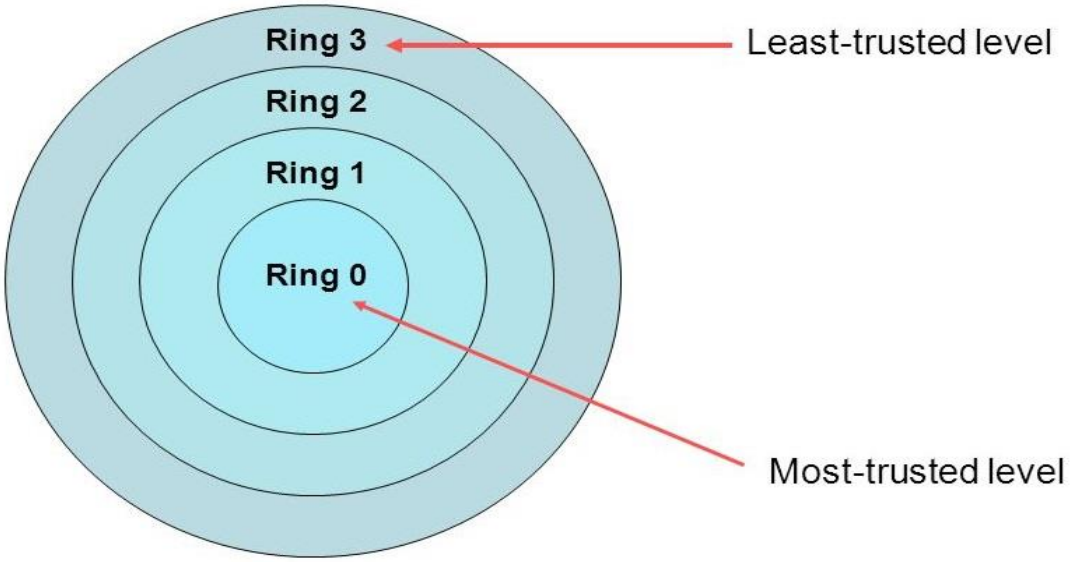
Processor Privilege Rings

Processor privilege rings is a security mechanism used by operating system to provide security and manage hardware and user requests. There are four levels define in intel x86 Privilege level.



1. Ring 0:- Ring 0 is the most trusted and privileged ring. Only ring 0 have permissions to make changes or communicate with hardware. All Kernel code or important system files run under ring 0.
2. Ring 1: - Ring 1 have no such actual privilege level, but since it can host multiple kernels all of which believe they have ring 0 access to the system.
3. Ring 3: - This is the least trusted level . User applications or programs run under ring 3.

When a system call make a request from less privilege level to more privilege level ring, Functions need to share data space then return form more privilege ring to less privilege level.

Blue pill Rootkit

The blue pill rootkit is a virtual-machine based rootkit malware that executes as a hypervisor to gain control of computer resources. It was designed by Joanna Rutkowska and originally demonstrated at the Black Hat Briefings on August 3, 2006, with a reference implementation for the Microsoft Windows Vista kernel.

The hypervisor installs without requiring a restart and the computer functions normally, without degradation of speed or services, which makes detection difficult.

The hypervisor is invisible to the operating system and has full privileges to make any change desired. The malware can intercept any internal communication between the operating system and system hardware and software and send a false response.