Intro to Binary Exploitation

Nathan Huckleberry

University of Texas at Austin

September 30, 2020

Table of Contents

Table of Contents

What is Computer Architecture?

- Computer Architecture involves instruction set architecture design, microarchitecture design, logic design, and implementation

What is Computer Architecture?

- Assembly and circuits

Table of Contents

Vocabulary

- **Assembly:** Overall term for all low level human-"readable" code.
- **Instruction Set Architecture (ISA):** A specific assembly language
- **Machine Code:** Low level machine-readable code.
- **Register:** Tiny storage on CPU. Stores integers.
- **Memory:** Bigger storage in RAM. Stores strings, data structures, etc.

Common ISA

- x86-64/amd64
- arm64/aarch64
- mips64
- x86/i386
- arm32

Interesting Programs

Interesting programs generally consist of:

- Doing stuff
- Having stuff

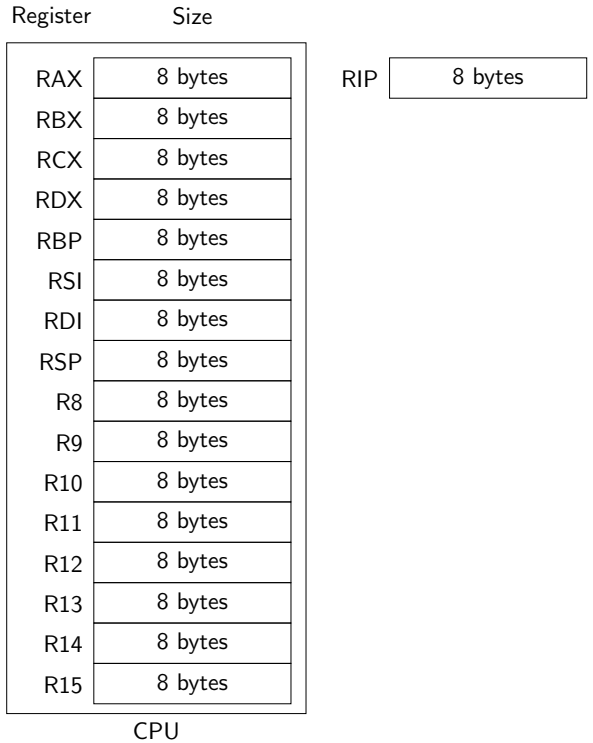
Interesting Programs

Interesting programs generally consist of:

- Executing instructions
- Using variables

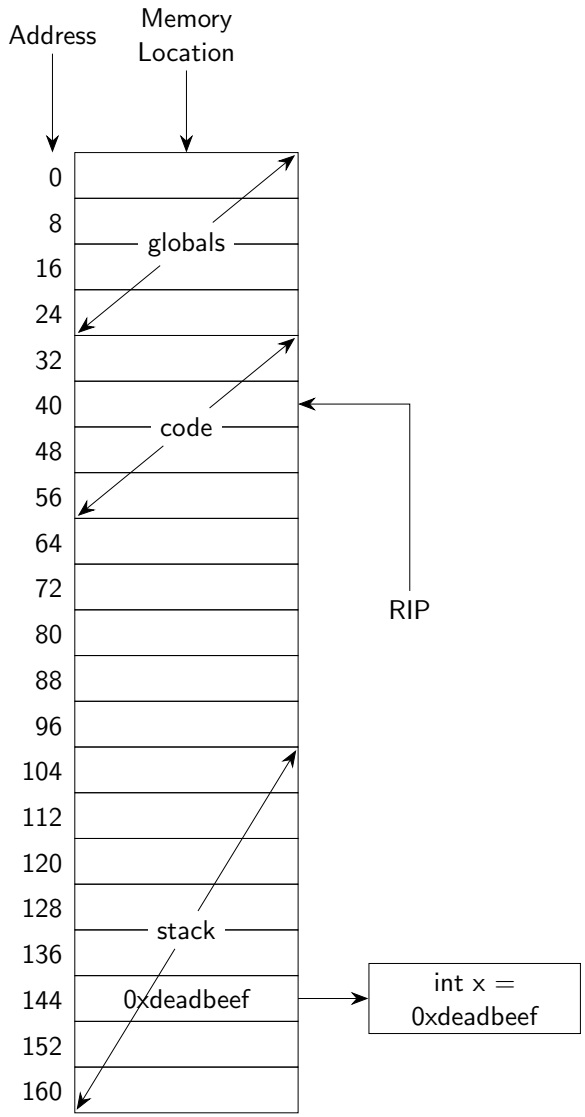
Registers

- Stores integer data.
- Only 16 Registers.
- Many have special purposes.
- Not much room for program variables, data structures etc.
- Where to find variables.
- What instruction to run next.



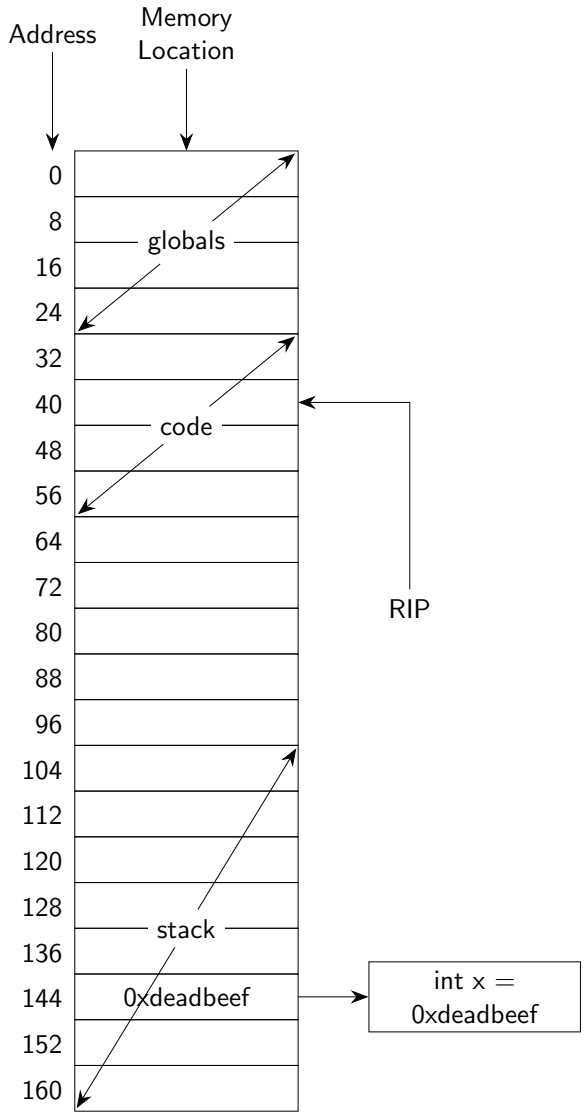
Memory

- Memory can be thought of as a big byte array.
- Pointers are just indexes into this array.
- Pointers are commonly referred to as "addresses".



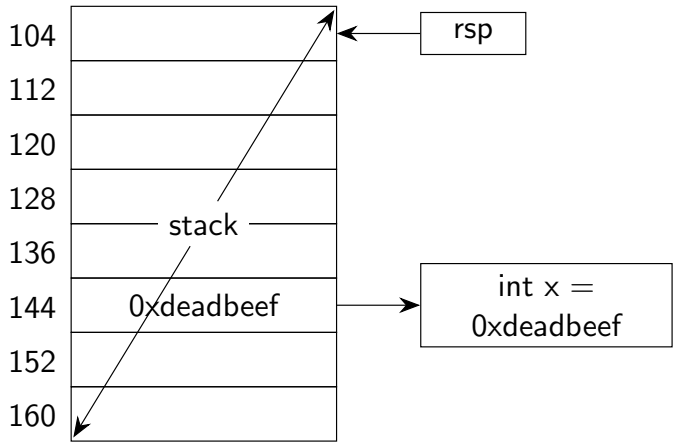
Memory

- Memory stores 99% of variables.
- The actual machine code is stored in memory.
- The registers RIP, RBP and RSP are pointers into memory
- RIP keeps track of what instruction should be executed next.
- RBP and RSP keep track of memory on the stack.



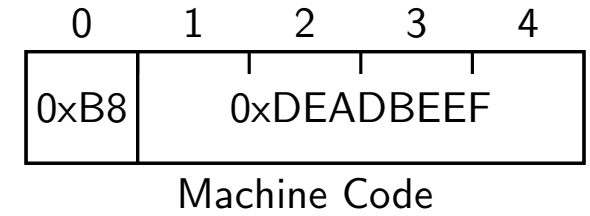
Stack

- Function variables and writable data live in the stack.
- The stack grows and shrinks while the program runs.
- The stack grows towards smaller addresses.
- RSP points to top of the stack.



Machine Code

- Code is represented as bytes in memory.
- The numerical value of the bytes tells the cpu what to do.



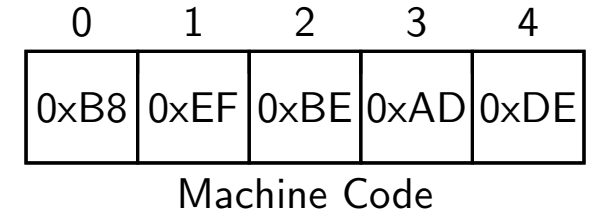
Machine Code

```
mov eax, 0xdeadbeef
```

Assembly

Machine Code

- Code is represented as bytes in memory.
- The numerical value of the bytes tells the cpu what to do.
- Most architectures are little endian so bytes show up backwards



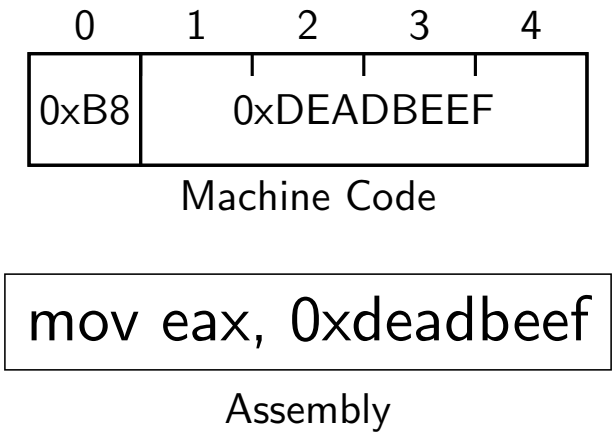
Machine Code

```
mov eax, 0xdeadbeef
```

Assembly

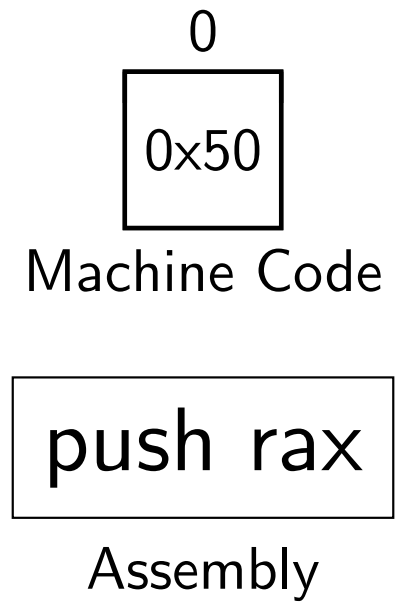
Mov Instruction

- Move immediate value into register.



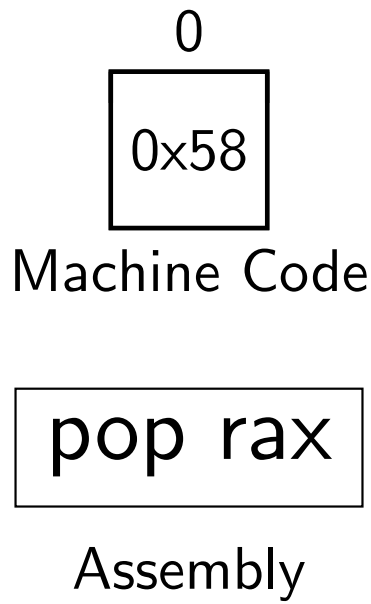
Push Instruction

- Decrement rsp by 8.
- Store the value in rax into memory at rsp.



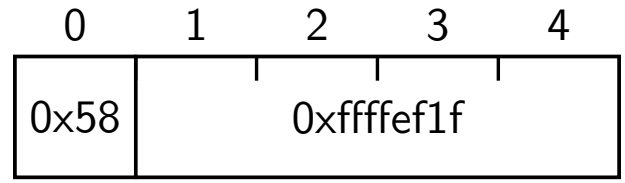
Pop Instruction

- Load the value in memory at rsp into rax.
- Increment rsp by 8.



Call Instruction

- Push rip onto stack
- Jump to call address



Machine Code

```
call <square>
```

Assembly

Ret Instruction

- Pop into rip
- Continue execution at rip

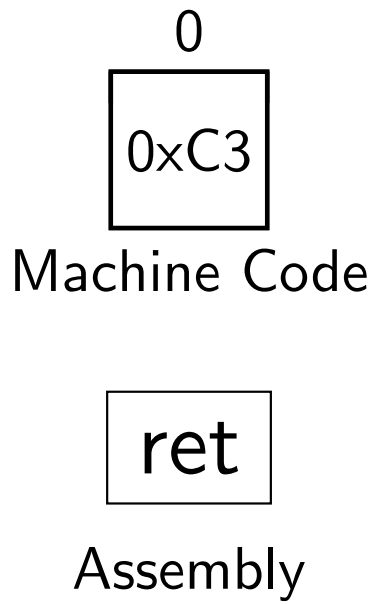


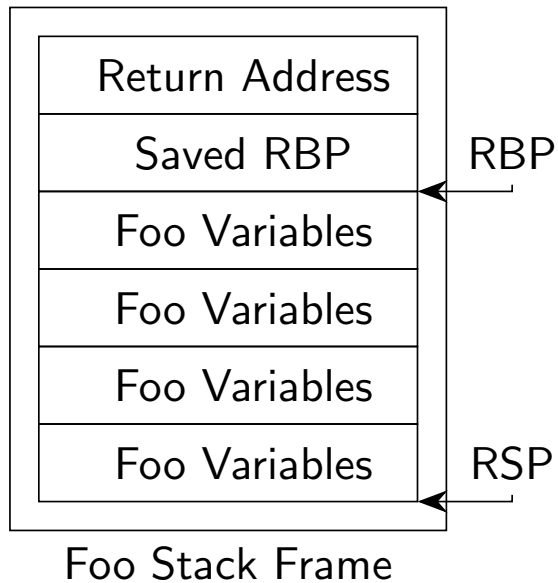
Table of Contents

Functions

- Functions are almost completely self contained in stack frames.
- Variables for the current function and some extra function metadata is stored in the stack frame.

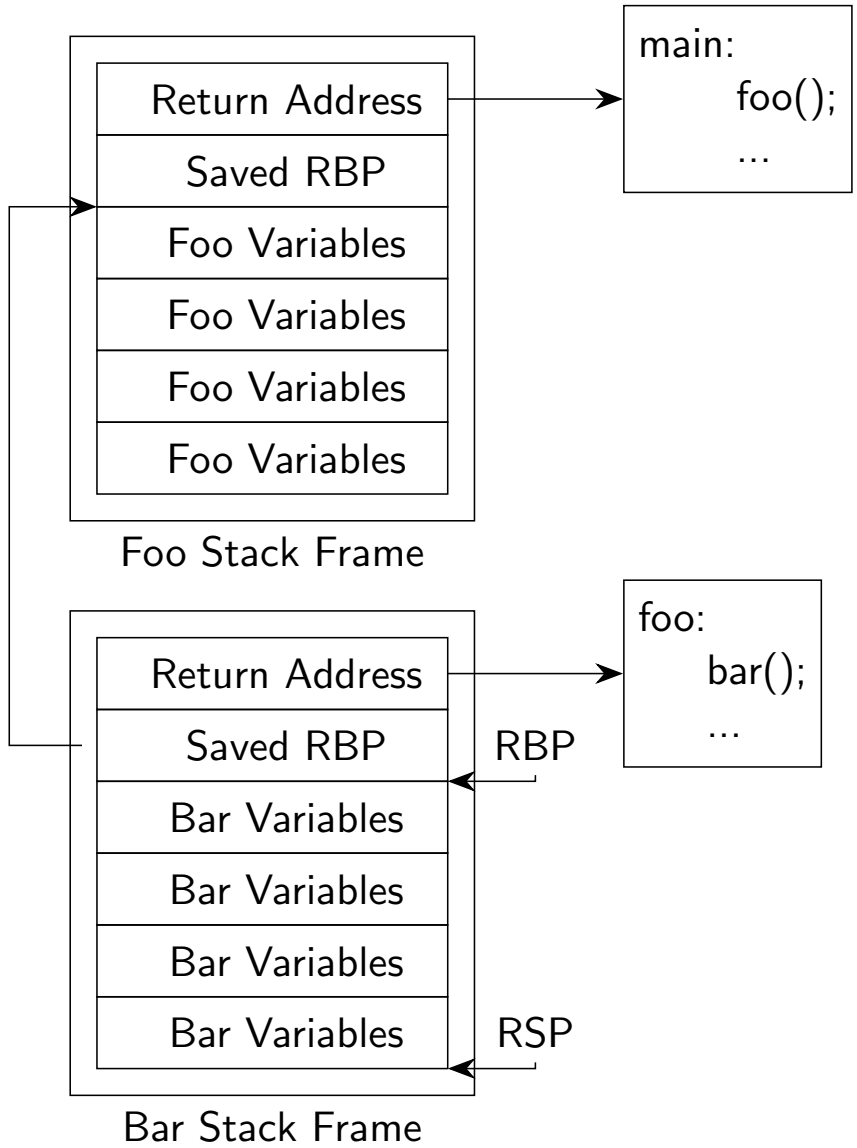
Stack Frames

- Store variables for current function.
- Function metadata before stack frame base.



Stack Frames

- Store variables for current function.
- Function metadata before stack frame base.
- Stack frames are defined in the function prologue.



Stack Frames

Listing 1: go.c

```
1  int multiply(int x, int y) {
2      puts("multiplying..\n");
3      return x*y;
4  }
```

Listing 2: x86-64 go.o

```
1  .LC0:
2      .string "multiplying..\n"
3
4  multiply(int, int):
5      push rbp
6      mov rbp, rsp
7      sub rsp, 16
8      mov DWORD PTR [rbp-4], edi
9      mov DWORD PTR [rbp-8], esi
10     mov edi, OFFSET FLAT:.LC0
11     call puts
12     mov eax, DWORD PTR [rbp-4]
13     imul eax, DWORD PTR [rbp-8]
14     leave
15     ret
```

Calling Convention

- Arguments passed through rdi, rsi, rdx, rcx, r8, r9
- 7th and onward arguments are passed through the stack
- Return value put in rax

Listing 3: x86-64 go.o

```
1  main:
2      push rbp
3      mov rbp, rsp
4      mov esi, 4
5      mov edi, 5
6      call multiply(int, int)
7      mov eax, 0
8      pop rbp
9      ret
```

Table of Contents

Strings in C

- Strings in C are represented as arrays of characters.
- There is no bounds checking when accessing arrays.
- We can read and write out of array bounds in C.

Listing 4: x86-64 go.o

```
1 void user_input() {
2     char x[50];
3     gets(x);
4 }
```

Vulnerable functions

Listing 5: Man Page For gets

```
1 Never use gets(). Because it is impossible to tell without
2 knowing the data in advance how many characters gets()
3 will read, and because gets() will continue to store
4 characters past the end of the buffer, it is extremely
5 dangerous to use. It has been used to break computer
6 security. Use fgets() instead.
```

Overwriting Sensitive Data

Listing 6: x86-64 go.o

```
1  user_input:
2      push rbp
3      mov rbp, rsp
4      sub rsp, 64
5      lea rax, [rbp-64]
6      mov rdi, rax
7      mov eax, 0
8      call gets
9      nop
10     leave
11     ret
```

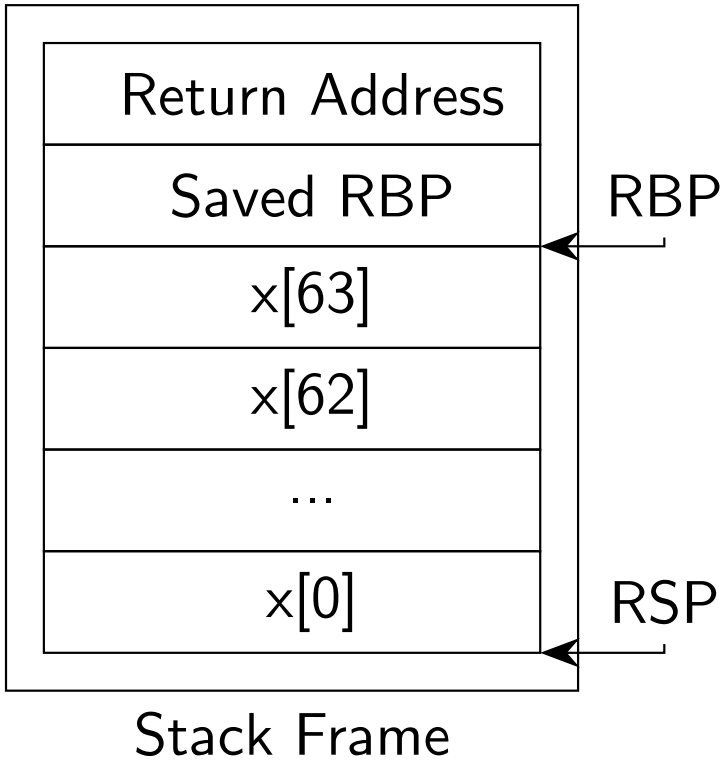
Listing 7: x86-64 go.o

```
1  void user_input() {
2      char x[50];
3      gets(x);
4  }
```

Overwriting Sensitive Data

Listing 8: x86-64 go.o

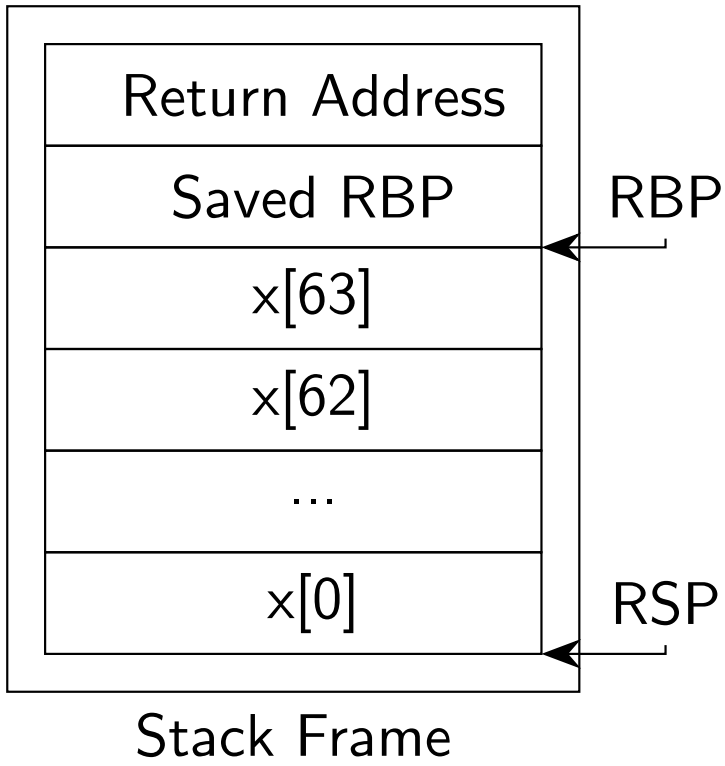
```
1  user_input:
2      push rbp
3      mov rbp, rsp
4      sub rsp, 64
5      lea rax, [rbp-64]
6      mov rdi, rax
7      mov eax, 0
8      call gets
9      nop
10     leave
11     ret
```



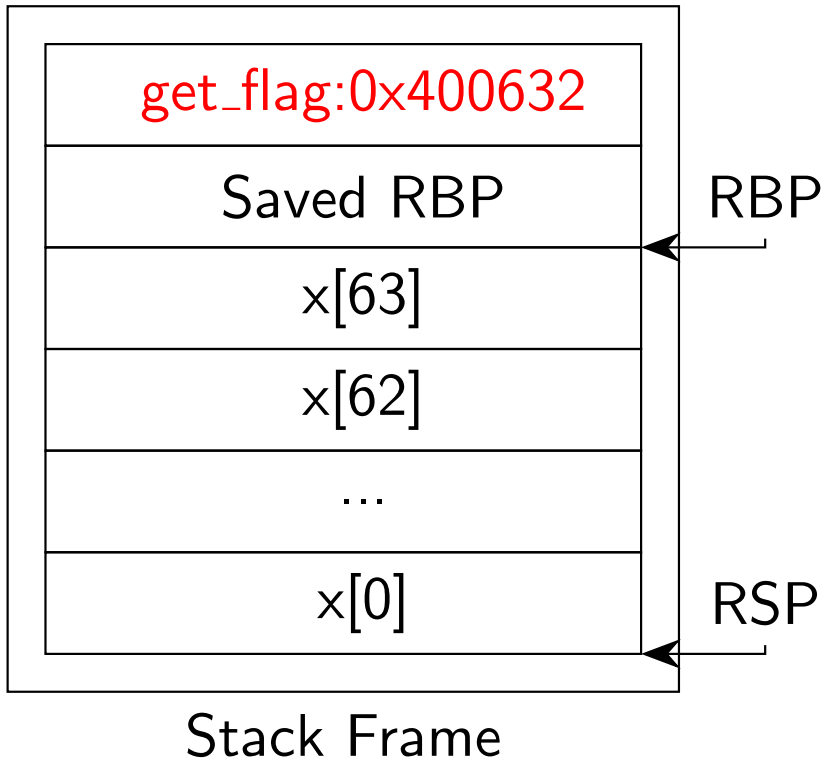
Overwriting Sensitive Data

- Overwriting the return address allows us to redirect program execution.
- When the function returns the program will jump to the address we write.

Stack Frame

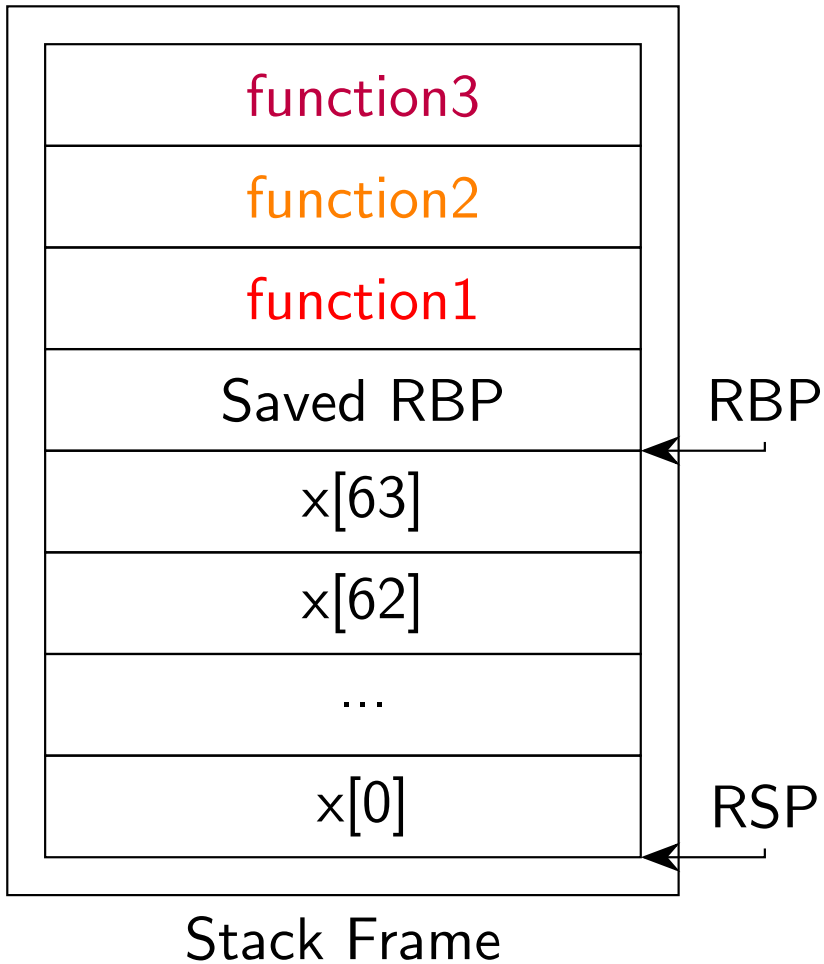


Stack Frame



Stack Frame

- Functions can also be chained together
- This is known as a ROP-chain
- function1 will be called, then function2, then function3



What to overwrite RIP to

- Easy problems have a "get flag" function
- Libc built-in functions like system() are useful
- ROP gadgets
- Jump straight to libc system() using an address leak
- Jump to onegadget in libc using an address leak

ROP Gadgets

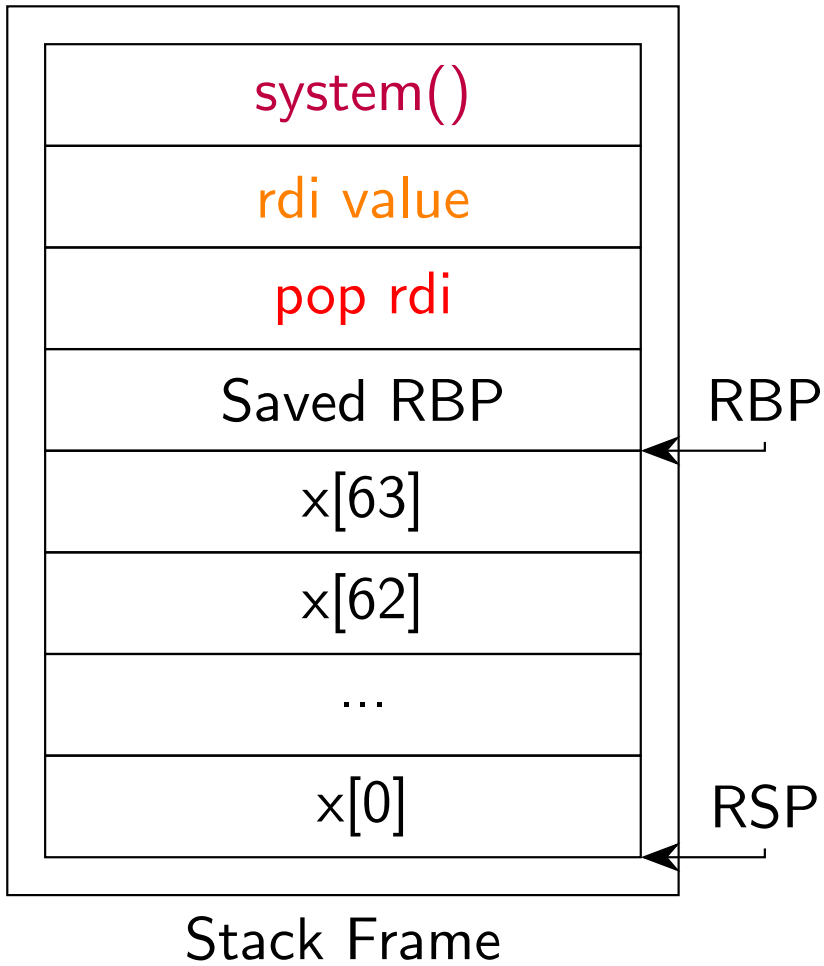
- A short instruction sequence followed by a ret instruction
- Can be put into a ROP-chain the same way as a function
- Pop gadgets are useful for controlling registers

Listing 9: pop rdi gadget

```
1 pop rdi
2 ret
```

ROP Gadgets

- A short instruction sequence followed by a ret instruction
- Can be put into a ROP-chain the same way as a function
- This will call system() with an attacker controlled rdi



ROP Gagets

- Rop gadgets can be found using a tool called ROPGadget

Demo

- nugatory.pwnables.org

Commands to Remember

Listing 10: Commands

```
1 objdump -d prog.o
2 gdb prog.o
3 (python3 -c "print('a'*20)"; cat -) | nc ctf.isss.io 9002
4 ROPGadget --binary pwnable
```