CS3510: Operating Systems - I

Assignment 1

Soumi Chakraborty
ES19BTECH11017

1) **How does the distinction between kernel mode and user mode function as a rudimentary form of protection (security)?**

The operating system executes instructions that deals with both hardware and software. And some instructions, when executed incorrectly or by an unauthorised entity might affect the functioning of the system adversely. The hardware allows these privileged and sensitive instructions to be executed only in the kernel mode.

In the kernel mode, tasks are executed on behalf of the operating system. The user mode has fewer privileges as compared to the kernel mode. The user mode cannot access or execute any of the tasks that the hardware deems as privileged; that is, it doesn't even have access to the hardware in this mode. Any request to execute a privileged instruction from the user mode is not permitted by the hardware and it gets trapped. Moreover, things like I/O control, timer management, and interrupt management all fall under privileged instructions, and are thereby not accessible in the user mode.

In this way, by restricting access to a lot of instructions in the user mode, the distinction between kernel mode and user mode protects the important resources.

2) **Which of the following instructions should be privileged?**

a. Set value of timer
Privileged.

b. Read the clock.
Not privileged.

c. Clear memory.
Privileged.

d. Issue a trap instruction.
Not privileged.

3) **Some early computers protected the operating system by placing it in a memory partition that could not be modified by either the user job or the operating system itself. Describe two difficulties that you think could arise with such a scheme.**

A couple of difficulties that could arise in this scenario:

- Since the OS cannot be accessed or modified by anyone, it can never be updated to newer versions. Moreover, in the event of any errors or issues with the operating system, the computer will have to live with the glitch because it can't be fixed by anyone. And having an operating system which will never get updated is a pretty serious problem, especially in today's world. For example, Windows gets mega updates and newer versions fairly regularly, each more powerful than the last. A laptop stuck with a single version of WIndows forever wouldn't just become severely outdated within a few short years but also become highly incompetent to keep up with the rest of the world.
- Since the OS partition cannot be accessed or modified by anyone, all sensitive data like authorisation credentials, etc. will have to be stored in unprotected regions of the disk which have no overview. This is rather unsafe as this information can be retrieved by anyone which compromises the safety of the system.