OS work 1- Report

Question 1:

Set value of computer clock:
Protected: Current value of the computer clock can affect many other processes running on the computer like calendar events, work applications that relay on time to measure work time. Also showing wrong time to the user can confusion and mistakes (running late to events and etc.)

Read the computer clock:
Unprotected: Many apps can and need to use the current time to function properly. Knowing the time won't affect the overall system or cause a breach of privacy.

Make intensive calculations:
Protected: Running intensive calculations can cause a disruption of the normal working conditions of the device – slowdowns and crashes. These calculations should be checked by the system for malicious code (if ran by a process independently from the user) or given a permission from the user.

Read the memory of other processes:
Protected: It can harm the privacy of the user by gaining personal information from other processes. For example, stealing passwords and bank information from the browser memory by another processes on the system.

Issue a trap/exception instruction:
Unprotected: Every process should be able to raise trap for its own needs, because the trap instruction (int) cannot cause any damage on a modern CPU because of its limited capabilities. Exceptions are raised solely by the CPU therefore it can't be issued on demand by processes (the Exception itself, not the error that triggered it).

Block all interrupts in the system:
Protected: Such operation will significantly endanger the integrity and operations of the OS and the system by denying it knowledge of important events like the system timer event or process errors etc.

Switch from user to kernel mode (change the mode-bit):
Unprotected: Any program might need to do a syscall in order to request access to memory, storage or another external device. The syscall itself is already

monitored by the kernel so another layer of protection in this case might be redundant.

Switch from kernel to user mode (change the mode-bit):
Protected: Taking over control from the kernel should not be allowed regularly as the kernel is the component that manages the OS and allow it to maintain its operation and might be exploited by malicious code to gain control over the system.

Read the keyboard input:
Protected: Free access to the keyboard input is a major risk to security and privacy of the user as It can be used by keyloggers and malicious processes to steal private user information such and passwords and private correspondences.

Read the mouse input:
Protected: Like the keyboard privacy concerns, the mouse input can be used to spy on the users.

Access the hard disk drive (HDD) for writing:
Protected: Free access to the HDD for writing can be dangerous for the integrity of the data on the device. A process can simply override data on the device and even outright delete all of its contents.

Access the Wi-Fi hardware for sending packets:
Protected: Processes should not be able to freely access hardware. In this instance connecting directly to the Wi-Fi hardware can be a major security and privacy risk as it can be used to covertly connect to hostile networks and send data from the device or simply send data unsupervised by the OS and the kernel in the connected network.

Controlling the keyboard status LEDs: CAPS-LOCK & NUM-LOCK:
Protected: Even such a minor function can cause a disruption for the user experience if left open for any process to control (in case of a bug in a process or malicious intent)

Controlling the microphone (recording):
Protected: An obvious risk to the privacy of the user. Recording the user and the surrounding area can be used against the user in multiple ways (blackmail, information stealing and espionage) and this access should be regulated heavily.

Shutting down the computer:
Protected: The ability to shut down the device can be a major risk for the system and potentially harm the OS and the user; Shutting down in a middle of an important process, causing data loss due to a sudden shutdown or just completely making the device inoperable by shutting it down each time the system boots up.

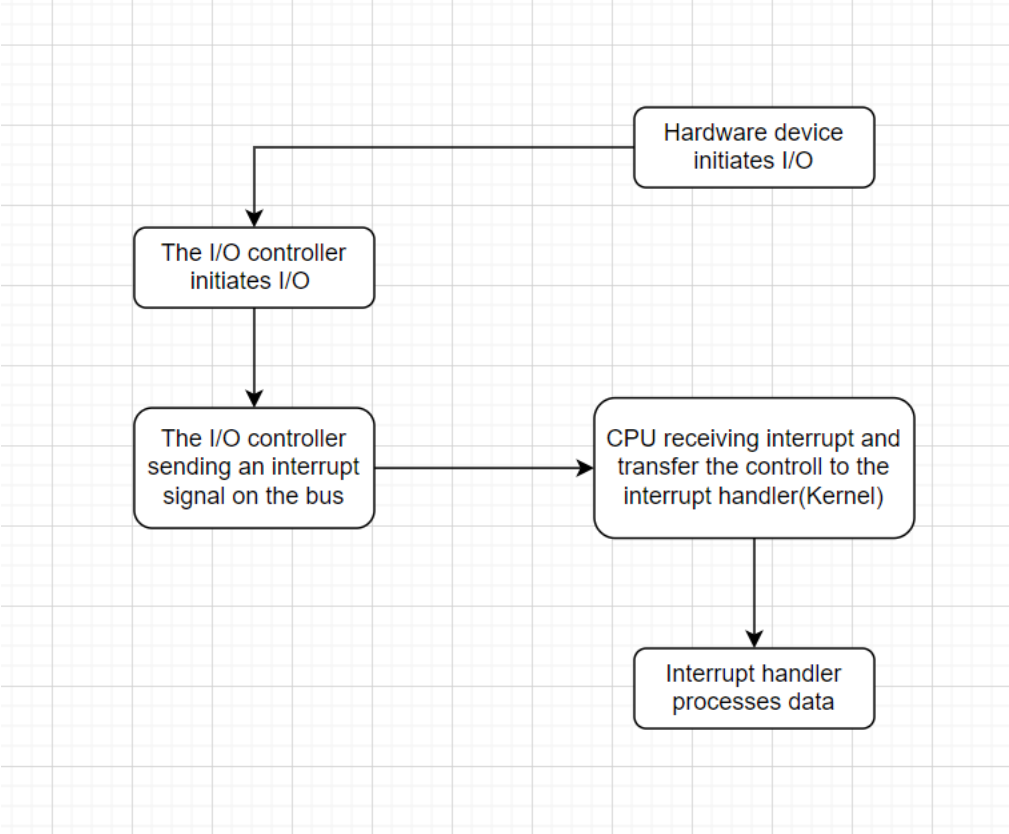
Question 2:

Interrupt table:

An interrupt table is the memory location of an interrupt handler, which prioritizes interrupts and saves them in a queue if more than one interrupt is waiting to be handled.

The interrupt table contains the addresses of all the service routines.

An interrupt is a signal from a device attached to a computer, or from a program within the computer, that tells the operating system to stop and decide what to do next. Once the OS has saved the execution state, it starts to execute the interrupt handler at the interrupt vector.

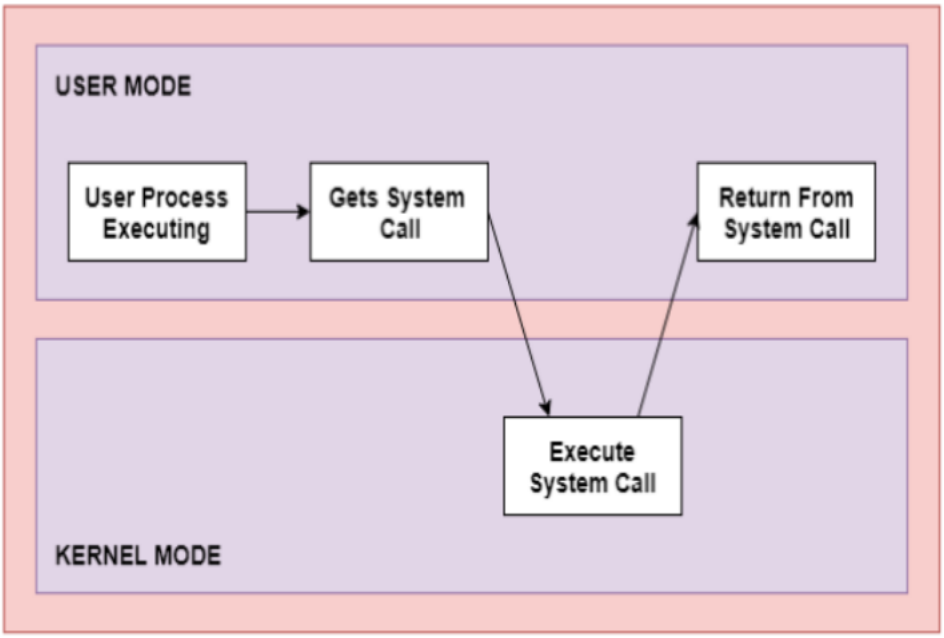


System call table:

A system call is the programmatic way in which a computer program requests a service from the kernel of the operating system.
System calls are usually made when a process in user mode requires access to a resource. Then it requests the kernel to provide the resource via a system call.

In general, system calls are required in the following situations:

1. If a file system requires the creation or deletion of files. Reading and writing from files also require a system call.
2. Creation and management of new processes.
3. Network connections also require system calls. This includes sending and receiving packets.
4. Access to a hardware devices such as a printer, scanner etc. requires a system call.



As can be seen from this diagram, the processes execute normally in the user mode until a system call interrupts this. Then the system call is executed on a priority basis in the kernel mode. After the execution of the system call, the control returns to the user mode and execution of user processes can be resumed.

Direct Memory Access (DMA):

DMA is a method of transferring data from the computer‘s RAM to another part of the computer without processing it using the CPU. While most data that is input or output from your computer is processed by the CPU, some data does not require processing, or can be processed by another device.

In these situations, DMA can save processing time and is a more efficient way to move data from the computer’s memory to other devices.

DMA module itself controls exchange of data between main memory and the I/O device.

CPU is only involved at the beginning and end of the transfer and interrupted only after entire block has been transferred.

The main advantage of the DMA is the speed up of the read-write tasks because of the transferring of the data without the involvement of the processor.

A disadvantage of the DMA is the cache coherence problem can be seen when DMA is used for data transfer. If a CPU has a cache and external memory, then the data the DMA controller has access to (stored in RAM) may not be updated with the correct data stored in the cache.

Question 3:

1. **Batch OS:**
   Where it is used:
   It is used mainly when the system's users do not work directly on the machine and create their job offline.
   Advantages:
   1. The overall time taken by the system to execute all the programs will be reduced.
   2. The Batch Operating System can be shared between multiple users.
   Disadvantages:
   1. Interventions are required between two batches.
   2. No direct interaction between users and jobs.
2. **Time Sharing OS:**
   Where it is used:
   It is used where many programs might need to run simultaneously, like a mainframe for example.
   Advantages:
   1. Since equal time quantum is given to each process, so each process gets equal opportunity to execute.
   2. The CPU will be busy in most of the cases and this is good to have case.
   Disadvantages:
   1. Process having higher priority will not get the chance to be executed first because the equal opportunity is given to each process.
   2. Such system requires competent main memory management in order to switch tasks in or out of the memory in rapid succession.
3. **Distributed OS:**
   Where it is used:
   It was used in the past for research and never saw commercial success because of the rise of multiprocessor systems and multi-core systems.
   Advantages:
   1. Since the systems are connected with each other so, the failure of one system can't stop the execution of processes because other systems can

do the execution.
2. Resources are shared between each other.

Disadvantages:

1. Since the data is shared among all the computers, so to make the data secure and accessible to few computers, you need to put some extra efforts.
2. If there is a problem in the communication network then the whole communication will be broken.

4. **Network OS:**

Where it is used:

It is used mainly for servers in a network with other end-users (clients).

Advantages:

1. Highly stable centralized servers.
2. Server access is possible remotely from different locations and types of systems.

Disadvantages:

1. User has to depend on a central location for most operations.
2. Maintenance and updates are required regularly.

5. **Embedded OS:**

Where it is used:

It is used any devices that needs computing power for a particular job but does not require external hardware to function – it is mostly self-sufficient on the circuitry it was built into.

Advantages:

1. Low cost.
2. Since it is dedicated to a particular job, so it is fast.

Disadvantages:

1. Performs a single job.
2. Hard to upgrade and scale.

6. **Real-Time OS:**

Where it is used:

It is used in systems that require great precision and very short response times like robots, military systems, spacecraft/aircraft control systems, etc.

Advantages:

1. There is maximum utilization of devices and resources.
2. These systems are almost error-free.

Disadvantages:

1. The algorithms used in Real-time Operating System is very complex.
2. Specific device drivers are used for responding to the interrupts as soon as possible.

7. **Mobile OS:**
   Where it is used:
   It is used in portable devices like smartphones, smartwatches, tablets.
   Advantages:
   1. Built with Mobile users' needs in mind (interfaces, features)
   2. Can be very flexible and allow installation of any app that is compatible with the device's hardware (Mostly Android)
   Disadvantages:
   1. Open-source Mobile OS (Like Android) can be more easily compromised by vulnerabilities.
   2. Built specifically for Mobile type devices and won't function well on devices that are not lacking the usual mobile features (e.g touchscreen)
8. **Desktop OS:**
   Where it is used:
   It is the main OS type in the market, used for Personal Computers.
   Advantages:
   1. Able to be used for almost any task – Office work, graphical design, gaming and any other general use.
   2. It is usually supported by the company making it (e.g Microsoft) for many years, keeping it optimized and secured.
   Disadvantages:
   1. Need to support many combinations of hardware – different manufactures, quality and speed of the system components.
   2. Because of its complicated design and the need to support many hardware and software options there is a lot of room to create malware and protecting Desktop OS users is challenging.
9. **Server OS:**
   Where it is used:
   It is used to power servers exclusively.
   Advantages:
   1. Focused on computing power.
   2. Server operating systems help enable and facilitate typical server roles such as Web server, mail server, file server, database server, application server and print server.
   Disadvantages:
   1. Lacking User experience features and user-friendly GUI.
   2. Built for a very specific role.

PS5:

1. HW:

- CPU: AMD 8x Zen 2 Cores at 3.5GHz with SMT
- RAM: 16 GB GDDR6/256-bit RAM
- GPU: 10.28 TFLOPS, 36 CUs at 2.23GHz with variable frequency
- Hard Drive: The SSD in the PS5 has a 825GB capacity

2. I/O:
   Headphones, Controllers, USB, Memory card.

3. OS:
   PS5 operating system is: orbis OS based on Free BSD 12.
   This OS works like Linux OS as a desktop OS but has SOC architecture.

The PlayStation runs many apps such as Spotify, YouTube, Netflix and more. Therefore, it must support many actions that are like running apps on a desktop operating system.

Unlike a desktop operating system, the PlayStation main goal is to run games, so it has several additional features.

A fast SSD was the top request from game developers so the goal not only was to have a theoretical raw read speed 100 times faster than PS4, but to eliminate I/O bottleneck points so the performance target could be made effective. To this end, Sony designed a custom chip with multiple coprocessors to work in unison with the flash memory controller to reduce latency and channel data more efficiently around the system. At peak, the custom unit is capable of processing up to 22 GB/s of compressible data.

Tesla:

The main computing system that Tesla cars have is the entertainment touchscreen, which runs on a custom version of Linux Ubuntu (using INVIDIA's Tegra SoC).
Tesla uses Linux for some of their systems (the Media Control Unit and Instrument Cluster) for a number of reasons:
1. Creating a new OS from scratch can be extremely expensive.
2. Linux is very customizable and therefore Tesla can modify it to meet their needs.
3. Linux has many security features, and when dealing with controlling vehicles like in Tesla's case, security is a very high priority.

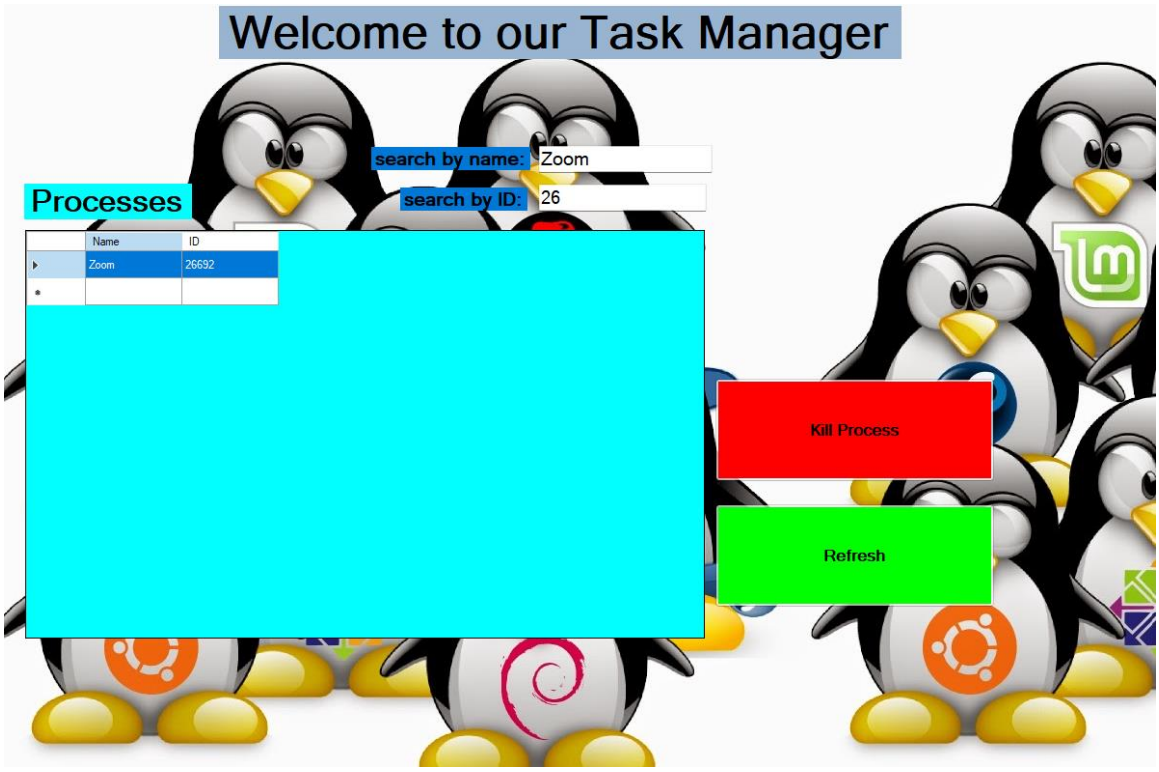
Question 4:

Our task manager displaying all the processes running on the OS.

The results can be filtered by process name or process ID.

The user can refresh the processes to see all the new processes that started to run after running the program.

Each process can be chosen by the user from the table or by typing his name or ID and the can be killed by the killing button.


Welcome to our Task Manager
search by name:
Zoom
search by ID:
26
Processes
Name
ID
Zoom
26692
Kill Process
Refresh