Model-Specific Registers (MSRs) and Their Architecture

Reda Ouzidane

What are MSRs?

Model-Specific Registers (MSRs) are special-purpose registers used in x86 and x64 processors to control low-level CPU features. They can only be accessed from **ring 0** (kernel mode) using the `RDMSR` and `WRMSR` instructions.

MSR Architecture Overview

Key Registers and Their Functions

Register Name	**Purpose**
`IA32_SYSENTER_CS`	Segment selector for SYSENTER
`IA32_SYSENTER_ESP`	Stack pointer for SYSENTER
`IA32_SYSENTER_EIP`	Instruction pointer for SYSENTER
`IA32_LSTAR`	SYSCALL target address (64-bit)
`IA32_EFER`	Enables SYSCALL/SYSRET, NX bit, SVME
`IA32_DEBUGCTL`	Debug control flags
`IA32_FS_BASE`, `IA32_GS_BASE`	TLS base addresses
`IA32_TSC`	Time Stamp Counter
`IA32_VMX_*`	VMX virtualization control

Accessing MSRs

Only kernel-mode code can read/write MSRs:

```
mov ecx, 0xC0000082 ; IA32_LSTAR MSR
rdmsr               ; Read into EDX:EAX
; Modify EDX:EAX
wrmsr               ; Write back to MSR
```

Security Relevance

- MSRs control SYSCALL/SYSENTER entry points.

- Rootkits may hijack `IA32_LSTAR` to redirect system calls.
- MSRs are used in VMX (Intel VT-x) and SVM (AMD-V) for virtualization.
- Some MSRs track processor time and performance.

Written by Reda Ouzidane