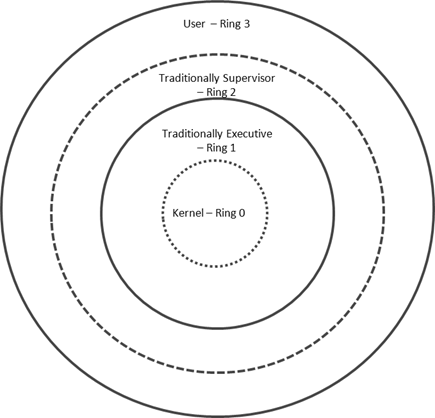
**Assignment 3**

**Processor Rings**

To restrict (protect) critical resources like IO, memory, ports etc, CPU in liaison with the OS provides privilege levels.

Privilege levels are also called protection rings. Protection rings are mechanism to protect data and functionality from faults and malicious behavior. Protection rings are represented as concentric circle. Drawn below:-



Purposes of the ring is:-

1. Ring 0:- OS Kernel

2. Ring 1:- OS Services

3. Ring 2:- Custom Extensions

4 Ring 3:- User application

All user code runs at Ring 3 and kernel code runs at Ring 0. Ring 1 and Ring 2 are almost never used by any OS implementation. Code at Ring 0 can access hardware directly and thus kernel is implemented at this ring.

Special gates between the ring are provided to allow an outer ring to access inner ring’s resources in a predifined manner. These gates are called call gates.

**Blue pill**

The blue pill rootkit is the malware that executes as a hypervisor to gain control of computer resources. A hypervisor is a hardware virtualization technique that allows multiple guest operating systems (OS) to run on a single host system at the same time. The hypervisor installs without restart and the computer functions degradation of speed and services, which makes detection difficult. The hypervisor is also known as virtual machine manager (VMM).

The name *blue pill* is a reference to the science fiction movie *The Matrix*. Neo, the main character, is offered a choice between a blue pill, which will allow him to live obliviously in the virtual reality environment of The Matrix, and a red pill that will allow him to understand his situation and ultimately escape from The Matrix.

Submitted by :- Monika