Name: Sayma Akter Shumi **ID: IT-18032**

1. a) What is Error handling? Write about I/O protection? 2+2

b) Define I/O interface? Write down application of I/O interface? 2+3

c)Differentiate between interrupt & polling? 5

2. a) What is polling? What is the main purpose of power management? 2+2

b) Draw a kernel I/O structure? 5

c) What are the common security threats? Explain 5

3. a) Describe difference between protection & security in OS? 4

b) What is domain switching? Write down the goals of protection in OS? 2+2

c) What is security problem? How we can prevent security threats? 2+4

4. a) What is virtual machine? How do virtual machine work?

How do virtual machines relate to operating systems? 2+3

b) Why do we need virtual machine in OS? 4

c) How do I use a virtual machine? Is virtual safe? 2+3

5. a) Write different virtual machine program? 5

b) How many types of virtual machine are there? 4

c) Explain advantages & disadvantages of virtual machine? 5

6. a) What is Java virtual machine? Write down its benefits? 2+2

b) Discuss two types of distributed operating system? 5

c) Describe advantages & disadvantages of distributed operating system? 5

7. a) Define network operating system? Write down types of network operating system? 2+2

b) Differentiate between distributed operating system & network operating system? 5

c) What is routing? Why is routing so important in OS? 2+3

8. a) What is Linux in OS? Why do we use Linux? 2+3

b) What are the advantages of Linux? 5

c) Write down the security system goals? 4

Answer to the question number (1)

a)

Error handling:

Error handling refers to the routines in a program that respond to abnormal input or conditions. The quality of such routines is based on the clarity of the error messages and the options given to users for resolving the problem.

I/O protection:

Input/output is protected by making all input/output instructions privileged. While running in user mode, the CPU cannot execute them; thus, user code, which runs in user mode, cannot execute them. User code requests I/O by making appropriate system calls.

b)

I/O interface:

The method that is used to transfer information between internal storage and external I/O devices is known as I/O interface. There exists special hardware components between CPU and peripherals to supervise and synchronize all the input and output transfers that are called interface units.

Application of I/O interface:

- I/O system calls encapsulate device behaviors in generic classes
- Device-driver layer hides differences among I/O controllers from kernel
- Devices vary in many dimensions
- Character-stream or block
- Sequential or random-access
- Sharable or dedicated
- Speed of operation
- read-write, read only, or write only
- Operating System Concepts.

c)

Difference between interrupt & polling:

- In interrupt, the device notifies the CPU that it needs servicing whereas, in polling CPU repeatedly checks whether a device needs servicing.
- Interrupt is a hardware mechanism as CPU has a wire, interrupt-request line which signal that interrupt has occurred. On the other hands, Polling is a protocol that keeps checking the **control bits** to notify whether a device has something to execute.
- Interrupt handler handles the interrupts generated by the devices. On the other hands, in polling, CPU services the device when they require.
- Interrupts are signalled by the interrupt-request line. However, Command-ready bit indicate that the device needs servicing.
- In interrupts, CPU is only disturbed when any device interrupts it. On the other hand, in polling, CPU waste lots of CPU cycles by repeatedly checking the command-ready bit of every device.
- An interrupt can occur at any instant of time whereas, CPU keeps polling the device at the regular intervals.

- Polling becomes inefficient when CPU keeps on polling the device and rarely finds any device ready for servicing. On the other hands, interrupts become inefficient when the devices keep on interrupting the CPU processing repeatedly.

Answer to the question number (2)

a)

Polling:

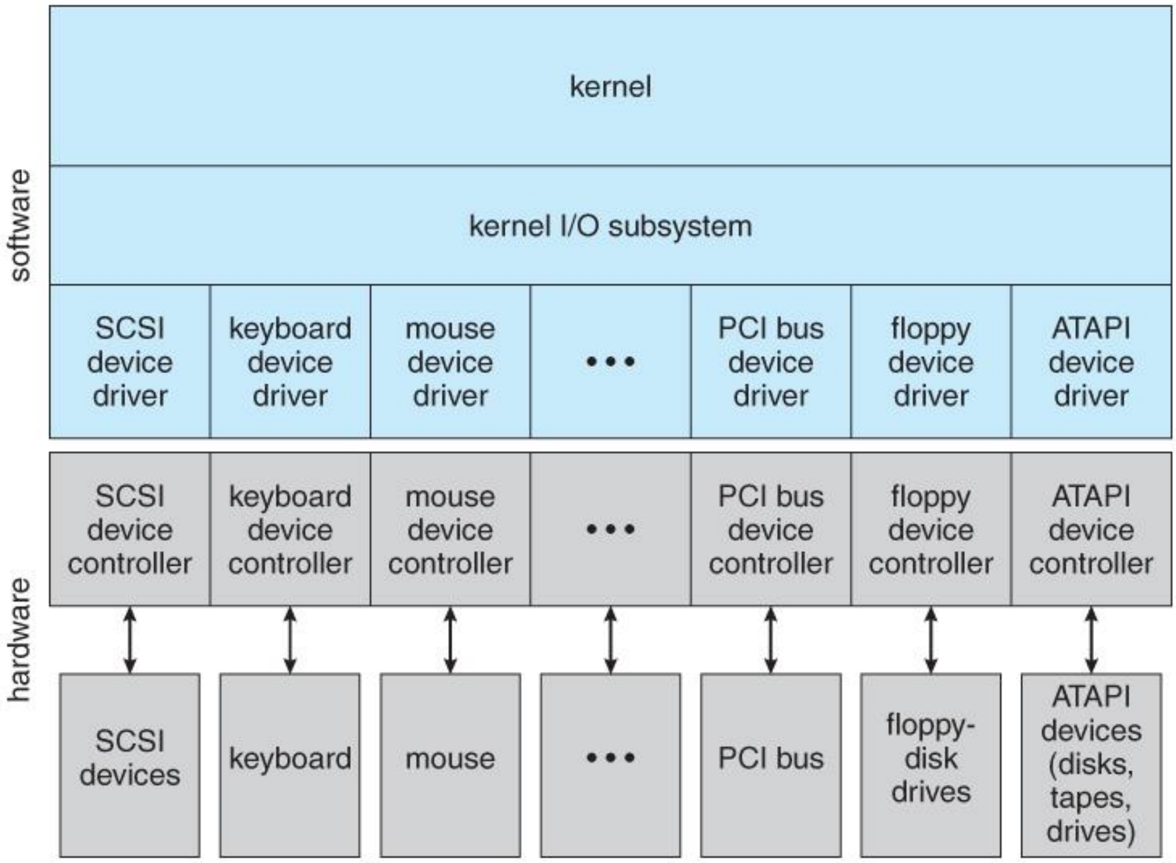
Polling is the process where the computer or controlling device waits for an external device to check for its readiness or state, often with low-level hardware. Although not as wasteful of CPU cycles as busy waiting, this is generally not as efficient as the alternative to polling, interrupt-driven I/O.

Purpose of power management:

Device power management automatically reduces the amount of power used by individual devices when they are not in demand to perform some function. Disk drives, monitors, adapters, and even CPUs can provide this power-saving feature. The effect of device power management is transparent to the computer user.

b)

Kernel I/O structure:



c)

Common security threats:

- Spam. Spam is one of the most common security threats. ...
- Pharming
- Phishing. ...
- Ransomware. ...
- Computer worm. ...
- Spyware / Trojan Horse. ...
- Distributed denial-of-service attack. ...
- Network of zombie computers.

Another reason that operating system security is so important is that ultimately all of our software relies on proper behavior of the underlying hardware: the processor, the memory, and the peripheral devices. So large, complex programs are likely to be harder to Page 2 secure than small, simple programs.

Answer to the question number (3)

a)

Difference between protection & security in OS:

Definition

Protection is a method used in operating systems that manages threats within the system to maintain the proper functioning of the system. Security is a method used in operating systems that handles the threats from outside of the system to maintain the proper functioning of the system. This constitutes the basic difference between protection and security.

Main Focus

The main difference between protection and security is that while protection focuses on internal threats of the system, security focuses on external threats to the system.

Functionality

Protection provides a mechanism for controlling the access to programs, processes, and user resources. Security provides a mechanism to safeguard the system resources and user resources from external users.

Policy

Another difference between protection and security is their policy. Protection policy specifies whether a user can access a specific resource. The owner of the resource performs this function when creating it. Security policy specifies whether a person can become a user of the system. It is performed by the system administrator.

Mechanisms

Furthermore, protection involves mechanisms such as setting or changing protection information of a resource and checking whether that resource is accessible by a user. Security involves mechanisms such as adding, deleting users, verifying whether a specific user is authorized, using anti-malware software, etc.

Conclusion

There is a distinct difference between protection and security even though these two words are used interchangeably, The difference between protection and security is that protection focuses on internal threats in a computer system while Security focuses on external threats of a computer system.

b)

Domain switching is achieved by a process in one ring calling upon a process operating in a lower ring, which is controlled by several factors stored with each segment descriptor: An access bracket, defined by integers b1 <= b2.

Goals of protection in OS:

- Obviously to prevent malicious misuse of the system by users or programs. See chapter 15 for a more thorough coverage of this goal.
- To ensure that each shared resource is used only in accordance with system policies, which may be set either by system designers or by system administrators.
- To ensure that errant programs cause the minimal amount of damage possible.
- Note that protection systems only provide the mechanisms for enforcing policies and ensuring reliable systems. It is up to administrators and users to implement those mechanisms effectively.

c)

Security problem:

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.

Prevention of security threats:

- Install Anti-Virus Software
- Ensure that the anti-virus software is up to date
- Employ a firewall to protect networks
- Filter all email traffic
- Educate all users to be careful of suspicious e-mails
- Scan Internet Downloads
- Don't run programs of unknown origin
- Implement a vulnerability management program.

Answer to the question number (4)

a)

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.

The virtual machine runs as a process in an application window, similar to any other application, on the operating system of the physical machine. Key files that make up a virtual machine include a log file, NVRAM setting file, virtual disk file and configuration file.

Virtual Machine abstracts the hardware of our personal computer such as CPU, disk drives, memory, NIC (Network Interface Card) etc, into many different execution environments as per our requirements, hence giving us a feel that each execution environment is a single computer. For example, VirtualBox.

b)

Need for virtual machines varies from user to user. For example

1.Using different Operating system:

If someone needs to work on different operating system on top of another OS. E.g. You may want to use Linux for your work on top of windows. This is one the best use of virtual machine.

2. Running old applications:

If you have an application that won't support on windows 10 or windows 8 but supports on windows 7, all you need to do is install windows 7 within virtual machine and use it. You don't need to install windows 7 for that application.

3. Testing softwares:

If you are a developer and working on some new software and wants to test its functionality you can use virtual machines for this purpose. Primary reason to use virtual machine for this is in case your software gets crashes in between it won't effect your memory including your hard disk and ram of your host operating system.

4. Easy to replicate:

Once you have installed your operating system in virtual machine and configured it completely then virtual machines can be saved as appliance. This appliance can be used by another user and can be easily copied and used on another computer.

5. Creating your personal cloud computer:

If you don't want to take your laptop to office, leave it and take your mobile and access the laptop via Remote Desktop Protocol (RDP) over the internet. This will let you access same laptop environment. (may be with no fancy graphics).

c)

To create a virtual machine using VMware Workstation:

- Launch VMware Workstation.
- Click New Virtual Machine.
- Select the type of virtual machine you want to create and click Next: ...
- Click Next.
- Select your guest operating system (OS), then click Next. ...
- Click Next.
- Enter your Product Key.
- Create a user name and password.

Virtual machines are an isolated environment from the physical operating system, so you can run potentially dangerous stuff, such as malware, without fear of compromising your main OS. They're a safe environment, but there are exploits against virtualization software, allowing malware to spread to the physical system.

Answer to the question number (5)

a)

There are several different virtual machine programs you can choose from:

VirtualBox: (Windows, Linux, Mac OS X): VirtualBox is very popular because it's open-source and completely free. There's no paid version of VirtualBox, so you don't have to deal with the usual "upgrade to get more features" upsells and nags. VirtualBox works very well, particularly on Windows and Linux where there's less competition, making it a good place to start with VMs.

· **VMware Player**: (Windows, Linux): VMware has their own line of virtual machine programs. You can use VMware Player on Windows or Linux as a free, basic virtual machine tool. More advanced features—many of which are found in VirtualBox for free—require upgrading to the paid VMware Workstation program. We recommend starting out with VirtualBox, but if it doesn't work properly you may want to try VMware Player.

· **VMware Fusion**: (Mac OS X): Mac users must buy VMware Fusion to use a VMware product, since the free VMware Player isn't available on a Mac. However, VMware Fusion is more polished.

· **Parallels Desktop**: (Mac OS X): Macs also have Parallels Desktop available. Both Parallels Desktop and VMware Fusion for Mac are more polished than the virtual machine programs on other platforms, since they're marketed to average Mac users who might want to run Windows software.

b)

The Two Types of Virtual Machines:

· **Process virtual machines**: Execute computer programs in a platform independent environment. It masks the information of the underlying hardware or operating system.

· **System virtual machines**: Support the sharing of a host computer's physical resources between multiple virtual machines.

c)

The main advantages of virtual machines:

- Multiple OS environments can exist simultaneously on the same machine, isolated from each other;
- Virtual machine can offer an instruction set architecture that differs from real computer's;
- Easy maintenance, application provisioning, availability and convenient recovery.

Disadvantages of virtual machines:

- Virtual machines are less efficient than real machines because they access the hardware indirectly. Running software on top of the host operating system means that it will have to request access to the hardware from the host. That will slow the usability.
- When several virtual machines are running on the same host, performance may be hindered if the computer it's running on lacks sufficient power. Your virtual machine still uses the resources of your host machine. The more powerful the host computer, the more quickly the virtual machine will run.
- A virtual machine can be infected with the weaknesses of the host machine. As an example, process isolation is a feature usually employed by operating systems. However, there are bugs that violate it. A regular computer devoid of virtual machines would then only be affected. But, a computer with a number of virtual machines would then infect each of those "machines" as well.

Answer to the question number (6)

a)

Java virtual machine:

A Java virtual machine (JVM) is a virtual machine that enables a computer to run Java programs as well as programs written in other languages that are also compiled to Java bytecode. The JVM reference implementation is developed by the OpenJDK project as open source code and includes a JIT compiler called HotSpot.

Benefits of JVM:

- **Multiplatform.** The Java virtual machine interprets/JITs the same bytecodes, thus, because of that, the same Java binaries can run without modification in any platform where a JVM exists.
- **Control.** The JVM takes control of several tasks: Memory management, exception handling, memory safe references, sandboxing, etc.

b)

There are two types of Distributed Operating Systems:

- Network Operating Systems
- Distributed Operating Systems

Network-Operating Systems:

- Users are aware of multiplicity of machines
- Access to resources of various machines is done explicitly by:

1. Remote logging into the appropriate remote machine (telnet, ssh)

2. Remote Desktop (Microsoft Windows)

3. Transferring data from remote machines to local machines, via the File Transfer Protocol (FTP) mechanism

- Users must change paradigms – establish a session, give network based Commands

    1. More difficult for users

Distributed operating system :

- Users not aware of multiplicity of machines

    Access to remote resources similar to access to local Resources

- Data Migration – transfer data by transferring entire file, or transferring only those portions of the file necessary for the immediate task

- Computation Migration – transfer the computation, rather than the data, across the system

    Via remote procedure calls (RPCs)

    or via messaging systemore difficult for users.

c)

Some advantages of Distributed Systems are as follows –

- All the nodes in the distributed system are connected to each other. So nodes can easily share data with other nodes.

- More nodes can easily be added to the distributed system i.e. it can be scaled as required.

- Failure of one node does not lead to the failure of the entire distributed system. Other nodes can still communicate with each other.
- Resources like printers can be shared with multiple nodes rather than being restricted to just one.

Some disadvantages of Distributed Systems are as follows –

- It is difficult to provide adequate security in distributed systems because the nodes as well as the connections need to be secured.

- Some messages and data can be lost in the network while moving from one node to another.

- The database connected to the distributed systems is quite complicated and difficult to handle as compared to a single user system.

- Overloading may occur in the network if all the nodes of the distributed system try to send data at once.

Answer to the question number (7)

a)

Network Operating System:

A network operating system (NOS) is an operating system that manages network resources: essentially, an operating system that includes special functions for connecting computers and devices into a local area network (LAN).

Types of Network Operating System:

There are two basic types of network operating systems, the peer-to-peer NOS and the client/server NOS:

1. Peer-to-peer network operating systems allow users to share network resources saved in a common, accessible network location. In this architecture, all devices are treated equally in terms of functionality. Peer-to-peer usually works best for small to medium LANs and is cheaper to set up.
2. Client/server network operating systems provide users with access to resources through a server. In this architecture, all functions and applications are unified under one file server that can be used to execute individual client actions regardless of physical location. Client/server tends to be most expensive to implement and requires a large amount of technical maintenance. An advantage to the client/server model is that the network is controlled centrally, makes changes or additions to technology easier to incorporate.

b)

Difference between Network Operating System & Distributed Operating System:

1. The main goal of the network operating system is to provide local services to the remote client. On the other hand, the objective of the distributed operating system is to provide the hardware resource management.
2. Network operating systems are said to be loosely coupled systems and are used in heterogeneous computers. As against, distributed operating system is considered as tightly coupled systems mainly used in multiprocessors or homogeneous computers.
3. The network operating system has two-tier client/server architecture, while n-tier architecture is employed in the distributed operating system.
4. Transparency in the network operating system is low. Conversely, the distributed operating system has high transparency, and it hides the resource utilisation.
5. In the distributed operating system the communication between the computers (nodes) is achieved by shared memory or sending messages. On the contrary, the network operating system sends files in order to communicate with other nodes.
6. Network operating system manages resources at each node while in the distributed operating system, the resources are globally managed whether it is centred or distributed.
7. The network operating system is easily implemented as compared to the distributed operating system.

8. Scalability of the network operating system is higher than the distributed operating system, and also it is more open to the user.
9. In network operating system the operating system installed in the computers can vary whereas it is not the case in the distributed operating system.
10. The network operating system is more autonomous than the distributed operating system. In contrast, the distributed operating system is more fault tolerant.

c)

Routing:

Routing is a process which is performed by layer 3 (or network layer) devices in order to deliver the packet by choosing an optimal path from one network to another. Static routing is a process in which we have to manually add routes in routing table.

Importance of routing:

It's vitally important to the Internet and we tend to overlook it until something goes wrong. Routing determines how packets (data sent over a network or networks) containing information, like email messages, website data, and voice-over-IP (VoIP) calls, move from one place to another on the Internet.

Answer to the question number (8)

a)

Linux:

Linux is one of popular version of UNIX operating System. It is open source as its source code is freely available. It is free to use. Linux was designed considering UNIX compatibility. Its functionality list is quite similar to that of UNIX.

So, being an efficient OS, Linux distributions could be fitted to a range of systems (low-end or high-end). In contrast, Windows operating system has a higher hardware requirement. ... Well, that is the reason most of the servers across the world prefer to run on Linux than on a Windows hosting environment.

b)

Advantages of Linux:

- Open Source. One of the main advantages of Linux is that it is an open source operating system i.e. its source code is easily available for everyone.
- Security.
- Revive older computer systems.
- Software Updates.
- Customization.
- Various Distributions.
- Free to use (Low Cost) .
- Large Community Support.

c)

The following security goals are aimed:

Integrity:

The objects in the system mustn’t be accessed by any unauthorized user & any user not having sufficient rights should not be allowed to modify the important system files and resources.

Secrecy:

The objects of the system must be accessible only to a limited number of authorized users. Not everyone should be able to view the system files.

Availability:

All the resources of the system must be accessible to all the authorized users i.e. only one user/process should not have the right to hog all the system resources. If such kind of situation occurs, denial of service could happen. In this kind of situation, a malware might hog the resources for itself & thus preventing the legitimate processes from accessing the system resources.