Understanding KiSystemCall64 in Windows Kernel

Reda Ouzidane

What is `KiSystemCall64`?

`KiSystemCall64` is a low-level kernel function in Windows responsible for handling system calls from user mode on 64-bit systems.

When a 64-bit application makes a system call, it executes the `SYSCALL` instruction, which switches the CPU from user mode (Ring 3) to kernel mode (Ring 0) and jumps to the address stored in the `IA32_LSTAR` register. This address points to `KiSystemCall64`.

What Does `KiSystemCall64` Do?

Once control is transferred to `KiSystemCall64`, it performs the following tasks:

- **Saves the CPU state**: It saves the state of the registers, flags, and other important execution data.
- **Validates syscall parameters**: It ensures the parameters passed by the user-mode application are valid.
- **System call dispatch**: `KiSystemCall64` looks up the requested system call number in the System Service Dispatch Table (SSDT) and dispatches the appropriate kernel function (e.g., `NtOpenProcess`, `NtCreateFile`).
- **Restores the state and returns**: Once the system call completes, the function restores the CPU state and returns to user mode using the `SYSRET` instruction.

System Call Flow

1. User-mode code executes `SYSCALL`.
2. The CPU jumps to the address in `IA32_LSTAR`, which points to `KiSystemCall64`.
3. `KiSystemCall64` performs the following:
    - Saves state
    - Validates parameters
    - Dispatches the system call from SSDT
    - Restores state and returns with `SYSRET`

Why It Matters

- `KiSystemCall64` is the gateway between user-mode and kernel-mode code.
- If an attacker can hijack `KiSystemCall64`, they can control the execution of system calls.
- Tools like rootkits often hook or redirect `KiSystemCall64` to gain persistence or escalate privileges.
- It is heavily protected by security mechanisms like PatchGuard, VBS, and HVCI.

Security Protections

In modern versions of Windows, `KiSystemCall64` is protected by several security features:

- **PatchGuard (Kernel Patch Protection)**: Prevents unauthorized modifications to kernel functions like `KiSystemCall64`.
- **Hypervisor-based Code Integrity (HVCI)**: Ensures that kernel-mode code is integrity-checked using a hypervisor.
- **Virtualization-Based Security (VBS)**: Provides isolation for critical security components.