Understanding INT 0x2E and the Windows Kernel

Reda Ouzidane

INT 0x2E – System Call Interrupt

Historically, `0x2E` (in hexadecimal) refers to the interrupt number used by:

> **INT 2E – System Call Interrupt**
> Used in older versions of Windows (e.g., Windows NT, 2000, XP) to transition from **user mode to kernel mode**.

How It Worked

When a user-mode application needed to call a kernel-mode service (such as `NtCreateFile`), it would:

- Set up the system call arguments.
- Trigger `INT 2E`, which caused a software interrupt.
- The CPU switched to **ring 0 (kernel mode)**, and the Windows kernel handled the request.

Why It's Legacy

`INT 2E` was replaced in newer Windows versions (from XP SP2 and especially Vista onward) by more efficient instructions like `SYSENTER` and `SYSCALL`. Modern system calls now use:

- `KiFastCallEntry`
- System call stubs in `ntdll.dll`

Use in Malware and Reverse Engineering

- Malware or rootkits may still use `INT 2E` for backward compatibility or evasion.
- Some shellcode uses `INT 0x2E` when targeting legacy systems.

Example Assembly

```
mov eax, 0x0F      ; Syscall number
mov ebx, param1
mov ecx, param2
int 0x2e           ; Trap to kernel
```

Summary Table

Hex	**Meaning**	**Context**
0x2E	Interrupt vector for INT 2E	Legacy system call method in Windows

Written by Reda Ouzidane