Tanvir_Ahmed_IT-18043_OS_CT-03

1.a) What Does Operating System Security (OS Security) Mean?
b) How to ensure OS security?
c) What Cyber Threats Can Operating System Security Protect Against?

2.a) What is protection in a computer system?
b) What are the Goals of Protection?
c) What are the Principles of Protection?

3.a) What is Domain of protection?
b) Explain Domain Structures.
c) Describe Access Matrix.

4.a) What is Access Control?
b) What are the main differences between capability lists and access lists?
c) What is Capability-based System?

5.a) What are the Security Measures Level?
b) What are the Program threats?
c) What are the System Threats?

6.a) What is Virtual machine? Why virtual machine?
b) How many types of virtual machines are there?
c) Advantages and disadvantages of virtual machines?

7.a) What is Linux?What are the basic components of Linux?What is the difference between UNIX and LINUX?
b) What is BASH?What is the basic difference between BASH and DOS?
c) What is LILO, swap space, Linux Kernel, Bootloader, Init system, Daemons, Graphical server, Desktop environment, Applications?
d) Describe the root account. How do you change permissions under Linux? In Linux, what names are assigned to the different serial ports?

8.a) What type of operating system is Windows? Features of Windows Pro.
b) Describe the booting process for a Windows system?
c) Write the three main architectural layers of the Windows kernel?

Ans to the question NO - 1(a)

Operating system security (OS security) is the process of ensuring OS integrity, confidentiality and availability.

OS security refers to specified steps or measures used to protect the OS from threats, viruses, worms, malware or remote hacker intrusions. OS security encompasses all preventive-control techniques, which safeguard any computer assets capable of being stolen, edited or deleted if OS security is compromised.

Ans to the question NO - 1(b)

OS security may be approached in many ways, including adherence to the following:

- Performing regular OS patch updates
- Installing updated antivirus engines and software
- Scrutinizing all incoming and outgoing network traffic through a firewall
- Creating secure accounts with required privileges only (i.e., user management)

Ans to the question NO - 1(c)

1. Computer virus

We've all heard about them, and we all have our fears. For everyday Internet users, computer viruses are one of the most common network threats in cybersecurity. Statistics show that approximately 33% of household computers are affected with some type of malware, more than half of which are viruses.

Computer viruses are pieces of software that are designed to be spread from one computer to another. They're often sent as email attachments or downloaded from specific websites with the intent to infect your computer — and other computers on your contact list — by using systems on your network. Viruses are known to send spam, disable your security settings, corrupt and steal data from your computer including personal information such as passwords, even going as far as to delete everything on your hard drive.

2. Rogue security software

Leveraging the fear of computer viruses, scammers have a found a new way to commit Internet fraud.

Rogue security software is malicious software that mislead users to believe that they have network security issues, most commonly a computer virus installed on their computer or that their security measures are not up to date. Then they offer to install or update users' security settings. They'll either ask you to download their program to remove the alleged viruses, or to pay for a tool. Both cases lead to actual malware being installed on your computer.

3. Trojan horse

Metaphorically, a "Trojan horse" refers to tricking someone into inviting an attacker into a securely protected area. In computing, it holds a very similar meaning — a Trojan horse, or "Trojan," is a malicious bit of attacking code or software that tricks users into running it willingly, by hiding behind a legitimate program.

They spread often by email; it may appear as an email from someone you know, and when you click on the email and its included attachment, you've immediately downloaded malware to your computer. Trojans also spread when you click on a false advertisement.

Once inside your computer, a Trojan horse can record your passwords by logging keystrokes, hijacking your webcam, and stealing any sensitive data you may have on your computer.

4. Adware and spyware

By "adware" we consider any software that is designed to track data of your browsing habits and, based on that, show you advertisements and pop-ups. Adware collects data with your consent — and is even a legitimate source of income for companies that allow users to try their software for free, but with advertisements showing while using the software. The adware clause is often hidden in related User Agreement docs, but it can be checked by carefully reading anything you accept while installing software. The presence of adware on your computer is noticeable only in those pop-ups, and sometimes it can slow down your computer's processor and internet connection speed.

When adware is downloaded without consent, it is considered malicious.

Spyware works similarly to adware, but is installed on your computer without your knowledge. It can contain keyloggers that record personal information including email addresses, passwords, even credit card numbers, making it dangerous because of the high risk of identity theft.

5. Computer worm

Computer worms are pieces of malware programs that replicate quickly and spread from one computer to another. A worm spreads from an infected computer by sending itself to all of the computer's contacts, then immediately to the contacts of the other computers.

A worm spreads from an infected computer by sending itself to all of the computer's contacts,, then immediately to the contacts of the other computers

Interestingly, they are not always designed to cause harm; there are worms that are made just to spread. Transmission of worms is also often done by exploiting software vulnerabilities. While we don't hear about them much today, computer worm are one of the most common computer network threats.

6. DOS and DDOS attack

Have you ever found yourself waiting impatiently for the online release of a product, one that you're eagerly waiting to purchase? You keep refreshing the page, waiting for that moment when the product will go live. Then, as you press F5 for the last time, the page shows an error: "Service Unavailable." The server must be overloaded!

There are indeed cases like these where a website's server gets overloaded with traffic and simply crashes, sometimes when a news story breaks. But more commonly, this is what happens to a website during a DoS attack, or denial-of-service, a malicious traffic overload that occurs when attackers overflood a website with traffic. When a website has too much traffic, it’s unable to serve its content to visitors.

A DoS attack is performed by one machine and its internet connection, by flooding a website with packets and making it impossible for legitimate users to access the content of flooded website. Fortunately, you can’t really overload a server with a single other server or a PC anymore. In the past years it hasn’t been that common if anything, then by flaws in the protocol.

A DDoS attack, or distributed denial-of-service attack, is similar to DoS, but is more forceful. It’s harder to overcome a DDoS attack. It’s launched from several computers, and the number of computers involved can range from just a couple of them to thousands or even more.

Since it’s likely that not all of those machines belong to the attacker, they are compromised and added to the attacker’s network by malware. These computers can be distributed around the entire globe, and that network of compromised computers is called botnet.

Since the attack comes from so many different IP addresses simultaneously, a DDoS attack is much more difficult for the victim to locate and defend against.

7. Phishing

Phishing is a method of a social engineering with the goal of obtaining sensitive data such as passwords, usernames, credit card numbers.

The attacks often come in the form of instant messages or phishing emails designed to appear legitimate. The recipient of the email is then tricked into opening a malicious link, which leads to the installation of malware on the recipient’s computer. It can also obtain personal information by sending an email that appears to be sent from a bank, asking to verify your identity by giving away your private information.

Uncovering phishing domains can be done easily with SecurityTrails.

8. Rootkit

Rootkit is a collection of software tools that enables remote control and administration-level access over a computer or computer networks. Once remote access is obtained, the rootkit can perform a number of malicious actions; they come equipped with keyloggers, password stealers and antivirus disablers.

Rootkits are installed by hiding in legitimate software: when you give permission to that software to make changes to your OS, the rootkit installs itself in your computer and waits for the hacker to activate it. Other ways of rootkit distribution include phishing emails, malicious links, files, and downloading software from suspicious websites.

9. SQL Injection attack

We know today that many servers storing data for websites use SQL. As technology has progressed, network security threats have advanced, leading us to the threat of SQL injection attacks.

SQL injection attacks are designed to target data-driven applications by exploiting security vulnerabilities in the application's software. They use malicious code to obtain private data, change and even destroy that data, and can go as far as to void transactions on websites. It has quickly become one of the most dangerous privacy issues for data confidentiality. You can read more on the history of SQL injection attacks to better understand the threat it poses to cybersecurity.

10. MIM attacks

Man-in-the-middle attacks are cybersecurity attacks that allow the attacker to eavesdrop on communication between two targets. It can listen to a communication which should, in normal settings, be private.

As an example, a man-in-the-middle attack happens when the attacker wants to intercept a communication between person A and person B. Person A sends their public key to person B, but the attacker intercepts it and sends a forged message to person B, representing themselves as A, but instead it has the attackers public key. B believes that the message comes from person A and encrypts the message with the attackers public key, sends it back to A, but attacker again intercepts this message, opens the message with private key, possibly alters it, and re-encrypts it using the public key that was firstly provided by person A. Again, when the message is transferred back to person A, they believe it comes from person B, and this way, we have an attacker in the middle that eavesdrops the communication between two targets.

Here are just some of the types of MITM attacks:

- DNS spoofing
- HTTPS spoofing
- IP spoofing
- ARP spoofing
- SSL hijacking
- Wi-Fi hacking

Ans to the question NO -2(a)

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.

Ans to the question NO -2(b)

Goals of protection :

1. Provides a means to distinguish between authorized and unauthorized usage.
2. To prevent mischievously, intentional violation of an access restriction by the user.
3. To ensure that each program component which is active in a system uses system resources only in ways consistent with stated policies. (This gives a reliable system).
4. To detect latent errors at the interfaces between the component subsystems. (This can improve reliability). Early detection helps in preventing malfunctioning of subsystems.
5. To enforce policies governing resource usage.

Ans to the question NO -2(c)

Principles of protection :

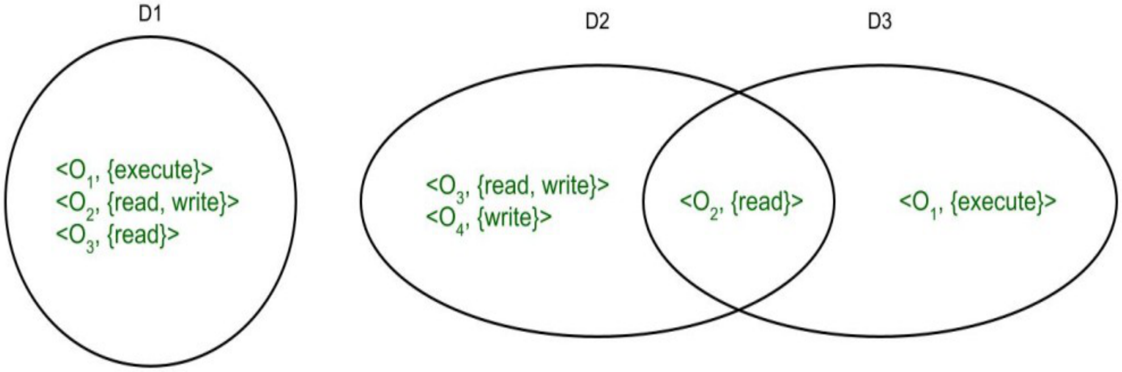
1. The time-tested guiding principle used for protection is called the principle of least privilege. It states that programs, users and even systems be given just enough privileges to perform their tasks.
2. An OS following this principle implements its features, programs, system calls, and data structures so that failure or compromise of a component does the minimum damage and allows minimum damage to be done. Such OS has fine-grained access control.

3. It provides mechanisms to enable privileges when they are needed and to disable them when not needed.
4. Privileged function access have audit trails that enable programmer or systems administrator or law-enforcement officer to trace all protection and security activities of the system.
5. We can create separate accounts for each user with just the privileges that the user needs.

Ans to the question NO -3(a)

Domain of Protection :

- The protection policies limit the access of each process with respect to their resource handling. A process is bound to use only those resources which it requires to complete its task, in the time limit that it requires and also the mode in which it is required. That is the protected domain of a process.
- A computer system has processes and objects, which are treated as abstract data types, and these objects have operations specific to them. A domain element is described as <object, {set of operations on object}>.
- Each domain consists of a set of objects and the operations that can be performed on them. A domain can consist of either only a process or a procedure or a user. Then, if a domain corresponds to a procedure, then changing domain would mean changing procedure ID. Objects may share a common operation or two. Then the domains overlap.



Association between process and domain :

Processes switch from one domain to other when they have the access right to do so. It can be of two types as follows.

1. **Fixed or static –**

   In fixed association, all the access rights can be given to the processes at the very beginning but that give rise to a lot of access rights for domain switching. So, a way of changing the contents of the domain are found dynamically.

2. **Changing or dynamic –**

   In dynamic association where a process can switch dynamically, creating a new domain in the process, if need be.

Ans to the question NO -3(b)

Domain Structure

- A protection domain specifies the resources that a process may access.
- Each domain defines a set of objects and the types of operations that may be invoked on each object.
- An access right is the ability to execute an operation on an object.

- A domain is defined as a set of < object, { access right set } > pairs, as shown below. Note that some domains may be disjoint while others overlap.

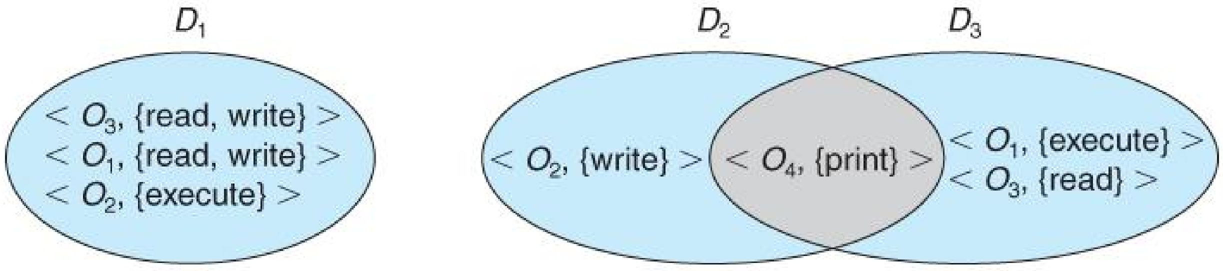


Figure 14.1 - System with three protection domains.

- The association between a process and a domain may be static or dynamic.
    - If the association is static, then the need-to-know principle requires a way of changing the contents of the domain dynamically.
    - If the association is dynamic, then there needs to be a mechanism for ***domain switching.***
- Domains may be realized in different fashions - as users, or as processes, or as procedures. E.g. if each user corresponds to a domain, then that domain defines the access of that user, and changing domains involves changing user ID.

Ans to the question NO -3(c)

Access Matrix is a security model of protection state in computer system. It is represented as a matrix. Access matrix is used to define the rights of each process executing in the domain with respect to each object. The rows of matrix represent domains and columns represent objects. Each cell of matrix represents set of access rights which are given to the processes of domain means each entry(i, j) defines the set of operations that a process executing in domain Di can invoke on object Oj.

	F1	F2	F3	Printer
D1	read		read	
D2				print

D3		read	execute	
D4	read write		read write	

According to the above matrix: there are four domains and four objects- three files(F1, F2, F3) and one printer. A process executing in D1 can read files F1 and F3. A process executing in domain D4 has same rights as D1 but it can also write on files. Printer can be accessed by only one process executing in domain D2. The mechanism of access matrix consists of many policies and semantic properties. Specifically, We must ensure that a process executing in domain Di can access only those objects that are specified in row i.

Policies of access matrix concerning protection involve which rights should be included in the (i, j)th entry. We must also decide the domain in which each process executes. This policy is usually decided by the operating system. The Users decide the contents of the access-matrix entries.

Association between the domain and processes can be either static or dynamic. Access matrix provides an mechanism for defining the control for this association between domain and processes. When we switch a process from one domain to another, we execute a switch operation on an object(the domain). We can control domain switching by including domains among the objects of the access matrix. Processes should be able to switch from one domain (Di) to another domain (Dj) if and only is a switch right is given to access(i, j).

	F1	F2	F3	Printer	D1	D2	D3	D4
D1	read		read			switch		
D2				print			switch	switch
D3		read	execute					
D4	read write		read write		switch			

According to the matrix: a process executing in domain D2 can switch to domain D3 and D4. A process executing in domain D4 can switch to domain D1 and process executing in domain D1 can switch to domain D2.

Ans to the question NO -4(a)

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.

There are two types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and data.

To secure a facility, organizations use electronic access control systems that rely on user credentials, access card readers, auditing and reports to track employee access to restricted business locations and proprietary areas, such as data centers. Some of these systems incorporate access control panels to restrict entry to rooms and buildings, as well as alarms and lockdown capabilities, to prevent unauthorized access or operations.

Access control systems perform identification authentication and authorization of users and entities by evaluating required login credentials that can include passwords, personal identification numbers (PINs), biometric scans, security tokens or other authentication factors. Multifactor authentication (MFA), which requires two or more authentication factors, is often an important part of a layered defense to protect access control systems.

Why is access control important?

The goal of access control is to minimize the security risk of unauthorized access to physical and logical systems. Access control is a fundamental component of security compliance programs that ensures security technology and access control policies are in place to protect confidential information, such as customer data. Most organizations have infrastructure and procedures that limit access to networks, computer systems, applications, files and sensitive data, such as personally identifiable information (PII) and intellectual property.

Access control systems are complex and can be challenging to manage in dynamic IT environments that involve on-premises systems and cloud services. After some high-profile breaches, technology vendors have shifted away from single sign-on (SSO) systems to unified access management, which offers access controls for on-premises and cloud environments.

How access control works

These security controls work by identifying an individual or entity, verifying that the person or application is who or what it claims to be, and authorizing the access level and set of actions associated with the username or Internet Protocol (IP) address. Directory services and protocols, including Lightweight Directory Access Protocol (LDAP) and Security Assertion Markup Language (SAML), provide access controls for authenticating and authorizing users and entities and enabling them to connect to computer resources, such as distributed applications and web servers.

Organizations use different access control models depending on their compliance requirements and the security levels of information technology (IT) they are trying to protect.

Types of access control

The main models of access control are the following:

- **Mandatory access control (MAC).** This is a security model in which access rights are regulated by a central authority based on multiple levels of security. Often used in government and military environments, classifications are assigned to system resources and the operating system (OS) or security kernel. It grants or denies access to those resource objects based on the information security clearance of the user or device. For example, Security Enhanced Linux (SELinux) is an implementation of MAC on the Linux OS.
- **Discretionary access control (DAC).** This is an access control method in which owners or administrators of the protected system,

data or resource set the policies defining who or what is authorized to access the resource. Many of these systems enable administrators to limit the propagation of access rights. A common criticism of DAC systems is a lack of centralized control.

- **Role-based access control (RBAC).** This is a widely used access control mechanism that restricts access to computer resources based on individuals or groups with defined business functions -- e.g., executive level, engineer level 1, etc. -- rather than the identities of individual users. The role-based security model relies on a complex structure of role assignments, role authorizations and role permissions developed using role engineering to regulate employee access to systems. RBAC systems can be used to enforce MAC and DAC frameworks.
- **Rule-based access control.** This is a security model in which the system administrator defines the rules that govern access to resource objects. Often, these rules are based on conditions, such as time of day or location. It is not uncommon to use some form of both rule-based access control and RBAC to enforce access policies and procedures.
- **Attribute-based access control (ABAC).** This is a methodology that manages access rights by evaluating a set of rules, policies and relationships using the attributes of users, systems and environmental conditions.

Implementing access control

Access control is a process that is integrated into an organization's IT environment. It can involve identity management and access management systems. These systems provide access control software, a user database, and management tools for access control policies, auditing and enforcement.

When a user is added to an access management system, system administrators use an automated provisioning system to set up permissions based on access control frameworks, job responsibilities and workflows.

The best practice of least privilege restricts access to only resources that employees require to perform their immediate job functions.

Challenges of access control

Many of the challenges of access control stem from the highly distributed nature of modern IT. It is difficult to keep track of constantly evolving assets as they are spread out both physically and logically. Some specific examples include the following:

- dynamically managing distributed IT environments;
- password fatigue;
- compliance visibility through consistent reporting;

- centralizing user directories and avoiding application-specific silos; and
- data governance and visibility through consistent reporting.

Modern access control strategies need to be dynamic. Traditional access control strategies are more static because most of a company's computing assets were held on premises. Modern IT environments consist of many cloud-based and hybrid implementations, which spreads assets out over physical locations and over a variety of unique devices. A singular security fence that protects on-premises assets is becoming less useful because assets are becoming more distributed.

To ensure data security, organizations must verify individuals' identities because the assets they use are more transient and distributed. The asset itself says less about the individual user than it used to.

Organizations often struggle with authorization over authentication. Authentication is the process of verifying an individual is who they say they are through the use of biometric identification and MFA. The distributed nature of assets gives organizations many avenues for authenticating an individual.

The process that companies struggle with more is authorization, which is the act of giving individuals the correct data access based on their authenticated identity. One example of where this might fall short is if an individual leaves a job but still has access to that company's assets. This can create security holes because the asset the individual uses for work -- a smartphone with company software on it, for example -- is still connected to the company's internal infrastructure but is no longer being monitored because the individual is no longer with the company. Left unchecked, this can cause problems for an organization.

If the ex-employee's device were to be hacked, the hacker could gain access to sensitive company data unbeknownst to the company because the device is no longer visible to the company in many ways but still connected to company infrastructure. The hacker may be able to change passwords, view sensitive information or even sell employee credentials or consumer data on the dark web for other hackers to use.

One solution to this problem is strict monitoring and reporting on who has access to protected resources so that, when a change occurs, it can be immediately identified and access control lists (ACLs) and permissions can be updated to reflect the change.

Another often overlooked challenge of access control is the user experience (UX) design of access control technologies. If a particular access management technology is difficult to use, an employee may use it incorrectly or circumvent it entirely, which creates security holes and compliance gaps. If a reporting or monitoring application is difficult to use, then the reports themselves may be compromised due to an employee mistake, which then would result in a security gap because an important permissions change or security vulnerability went unreported.

Access control software

There are many types of access control software and technology, and often, multiple components are used together to maintain access control. The software tools may be on premises, in the cloud or a hybrid of both. They may focus primarily on a company's internal access management or may focus outwardly on access management for customers. Some of the types of access management software tools include the following:

- reporting and monitoring applications
- password management tools
- provisioning tools
- identity repositories
- security policy enforcement tools

Microsoft Active Directory (AD) is one example of software that includes most of the tools listed above in a single offering. Other vendors with popular products for identity and access management (IAM) include IBM, Idaptive and Okta.

Ans to the question NO -4(b)

An access list is a list for each object consisting of the domains with a nonempty set of access rights for that object. A capability list is a list of objects and the operations allowed on those objects for each domain.

Ans to the question NO -4(c)

Capability-based security is a concept in the design of secure computing systems, one of the existing security models. A **capability** (known in some systems as a **key**) is a communicable, unforgeable token of authority. It refers to a value that references an object along with an associated set of access rights. A user program on a capability-based operating system must use a capability to access an object. Capability-based security refers to the principle of designing user programs such that they directly share capabilities with each other according to the principle of least privilege, and to the operating system infrastructure necessary to make such transactions efficient and secure. Capability-based security is to be contrasted with an approach that uses hierarchical protection domains.

Although most operating systems implement a facility which resembles capabilities, they typically do not provide enough support to allow for the exchange of capabilities among possibly mutually untrusting entities to be the primary means of granting and distributing access rights throughout the system. A capability-based system, in contrast, is designed with that goal in mind.

Ans to the question NO -5(a)

To protect the system, Security measures can be taken at the following levels:

- **Physical:**

  The sites containing computer systems must be physically secured against armed and malicious intruders. The workstations must be carefully protected.
- **Human:**

  Only appropriate users must have the authorization to access the system. Phishing(collecting confidential information) and Dumpster

Diving(collecting basic information so as to gain unauthorized access) must be avoided.

- **Operating system:**

  The system must protect itself from accidental or purposeful security breaches.

- **Networking System:**

  Almost all of the information is shared between different systems via a network. Intercepting these data could be just as harmful as breaking into a computer. Henceforth, Network should be properly secured against such attacks.

Usually, Anti Malware programs are used to periodically detect and remove such viruses and threats. Additionally, to protect the system from the Network Threats, Firewall is also be used.

Ans to the question NO -5(b)

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**.

Types of Program Threats –

1. **Virus:**

   An infamous threat, known most widely. It is a self-replicating and a malicious thread which attaches itself to a system file and then rapidly replicates itself, modifying and destroying essential files leading to a system breakdown.

   Further, Types of computer viruses can be described briefly as follows:

   – file/parasitic – appends itself to a file

– boot/memory – infects the boot sector

– macro – written in a high-level language like VB and affects MS Office files

– source code – searches and modifies source codes

– polymorphic – changes in copying each time

– encrypted – encrypted virus + decrypting code

– stealth – avoids detection by modifying parts of the system that can be used to detect it, like the read system call

– tunneling – installs itself in the interrupt service routines and device drivers

– multipartite – infects multiple parts of the system

2. **Trojan Horse:**

   A code segment that misuses its environment is called a Trojan Horse. They seem to be attractive and harmless cover program but are a really harmful hidden program which can be used as the virus carrier. In one of the versions of Trojan, User is fooled to enter its confidential login details on an application. Those details are stolen by a login emulator and can be further used as a way of information breaches.

   Another variance is Spyware, Spyware accompanies a program that the user has chosen to install and downloads ads to display on the user’s system, thereby creating pop-up browser windows and when certain sites are visited by the user, it captures essential information and sends it over to the remote server. Such attacks are also known as **Covert Channels**.

3. **Trap Door:**

   The designer of a program or system might leave a hole in the software that only he is capable of using, the Trap Door works on the similar principles. Trap Doors are quite difficult to detect as to analyze them, one needs to go through the source code of all the components of the system.

4. **Logic Bomb:**

   A program that initiates a security attack only under a specific situation.

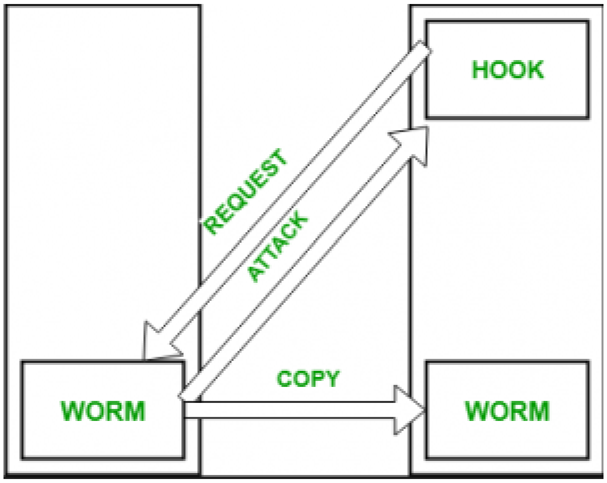
Ans to the question NO -5(c)

Aside from the program threats, various system threats are also endangering the security of our system:

1. **Worm:**

   An infection program which spreads through networks. Unlike a virus, they target mainly LANs. A computer affected by a worm attacks the target system and writes a small program “hook” on it. This hook is further used to copy the worm to the target computer. This process repeats recursively, and soon enough all the systems of the LAN are affected. It uses the spawn mechanism to duplicate itself. The worm spawns copies of itself, using up a majority of system resources and also locking out all other processes.

The basic functionality of a the worm can be represented as:



2. **Port Scanning:**

   It is a means by which the cracker identifies the vulnerabilities of the system to attack. It is an automated process which involves creating a TCP/IP connection to a specific port. To protect the identity of the attacker, port scanning attacks are launched from **Zombie Systems**, that is systems which were previously independent systems that are also serving their owners while being used for such notorious purposes.

3. **Denial of Service:**

   Such attacks aren’t aimed for the purpose of collecting information or destroying system files. Rather, they are used for disrupting the legitimate use of a system or facility.

   These attacks are generally network based. They fall into two categories:

   – Attacks in this first category use so many system resources that no useful work can be performed.

   For example, downloading a file from a website that proceeds to use all available CPU time.

   – Attacks in the second category involves disrupting the network of the facility. These attacks are a result of the abuse of some fundamental TCP/IP principles.

fundamental functionality of TCP/IP.

Ans to the question NO -6(a)

A **Virtual Machine** (VM) is a compute resource that uses software instead of a physical computer to run programs and deploy apps.

7 Practical Reasons to Start Using a Virtual Machine:

1. Try New Operating Systems
2. Run Old or Incompatible Software
3. Develop Software for Other Platforms
4. Handle Potential Malware Safely
5. Tear Apart Your System
6. Take Advantage of VM Snapshots
7. Clone a System to Another Machine

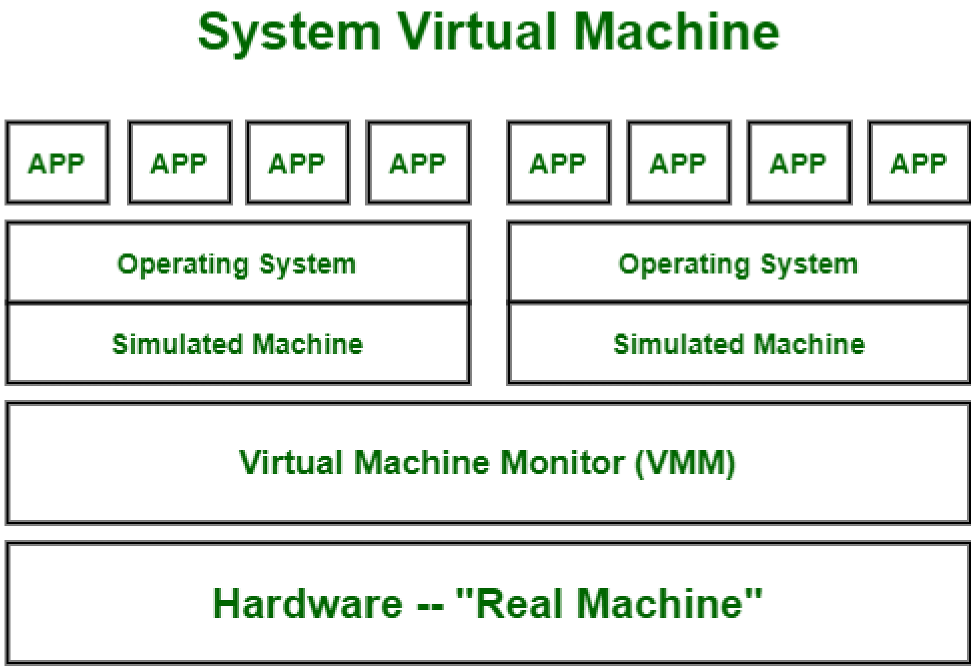
Ans to the question NO -6(b)

You can classify virtual machines into two types:

1. System Virtual Machine:

These types of virtual machines gives us complete system platform and gives the execution of the complete virtual operating system. Just like virtual box, system virtual machine is providing an environment for an OS to be installed completely. We can see in below image that our hardware of Real Machine is being distributed between two simulated operating systems by Virtual machine monitor.

And then some programs, processes are going on in that distributed hardware of simulated machines separately.

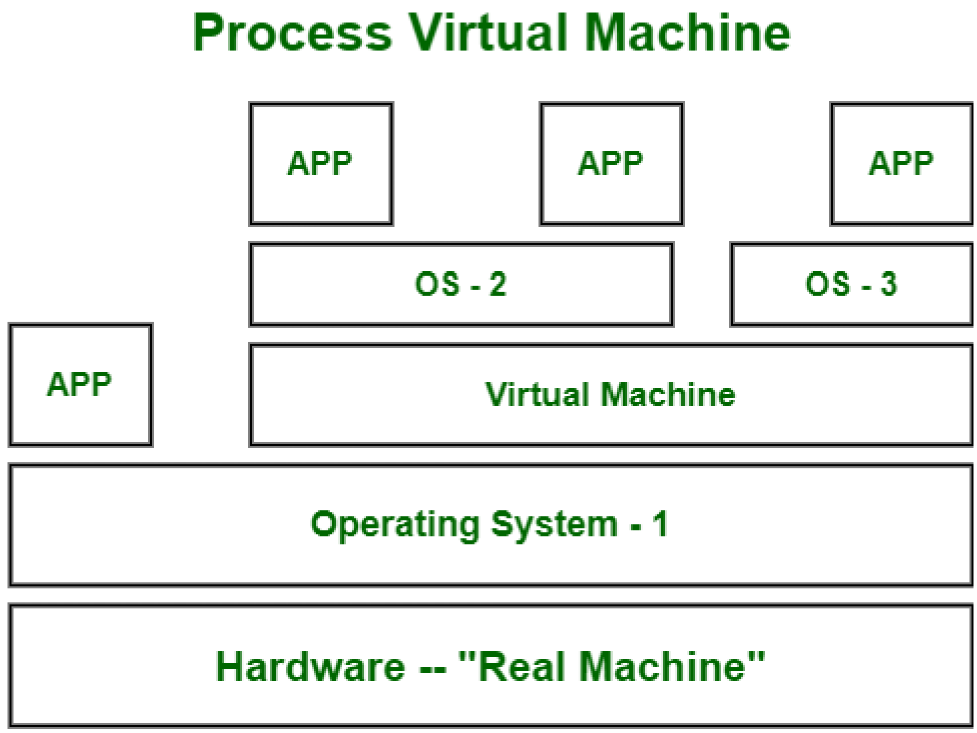


2. Process Virtual Machine :

While process virtual machines, unlike system virtual machine, does not provide us with the facility to install the virtual operating system completely. Rather it creates virtual environment of that OS while using some app or program and this environment will be destroyed as soon as we exit from that app. Like in below image, there are some apps running on main OS as well some virtual machines are created to run other apps. This shows that as those programs required different OS, process virtual machine provided them with that for the time being those programs are running.

Example –

Wine software in Linux helps to run Windows applications.



Ans to the question NO -6(c)

VM Advantages:

- Can use multiple operating system environments on the same computer.
- Virtual machines can provide an instruction set architecture, or ISA, structure different than the actual computer. The ISA serves as the interface between software and hardware.
- When you create your virtual machine, you create a virtual hard disk. So, everything on that machine can crash, but if it does, it won’t affect the host machine.
- There are security benefits to running virtual machines. For example, if you need to run an application of questionable security, you can run it in a guest operating system. So, if the application causes damage, then it will be only temporary after the guest is shut down. Virtual machines also

allow for better security forensics by monitoring guest operating systems for deficiencies and allowing the user to quarantine it for analysis.

VM Disadvantages:

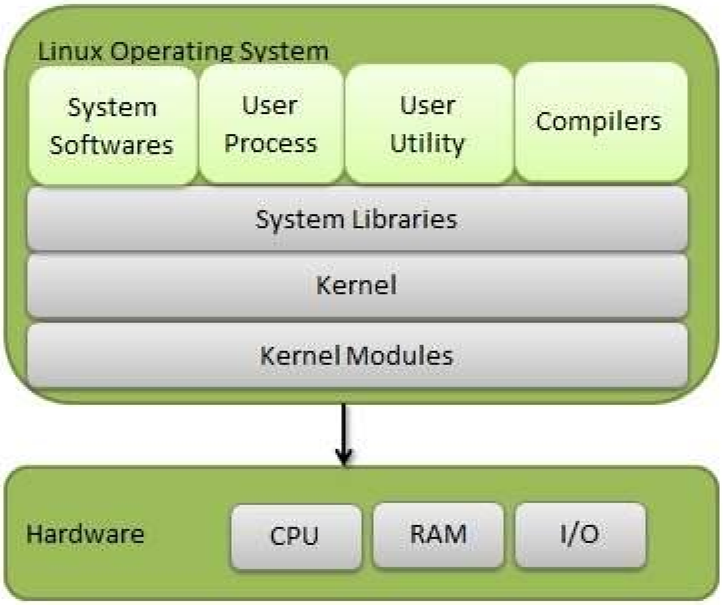
- Virtual machines are less efficient than real machines because they access the hardware indirectly. Running software on top of the host operating system means that it will have to request access to the hardware from the host. That will slow the usability.
- When several virtual machines are running 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.

Ans to the question NO -7(a)

Just like Windows, iOS, and Mac OS, Linux is an operating system. In fact, one of the most popular platforms on the planet, Android, is powered by the Linux operating system. An operating system is software that manages all of the hardware resources associated with your desktop or laptop. To put it simply, the operating system manages the communication between your software and your hardware. Without the operating system (OS), the software wouldn?t function.

Linux Operating System has primarily three components

- Kernel − Kernel is the core part of Linux. It is responsible for all major activities of this operating system. It consists of various modules and it interacts directly with the underlying hardware. Kernel provides the required abstraction to hide low level hardware details to system or application programs.
- System Library − System libraries are special functions or programs using which application programs or system utilities accesses Kernel's features. These libraries implement most of the functionalities of the operating system and do not requires kernel module's code access rights.
- System Utility − System Utility programs are responsible to do specialized, individual level tasks.



Difference between Unix and Linux

Key Differences	Linux	Unix

Cost	Linux is freely distributed, downloaded through magazines, Books, website, etc. There are paid versions also available for Linux.	Different flavors of Unix have different pricing depending upon the type of vendor.
Development	Linux is Open Source, and thousands of programmer collaborate online and contribute to its development.	Unix systems have different versions. These versions are primarily developed by AT&T as well as other commercial vendors.
User	Everyone. From home users to developers and computer enthusiasts alike.	The UNIX can be used in internet servers, workstations, and PCs.
Text made interface	BASH is the Linux default shell. It offers support for multiple command interpreters.	Originally made to work in Bourne Shell. However, it is now compatible with many others software.
GUI	Linux provides two GUIs,viz., KDE and Gnome. Though there are many alternatives such as Mate, LXDE, Xfce, etc.	Common Desktop Environment and also has Gnome.
Viruses	Linux has had about 60-100 viruses listed to date which are currently not spreading.	There are between 80 to 120 viruses reported till date in Unix.

Threat detection	Threat detection and solution is very fast because Linux is mainly community driven. So, if any Linux user posts any kind of threat, a team of qualified developers starts working to resolve this threat.	Unix users require longer wait time, to get the proper bug fixing patch.
Architectures	Initially developed for Intel's x86 hardware processors. It is available for over twenty different types of CPU which also includes an ARM.	It is available on PA-RISC and Itanium machines.
Usage	Linux OS can be installed on various types of devices like mobile, tablet computers.	The UNIX operating system is used for internet servers, workstations & PCs.
Best feature	Kernel update without reboot	Feta ZFS - next generation filesystem DTrace - dynamic Kernel Tracing
Versions	Different Versions of Linux are Redhat, Ubuntu, OpenSuse, etc.	Different Versions of Unix are HP-UX, AIS, BSD, etc.
Supported file type	The Filesystems supported by file type like xfs, nfs, cramfsm ext 1 to 4, ufs, devpts, NTFS.	The Filesystems supported by file types are zfs, hfx, GPS, xfs, vxfs.
Portability	Linux is portable and is booted from a USB Stick	Unix is not portable

Source Code	The source is available to the general public	The source code is not available to anyone.

Ans to the question NO -7(b)

BASH is short for Bourne Again SHell. It was written by Steve Bourne as a replacement to the original Bourne Shell (represented by /bin/sh). It combines all the features from the original version of Bourne Shell, plus additional functions to make it easier and more convenient to use. It has since been adapted as the default shell for most systems running Linux.

The key differences between the BASH and DOS console lie in 3 areas:

- BASH commands are case sensitive while DOS commands are not;

- Under BASH, / character is a directory separator and \ acts as an escape character. Under DOS, / serves as a command argument delimiter and \ is the directory separator

- DOS follows a convention in naming files, which is 8 character file name followed by a dot and 3 characters for the extension. BASH follows no such convention.

Ans to the question NO -7(c)

LILO - LILO is a bootloader for Linux. It is used mainly to load the Linux operating system into main memory so that it can begin its operations.

Bootloader – The software that manages the boot process of your computer. For most users, this will simply be a splash screen that pops up and eventually goes away to boot into the operating system.

Kernel – This is the one piece of the whole that is actually called ?Linux?. The kernel is the core of the system and manages the CPU, memory, and peripheral devices. The kernel is the lowest level of the OS.

Swap Space - Swap space is a certain amount of space used by Linux to temporarily hold some programs that are running concurrently. This happens when RAM does not have enough memory to hold all programs that are executing.

Init system – This is a sub-system that bootstraps the user space and is charged with controlling daemons. One of the most widely used init systems is systemd? which also happens to be one of the most controversial. It is the init system that manages the boot process, once the initial booting is handed over from the bootloader (i.e., GRUB or GRand Unified Bootloader).

Daemons – These are background services (printing, sound, scheduling, etc.) that either start up during boot or after you log into the desktop.

Graphical server – This is the sub-system that displays the graphics on your monitor. It is commonly referred to as the X server or just X.

Desktop environment – This is the piece that the users actually interact with. There are many desktop environments to choose from (GNOME, Cinnamon, Mate, Pantheon, Enlightenment, KDE, Xfce, etc.). Each desktop environment includes built-in applications (such as file managers, configuration tools, web browsers, and games).

Applications – Desktop environments do not offer the full array of apps. Just like Windows and macOS, Linux offers thousands upon thousands of high-quality software titles that can be easily found and installed. Most modern Linux distributions (more on this below) include App Store-like tools that centralize and simplify application installation. For example, Ubuntu Linux has the Ubuntu Software Center (a rebrand of GNOME Software? Figure 1) which allows you to quickly search among the thousands of apps and install them from one centralized location.

Ans to the question NO -7(d)

Root Account : The root account is like a systems administrator account and allows you full control of the system. Here you can create and maintain user accounts, assigning different permissions for each account. It is the default account every time you install Linux.

Change permissions under Linux : Assuming you are the system administrator or the owner of a file or directory, you can grant permission using the chmod command. Use + symbol to add permission or – symbol to deny permission, along with any of the following letters: u (user), g (group), o (others), a (all), r (read), w (write) and x (execute).
For example, the command chmod go+rw FILE1.TXT grants read and write access to the file FILE1.TXT, which is assigned to groups and others.

Serial ports are identified as /dev/ttyS0 to /dev/ttyS7. These are the equivalent names of COM1 to COM8 in Windows.

Ans to the question NO -8(a)

Windows is a **GUI(graphical operating system)** based Operating System. Windows designed and developed by Microsoft. The First version or we can call the first edition of the Windows Operating system was **introduced by Microsoft on November 10, 1983**, and the name of that version is Windows 1.0.

In **Windows Operating System** provides an interface to the user to play games, store files, store database, Developing Desktop applications, and other applications, and we can Run so many types of Application programs. It allows users to create files, delete files, update files and we can also download or upload a file or any file on the Internet.

Windows XP was developed and released by Microsoft in **2001**, Microsoft designed its various versions for types of operating systems based on their features and functions such as **Home computing, professional**, and also other versions of windows. and also based on CPU bit size x86 and x64, like **Intel** and **AMD** processor. and now the current version is windows 10.

Features of **Windows Pro**

- Hyper-V
- Group policy management
- Xbox Streaming

- Core Windows Apps
- Bitlocker
- Remote Desktop
- Trusted Boot

Ans to the question NO -8(b)

Phase 1 – Preboot

In this phase, the PC’s firmware is in charge and initiates a POST and loads the firmware settings. Once all this works (hopefully), the system identifies a valid system disk and reads the MBR. The system then starts the Windows Boot Manager. This is located here: %SystemDrive%\bootmgr

Phase 2 – Windows Boot Manager

It is the job of the Windows Boot Manager to find and start the Windows loader (Winload.exe). This is located on the Windows boot partition – %SystemRoot%\system32\winload.exe

Phase 3 – Windows Operating System Loader

In this phase, essential drivers required to start the Windows kernel are loaded and the kernel starts to run. The key file here is %SystemRoot%\system32\ntoskrnl.exe

Phase 4 – Windows NT OS Kernel

The kernel loads the system registry hive into memory and loads the drivers that are marked as BOOT_START. The kernel then passes control to the session manager process (Smss.exe).

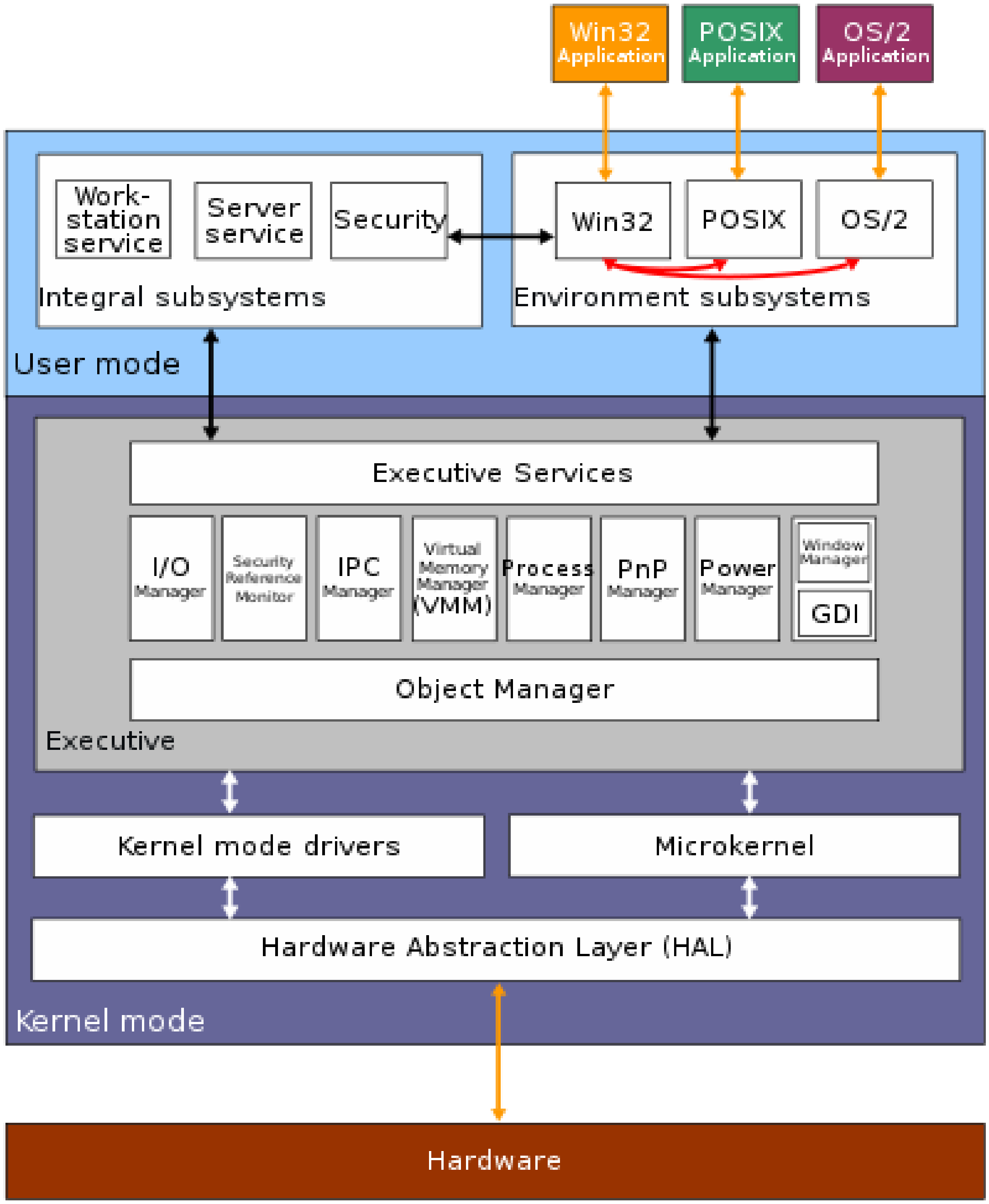
Ans to the question NO -8(c)

The **architecture of Windows NT**, a line of operating systems produced and sold by Microsoft, is a layered design that consists of two main components, user mode and kernel mode. It is a preemptive, reentrant multitasking operating system, which has been designed to work with uniprocessor and symmetrical multiprocessor (SMP)-based computers. To process input/output (I/O) requests, they use packet-driven I/O, which utilizes I/O request packets (IRPs) and asynchronous I/O. Starting with Windows XP, Microsoft began making 64-bit versions of Windows available; before this, there were only 32-bit versions of these operating systems.

Programs and subsystems in user mode are limited in terms of what system resources they have access to, while the kernel mode has unrestricted access to the system memory and external devices. Kernel mode in Windows NT has full access to the hardware and system resources of the computer. The Windows NT kernel is a hybrid kernel; the architecture comprises a simple kernel, hardware abstraction layer (HAL), drivers, and a range of services (collectively named Executive), which all exist in kernel mode.[1]

User mode in Windows NT is made of subsystems capable of passing I/O requests to the appropriate kernel mode device drivers by using the I/O manager. The user mode layer of Windows NT is made up of the "Environment subsystems", which run applications written for many different types of operating systems, and the "Integral subsystem", which operates system-specific functions on behalf of environment subsystems. The kernel mode stops user mode services and applications from accessing critical areas of the operating system that they should not have access to.

The Executive interfaces, with all the user mode subsystems, deal with I/O, object management, security and process management. The kernel sits between the hardware abstraction layer and the Executive to provide *multiprocessor synchronization*, thread and interrupt scheduling and dispatching, and trap handling and exception dispatching. The kernel is also responsible for initializing device drivers at bootup. Kernel mode drivers exist in three levels: highest level drivers, intermediate drivers and low-level drivers. Windows Driver Model (WDM) exists in the intermediate layer and was mainly designed to be binary and source compatible between Windows 98 and Windows 2000. The lowest level drivers are either legacy Windows NT device drivers that control a device directly or can be a plug and play (PnP) hardware bus.


Win32 Application
POSIX Application
OS/2 Application
Work-station service
Server service
Security
Integral subsystems
Win32
POSIX
OS/2
Environment subsystems
User mode
Executive Services
I/O Manager
Security Reference Monitor
IPC Manager
Virtual Memory Manager (VMM)
Process Manager
PnP Manager
Power Manager
Window Manager
GDI
Object Manager
Executive
Kernel mode drivers
Microkernel
Hardware Abstraction Layer (HAL)
Kernel mode
Hardware