|  |
| --- |
| **Subject :Operating System Sub Teacher:Prof.S.S.Shete**  **Class: S.E.Computer Engg. Roll no :-**  **Practical No.: 01 Date:** |

**Title:-** Study of Commercial and Open source operating system and design structure of these of operating systems.

**Aim:-**Study of Commercial and Open source operating system and design structure of these of operating systems.

A] Study of basic structure

B] Study the file System

C] Study security aspects of Operating Systems.

D] e.g.Windows OS.,Linux OS.

**Theory :-**

**A] Study of basic structure: Operating System structure:-**

• An OS consists of all of these components, plus:

1. Many other components

2. System programs (privileged and non-privileged)

• e.g., bootstrap code, the in it program.

• **Major issue:**

1] How do we organize all this?

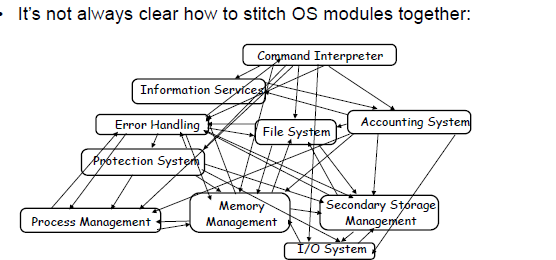
2] What are all of the code modules, and where do they exist?

3] How do they cooperate?

• Massive software engineering and design problem

4] Design a large, complex program that:

• performs well, is reliable, is extensible, is backwards compatible.



**Fig: Structure Of Operating System**

**B] File System:-**A file is a named collection of related information that is recorded on secondary storage such as magnetic disks, magnetic tapes and optical disks. In general, a file is a sequence of bits, bytes, lines or records whose meaning is defined by the files creator and user.

**File Structure:-** A File Structure should be according to a required format that the operating system can understand.

1] A file has a certain defined structure according to its type.

2] Text file is a sequence of characters organized into lines.

3] A source file is a sequence of procedures and functions.

4] An object file is a sequence of bytes organized into blocks that are understand able by the machine.

5] When an operating system defines different file structures, it also contains the code to support these file structure. Unix, MS-DOS support minimum number of file structure.

**File Type:-** File type refers to the ability of the operating system to distinguish different types of file such as text files source files and binary files etc. Many operating systems support many types of files. Operating system like MS-DOS and UNIX have the following types of files:

**1] Ordinary files**

* These are the files that contain user information.
* These may have text, databases or executable program.
* The user can apply various operations on such files like add, modify, delete or eve remove the entire file.

**2] Directory files**

* These files contain list of file names and other information related to these files.

**3] Special files**

* These files are also known as device files.
* These files represent physical device like disks, terminals, printers, networks, tape drive etc.
* These files are of two types:

**4] Character special files** - data is handled character by character as in case of terminals or printers.

**5] Block special files** - data is handled in blocks as in the case of disks and tapes.

**6] File Access Mechanisms:-**

File access mechanism refers to the manner in which the records of a file may be accessed.

There are several ways to access files:

* Sequential access
* Direct/Random access
* Indexed sequential access

**7] Sequential access:-**

A sequential access is that in which the records are accessed in some sequence, i.e., the information in the file is processed in order, one record after the other. This access method

is the most primitive one. Example: Compilers usually access files in this fashion.

**8] Direct/Random access:-**

* Random access file organization provides, accessing the records directly.
* Each record has its own address on the file with by the help of which it can be directly accessed for reading or writing.
* The records need not be in any sequence within the file and they need not be in adjacent locations on the storage medium.

**9] Indexed sequential access:-**

* This mechanism is built up on base of sequential access.
* An index is created for each file which contains pointers to various blocks.
* Index is searched sequentially and its pointer is used to access the file directly.

**10] Space Allocation:-**

Files are allocated disk spaces by operating system. Operating systems deploy following

three main ways to allocate disk space to files.

* Contiguous Allocation
* Linked Allocation
* Indexed Allocation

**11] Contiguous Allocation:-**

* Each file occupies a contiguous address space on disk.
* Assigned disk address is in linear order.
* Easy to implement.
* External fragmentation is a major issue with this type of allocation technique.

**12] Linked Allocation:-**

* Each file carries a list of links to disk blocks.
* Directory contains link / pointer to first block of a file.
* No external fragmentation.
* Effectively used in sequential access file.
* Inefficient in case of direct access file.

**13] Indexed Allocation:-**

* Provides solutions to problems of contiguous and linked allocation.
* An index block is created having all pointers to files.
* Each file has its own index block which stores the addresses of disk space occupied by the file. Directory contains the addresses of index blocks of files.13. Operating System ─ File S

**C] Study security aspects of Operating Systems.** Security refers to providing a protection system to computer system resources such as CPU, memory, disk, software programs and most importantly data/information stored in the computer system. If a computer program is run by an unauthorized user, then he/she may cause severe damage to computer or data stored in it. So a computer system must be protected against unauthorized access, malicious access to system memory, viruses, worms etc. We're going to discuss following topics in this chapter:

1. Authentication

2. One Time passwords

3. Program Threats

4. System Threats

5. Computer Security Classifications

**1] Authentication:-** Authentication refers to identifying each user of the system and associating the executing programs with those users. It is the responsibility of the Operating System to create a protection system which ensures that a user who is running a particular program is authentic. Operating Systems generally identifies/authenticates users using following three ways:

i] **Username / Password** - User need to enter a registered username and password with Operating system to login into the system.

**ii] User card/key** - User need to punch card in card slot, or enter key generated by key generator in option provided by operating system to login into the system.

iii] **User attribute - fingerprint/ eye retina pattern/ signature** - User need to pass his/her attribute via designated input device used by operating system to login into the system.

**2] One Time passwords:-**One-time passwords provide additional security along with normal authentication. In One Time Password system, a unique password is required every time user tries to login into the system. Once a one-time password is used, then it cannot be used again. One-time password is implemented in various ways.

**I] Random numbers** - Users are provided cards having numbers printed along with corresponding alphabets. System asks for numbers corresponding to few alphabets randomly chosen.

II] **Secret key** - User are provided a hardware device which can create a secret id mapped with user id. System asks for such secret id which is to be generated every time prior to login.

III] **Network password** - Some commercial applications send one-time passwords to user on registered mobile/ email which is required to be entered prior to login.

**3] Program Threats**

Operating system's processes and kernel do the designated task as instructed. If a user program made these process do malicious tasks, then it is known as **Program Threats**. One of the common example of program threat is a program installed in a computer which can store and send user credentials via network to some hacker. Following is the list of some well-known program threats.

1] **Trojan Horse** - Such program traps user login credentials and stores them to send to malicious user who can later on login to computer and can access system resources.

2] **Trap Door** - If a program which is designed to work as required, have a security hole in its code and performs illegal action without knowledge of user then it is called to have a trap door.

**3] Logic Bomb** - Logic bomb is a situation when a program misbehaves only when certain conditions met otherwise it works as a genuine program. It is harder to detect.

4] **Virus** - Virus as name suggest can replicate them on computer system. They are highly dangerous and can modify/delete user files, crash systems. A virus is generally a small code embedded in a program. As user accesses the program, the virus starts getting embedded in other files/ programs and can make system unusable for user.

**4] System Threats:-** System threats refers to misuse of system services and network connections to put user in trouble. System threats can be used to launch program threats on a complete network called as program attack. System threats create such an environment that operating system resources/ user files are misused. Following is the list of some well-known system threats.

I] **Worm** -Worm is a process which can choked down a system performance by using system resources to extreme levels. A Worm process generates its multiple copies where each copy uses system resources, prevents all other processes to get required resources. Worm’s processes can even shut down an entire network.

II] **Port Scanning** - Port scanning is a mechanism or means by which a hacker can detects system vulnerabilities to make an attack on the system.

III] **Denial of Service** - Denial of service attacks normally prevents user to make legitimate use of the system. For example, a user may not be able to use internet if denial of service attacks browser's content settings.

**Computer Security Classifications:-** Computer System's Evaluation Criteria there are four security classifications in computer systems: A, B, C, and D. This is widely used specifications to determine and model the security of systems and of security solutions. **Following is the brief description of each classification.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **S.N.** | | **Classification** | **Type** | **Description** | |
| 1 | | TYPE A | Highest Level | Uses formal design specifications and  Verification techniques. Grants a high degree of assurance of Process security. | |
| 2 | | TYPT B | Provides mandatory protection system. | Have all the properties  of a class C2 system. Attaches a sensitivity label to each  object. It is of three types.  **B1** - Maintains the security label of each object in the  system. Label is used for making decisions to access  control.  **B2** - Extends the sensitivity labels to each system  resource, such as storage objects, supports covert  channels and auditing of events.  **B3** - Allows creating lists or user groups for access control  to grant access or revoke access to a given  named object. | |
| 3 | | TYPE C | Provides protection and user accountability using audit  capabilities. | It is of two types.  **C1** - Incorporates controls so that users can protect their  private information and keep other users from accidentally  reading / deleting their data. UNIX versions are mostly Cl  class.  **C2** - Adds an individual-level access control to the capabilities  of a Cl level system | |
| 4 | TYPE D | | Lowest level. | | Minimum protection. MS-DOS, Window 3.1 fall in  this category. |

**D] e.g.1] Linux Operating System.**

**2] Windows Operating System.**

**Linux Operating System has primarily three components:-**

1] **Kernel** - Kernel is the core part of Linux. It is responsible for all major activities of this operating system. It consists of various modules and it interacts directly with the underlying hardware. Kernel provides the required abstraction to hide low level hardware details to system or application programs.

2] **System Library** - System libraries are special functions or programs using which application programs or system utilities accesses Kernel's features. These libraries implement most of the functionalities of the operating system and do not requires kernel module's code access rights.

3] **System Utility** - System Utility programs are responsible to do specialized, individual level tasks.

**Basic Features:-**

**1] Following are some of the important features of Linux Operating System.**

I] **Portable** – Portability means software can works on different types of hardware in same way. A Linux kernel and application program supports their installation on any kind of hardware platform.

II] **Open Source** – Linux source code is freely available and it is community based development project. Multiple teams work in collaboration to enhance the capability of Linux operating system and it is continuously evolving.

III] **Multi-User** – Linux is a multiuser system means multiple users can access system resources like memory/ ram/ application programs at same time.

IV] **Multiprogramming** – Linux is a multiprogramming system means multiple applications can run at same time.

V] **Hierarchical File System** – Linux provides a standard file structure in which system files/ user files are arranged.

VI] **Shell** – Linux provides a special interpreter program which can be used to execute commands of the operating system. It can be used to do various types of operations, call application programs. Etc.

VII] **Security** – Linux provides user security using authentication features like password protection/ controlled access to specific files/ encryption of data.

**2] Following are some of the important features of Windows Operating System.**

1] Less crashing**.**

2] Treats a CD-RW like a real drive.

3] System Restore.

4] Auto play.

5] Software Restriction Policies.

6] Windows Security Center.

**Conclusion:-**In above practical we can successfully studied that commercial and open source operating system and also study is difference between commercial and open source operating system are as follows:

|  |  |  |
| --- | --- | --- |
| **Sr.No.** | **Commercial Operating System** | **Open Source Operating System** |
| **1.** | Commercial systems are created & supported by for-profit companies(eg Microsoft) that typically sell licenses for the use of their software & that are driven by maximizing profits. | Open source systems are overseen by dedicated communities of developers who  contribute modifications to improve product continually & who decide on course of software based on needs of community. |
| **2.** | Commercial software,on the other hand, requires purchasing a license. | Open source Software is generally free or has low-cost licensing options. |
| **3.** | Commercial CMS can be a good choice for your organization if theunderlying platform(eg.Microsoft-based technology)meshes well with other software already used by your organization. | If your organization doesn’t have a specific technology or marketing roadmap in place,but requires a website with virtually unlimited custom solution based on LAMP may be better choice. |
| **4.** | Purchased without it’s source code. | Purchased with it’s source code. |
| **5.** | User must pay to get the proprietary software. | User can get open software for free of charge. |
| **6.** | User cannot modify the software. | User can modify Software. |
| **7.** | User must have a license from vendor before install into computer. | Users can install software freely into any computer. |
| **8.** | Full support from vendor if anything happened to the software. | No one is responsible to the software. |
| **9.** | Commercial OS is Insecure. | Open source OS is Secure. |
| **10.** | High Hardware cost. | Low Hardware cost. |
| **11.** | Not customizable. | Customizable & Features. |
| **12.** | Eg.Windows vista, MS Word,Adobe Photoshop etc. | Eg.Linux,Ubuntu,Open-Office,org Write,GIMP |