Sri Lanka Institute of Information Technology

Evaluating The Features of Various OS

Group Assignment

IE2032-Secure Operating System

Submitted by:

Student Registration number	Student Name
IT22353184	R.M.C.A. Rathnayaka
IT22921512	S.I.B. Jayawardhana
IT22199508	A.M.M.I.P Athapaththu
IT22298508	W.M.K.R Wanasinghe

2023 – WD – Y2S1 - 07

Table of Contents

- Linux as Server type OS
  - Memory management in Linux
  - Process management in Linux
  - File management in Linux
  - Device management in Linux
  - Network management in Linux

- Android as mobile OS
  - Memory management in Android
  - Process management in Android
  - File management in Android
  - Device management in Android
  - Network management in Android

5. Provide a stable, portable, reliable, safe, well-behaved environment.
   - Windows as a client type OS
     - System Architecture
     - Error Handling and Recovery
     - Security Features
     - User Interface Design
     - Testing and Quality Assurance
     - Documentation and Support

   - Linux as Server type OS
     - Long-Term Support (LTS)
     - Security Updates
     - Access Control
     - Community and Support
     - Open Standards and Compatibility

   - Android as mobile OS
     - Open Source and Customizability
     - Application Ecosystem
     - Regular Updates and Improvements
     - Interoperability with Google Services

6. Share Resources among users fairly, efficiently and safely.

- Windows as a client type OS
  - User account control (UAC)
  - Group policy
  - Task manager
  - Windows update optimization
  - User education
  - Security measures

- Linux as Server type OS
  - Quotas
  - File permissions
  - Accounts and groups
  - Scheduler policies
  - Control groups

- Android as mobile OS
  - Application isolation
  - Resource allocation
  - Permissions model
  - Battery optimization
  - App lifecycle
  - Security measures

Abstract

Operating systems are the fundamental software frameworks that helps computer devices and mobile devices to operate properly. Operating systems creates the connection between user and the hardware of the device. Windows, Linux and Android are popular operating systems among the operating systems. Each operating system carries out its own variety of features and characteristics. Windows, developed by Microsoft is widely used in personal computers and enterprise environment mainly because of its user-friendly interface. Linux is an open-source operating system that is well known for its security, flexibility and its customizability. Android developed by google is dominant mobile operating system that offers a user-friendly interface. Android covers a vast ecosystem of mobile apps and crucial within its security measures. Each of these operating systems includes unique features to behave in resource demand conflict, effective resource management, ensuring stability, portability, reliability and maintaining security. The way and the characteristics that each operating system use to resolve conflict in resource demand, providing a well-behaved environment, managing resources like memory, processor, file and ensuring security are explored in this report.

Introduction

The operating system (OS) emerges as the unsung hero in the realm of computing, the operating system serves as the backbone of computing, it manages resources and turns computer devices into effective and intelligent tools, by providing a platform for diverse applications from networking to gaming, all while maintaining energy and optimal resource utilization.

This assignment sets out on a quest to unravel the OS through examination of it's functions as a resource manager and an extended machine across many computing devices. We shall have a better understanding of the significance of the OS in modern computing, paving the way for innovations that continue to shape our digital Future.

1. The Level of security on operating systems

1.1) Windows as a client type OS

The Windows operating system's security features include a number of layers and safeguards that are intended to shield your machine and data from a variety of attacks and threats. These layers and tools help in establishing a robust defense system to ensure the confidentiality, integrity and availability of the information of the user and the system. Security features of windows has evolved through the new versions of windows operating systems.

System security, Network security, Virus and Threat protection, Encryption and data protection, Application security can be identified as main layers of security in windows operating system. Under these layers there are main features that helps in safe guarding the windows operating system environment.

1.**Secure boot and trusted boot**:

Secure boot and trusted boot ensure that only trusted software components, including the operating system, drivers, and firmware, can run during the boot process and prevents malware and corrupted components from loading during the boot process.

Apart from that windows system has Measured Boot that looks in to all important code and configuration settings during the boot of Windows.

2.**windows security policies and monitoring and auditing:**

Administrators can design and enforce security policies using policies, guaranteeing uniform security settings and configurations, across the network.

And allows administrators monitoring and auditing to track security threats and activities, to identify and respond to security incidents.

3.**User authentication and Access control**:

Security measures in windows starts at User level. Windows allows to create multiple accounts with its own permissions. With authentication methods like pin, password, bio metrics ensures only authorized user can gain access to the account, to prevent unauthorized changes and threats to the system and accounts.

Security measures; User Account Control (UAC)

4.**Update windows**:

Operating system needs be updates regularly to have new security features and important security updates to fix vulnerabilities that have been identified and could be used by attackers.

5.**Network security**:

Windows includes protocols like Transport Layer Security (TLS) and Domain Name System (DNS) security to eliminate cryptographic algorithms and allows administrators to ensure their devices protect DNS queries from attackers.

Also have windows defender firewall to reduce attacking surface of a device increases manageability and decreases the impact of a successful attack and helps to block incoming and outgoing network traffic.

6.**Windows defender Antivirus**:

Window includes a built-in antivirus software that provides real time, behavior-based, and heuristic protection against malware, virus and other threats.

This continually scans for malware and threats and also detects and blocks potentially unwanted applications that may impact the system.

7.**Data Encryption**:

Windows offers features like BitLocker management and BitLocker enablement to protect sensitive data from unauthorized access. BitLocker provides encryption for the OS, fixed data, and removable storges and has Recovery key management.

Windows provide Personal data encryption to protect personal data such as user document and other files. Also includes Email encryption that enables users to encrypt outgoing email messages and attachments.

8.**Application security**:

Features like Smart app control, AppLocker and Windows Defender SmartScreen help you manage which programs can run on your PC and safeguard you from potentially dangerous apps. These features prevent users from running malicious applications on Windows device by blocking untrusted applications.

AppLocker allows you to specify which applications are allowed to run on your system. And by examining the reputation of websites and files you access online, Windows Defender SmartScreen assists in defending you from harmful websites and downloads.

https://learn.microsoft.com/en-us/windows/security/operating-system-security/

1.2) Linux as Server type OS

Linux operating system is open-source, increasingly popular and more secure operating system. As a server operating system Linux is a popular choice because of its security features and flexibility. The security of Linux is based on its open-source nature, which allows global community of developers to continuously improve the security and give solutions for the threats. There are some key security features that contribute in system environment secure.

1.User and Group permissions

Linux uses a strong permission system that assign specific permissions to access files, directories and system resources. These set of permissions limits the unauthorized access to critical files and data and create a fine level of access control in the system.

For an example Linux uses write(w), read(r), execute(x) to specify permissions for a file or a directory. And can limit who can read and modify a sensitive configuration file by using 'chmod' command, allowing only root user to do so.

2.User Account Control

Linux system includes a robust user account policy and encourage the user to use a strong password and use two factor authentication method to enface the security. When creating a password user must adhere to specific rules and using tools like 'passwd' administrators can set policies and add password expiration time to force users to exchange passwords time to time. This helps to prevent attackers from password-guessing and brute forcing.

3.Firewalls

Linux comes with a built-in firewall and includes tools like ‘iptables’ and ‘firewalld’. With these tools user can control incoming and outgoing network traffic to prevent unauthorized access, reduce exposure to potential threats and build proper rules for network communication.

- Iptables: - A tool that allows administrators to set packet filtering, network address translation and port forwarding.
- Firewalld: - a tool that simplifies the managing process of the firewall rules for administrators to use and access.

4.Security updates and modules

Security updates and patches to fix know vulnerabilities are regularly released through Linux distributions to keep the server secure and safe. There are package mangers like ‘apt’ and ‘yum’ to regular updates.

Linux is compatible with a number of security framework and modules, like AppArmor and SELinux (security-enhanced Linux), which offers mandatory access control and lessen the effects of security breaches.

- SELinux: - A security module that is integrated in to Linux kernel, by NSA. It enforces mandatory access control policies.
- AppArmor: - A framework that supports application-level security.

5.Encryption

Linux enforces strong encryption protocols, such as SSH for secure remote access and tools like openssl for securing data in transmit.

Secure shell (SSH) is a widely used protocol for secure remote access for Linux servers and it uses encryption to safeguard communication between the client and server, preventing eavesdropping and unwanted access to login credentials. It ensures the confidentiality and integrity of data exchanged between the client and server.

6.Resource Isolation

By isolating apps and services into separate contexts, resource isolation via technologies such as virtualization like KVM and containers like Docker improves security by avoiding the impact of one compromised service on others.

Kernel-based virtual machine (kvm) popular open-source virtualization technology for linux. With virtualization, a single physical server may contain several virtual machines, each with a separate operating system and set of separated resources.

- https://linuxsecurity.com/features/how-secure-is-linux
- https://www.thesslstore.com/blog/linux-server-security-linux-hardening-best-practices/

1.3) Android as mobile OS

Android is a popular operating system developed by google which is known for its strong security features. Android has evolved through time with new versions and devices. The security features in android are designed to protect user data, device and applications. This is an open-source software built on Linux-kernel that is designed to run on a variety of devices and form factors.

1.Secure kernel

Android system is based on Linux-kernel which builds a strong foundation of security for android system.to prevent unauthorized access to system resources, the Linux kernel implements memory protection, access controls and process isolation.

Process isolation: - A security feature that ensure various android system processes don't crash with one another. The Linux kernel uses a feature called "process separation" for that to keeps apps isolated.

Access controls: - what resources and actions a process or user may utilize is determined by access controls. For that android uses the file permissions and user permissions access techniques implemented by the Linux kernel to enforce access controls.

Memory protection: - this feature restricts one process from accessing memory that has been assigned to another. Linux kernel acts in when one process tries to read or write to memory that was already allocated for another process.

2.Trusted boot

It is also known as secure boot or verified boot which is included in Android device to ensure the integrity of the system during the boot process. And designed to prevent unauthorized modifications to the operating system and bootloader, aiding in maintaining the security of the device.

3.App Sandboxing

Android apps run in isolated sandboxes, apps cannot directly access the data or the resources of other apps and operates independently. This method helps security patches and unauthorized access from affecting one app to another. For this android assigns a unique user ID to each app and runs it in its own process. Only the app itself can access the files and the database that contains the app's data because file permissions secure these data and directories and it is not possible for one app to directly read or alter data of another app.

4.Android permission System

Permission system on android is an essential part of the system's security model and designed give user authority over the security of their data and device while limiting the resources that apps can access and the actions they can carry out when approved by permission system. These permissions are divided into groups based on how the operate.

- Normal permissions: These permissions are automatically included in apps and user do not have any control over them and do not compromise user privacy or data.

- Dangerous permissions: regarded as sensitive permissions that have ability access user data or carry out functions that compromise the security.

- Signature permissions: Apps which are signed with the same digital certificate as the app that defines the permission have the ability to provide these permissions.

- Special permissions: certain features of a device are dealt with special permissions.
  Ex: notification access, camera access, usage access, calling Access

5.Google play protect

A security function that helps to improve the security of android devices by scanning apps that are available on Google play store for possible security threats and viruses. This serves as an additional layer of defense to reduces the possibility that users may download malicious programs. It helps preserving user data and device security because of its extensive app testing and monitoring.

Apps in google play store continuously gets scanned automatically and checks form known malware and threats. When submitting apps in to the play store, they are checked for compliance with Google's policies and guidelines. And google play protect uses algorithms and machine learning to detect harmful apps and then inform users.

6.Biometric Authentication

In Android, biometric authentication uses a person's distinct physical characteristics or behavioral pattern to confirm their identification. Android enhances device and user data security by supporting multiple biometric authentication methods such as fingerprint and face recognition. This biometric data is kept on the device in an isolated enclave, hardware based, segregated space that is extremely difficult to tamper. Biometric sensors are equipped with extra security features like liveness detection to guaranty that biometric is taken from a real live person.

7.Encryption

Once a device has been encrypted, all the data created by users is automatically encrypted before being stored on disk and all reads automatically decrypted before sending it back to the calling process. Android devices provide the function of full disk encryption which allows to encrypt all the data on device's storage. This is a key based encryption method, and when data is encrypted by a robust algorithm, an unique encryption is created. Encryption makes sure that the data cannot be read by unauthorized individuals, even they managed to gain access to the device.

8.Security updates

For android, Google releases security updates monthly to fix know vulnerabilities and security issues. Depending on device manufacturers and versions the prompt distribution of these updates differs but it plays an essential part in maintaining a secure environment in the system. The most crucial part to maintain security of the device is updating the android system to enhance the system with new security features to avoid possible exposure to attacks and threats.

- https://medium.com/mobis3c/introduction-to-android-security-64609edeb18c

2.Manage memory, processor, file, etc.

Operating systems are complex pieces of software that control the core of functions of a computer. By using methods like virtual memory, they allocate and monitor memory utilization, guaranteeing that programs run without interruption.

Operating systems control the CPU, managing interrupts and scheduling operations to provide multitasking, Furthermore, they permit data exchange and maintaining the structure, rights and integrity of files.

Basically, operating systems offer a seamless and safe environment that enables users and applications to effectively communicate with the computer hardware.

2.1) Windows as a client type OS

A) Memory management in windows

Virtual memory is one of the complex memory management strategies used by windows. This enables the operating system to utilize extra RAM from the computer's hard drive, ensuring that programs can still execute even when the actual RAM is fully used.

Windows controls paging a dynamically distributes memory to running programs, switching data between RAM and disk as necessary. Additionally, it guarantees memory protection by forbidding programs from accessing one another's memory.

Here's how windows manage memory:

Virtual memory

As a virtual memory, windows makes use of both the system's physical RAM and portion of the hard drive or SSD. Applications are able to utilize more memory than actually available because to this expanded virtual memory space.

RAM Management

Windows uses many ways to manage the RAM.it gives priority to active process making sure that the most important application can use the available RAM.

Page File

The page file, aka the swap file is a file on the hard drive which acts as an extension of physical memory.

B) Process management in Windows

Windows uses process scheduling algorithms to manage the CPU efficiently. Preemptive multitasking is used, enabling the simultaneous operation of several Apps. Windows 'Task Manager utility offers real-time data on active processes and system performance. When switching between contexts, Windows maintains CPU states and resolves interrupts, allowing for seamless program switching and effective CPU resource use.

Task Manager

Task Manager is a vital tool for managing processes in windows.

Process Scheduling

A preemptive multitasking architecture that enables several programs to run at once.

Background Processes

Windows effectively manages background processes, ensuring that crucial system functions and services continue to operate without interfering with foreground programs.

C) File Management in Windows

User can manage files and directories using an easy-to-use interface provided by windows file explorer. Windows is compatible with a number of file systems, including NTFS(New Technology File),which provides capabilities like compression, encryption and file and folder permissions. It oversees file I/O activities, guaranteeing data integrity and quick read/write operations. Windows is compatible with home networks and cloud storage services and it supports network file systems like SMB (Server Message Block) to make file sharing and synchronization simple.

Further, windows operating systems provide tools like windows Update to maintain system updates and make sure that performance and security fixes are consistently installed. In general, window's management features offer customers a dependable, responsive and user-friendly working on client devices.

Here are some tools provided by windows to facilitate file management:

File explorer

File explorer is the primary tool for managing files and folders in windows.

Hierarchy and File Organization:

Window's hierarchical file folder organization enables users to set up a folder hierarchy for convenient organization.

File operations:

File actions which are supported by windows includes copy, cut, paste and delete. Users have the option to copy files across drives or folders ,move files within the same drive, permanently delete files or folders or move them to the recycle bin to later recovery.

D) Device Management in windows

Device Management refers to control of numerous computer hardware devices, such as as external drives, printers, scanners, and cameras and external storage are just a few of hardware devices that operating systems control. They offer drivers that facilitate communication between the operating system and hardware devices, enabling users to use various peripherals without any problems.

Here are some ways how device management works in windows OS:

Device detection and installation

The operating system on your Windows Computer identifies new hardware when you connect it, Windows recognizes the device using a database of drivers and ,if necessary prompts you to install the correct driver . additionally, Windows update can automatically download and install new drivers.

Device Manager

Device Manager is a built-in Windows utility that allows users to view and manage hardware devices. To open device manager you can search the device manager from the search bar in the starting menu. It offers a hierarchical view of different hardware groups and types of devices, Users can update drivers turn off devices, see properties, and troubleshoot hardware problems from here.

Plug and Play

When a device is connected to a computer, plug and play technology supported by windows, enables automatic device recognition and configuration.by eliminating the need for human user intervention, plug and play streamlines the process of adding or uninstalling hardware devices. Most of the time, windows discovers new devices automatically and makes sure they are operational before requiring manual driver installation.

Device Troubleshooting

Windows come with built-in capabilities for identifying and fixing common device problems. These tools enable users to troubleshoot without specialized technical knowledge by automatically resolving device related issues.

E) Network Management in Windows

Users can connect to the internet or local networks thanks to the operating system, which manage network connectivity. They control IP addresses. Network protocols and network devices. Operating systems offer features for setting up wireless connections ,controlling network security settings ,and configuring proxy settings, among other things.

Windows has a number of tools and functions for network management that let users configure and troubleshoot network connections. Here is how windows handles network management:

Network and Sharing Center :

Network and sharing center is a central hub in windows for managing network connections.

Windows Networking Troubleshooter :

A built-in troubleshooting tool for windows is dedicated to identifying and resolving network related issues.

Windows Firewall and Security center:

The windows firewall shields the machine from network based unlawful access.

2.2) Linux as a server type OS

Linux is well known for server operating systems due to its dependability, security, adaptability and open source status.

The following are some reasons why Linux is a popular server operating system.

- open source and cost-Effective.
- Stability and reliability
- Security
- Flexibility and customizability
- Support for various Hardware Architectures

A) Memory management in Linux

In Linux, like in all present day operating systems, memory management is a crucial component that assures effective use of the systems physical memory (RAM)and offers a stable environment for executing applications.

A small summary of linux memory management is below:

Virtual Memory

Linux uses virtual memory to provide a large memory than physical RAM provides. It includes both RAM and swap space on hard drive. It shifts often accessible data to the swap space when the physical RAM is fully used, freezing the RAM for more urgent demands.

Swap spaces

Swap spacing in linux acts as an extension of physical memory.

Memory protection

In order to preventing one process from accessing the memory space assigned to another process, Linux offers memory protection methods.

Kernal Samepage Merging(KSM)

KSM combines identical memory pages from many processes into a single page.

B) Process management in Linux

In Linux, managing the execution and termination of applications or processes within the operating system is known as process management.

Following is a summary of process management in Linux:

Process Identification

In linux each process ID is identified by a unique Process ID(PID).They are essential for tracking ,managing and communicating with processes.

Process Creation

In Linux process are created using system calls like ‘fork()’ or ‘exec’. fork() creates a new process while exec() loads a new program into the current process.

Process scheduling

Linux uses a preemptive and priority-based scheduler.

C) File Management in Linux

A variety of commands ,tools , and permissions are used in Linux file management to give users and administrators effective control over files and directories.

Following are some crucial elements of Linux file management:

File system hierarchy

Linux organizes files into a hierarchical directory structure.

File and Directory commands

ls – list the files and directories in current directory

cp- copies files and directories

mv-moves or renames files and directories

mkdir - creates new directories

chmod - changes file permissions

grep-searches for specific patterns within files

D) Device Management in Linux

Linux device management include configuring, controlling and interfacing with linked hardware devices.

Device files in /dev:

- In linux, hardware devices are shown as special files located in the '/dev'directory.
- Hard drives can be represented by '/dev/sda '.
- Partitions on the drive can be represented as '/dev/sda','/dev/sda2'

E) Network Management in Linux

Configuring, observing and debugging network connections and services are all part of Linux network management.
Some key aspects of network management in linux are listed below,

- Network configuration
- IP addressing and Routing
- DNS configuration
- Firewall and security
- Network monitoring and diagnostics
- etc

2.3) Android as a Mobile type OS

Android is a well known mobile operating system developed by google. This system is based on the Linux kernal and designed mainly for touchscreen mobile devices like smartphones and tablets.

Android has grown to become the most widely used mobile operating system worldwide due to it's adaptability, customization options and big application ecosystem.

Here are some salient characteristics of Android as a mobile operating system,

Open Source - allowing manufacturers to customize and modify the system according to their needs.

User Interface - Provides a highly customizable user interface.

Google play store - The android's official Appstore.

Multitasking - Allows user to switch between applications seamlessly.

A) Memory management in Android

An important feature of Android's operating system that guarantees optimal use of a device's physical memory (RAM) is memory management. For a seamless user experience and to keep apps from using too many resources efficient memory management is crucial.

Following are some key aspects of memory management in Android,

Low memory killer

Android has a feature called the low memory killer (LMK) to keep the system running smoothly when memory is scare. LMK keeps track of how much memory is being used by the system and, if necessary kills low priority background processes to make room for foreground programs and essential system functions.

Background Process Limitations

Android has a cap on how much resources background processes can use. To reduce excessive battery drain and data usage when not in use, background programs have their CPU usage and network access restrictions.

There are more key aspects of memory management in android like,

- App lifecycle and Process states
- Java Garbage collection
- Memory Heap
- Large object handling

B) Process Management in Android

Android process management includes handling the lifecycle, prioritization and termination of applications and background processes which are running on the device OS .

Some key aspects of android process management are below,

Application Lifecycle

A well defined lifecycle for android apps includes the functions like,

- onCreate()
- onStart()
- onResume()
- onPause()
- onStop()
- onDestroy()

For developers to properly deal with user interactions and system events,they must comprehend and manage these lifecycle mechanisms.

Activity stacks

Activities are managed in android in a stack (back stack).A new action is pushed into the stack when it begins.

- Foreground and Background processes
- Service components
- Broadcast Receivers
- And Intent Filters are some more examples of Process Management in Android.

C)File management in android

File management in android includes handling of files and directories within application's private storage and external storage.

Internal storage

Internal storage is only accessed by the app itself, can be used by apps to store private data.

File paths and Directories

File paths and directories are fundamental ideas in Android.At /data/data/package_name>,each app has a private storage directory that is exclusively visible to that app.

Few more examples of File management in Android are given below,

- File access permissions
- External Storage
- Media store
- Content providers
- File picker Intent

D) Device Management in Android

Android device administration involves handling the hardware, sensors and resources of the Android device. Android offers developers APIs to interact with various device features, ensuring that applications work seamlessly with various underlying hardware.

Here are some essential elements of Android device management.

Permissions

Android applications need the right permissions to access particular device functionalities. In order to apps to access necessary hardware resources, users must give certain rights.

Sensors

Android devices come with various equipped variety of sensors, including an accelerometer, gyroscope, magnetometer, proximity sensor etc.

Battery Management

Using the battery Manager API, developers may keep an eye on device's battery level, status and overall health.

It is possible to prolong the battery life of the device by implementing effective background processing and reducing network queries.

- Storage, biometric authentication, Camera and multimedia, location dervices are another few examples of device management in android.

E) Network Management in Android

Monitoring network status responding to network requests,and optimizing data usage are just a few of responsibilities involved in managing network connections on android applications.

Some key aspects of Network Management in android are listed below,

Permissions

Making sure your app has the necessary permissions to access the internet.

Checking Network availability

Use the "connectivitymanager" to check network availability before making network requests.

Security considerations

When dealing with sensitive data, always use secure connections like HTTPS. To enable secure connectivity with your backend services, provide appropriate authentication methods.

3. Provide a stable, portable, reliable, safe, well-behaved environment.

- Providing a stable, portable, reliable, safe, and well-behaved environment using operating systems is needed to ensure the efficient and secure operation of computer systems.

➢ Stability:

Operating systems manage hardware resources, prevent crashes or failures, and handle errors, conflicts, and unexpected events to ensure system stability and smooth operation**.**

➢ Portability:

Operating systems are designed to be portable across different hardware platforms, allowing software to be used on various computer hardware without significant modifications, ensuring flexibility and similarity**.**

➢ Reliability:

Operating systems aim to ensure high reliability by minimizing downtime and data loss, using features like backup, redundancy, and fault tolerance to maintain system functionality.

➢ Safety:

Operating system safety features like access control mechanisms, user authentication, and encryption are essential for maintaining system security and integrity.

- **Well-Behaved Environment:**

  Operating systems enforce rules and standards to promote good behavior among software applications and users, manage resource allocation, and prevent monopolization and instability.

3.1) Windows as a client type OS

- To create a secure, reliable, and safe environment similar to Windows as a client-type operating system, several features and components must be considered.

- A stable OS ensures smooth operation without frequent crashes, errors, or system instability through rigorous testing, debugging, and the use of reliable software components.

- Portability is the OS's ability to run on different hardware architectures or platforms without significant modifications, typically achieved through abstraction layers.

- A reliable OS ensures consistent performance without unexpected failures through robust error handling, backup systems, redundancy, regular maintenance, and updates.

- OS safety involves security measures like user authentication, access control, encryption, and security patches to protect against unauthorized access, data breaches, and other security threats.

- A well-behaved OS should be user-friendly, intuitive, and easy to manage, ensuring consistent design and user experience for easy access and management of applications, files, and settings.

❖ To create an operating system with these features, various factors must be considered.

- **System Architecture:**

  Select a system architecture that is stable and adaptable, capable of functioning on various hardware platforms.

- **Error Handling and Recovery:**

  The recommendation is to establish robust error handling and recovery mechanisms to prevent system crashes and minimize data loss.

- **Security Features:**

  To ensure system safety, it is essential to incorporate security features such as user authentication, access control, firewall, and regular security updates.

- **User Interface Design:**

  Provide a user-friendly user interface that is easy to use and intuitive, with settings and programs accessible with ease.

- **Testing and Quality Assurance:**

  Regularly test the operating system to identify and fix stability, reliability, and security issues, and provide regular updates and patches to address vulnerabilities.

- **Documentation and Support:**

  The organization aims to offer comprehensive documentation and support resources to help users effectively use the OS and resolve any issues they may encounter.

3.2) Linux as a server type OS

- **Stability:**
  - **Long-Term Support (LTS):**

    Linux distributions often offer LTS releases, which are extended updates and security patches, typically five years or more, to maintain system stability and prevent disruptions.

- **Safety:**
  - **Security Updates:**

    Linux distributions regularly release security updates to address vulnerabilities and issues, ensuring a safe server environment through a proactive approach.

  - **Access Control:**

    Linux provides robust access control through user permissions, file ownership, and security policies, enabling administrators to establish and enforce stringent security measures.

- **Well-Behaved Environment:**
  - **Community and Support:**

    Linux's active user and developer community ensures a stable environment by providing support, best practices, and ongoing development, thereby maintaining server integrity.

- **Open Standards and Compatibility:**

  Linux, due to its open standards and protocols, ensures interoperability and compatibility with a wide range of software and hardware, making it ideal for integrating with various systems and technologies.

3.3) Android as mobile OS

- As a mobile operating system, Android has a number of characteristics that work together to give users and developers a stable, portable, reliable, safe, and well-behaved environment. Here are four key features that contribute to these qualities:

  - **Open Source and Customizability:**

    Android, an open-source platform, allows manufacturers to customize its operating system to fit various hardware configurations and user preferences. This allows for compatibility with Android apps on various devices, including smartphones, tablets, and smart TVs, ensuring portability across various platforms.

  - **Application Ecosystem:**

    Android shows a vast and diverse ecosystem of applications available through the Google Play Store. This huge app library provides users with a wide range of choices and confirms that they can find apps to suit their needs. This variety contributes to a well-behaved environment by enabling users to find the right apps to meet their requirements.

  - **Regular Updates and Improvements:**

    Google, the creator of the Android operating system, regularly releases updates, including bug fixes, security patches, and feature enhancements, to ensure the reliability and safety of Android devices and protect them from potential security threats.

  - **Interoperability with Google Services:**

    Android's seamless integration with Google services like Drive, Photos, Gmail, and Maps enhances user experience and contributes to the reliability and stability of the Android ecosystem, ensuring seamless data and service functionality within the Android environment.

4. SHARE RESOURCES AMONG USERS FAIRLY, EFFICIENTLY AND SAFELY

- **Fairly – equitable resource sharing refers to the distribution of resources among users according to priority.**
- **Efficiently – the aim is to optimize the use of resources. This affects resource consumption and system performance.**
- **Safely - Safe resource sharing is about protecting resources from misuse, unauthorized access, or security threats**

4.1) Windows as a client type OS

- **User account control (UAC)**

User accounts and permissions are essential for efficient resource sharing and security in computing environments. User accounts provide unique identities, while permissions dictate access to specific resources.

Superusers have the highest level of access, while "sudo" grants temporary privileges for authorized users.

Understanding and managing user accounts and permissions is crucial for maintaining an organized and secure computing environment.

- **Group policy**

Group policy is a crucial feature in Microsoft Windows operating systems, enabling administrators to define and enforce specific configurations, security settings, and restrictions for user and computer accounts within an Active Directory domain, simplifying the management of large numbers of computers and users.

- ## Task manager

Task Manager is a crucial Windows utility that offers real-time monitoring, control, and management of processes and system performance. It provides insights into CPU, memory, disk, and network usage and enables users to identify resource-intensive applications, start and terminate processes, set priorities, and view performance metrics. This is also used to close any programs when needed.

- ## Windows update optimization

For a Windows operating system to remain effective and stable, Windows update optimization is essential.

It entails managing upgrades, planning them for off-peak times, keeping an eye out for problems, and establishing an appropriate strategy.

Updates are sent by relevant organizations to maintain quality.

Regular optimization reduces downtime and potential issues by preventing resource conflicts and improving system functionality.

This procedure guarantees the stability of the system and reduces disruptions.

- ## User education

Due to a lack of user education many people are facing various problems nowadays

User education is crucial for a secure computing environment, enabling users to make informed decisions about technology use.

It provides knowledge on best practices, security threats, and organizational policies.

User education enhances digital literacy and promotes a security-conscious culture, empowering users to identify and respond to potential risks.

- ## Security measures

Security measures are essential safeguards for data, systems, and resources against internal and external threats.

They include firewalls, encryption protocols, intrusion detection systems, antivirus software, access controls, and regular updates.

These measures help identify vulnerabilities, protect against malware, and ensure industry regulations compliance in the digital world.

4.2) Linux as a server type OS

- **Quotas**

Quotas are crucial resource management tools in the Linux operating system, controlling and limiting users' or groups' consumption of disk space and files.

They prevent single users from exhausting available storage, ensuring fair resource sharing and system performance.

Linux offers user and group quotas, allowing for fine-grained resource management tailored to specific user needs or organizational policies

- **File permissions**

File permissions in Linux are crucial for access control and security, limiting file and directory access to authorized users or processes.

They are categorized into three groups: owner, group, and others. Administrators can define access privileges using read, write, and execute attributes.

File ownership and group associations are essential for specific access control. Properly configured file permissions protect sensitive data, enhance security, and ensure resource integrity, making them an essential part of a secure Linux system.

- **Accounts and groups**

User accounts and groups in Linux are crucial for managing access control and resource allocation within the operating system.

User accounts are unique profiles with unique usernames and IDs, while groups categorize users based on shared roles, simplifying access control and defining collective resource-sharing policies.

- **Scheduler policies**

Linux scheduler policies are crucial for optimizing system performance and ensuring fair resource allocation among running processes.

The Completely Fair Scheduler (CFS) is a widely used policy, ensuring fair allocation of CPU time based on priority and resource requirements.

This ensures no single process hogs system resources, maintaining system responsiveness and equitable sharing of CPU time among active tasks. Scheduler policies are essential for a balanced user experience.

- **Control groups**

Control Groups are a crucial feature in the Linux operating system that enable fine-grained control and resource management of processes and groups.

They efficiently allocate and monitor system resources like CPU, memory, I/O, and network bandwidth, ensuring resource limits are enforced, resource contention is prevented, and system stability is maintained.

Control groups also offer dynamic resource adjustment, preventing over-utilization and promoting fair allocation.

4.3) Android as mobile OS

- ## Application isolation

Application isolation is a key security feature in the Android operating system, where each app operates in its own sandbox, preventing direct access to other apps' resources or data.

This prevents malicious apps from disrupting system performance or posing security risks.

This isolation mechanism enhances user safety and privacy by preventing unauthorized access to sensitive data, making Android a trusted choice for mobile devices.

- ## Resource allocation

Android's resource allocation system prioritizes foreground applications for efficient user interactions and considers background processes to prevent excessive battery drain.

Its effective task and memory management ensures efficient resource usage, suspending or closing background tasks when necessary.

This fine-grained allocation maintains system stability, responsiveness, and efficiency, allowing users to run multiple apps and tasks without compromising system performance or draining the device's battery.

- ## Permissions model

The Permissions model in Android governs how apps access and interact with user data and sensitive resources on a mobile device.

Users can grant or deny permissions for specific actions or device features, enhancing security and privacy.

The model also allows users to review app permissions before installation, promoting transparency and informed decision-making.

This model strengthens Android's security, and trustworthiness, and enables a wide range of app functionalities.

- **Battery optimization**

Android's battery optimization feature extends mobile device battery life while maintaining user productivity.

Techniques like Doze and App Standby reduce power consumption by limiting background processes and network activity.

These features manage resources efficiently, minimizing battery drain during inactivity.

Android also provides users with insights into app battery usage, helping them identify resource-hungry apps and optimize power consumption.

These features enhance device longevity and user experience.

- **App lifecycle**

The Android app lifecycle is a framework that governs application behavior and interaction with the system. It defines states from creation to destruction and manages transitions.

It ensures efficient resource utilization and system stability by allowing apps to release resources when no longer needed.

This lifecycle allows developers to create apps that respond appropriately to user actions and conserve resources, improving the user experience on Android devices.

- **Security measures**

Android's security measures are comprehensive, encompassing app sandboxing, a robust permission system, encryption for data, regular updates, and Play Protect.

These measures protect user data and device integrity, ensuring a safe and trusted environment for users and developers.

They also ensure app permissions for sensitive actions, encryption for data at rest and in transit, and regular updates to address vulnerabilities.