Protection Rings

Return to Glossary

Protection Rings, also known as **Hierarchical Protection Domains**, are mechanisms to protect data and functionality from faults (by improving fault tolerance) and malicious behavior (by providing computer security).

Operating Systems (OSs) provide different levels of access to resources. A **Protection Rings** is one of two or more hierarchical levels or layers of privilege within the architecture of a computer system. This is generally hardware-enforced by some CPU architectures that provide different CPU modes at the hardware or microcode level. Rings are arranged in a hierarchy from most privileged (most trusted, usually numbered zero) to least privileged (least trusted, usually with the highest ring number). On most operating systems, Ring 0 is the level with the most privileges and interacts most directly with the physical hardware such as the CPU and memory.

In normal usage, the rings are allocated as follows[1)]:

- **Ring 0**: Kernel {the highest privilege}
- **Ring 1**: Device Drivers
- **Ring 2**: Device Drivers
- **Ring 3**: User Applications {the lowest privilege}

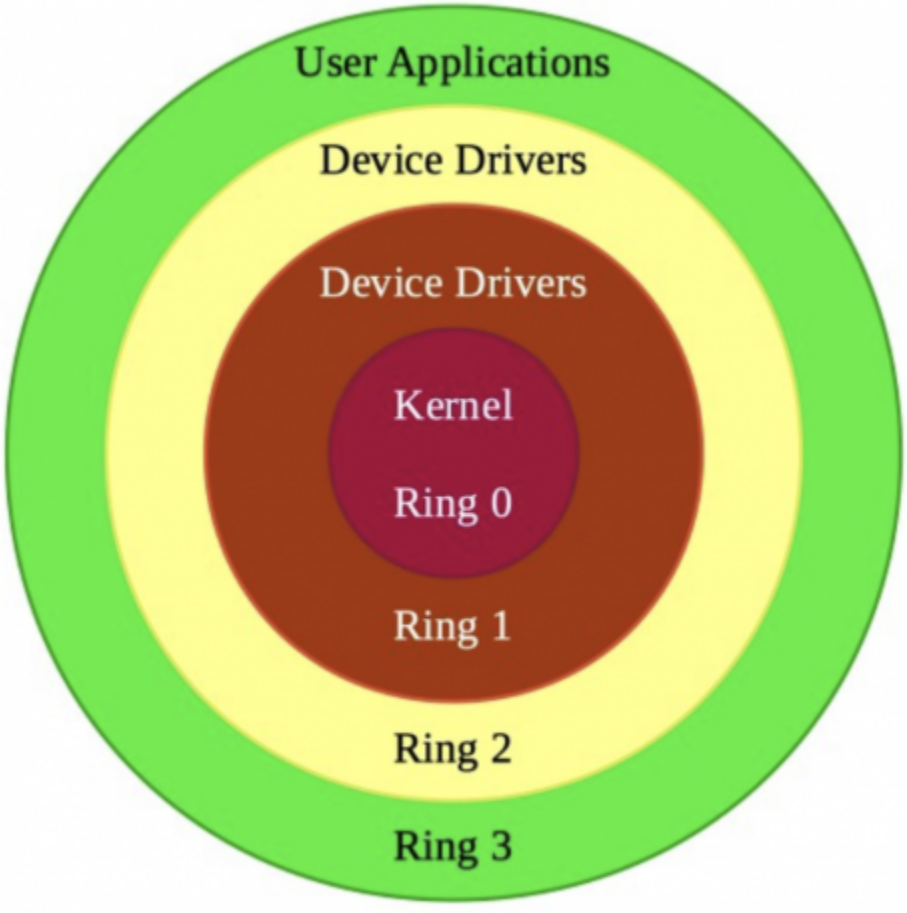

Figure 1: x86 Protection Rings or Layers (From RealWorldCyberSecurity)

Special call gates between rings are provided to allow an outer ring to access an inner ring's resources in a predefined manner, as opposed to allowing arbitrary usage. Correctly gating access between rings can improve security by preventing programs from one ring or privilege level from misusing resources intended for programs in another. For example, spyware running as a user program in Ring 3 should be prevented from turning on a web camera without informing the user, since hardware access should be a Ring 1 function reserved for device drivers. Programs such as web browsers running in higher numbered rings must request access to the network, a resource restricted to a lower numbered ring.

However, with the advent of Virtual Machines, the definition of the **Protection Rings** has expanded using Negative Rings [2)]:

the complete view of the ring architecture becomes:

- **Ring -3**: Management Engine (ME) {the highest Privilege}
- **Ring -2**: System Management Mode (SMM)
- **Ring -1**: Hypervisor
- **Ring 0**: Kernel
- **Ring 1**: Device Drivers
- **Ring 2**: Device Drivers
- **Ring 3**: User Applications {the lowest Privilege}

Figure 2: x86 Negative Protection Rings or Layers (From RealWorldCyberSecurity)

Source: https://en.wikipedia.org/wiki/Protection_ring

[1] , [2]

RealWorldCyberSecurity, 22 April 2020, Accessed: 21 January 2022, https://medium.com/swlh/negative-rings-in-intel-architecture-the-security-threats-youve-probably-never-heard-of-d725a4b6f831