

# MINIX 3 Privilege Ring Architecture

IPC Message (via kernel)  
Process A → Kernel → Process B

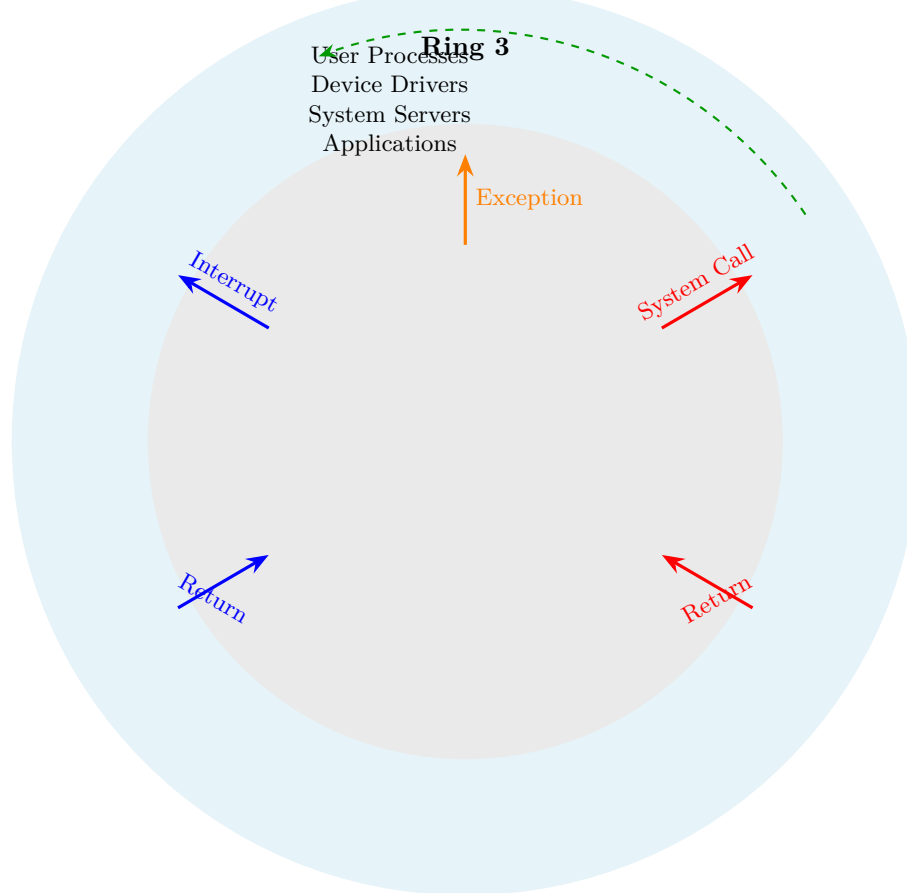
**Ring 0 Capabilities:**

- All CPU instructions
- I/O port access
- Control registers
- GDT/IDT/TSS modification
- Interrupt enable/disable
- Memory protection setup

**Ring 3 Restrictions:**

- No privileged instructions
- No direct I/O access
- Cannot disable interrupts
- Cannot modify page tables
- Must use system calls for kernel services

**Inter-Process Communication:**  
User processes cannot directly access each other  
All IPC via kernel:  
Sender → Kernel → Receiver  
Kernel validates endpoints and copies messages safely



## System Call Gates

Three mechanisms:

- INT 0x33 (legacy)
- SYSENTER/SYSEXIT (Intel)
- SYSCALL/SYSRET (AMD)

## Handlers in IDT:

mpx.S:220 (SYSENTER)

mpx.S:202 (SYSCALL)

mpx.S:265 (INT)

## Interrupt Gates

Hardware IRQs 0-15

Handlers: hwint00-15

mpx.S:98-190

## Exception Gates

CPU traps (#PF, #GP, etc.)

Handler: exception\_entry

mpx.S:347

## Privilege Checks

CS.RPL field determines ring:

- 0 = Kernel (privileged)
- 3 = User (unprivileged)

IDT gates enforce CPL checking

## Key Protection:

Only Ring 0 can execute:

LGDT, LIDT, LTR, CLI, STI,  
MOV to CR\*, INVLPG, HLT