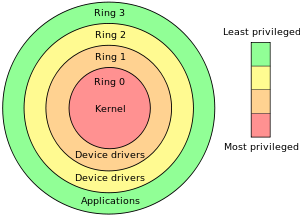
## PROCESSOR PRIVILEGE RINGS

Processor Privilege Rings or protection rings is a mechanism that aims to provide security and fault tolerance by restricting usage of and/or access to specialized, privileged functionality or resources to specific modes/privilege levels of the CPU.

It is usually said about 4 rings level 0 to 3.Ring 0 is most privileged and Ring 3 is less privileged .in ring 0 code can access hardware directly, therefore kernel is implemented at this ring. All least trusted code run at ring 3, thus user code would run at ring3.Ring1 and ring2 are not used by any of the modern os.

When system call is made from less privileged to more privileged ring , functions need to share data space and return from more privileged ring to lesser privileged ring , this space can be analyzed by caller , creating a security hole.



# BLUE PILL

Blue Pill is about hijacking an operating system , moving intyo a virtual machine and taking control of it. It was a new breed of malicious programs that would slip themselves underneath the operating system in a virtual machine hypervisor.

Hypervisor( Computer softwares that creates and run virtual machines) installs without requiring restart and the computer functions normally , without degradation of speed or services which makes detection difficult.

Blue pill works by taking advantage of hardware virtualization technology in processors from advanced micro devices. Virtualization allows computers to simultaneously run multiple operating system and applications in separate partitions . “Using this virtualization technology should allow us to develop malware that is 100% undetectable” .

**Submitted By:**

**Praveen Kumar Singh**

**M.C.A(L.E.), 3rd sem**