privilege levels are managed with system of permissions that dictate which users can access and modify files, directories and other system resources.

— Kernel mode:

kernal model is a privileged mode in which the operating system kernel operates. It has complete access to all system resources and hardware.

— Features:

Full System Access: The kernel can execute any instruction and access any memory address.

privileged Instructions: Kernel mode can execute privileged instructions that are restricted in user mode (eg. I/O operations, process management).

Resource Management: The kernal manages system resources such as memory, CPU and device.

Security and Stability: Running in kernal mode provides high privileges but also high risk, as errors can crash the entire system.

— User mode:

user mode is a restricted mode in which user applications operate. It has limited access to system resource and hardware.

— Features:

Restricted Access: It can not directly access kernal resources and hardware.

safety: kernal enhancing system stability and securities.

Sandboxing: Each user process runs in its own Sandboxed environment.

System calls: User process interact with the kernel through system call.