

Introduction to Information Security

Prof. Dilip H. Ayyar

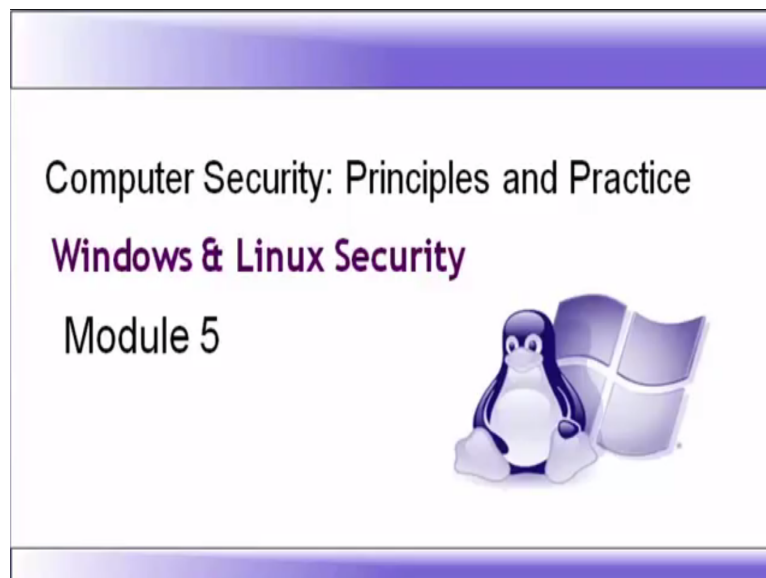
Department of Computer Science and Engineering

Indian Institute of Technology, Madras

Lecture – 51

Computer Security - Principles and practice

(Refer Slide Time: 00:10)



Hi everyone, now that we have completed module 4, we will now move on to module 5. Here we will look at the most popular OS today operating system that is Windows and Linux and some of the security features. When we talk about security many components come into play. The security of the OS itself, active directory services, the email, anti-virus or malware, firewall that is built into the OS nowadays, the browser security that is your internet explorer, your firefox, your google chrome, encryption of data security of laptops.

So, there are so many things that will be covered, but we will restrict ourselves here to the basics of Windows and Linux security. Now, as I take you through the slides I will talk about issues in the right places. You have to understand that the idea here is not to compare which operating system is better, but to give you a perspective on how each OS is built and their

architecture. You will also find a lot of resources online, if you need to go in depth to learn about the operating system intricacies.

Operating system persay is only a component of the info sec framework. Now, we have seen in module 2, 3 what is ISO 27001? The components that constitute the framework for infosec. We have also seen what is COBIT and what are the parameters that constitute the 7 pillars. You have to correlate the OS security component to ISO 27001 and COBIT wherever they apply to apply that principle into how you will fix the operating system security.

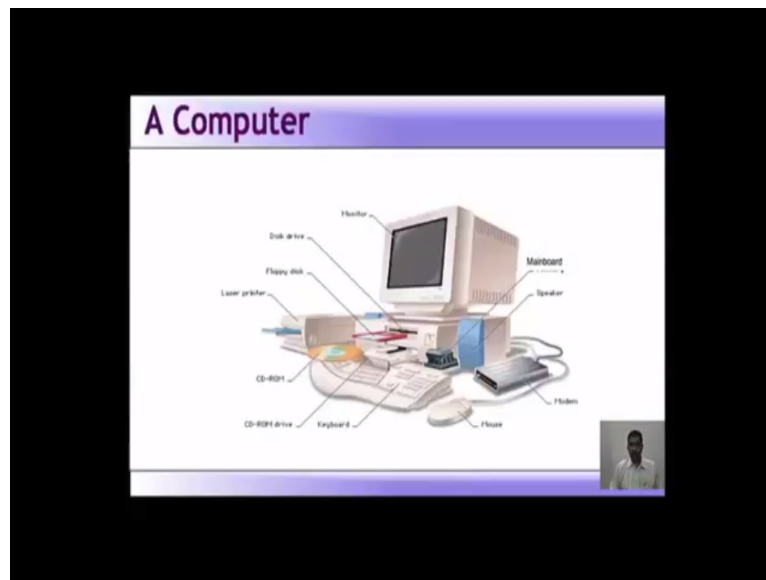
The important thing to note here is that you have to be up to date with the releases of different operating systems. Now, if you take for example, Ubuntu 10.04 was very popular operating system, now the current version is 14.10 long term release or long term support. Similarly, Windows XP was very popular, now it is Windows 8.1 Windows is planning to Microsoft is planning to release 10. Now, the security features from what was there in XP is totally different from that of Windows 8 or Windows 10.

The same is the case for servers the security features that was there in Windows 2000 or 2003 have been enhanced to make the operating system more secure in say 2008 and 2012. Some years back breaking into Windows means deleting the SAM, SAM file. Of course, you have to use a live CD go into Windows directory or boot with the live CD first go into the partition where the SAM file was located and delete the SAM file. Now, as the years progressed as the security gained importance or as more and more threats and attacks were being done on the operating systems, Windows also has evolved in security.

So, things became a bit more difficult. One had to find other ways to break into Windows. I remember there was a very popular hack when Windows 7 came in that was exploiting the sticky key functionality. You can youtube those videos there are still videos available in youtube which says how to break into Windows using the sticky key method. Now Microsoft is since thrashed all those vulnerabilities, but even now there are methods and tools available to break into OS.

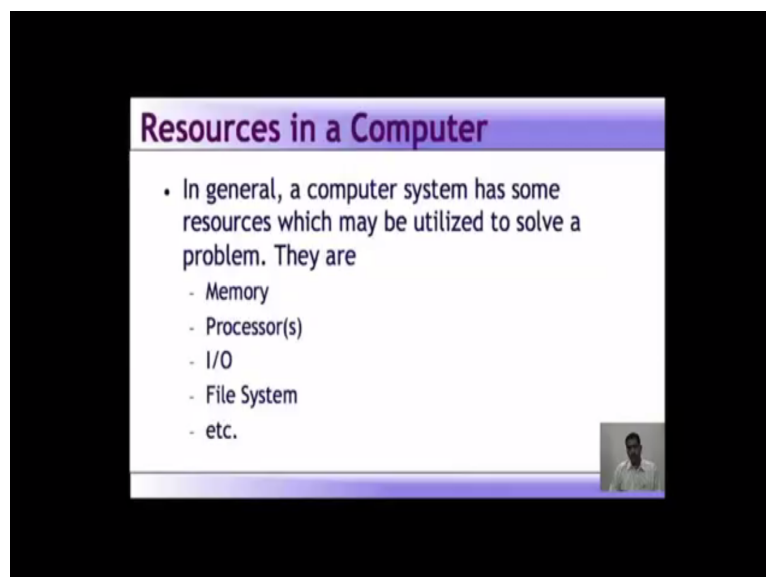
Again I am not specifically talking about Windows, the same is the case with Linux also, but for this session or for this particular module we will stick to the basic and understand how OS works and some of the features that are built into the OS.

(Refer Slide Time: 04:39)



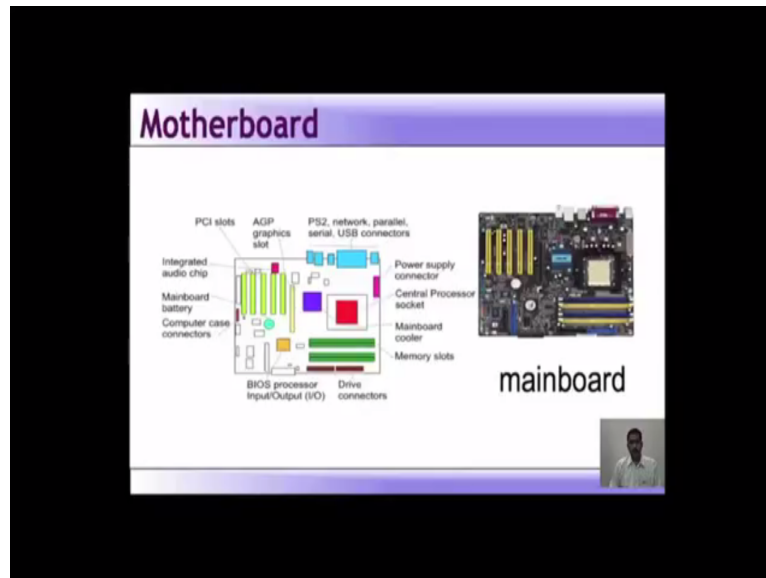
Now, we look at what is a computer everybody knows what a computer is. We will just go quickly for the benefit of people who do not know. Now computer is a collection of different components put together. There are input devices like keyboard and mouse, output devices like monitor and printer, floppy disk is storage device CD ROM is storage device there are speakers for audio. There is modem for communication. So, a computer consists of different components put together.

(Refer Slide Time: 05:16)



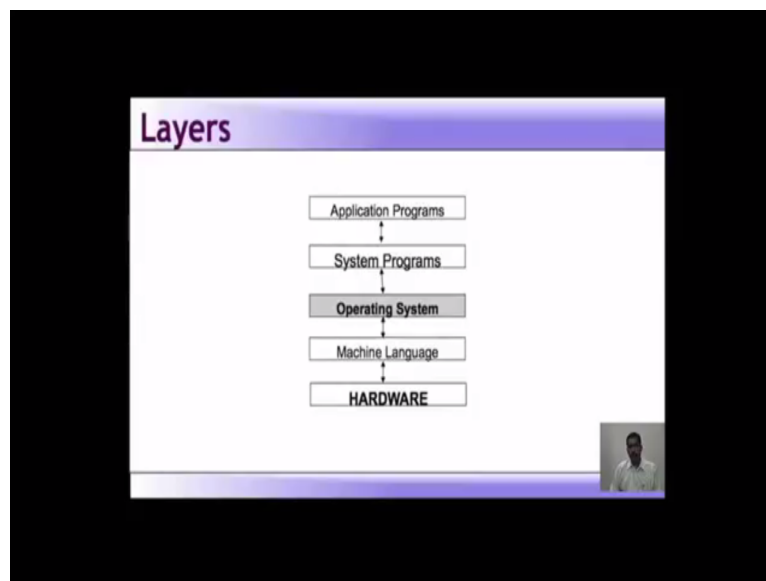
What are the resources in a computer? In general a computer system has some resources which are be utilized to solve a particular problem. What are they memory? Memory, processors, input output devices, the file system itself, Windows used NTFS, EAC 3 and EAC 4 are used in Linux, Mac uses a different file system, so these are the resources in a computer.

(Refer Slide Time: 05:53)



Now, the main heart of the computer or the main component of the computer is the motherboard. The mother board has got separate devices integrated into it, such as the PCI slots, audio, PS2 connector, serial connector, parallel for olden type of printers, USB connector, SMPS or simple power supply connectors, the processor itself will come here the. Integrated audio chip is there, BIOS is there. So, these are the components of a mother board. If you look on the right, that is a how a motherboard for a desktop looks.

(Refer Slide Time: 06:45)



There are different layers when you talk about the computer itself. The hardware layer which is the bottom most layer on top of it sits the machine language layer. On top of it is the operating system. Then the system program to communicate to the hardware, then the application program like the Microsoft office, all these are called the application program layer.

(Refer Slide Time: 07:18)

What is operating system?

- o **Interface** between hardware and user.
- o **Handle** technical details without user intervention.
- o A Collection of programs
 - Operating system
 - Systems software
 - **Kernel**
 - Utilities
 - Device drivers
 - Language translators

The diagram illustrates a layered architecture with four levels: User (top, red), Application (green), Operating System (blue), and Hardware (bottom, red). Bidirectional arrows connect each adjacent layer, indicating interaction. A small video inset of a person is visible in the bottom right corner of the slide.

Taskbar: Mail - SkyRay..., Microsoft Excel - ..., module 5 part1 - ..., VLC media player, 11:59 AM 4/3/2016

But what exactly is an operating system? It is the interface between the hardware and the user. It handles technical details without user intervention. It is a collection of programs, the operating system itself combines the operating system software, system software, kernels, utilities, the device drivers the language translators. Here language translator is not from Hindi to English or Tamil to Malayalam, it is basically how the software part is converted into a hardware part that translation happens here.

(Refer Slide Time: 08:02)

What is operating system?

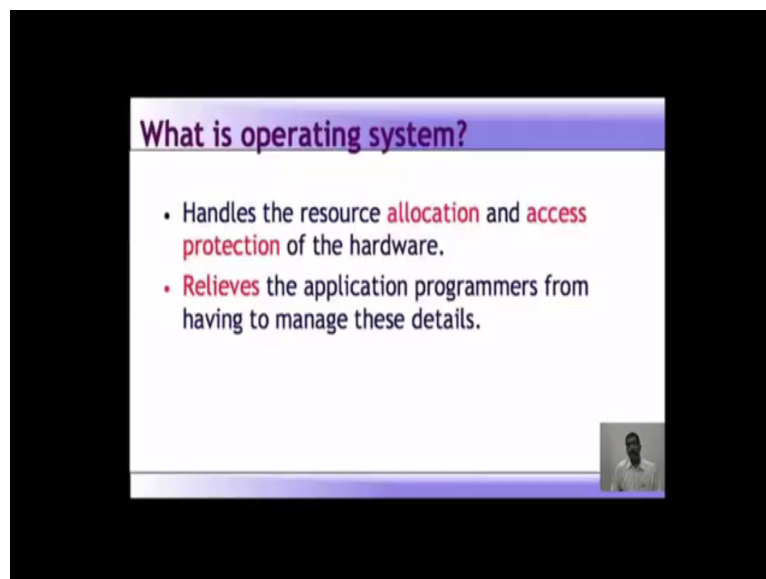
- Responsible for the **management** and **coordination** of activities and the **sharing** of the resources of a computer
- Acts as a **host** for computing applications run on the machine.
- Determines which applications should **run** in what **order** and how much **time** should be allowed for each application before giving another application a turn (in **multitasking** OS).

A small video inset of a person is visible in the bottom right corner of the slide.

What is the responsibility for the OS? It is responsible for the management and coordination of activities and sharing of resources of a computer. So, basically what it does, when you install the OS? It manages the resources in a computer, it coordinates activities within the computer like it gives preferences to some applications over others. And then resources are shared like a memory is shared, the hard disk is shared based on what access control is set, all these things are shared. It act as a host for computing applications that run on the machine. So, basically it is a server, it serves the resources or the computing application that are run on that machine.

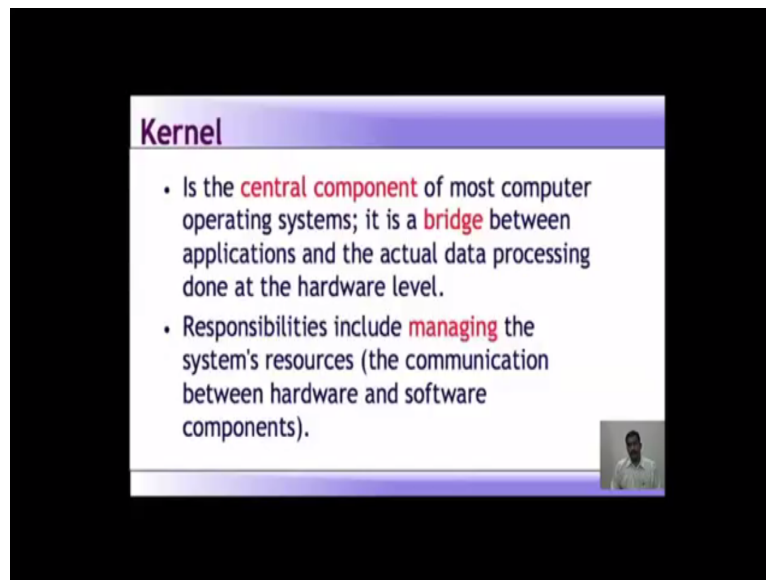
When you come to a desktop, it is again a server for a single user. It determines which application should run in what order and how much time should be allowed for each application before giving another application a turn, in multi-tasking OS this is what happens. Basically the OS will determine which has got a priority to run over some other functions which are running. That is what the OS does it, it handles the resource allocation and access protection of the hardware.

(Refer Slide Time: 09:37)



We have already gone through resource allocation. It relieves the application programmers from having to manage these details. Application programmers will develop application on certain technology, install it on the operating system. The operating system will communicate with the hardware or it will translate what that software is meant to do hardware layer where ever it is required that is basically what is called as the language translation.

(Refer Slide Time: 10:08)

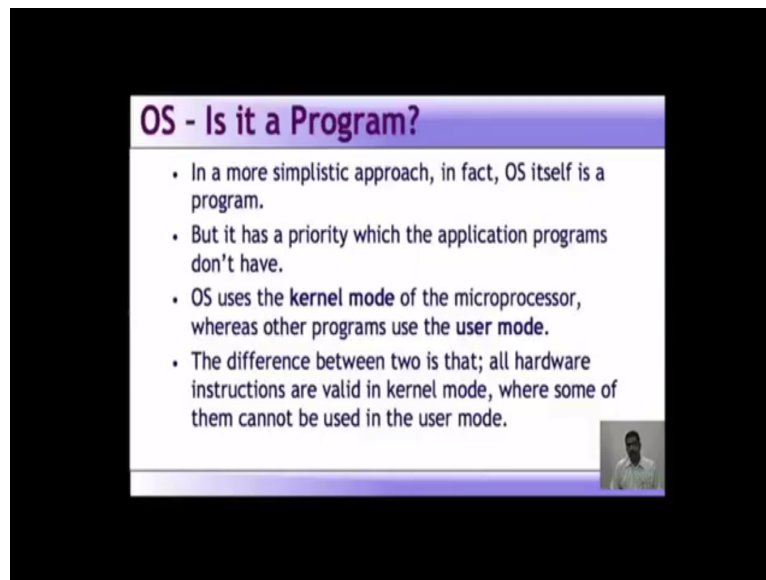


The slide is titled "Kernel" in a purple header. It contains two bullet points: "• Is the central component of most computer operating systems; it is a bridge between applications and the actual data processing done at the hardware level." and "• Responsibilities include managing the system's resources (the communication between hardware and software components)." A small video inset of a person is visible in the bottom right corner of the slide.

Now, there is something called a kernel. The kernel is the central component of most computer operating systems. You can also call it as a bridge between the applications and the actual data processing which is done in the hardware level. The responsibilities for a kernel include managing the system resources that is, it handles the communication between the hardware and software components. So, what you have to understand about the kernel is, one it is the central component of a computer system, computer operating system. It is a bridge between the application and the actual data processing.

The actual data processing happens at the hardware level. So, it is a bridge between the application and the hardware. And what it does, it manages the system resources or the communication that pass back and forth between the hardware and the software components.

(Refer Slide Time: 11:09)



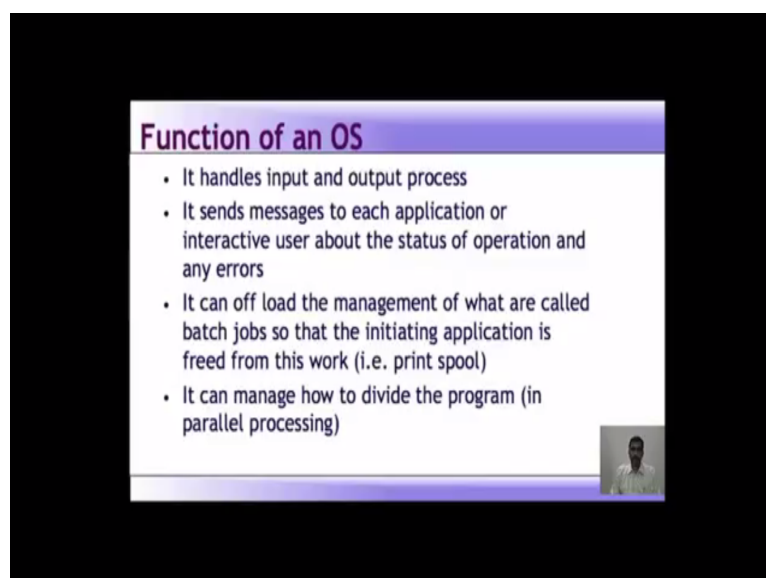
OS - Is it a Program?

- In a more simplistic approach, in fact, OS itself is a program.
- But it has a priority which the application programs don't have.
- OS uses the **kernel mode** of the microprocessor, whereas other programs use the **user mode**.
- The difference between two is that; all hardware instructions are valid in kernel mode, where some of them cannot be used in the user mode.

Video inset showing a person speaking.

Is it a program? Operating system, in very simple term it is a program itself or a collection of programs. It has the priority which the application programs do not have. So, what is the difference here, this is a program which has priority on what resources to allocate to which program. The OS uses kernel mode of the microprocessor, whereas the other programs use the user mode of the microprocessor. What is the difference between the kernel mode and the user mode? All hardware instructions are valid in the kernel mode, whereas some of them or some of the hardware instructions are not valid in the user mode. What are the functions of an OS?

(Refer Slide Time: 12:08)



Function of an OS

- It handles input and output process
- It sends messages to each application or interactive user about the status of operation and any errors
- It can off load the management of what are called batch jobs so that the initiating application is freed from this work (i.e. print spool)
- It can manage how to divide the program (in parallel processing)

Video inset showing a person speaking.

So we have seen it handles the input and output processes. It sends message to each application or interactive user about the status of operation and error. So, if you get an error, you get Windows cannot do this function your application has crashed. So, whatever error or status of operation is there, it alerts the user on what is the actual state of operation. It can off load the management of what are called the batch jobs. We have seen batch job in the domain 2 and 3. .

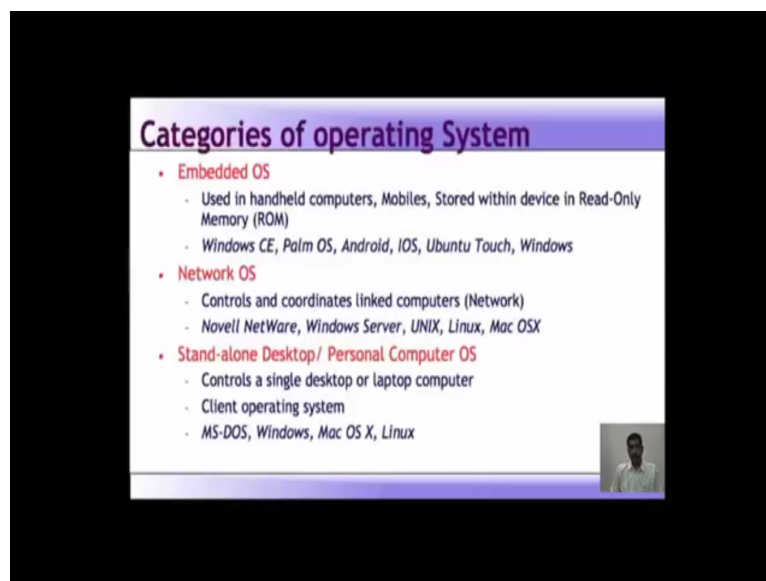
So, initiating the application is freed from this work. So, spool, spool has got an acronym actually the acronym is simultaneous peripheral operation online. You can also call it a kind of buffering. The most common that you see or the kind of spool you see is print spooling. What is basically does is it places a task, task or you can say a print job it will queue for extended or later processing. The most common spooling application that we find nowadays or quite sometimes is print spooling.

Let us say a document are formatted for printing. It is stored in an area on a disk and it is retrieved and printed by a printer. And it is alright whatever is the speed of the printer. The printers typically can print only a single document at a time and it will require seconds or minutes to do so. So, with spooling you can buffer or multiple process can write document to the print screen without delay. So, as soon as the processors requests the document in the spool, the processor can perform other task while a separate printing process operates the printer, did you get the point? Good, now if you take an example of spooling the organization is preparing a payroll. The actual computation may take only a matter of minutes or even seconds, but the printing may take a long time assuming there are 1500 people working. Now, we have to print fifteen hundred salary slip may take quite some time. So, if the program is printed directly then the CPU, the memory the peripheral would be tied upon or it would not be available until the actual process is finished.

Now, this is the same case with the personal computer also. Without the facility of spooling, may be a word document will not be able to continue until the printing is finished. So, without spooling most programs will be allocated to pattern or past processing or long way or you can say it is inefficient paradigm. Now, the batch processing system that we spoke about now uses spooling to maintain a queue of ready to run job.

So, basically what it does is it runs a queue of ready to run job, which can be started as soon as the system finishes the current job. So, that is what it means. Now, the OS can also manage how to divide the program in parallel processing. Parallel processing is the simultaneous use of more than one processor nowadays you have dual core octa core. So, different cores are there. So, it is a simultaneous use of more than one core or one processor to execute a program or multiple computational threads. Ideally where it is used? Ideally, parallel processing makes the program runs faster because there are more engine or more CPU or more cores that are running.

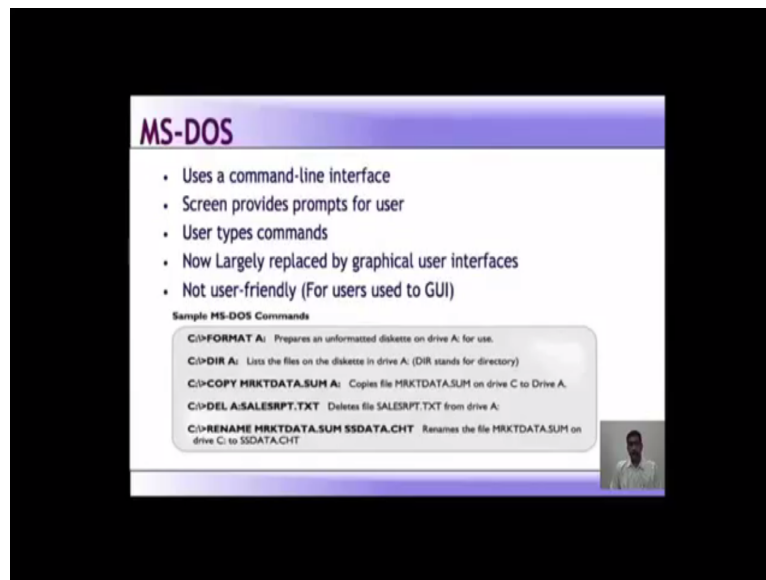
(Refer Slide Time: 16:42)



Under the operating system also there are categories. There are embedded OSs; embedded OSs are used in hand held, computers mobiles stored within the device in ROM read only memory. Examples of that is Windows CE, palm OS android IOS, Ubuntu touch, Windows. Then there is network OS which controls and coordinates linked computers what are the linked computers, it is a network, we have seen in domain 4. Example of that is Novell, Windows Server, Unix server, Linux, Mac OSX. Then there are stand alone or desktop

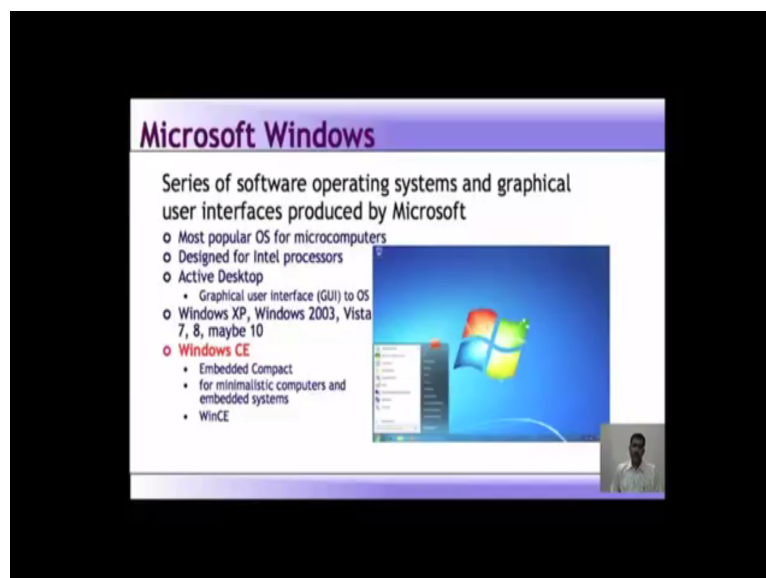
personal computer OS, it controls a single desktop or a laptop computer it has its own client operating system examples of it is MS dos Windows mac OS x Linux there are several categories even in these 3 OSs there are so many OSs available.

(Refer Slide Time: 17:48)



Let us take a look at traditional OS this is MS DOS, I think many of you would not have had the opportunity to work with MS dos itself. MS DOS uses a command line. So, it is totally based on command line. The screen provides prompts for users. User types the commands now it is largely replaced by GUI, MS DOS is not user friendly. Now some sample MS dos commands are format copy, delete, rename.

(Refer Slide Time: 18:35)



Then came your Microsoft Windows, it is a series of software operating systems and GUI produced by Microsoft. Now, Windows is the most popular OS for microcomputers it has

been designed for intel processors. It has an active desktop that is a GUI means, with GUI you can control everything. versions of that you know about XP, 2003, Vista, 7, 8 and we see 10 is coming and then Windows CE for embedded compact or compact embedded for minimalistic computers and embedded systems. So, win CE is the version for that.

(Refer Slide Time: 19:23)



Then the apple mac OS Macintosh operating system. It is a series of GUI based operating systems it runs on mac computer. It was designed for power PC microprocessors. Now, it is the first commercially successful GUI. It is also said that Microsoft borrowed the ideas from apple to make the product. It has served as a model for Windows and other GUI products developed since then. OS x latest version is 10. 10 .X Yosemite. Now, the newer mac system can run both on intel and on power PC. Now, let us look at what a Windows security architecture is like.

(Refer Slide Time: 20:16)

Windows Security Architecture

- Security Reference Monitor
- Local Security Authority
- Security Account Manager
- Active Directory
- Local vs. Domain Accounts
- Access Control Lists
- Integrity Control
- User Account Controls



Here, what I would like to point out is, anyone who wants to understand how security works in Windows must have the knowledge of the basic fundamental security blocks of the security systems. Now, there are many components in Windows that make up the fundamental security infrastructure. There are the security reference monitor, local security authority, security account manager, active directory, then local versus domain accounts, the access control lists, the integrity controls, the user account control. We will look at each of these components in the coming slides.

(Refer Slide Time: 21:06)

Security Reference Monitor (SRM)

- Kernel Mode Component that
 - Performs Access Checks
 - Generates Audit Log Entries
 - Manipulates User Privileges



We look first at security reference monitor. It is a kernel mode component that performs access checks, that generates audit log entries, that manipulates the user privileges. So,

simply put or in simple terms it checks for proper authorization before granting access to objects. What is the object manager? Object manager is the client of a SRM, SRM here is security reference monitor. It ask the SRM if the process has proper rights to execute a certain type of action on a particular object.

It uses the access control list to do this, then it implements a auditing function to keep track of attempts, to access an object. It also implements department of different C2 level security. What is C2 level security? I will read out some of the important list of the C2 level security as the design by the department of defense. One is it must be possible to control access to the resource by granting or denying access to the individual users or named group of users.

Memory must be protected so that its contents cannot be read after a process freeze it. That means once a particular process is over the contents of the memory should be flushed. Anybody else doing a memory dump should not be able to see what the previous activities were. Similarly, a secure file system such as NTFS should be protected. Then users must identify themselves in a unique manner such as a password, when they log on or auditing or auditable actions must identify the user performing the action.

The system administrators must be able to audit security related events that means the system should be capable of producing logs. However, access to the security related events audit data must be limited to authorized administrators. So, people who have a genuine need for looking at the logs, such as security auditors or people who are administering the particular machine only should have access to the logs.

The system must be protected from external interference or tampering such as modification of the running system or of systems files stored on the disk. So, this operating system should be adequately protected from external interference, like interference can be a hack or a tampering such as modification of the running system or of system files are stored on the disk. So the operating system should adequately protected from external interference. The interference can be a hack or a tampering such as modification of the running system, so that there should not be anyway to modify something to perform some other function on the system files which are stored on the disk. These are some of the important lists from the C2 level security implemented by POD.

(Refer Slide Time: 24:48)

Local Security Authority (LSA)

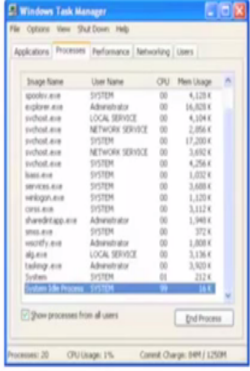



Image Name	User Name	CPU	Mem Usage
System Idle Process	SYSTEM	00	0 K
smss.exe	SYSTEM	00	4,128 K
explorer.exe	Administrator	00	16,320 K
notepad.exe	LOCAL SERVICE	00	4,104 K
notepad.exe	NETWORK SERVICE	00	2,884 K
notepad.exe	SYSTEM	00	17,208 K
notepad.exe	NETWORK SERVICE	00	3,960 K
notepad.exe	SYSTEM	00	4,264 K
lsass.exe	SYSTEM	00	1,632 K
services.exe	SYSTEM	00	3,688 K
winlogon.exe	SYSTEM	00	1,120 K
csrss.exe	SYSTEM	00	3,112 K
shareddiagapi.exe	Administrator	00	1,944 K
smss.exe	SYSTEM	00	372 K
smssfu.exe	Administrator	00	1,808 K
alg.exe	LOCAL SERVICE	00	3,136 K
taskmgr.exe	Administrator	00	3,920 K
System	SYSTEM	00	724 K

- Responsible for enforcing local security policy
 - Lsass.exe
 - User mode
- Issues security tokens to accounts
- Key component of the logon process



Now, we will look at local security authority or LSA. It is responsible for enforcing local security policy. Lsass.exe and user mode. Issues security tokens to the accounts. So, local security authority issues tokens to the account and it is a key component of the log on process. What does all this mean that means your local security authority resides in the user mode process names Lsass.exe and it is responsible for enforcing local security policy in Windows.

LSA is also responsible for validating users for both local and remote login. It issues security tokens to the accounts for people who log in. Now, if you talk about we just spoke about local security policy, what that local security policy password cum policy which is the complexity of whole expedition and renaming of administrators, enabling disabling of USB devices, auditing, policy privilege setting. Now, during the local or interactive log on to the machine. Here local means you are sitting in front of the system and performing a function, it is interacting with the computer.

So, during the local or interactive log on to the machine, a person enters his or her name and password in the log on page or in the log in dialogue. This information is passed to the local security authority which then calls the appropriate authentication package.