LESSON 7



ASM

The Stack

Learn it all @MyWebUniversity



A FREE MYWEBUNIVERSITY COURSE

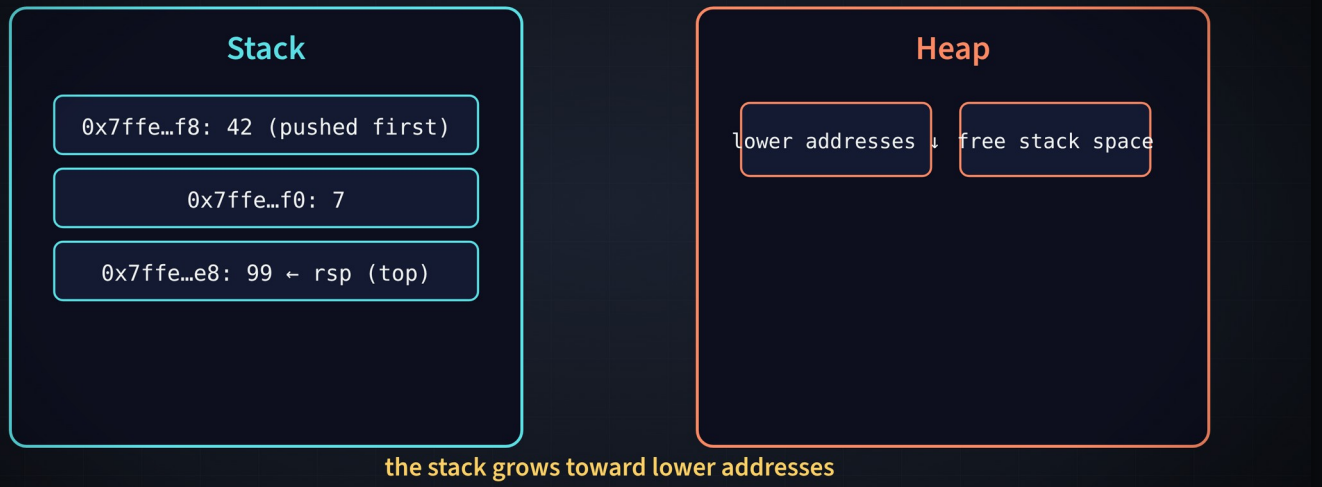
ASSEMBLY LANGUAGE

LESSON 7

The Stack: push, pop, call and ret

rsp, push and pop, call and ret, return addresses and stack frames

What Is the Stack?



- The stack is a region of memory used last in, first out. rsp, the stack pointer, always …
- On x86 the stack grows downward: pushing makes rsp smaller, and popping makes it bigger.

01

push and pop

stack.asm

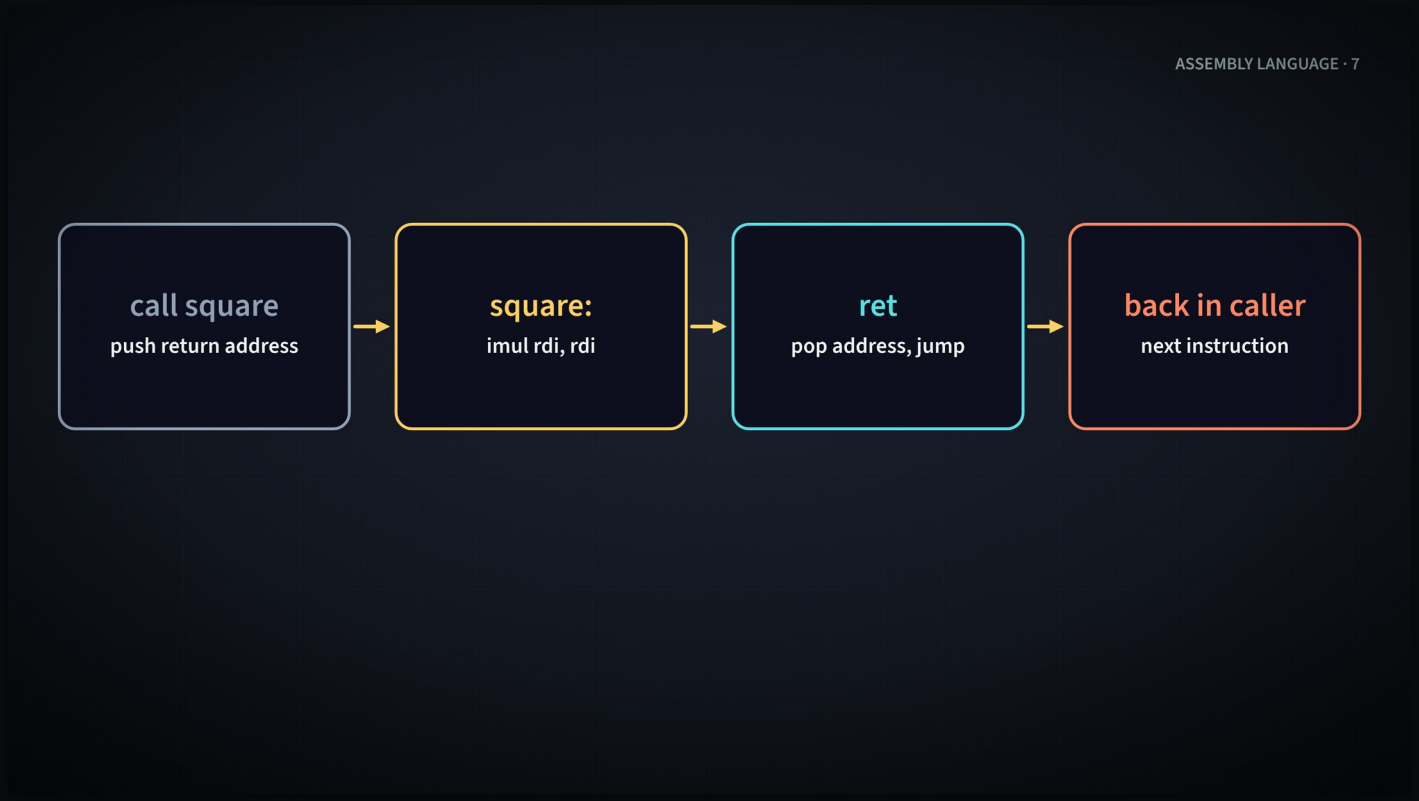
```
push rbx              ; save rbx
push r12              ; save r12
; ... use rbx and r12 freely ...
pop r12               ; restore in reverse order
pop rbx

; push rax  ==  sub rsp, 8 / mov [rsp], rax
; pop rax   ==  mov rax, [rsp] / add rsp, 8
```

- push subtracts eight from rsp and writes a value there. pop reads the value at rsp into a …
- Use them to save registers you need to keep, and always pop in the reverse order you pushed.

02

call and ret



- call square — push return address
- square: — imul rdi, rdi
- ret — pop address, jump

03

Stack Frames

ASSEMBLY LANGUAGE · 7

frame.asm

```
my_func:
    push rbp              ; prologue
    mov  rbp, rsp
    sub  rsp, 16          ; room for 2 locals
    mov  qword [rbp-8], 0     ; local a
    mov  qword [rbp-16], 5    ; local b
    ; ...
    mov  rsp, rbp         ; epilogue
    pop  rbp
    ret
```

- Each function call gets its own stack frame for local variables and saved registers. The …
- The epilogue undoes it. Local variables live at negative offsets from rbp.

04

Stack Bugs

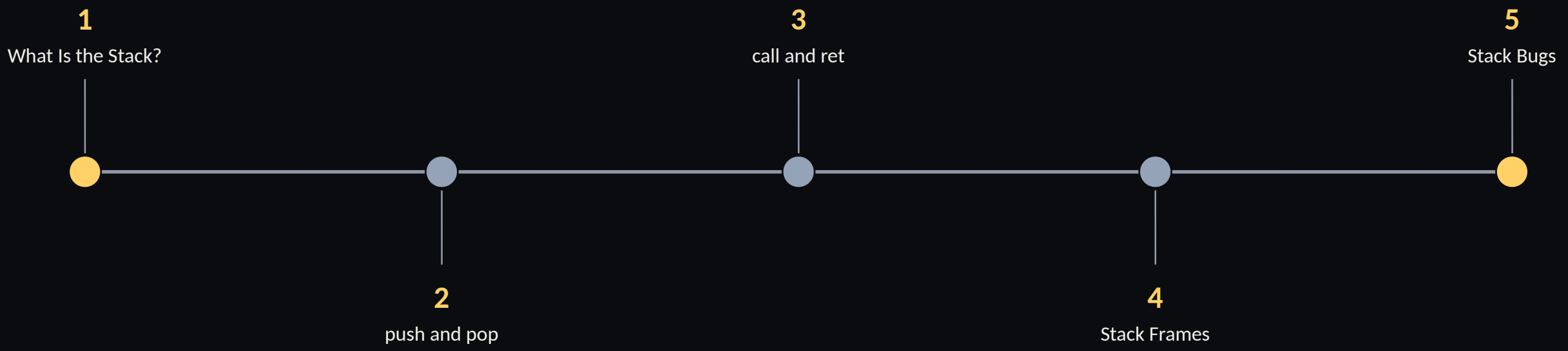
terminal

```
$ ./broken
Segmentation fault (core dumped)
$ gdb ./broken
(gdb) run
Program received signal SIGSEGV
0x0000000000000000 in ?? ()    ← ret jumped to address 0
```

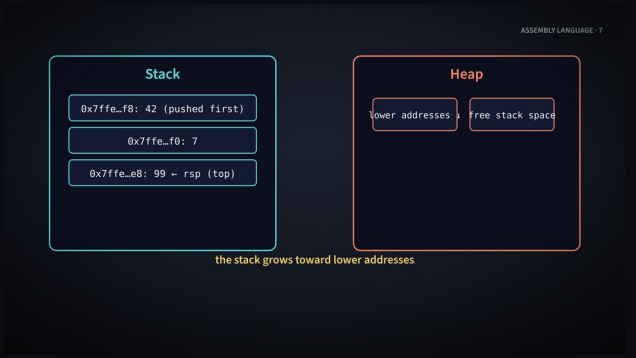
- If pushes and pops do not match, ret jumps to the wrong address and the program crashes. …
- Writing past a local buffer can overwrite the return address. This is the classic buffer …

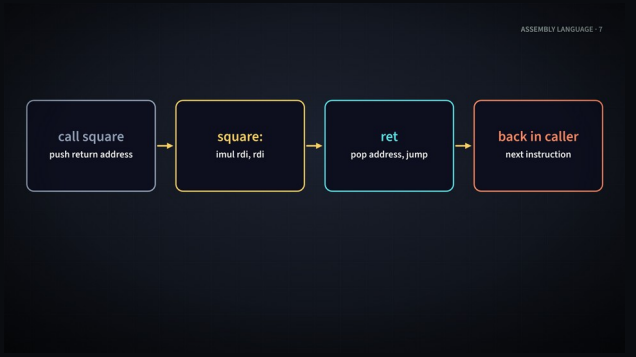
05

Lesson Map


1
What Is the Stack?
2
push and pop
3
call and ret
4
Stack Frames
5
Stack Bugs

Sources and Further Reading





Thank you for watching

MyWebUniversity.com

Free technical education since 2000 — English and Dari

@MyWebUniversity · @MyWebUniversity-Dari