Privilege Levels and Cache Mechanisms in the 80826 Microprocessor

By
Liza Sharma
Nimi Sherpa
Monika Neupane

Privilege Levels in 80286

- In the Intel 80286 microprocessor, privilege levels are a hierarchical security mechanism that controls access rights of software running on the system.

- This allows the operating system to isolate critical functions from less trusted applications, improving overall system security and reliability.

- There are four Rings, ranging from 0 to 3.

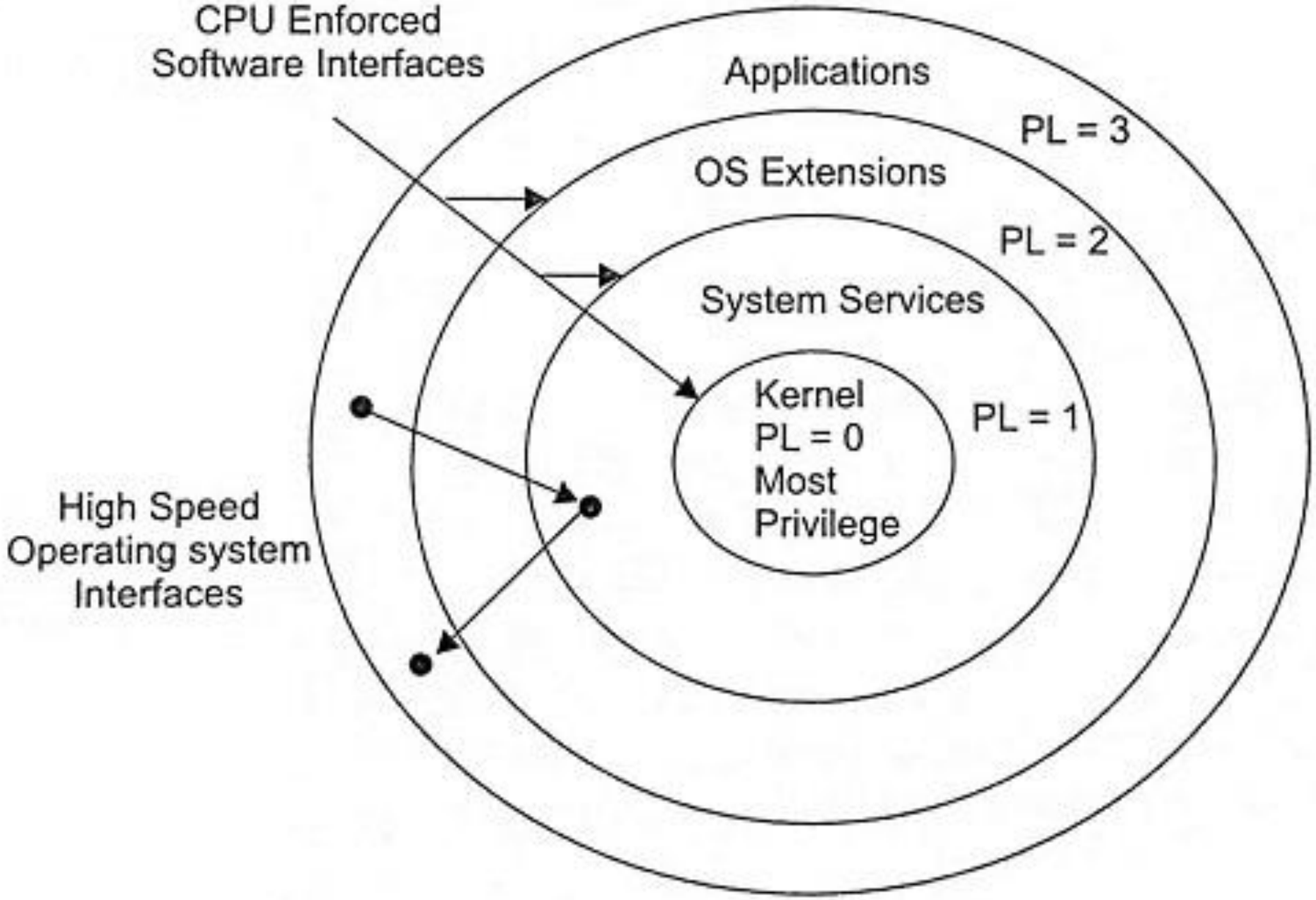

Fig. 11.30 *Four-level privilege*

The Four Privilege Rings

Ring 0(Kernel Mode):

- Ring 0 is the most privileged level in the 80286 microprocessor’s hierarchical privilege system. It's also referred to as Kernel Mode.

Key Characteristics of Ring 0:

- Ring 0 has unrestricted access to all hardware components, including the CPU, memory, and input/output (I/O) devices.

- It allows the execution of specific CPU instructions that are forbidden at lower privilege levels (e.g., enabling/disabling interrupts, setting control registers).

Ring 1: Device Driver Mode

- It was intended for device drivers, which needed elevated access to interact with hardware components but still required some limitations to ensure system stability.

Device Management:

Device Driver Mode grants programs the ability to directly manage and control specific hardware devices, such as storage controllers, network interfaces, and input/output peripherals.

Ring 2:

- Ring 2 is reserved for server-side components that needed elevated access but not the full privileges of the kernel.
- It is often used for code that requires more privileges than user applications but less than kernel-level operations(certain types of middleware or service layers).

Ring 3:

- Ring 3 is the least privileged level in the CPU privilege ring model, typically used by user-level applications.
- Running user applications in Ring 3 protects the system from unintended or malicious actions.

Descriptor Cache

- **Function: The 80286 includes a cache for segment descriptors to speed up access. This cache helps in reducing the overhead associated with descriptor fetching and improves performance.**

- **Segment Registers:**

- **CS (Code Segment): Contains the base address and attributes of the code segment.**

- **DS (Data Segment): Contains the base address and attributes of the data segment.**

- **SS (Stack Segment): Contains the base address and attributes of the stack segment.**

- **ES (Extra Segment): Used for additional data segments**

Privilege levels with working and descriptor cache of 80286

- Segment Descriptors: Stored in the Global Descriptor Table (GDT) and Local Descriptor Table (LDT).
- Descriptor Privilege Levels (DPL):
- DPL 0: Highest access level, usually for kernel segments.
- DPL 1 and 2: Intermediate access levels, used for system processes.
- DPL 3: Lowest access level, for user-mode applications.

How privilege levels work with descriptor cache in 80286 mp:

•Descriptor Cache:
Enhances performance by storing segment descriptors for fast access.

•Privilege Levels:
Enforced by checking segment descriptor attributes against the current privilege level.

•Protected Mode:
• Uses privilege levels and the descriptor cache to manage access and protect system resources effectively.

In summary, in Protected Mode, the descriptor cache of the 80286 helps speed up memory access by caching segment descriptors, while privilege levels ensure that access to segments is controlled according to the privilege level of the executing code. This mechanism helps maintain system stability and security.

Summary

- The 80286 microprocessor has four privilege levels:
- Ring 0 (kernel), Ring 1, Ring 2, and Ring 3 (user).
- 80826 microprocessor uses segment descriptors for memory management, defining segment access and privileges.

Thank you!