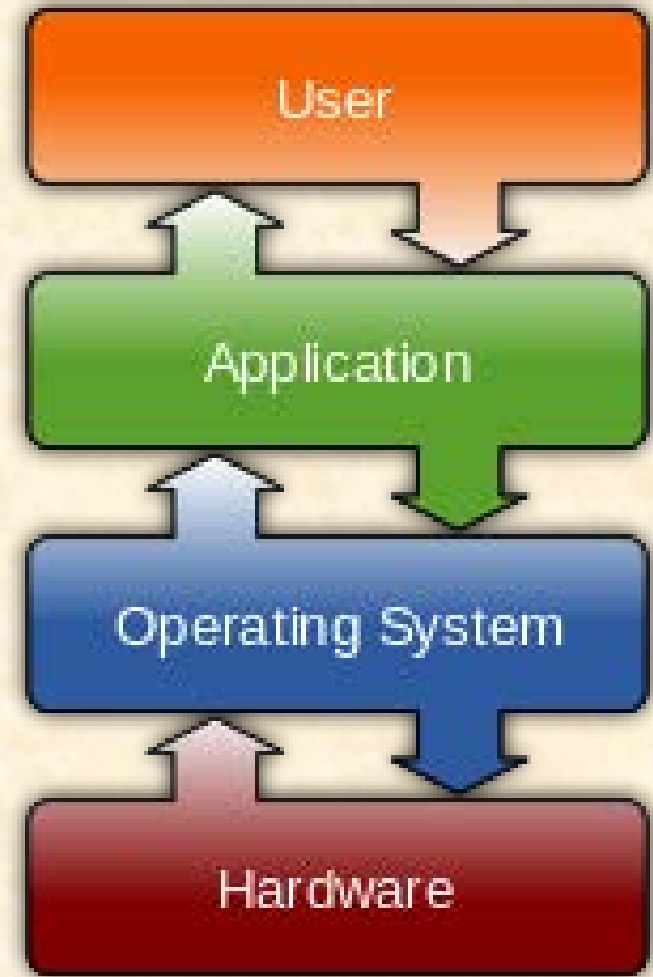
How OS Works ?

An Operating System (**OS**) works as a Master or Controller Program which takes instructions from the user and controls Hardware component as per user instruction.

It works as a middleman (interface) between machine and user. It manages all the resources like Memory, CPU time and devices on behalf of user or application program.

A machine (hardware) alone can not do anything, unless it is supervised and controlled by OS.

So, Operating System plays a very important role in computer operation.



Functions of Operating System

Operating System works as Resource Manager and makes computer functional. OS performs the following functions-

Process Management

Loads, schedules and execute process/programs.

Memory Management

Allocates memory to program and keeps record of free memory.

I/O Device Management

Communicate and controls various I/O devices.

File Management

Manages files and folders (create/access /delete/copy etc.) on storage devices.

Interface Management

Provides user-familiar and GUI interface to users.

Security Management

Provides security through user-name and passwords etc.

A program is called **Process** ,when it is being executed by the CPU.

Types of Operating Systems

❑ Single User OS

It allows one user to work at a time. It is also **Single-Program** OS i.e. only one program can be loaded and executed at a time. Example- MS DOS.

❑ Multi-User OS

It allows two or more users to run programs at the same time. These are **Multi-Program** and **Time-Sharing** OS, since multiple program can be loaded and executed by sharing CPU time among multiple users at the same time. Unix, Linux and Windows are common example of Multi-User OS.

❑ Real Time OS

A Real-time OS responds instantly, when input is given. The response time is pre-determined. Each job is completed in a specified dead line. It is used in Robotics, Communication and Flight Control System. LYNX and Windows CE are example of Real-Time OS.

Language Processors

A computer can understand only machine language (Low level) or Binary language (0 and 1). A program written in High Level Languages (HLL) must be converted into its equivalent Machine code, so that computer can understand and execute. This conversion is done by Language Processors.

There are so many High-Level Programming Languages like BASIC, C, C++, Java, Python etc., where a program can be written and converted in equivalent Machine Level code.

The Language processors are divided into three types-

★ **Assembler**

★ **Interpreter**

★ **Compiler**

□ **Assembler:**

Assembler converts program written in Assembly Level Language into Machine level. Assembly Language consists of mnemonic codes, which to be converted (assembled) into machine code by using Assembler program.

Language Processor

❑ Interpreter:

Interpreter converts High Level Language (HLL) program into Machine level code in line by line manner and executes it. If any error occurs, it reports the error and stops the translation. Execution resumes after error is removed. The Interpreter is required each time when program is to be executed.

❑ Compiler:

Compiler converts the entire HLL program into machine code in one go, and reports all the errors along with line numbers. After removing the errors, Program is re-compiled and executed. It creates an object file (.exe/ .com), which can be executed directly. So that, compiler is not required each time when program is to be executed.



Application Software

□ Utility Software:

The software which keep our computer trouble free by performing some House-keeping jobs, are called Utility Software. The following Utility software are commonly used –

Text Editor : It help to create, store or edit a text file. A text file contains typed text (alphabets, numbers and special characters etc.) with little formatting. Example : **Notepad, Notepad ++, Gedit** etc.

Backup Utilities : This utility software facilitates users to take back-up of important files and folders on storage media like CD/ DVD or Pen drive. This back-up data can be restored in case of any failure or damage to the system. Back-up & Restore Utility can be found in Control Panel of Windows 7 OS.

Disk Defragmenter : Disk Defragment utility speeds up the computer by Re-arranging fragmented and scattered files in contiguous location on the disk. It is found in Accessories Tab of Windows OS.

File Compression Utility: This Utility can reduce file/folder size by compressing (zipping). It is useful when a big-sized file to be stored on CD/Pen drive or to be sent through e-mail as attachment. Example: **WinZip, 7Zip, WinRAR** etc.

Anti Virus software: This utility software is used to detect and remove Virus from the computer. It also protects computer from un-wanted and malicious programs. Example: **QuickHeal AV, Norton AV, Avast AV** etc.

Application Software

❑ General Purpose Application Software:

General purpose application software are **Ready-to-use software** (Software package) which are designed to carry day-to-day work of users. Most commonly used Software packages are-

Word Processor: This software is used to create a document file including text, graphics and tables with intensive formatting. It is commonly used for writing letters, project reports, official documents and publishing books etc.

Example: **MS Word, MS Publisher, Writer (Open Office)** etc.

Spreadsheet Tool : Spreadsheet software provide tabular sheets which can be used for formula-based calculations, Statistical Analysis of data and creation of Graphs etc. Example: **MS Excel, Lotus and Calc (Open Office)** etc.

Presentation Tools: These software are used to create a presentation on any topic. A presentation consists of slides with text, graphics, animations, sound and video. Example: **MS Power Point, Impress (Open Office)** etc.

Data Base Management System (DBMS): These software facilitates creations, maintenance and use of database (collection of records) for any organization. Example: **MS Access, FoxPro, Oracle, MySQL** etc.

Graphics & Multimedia Software: These software facilitates editing of images and creation of multimedia presentations and animations.

Example: **Photoshop, Corel Draw, Director, 3D Max** etc.

Application Software

❑ Specific Purpose Application Software:

Specific purpose application software are **Customizable** software which are designed to carry **specific task of Real-life Business Application** area. Some specific areas for which these software are used, are discussed below-

Payroll Management : This software is used in the Organizations and Institutions to calculate wage or pay of employees, generation pay-slips and reports etc. It keeps record of various allowances, deductions and taxes etc.

Hotel Management: These software are used in the Hotel sector for Hotel Administration, Maintaining Accounts, Billing, Management of Room, Food and beverage, and Room reservation etc.

Reservation System: These software are used at Railway, Airport and Bus Reservation offices to check availability of seats on particular date, Seat Reservation and Printing of tickets etc.

Inventory Management System: These software are used in Departmental stores, Institutions and Factories to keep record of the stock (Raw Material, Products), Managing sales and purchase etc.

Evaluation & Report Card Generator Software: This software is used in schools, colleges and Universities to perform calculations and prepare Marks-statement/ Grade Cards, Certificates after examinations. These software can also perform On-Line test for evaluating performance of the students.

Application Software

❑ Developer Tools:

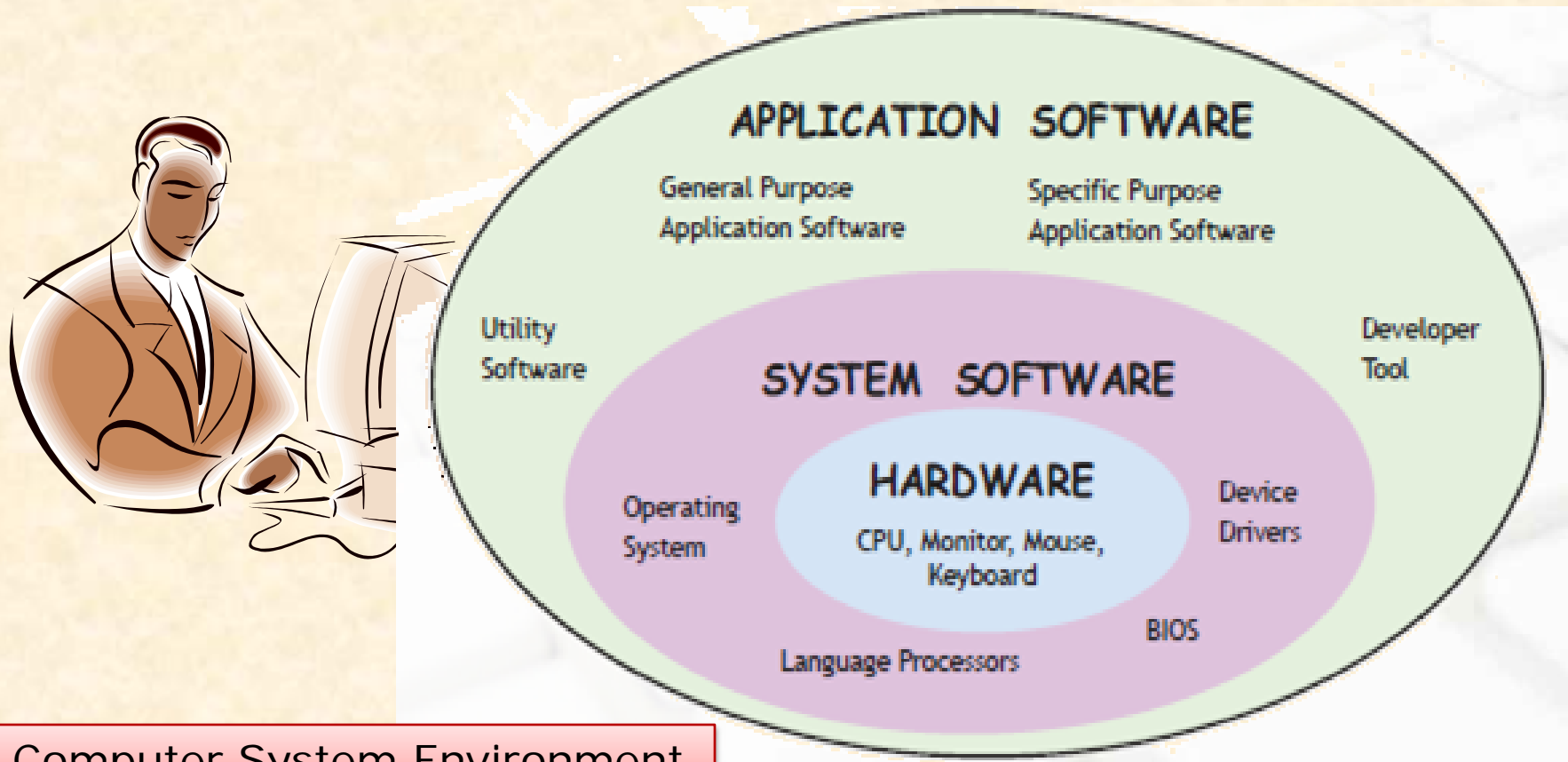
The design and development of Computer Software is also a tedious job which includes Writing source codes, Editing in source codes, Compiling, finding errors (bug) and removing bugs (debugging). Software Development tools (Developer tools) facilitate Software Engineer or Programmer in design and development of a software. These tools are also called **Integrated Development Environment (IDE)**, which consists of the following components-

- ❖ Source Code Editor
- ❖ Graphical User Interface (GUI) Builder
- ❖ Compiler/Interpreter
- ❖ Debugger
- ❖ Application Packager or Builder

Example: Visual Basic IDE, JAVA IDE (NetBeans), Turbo C++ IDE etc.

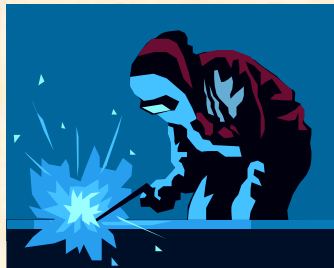
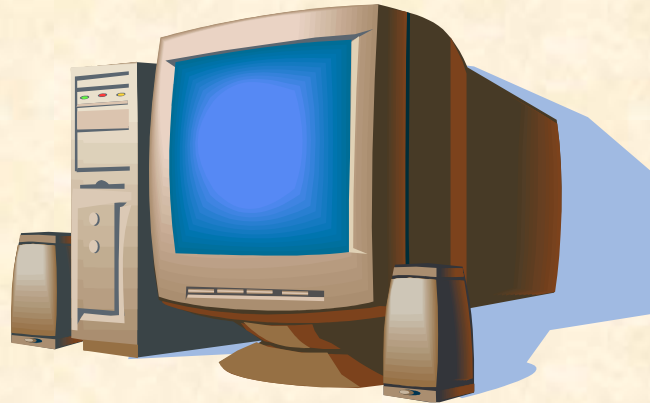
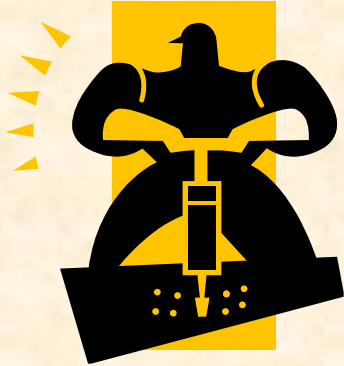
Relationship among Hardware & Software

The Hardware (physical components) and Software (System and Application) together makes an environment for computing. User is overall in-charge of this environment.



Computer System Environment

System Security



What is System/Information Security ?

- ❑ System or Information Security refers the protection of information and system resources with respect to confidentiality and integrity.
- ❑ System Security covers three dimensions of security known as **CIA**, which are-

Confidentiality:-

Ensure that information is not accessed by unauthorized persons i.e. protection against unauthorized access.

Integrity:

Ensure that information is not changed by unauthorized persons i.e. protection against unauthorized modification.

Authentication:

Ensure that users are the persons they claim to be i.e. Identification of Authorized user.

Threats to Computer Security

- ☐ Virus
- ☐ Worms
- ☐ Trojans
- ☐ Spyware
- ☐ Adware
- ☐ Spamming
- ☐ Phishing
- ☐ PC Intrusion- DoS (Denial of service) Attack

Computer viruses, Worms, Trojan, Spyware, Adware etc. are called Malware, because they are cause of malfunctioning of computers.

Viruses

- ❑ Computer viruses are malicious and self-replicating codes/programs that cause damage to data and files on the system.
- ❑ Computer Virus are self-replicating program i.e. they can make their own copy and infect other files stored on the computer.
- ❑ Virus can infect only software part of computer like Boot block, OS, System files, application program and data files.
- ❑ Computer Virus can automatically transferred from one computer to another through a network, Internet or removable media such as CD,DVD, Memory cards and Pen Drive etc.
- ❑ Major Symptoms of viral infection are– Slow execution of program, Damage or deletion of OS files and Data files.

“Creeper” was the first experimental virus, developed by Bob Thomas, which was detected on ARPANET in early 1970s.

Types of Computer Viruses

❑ Boot Sector Virus

Infects Master Boot Record (MBR) and loaded into memory with OS files, each time when system is booted/started.

❑ File Virus

Also called parasitic viruses which attached themselves with executable files (.exe/ .com) and loaded into memory when such program is loaded for execution.

❑ Macro Virus

Written in Macro Language (MS Excel/ Word) and typically infects system by e-mail. They can delete/ damage files.

❑ Polymorphic Virus

These viruses can mutate their code to hide themselves. They are difficult to detect and remove for Signature-based Anti virus program. They can also produce a new type of code (virus) by changing in their code during self-replicating/copying.

Worms & Trojans

❑ Worm

Worm is malicious program which replicates continuously and eats entire disk space or memory.

Unlike virus, it does not need host program to spread itself. It copies itself until all the disk space or memory is filled.

Worms are less destructive than virus, because worm does not corrupt other files. It only eats up the memory and slow down the computer.

❑ Trojan Horses

It is a program that appears harmless (like utility program) but actually performs malicious functions like deletion or modification of files. Trojan are more dangerous than virus and Worm. They can damage security system, download and install unwanted s/w, theft of private information like user name, password and e-mails etc.

Generally, they are tools of hackers and transferred through freeware, shareware and games installed by the users.

Spyware & Adware

❑ Spyware:

- Spyware is a program designed to spy on your activities and report this data to its developer. Mostly they are downloaded from Websites/ Internet and secretly installed without your consent.
- Generally, Spyware steals private information like username, password, bank details etc. and passes it to its developer, who can pass it to other interested people.

❑ Adware:

Adware are the malware programs that deliver unwanted advertisement to your computer (in Pop-up form). They are also get installed as tool bar in web browser program. They consume network bandwidth. It can display pop-up ads or irritating message and can slow down Internet speed.

Spam & Phishing

❑ Spam (Unwanted bulk-Mails)

- Spamming refers to the unwanted bulk-mail sent by an identified or unidentified sources in the mailbox.
- In non-malicious form, it can be an Product promotion or advertisement e-mail sent by unknown account.
- In malicious-form, the attacker keeps on sending bulk mail until mail-server runs out of disk space, which may cause bounce of useful mails.

❑ Phishing

- Phishing is a process of attempting to acquire sensitive information such as User name and password, credit card number, bank account details etc., by web-site link, sending e-mail from sources (which look authentic) or voice call.
 - In Phishing, user himself discloses private information in response to such attempts.
-

PC Intrusion

- ❑ A Computer system may be a potential target for hackers when it is connected to Internet. Your computer can be accessed and used as a platform to spread malwares and carry unethetical activities by hackers.
 - ❑ PC Intrusion refers to the unauthorized access of computer by the Hacker or malicious program.
 - ❑ Generally, this types of attack may eats up all the resources of the computer, which may cause to stop of the functionality of the computer system or Program and System come to a halt state. This is called **DoS** (Denial of Service Attack)
 - ❑ Some time, an attacker program can delete critical OS files and data files. This is called **Sweeper** attack.
-

Security Principles

- ❑ The security of data/information/computer and Network resources is based on some security measures and safeguards designed to protect from security threats.
 - ❑ 'Prevention is better than cure' principle is applicable in System security too.
 - **Active Protection:**

Installation of some Security programs and Firewall for protection against Viruses, Spyware, Adware and PC Intrusion.
 - **Preventive Measures:**

You should opt some preventive measures to avoid such happenings.
-

Desktop Security

❑ Authorization (User Name/Login ID)

Some thing do you Know?

User Authorization is done by a valid User Name/Login Id etc. User Name is a code which authorizes user to get computer access after log-in.

❑ Authentication (Password)

User is Authenticated by a valid password etc. Password is a secret code that is used to authenticate or confirm user's identity. Password should strong enough to avoid guessing. Generally, User name and Password in combination is used to provides better security.

❑ Biometric Identification (Physical Authentication)

Something do you have?

To provide more strong security, a system may have Biometric devices to identify a person by unique biological properties like Finger print , Retina Scan, Voice or Face Recognition etc., which can not be transferred or stolen by others.

Desktop Security

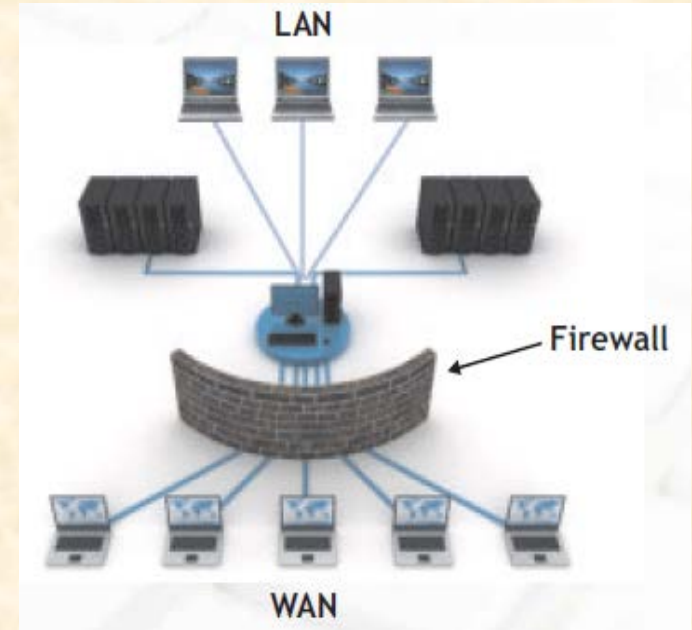
❑ Anti-Virus tool for Malicious Program

- ❖ These Program removes various malicious programs like Virus, Worms, Spywares and Trojan etc.
 - ❖ Anti-virus tools not only remove virus and other infections but at the same time also protect our system from data loss, destruction and attack of external threats like virus, worm and Trojans.
 - ❖ The small code of virus which embedded with a file, is called its **Signature**. Signature is used to identify the virus.
 - ❖ Generally, Anti-virus uses Signature-based methods to identify a virus i.e. it compares the contents of files to known virus code (signature) stored in a database. It is strongly recommended to get updated database of Virus signatures by updating Anti-virus program regularly.
 - ❖ Some advanced Anti-virus programs uses Heuristics and Rootkit detection method along with Signature-based method to identify new and unknown viruses.
 - ❖ Some commonly used Anti-virus programs are- Quick Heal, Avast, Norton AV, McAfee, AVG, Kaspersky etc.
-

Network Security

❑ Firewall

Firewall is a system (H/w or S/w) which acts like a gate to protect Computer or Network from unauthorized access. It monitors the network access as per rules defined by the Network Administrator. All requests entering or leaving the LAN passed through Firewall, which examines each requests and blocks those access that do not meet the security criteria.



❑ Intrusion Detection System (IDS)

It is system which identifies various Intrusion and monitors the system and Network resources, and users activities. It notifies to authorities in case suspicious happenings. It is advanced system than Firewall, which provides a watch on user's suspicious activities and access for Network resources.

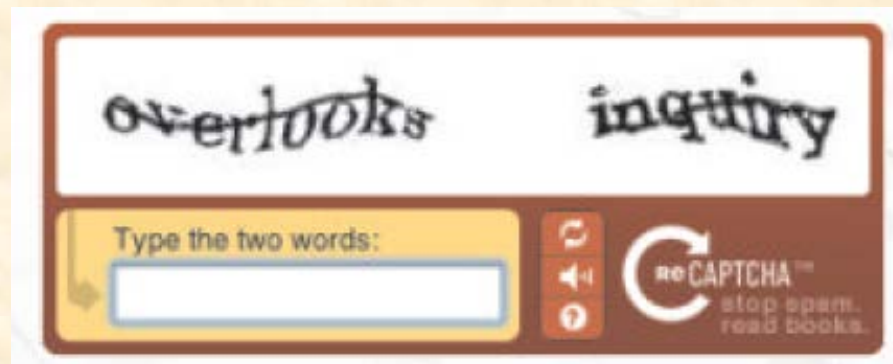
Network Security tools

❑ File Access Permissions

Files and folders stored on the computers may have limited access permissions like **Read**, **Modify**, **Create** and **Execute** permission (rights) as per need of the other users in the network. Sometimes a file may also have password to open or modify the contents to provide additional security at file level.

❑ CAPTCHA :

CAPTCHA(**C**ompletely **A**utomated **P**ublic **T**uring Test to tell **C**omputers and **H**uman **A**part) is a program that displays distorted text/images as a challenge, which can read by human beings only. It ensures that website/program is being accessed by human being and not by malicious computer programs (bots).



Network Security tools

❑ Digital Signature :

Digital signature is a method for providing the authenticity of a message, document or attachment sent through e-mail. It is commonly used in Financial and Legal transactions where forgery and tempering of document is possible. It works like a valid signature of a person on a document which ensures recipient about authenticity of document.

❑ Digital Certificate :

Digital Certificate (Public Key Certificate) is an electronic document which uses digital signature and requires a public key or password to open or decode a document. It verifies and ensures that document belongs to an authorized individual or organization.

❑ Cookies :

A Cookie is a small text file containing information regarding a website preferences and some private data of user. It is placed in the system by web-server as a header and sent back by the web browser each time to provide information about visitor. It can also be used for authentication and Session tracking. Some cookies may violate privacy issue by transferring user's private data like name and passwords etc. So, cookies should be monitored while accessing website on the Internet.

Preventive Measures

- ✓ **Install a effective and reliable Anti-virus and Anti-Spyware program.**
 - ✓ **Keep your Anti-virus program update.**
 - ✓ **Think twice before downloading anything from Internet. (Always Download from trusted sites)**
 - ✓ **Be careful while opening e-mails.**
 - ✓ **Implement proper Security policy.**
 - ✓ **Use proper File access permissions when it is being shared among users.**
 - ✓ **Use Filter utility to get off spam.**
 - ✓ **Keep your e-mail address, passwords etc. private.**
 - ✓ **Install Firewall to prevent unauthorized access to or from a private network.**
 - ✓ **Disable cookies to avoid misuse of private data.**
 - ✓ **Disconnect Internet when it is not in use.**
-

Cyber Crime & Cyber Law

❑ **Cyber crime (Computer Crime)**

Cyber crime refers to any crime wherein the computer is either a tool or a target or both. Some forms of Cyber Crime are-

- ❖ Creating and sending Spam mails
- ❖ Posting offensive messages on Social Networking Portals.
- ❖ Hacking of Computer or Cracking Security systems.
- ❖ Unethical Financial transactions and Fraud through Internet
- ❖ Harassment through e-mails and web messages.
- ❖ Cyber terrorism.
- ❖ Creation & Propagation of Virus, Worms or Trojans etc.

❑ **Cyber Law :**

Like traditional crime such as theft, fraud, forgery, defamation and mischief, Cyber Crime are also treated as criminal activities and are subject of punishment. The Information Technology Act 2000 (IT Act) in India provides legal support to the computer users against cyber crime. The Cyber Police have right in respect of all the offences committed under IT Act. It also deals with Intellectual property rights on Internet.

Social Networking

Social Networking is an application of Internet to communicate worldwide among known and unknown users, share thoughts, experiences and expertise, happiness and sorrows, and performing group communication and friendship. Some commonly used Social Networking sites are- Facebook, Twitter, Netlog, Hi5 and Orkut etc.

Although, on-line social networking is very useful but there are certain risk and danger, because you may share your personal details to strangers. Some common threats pertaining on these websites are-

- ❖ Unknown users can misuse your personal information.
- ❖ Presence of abusive and unwanted contents.
- ❖ Fake identity of someone known to you or someone famous.
- ❖ Hacking and misuse of your account.

You should take the following precautions, while working on these sites-

- ❖ Do not disclose your personal information to strangers.
 - ❖ Do not approve friendship request of unknown users and avoid to join groups having abusive and unwanted contents.
 - ❖ Block un-ethical users and fake Identities, and immediately report about the same to service providers.
-