CS3510 : Operating Systems - 1
Theory Assignment - 1

1. The distinction between the user mode and kernel mode function gives security as described below.

    - **Privileged instructions** are some set of machine instructions that may cause unnecessary harm to the OS. These underlying privileged instructions can only be performed in the kernel mode.
    - If the user mode tries to execute these privileged instructions, then the hardware will not execute them and in turn, considers them as illegal and traps(a software driven interrupt) to the OS. As a result, the OS can stop the execution of these dangerous instructions in the user mode itself. Hence providing protection.
    - **Hardware devices** can only be accessed when the program is being executed in kernel mode. Hardware devices can't be accessed when the CPU is in user mode.
    - Interrupts can only be controlled when the CPU is running in kernel mode.
    - If the CPU is running in the user mode the **capacity** is limited by OS.

2.

    A. **Set value of timer** - This instruction should be **privileged.** The job scheduling depends on the timer. If a user program is exceeding the timer, then the kernel interrupts and control is given to the OS. But if this instruction can be accessed by the user program, it would arbitrarily set the timer and occupy the CPU. Because of this other programs might get affected. Hence this instruction should be privileged.

    B. **Read the clock** - This instruction should be **Non privileged.** It's not a risky operation to read the clock, as it can't interfere with the kernel operations.

    C. **Clear memory** - This instruction should be **privileged.** If this instruction could be performed by a user program and it erases a chunk of memory which was assigned to another program by OS, it is fatal. Hence this instruction should be privileged.

    D. **Issue a trap instruction -** This instruction should be **Non privileged.** Trap is just a software driven interrupt, hence both can have access to the trap instruction.

3. The two difficulties that could occur with this schema are :

1. To access the important data that is stored in OS such as passwords,controls etc should be stored in a rather unprotected memory block and be retrieved by the user, as we cannot store them in the protected memory block.

2. As the OS is in a memory partition that can't be accessed by both user and kernel, we can't update or modify(*fix bugs or better way of writing code*) the OS when needed.