Understanding IA32_LSTAR and RDMSR

Reda Ouzidane

What is IA32_LSTAR?

`IA32_LSTAR` is a Model-Specific Register (MSR) identified by the index `0xC0000082`. It is used in 64-bit Intel and AMD CPUs to define the target instruction pointer (RIP) for the `SYSCALL` instruction.

When a user-mode application executes `SYSCALL`, the CPU switches to kernel mode (Ring 0) and sets the RIP to the value stored in `IA32_LSTAR`. This is typically the system call handler entry point.

How is IA32_LSTAR Accessed?

Only code running in kernel mode (Ring 0) can access MSRs using the `RDMSR` and `WRMSR` instructions.

Reading IA32_LSTAR with RDMSR

```
mov ecx, 0xC0000082    ; IA32_LSTAR MSR index
rdmsr                  ; Result in EDX:EAX
shl rdx, 32
or rax, rdx            ; Combine EDX:EAX into full 64-bit RIP
```

Writing IA32_LSTAR with WRMSR

```
mov ecx, 0xC0000082    ; IA32_LSTAR
mov edx, high32        ; High 32 bits of target address
mov eax, low32         ; Low 32 bits
wrmsr                  ; Write new syscall handler address
```

Why It Matters in Security

- `IA32_LSTAR` determines where the OS jumps on a syscall.
- Attackers can hijack it to redirect syscalls to a malicious handler.
- Security tools and hypervisors monitor or virtualize this register.
- It is a common target in rootkits, kernel exploits, and CTF challenges.

Relevant MSRs for SYSCALL

Register	MSR Index	Purpose
IA32_LSTAR	0xC0000082	RIP target on SYSCALL instruction (64-bit only)
IA32_STAR	0xC0000081	Segment selectors for SYSCALL & SYSRET
IA32_EFER	0xC0000080	Enables SYSCALL/SYSRET instructions and NX bit