Name : Farhana Afrin Shikha

ID:IT-18038

Course Title:Operating system

CT:03

1.a)What do you mean by protection?Need of protection.	2+2
b) Describe the role of protection.	6
c) Write down the goals of protection.	4
2.a)What does operating system security mean?	4
b) What is authentication?	5
c) Describe about system threats.	5
3.a)Explain about program threat.	4
b) What is virtual machine and how does it work?	3+3
c) Why we use a virtual machine?	4
4.a)Write the advantages of virtual machine.	6
b) Describe about two types of virtual machine.	4
c) What does distributed operating system mean?	4

5.a)What are the advantages and disadvantages of distributed operating system? 2+2

b) Write down the reasons of distributed system? 6

c) Explain the types of distributed operating system. 4

6.a)Give some example of distributed operating system. 4

b) what are the features of distributed operating system? 5

c) Explain architecture of distributed operating system. 5

7.a)What is linux?Who created linux? 2+2

b)Why we need an operating system? 4

c)Describe the benefits of using linux. 6

8.a)What are the differences between linux and windows? 5

b)How does linux operating system work? 5

c)Explain linux licensing. 4

Answer to the question number (1)

a)

Protection: Protection refers to a mechanism which controls the access of programs, processes, or users to the resources defined by a computer system. We can take protection as a helper to multi programming operating system, so that many users might safely share a common logical name space such as directory or files.

Need of Protection:

- To prevent the access of unauthorized users and
- To ensure that each active programs or processes in the system uses resources only as the stated policy,
- To improve reliability by detecting latent errors.

b)

Role of Protection:

The role of protection is to provide a mechanism that implement policies which defines the uses of resources in the computer system.Some policies are defined at the time of design of the system, some are designed by management of the system and some are defined by the users of the system to protect their own files and programs.

Every application has different policies for use of the resources and they may change over time so protection of the system is not only concern of the designer of the operating system. Application programmer should also design the protection mechanism to protect their system against misuse.

Policy is different from mechanism. Mechanisms determine how something will be done and policies determine what will be done.Policies are changed over time and place to place. Separation of mechanism and policy is important for the flexibility of the system.

c)

Goals of protection:

- In one protection model, computer consists of a collection of objects, hardware or software
- Each object has a unique name and can be accessed throughν a well-defined set of operations
- Protection problem - ensure that each object is accessedν correctly and only by those processes that are allowed to do so

Answer to the question number (2)

a)

Security: Security refers to providing a protection system to computer system resources such as CPU, memory, disk, software programs and most importantly data/information stored in the computer system. If a computer program is run by an unauthorized user, then he/she may cause severe damage to computer or data stored in it. So a computer system must be protected against unauthorized access, malicious access to system memory, viruses, worms etc.

b)

Authentication:

Authentication refers to identifying each user of the system and associating the executing programs with those users. It is the responsibility of the Operating System to create a protection system which ensures that a user who is running a particular program is authentic. Operating Systems generally identifies/authenticates users using following three ways −

- Username / Password − User need to enter a registered username and password with Operating system to login into the system.
- User card/key − User need to punch card in card slot, or enter key generated by key generator in option provided by operating system to login into the system.
- User attribute - fingerprint/ eye retina pattern/ signature − User need to pass his/her attribute via designated input device used by operating system to login into the system.

c)

System Threats:

System threats refers to misuse of system services and network connections to put user in trouble. System threats can be used to launch program threats on a complete network called as program attack. System threats creates such an environment that operating system resources/ user files are misused. Following is the list of some well-known system threats.

- Worm − Worm is a process which can choked down a system performance by using system resources to extreme levels. A Worm process generates its multiple copies where each copy uses system resources, prevents all other processes to get required resources. Worms processes can even shut down an entire network.
- Port Scanning − Port scanning is a mechanism or means by which a hacker can detects system vulnerabilities to make an attack on the system.
- Denial of Service − Denial of service attacks normally prevents user to make legitimate use of the system. For example, a user may not be able to use internet if denial of service attacks browser's content settings

Answer to the question number (3)

a)

Program Threats:

Operating system's processes and kernel do the designated task as instructed. If a user program made these process do malicious tasks, then it is known as Program Threats. One of the common example of program threat is a program installed in a computer which can store and send user credentials via network to some hacker. Following is the list of some well-known program threats.

- Trojan Horse − Such program traps user login credentials and stores them to send to malicious user who can later on login to computer and can access system resources.
- Trap Door − If a program which is designed to work as required, have a security hole in its code and perform illegal action without knowledge of user then it is called to have a trap door.
- Logic Bomb − Logic bomb is a situation when a program misbehaves only when certain conditions met otherwise it works as a genuine program. It is harder to detect.
- Virus − Virus as name suggest can replicate themselves on computer system. They are highly dangerous and can modify/delete user files, crash systems. A virus is generatlly a small code embedded in a program. As user accesses the program, the virus starts getting embedded in other files/ programs and can make system unusable for user.

b)

Virtual machine:

A virtual machine (VM) is an operating system (OS) or application environment that is installed on software, which imitates dedicated hardware. The end user has the same experience on a VM as they would on dedicated hardware.

A VM provides an isolated environment for running its own OS and applications independently from the underlying host system or from other VMs on that host. The VM's OS is commonly referred to as the guest OS, and it can be the same as or different from the host OS or the other VMs. In this way, a single computer can host multiple VMs, all running different OSes and applications, without affecting or interfering with each other. The VM is still dependent on the host's physical resources, but those resources are virtualized and distributed across the VMs and can be reassigned as necessary, making it possible to run different environments simultaneously, as well as accommodate fluctuating workloads.

- From the user's perspective, the VM operates much like a bare-metal machine. In most cases, users connecting to a VM won't be able to tell that it's a virtual environment. The guest OS and its applications can be configured and updated as necessary and new applications installed or removed, without affecting the host or other VMs. Resources such as CPUs (central processing units), memory and storage appear much like they do on a physical computer. Although users might run into occasional glitches, such as not being able to run an application in a virtual environment, these types of issues tend to be minimal.

c)

- VMs help organizations consolidate servers and better utilize hardware resources. Because a single server can run multiple VMs simultaneously, organizations can use resources on a single server more efficiently, reducing the need to spread workloads across multiple servers, which often operate below capacity. In this way, organizations save capital and operating expenses.

- VMs provide isolated environments, making it possible to run different types of OSes and applications on a single server. Organizations can deploy legacy and business applications in

the environments they require, without having to deal with contention issues or needing to purchase multiple servers to support different environments.

- VMs make it easy to scale applications and accommodate fluctuating workloads, which is one reason virtualization plays such a key role in cloud computing and systems such as hyper-converged infrastructure (HCI).
- Organizations also turn to VMs because of the extra layer of security they provide against potential threats. If a VM is compromised, it can be deleted or rolled back to a recent backup or snapshot. Because it's isolated from the host and other VMs, the threat is limited to that VM.

Answer to the question number (4)

a)

Advantages of virtual machine:

Although containers and other modern application technologies have affected VM usage, VMs continue to be deployed extensively by organizations of all sizes because they offer several important benefits, including:

- Virtualization limits costs by reducing the need for physical hardware systems. VMs use hardware resources more efficiently than bare-metal deployments. This reduces the number of servers that must be deployed and the associated maintenance costs. It also lowers the demand for power and cooling.

- VMs are isolated, self-contained environments that can run different types of applications and OSes on the same server, eliminating potential contention and security issues, as well as the need to deploy multiple physical servers.
- VMs can be easily moved, copied and reassigned between host servers, as well as between on-premises and cloud environments, improving hardware resource utilization, while making it easier to scale applications.
- VMs ease management in multiple ways. Administrators, developers and testers can quickly deploy VMs, and multiple VMs can be easily managed from a centralized interface. Admins can also take advantage of virtual environments to simplify backups, disaster recovery (DR), new deployments and basic system administration tasks.
- Because VMs operate in isolated environments, they can provide an extra level of protection against malicious attacks. They also support such features as snapshots and backups, which make it easy to roll back a VM in the event the current one becomes compromised or corrupted.

b)

Two types of VM:

VMs are often categorized by the type of hypervisor that manages them or by the type of workloads they support. However, VMs are also categorized by VM type:

1. Process VMs. A process VM is a temporary, platform-independent programming environment for executing a single process as an application. The environment provides a high-level abstraction that masks the underlying hardware or OS. A process VM is created when the process starts and is destroyed when the process ends. Two common examples of process VMs are Java Virtual Machine, which is part of the Java platform, and Common Language Runtime, which is used for the .NET Framework.
2. System VMs. A system VM is a fully virtualized environment that's hosted on a physical server and runs its own OS. The VM shares the host's physical resources but provides a complete environment for running applications and services, like a physical machine, but without the overhead. System VMs rely on a hypervisor to virtualize the hardware resources

and make them available to VM environments. Common examples of system VMs include those supported by virtualization platforms such as VMware vSphere and Microsoft Hyper-V.

c)

Distributed operating system:

An operating system (OS) is basically a collection of software that manages computer hardware resources and provides common services for computer programs. Operating system is a crucial component of the system software in a computer system.

Distributed Operating System is one of the important type of operating system.

Multiple central processors are used by Distributed systems to serve multiple real-time applications and multiple users. Accordingly, Data processing jobs are distributed among the processors.

Processors communicate with each other through various communication lines (like high-speed buses or telephone lines). These are known as loosely coupled systems or distributed systems. Processors in this system may vary in size and function. They are referred as sites, nodes, computers, and so on.

Answer to the question number (5)

a)

Advantages of Distributed Operating System:

- The load on the system decreases.
- If one system stops it will not affect the other.
- The system shares a workload that makes calculations easy.

- The size of the system can be set according to requirements.

Disadvantages of Distributed Operating System:

- The cost for set up is more.
- Failure of the main system will affect the whole system.
- Programming is complex.

b)

Reasons for distributed systems :

- Resource sharing
  - Sharing and printing files at remote sites
  - Processing information in a distributed database
  - Using remote specialized hardware devices

- Computation speedup – load sharing or job migration
- Reliability – detect and recover from site failure, functionλ transfer, reintegrate failed site Communication – message passing
  - All higher-level functions of a standalone system can be4 expanded to encompass a distributed system
- Computers can be downsized, more flexibility, better userλ interfaces and easier maintenance by moving from large system to multiple smaller systems performing distributed computing

c)

There are mainly two types of distributed operating system, they are as follows:

1. Client/Server Systems

In this system, the client requests the server for a resource. On the other hand, the server provides this resource to the client. One client contacts only a single server at a time. Whereas a single server can deal with multiple clients simultaneously. The clients and servers connect through a computer network in the system.

2. Peer to Peer Systems

In this system, the nodes play an important role. All the work equally divides among the nodes. Furthermore, these nodes can share data or resources as per the requirement. Again, they require a network to connect.

Answer to the question number (6)

a)

Examples of Distributed Operating System:

Few examples of a distributed OS are as follows:

- AIX operating system for IBM RS/6000 computers.
- Solaris operating system for SUN multiprocessor workstations.
- Mach/OS is a multitasking and multithreading UNIX compatible operating system.
- OSF/1 operating system

b)

The features of distributed os are as follows:

1. Resource Sharing

The main important feature of this system is that it allows users to share resources. Moreover, they can share resources in a secure and controlled manner. Resources can be of any type. For example, some common resources which are shared can be printers, files, data, storage, web pages, etc.

2. Openness

This means that the services which the system provides are openly displayed through interfaces. Moreover, these interfaces provide only the syntax of the services. For example, the type of functions, their return types, parameters, etc. These interfaces use Interface Definition Languages (IDL).

3. Concurrency

It means that several tasks take place at different nodes of the system simultaneously. Moreover, these tasks can also interact with each other. It results in increasing the efficiency of the system.

4. Scalability

It refers to the fact that the efficiency of the system should not change when more nodes are added to the system. Moreover, the performance for the system with 100 nodes should be equal to the system with 1000 nodes.

5. Fault Tolerance

It means that the user can still work with the system in the case, hardware, or software fails.

6. Transparency

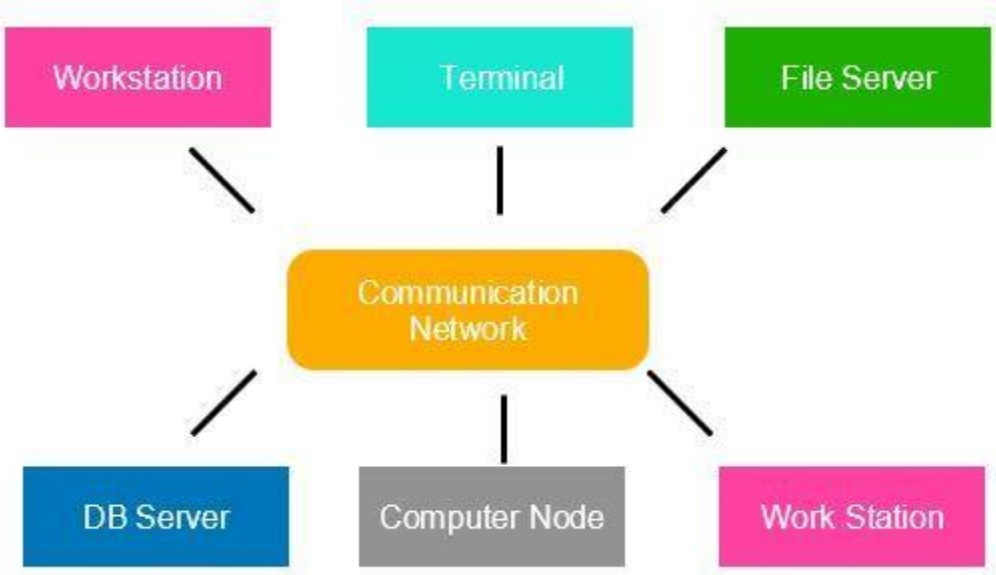
It is the most important feature of the system. The main goal of a distributed OS is to hide the fact that the resources are being shared.

c)

Architecture of a Distributed Operating System:
In a DOS the following occurs:

- All software and hardware compounds are located remotely. In order for them to communicate with each other, they pass messages.
- One of the most important aspects of a distributed system is resource sharing. Resources are managed by servers and clients use these resources.

A DOS runs on a number of independent sites which are connected through a communication network. However it is portrayed to the user that they run their own operating system.



Answer to the question number (7)

a)

Linux:

LINUX is an operating system or a kernel distributed under an open-source license. Its functionality list is quite like UNIX. The kernel is a program at the heart of the Linux operating system that takes care of fundamental stuff, like letting hardware communicate with software.

Who created Linux:

Linux is an operating system or a kernel which germinated as an idea in the mind of young and bright Linus Torvalds when he was a computer science student. He used to work on the UNIX OS (proprietary software) and thought that it needed improvements.

However, when his suggestions were rejected by the designers of UNIX, he thought of launching an OS which will be receptive to changes, modifications suggested by its users.

b)

Why do you need an OS:

Every time you switch on your computer, you see a screen where you can perform different activities like write, browse the internet or watch a video. What is it that makes the computer hardware work like that? How does the processor on your computer know that you are asking it to run a mp3 file?

Well, it is the operating system or the kernel which does this work. So, to work on your computer, you need an Operating System(OS). In fact, you are using one as you read this on your computer. Now, you may have used popular OS's like Windows, Apple OS X, but here we will learn introduction to Linux operating system, Linux overview and what benefits it offers over other OS choices.

c)

The benefits of using Linux:

Linux OS now enjoys popularity at its prime, and it's famous among programmers as well as regular computer users around the world. Its main benefits are -

It offers a free operating system. You do not have to shell hundreds of dollars to get the OS like Windows!

- Being open-source, anyone with programming knowledge can modify it.
- It is easy to learn Linux for beginners
- The Linux operating systems now offer millions of programs/applications and Linux softwares to choose from, most of them are free!

- Once you have Linux installed you no longer need an antivirus! Linux is a highly secure system. More so, there is a global development community constantly looking at ways to enhance its security. With each upgrade, the OS becomes more secure and robust

- Linux freeware is the OS of choice for Server environments due to its stability and reliability (Mega-companies like Amazon, Facebook, and Google use Linux for their Servers). A Linux based server could run non-stop without a reboot for years on end.

Answer to the question number (8)

a)

Here is the main difference between Windows and Linux:

Windows	Linux
Windows uses different data drives like C: D: E to stored files and folders.	Unix/Linux uses a tree like a hierarchical file system.
Windows has different drives like C: D: E	There are no drives in Linux
Hard drives, CD-ROMs, printers are considered as devices	Peripherals like hard drives, CD-ROMs, printers are also considered files in Linux/Unix
There are 4 types of user account types 1) Administrator, 2) Standard, 3) Child, 4) Guest	There are 3 types of user account types 1) Regular, 2) Root and 3) Service Account
Administrator user has all administrative privileges of computers.	Root user is the super user and has all administrative privileges.
In Windows, you cannot have 2 files with the same name in the same folder	Linux file naming convention is case sensitive. Thus, sample and SAMPLE are 2 different files in Linux/Unix operating system.
In windows, My Documents is default home directory.	For every user /home/username directory is created which is called his

	home directory.

b)

How Linux Works:

Not everyone uses Linux because it is a little harder to manage than Microsoft Windows, however if you get use to it there are more configuration options than Windows and it offers more flexibility of usage.

- Linux Kernel: The Linux kernel is what distinguishes the Linux operating system from other systems. The kernel is located in the central portion of the operating system and controls the operating system security, hardware interfaces, and acts as the primary resource for the operating system itself. The kernel contains a source code that is available to everyone which allows you to edit and modify your operating system to suit your individual needs. Many companies and organizations have used the kernel to design operating systems that are customized to their company's needs and requirements.
- Server Platform: Linux is referred to as a server platform because it has the capability to form the foundation for which an operating system can be built and has been used as an alternative to the Microsoft Windows operating system. Because of its capability to act as a platform it can also be used as a microchip for other devices and appliances.

c)

Linux Licensing:

Linus Torvalds has given linux kernel license to GNU General Public License (GPL) version 2. GNU make sure that any software source code licensed under it have to make originating source code open and freely availble to all its users. Here, freely doesn't mean by cost but it means that it is freely available to users to distribute and modify the code.

There is the third version of GNU, GNU Lesser General Public License (LGPL) version 3. But it imposes some more permissions on the license. Torvalds doesn't like some provisions in version 3 and have announced that linux kernel will not come under version 3.