Invocazione delle chiamate di sistema

Leonardo Bizzoni

January 29, 2024

L'invocazione di una syscall, a differenza di una normale funzione, richiedere il cambiamento della modalità di funzionamento della CPU da user-mode a kernel-mode. Per effettuare questo passaggio è necessario:

- Preparare gli argomenti da passare alla syscall.
- Indicare l'**indirizzo della procedura** da chiamare.

Successivamente viene chiamata un'opportuna istruzione macchina (*es. INT, SVC, SYSCALL*) che genera un'eccezione e cede il controllo ad una subroutine del kernel (*in kernel-mode*) che gestisce l'eccezione. Questa subroutine, detta **system call interface**, legge l'identificatore della chiamata di sistema (*se si sta facendo una chiamata di sistema*), cerca all'interno di una **tabella interna** l'identificatore e, se lo trova, salta (*JMP*) all'indirizzo della procedura associata la quale leggerà gli argomenti ed effettuerà la funzionalità richiesta.

Alla fine dell'esecuzione la CPU torna in user-mode.

1 Esempio Assembly x86-64

```
section .data
        hello db 'Hello, World!', 0xA, 0  ; 0xA è il `\n`
        len   equ $ - hello   ; $ = indirizzo attuale

section .text
        global _start

_start:
        mov rax, 1       ; sys_write stdout `len` "Hello, World!\n"
        mov rdi, 1       ; Scrivi su stdout
```

```
mov rsi, hello   ;     una stringa "Hello, World!\n"
mov rdx, len     ;     di lunghezza ‘len‘
syscall          ; Genera l’eccezione e passa in kernel-mode

                 ; Siamo tornati in user-mode
mov rax, 60      ; sys_exit 0
mov rdi, 0
syscall
```