LESSON 8



ASM

Calling Convention

Learn it all @MyWebUniversity



A FREE MYWEBUNIVERSITY COURSE

ASSEMBLY LANGUAGE

LESSON 8

Functions and the Calling Convention

The System V ABI: argument registers, return values, caller- and callee-saved registers, alignment a

Why a Calling Convention?

Argument	Register
1st · 2nd · 3rd	rdi · rsi · rdx
4th · 5th · 6th	rcx · r8 · r9
7th and more	on the stack
return value	rax
float args	xmm0 … xmm7

- A calling convention is an agreement: where arguments go, where the result comes back, and …
- On Linux and macOS, x86-64 uses the System V ABI. Following it lets your assembly call C, …

01

Caller-Saved and Callee-Saved



- A function may freely change rax, rcx, rdx, rsi, rdi and r8 to r11. If the caller needs ...
- rbx, rbp and r12 to r15 must be preserved: if a function uses them, it pushes them first ...

02

Writing a Function

ASSEMBLY LANGUAGE · 8

add3.asm

```
; long add3(long a, long b, long c)
global add3
add3:
    lea rax, [rdi + rsi]
    add rax, rdx
    ret

; caller:
    mov rdi, 10
    mov rsi, 20
    mov rdx, 12
    call add3          ; rax = 42
```

- This function adds three numbers. The arguments arrive in rdi, rsi and rdx, and the result …
- It uses only scratch registers, so it needs no prologue at all.

03

Stack Alignment

ASSEMBLY LANGUAGE · 8

align.asm

```
my_func:                ; on entry rsp ends in ...8
    push rbx            ; now rsp ends in ...0  ✓ aligned
    ; call other functions safely here
    pop rbx
    ret

other:
    sub rsp, 8          ; align before calling
    call printf
    add rsp, 8
    ret
```

- Before a call, rsp must be a multiple of sixteen. call pushes eight bytes, so inside a …
- Breaking this rule makes library functions like printf crash in mysterious ways.

04

Recursion

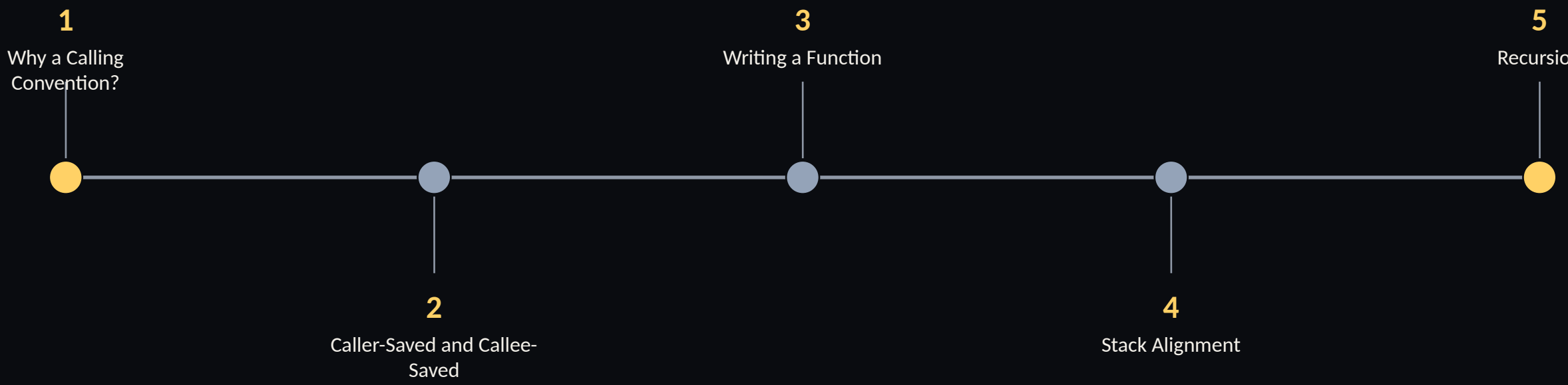
fact.asm

```
; long fact(long n)
fact:
    cmp rdi, 1
    jle .base
    push rbx
    mov rbx, rdi          ; keep n
    dec rdi
    call fact             ; rax = fact(n-1)
    imul rax, rbx         ; n * fact(n-1)
    pop rbx
    ret
.base:
    mov eax, 1
    ret
```

- Recursive functions work naturally because every call gets its own stack frame. Save what …
- Here is factorial: if n is at most one return one, otherwise n times factorial of n minus one.

05

Lesson Map


1
Why a Calling Convention?
2
Caller-Saved and Callee-Saved
3
Writing a Function
4
Stack Alignment
5
Recursion

Sources and Further Reading





Thank you for watching

MyWebUniversity.com

Free technical education since 2000 — English and Dari

@MyWebUniversity · @MyWebUniversity-Dari