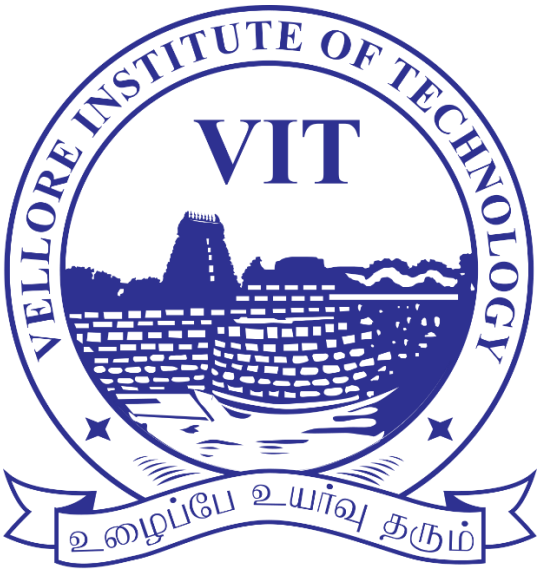


OPERATING SYSTEMS

DIGITAL ASSIGNMENT-1

Name: **VIBHU KUMAR SINGH**
Reg. No: **19BCE0215**
Teacher: **Manikandan K.**

1) Consider a file system in which a file can be deleted and its disk space reclaimed while links to that file still exist. What problems may occur if a new file is created in the same storage area or with the same absolute path name? How can these problems be avoided?

DATE: __/__/__

Ans1) Let F_1 be the old file and F_2 be the new file. A user wishing to access F_1 through an existing link will actually access F_2. Note that the access protection for file F_2 is used rather than the one associated with F_2.

This problem can be avoided by ensuring that all links to a deleted file are deleted also. This can be accomplished in several ways:

a) maintain a list of all links to a file, removing each of them when the file is deleted.

b) retain the links, removing them when attempt is made to access a deleted file.

c) maintain a file reference list (or counter), deleting the file only after all links or references to that file have been deleted.

2) Consider a file system that uses a modified contiguous-allocation scheme with support for extents. A file is a collection of extents, with each extent corresponding to a contiguous set of blocks. A key issue in such systems is the degree of variability in the size of the extents. What are the advantages and disadvantages of the following schemes?

a. All extents are of the same size, and the size is predetermined.

b. Extents can be of any size and are allocated dynamically.

c. Extents can be of a few fixed sizes, and these sizes are predetermined.

DATE: __/__/____

Ans 2) If all extents are of the same size, and the sizes is predetermined, then it simplifies the block allocation scheme. A simple bit map or free list for extents would suffice. If ithe extents can be of any size and are allocated dynamically, then more complex allocation schemes are required. It might be difficult to find an extent of the appropriate size and there might be external fragmentation. One could use the Buddy System allocator discussed in the previous chapter to design an appropriate allocator.

When the extents be of few fixed sizes, and these sizes are predetermined, one would have to maintain a seperate bitmap or free list for each possible size. This scheme is of intermediate complexity and of intermediate flexibility in comparison to the earlier schemes.

3) If all the access rights to an object are deleted, the object can no longer be accessed. At this point the object should also be deleted, and the space it occupies should be returned to the system. Suggest an efficient implementation of this scheme.

DATE: __/__/__

Ans 3) We should use reference count scheme for the given problem. The reason for this are as follows:

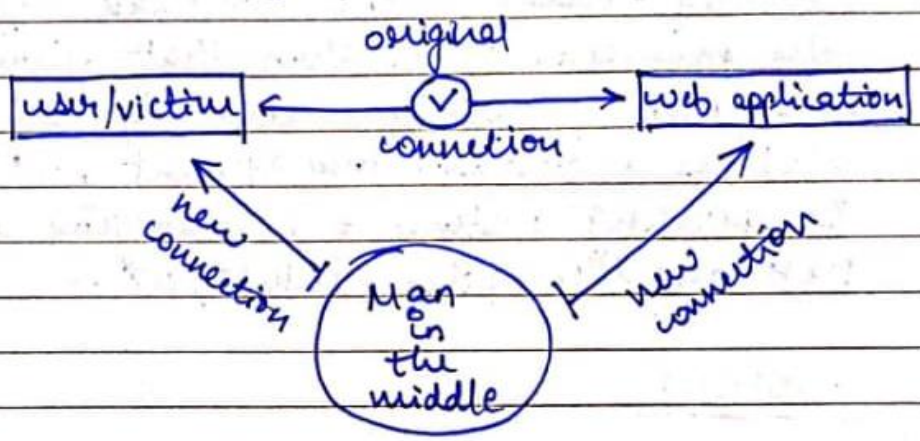
> Reference counting approach is super simple. It is based on the idea of counting the number of pointer references to an allocated object. It's a direct method that also happens to be naturally incremental as it distributes the memory management overhead throughout the program. Other than that memory management, reference counting is also broadly used as a resource management mechanism in operating systems for managing system resources like files, sockets, etc.

WORKING

Under reference counting approach, each allocated object contains a reference counter field. The memory manager is responsible for maintaining the invariant that -- at all times -- the reference count of each object is equal to the number of direct pointer references to that object.

4) What commonly used computer programs are prone to man-in-the-middle attacks? Discuss solutions for preventing this form of attack.

Ans 4) A man-in-the-Middle (MITM) attack happens when a hacker inserts themselves between a user and a website. This kind of attack comes in several forms. For eg, a fake banking website may be used to capture financial login information. This fake site is "in the middle" between the user and the actual bank website.



There are various types of MITM attacks, such as:

① Wifi Eavesdropping:
Wifi eavesdropping attack happens when a hacker creates its own wifi hotspot, called an "Evil Twin". They make the connection look just like the authentic one, down to the network ID and password. Users may accidentally (or automatically) connect to the "Evil Twin", allowing the hacker to snoop on their activity.

DATE: __/__/____

② DNS spoofing:

A hacker can create a fake DNS server. This is called "spoofing". The fake server routes a real website name to a different IP address. The hacker can create a phony website at the new IP address that looks just like a genuine website. Once you visit the fake site, an attacker can gain access to your sensitive information and personal data.

③ IP spoofing attacks:

In IP spoofing, hackers mimic the IP address of an authorized device. To the network, the device looks like its approved. This can allow an unauthorized user to infiltrate a network. They may stay silent, and record activity or they launch a Denial of Service (DoS) attack.

④ Email Hijacking:

In this type of cyber security attack, a hacker compromises a user's email account. Often, the hacker silently waits, gathering information and eavesdropping on the email conversations. Hackers may have a search script that looks for specific words, like "bank" or "secret document strategies".

DATE: __/__/____

Email hijacking work well with social engineering, hackers might use information from a hacked account to impersonate an online friend for taking out information and plan on attack.

MITM Prevention:

1) Use a Virtual Private Network (VPN) to encrypt your web traffic.

2) Secure your network with intrusion detection system.

3) Have long firewalls and protocols to prevent unauthorized access. Use third-party penetration testing tools, software, and HTTPS encryption to help detect block spoofing attempts.

4) Install antivirus and malware protection.

5) Sure your communications encryption is the best defence to protect against encrypted communication.

6) Avoid using public-wifi networks.

5) Discuss the following with neat diagram

a. Virtualization and its types

b. Hypervisor

Ans 5 a) Virtualization is a technique of how to separate a service from the underlying physical delivery of that service. It is the process of creating a virtual version of something like computer hardware. It is initially developed during the mainframe era. It involves using specialized software to create a virtual or software-created version of a computer resource rather than the actual version of the same resource.

With the help of virtualization, multiple OS and application can run on same machine and its hardware at the same time, increasing the utilization and flexibility of hardware.

In other words, one of the main cost effective, hardware reducing, and energy saving techniques used by cloud providers is virtualization. It allows to share a single physical instance of a resource or an application among multiple customers and organizations at the same time. It does this by assigning a logical name to a physical storage and providing a pointer to that physical resource on demand. The term virtualization is often synonymous with hardware virtualization, which plays a fundamental role in effecting delivering Infrastructure-as-a-Service (IaaS) solutions for cloud computing. Moreover, virtualization technologies provide a virtual environment for not only executing applications

DATE: / /

but also for storage, memory and networking.

* Types of Virtualization :

1> Application Virtualization

Application virtualization helps a user to have a remote access of an application from a server. The server stores all personal information and other characteristics of the application but can still run on a local workstation through internet. Example of this would be a ~~one~~ user who wnts to run two different versions of the same software. Technologies that use application virtualization are hosted applications and packaged applications.

2> Network virtualization

The ability to run multiple virtual networkes with each has a seperate control and data plan. It co-exists together on top of one physical network. It can be managed by individual parties that potentially confidential to each other.

Network virtualization allows the users OS to be remotely on a service in the data center. It allows the user to access their desktop virtually, from any location by different machine. Users who wants

DATE: __/__/__

Network virtualization provides a facility to create and provision virtual networks — logical switches, routers, firewalls, load balancer, Virtual Private Network (VPN), and workload security within days or even in weeks.

3> Desktop Virtualization

Desktop virtualization allows the user's OS to be remotely stored in a server in the data center. It allows the user to access their desktop virtually, from any location by different machine. Users who want specific operating systems other that Windows Server will need to have a virtual desktop. Main benefits of desktop virtualization are user mobility, portability, easy management of software installation, updates and patches.

4> Storage Virtualization

Storage virtualization is an array of servers that are managed by a virtual storage system. The servers aren't aware of exactly where their data is stored, and instead function more like worker bees in a hive. It makes managing storage from multiple sources to be udnudged and utilized as a single repository. Storage virtualization software maintenit smooth operations, consistent performance and a continuous suite of advanced functions despite changes, break down and

differences in the underlying equipment.

* Benefits of Virtualization:

1) More effient and flexible allocation of resources.

2) Enhance development productivity.

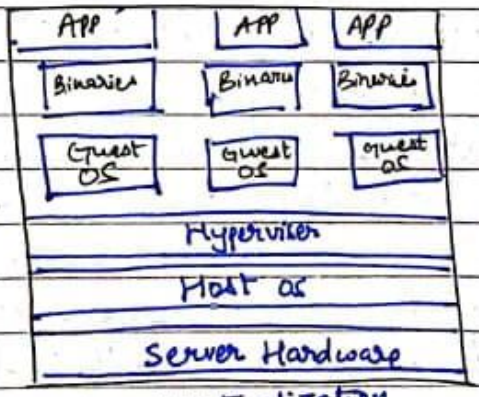
3) It lowers the cost of IT infrastructure.

4) Remote access and rapid scalibility.

5) High availibity and disaster recovery.

6) Pay per use of the IT infrastructure on demand.

7) Enables running multiple OS.



Virtualization Diagram

DATE: __/__/____

Ans 5b) Hypervisor is a form of virtualization software used in Cloud hosting to divide and allocate the resources on various pieces of hardware. The program which provide partitioning, isolation or abstraction is called virtualization hypervisor.
Hypervisor is a hardware virtualization technique that allows multiple guest OS to run on a single host system at the same time. A hypervisor is sometimes also called a virtual machine manager (VMM).

* Types of Hypervisor:

1) Hypervisor runs directly on underlying host system. It is also known as "Native Hypervisor" or "bare metal hypervisor". It does not require any base server OS. It has direct access to hardware resources. Examples of type 1 hypervisor include VMware ESXi, Citrix, XenServer and Microsft Hyper-V hypervisor.

2) Type 2 Hypervisor:

A host operating system runs on underlying host system. It is also known as "Hosted Hypervisor". Basically a software installed on an operating system. Hypervisor asks OS to make hardware calls. Example of Type 2 hypervisors include VMware player or Parallel Desktop. Hosted hypervisors are often found on endpoints like PCs.

GP 3

DATE: __/__/____

HYPERVISOR REFERENCE MODEL:

There are 3 main modules coordinate in order to emulate the underlying hardware:

1) Dispatcher
2) Allocator
3) Interpreter.

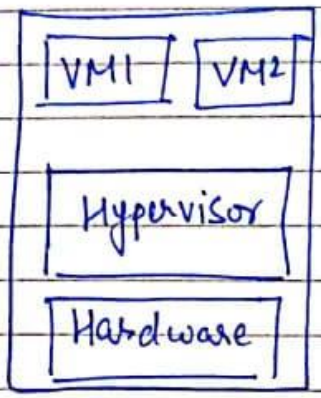
Dispatcher:
The dispatcher behaves like the entry point of the monitor and reroutes the instructions of the virtual machine instance to one of the other two modules.

Allocator:
The allocator is responsible for deciding the system resources to be provided to the virtual machine instance. It means whatever virtual machine tries to execute an instruction that results in changing the machine resources associated with the virtual machine, the allocator is invoked by the dispatcher.

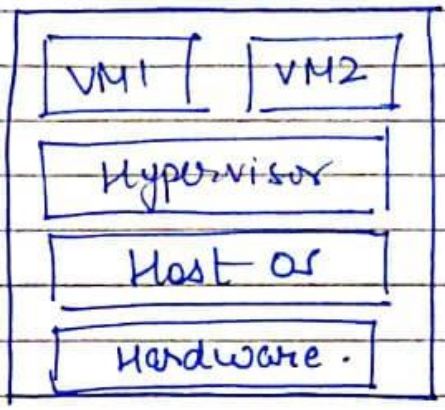
Interpreter:
The interpreter module consists of interpreter routines. These are executed, whenever virtual machine executes a priviliged instruction.

DATE: __/__/____

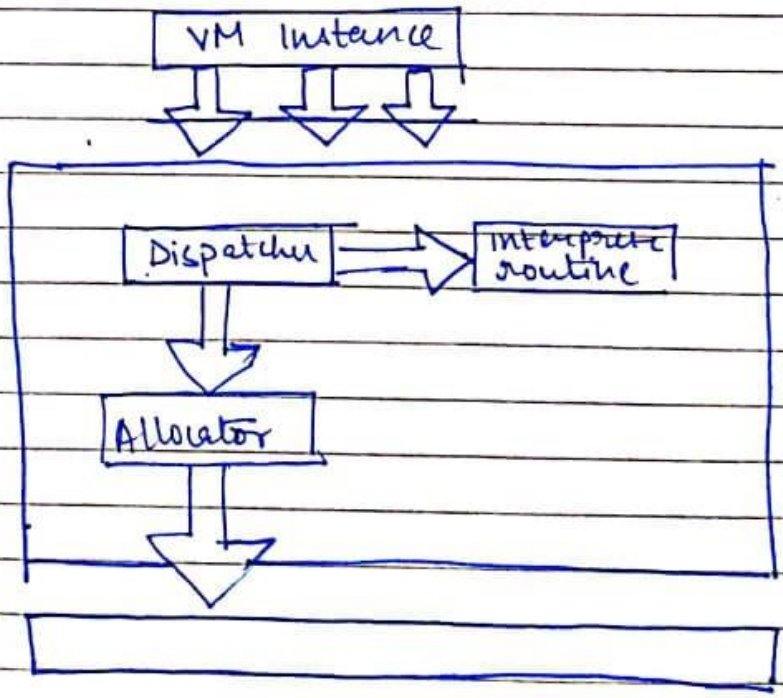
Diagrams :



Types of Hypervisor (1)



Types of Hypervisor (2)



Hypervisor Reference Model.