SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

FACULTY OF COMPUTING

SECURED OPERATING SYSTEM – IE2032

ASSINGMENT

GROUP NO 28

GROUP DETAILS

Group Number: 28

	Student ID	Student Name	E-mail	Contact Number
1	IT22603104	DIAS M.P.U	IT22603104@my.sliit.lk	0717031982
2	IT22325150	NETMINI H.W.D	IT22325150@my.sliit.lk	0768600204
3	IT22560094	RANASINGHE T.M.R	IT22560094@my.sliit.lk	0781904889
4	IT22564740	HESHAN Y.B.K	IT22564740@my.sliit.lk	0703767354

TERMS OF REFERENCE

A report submitted in fulfilment of the requirement for the module IE2032-Secured operating system, Sri Lanka Institute of Information Technology. The scope of this report is to discuss some of the characteristics of operating systems such as Windows, Linux, Android and MacOS.

ACKNOWLEDGMENT

We would like to express our deepest gratitude to Ms. Suranjini Silva, the lecturer for our Secured Operating System module, for her invaluable guidance. And we wanted to offer our heartfelt thanks to the staff of the Sri Lanka Institute of Information Technology for providing essential resources. Special thanks to our colleagues for their insightful discussions, as well as the authors of the referenced documentation. Finally, our family and friends deserve our appreciation for their continuous support during this project.

TABLE OF CONTENTS

Well-behaved environment 3. Share resources among users fairly, efficiently and safety. Users and Group management Share resources. Safety 4. Manage memory, processor, file etc.	
Mac Operating system 1. Support many devices simultaneously. 2. Provide a stable, portable, reliable, safe, well-behaved environment. 2.1. Stability 2.2. Portability 2.3. Reliability 2.4. Safety 2.5. Well-behaved environment 3. Manage memory and process. 3.1. Memory management 3.2. Process management 4. The level of security it provides. 4.1. Hardware security 4.2. System security	
Android Mobile operating system 1. The level of security it provides. 2. Hide the implementation details. 3. Manage memory, processor, file etc. 4. Resolve conflict in resource demand.	
INDIVIDUAL CONTRIBUTION	
CONCLUSION	
REFERENCES	

ABSTRACT

In our research we have a valuable journey to understand the different kinds of operating systems and their unique features. Our primary aim is to gain more knowledge and understanding of the unique features of the operating systems, which are Linux, MacOS, Windows and Android. As part of our research, we examine and analyze these platforms. Which is Level of security it provides, manage memory- process-file, hide the implementation details, provide a stable, portable, reliable, safe, well-behaved environment, Support many devices simultaneously and many more topics. As a result of our research, we hope to give useful and reliable information that helps users to make their own decisions and select the most suitable operating system for their specific needs.

INTRODUCTION

Operating system is an essential aspect in any modern day computer devices. The operating system provides an interface to efficient management of users and hardware. From embedded systems to super computers, operating systems plays an vital role for computation processes. This report was created to discuss some of the aspects in operating systems including Linux, Windows, MacOS, Android. These operating systems covers all the operating system types such as Server, Client and Mobile operating system.

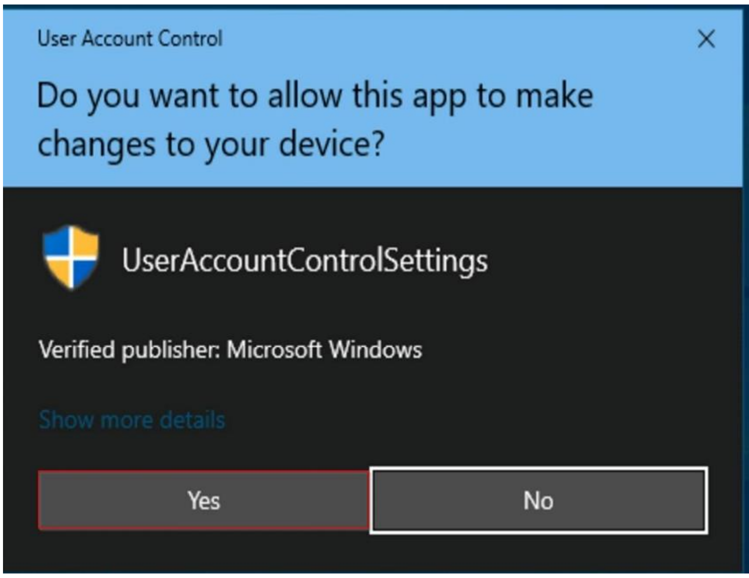
Linux operating system is more widely used in Computer servers due to the compatibility with open-source development. This report covers some of the key concepts and methods used in Linux operating system such as efficient environment, security controls, efficient management of hardware and management of users. Windows operating system is well known due to the robust and efficient environment. This report navigates through some of the aspects in windows operating system providing readers to have profound understanding of the methods and concepts. Stable, reliable and efficient environment in MacOS provides user to have more robust working environment. This report delves into some of the key aspects used in MacOS. Due to the portable environment of Android operating system, most of the mobile device making companies have embedded android into their devices.

Through an comprehensive examination of these operating system, this report aims to provide knowledge with real world examples.

WINDOWS OPERATING SYSTEM

1. The level of security it provides.

1.1 User account control. (UAC)

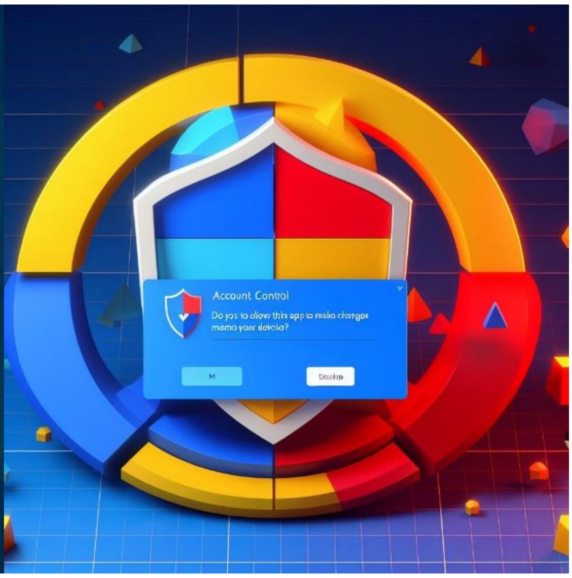


User Account Control

Do you want to allow this app to make changes to your device?

UserAccountControlSettings

Verified publisher: Microsoft Windows



User account control is a windows security feature. It is designed to protect the operating system from unauthorized changes. When a user launches a program a personal access token is attached to it. That personal access token contains the user identifier and their associated privileges. Windows automatically assigns tokens to the programs. User access control check user tokens and if user has privileged access, then only an invisible additional token is created. We called it “User tokens and program execution”.

Windows OS administrators have both types of tokens. Which are administrative tokens and Standard user access tokens (Sat tokens). Windows process can receive only one of these tokens at a time. And it is not changeable after assigning. Because of this mechanism, programs are allowed to request additional privileges during their operation.

Programs running with an administrative token can pass this token to other processors. According to the Token inheritance additional privileges are granted. This User account control feature ensures higher privileges are only executed when it's authorized by the user.

Certain predefine groups such as,

1. Administrators-users who have full control over the system.
2. Back up operators-users who are responsible for managing data back up and restoration.
3. Power users- have more control than the regular users, less control than the administrators.
4. Guest users-users who have restricted privileges or temporary access
5. Remote users-users who have rights to connect to the system from outside the network.
6. And much more... have special rights to the system.

These rights allow them to perform actions like creating copies, accessing data, changing system settings, system configuration, file access, user account management, audit log access and system updates. So, the token assignment depends on the above-mentioned group membership and their legitimate level of access.

User access control improves the security of windows by limiting the access that malicious code has to execute with the administrator privileges. Because UAC continuously informs decisions and actions that may affect the stability and security of their devices.

Benefits of User access control.

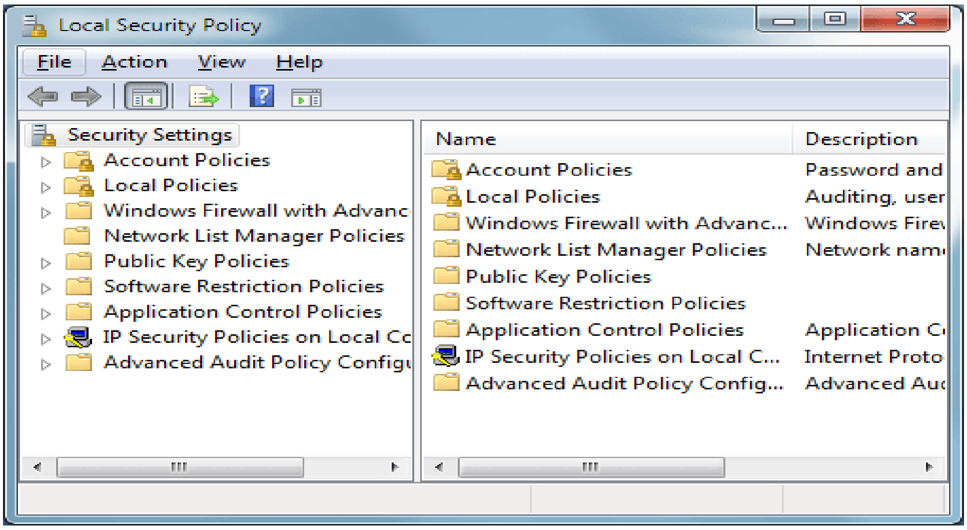
Benefit	Description
Enhanced security	Prevent unauthorized or unintentional system alterations.
Least privilege principle	Reduce the damage from malware or unauthorized software. Promote default operation with standard user permission.
User awareness	Inform users about applications which are attempting system level changes. Encourage user decision on what runs on their windows operating system
Mitigation human errors	Prevent unintentional system changes. Always requires user confirmation/permission for actions affecting the windows system scalability.
Support the multi-user environment	Suitable for use in multi-user settings. Ensure each user is accountable for their actions.

1.2 Security Policies.

The first step to improving the security of any aspect is to have a security policy. Generally, it includes a statement of what is secured. For example

- Password policy- require users to create strong passwords using different combination of characters
- Two factor authentication-grant access only the legitimate users.
- Regular software updates-Ensure the security software's are regularly updated to prevent known vulnerabilities.
- Backup and disaster recovery-ensure critical data can be restored an any failure.
- Logging and monitoring-configure loggings and regularly review loggings.

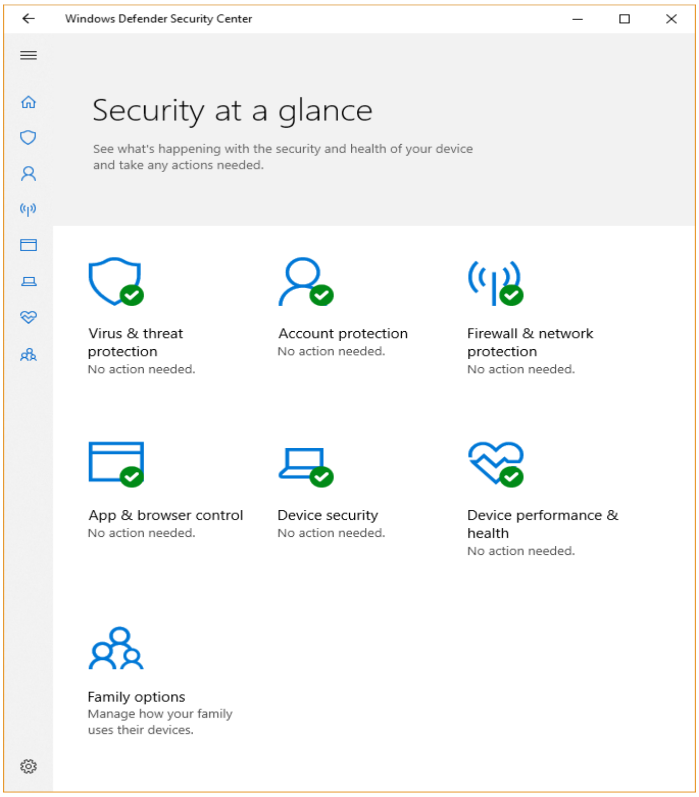
Without a policy it is impossible for users and administrators to know what is permissible, what is required and what is not allowed.



Security Settings
- Account Policies
- Local Policies
- Windows Firewall with Advanc
- Network List Manager Policies
- Public Key Policies
- Software Restriction Policies
- Application Control Policies
- IP Security Policies on Local Cc
- Advanced Audit Policy Configu

Name	Description
Account Policies	Password and
Local Policies	Auditing, user
Windows Firewall with Advanc...	Windows Firev
Network List Manager Policies	Network nam
Public Key Policies	
Software Restriction Policies	
Application Control Policies	Application C
IP Security Policies on Local C...	Internet Proto
Advanced Audit Policy Config...	Advanced Auc

1.3 Windows Defender and Antivirus.



Security at a glance

See what's happening with the security and health of your device and take any actions needed.

Virus & threat protection
No action needed.

Account protection
No action needed.

Firewall & network protection
No action needed.

App & browser control
No action needed.

Device security
No action needed.

Device performance & health
No action needed.

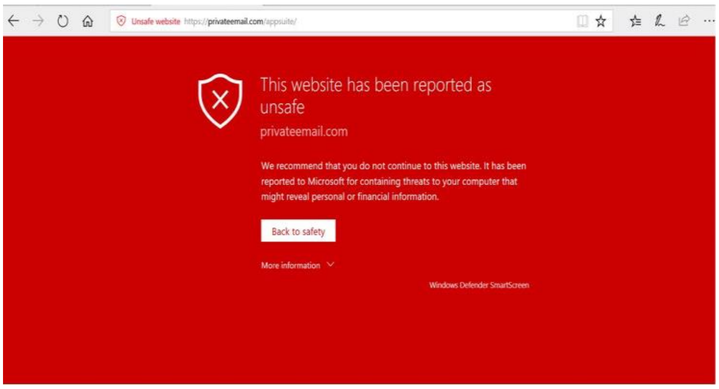
Family options
Manage how your family uses their devices.

Microsoft defender and antivirus protection program formally known as windows defender. It is not like the other antivirus programs because windows defender is free and does not need additional installation. This software is built to detect and remove malware from windows base computer. These windows defender antiviruses are available in windows 10, windows 11 and in version of windows server. There are several kinds of features in the windows defender. For example, automatically backing up files to one drive, expansive parent control settings and the password verification replaced by using face recognition, fingerprint technology and many more. This defender tracks our data and manages it. So, it gives us more control over our privacy settings when we are browsing the web pages. It also has a password generator plus password monitor, that will let the user know if any of the users' password was compromised.

The bellow table describes windows defender and antivirus softwares' three different modes [01].

Mode	Description
Active mode	Work as the primary antivirus software in the device. File scanning/ detect the threats/ remediated threats/listed in organization security report.
Passive mode	Does not Work as the primary antivirus software in the device. File scanning/ detect the threats/listed in organization security report. But it does not remediate threats.
Disabled or uninstalled	Windows defender and antivirus do not work. File scanning/ detect the threats/ remediated threats/listed in organization security report does not happen. Disabling or uninstalling the defender is not recommended.

Benefits of windows defender and antivirus.



This website has been reported as unsafe

privateemail.com

We recommend that you do not continue to this website. It has been reported to Microsoft for containing threats to your computer that might reveal personal or financial information.

Unsafe website https://privateemail.com/appsuite/
Back to safety
More information
Windows Defender SmartScreen

Benefit	Description
Real-time protection	Continuously monitoring the operating system.
Law system impact	This windows defender was designed to have minimal impact on your machine performance.
Phishing protection	Including Anti fishing features helps to protect operating system from fraudulent web sites and scam emails.
Firewall integration	This helps to prevent unauthorized access to networks and operating systems.

customization	Users can often configure the antivirus software to suit their specific needs. This gives more control to users over the security settings.

1.4 Firewall and Network security.

There are lots of valuable materials on the web because connecting to the web is important. When a computer connected to the internet it exposes two kinds of dangers. Which are incoming dangers and outgoing dangers [2].

Incoming dangers	Malware	Phishing	DOS Denial of service	Unwanted content	virus	spyware
Outgoing Dangers	Botnets	Unwanted communication	E-mail spam	Data leaks	Resource exploitation	Unintentional sharing

Because of that we need a mechanism to keep good bits in and bad bits out. So, using firewall we can fulfill our need. This mechanism forces every bit which is entering or leaving to go through a single draw bridge. Where are all these bits going to be inspected by the input-output police. The same method is used to check network policy. Many LANs are connected in arbitrary ways, but all traffic to or from the mechanism is forced through an electronic drawbridge, which is called the firewall.

There are two basic varieties in the firewall, hardware and software. Companies with LANs usually protect hardware firewalls. Homes which have individual LANs are protected by software firewalls. Firewalls have rules to decide what is allowed to in and what is allowed to out. But these rules can change the owner of the particular firewall. To allow this most firewalls have a mini web server in it. The simplest kind of firewall is the stateless firewall.

These stateless firewalls first read the header of each packet passing through and do the inspection part. Next it decided that inspected packets are going to pass or discard. This decision is mainly based on that inspected header and the firewall's rules. Packet headers include various types of information. Which are source and destination addresses, Source and destination port numbers, Sequence and acknowledgement numbers, time to live or hop limit (TTL), protocoled information, options and flags, type of service and protocol and some other fields.

In addition to the stateless firewalls there are different kinds of firewalls used in windows operating systems.

Firewall	Description
Windows firewall	• This is a basic built in firewall in most windows versions. • Filter network traffic based on predefined rules and inspections. • It inspects packet headers, ports and protocols. • Provide basic security for most users. • It can block unauthorized network access.
Windows defender firewall with advanced security	• have extended functions in windows firewall. • It allows users to customize firewall rules based on programs, ports and IP addresses. • It inspects packet headers, ports and protocols and makes decisions. • Offers a higher level of security than the basic firewall. • Suitable for users who have specific security requirements.
Third party firewalls	• Normally it provides more advanced features than the basic windows firewall. • These firewalls inspect packets headers, content and the behavior. • Because of that it can do a deep packet inspection and provide higher security. • Users who require higher security effectively and who want to customize options this is more suitable for them.
Application firewalls.	• This is built for focusing and monitoring specific applications and controlling them. • To prevent unauthorized data access and data exploitation it uses two parameters. • Which is packet inspection and application behavior analysis. • Provide higher security for the application layer.

2. Manage memory, processor, file, etc.

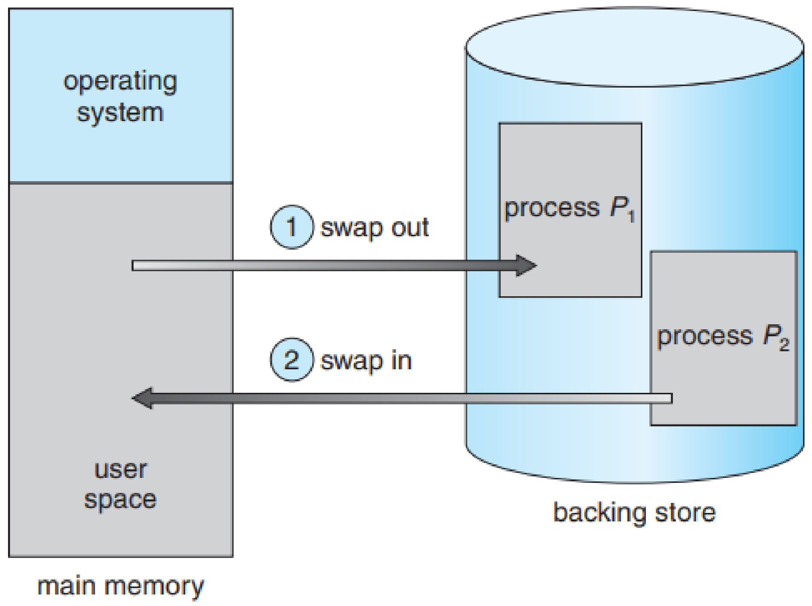
2.1 Memory management.

Execute programs is the main purpose of an operating system. During the execution these programs data need to be in the memory. To improve both utilization of the CPU and speed of its response time is more important. To fulfil that general purpose computers, have several processors in the memory. Memory management system is the mechanism of doing that. Creating that mechanism, we need to beware of hardware design of the system, memory allocation, memory protection, memory deallocation, swap space, resource monitoring, scalability and concurrency are some of them. Modern computer systems' memory is central to the operating system. Memory has a large array of bytes; each byte has its own address. According to the values of the program counter CPU fetches instruction and pass it to the memory. This instruction may cause additional loading and storing memory address space.

Memory management system has a typical instruction execution cycle. First fetches an instruction from memory. These instructions and addresses are based on the program counter. Retrieve those instructions and it will send to the cache or random-access memory. Perform the operations these fetched instructions need to be decoded. To do that the operating system uses an addressing mode and decodes the instructions. Next using that decoded instructions CPU performs the actual operation. In this execution step arithmetic or logical operations, Data manipulations or control transfers will be involved. Next step is known as memory access step. In this step those instructions which perform actual tasks such as storing and loading data will be detected. Finally reading and writing memory locations for those operations are carried out. The final step is the write back step. In this stage the results of the executed instructions are written back to the appropriate registers or memory locations.

Swapping

Windows operating systems use swapping as a form of virtual memory management method [3]. To execute a process, it should be in the memory. However, the process can be swapped temporarily out from the memory and then brought back and backing store into the memory for continued the execution. Swapping makes a space in the real physical memory of the operating system. It increases the degree of multi programming in the windows operating system.



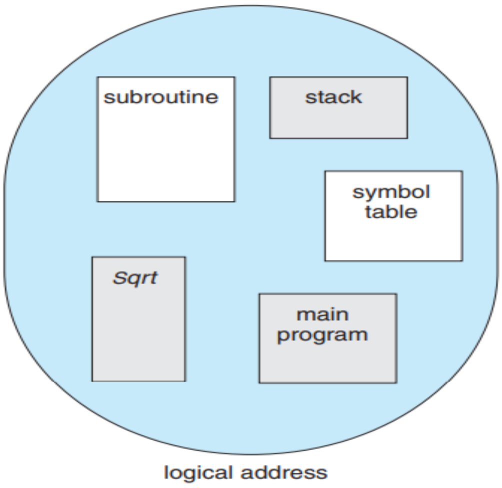
. There are some advantages of having swapping method in the memory management procedure. Standard swapping involves moving the process between the main memory and a backing store. The backing store is a large disk. This backing store disk is large enough to accommodate all the memory images copies for all users. And it needs to have direct access to the memory images. The operating system maintains the ready queue. It knows all the memory images are in the backing store or in the memory or ready to run. Next most important thing is dispatcher. Deciding the next execution process is also important. Whenever the CPU schedulers decide the next process, we call it dispatcher segmentation.

Advantages	Description
Process Isolation	Swapping ensures that each process operates in its own isolated memory space. Prevent one process from affecting another process.
Efficient resource usage.	Allows processors to run simultaneously. Does not require excessive amounts of physical RAM.
Prioritization.	The operating system can prioritize pages from swapping. That ensures important or frequently used data remains in the RAM.

Segmentation

In Segmentation method memory divides into two segments. This is another memory management technique. These segments represent logical units. Code segment, data segment or stack segments are some of it. In the window's operating systems segmentation is used as foundation for memory protection, operate multitasking and process multiple processors. Windows segments are created to represent different aspects of a process. Code, data and stack segments are some of them. These segmentation methods ensure that the process cannot access memory outside its own segment. So, that enhances memory protection.

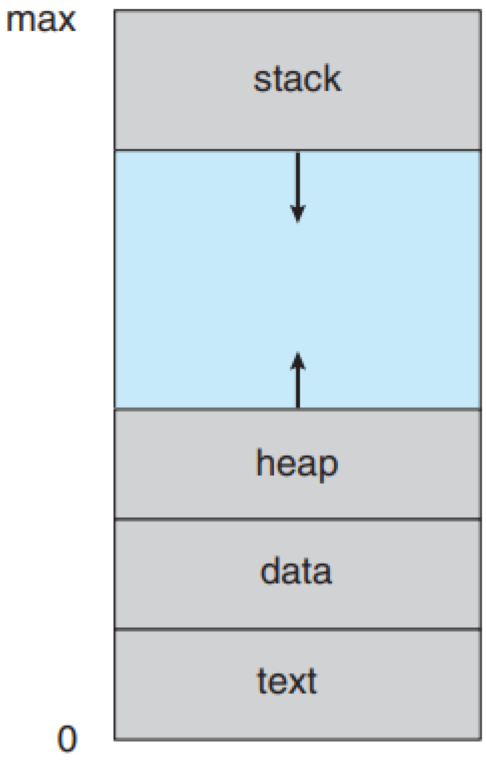
This memory management schema supports the programmers to view the memory. A logical address space is called a collection of segments.

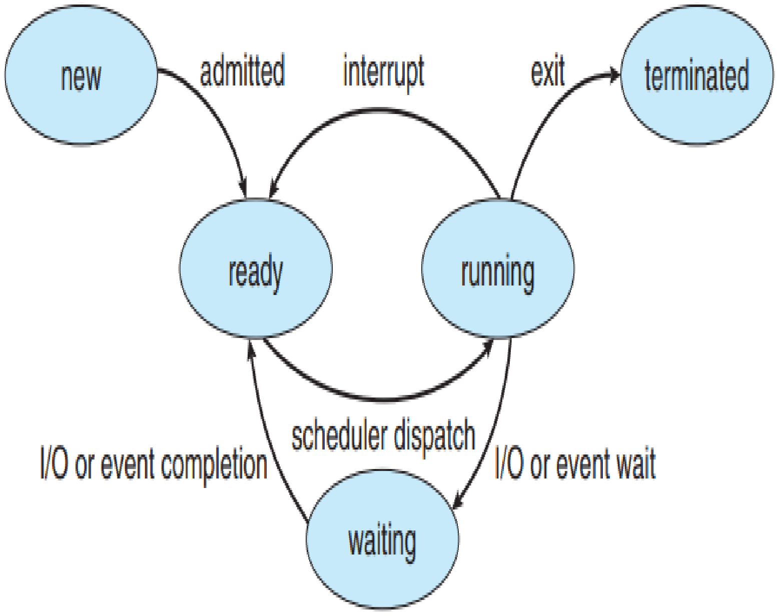


Each segment has a name and length. The address represents both the segment name and the offset within the segment.Programmers specify each address by two quantities. Which is a segment name and offset. For simple implementation segments are numbered. It is called segment number, rather than by segment name.
<Segment-number, offset> [4]

There are some advantages of segmentation in windows. Segmentation restricts a process from accessing memory outside it allocated segment. It gives memory protection. Segmentation ensures one process cannot interfere with another process. We call it process isolation. Also, dynamic memory allocation is another advantage of this segmentation technique. Segments can resize dynamically, which is important for managing variable memory requirements.

2.2 Processor management.





Process can simply be defined as a program in execution. Also, this process will need certain resources. Such resources are CPU time, memory, files and input output devices to accomplish its task. These resources are alllocated to the process. A process is a unit of work in an operating system. However, one system consists of a collection of processes. Operating system processors execute system code and user processes execute user code. The operating system is responsible for aspects of process and thread management. For example,

- Creation and deletion of both user and system processes.
- Scheduling of processes.
- Mechanism for synchronization-communication.
- Deadlock handling for processes.

In the creation process step it involves new process which called child process and existing process called as parent process. This parent process may use system calls or API functions to create a new process/child process [5]. Next step is process termination. Normally the parent process or the operating system terminate the process. Resources allocated to the process will be released at the end of this step. The process state transition is the next step. Process can be in various states such as running, ready or blocked states. The operating system manages these states and makes the transition between them. It is based on process execution or input output operations. The process synchronization step starts as the next step. It needs to ensure proper coordination between processes. Synchronization mechanism helps to fulfill that. Process may need to communicate with each other. That is the next step named as Inter-process communication. Windows operating system provides various mechanisms like pipes, sockets and named pipes.

Process scheduling

The process scheduling is a task which is selecting which process should run next on the CPU. Windows operating system uses various scheduling algorithms. Priority based scheduling, round-robin scheduling, multilevel queue scheduling, Multi feedback queue scheduling, shortest job next scheduling, first come first served scheduling, priority inheritance scheduling, round robin with priority scheduling, fixed priority preemptive scheduling, fair share scheduling.

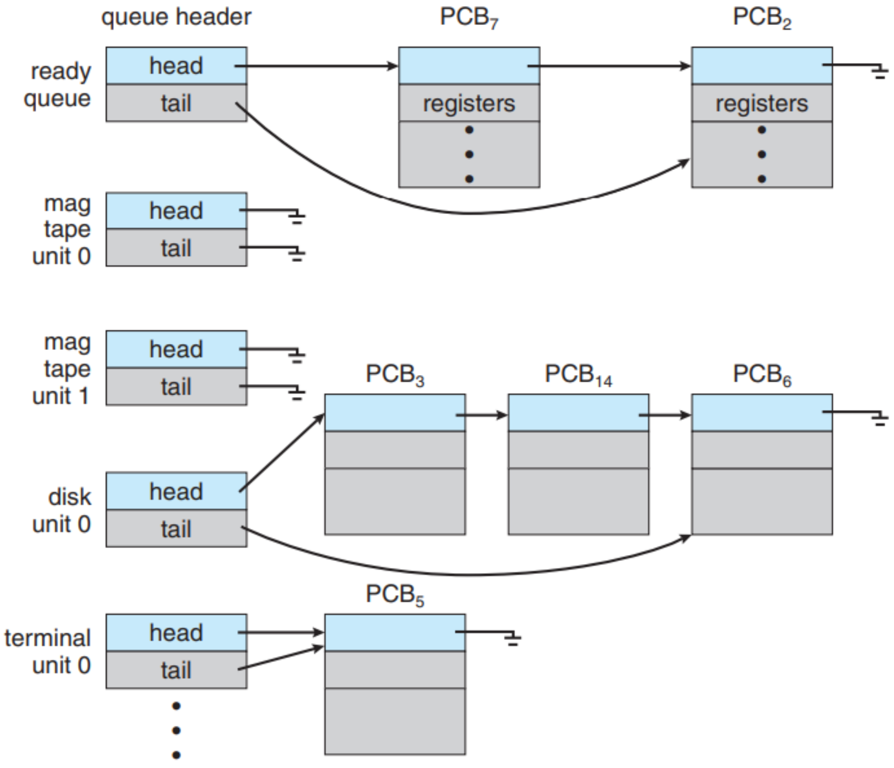


Figure 3.5 The ready queue and various I/O device queues.

The object of multi programming is to have running process all the time and busy the CPU as much as possible. It is named maximum CPU utilization. The objective of time sharing is to witch the CPU among the processors frequently. It gives a space for users to interact with each program while it is running. To fulfill this objective, the process scheduler selects an available process for program execution from the CPU. But the single processor systems there will never be more than one process running. There are few process scheduling topics to discuss.

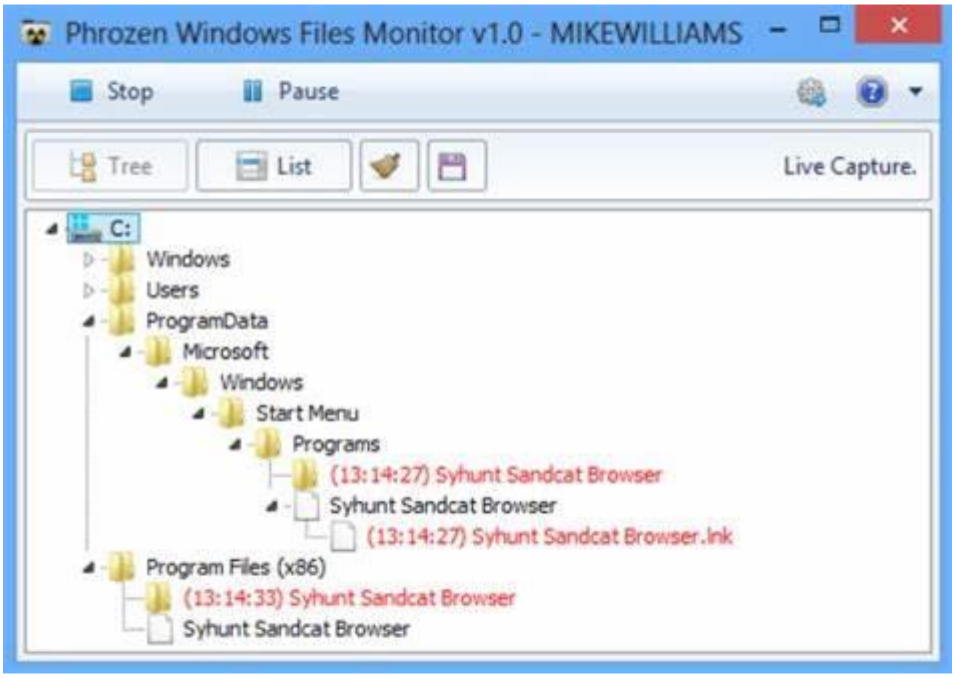
Topic	Description
Dispatcher	It selects the process from the ready queue and allocates the CPU to it.
Priority levels	Windows assign priority levels to process. Higher priority processors will execute first, and the lower priority ones execute later. Priority levels are dynamic it can be changed during the execution.
Process preemptive	If a higher priority process becomes run or current process's time quantum expires then it named process can be preemptive. Windows operating system handle preemptive to ensure fair resource sharing.

2.3 File system management.

File system is the most visible aspect of an operating system. It provides mechanisms for access to both data and programs in the operating system. Computers can store information on various storage media. Such as magnetic disks, magnetic tapes and optical disks. The operating system abstracts from the physical properties of its storage devices to define a logical unit the file. Files are mapped by the operating system on to physical devices. A file is named collection of related information that is recorded on secondary storage [7]. Commonly files represent programs both source and object forms and data. Data files may be numeric, alphabetical, alphanumerical or binary. The information in a file is defined by its creator. It can store many different types of information. For example, source or executable programs, numeric or text data, photos, music, video and many more. A file has a certain defined structure depending on its type.

- Text file- sequence characters organized into lines.
- Source file- sequence of functions.
- - further organized as declaration followed by executable statements.
- Executable file- series of code sections that the loader can bring into memory and execute.

Windows operating system supports different types of file systems.



```
C:
  Windows
  Users
  ProgramData
    Microsoft
      Windows
        Start Menu
          Programs
            (13:14:27) Syhunt Sandcat Browser
            Syhunt Sandcat Browser
              (13:14:27) Syhunt Sandcat Browser.lnk
  Program Files (x86)
    (13:14:33) Syhunt Sandcat Browser
    Syhunt Sandcat Browser
```

File type	Description
NTFS- new technology file system	Primary file system used in modern windows operating systems. It offers advanced features like file and folder permission/encryption/compression and support for large volume.
FAT32-File allocation table	Older file system with broad compatibility. Used for smaller storage devices. For example, USB devices and memory cars.
Ex FAT-extended file allocation table	Design to overcome the limitations of FAT32. Compatibility with different platforms is needed. Suitable for flash drives, SD cards and other removable media.
ReFS-Resilient File system	The modern file system introduced in windows server. Designed for fulfill data integrity, scalability and higher fault tolerance.
CDFS-compact disc file system	CDFS is used for reading data from CD's and DVD's. This is a read only file system designed for optical disks.

3. Support many devices simultaneously.

The windows operating system developed by Microsoft is most widely used in the world. The main reason for that is windows can support various kinds of hardware devices. For examples desktop and laptop computers, tablets, mobile devices, servers, printers and scanners, monitors and displays, input devices, external storage devices, graphic and video cards, network adaptors, audio devices, camera and web cams, portable media players, gaming devices, smart home devices, IOT devices, digital cameras and camcorders and biometric devices can be identified. Here are some details about it.

Devise	Brands	Windows version	Description
Personal computers	MSI Dell HP Lenovo Acer ASUS	Windows 10 Windows 11	• Primarily used on desktops and laptops. • Provide various things like productivity, entertainment, security and many more.
Tablets	Microsoft surface Samsung galaxy	Windows 10 Windows 11	Windows offers touch friendly interface for on the go computing.
Mobile devices	Microsoft Lumia Acer liquid Archos Cesium Xiaomi Mi 4	Windows mobile	Windows mobile version is designed for mobile phone operating systems.
Servers	Dell power Edge HP ProLiant Lenovo Think Server	Windows server 2019	Windows server version used for various purposes. Including file storage, web hosting and enterprise services are some of them.
Printers and scanners	HP Epson Canon Brother	Windows 10 Windows 8.1 Windows 7	Device manufacturers decide the software and device driver types.
Monitors and displays	Dell LG Samsung Acer	Windows 11 Windows 10 Windows 8.1 Windows 7	Have a wide range of display technologies including LCD monitors, projectors and multiple monitor setups.
Input devices	Logitech Microsoft Razer	Windows 11 Windows 10 Windows 7 Windows vista Windows XP	Windows operating system works with different kinds of input devices. Such as keyboards, mikes, touch pads and stylus pens.

So, the windows operating systems support a wide range of devices simultaneously. There are some advantages of this multidevice support and compatibility.

- Universal plug and play –UPnP

Universal plug and play support in windows devices and automatically discover and configure in network. This is simply known as the process of adding and using network devices. Such as printers and media servers.

- Unified user experience.

Windows supports various kinds of devices. Such as desktop, laptop, tablet, or mobile devices. It helps to give a unified user experience across the different devices.

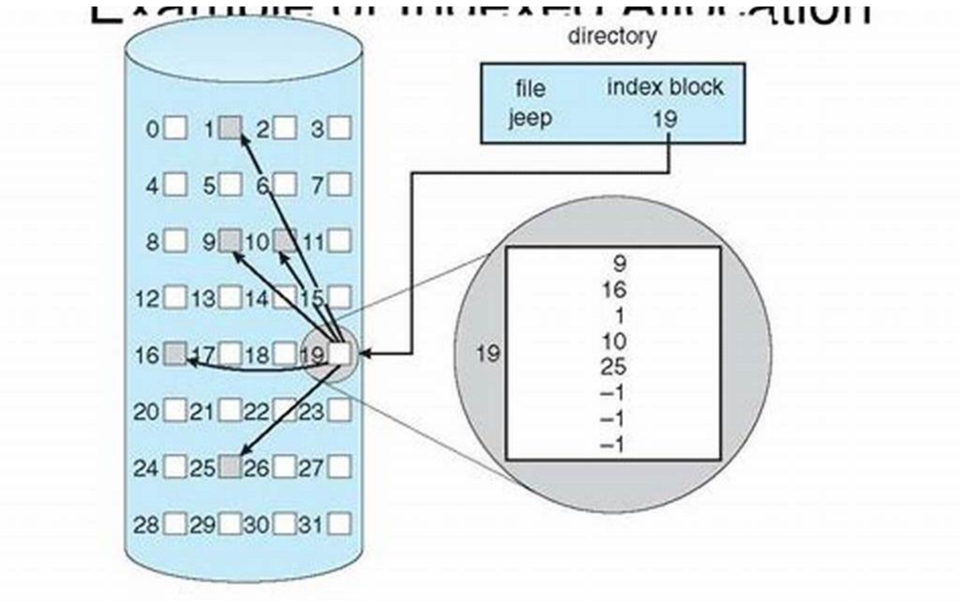
- Cross-platform compatibility

Windows operating systems are designed to interact with various platforms. Windows can communicate with Android and IOS devices through applications and cloud services.

- Enhanced productivity

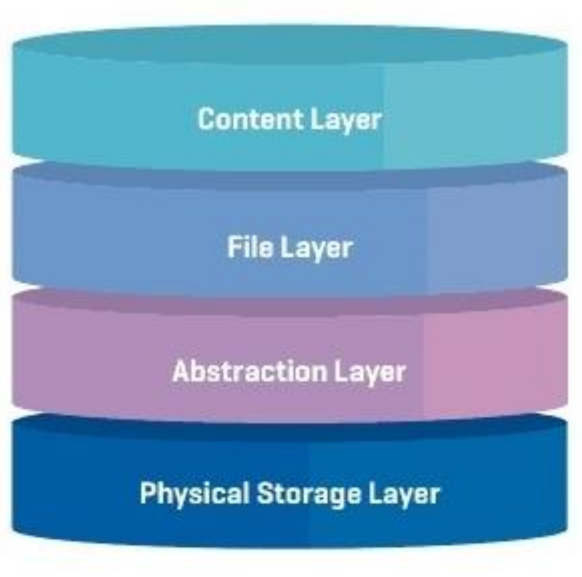
Because of the Multiuser support users can access their data, applications and settings from different devices. For example, windows Sync, Microsoft 365 and OneDrive enable users to work with any ware any device any time.

4.Hides the implementation details.



Windows operating system does a lot of work in the backend, but it does not bother the user with all the technical stuff. It hides the complicated files and confusing details so users can just use their device easily. So, this hiding implementation details mechanism allows user to work without knowing the mechanism. This makes windows devices user friendly and simple computer experience. Windows operating system ensures that the user can communicate with their devices using a language user understands. It is like a translator converting user requests into actions the device can perform. It is all about making technical more accessible and less intimidating.

4.1 Abstract layers in windows.



Abstraction layer is like secret translator. It helps the operating system talk to hardware and software without revealing all the mechanisms and techniques. Hardware abstraction layer hides the nitty-gritty details. So, windows can work on a lot of different machines. Application programming interfaces are set of rules that help software programs communicate with windows operating systems. Therefore, there are some advantages of having abstract layers on windows. Because of hiding the differences in hardware windows can work wide range of computers. It is called hardware compatibility. The other advantage is device support. Device drivers make sure that the other devices can easily be connected to windows. Softwrae flexibility is another advantage. Applications programming interface make it easier for software developers to create programs without knowing the technical hardware details.

4.2 Accessibility in windows.

Accessible tools are helpful tools for people with disabilities. It includes things like screen readers, screen magnf

iers, voice recognition software, text to speech tools and many more. This screen reader application converts text into speech or brail. Also, the voice recognition enables hand-free computer operations. These features make sure that anyone can use windows effectively. There are some advantages of having Accessibility in windows operating systems.

Advantage	Description
Inclusivity	Accessibility feature ensures windows can be used by any person.
Productivity	These features empower users to become more productive and independent.
Lagle complains	This helps organizations meet legal requirements related to providing accessible technologies and services.

LINUX OPERATING SYSTEM

1. SECURITY LEVEL OF LINUX OPERATING SYSTEM

USER PERMISSION AND PRIVILLEGE MANAGEMENT

Linux operating system is widely used in servers such as Database servers, file server, email server and web server due to managing and handling of concurrent access. For instance, multiple users have access to resources available on the server by managing concurrent access to it. To manage the integrity of data the concept of permission and privileges emerge.

Linux permissions ensure that users are allowed to access resources with given privileges. This method of managing users enables sharing resources among several users to use the operating system concurrently.

For the convenience of managing permissions to resources, three types of permissions are implemented [8].

USER

GROUP

OTHER (PUBLIC)

Moreover, “USER” accounts are further categorized into three types [8].

ROOT USER ACCOUNTS – also known as “superuser”. This type of user has complete access to resources across systems.

REGULAR USER ACCOUNTS – also known as “standard user”. This type of user can perform only authorized functions only.

SERVICE USER ACCOUNTS – Created by user applications. All privileges of “USER” account are available for this type of user.

Additionally, there are three types of access controls to resources.

Read(r) - To view the content of the file or to view the names of the files inside a directory.

Write (w) - To perform any modification of resources.

Execution(e) - To execute the files if the user has read permission to resource.

In Linux system command *$ ls -la* is used to demonstrate the details of files and directories in current working directory.

```
$ls                                                                                -al
total                                                                                0
-rw-r--r--       1      un9       group1      9       Apr     22      13:42       file
^  ^             ^              ^               ^            ^                       ^
|                 |       |         |           |       |                  └──        ❶
|                    |           |            |              |          └──           ❷
|                      |             |              | ❻               └──             ❸
|                          |                 |❺                    └──                ❹
|                                                                                  └──
|                                                                                  └──
└──   ❼
```

1 – This indicates the name of the file

2 – Date of which the last modification to file

3 – This indicates the size of the file in bytes

4 – Name of the group which the file is belongs to

5 – Name of the user which the file is owned by

6 – Indicates number of hard links to the file

7 – Mode of the file. “-” indicates a file while “d” indicates a directory.

In the above example access controls for each user account are listed. Generally, access controls for each user account are listed in the following format.

`-<user-access-controls><group-access-controls><public-access-controls>`

`Ex: -rw-r--r--`

In the above example, the user (in green colour) is given with both read and write permission to the file. Group users (in blue colour) are given permission to read only while public users (other users) are given permission to read only (in red colour).

FILE SYSTEM SECURITY

In Linux environments, access control to either files or directories can be changed. Mainly commands such as “chmod” and “chown” can be used to modify these privileges. Two methods are used to change privileges [9].

1. Absolute method
2. Symbolic method

In absolute method modifications can be implemented using octal values. These numberic arguments can be specified to change according to your desired modification. Indications of octal values are here as follows.

```
0 indicates no permission.

1 indicates execute permission.

2 indicates write permission.

4 indicates read permission.
```

Access Class	User	Group	Other
Symbolic Mode	r w x	r - x	- - -
Binary Mode	1 1 1	1 0 1	0 0 0
Octal Equivalent	7	5	0

Ex: `$ chmod 744`

In this command,

Number 7 demonstrates, give all the permission (read, write, execution) are given to “User”

Number 4 demonstrates, give read permission only to the “group” user

Number 4 (number at third place) demonstrates, give read permission to the “public” user.

In symbolic method, filer permission is granted by combining and specifying r,w,e characters.

Ex: `chmod a+rw file.txt`

In above example demonstrate to grant read, write and execute permissions to file called “file.txt”

NETWORK SECURITY

In Linux environments, security of network plays a major role. Linux consists of various implemented measures to safeguard Linux based system from threats such as unauthorized access, data breaches and cyber threats.

Open-source compatibility has made Linux to have a robust foundation to implement various network safeguarding mechanisms to protect network environments. The following context addresses various mechanisms in Linux operating system to safeguard networking environments.

FIREWALL MANAGEMENT

Linux firewall is a virtual wall to protect our systems from unauthorized access and unwanted traffic. It can be used to block IP addresses, specified subnets, ports and services. To maintain the firewall policies, Linux system consists of system daemon called "Firewalld". Firewalld is a tool available in Linux which can be updated in real time if any change occurs in the networking environment [10].

Linux firewalls consist of various different types. IPCop, IPtables, Shorewall and UFW are some of them.

NETWORK SECURITY SERVICES

To safeguard systems from unwanted access and traffic, Linux operating system provides customization to different ports, IP addresses and protocols [10].

1.Allowing SSH traffic

All traffic on SSH ports is allowed. By using this remote connection to any other system in the network.

2.Allowing incoming traffic on specified ports

To specify traffic on specific port

3.Blocking incoming traffic on specified IP address

TCP WRAPPER

A software package which is available in Linux operating system to restrict services on TCP excluding UDP and ICMP. This was originally designed by vietse venema to filter out network access to internet protocol servers on Linux operating system [10].

VPN SUPPORT

VPN stands for Virtual Private Network. VPN is a point-to-point connection which masks internet traffic. VPN ensures secure connection, remote access, Anonymity, Unblock content, Bypass ISP throttling [10].

SECURITY AUDITING AND LOGGING

The Linux operating system consists of a tool called “auditd” to collect and write audit log files. Auditd is a daemon which runs in the background while the operating system operates.

PACKAGE MANAGEMENT AND UPDATES

Package management is a process of installing, updating and removing software in Linux operating systems. Various Linux distributions (Linux distros) comes with their unique software package managers which allows users to manage software on their devices.

Apt, yum, pacman, DNF, zypper, are some of the most famous package managers for Linux operating system. Each package manager consists of unique functionalities.

OPEN-SOURCE SECURITY MODELS

Linux Security Model (LSM) is an open-source framework which supports Linux kernel excluding various security models. The framework has obtained license from GNU General Public License it has being a part of Linux Kernel since version 2.6. LSM was designed to address access control system in Linux with making minor modifications to the Linux kernel. LSM is in scope to solve the access control issue in Linux system while not making significant changes to main kernel.

2. PROVIDE A STABEL, PORTABLE, RELIABLE, SAFE, WELL-BEHAVED ENVIRONMENT

Linux operating system ensures efficient and safe working environments for the user by achieving various objectives. Features such as stable, portable, reliable, sage well-behaved enhances the overall quality of work and user experiences in Linux operating system. The following section addresses the role of each of those features in Linux operating system.

STABILITY

Linux operating systems achieve stability by enabling Kernel stability and software stability. Package management software manages the dependencies and likelihood of software by reducing conflicts which leads to unreliability of the system. In addition, Kernel stability ensures the protected environment in Linux systems.

Techniques such as Modular design of Linux kernel, Software package management, Community code review, Robust file system enables the stability of Linux Operating System.

Worldwide developers has contributed to the development of Linux operating system. This method of development model has enabled users to have more control over their devices which leads to stability of their devices.

PORTABILIY

Linux operating system has been used in variety of systems due to it compatibility with the hardware. For instance, systems such as personal computers, servers, mobiles and embedded systems operate with Linux operating system. Moreover, Libraries and standardized interfaces allows to run the programs developed in Linux kernel on other systems.

Techniques such as cross-platform development tools, Dynamic linking of programming libraries, POSIX compliance, Abstraction layers to separate hardware specific details from high level software ensures the portability of Linux operating system.

RELIABILITY

In terms of reliability of the operating system, Linux has the demanding reputation of being robust and stable. As we discussed earlier, open-source development of Linux offers more compatibility with reliability of the system [11].

Linux is designed with various techniques to establish reliability of the system. Following is some of the approaches to guarantee reliability.

1. User and group permission
2. Logs of user logins
3. Backup and recovery
4. Redundancy and failover
5. Data encryption tools

SAFETY

Most of the distributions of Linux provide security features such as access control systems, event logging, firewall functions and service updates. Such features enable users to configure the safety of their devices.

WELL-BEHAVED ENVIRONMENT

3. SHARE RESOURCES AMONG USERS FAIRLY, EFFICIENTLY AND SAFETY

Linux operating system provides sharing of finite resources among users and processors. Resources such as disk space, memory, CPU and devices connected devices through internet are shared among users to provide efficient and collaborative working environments. In Linux operating systems various techniques are implemented to achieve resource sharing among users equally and efficiently. The following section addresses some of the key aspects.

USER AND GROUP MANAGEMENT

Linux categorizes users into groups to utilize management of users. Each of user has defined permissions assigned to them. Administrators are given the permission to define access controls and allocate resources based on groups. Additionally, limiting resources to specific users or groups can also be configured in Linux systems. Administrators are allowed to define constraints on various resources such as CPU Time, File size, Memory usage etc.

SHARING RESOURCES

Finite resources are shared among users to maximize utilization of the system. Linux uses schedulers to manage disk I/O requests and CPU scheduling. Nowadays Linux uses **CFQ (Complete Fair Queueing)** scheduler to manage disk I/O requests providing equal access to disk access by allocating time slice for each process. The CFQ scheduling algorithm responsible of preventing processes from dominating disk I/O s.

Furthermore, **CFS (Complete Fair Scheduler)** algorithm ensures equal CPU scheduling by allocating time slices to processes based on their weight. The weight of the process is assigned by considering priority of each process. CFS scheduler ensures that processes with high priority get allocated more CPU time.

SAFETY

Linux implements security mechanisms to manage access to resources. For instance, uers permissions, SELinux and AppArmor facilitates access controls to protect resources from unauthorized actions or breaches. SELinux and AppArmor provides extra layer of security by defining access policies that restrict actions of processes and protect against unauthorized access to resources.

4. MANAGE MEMORY, PROCESSOR AND FILE IN LINUX OPERATING SYSTEM

MEMORY MANAGEMENT

Memory management in Linux Operating System Implies allocating computer memory, managing computer memory resources for running applications in the operating system. The virtual memory model of Linux operating system offers running multiple applications concurrently without interfering with other running processes. The objective of virtual memory is to map the memory addresses of programs to physical memory addresses. Virtual memory is responsible to allocate required memory to run applications.The following section addresses some of the concepts of Linux operating systems to manage memory of the devices.

VIRTUAL MEMORY PRIMER

Virtual memory primer a technique implemented in Linux operating system to allocate more memory than physical memory. Space in hard disk used as an additional extension to physical memory. Mainly, paging mechanism is used to develop virtual memory technique. In circumstances where running application requires more memory than available in memory, Linux kernel allocate more space by swapping the hard disk space. This method of managing memory prevents from occurring memory related crashes.

MEMORY PAGES

In the context of Linux memory management, memory pages is as essential part to maximize memory utilization. Memory page is the primary objective memory allocation. In memory pages, accessible physical memory is divided into pages with the relevant physical address. Nowadays, a page is fixed-size block (4KB) of contiguous memory.

Pages are then mapped into virtual addresses by allowing each and every process to allocate address space which is correspondent to physical address. Examples such as huge pages, zones, page cache, Nodes are examples of memory pages.

ANONYMOUS MEMORY

Anonymous memory is another type of dynamic memory allocation which is managed by the kernel at the runtime. This memory allocation is not associated with any specified device or file. Temporary data of process such as program stack and heap memory of processes are stored in memory.

Anonymous memory allocation makes management of memory more efficient and minimize the memory fragmentation issues. In addition, anonymous memory allocation is used to inter process communication while shared memory allows many processes to access same data.

OOM KILLER

OOM which stands for Out-of-Memory is a kernel feature available in Linux to recover memory from processes which causes interrupts to system's memory resources. OOM Killer is accountable for terminating processes which consumes a significant amount of memory in situations where system runs on minor memory space. In Linux systems processes which consumes significant memory spaces is identified by attributes such as process uses, age and priority. Operating system kernel then kills the identified process in order to maximize memory utilization.

COMPACTION

In the context of Linux memory management, **Compaction** is a kernel mechanism used to defragmentation of system memory. The main goal of compaction is to relocate the memory pages to create larger adjoining blocks of unused memory to improve system performance.

In the process of compaction, initially pages which are not in use are identified. Then identified memory pages are relocated between active memory pages to create larger space.

RECLAIM

In perspective of Linux memory management, **Reclaim** implies the process of releasing the unused memory by actively running programs or applications. System memory is allocated when the request made by process or application. Techniques such as slab reclamation, page reclamation and direct reclamation are provided by the Linux kernel.

Page reclamation attempts to release independent memory pages which are no longer in use while slab reclamation involves with releasing kernel memory for cache and buffer. Memory is directly reclaimed from running processes when the system is overloaded.

CMA (CONTGOUS MEMORY ALLOCATOR) DEBUGS INTERFACE

CMA is an interface to display and modify parameters and settings of **CMA**. Administrators and Developers have access to observe the allocation statics, view statistics of allocation and to calibrate allocation policies. Debugs interface provides a convenient method of troubleshooting and optimization of **CMA** usage in systems where contiguous memory allocation is an essential factor.

IDLE PAGE TRACKING **(IPT)**

Idle page tracking is another type of technique to identify memory pages which are not used by applications. These identified pages are allocated to other various purposes. The operating system attempts to scan memory periodically in order to identify idle pages. As we discussed earlier techniques such as compaction, swapping use these scanned information to increase the memory utilization. **IPT** is a vital component in virtual environments where memory overloading causes considerable number of issues.

KERNEL SAMEPAGE MERGING (KSM)

KSM is another type of memory utilizing feature available in Linux operating systems which allows multiple processes to share memory pages. Identical memory pages are identified and merges into one single page by the KSM. KSM is a vital feature in virtualized environments where multiple virtual machined operates on same physical server. In attempt to share identical memory pages minimize the memory required by each virtual machines to operates on a single server. **KSM** is an in-built feature which is available in various Linux distributions with customizations.

FILE MANAGEMENT

In the perspective of file management in Linux operating system implies organizing, controlling and manipulating files withing the Linux operating system. File management in Linux operating system consists of creating, listing, copying, moving, renaming and deleting of files. Open-source compatibility of Linux operating system offers users to manage files effectively. Generally, [13] Files in the Linux operating system can be categorized into three types such as regular files, directories and special files. Regular files, are the most commonly used files in Linux operating system which consists of data to used by various applications. Directories which acts as containers which consists of associated files to provide an hierarchical structure. Special files consists of system resources which only accessible to either hardware devices or system related information. They act as an intermediate between user and underlying system.

The following section explores different components use in Linux operating system to manage files efficiently.

HIERACHICAL STRUCTURE OF FILE SYSTEM

Linux follows an hierarchical structure of files for management of resources. The top level directory is commonly called "root" followed by other directories [13]. Each associated directory maintains the structure of the file system. In linux environments other associated directories are /bin, /home, /lib, /dev, /boot, /etc, /media etc.

FILE PERMISSION AND OWNERSHIP

Linux follows an access control to files and directories for different user types. These permissions are granted based on owner, group and user. The permissions include read, write and execution. Each file is associated with specific user and group. The command 'chmod' can be used to define limit access to resources [13].

FILE MANIPULATION

Linux consists with various different commands to perform manipulation on files and directories. Commands such as cp, mv, rm, rmdir, mkdir, touch are the most commonly used in Linux environments. In built text editors like nano, vim and emacs can be used to write to files. Following is the brief summary of each of these mentioned commands [13].

cp – To copy files

rm – to remove files

touch – To create files

mkdir – To create directories

rmdir – To remove directories

PROCESSOR MANAGEMENT IN LINUX OPERATING SYSTEM

In the perspective of processor management in Linux operating system implies the collaborating and utilization of the use of central processing unit of the device. Sheduling algorithms have been developed to maintain this task for efficient management of CPU.

The following section explains how Linux operating system manages the use of CPU by using different techniques.

SHEDUELER

For the maximized use of CPU Linux operates with **Complete fair scheduling (CSF)** Algorithm. Generally, this algorithm operates on weight-based processes. Processes with higher weight allocated more time to operate on CPU. In order to monitor the tasks which are based on priority based on the runtime, a red-black tree is being used.

Processes are assigned with a unique identifier which acts as priority level of the process. Negative values of priority level gets more allocated time on CPU while Positive values of priority allocated minor allocated time on CPU.

cgroups in Linux manage the limitation to resources of a group of processes to provide isolation and prioritized resource allocation. Administrators are given permission to manage users and groups and to define CPU management for each user and group.

MAC OPERATING SYSTEM

Mac operating system (MacOS) that was released by Apple and is used on all Apple devices. MacOS stands for Macintosh Operating System. It can be also considered as the pioneer of Graphical User Interface (GUI) operating system. With in the market of desktop and laptop computers, MacOS is second widely used desktop OS, after Microsoft Windows. [15]

Mac OS can offer functionality and services like Windows and Linux operating system. There are lot of features in macOS. Mainly,

1. Support many devices simultaneously.
2. Provide a stable, portable, reliable, safe, and well-behaved environment.
3. Manage memory, processor, file, etc.
4. The level of the security macOS provides.

Support many devices simultaneously

- The iPhone can wirelessly connect to the Mac as a web camera, allowing us to use the phone's high-quality cameras rather than the lower-resolution cameras that are frequently included in MacBooks. We may also use this function to capture a photo or scan a document and have it appeared on our Mac instantly. [16]

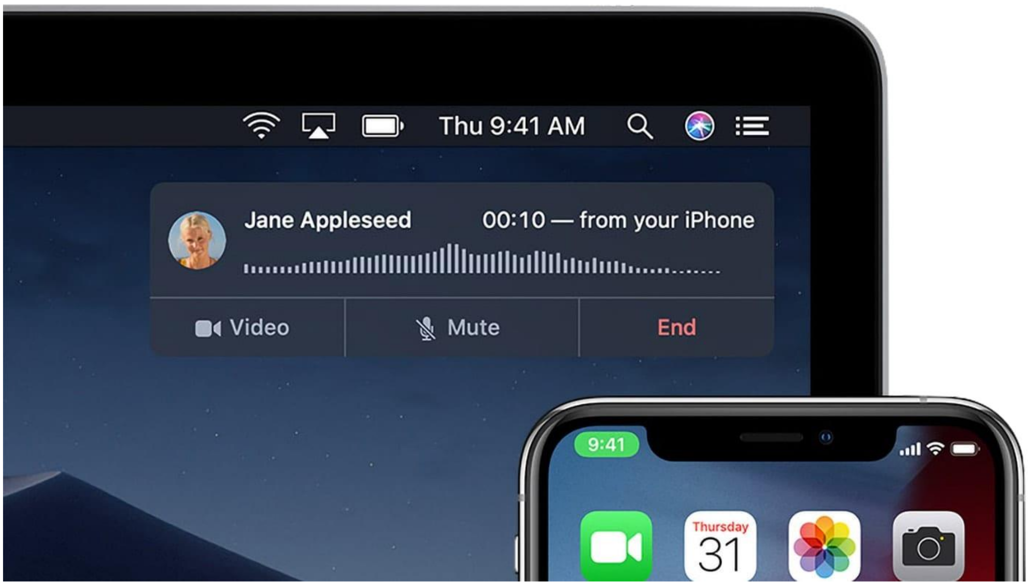
- All photos and files can be accessed from any device. [16]

- The user can copy a file on one device and paste it on another device. There is no need to use any additional functions. Everything is done in the same way as a single computer. [16]

- Allows a Mac keyboard and trackpad/mouse to operate a nearby iPad, or vice versa, if an iPad keyboard or mouse is used. And it allows any adjacent keyboard to control all devices. [16]

- We may utilize our iPad as a second screen for our Mac. By selecting the option to expand our screen, we may run one set of programs and browser tabs on our Mac while running an entirely separate app on our iPad. For example, view a video on the iPad while typing on the MacBook. We may also drag and drop papers and other things from one screen to another screen. [16]

- If we receive a call on our iPhone, we can answer the call from our Mac. [16]



- The computer can be unlocked using the Apple Watch. Entering a password is not required. [16]

U.S.
Thursday, September 21
10:09
Joe Lipscomb
Unlocking with Apple Watch...
Joe's MacBook Pro Unlocked by this Apple Watch

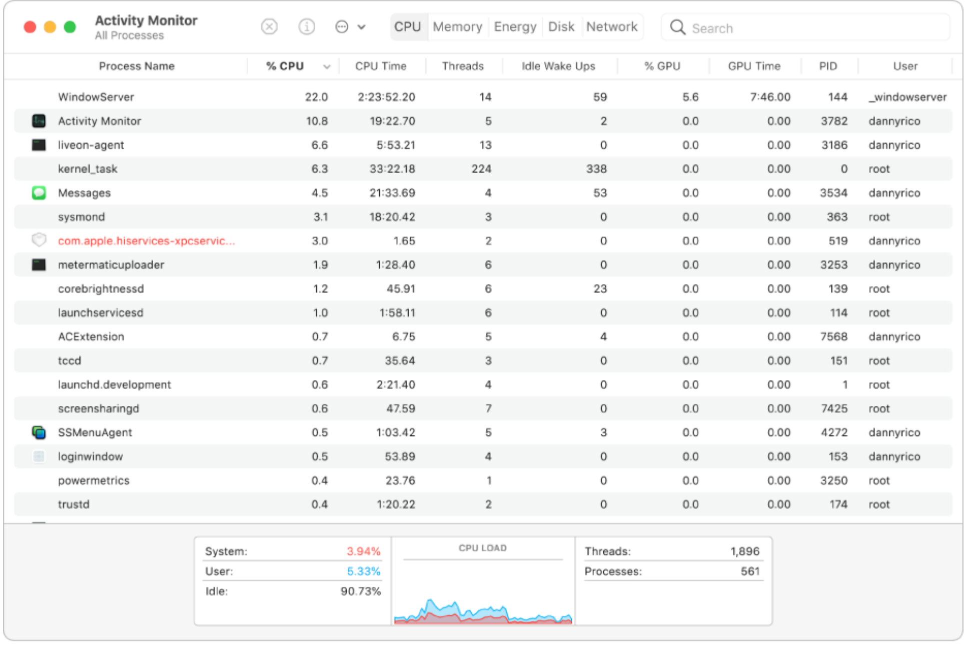
PROVIDE A STABLE, PORTABLE, RELIABLE, SAFE, AND WELL-BEHAVED ENVIRONMENT

Creating a stable, portable, reliable, safe, and well-behaved environment in macOS is essential for ensuring a smooth and secure computing experience. Apple's macOS operating system is well-known for its user-friendly interface and outstanding performance, by thankful to these features.

Stability

- Regular software updates keep macOS and other applications up to date with the latest updates and fixes. Apple releases updates to fix bugs, security vulnerabilities and improve stability. [17]

- System monitoring feature uses activity monitor to monitor system resource usages, identify resource hungry processes and address any performance issues. [17]



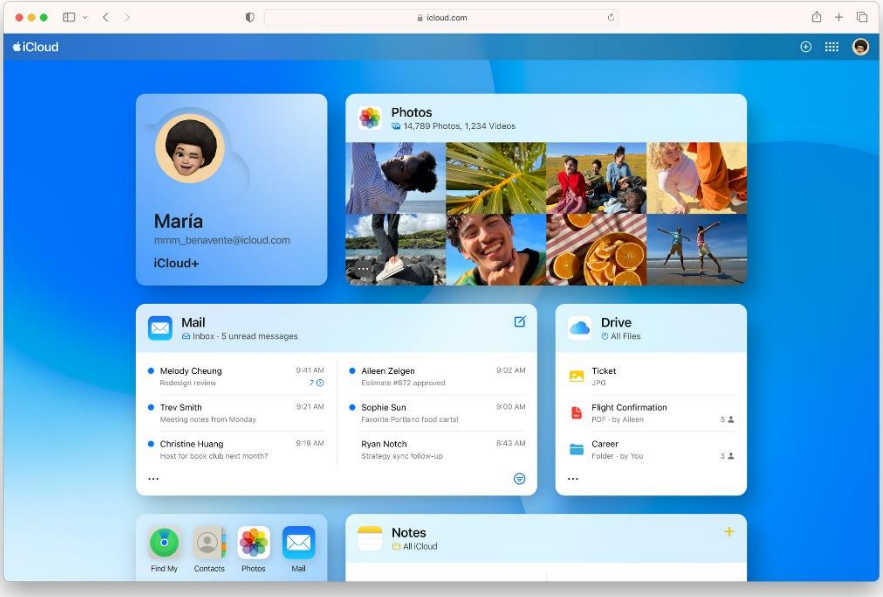
Process Name	% CPU	CPU Time	Threads	Idle Wake Ups	% GPU	GPU Time	PID	User
WindowServer	22.0	2:23:52.20	14	59	5.6	7:46.00	144	_windowserver
Activity Monitor	10.8	19:22.70	5	2	0.0	0.00	3782	dannyrico
liveon-agent	6.6	5:53.21	13	0	0.0	0.00	3186	dannyrico
kernel_task	6.3	33:22.18	224	338	0.0	0.00	0	root
Messages	4.5	21:33.69	4	53	0.0	0.00	3534	dannyrico
sysmond	3.1	18:20.42	3	0	0.0	0.00	363	root
com.apple.hiservices-xpcservic...	3.0	1.65	2	0	0.0	0.00	519	dannyrico
metermaticuploader	1.9	1:28.40	6	0	0.0	0.00	3253	dannyrico
corebrightnessd	1.2	45.91	6	23	0.0	0.00	139	root
launchservicesd	1.0	1:58.11	6	0	0.0	0.00	114	root
ACExtension	0.7	6.75	5	4	0.0	0.00	7568	dannyrico
tccd	0.7	35.64	3	0	0.0	0.00	151	root
launchd.development	0.6	2:21.40	4	0	0.0	0.00	1	root
screensharingd	0.6	47.59	7	0	0.0	0.00	7425	root
SSMenuAgent	0.5	1:03.42	5	3	0.0	0.00	4272	dannyrico
loginwindow	0.5	53.89	4	0	0.0	0.00	153	dannyrico
powermetrics	0.4	23.76	1	0	0.0	0.00	3250	root
trustd	0.4	1:20.22	2	0	0.0	0.00	174	root

System:	3.94%
User:	5.33%
Idle:	90.73%

Threads:	1,896
Processes:	561

Portability

- Use cloud services like iCloud, Dropbox, or Google Drive to store and sync important files and make them accessible from any device with an internet connection. [17]



Melody Cheung 9:41 AM
Redesign review

Trev Smith 9:21 AM
Meeting notes from Monday

Christine Huang 9:19 AM
Host for book club next month?

Aileen Zeigen 9:02 AM
Estimate #872 approved

Sophie Sun 9:00 AM
Favorite Portland food carts!

Ryan Notch 8:43 AM
Strategy sync follow-up

Ticket
JPG

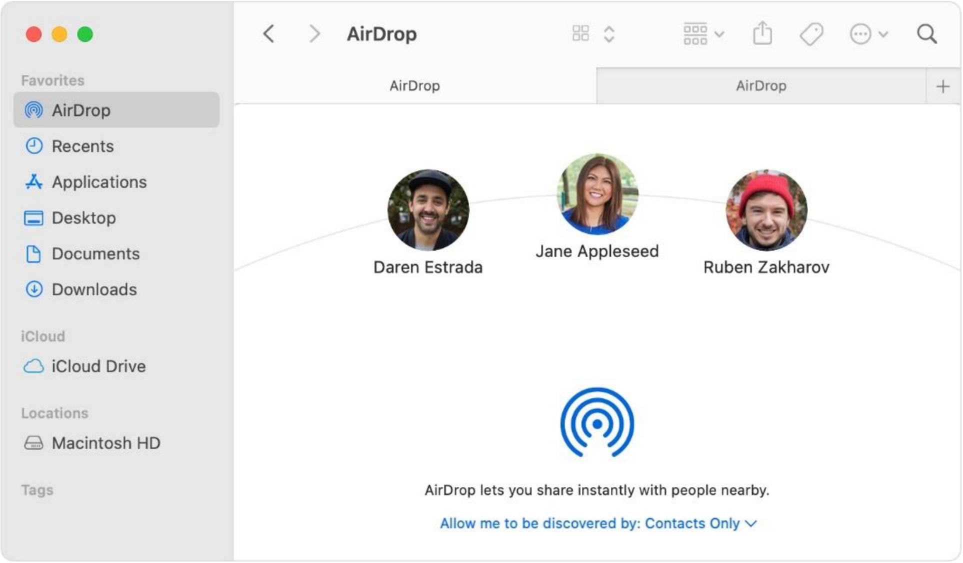
Flight Confirmation
PDF · by Aileen

Career
Folder · by You

- iCloud is Apple’s cloud storage service that is integrated into macOS. It allows users to store files, photos, and other data in the cloud by making it easy to access them from any Apple device. iCloud also syncs our data across devices, so we can pick up where we left off on our iPhone, iPad, or Mac. [17]

- If we have any USB drive or any external drive then, we may use time machines and other backup solutions automatically to ensure that our data is secure and easy to transfer to the new mac if needed. [17]

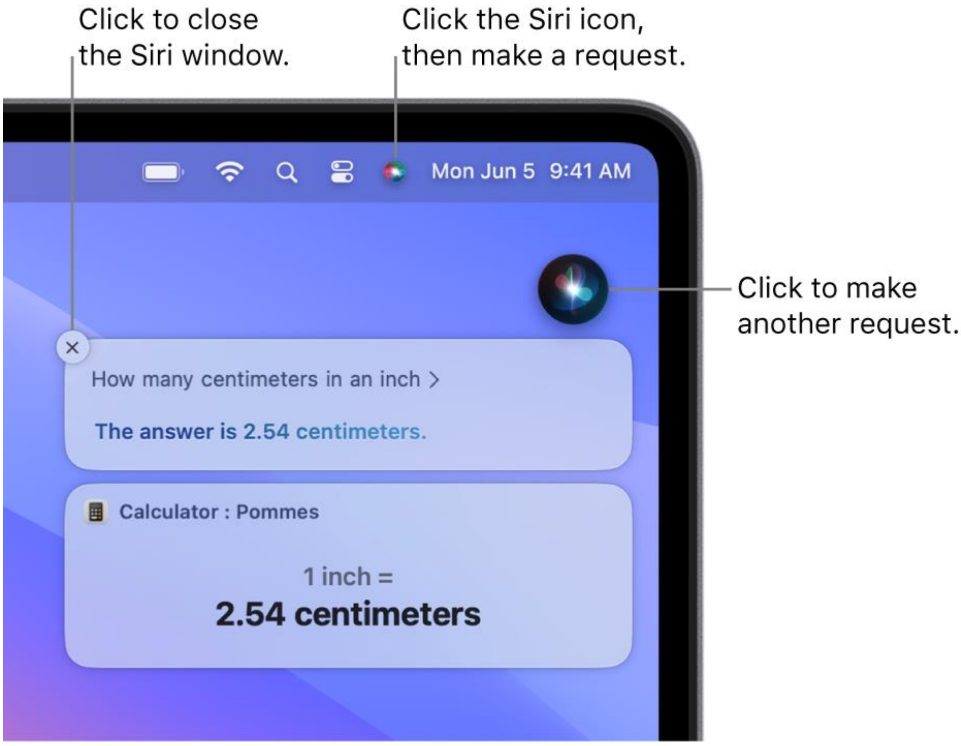
- Airdrop is a feature that allows us to share files wirelessly between Apple devices. With Airdrop, we can quickly and easily share files with friends and others without the need for cables or external storage devices. [17]



AirDrop lets you share instantly with people nearby.

Allow me to be discovered by: Contacts Only

- Siri is Apple’s virtual assistant that is built into macOS. It allows us to perform tasks hands-free using their voice. This can be used to set reminders, send messages, make phone calls, and more. And help us to find files on our computer, open apps, and adjust settings. [17]



Click to close the Siri window.

Click the Siri icon, then make a request.

Click to make another request.

Mon Jun 5 9:41 AM

How many centimeters in an inch >

The answer is 2.54 centimeters.

Calculator : Pommes

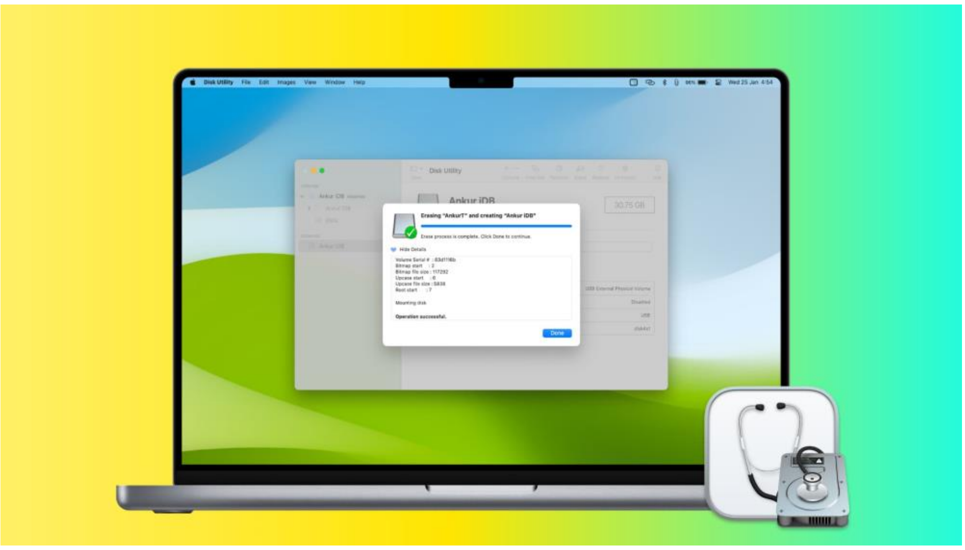
1 inch =

2.54 centimeters

Reliability

- Choose reliable hardware and peripherals. Apple's Mac hardware is well-known for its endurance and quality, which contributes to a more stable computer environment. [17]

- Test and troubleshoot hardware components like RAM, hard drives and external devices on a regular basis to identify and replace all failures. [17]



Erasing "AnkurT" and creating "Ankur iDB"

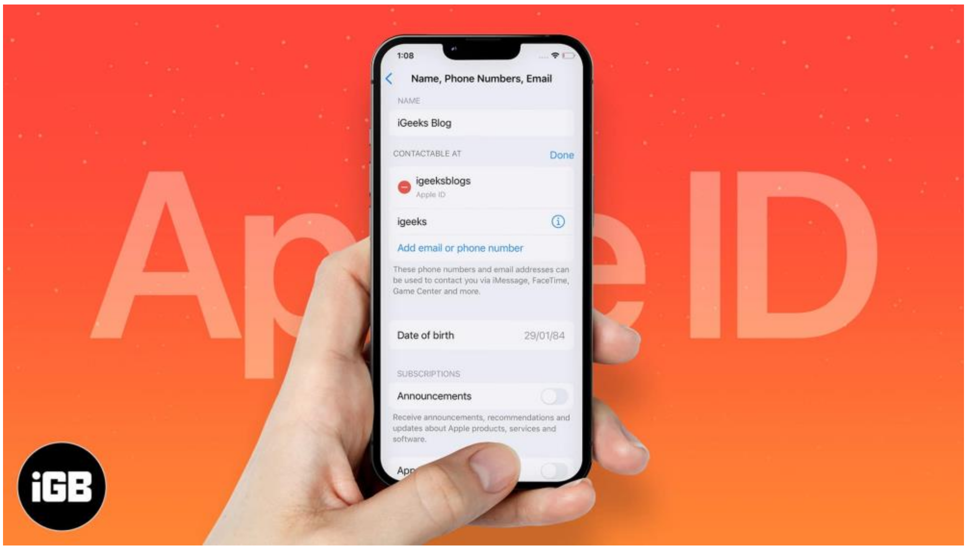
Erase process is complete. Click Done to continue.

```
Volume Serial # : 83d1116b
Bitmap start    : 2
Bitmap file size : 117292
Upcase start    : 6
Upcase file size : 5838
Root start      : 7

Mounting disk

Operation successful.
```

- Our Apple ID is the account that we use to access all Apple services like apple ID security, avoid phishing and family sharing by making all our devices work together seamlessly. [17]



iGeeks Blog

igeeksblogs
Apple ID

igeeks

These phone numbers and email addresses can be used to contact you via iMessage, FaceTime, Game Center and more.

Date of birth 29/01/84

Announcements

Receive announcements, recommendations and updates about Apple products, services and software.

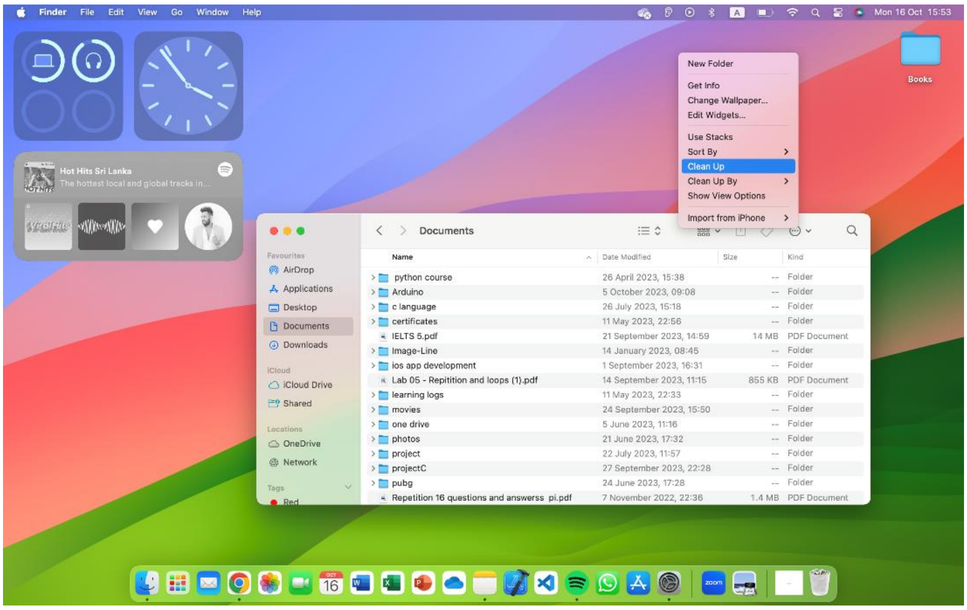
Safety

1. Install reputable antivirus and anti-malware software to protect against threats. MacOS has built-in security features like Gatekeeper, XProtect, and File Vault for enhanced protection. [17]
    1. Prevent devices from malware launching or executions. (app store or gatekeeper combine with Notarization)
    2. Block malware from running on systems. (gatekeeper, notarization and X protector)
    3. Remediate Malware that has been executed. (X protector)

2. Configure macOS's built-in firewall and network settings to protect against potential risks and prevent unauthorized access as well as to prevent the Mac from responding to ICMP (Internet Control Message Protocol) probing and portscan requests. [17]

Well behaved environment

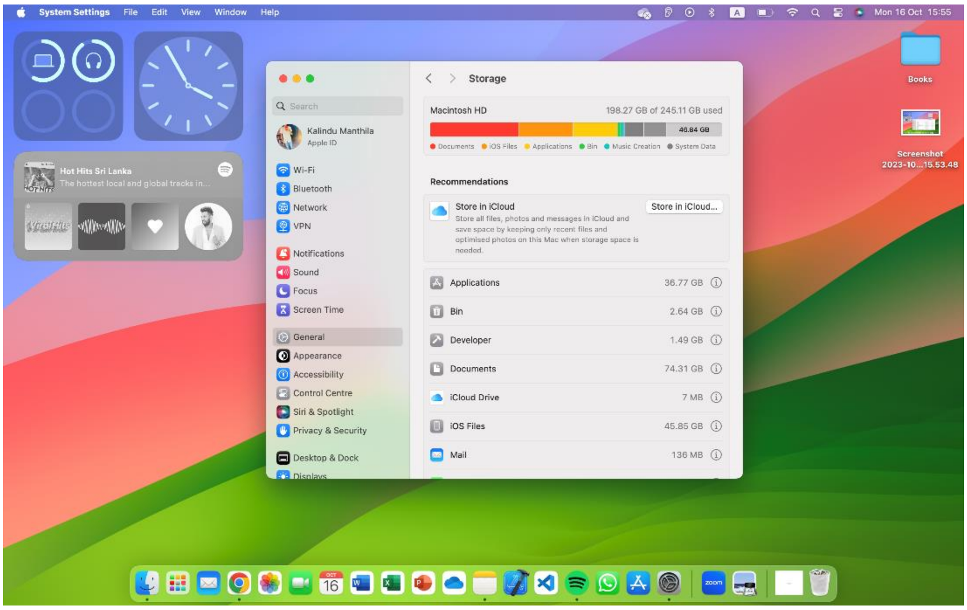
- We can use clean up function for Clean and organize our desktop, documents, and downloads folders on a regular basis. This increases not just the system's performance but also user productivity. [17]



Documents

Name	Date Modified	Size	Kind
python course	26 April 2023, 15:38	--	Folder
Arduino	5 October 2023, 09:08	--	Folder
c language	26 July 2023, 15:18	--	Folder
certificates	11 May 2023, 22:56	--	Folder
IELTS 5.pdf	21 September 2023, 14:59	14 MB	PDF Document
Image-Line	14 January 2023, 08:45	--	Folder
ios app development	1 September 2023, 16:31	--	Folder
Lab 05 - Repitition and loops (1).pdf	14 September 2023, 11:15	855 KB	PDF Document
learning logs	11 May 2023, 22:33	--	Folder
movies	24 September 2023, 15:50	--	Folder
one drive	5 June 2023, 11:16	--	Folder
photos	21 June 2023, 17:32	--	Folder
project	22 July 2023, 11:57	--	Folder
projectC	27 September 2023, 22:28	--	Folder
pubg	24 June 2023, 17:28	--	Folder
Repetition 16 questions and answerss pi.pdf	7 November 2022, 22:36	1.4 MB	PDF Document

- Remove any unwanted or old programs to clean the system. Make sure that all apps are appropriately closed when not in use to free up system resources. [17]



Storage

Macintosh HD 198.27 GB of 245.11 GB used

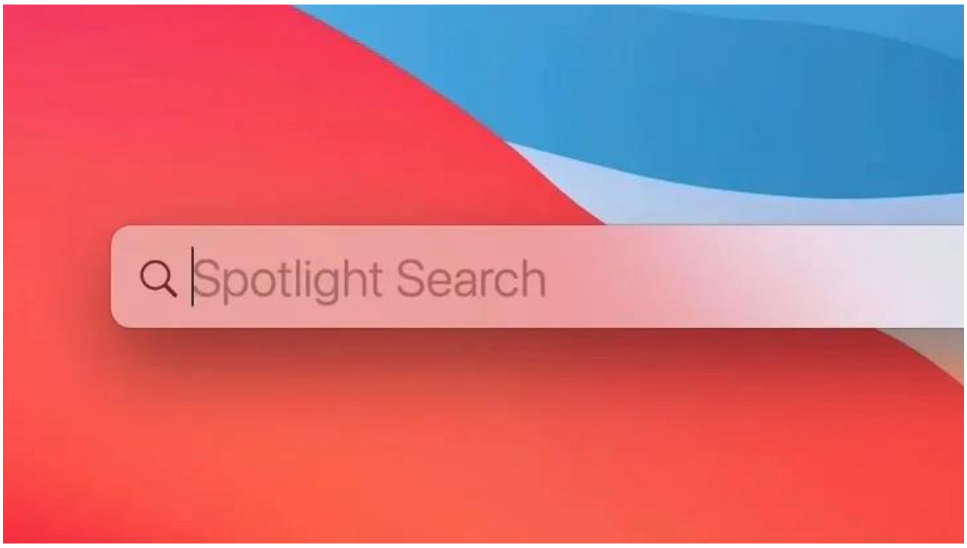
Recommendations

Store in iCloud

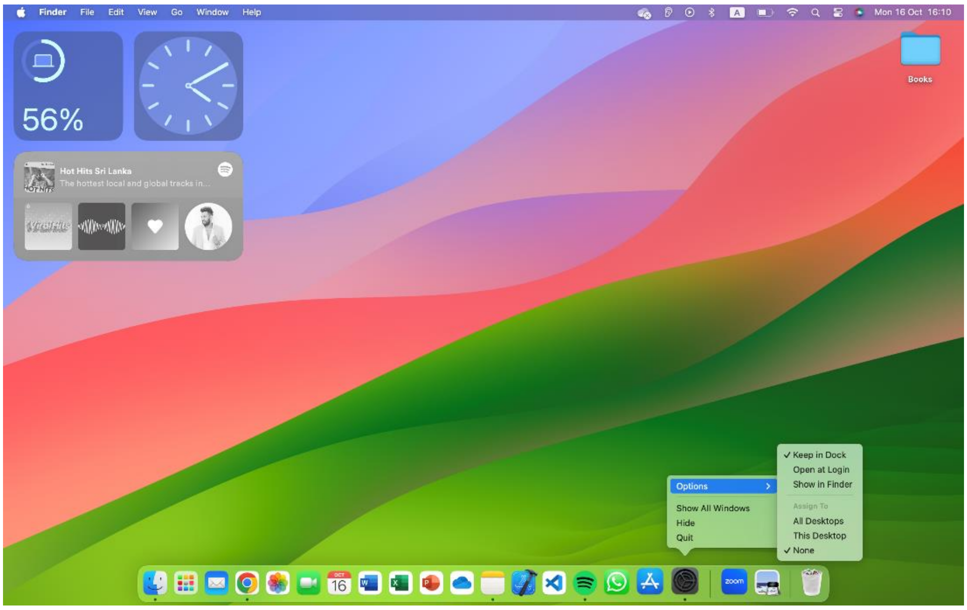
Store all files, photos and messages in iCloud and save space by keeping only recent files and optimised photos on this Mac when storage space is needed.

Applications	36.77 GB
Bin	2.64 GB
Developer	1.49 GB
Documents	74.31 GB
iCloud Drive	7 MB
iOS Files	45.85 GB
Mail	136 MB

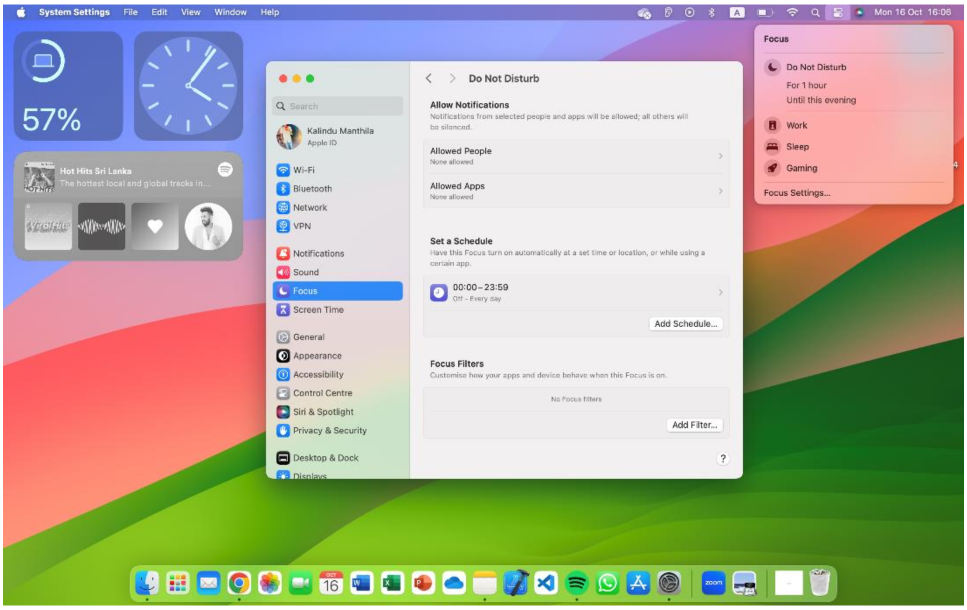
- Spotlight Search is one of the most useful features for all macOS users as it makes us efficient at using our new computer. By using the feature, we can find any app or file stored on our computer in a second, while saving our time and effort [17].



- The Dock is another special feature, and it is the location on our desktop where we may keep the apps, files, and folders that we use the most. We can customize the Dock by adding or removing items, adjusting its size, or removing it from the desktop. [17]



- ‘Focus Mode’ on Mac filters notifications based on our current task, helping us to focus on what is most important. We can select from preset Focus modes like **Do Not Disturb**, **Work**, **Sleep**, and **Gaming**, or customize our own based on our unique requirements. [17]



Do Not Disturb

Allow Notifications

Notifications from selected people and apps will be allowed; all others will be silenced.

Allowed People
None allowed

Allowed Apps
None allowed

Set a Schedule

Have this Focus turn on automatically at a set time or location, or while using a certain app.

00:00 – 23:59
Off - Every day

Add Schedule...

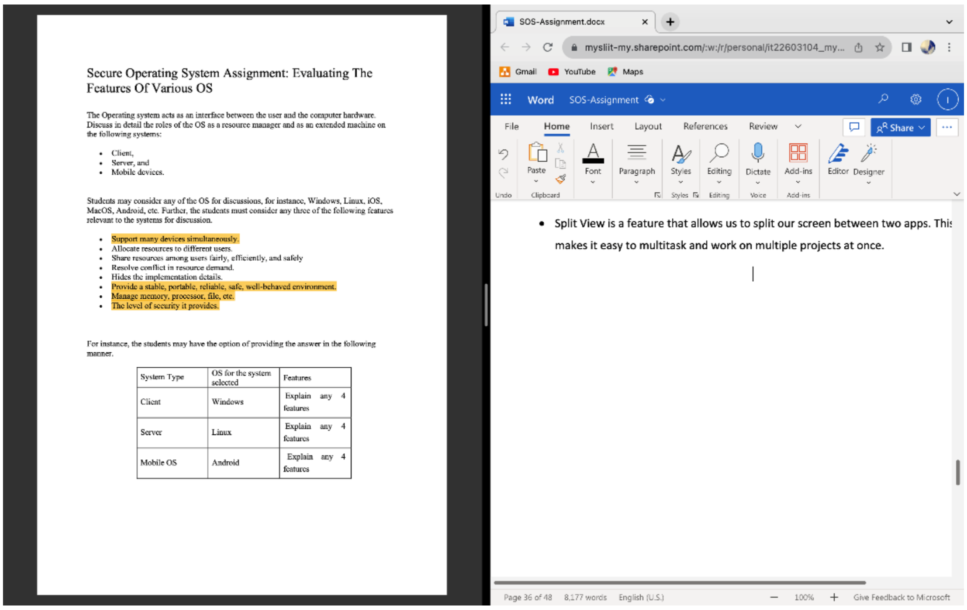
Focus Filters

Customise how your apps and device behave when this Focus is on.

No Focus filters

Add Filter...

- Split View is a feature that allows us to divide our screen into two sections between two apps. This makes it easy to do multiple things and work on multiple projects at same time. [17]



Secure Operating System Assignment: Evaluating The Features Of Various OS

The Operating system acts as an interface between the user and the computer hardware. Discuss in detail the roles of the OS as a resource manager and as an extended machine on the following systems:

- Client,
- Server, and
- Mobile devices.

Students may consider any of the OS for discussions, for instance, Windows, Linux, iOS, MacOS, Android, etc. Further, the students must consider any three of the following features relevant to the systems for discussion.

- Support many devices simultaneously.
- Allocate resources to different users.
- Share resources among users fairly, efficiently, and safely
- Resolve conflict in resource demand.
- Hides the implementation details.
- Provide a stable, portable, reliable, safe, well-behaved environment.
- Manage memory, processor, file, etc.
- The level of security it provides.

For instance, the students may have the option of providing the answer in the following manner.

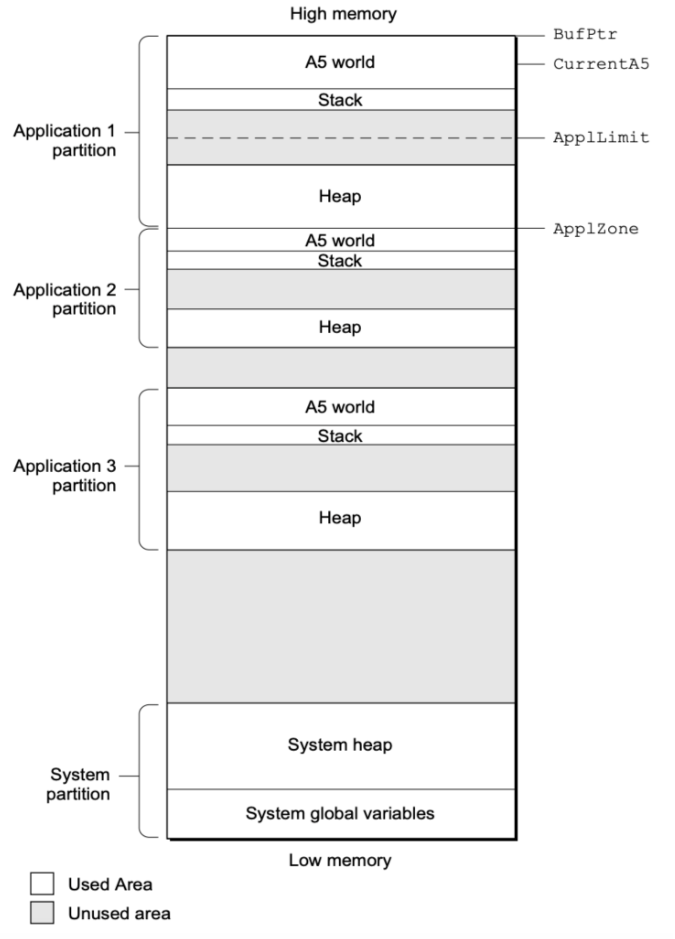
System Type	OS for the system selected	Features
Client	Windows	Explain any 4 features
Server	Linux	Explain any 4 features
Mobile OS	Android	Explain any 4 features

- Split View is a feature that allows us to split our screen between two apps. This makes it easy to multitask and work on multiple projects at once.

Manage memory, and process

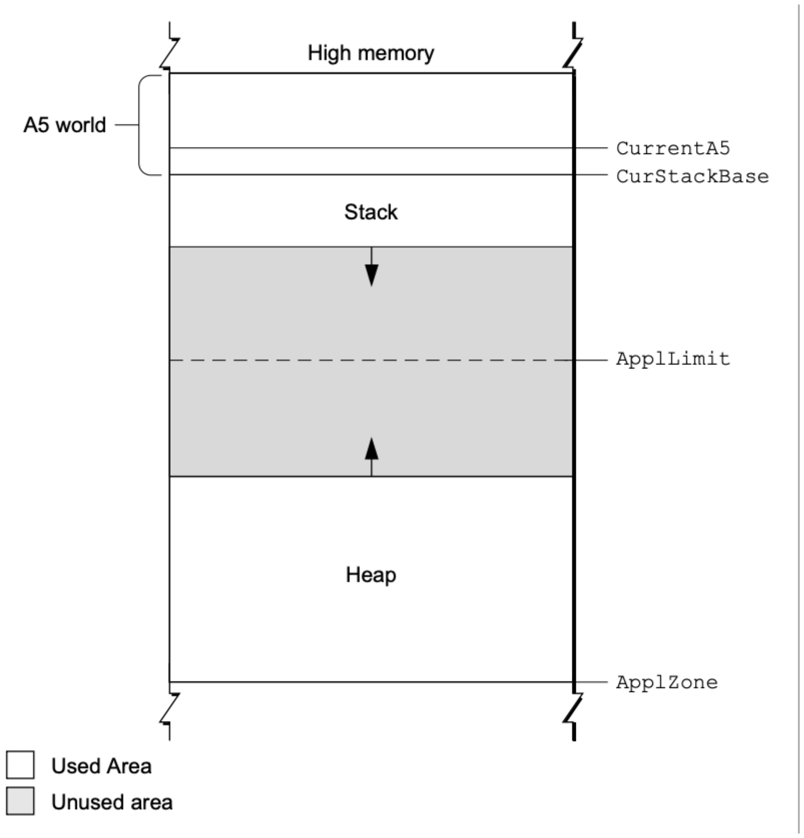
Memory and process management play an important role in macOS for the best system performance and user satisfaction. MacOS has tools and strategies for optimizing resource usage and providing a consistent user experience. Here is some info on how to manage each of these criteria effectively.

Memory Management

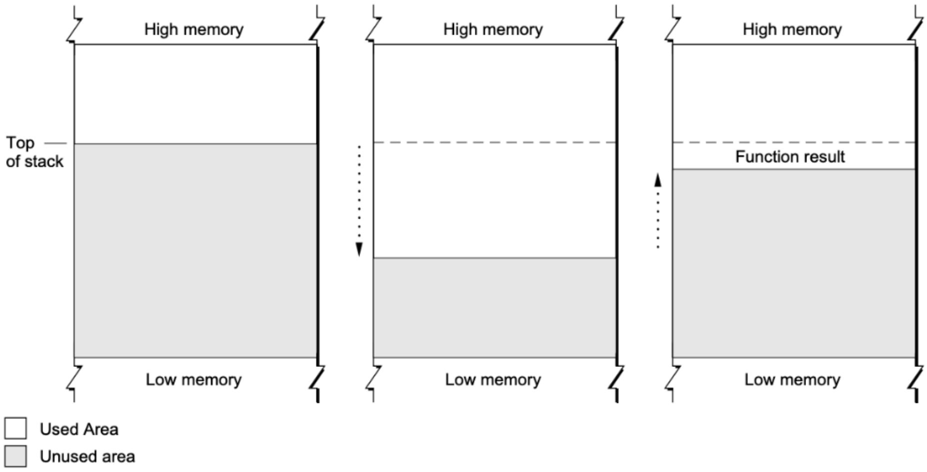


- Use the built-in Activity Monitor app to monitor memory usage and identify memory-hungry programmes. Sort processes by memory utilization to identify and stop programmes or processes that utilize an excessive amount of memory. [18]

- When we begin our program, the Operating System allocates a memory segment called the application partition for it. That partition comprises needed application code segments as well as other data related to the program. [18]

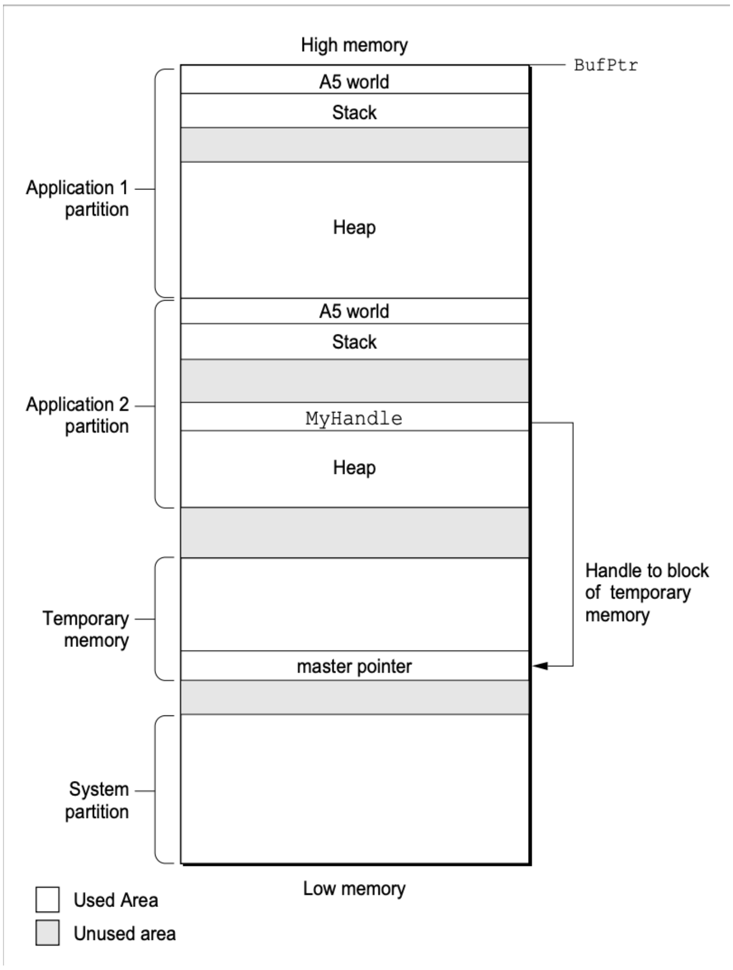


- A stack frame includes the parameters, local variables, and return address of the procedure. The diagram shows how the stack expands and contracts during a function call. If we use a high-level development language like Pascal, dynamic memory allocation on the stack is generally handled automatically. For each function or procedure call, the compiler generates the code that builds and deletes stack frames. [18]



- Each program in the Macintosh multitasking environment is limited to a particular memory partition (whose size is determined by information in that application's 'SIZE' resource). The size of our application's partition restricts the size of our application heap, and hence the sizes of the buffers and other data structures that we use. In general, we determined an application partition size that is large enough to accommodate all the buffers, resources, and other data that our program is expected to require while executing. [18]

  If we require more memory than is currently available in our application heap, we can request that the Operating System allow us to access any available memory that has not yet been assigned to another program. This memory, known as temporary memory, is allocated from the unused RAM that is accessible. [18]



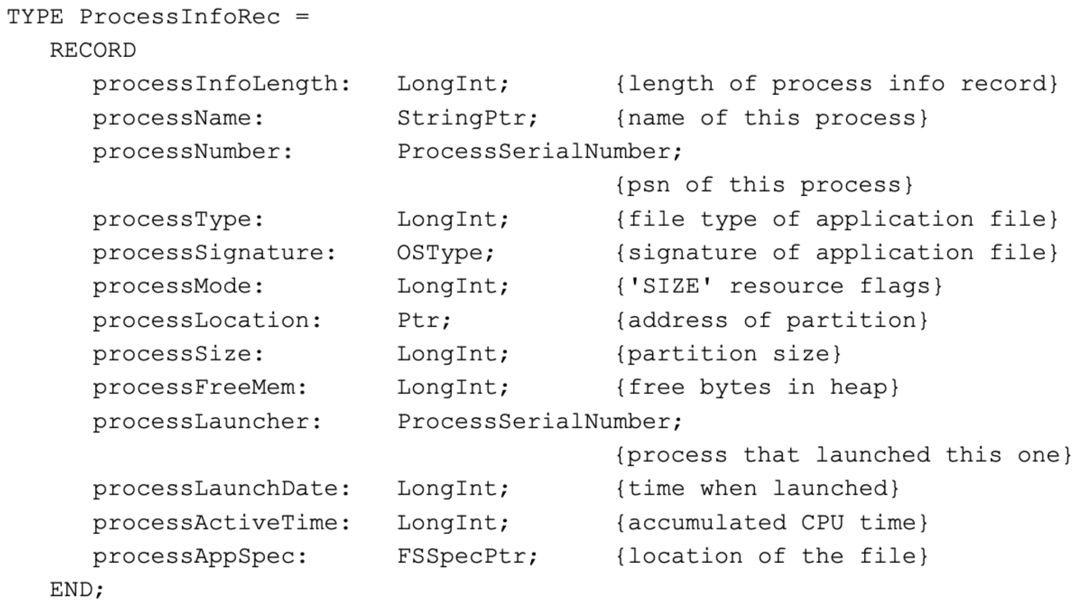
Process Management

- The Process Manager is a component of the Macintosh operating system that allows for cooperative multitasking. The Process Manager supervises application scheduling and execution as well as access to shared resources. [19]

- To find the process serial number of a process, we can use the `GetNextProcess`, `GetFrontProcess`, or `GetCurrentProcess` functions. The `GetCurrentProcess` function returns the process serial number of the currently running process, also known as the current process. This is the process whose A5 world is presently valid, it might be in the forefront or background. The `GetFrontProcess` function returns the foreground process's process serial number. If our process is operating in the background, for example, we may use `GetFrontProcess` to find which process is in the foreground. [19]

- If we want to get information about any process, including our own, we may use the *GetProcessInformation* function. For example, we may identify the application's name as it appears in the Application menu, the type and signature of the application, the number of bytes in the application's operating system partition, the total number of free bytes in the application heap, and the application that started the application for a given process. [19]

- The *GetProcessInformation* function returns information in the `ProcessInfoRec` data type as a process information record. [19]

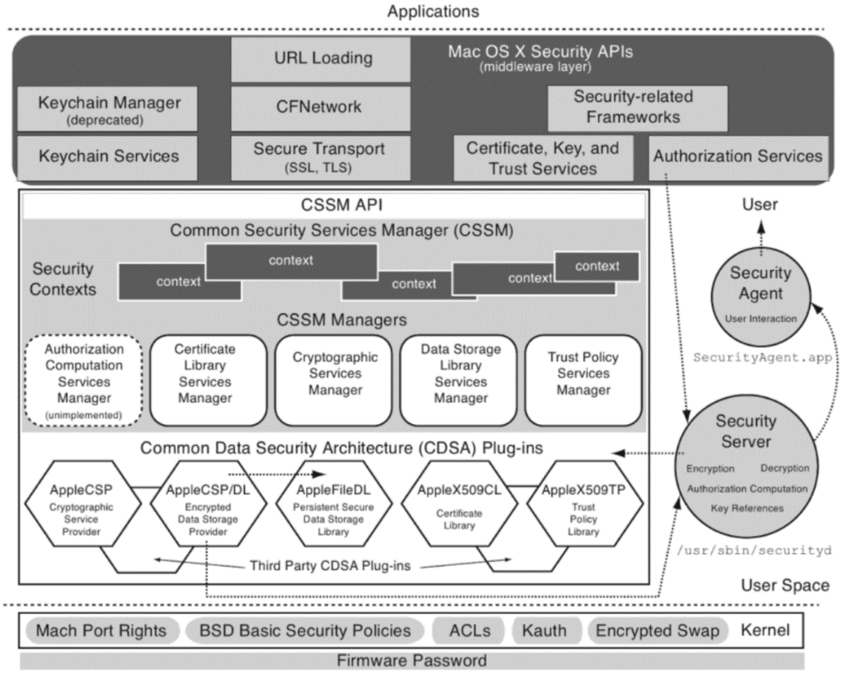


```
TYPE ProcessInfoRec =
   RECORD
      processInfoLength:   LongInt;       {length of process info record}
      processName:         StringPtr;     {name of this process}
      processNumber:       ProcessSerialNumber;
                                          {psn of this process}
      processType:         LongInt;       {file type of application file}
      processSignature:    OSType;        {signature of application file}
      processMode:         LongInt;       {'SIZE' resource flags}
      processLocation:     Ptr;           {address of partition}
      processSize:         LongInt;       {partition size}
      processFreeMem:      LongInt;       {free bytes in heap}
      processLauncher:     ProcessSerialNumber;
                                          {process that launched this one}
      processLaunchDate:   LongInt;       {time when launched}
      processActiveTime:   LongInt;       {accumulated CPU time}
      processAppSpec:      FSSpecPtr;     {location of the file}
   END;
```

The level of the security macOS provides

MacOS is developed with advanced, cutting-edge technologies that combine to keep our Mac and built-in programmes more private and secure. The macOS security architecture is divided into three distinct tiers. The Berkeley Software Distribution (BSD) and Mach are found at the bottom of the security stack. BSD is an open-source standard that oversees the basic file system and network functions, as well as user and group access control. [20]

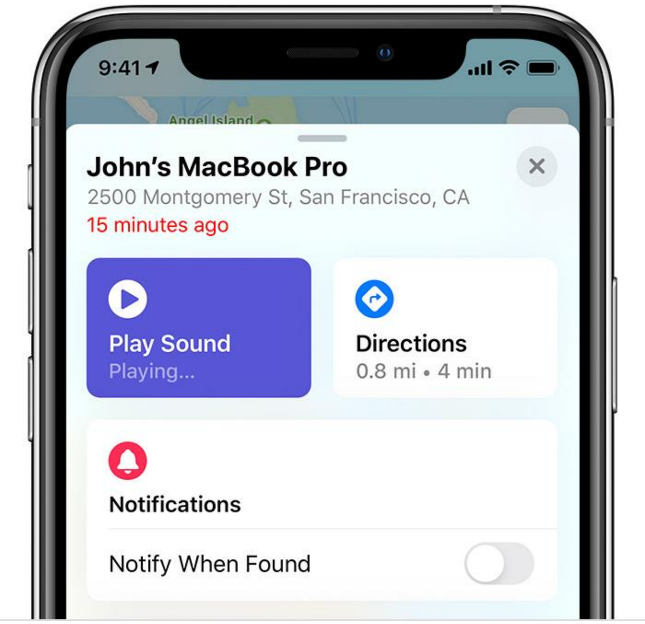
Macs are usually perceived as more secure than PCs, no internet-connected device is vulnerable to mobile device privacy and security issues. Macs have generally been subjected to fewer assaults, in part because they are less popular than Windows machines, and hence cybercriminals do not target them. [20]



Hardware security

- The Apple M1 chip, which includes a Secure Enclave, offers the same robust security features as the iPhone to the Mac, securing our login password, automatically encrypting our data, and enabling file-level encryption to keep us secure. And much as iOS has secured iPhone for years, the Apple M1 chip keeps macOS safe while it's operating. [21]

- The Find My app can help us find a lost Mac even if it's offline or asleep by giving out Bluetooth signals that neighboring Apple devices can detect. These devices then send the observed position of our Mac to iCloud, allowing us to find it. It's fully anonymous and encrypted end-to-end, so no one knows the name of any reporting device or the location of our Mac, not even Apple. And it all happens in the background, utilizing small pieces of data that ride on top of existing network traffic. So, we don't have to worry about our battery life, data use, or privacy being affected. [21]



9:41

Angel Island

John's MacBook Pro

2500 Montgomery St, San Francisco, CA

15 minutes ago

Play Sound

Playing...

Directions

0.8 mi • 4 min

Notifications

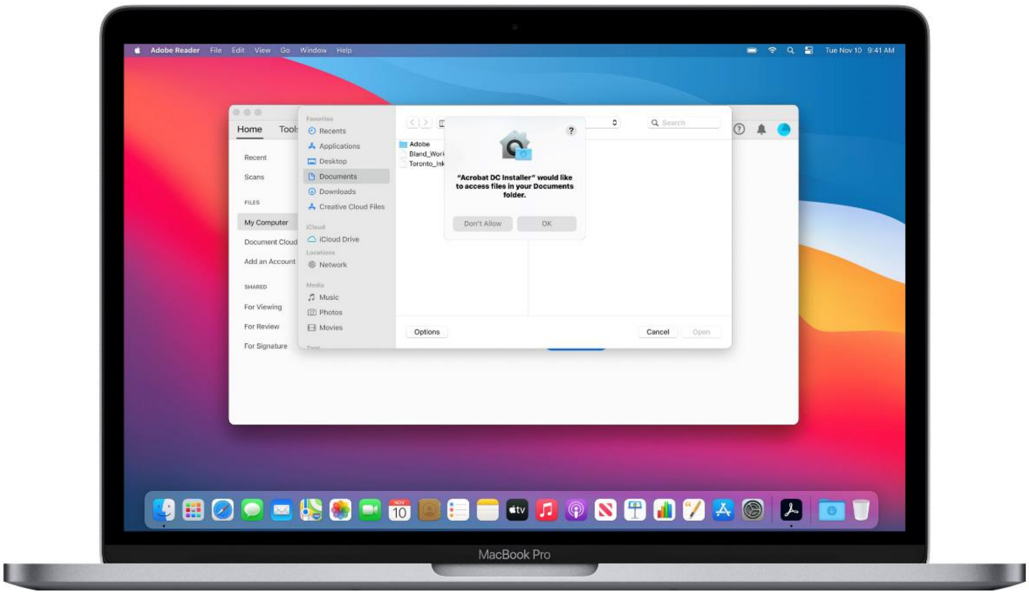
Notify When Found

- Activation Lock is supported by all Mac systems manufactured on the Apple M1 chip or with the Apple T2 Security Chip, just like our iPhone or iPad. So, if our Mac is ever misplaced or lost, we are the only one who can wipe and restart it. [21]

System security

- System security is meant to maximize the security of Apple devices' operating systems without compromising usability by utilizing the unique properties of Apple technology. The starting process, software upgrades, and the continuous functionality of the operating system all fall within the scope of system security. [21]

- System security is responsible for managing access to system resources in Apple devices to preserve usability, based on the specific abilities of Apple hardware. System security includes the boot-up process, software updates, and the safeguarding of computer system resources such as the CPU, RAM, disc, software programmes, and data. [21]



"Acrobat DC Installer" would like to access files in your Documents folder.

- The secure boot chain, system security, and app security features all play a role in ensuring that only trusted programmes and apps are running on a device. Apple products provide additional encryption mechanisms to protect user data even if other aspects of the security architecture are broken (for example, if a device is lost or running untrusted malware). All these capabilities assist both users and IT administrators by safeguarding personal and corporate data and enabling rapid and comprehensive remote wipes in the event of device theft or loss. [21]

ANDROID MOBILE OPERATING SYSTEM

Android is an operating system in mobile. It is a open source software. It was founded in Palo Alta in California. In 2003 Andy Rubin explained android project as a “Great potential to develop smart mobile devices that are more aware of their owner's location and preferences". He had trouble attracting early investors, and Android faced eviction from his office space. Android interface based on direct manipulation. We can enter input using touch. And we can use the keyboard for that. Like Bluetooth keyboard and virtual keyboard. Android devices boot to the home screen. That most famous apps are widgets, weather forecast and new ticker.

Third party apps are available in the google play store. We can download and install those apps in our android operating system. The top of the screen shows the status bar, it includes a connectivity of WIFI and flashlight, brightness level of the display. As well as it is included settings. Notifications show the status bar. Every apps are listed in the app list. We can show the recent app in our device. Recent list depending on and overlapping the android version. The app list accessed using gesture or button. It is depending on the android version. This operating system has a search engine. Example chrome. Android included mobile has a rechargeable battery. Software divided in to two categories. These are system software and application software. However, system software also installed by mobile manufacturing company. Application software content in play store, users can download and install it. Generally, we can add new extensional storage for android device (SD cards, memory chips). Mobile phones can be developed using settings. It has many hardware components in android mobile. Camera, RAM, pressure sensors and magnetometers etc. Generally, X86, X86-64 architecture used in latest version of the android. Android is a open source project. It does not include the play store. However, many original equipment manufacturers (OEMs) customize the source code to run on their hardware.

Android smartphones have a ability find the location. Some applications are used for it. As well as report the location of Wi-Fi access point. In 2018, Norwegian security section promotion has unearthed a serious Android security hole which can be exploited to steal login credentials, access and track location. Which could be found in all android versions. The vulnerability came by exploiting a bug in the multitasking system. Malicious apps overlay legitimate apps with fake login screens where users don't know when handing over security credentials. Users can be tricked into granting additional permissions to malicious applications.

THE LEVEL OF SECURITY PROVIDES

The Android operating system offers a multi-layered security architecture designed to protect user data and maintain the integrity of the platform. Android uses the Linux kernel at its core, which uses various security mechanisms such as process isolation and user-based permissions to ensure separation of application processes and prevention of unauthorized access to system resources. Additionally, Android includes strong cryptographic tools such as full disk encryption and secure boot to protect data at rest and on device startup. Furthermore, Android Security Mode enforces mandatory access control policies, enabling fine-grained control over app permissions and limiting the ability of malicious apps to compromise user data.

On top of these basic security features, Android provides a range of user-centric security. Features like Google Play Protect, which scans apps for potential threats, and the continuous release of security updates by Google and device manufacturers, help mitigate security vulnerabilities and protect against malware. Android also encourages developers to adopt secure coding practices and grants runtime permissions to grant apps access to sensitive resources on a case-by-case basis, giving users more control over their data. Android's security is strong, and it is imperative for users to be vigilant, keep their devices up-to-date, and install apps only from trusted sources to maintain a high level of security on their Android devices. Using the below security features on android mobile.

- Android platforms get the advantage of Linux-based protection.
- App signing allows developers to identify the author of the app.
- Android uses the concept of the user authentication gated cryptographic keys that key storage.
- Some devices have a fingerprint.
- Device is encrypted messages and decrypts automatically.
- Import and export asymmetric keys with appropriate padding mode.
- Verified boot strives to ensure all executed codes comes from a trusted source.

HIDE IMPLEMENTATION DETAILS

Android OS's ability to abstract and hide implementation details is a fundamental pillar of its design. By providing a well-defined application programming interface (API) that includes complex underlying processes, Android allows developers to focus on creating intuitive and user-friendly applications without having to delve into the complexities of hardware and low-level software interactions. This abstraction shields developers from the complexities of different device architectures, hardware drivers, and system-level operations, promoting a more streamlined and efficient development process. Ultimately, this feature empowers developers to deliver high-quality apps that work seamlessly across a wide range of Android devices for a diverse user base without the need for extensive, device-specific coding.

MANAGE MEMORY, PROCESSOR, FILE

Memory management plays a crucial role in Android. The OS uses a combination of techniques, including garbage collection, to reclaim memory that is no longer in use, which helps prevent application crashes due to excessive memory consumption. Android uses a managed memory model, which means that the OS takes care of allocating and distributing memory to applications. To further improve memory management, Android uses the Dalvik Virtual Machine (DVM) or Android Runtime (ART) concept, which automatically optimizes memory usage by converting bytecode to native code and managing memory allocation for applications. This process ensures that applications have access to the memory they need while preventing resource hogging.

Manages the Android processor efficiently to deliver a responsive user experience. The OS employs a task scheduler to allocate processor time to various applications and processes based on priority levels. This approach prevents any single application from monopolizing system resources and ensures that background tasks do not adversely affect the foreground experience. Additionally, Android supports multi-core processors, allowing for parallel processing and improved performance. Using application programming interfaces (APIs), developers can optimize their applications to run efficiently on different processors and CPU architectures, ensuring that the OS makes the most of available hardware resources.

Android provides a robust file management system that allows apps to store, access, and share data. Android's file system includes private storage for each app, where data is sandboxed and protected from other apps, ensuring user data privacy. It also supports shared storage areas and external storage for multiple applications or files that the user needs to access. The Android operating system manages file permissions, ensuring that apps only have access to the files and directories they are allowed to use. Furthermore, Android offers a content delivery framework that enables apps to securely share data with other apps, promoting a seamless user experience and facilitating data exchange between apps while maintaining data security and user consent.

Android OS excels at managing memory, processor resources and files to deliver a smooth and responsive user experience while ensuring data privacy and security. This combination of efficient resource allocation, memory management and file system capabilities are fundamental to the reliability and versatility of the Android platform.

RESOLVE CONFLICT IN RESOURCE DEMAND

Resolving resource demand conflicts is very important to maintain smooth and efficient operation of Android OS. Android uses several strategies to resolve these conflicts and ensure that applications and system processes can coexist without causing performance issues or crashes.

Android OS uses a priority-based scheduler to allocate CPU resources. By assigning different priorities to different system processes and applications, Android ensures that high-priority tasks such as core system functions and user interactions get the resources they need to run smoothly. Low-priority background tasks, on the other hand, can be limited in resource allocation, preventing them from overwhelming the system and degrading overall performance. This approach helps maintain responsiveness while minimizing conflicts between different resource-hungry components.

Android incorporates a process lifecycle management system that allows the OS to terminate or suspend background processes when memory is low. This mechanism ensures that foreground applications and essential system processes get the memory they need to run effectively, even in the face of competing resource demands. Background applications that are not actively in use can be paused or terminated, freeing up resources for more critical tasks. Android provides APIs for developers to optimize their applications and gracefully handle resource constraints, allowing them to release resources when not in use, thereby reducing potential conflicts.

Android's resource management extends to network resources and I/O operations. The OS uses various mechanisms to control network access and disk I/O, ensuring that applications do not monopolize these resources and interfere with the performance of other applications or the system as a whole. Network traffic shaping and file I/O rate limiting help ensure resource usage fairness and responsiveness, reducing conflicts arising from data-intensive applications.

The Android OS uses a combination of priority-based scheduling, process lifecycle management, and resource rate limiting to resolve resource demand conflicts. These strategies help maintain a balance between competing processes, ensuring that the system runs smoothly and efficiently even in the presence of resource-intensive applications and background tasks.

INDIVIDUAL CONTRIBUTION

Name	System Type	OS for the system selected	Features
DIAS M.P.U	Server	Linux operating system	1. Level of security in Linux operating system 2. Provide a stable, portable, reliable, safe and well-behaved environment. 3. Resource sharing among users fairly, efficiently and safely. 4. Manage memory, processor, file etc.
NETHMINI H.W.D	Client	Mac Operating System	1. Support many devices simultaneously. 2. Provide a stable, portable, reliable, safe, and well-behaved environment. 3. Manage memory, and process. 4. The level of the security macOS provides.
RANASINGHE T.M.R	Client	Windows operating system	1. The level of security it provides in windows operating system. 2. Manage memory, processor, file in windows operating system. 3. Windows operating system Support many devices simultaneously. 4. Windows operating system hides the implementation details.
HESHAN Y.B. K	Mobile	Android mobile operating system	1 . The level of security it provides. 2 . Hide implementation details.

			3 . Manage memory, processor, file etc 4 . Resource conflict in resource demand.

CONCLUSION

Our research we investigated four major operating systems and its key features. which is Linux, MacOS, Windows and android. Our research reveals both their strengths and weaknesses. Also, we have answered the core questions and provided valuable details to answer those questions. We made a note representing how important it is to support many devices and how various operating systems fulfill that, how to allocate resources fairly, resolve conflicts between the recourse demand, why these operating systems hide their complicated implementations details how did they do it and finally we assessed the level of security that each operating system offers.

Based on our findings users can gain a more advanced thinking patterns when they are going to select an operating system.in this regards we have effectively finished our thesis, by providing a deep examination of these key operating systems and their role in the modern computing.

REFERENCES

1. Stay protected with Windows Security

Stay protected with Windows Security - Microsoft Support

2. What are web threats

What are web threats and online Internet threats? (kaspersky.com)

3. Operating System Concepts Book by Abraham Silberschatz, Greg Gagne, and Peter Baer Galvin. Page 358

4. Operating System Concepts Book by Abraham Silberschatz, Greg Gagne, and Peter Baer Galvin. Page 388

5.Operating Systems: Three Easy Pieces Book by Andrea Arpaci-Dusseau and Remzi Arpaci-Dusseau. Page 29

6.Modern Operating Systems fourth edition by Andrew S. Tanenbaum, Herbert Bos. Page 537

7. File-System Management - Operating System Concepts Book by Abraham Silberschatz, Greg Gagne, and Peter Baer Galvin. Page 50

8. How to manage permissions and privileges in Linux?

How to Manage Permissions and Privileges in Linux? - Scaler Topics

9. File security

File security (tldp.org)

10. Linux Network security

Linux Administrator's Security Guide - Linux Network Security (linuxtopia.org)

11. Improving the reliability of commodity operating systems

MICHAEL M. SWIFT, BRIAN N. BERSHAD, and HENRY M. LEVY, University of Washington

12. Rapidly Growing Linux OS: Features and reliability

Journal, Norio Kurobani, 20 May 2005

13. File Management in Linux

File Management in Linux - Scaler Topics

14. Files and file system.

Files and file systems - IBM Documentation

15. MacOS

https://en.wikipedia.org/wiki/MacOS

16. Use Continuity to connect your Mac, iPhone, iPad, and Apple Watch
https://support.apple.com/en-us/102418

17. macOS features

https://www.apple.com/us/search/macos-features?page=1&sel=explore&src=globalnav&tab=explore

18. Introduction to Memory Management
https://developer.apple.com/library/archive/documentation/mac/pdf/Memory/Intro_to_Mem_Mgmt.pdf

19. Process Manager

https://developer.apple.com/library/archive/documentation/mac/pdf/Processes/Process_Manager.pdf

20. Security. Built right in.
https://www.apple.com/macos/security/

21. Apple Platform Security
https://support.apple.com/en-gb/guide/security/welcome/web