CHAPTER 2

SOFTWARE CONCEPTS

Software : Set of Instructions to perform a job called Software.

Type of Software

System Software
Application Software

System Software : S/w which requires for the Computer Operation.
Application Software : S/w which requires for the specific need of human to perform specific job.

Type of System S/w

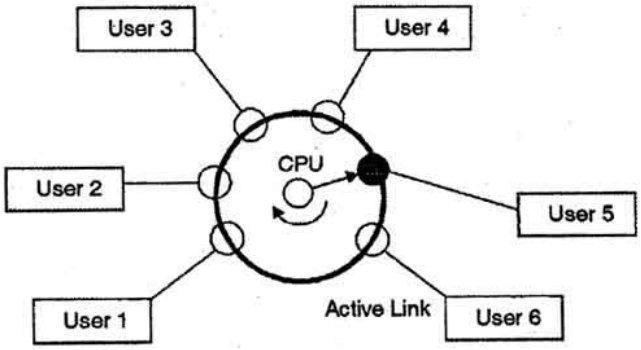
- Operating System
- Language Processor
- Utility Software

Operating System:
Operating System (OS) works as interface between User and Hardware.

The Operating System (OS) deals with all the basic functioning and the same is performed by the machines. For instance, showing the movement of the mouse on the screen when a person hovers the mouse. There are lots of Operating Systems available recently. The most popular and latest ones include the Windows XP, Mac, UNIX, Linux, Windows Vista, etc.

Type of OS :

- Single User OS : OS on which only one user can work at a time.
  Eg. Windows
- Multiuser OS : OS on which only more than one user can work at a time. Eg. Unix
- Real Time OS : OS which has to generate output within the specific defined time. Eg. RTLinux , LynxOS, QNX
- Time Sharing OS : OS which work on sharing of time slice amount the connected users.
  Eg. Multics, Unix



- Multiprocessing/Multitasking OS : OS which is able to perform multiple operation /task at a time.
  Eg. Windows 2000, IBM's OS/390, and Linux

Need of an Operating System:

This is the same question we ask to the persons one of them knows English and the other ones knows Spanish so we need one person who is able to communicate between two same is the answer here for why we need the Operating System it is the communication pathway between the user of the machine and the machine where machine knows only machine language i.e. '1' and '0' on the other hand the man knows the alphabetic language. so operating system gets the alphabetic language from the user and change it to the machine understandable language and vice versa.

In earlier day's user had to design the application according to the internal structure of the hardware. Operating System was needed to enable the user to design the application without concerning the details of the computer's internal structure. In general the boundary between the hardware & software is transparent to the user.

1. Easy interaction between the human & computer.
2. Starting computer operation automatically when power in turned on.
3. Loading & scheduling users program.
4. Controlling input & output.
5. Controlling program execution.
6. Managing use of main memory.
7. Providing security to users program.

For hardware functions such as input and output and memory allocation, the Operating System acts as an intermediary between application programs and the computer hardware, although the application code is usually executed directly by the hardware and will frequently call the OS or be interrupted by it.

Functions of an Operating System:

An operating system (OS) is a set of computer program that manages the hardware and software resources of a computer. At the foundation of all system software, the OS performs basic tasks such as controlling and allocating memory, prioritizing

system requests, controlling input and output devices, facilitating networking, and managing files. It also may provide a graphical user interface for higher level functions. Various services performed by operating systems are discussed below.

Process management:
It deals with running multiple processes. Most operating system allows a process to be assigned a priority which affects its allocation of CPU time. Interactive operating systems also employ some level of feedback in which the task with which the user is working receives higher priority. In many systems there is a background process which runs when no other process is waiting for the CPU.

Memory management:
The memory manager in an OS coordinates the memories by tracking which one is available, which is to be allocated or deallocated and how to swap between the main memory and secondary memories. The operating system tracks all memory used by each process so that when a process terminates, all memory used by that process will be available for other processes.

Disk and file systems:
Operating systems have a variety of native file systems that controls the creation, deletion, and access of files of data and programs.

Networking:
Most current operating systems are capable of using the TCP/IP networking protocols. This means that one system can appear on a network of the other and share resources such as files, printers, and scanners. Many operating systems also support one or more vendor-specific legacy networking protocols as well.

Security:
Most operating systems include some level of security.

Language Processor

Assembler: Assemblers create an object code by translating assembly instruction mnemonics into opcodes. They also determine symbolic names for memory locations as well as for other entities. A prime characteristic of assemblers is the use of symbolic references, which saves time consuming manual calculations and address updates after a program has been modified. The majority of assemblers also have macro facilities so that they can perform textual substitution, which means that they are able to create short sequences of instructions.

Compiler: A compiler is program that converts the instruction of a high level language into machine language as a whole. A program written in high level

language is called source program. After the source program is converted into machine language by the compiler, it is called an object program. The compiler checks each statement in the source program and generates machine instructions. Compiler also checks syntax errors in the program. A source program containing an error cannot be compiled into an object program. A compiler can translate the programs of only that language for which it is written. For example C++ compiler can translate only those programs, which are written in C++. Each machine required a separate compiler for each high level language.

Interpreter: An interpreter is a program that converts one statement of a program at a time. It executes this statement before translating the next statement of the source program. If there is an error in the statement, the interpreter will stop working and displays an error message.

The advantage of interpreters over compilers is that an error is found immediately. So the programmer can make corrections during program development.

Utility Software:

Compression Tools: Data compression can be used for many purposes on computers and achieved in many ways. There are two types of data compression, lossy and lossless. Lossy compression makes data smaller by removing excess data so that the end result is still acceptable for its purpose. This is a one-way process and the compressed data is the result. Lossless compression makes data smaller by looking for patterns that can be written more concisely. This is a reversible process and a compressed file is the result. This file will have to be decompressed to access the original data. Advantages of data compression are that compressed data will take up less space on a computer and be quicker to transmit

Data compression for computer files is a lossless compression
Data compression for audio can be lossy or lossless
Data compression of images can be either lossy or lossless depending on the compression format used.
Data compression of video is primarily lossy

Disk Defragmenter:

The process of defragmenting a computer disk consists of file-management methods to improve system stability. This procedure is generally used as part of various performance-improvement techniques within an operating system. The use of disk defragment software contains a list of benefits and setbacks users must consider before selecting an appropriate approach.

Antivirus: Antivirus software exists to protect computer users from viruses, worms and spyware. According to Symantec, the makers of Norton Antivirus, there are more than 1 million computer viruses. Because of the prevalence of the viruses, there are

a lot of options for computer users in the area of antivirus software. Commonly used Antivirus are Norton, Kaspersky, Quick heal etc.

Application Software:

Application software is what allows users to store information, create content and media, access information and communicate. Because most of the processes of the world now run on computers, there are many types of software to handle all the functions that are required. All software applications have specific hardware requirements.

There are two types of Application software

General purpose Application Software e.g. Word, Excel, DBMS etc.

Specific Purpose Application Software e.g. Inventory Management System, Payroll System, Railway Reservation System, Hotel Management System etc.

Computer Security Threats:

Computer systems are vulnerable to many threats that can inflict various types of damage resulting in significant losses. This damage can range from errors harming database integrity to fires destroying entire computer centers. Losses can stem, for example, from the actions of supposedly trusted employees defrauding a system, from outside hackers, or from careless data entry clerks. Precision in estimating computer security-related losses is not possible because many losses are never discovered, and others are "swept under the carpet" to avoid unfavorable publicity. The effects of various threats varies considerably. Some affect the confidentiality or integrity of data while others affect the availability of a system.

Malware:

Short for "malicious software," Malware refers to software programs designed to damage or do other unwanted actions on a computer system. In Spanish, "mal" is a prefix that means "bad," making the term "badware," which is a good way to remember it (even if you're not Spanish).

Common examples of Malware include viruses, worms, Trojan horses, and Spyware. Viruses, for example, can cause havoc on a computer's hard drive by deleting files or directory information. Spyware can gather data from a user's system without the user knowing it. This can include anything from the Web pages a user visits to personal information, such as credit card numbers.

Virus :

Like a biological virus, a computer virus is something you don't want to get. Computer viruses are small programs or scripts that can negatively affect the health of your computer. These malicious little programs can create files, move files, erase files, consume your computer's memory, and cause your computer not to function correctly. Some viruses can duplicate themselves, attach themselves to programs, and travel across networks. In fact opening an infected e-mail attachment is the most common way to get a virus.

We all know it's hard enough to get a computer to work well when it is healthy, let alone when it has been attacked by a virus. Therefore, it is better to prevent an attack than to try

and cure it. There are many antivirus programs available that scan incoming files for viruses before they can cause damage to your computer. Some of these programs include Norton Antivirus, McAfee Virus Scan, and Virex

Trojan Horse:
In Greek mythology, there is a story about the Trojan War. This war lasted many years, as the Greeks could not penetrate the heavily barricaded city of Troy. So one day, a few of the Greek soldiers brought the people of Troy a large wooden horse, which they accepted as a peace offering. The horse was moved inside the city walls, where it sat until the night. After the people of the city had fallen asleep, Greek soldiers jumped out of the wooden horse, opened the gates to let their fellow soldiers in, and took over the city.

So what is the moral of this story? Mainly, beware of Trojan horses. But how does that relate to computers? That's a good question. In the computing world, Trojan horses are more than just a myth. They really exist and can cause damage to your computer. Trojan horses are software programs that masquerade as regular programs, such as games, disk utilities, and even antivirus programs. But if they are run, these programs can do malicious things to your computer.

For example, a Trojan horse might appear to be a computer game, but once you double-click it, the program starts writing over certain parts of your hard drive, corrupting your data. While this is certainly something you want to avoid, it is good to know that these malicious programs are only dangerous if they are given a chance to run. Also, most antivirus programs can catch Trojan horses when scanning for viruses. Unlike viruses, however, Trojan horses don't replicate themselves. Though it is possible for a Trojan horse to be attached to a virus file that spreads to multiple computers.

Spyware:
As the name implies, this is software that "spies" on your computer. Nobody likes to be spied on, and your computer doesn't like it either. Spyware can capture information like Web browsing habits, e-mail messages, usernames and passwords, and credit card information. If left unchecked, the software can transmit this data to another person's computer over the Internet.

So how does Spyware get on your computer? Just like viruses, Spyware can be installed when you open an e-mail attachment containing the malicious software. It can also be installed when you install another program that has a Spyware installer attached to it. Because of the insidious nature of Spyware, most people don't even know when Spyware is on their computer. Fortunately, you can purchase anti-Spyware utilities that will search for Spyware on your computer and stomp the unwanted software out of your system.

Worm:

Just like regular worms tunnel through dirt and soil, computer worms tunnel through your computer's memory and hard drive. A computer worm is a type ofvirus that replicates itself, but does not alter any files on your machine. However, worms can still cause havoc by multiplying so many times that they take up your entire computer's available memory or hard disk space. If a worm consumes your memory, your computer will run very slowly and possibly even crash. If the worm affects your hard disk space, your computer will take a long time to access files and you will not be able to save or create new files until the worm has been eradicated.
Worms are hard to detect because they are typically invisible files. They often go unnoticed until your computer begins to slow down or starts having other problems. Unlike viruses and Trojan horses, worms can replicate themselves and travel between systems without any action from the user. For these reasons, it is good to have an antivirus program installed on your system that can detect and remove worms before they have a chance to replicate or spread to other computers. Security updates such as Windows Update also patch security holes that allow worms to infect your computer. So keep your security updates and virus definitions up-to-date and you should be able to keep your computer worm-free.
Virus detection and its removal:

Virus detection and its removal are made through an antivirus program which finds out viruses in a computer and then possibly removes or repairs the virus problem.Some of commonly used Virus detection and its removable tools are Norton Antivirus, McAfee, Virus Scan, Kaspersky and Quick Heal etc.

Digital Certificate:

A digital certificate is a pair of files on your computer that you can use to create the digital equivalent of handwritten signatures and sealed envelopes. Each pair of files is divided into two parts: the public key and the private key. The public key is the portion that is shared; the private key is the portion that you, and only you, should have access to. Your computer and programs understand how to share only the public portion of your keys so that others can see them, while still keeping your private keys secure.

For example, when sending an e-mail message, you can digitally sign the message by attaching your digital certificate. Once they receive the message, recipients can verify that it came from you by viewing the small attachment on the e-mail, which contains your public key information. This protects you from people who might try to "spoof" an e-mail that looks like it came from you but is really sent from a different e-mail account.

Digital Signature:
A digital signature authenticates electronic documents in a similar manner a handwritten signature authenticates printed documents. This signature cannot be forged and it asserts

that a named person wrote or otherwise agreed to the document to which the signature is attached. The recipient of a digitally signed message can verify that the message originated from the person whose signature is attached to the document and that the message has not been altered either intentionally or accidentally since it was signed. Also, the signer of a document cannot later disown it by claiming that the signature was forged. In other words, digital signatures enable the “authentication” and “non-repudiation” of digital messages, assuring the recipient of a digital message of both the identity of the sender and the integrity of the message.

A digital signature is issued by a Certification Authority (CA) and is signed with the CA’s private key. A digital signature typically contains the: Owner’s public key, the Owner’s name, Expiration date of the public key, the Name of the issuer (the CA that issued the Digital ID), Serial number of the digital signature, and the digital signature of the issuer. Digital signatures deploy the Public Key Infrastructure (PKI) technology.

Cookies:
A "cookie" is a small piece of information sent by a web server to store on a web browser so it can later be read back from that browser. This is useful for having the browser remember some specific information.

An example is when a browser stores your passwords and user ID's. They are also used to store preferences of start pages, both Microsoft and Netscape use cookies to create personal start pages. Common cookies which companies use is find info are listed below:
Online Ordering Systems
Site Personalization
Website Tracking

How Do They Work
A command line in the HTML of a document tell the browser to set a cookie of a certain name or value? Here is an example of some script used to set a cookie. Set-Cookie: NAME=VALUE; expir es=DATE; path=PATH; domain=DOMAIN_NAME; secure Cookies are usually run from CGI scripts, but they can also be set or read by JavaScript.

Firewall:
A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. It may be a hardware device or a software program (running on a secure host computer. In either case, it must have at least two network interfaces, one for the network it is intended to protect, and one for the network it is exposed to.
A firewall sits at the junction point or gateway between the two networks, usually a private network and a public network such as the Internet. The earliest firewalls were simply routers. The term firewall comes from the fact that by segmenting a network into different physical subnet works, they limited the damage that could spread from one subnet to another just like fire doors or firewalls.

Hardware Firewall
Hardware firewall providing protection to a Local Network.

Software Firewall:
Computer running firewall software to provide protection

A firewall examines all traffic routed between the two networks to see if it meets certain criteria. If it does, it is routed between the networks, otherwise it is stopped. A firewall filters both inbound and outbound traffic. It can also manage public access to private networked resources such as host applications. It can be used to log all attempts to enter the private network and trigger alarms when hostile or unauthorized entry is attempted. Firewalls can filter packets based on their source and destination addresses and port numbers. This is known as address filtering. Firewalls can also filter specific types of network traffic. This is also known as protocol filtering because the decision to forward or reject traffic is dependant upon the protocol used, for example HTTP, ftp or telnet. Firewalls can also filter traffic by packet attribute or state.

Password:

A password is an un-spaced sequence of characters used to determine that a computer user requesting access to a computer system is really that particular user. Typically, users of a multi-user or securely protected single-user system claim a unique name (often called a user ID) that can be generally known. In order to verify that someone entering that user ID really is that person, a second identification, the password, known only to that person and to the system itself, is entered by the user. A password is typically somewhere between four and 16 characters, depending on how the computer system is set up. When a password is entered, the computer system is careful not to display the characters on the display screen, in case others might see it.

File Access Permission:

File access permission means how to restrict the access to file or folder e.g.

File and Folder Permissions Used by Windows

Permission	Meaning for Folders	Meaning for Files
Read	Permits viewing and listing of files and subfolders	Permits viewing or accessing of the file's contents
Write	Permits adding of files and subfolders	Permits writing to a file
Read & Execute	Permits viewing and listing of files and subfolders as well as executing of files; inherited by files and folders	Permits viewing and accessing of the file's contents as well as executing

		of the file
List Folder Contents	Permits viewing and listing of files and subfolders as well as executing of files; inherited by folders only	N/A
Modify	Permits reading and writing of files and subfolders; allows deletion of the folder	Permits reading and writing of the file; allows deletion of the file
Full Control	Permits reading, writing, changing, and deleting of files and subfolders	Permits reading, writing, changing and deleting of the file