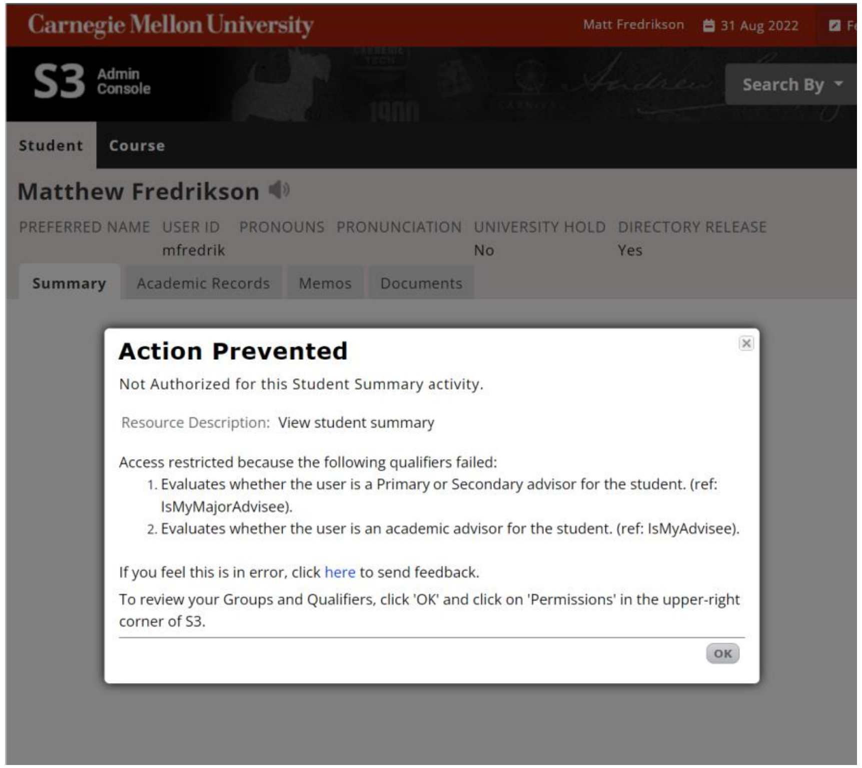
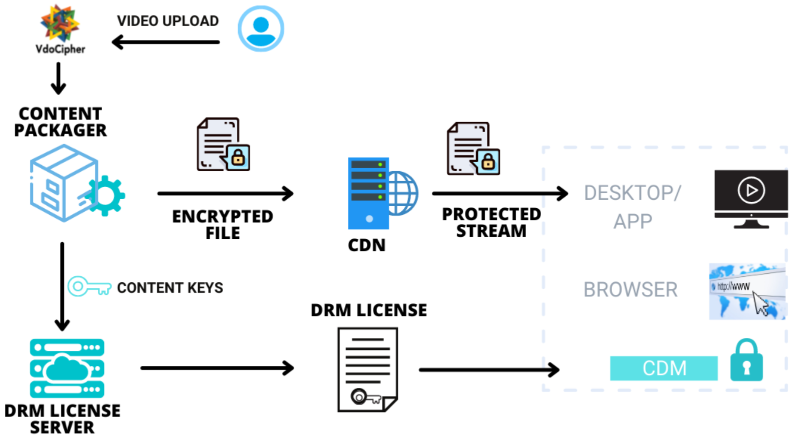
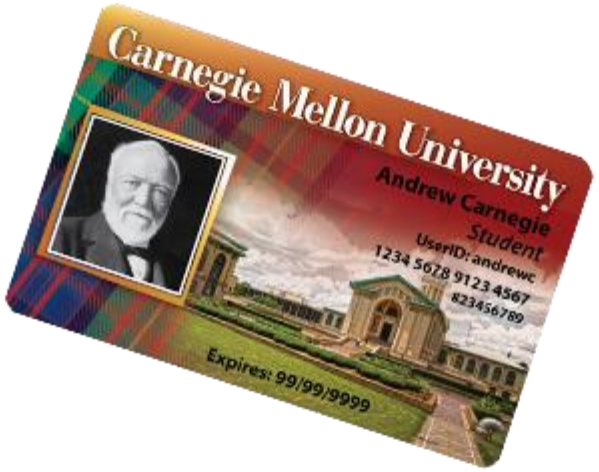
Lecture 2:
Safety & Proof

Policies everywhere







Today's goals

- Introduce safety policies
- Dive deeper into memory safety
- Understand limitations of heuristic defenses
- Formulate a good mitigation

Safety

A class of policies that can *always* be enforced at runtime

Equivalently, policies that prohibit irremediable events

Enforcement means: possible to ensure that unsafe things **never** happen

If the presented student ID is expired, deny entry

Only the student's primary advisor may view their summary

File's owner can read, write, execute, and others can only execute

Allocated memory must eventually be freed

Allocated memory must be freed within 500 cycles

Memory safety

- Goal is to prevent issues like the following:
  - Buffer overflow, over-read
  - Array index out-of-bounds
  - Uninitialized read/dereference, null dereference
  - Invalid page fault
  - Use after free, invalid/double free

Policy: program shouldn't access illegal memory regions

- In many cases, violations result in corrupted state, unstable behavior
- Sometimes they result in exploitable vulnerabilities

- Why is this *safety*?

Recap: Buffer overflow

Occurs when data is <u>written</u> to a location outside of the space allocated for a buffer

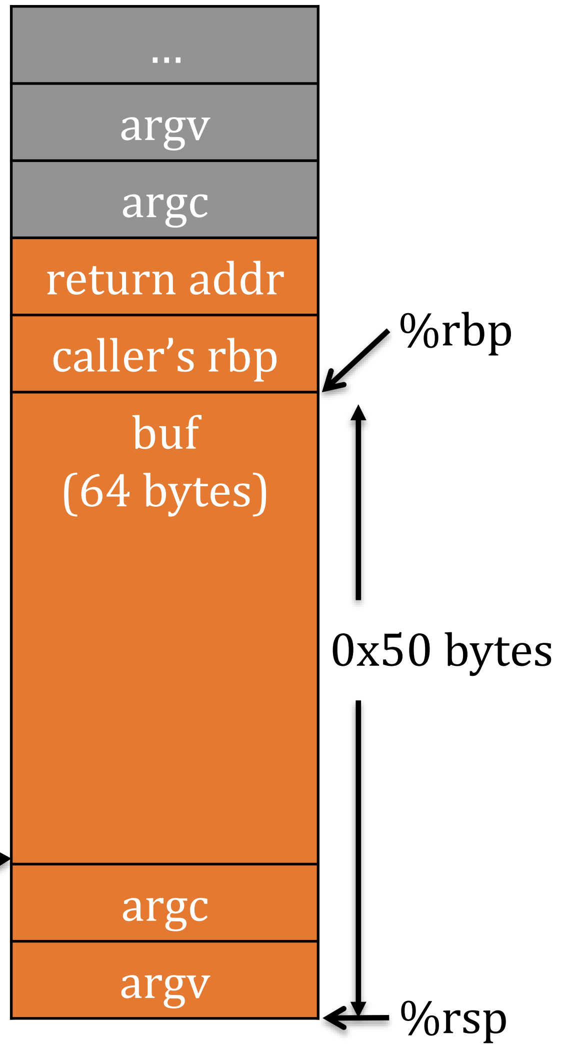
A buffer may be allocated:

- On the stack
  - Covered today
  - Easiest case to exploit
- On the heap
  - Not covered
  - May still be exploitable, but more advanced

Basic Example

```
int main(int argc, char **argv) {
    char buf[64];
    gets(buf);
}
Dump of assembly code for function main:
  4004fd: push   %rbp
  4004fe: mov    %rsp,%rbp
  400501: sub    $0x50,%rsp
  400505: mov    %rdi,-0x48(%rbp)
  400508: mov    %rsi,-0x50(%rbp)
  40050c: lea    -0x40(%rbp),%rax
  400510: mov    %rax,%rdi
  400518: callq  400400 <gets@plt>
  40051d: leaveq
  40051e: retq
```

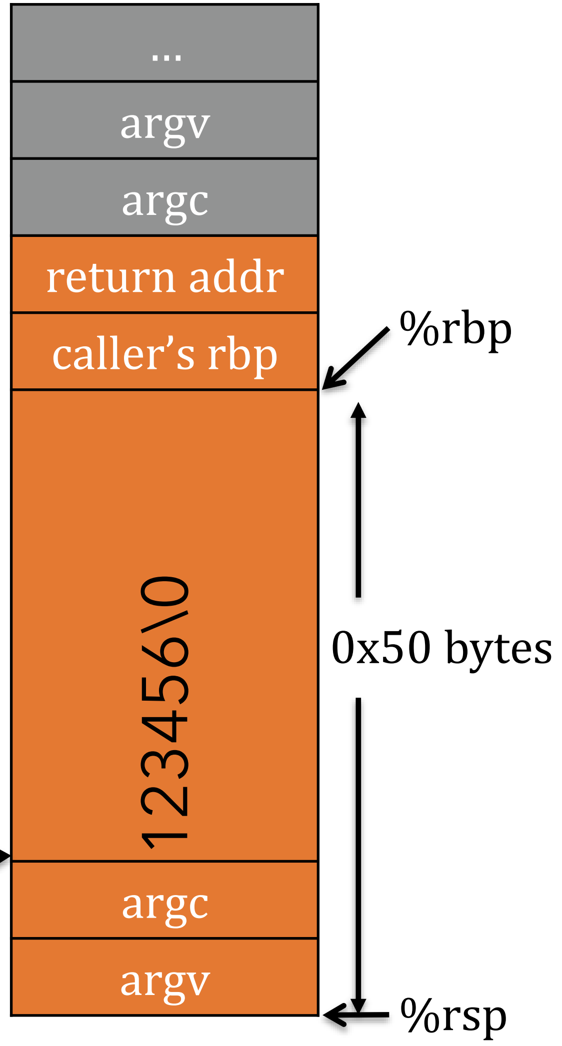
Reg	Value
rax	buf
rdi	buf



“123456”

```
int main(int argc, char **argv) {
    char buf[64];
    gets(buf);
}
Dump of assembly code for function main:
  4004fd: push   %rbp
  4004fe: mov    %rsp,%rbp
  400501: sub    $0x50,%rsp
  400505: mov    %rdi,-0x48(%rbp)
  400508: mov    %rsi,-0x50(%rbp)
  40050c: lea    -0x40(%rbp),%rax
  400510: mov    %rax,%rdi
  400518: callq  400400 <gets@plt>
  40051d: leaveq
  40051e: retq
```

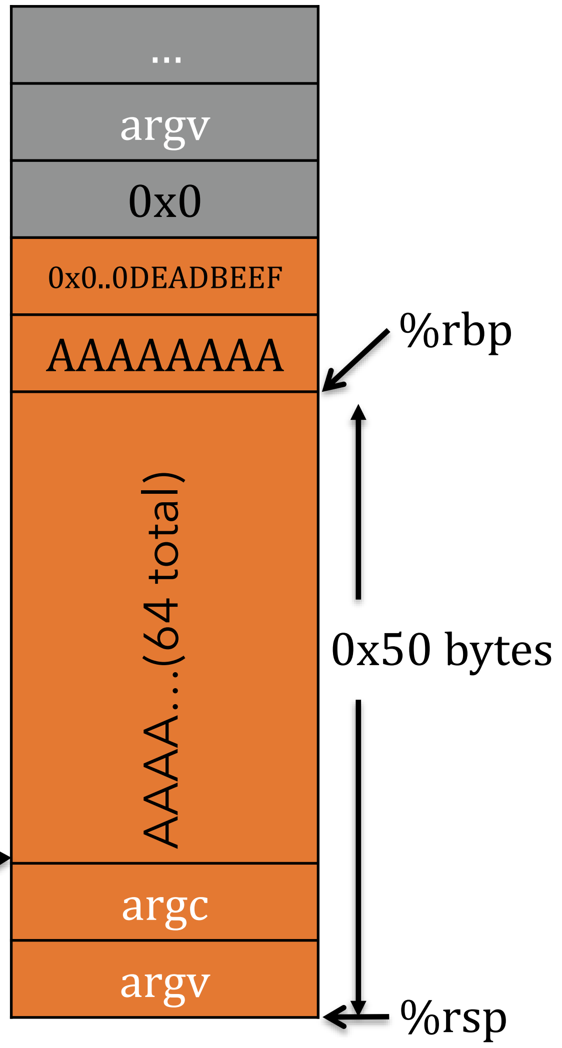
Reg	**Value**
rax	buf
rdi	buf



"A"x72 + "\xEF\xBE\xAD\xDE\x00\x00\x00\x00"

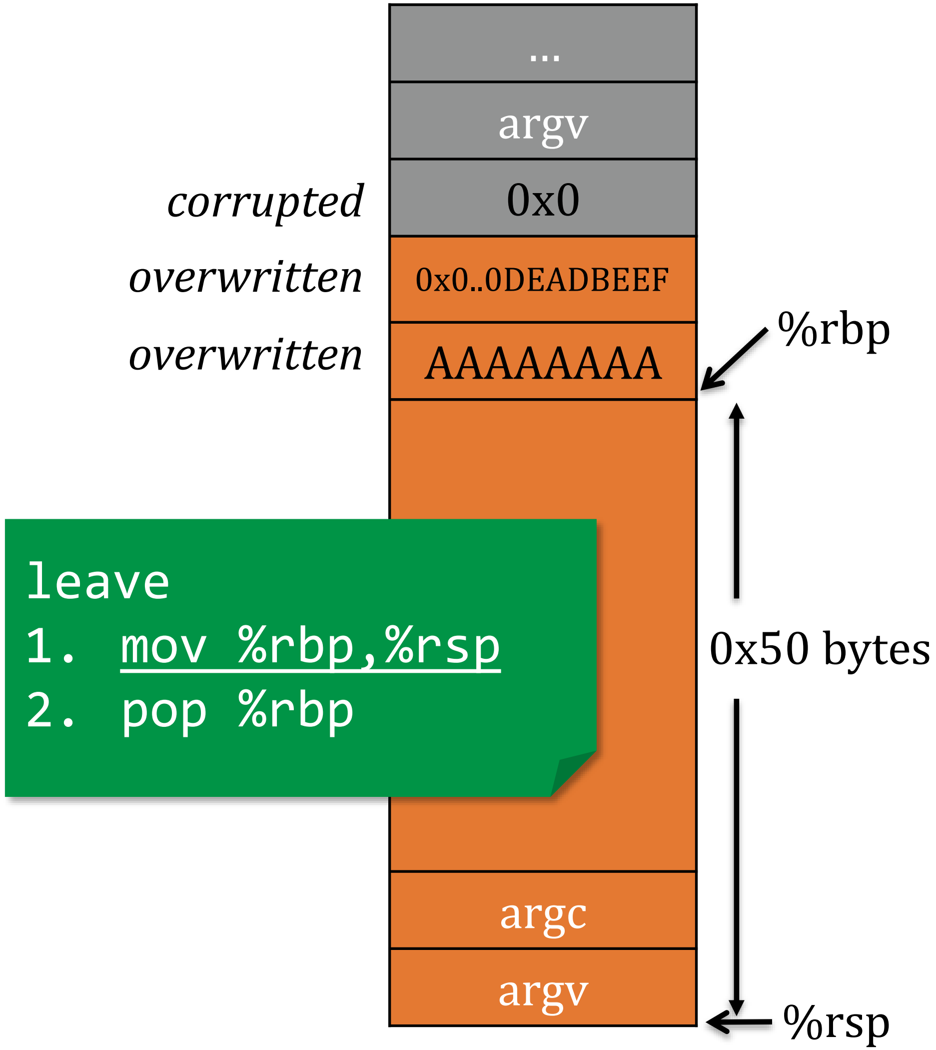
```
int main(int argc, char **argv) {
    char buf[64];
    gets(buf);
}
Dump of assembly code for function main:
  4004fd: push   %rbp
  4004fe: mov    %rsp,%rbp
  400501: sub    $0x50,%rsp
  400505: mov    %rdi,-0x48(%rbp)
  400508: mov    %rsi,-0x50(%rbp)
  40050c: lea    -0x40(%rbp),%rax
  400510: mov    %rax,%rdi
  400518: callq  400400 <gets@plt>
  40051d: leaveq
  40051e: retq
```

Reg	Value
rax	buf
rdi	buf



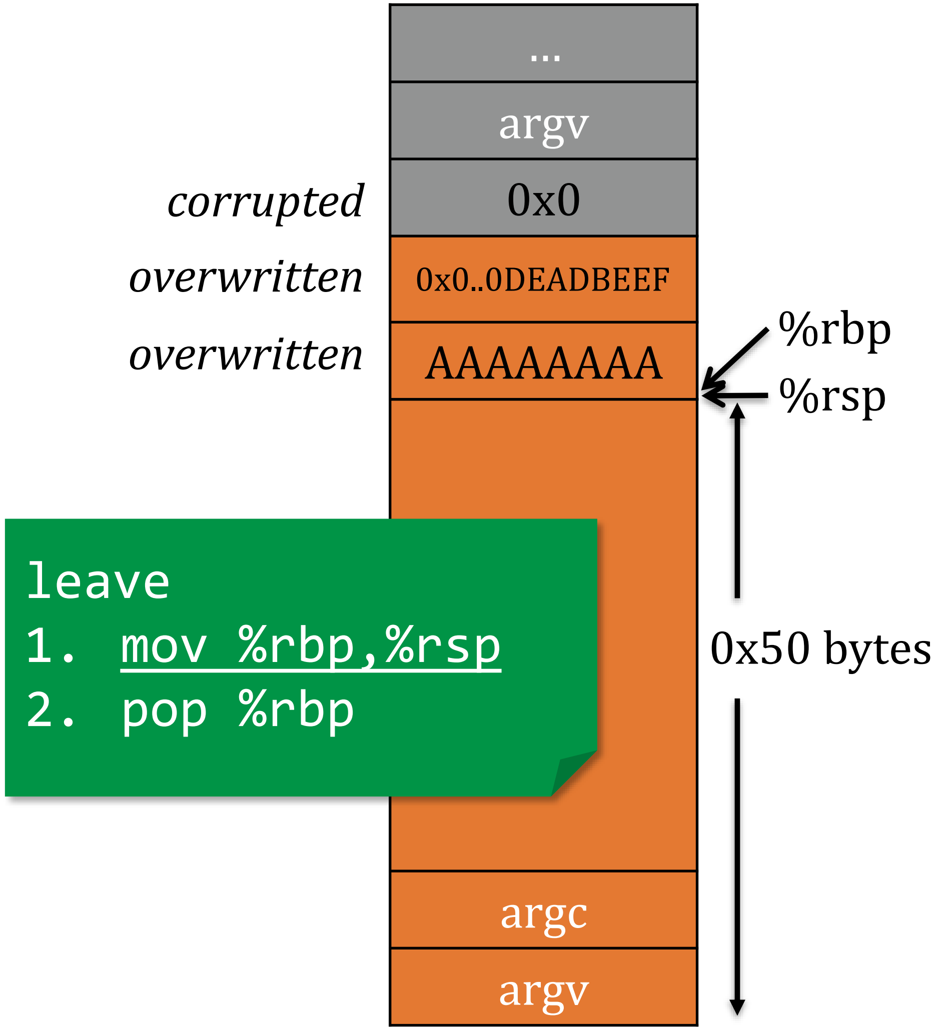
Frame teardown, part 1

```
int main(int argc, char **argv) {
    char buf[64];
    gets(buf);
}
Dump of assembly code for function main:
  4004fd: push   %rbp
  4004fe: mov    %rsp,%rbp
  400501: sub    $0x50,%rsp
  400505: mov    %rdi,-0x48(%rbp)
  400508: mov    %rsi,-0x50(%rbp)
  40050c: lea    -0x40(%rbp),%rax
  400510: mov    %rax,%rdi
  400518: callq  400400 <gets@plt>
  40051d: leaveq
  40051e: retq
```



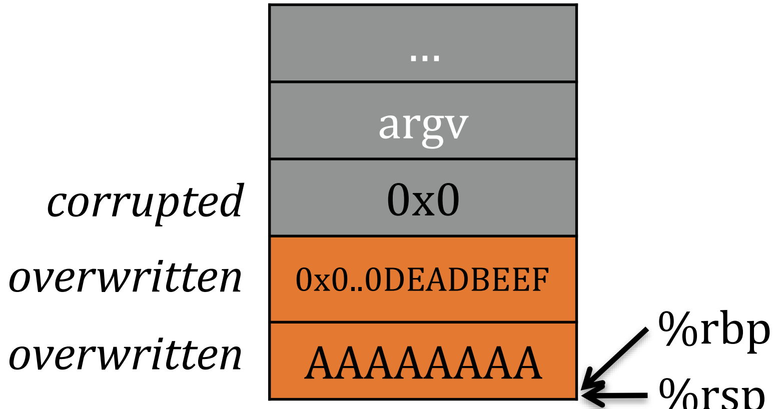
Frame teardown, part 1

```
int main(int argc, char **argv) {
    char buf[64];
    gets(buf);
}
Dump of assembly code for function main:
  4004fd: push   %rbp
  4004fe: mov    %rsp,%rbp
  400501: sub    $0x50,%rsp
  400505: mov    %rdi,-0x48(%rbp)
  400508: mov    %rsi,-0x50(%rbp)
  40050c: lea    -0x40(%rbp),%rax
  400510: mov    %rax,%rdi
  400518: callq  400400 <gets@plt>
  40051d: leaveq
  40051e: retq
```



Frame teardown, part 1

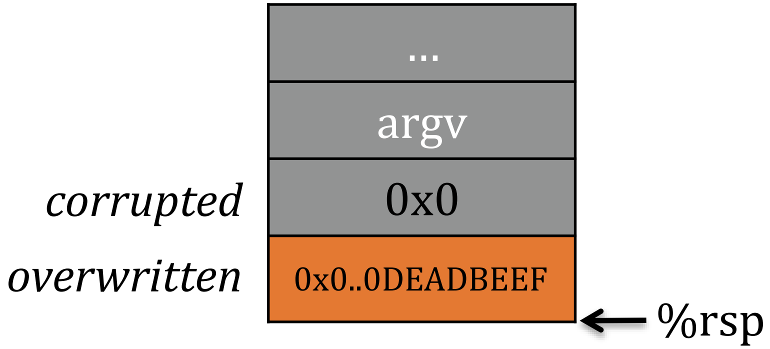
```
int main(int argc, char **argv) {
    char buf[64];
    gets(buf);
}
Dump of assembly code for function main:
  4004fd: push   %rbp
  4004fe: mov    %rsp,%rbp
  400501: sub    $0x50,%rsp
  400505: mov    %rdi,-0x48(%rbp)
  400508: mov    %rsi,-0x50(%rbp)
  40050c: lea    -0x40(%rbp),%rax
  400510: mov    %rax,%rdi
  400518: callq  400400 <gets@plt>
  40051d: leaveq
  40051e: retq
```




```
leave
1. mov %rbp,%rsp
2. pop %rbp
```

Frame teardown, part 2

```
int main(int argc, char **argv) {
    char buf[64];
    gets(buf);
}
Dump of assembly code for function main:
  4004fd: push   %rbp
  4004fe: mov    %rsp,%rbp
  400501: sub    $0x50,%rsp
  400505: mov    %rdi,-0x48(%rbp)
  400508: mov    %rsi,-0x50(%rbp)
  40050c: lea    -0x40(%rbp),%rax
  400510: mov    %rax,%rdi
  400518: callq  400400 <gets@plt>
  40051d: leaveq
  40051e: retq
```

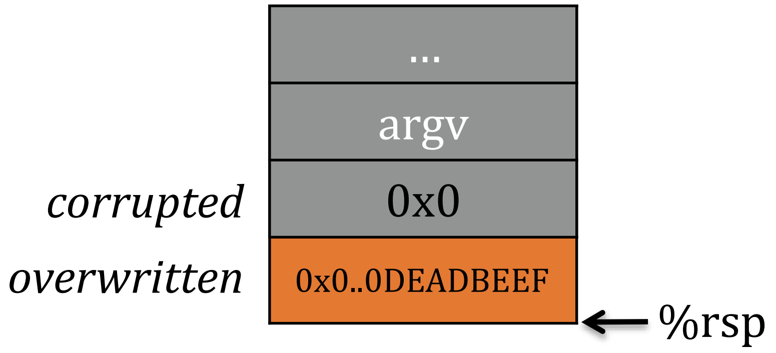


%rbp = AAAAAAAA

```
leave
1.  mov %rbp,%rsp
2.  pop %rbp
```

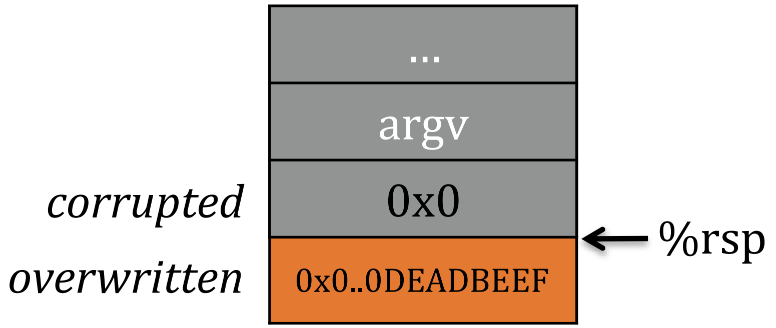
Frame teardown, part 3

```
int main(int argc, char **argv) {
    char buf[64];
    gets(buf);
}
Dump of assembly code for function main:
  4004fd: push   %rbp
  4004fe: mov    %rsp,%rbp
  400501: sub    $0x50,%rsp
  400505: mov    %rdi,-0x48(%rbp)
  400508: mov    %rsi,-0x50(%rbp)
  40050c: lea    -0x40(%rbp),%rax
  400510: mov    %rax,%rdi
  400518: callq  400400 <gets@plt>
  40051d: leaveq
  40051e: retq
```



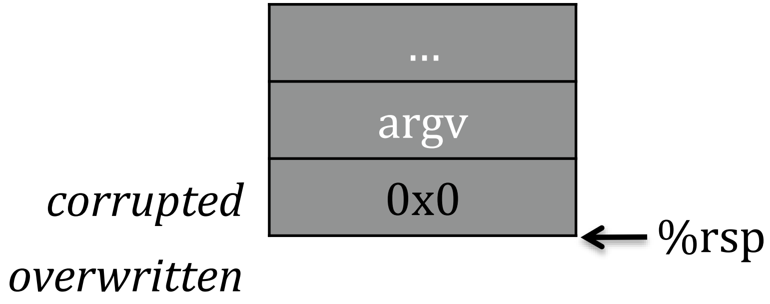
Frame teardown, part 3

```
int main(int argc, char **argv) {
    char buf[64];
    gets(buf);
}
Dump of assembly code for function main:
  4004fd: push   %rbp
  4004fe: mov    %rsp,%rbp
  400501: sub    $0x50,%rsp
  400505: mov    %rdi,-0x48(%rbp)
  400508: mov    %rsi,-0x50(%rbp)
  40050c: lea    -0x40(%rbp),%rax
  400510: mov    %rax,%rdi
  400518: callq  400400 <gets@plt>
  40051d: leaveq
  40051e: retq
```



Frame teardown, part 3

```
int main(int argc, char **argv) {
    char buf[64];
    gets(buf);
}
Dump of assembly code for function main:
  4004fd: push   %rbp
  4004fe: mov    %rsp,%rbp
  400501: sub    $0x50,%rsp
  400505: mov    %rdi,-0x48(%rbp)
  400508: mov    %rsi,-0x50(%rbp)
  40050c: lea    -0x40(%rbp),%rax
  400510: mov    %rax,%rdi
  400518: callq  400400 <gets@plt>
  40051d: leaveq
  40051e: retq
```



`%rip = 0x00000000DEADBEEF`

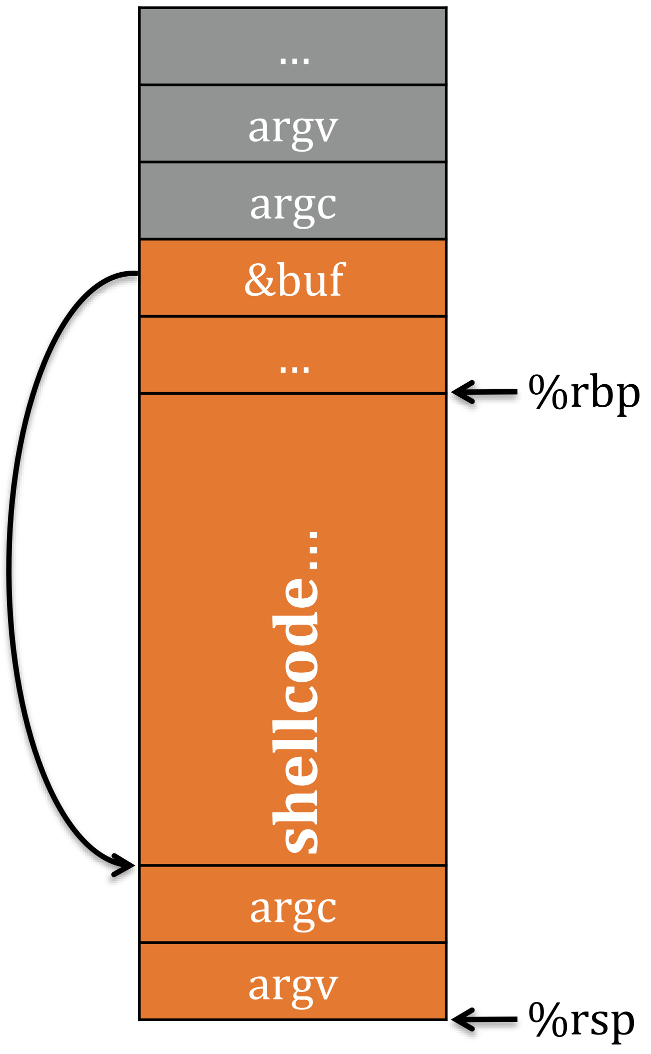
(probably crash)

Shellcode

Traditionally, we inject assembly instructions for `exec("/bin/sh")` into buffer.

- see "*Smashing the stack for fun and profit*" for exact string
- or search online

```
…
0x080483fa <+22>: call   0x8048300 <gets@plt>
0x080483ff <+27>: leave
0x08048400 <+28>: ret
```

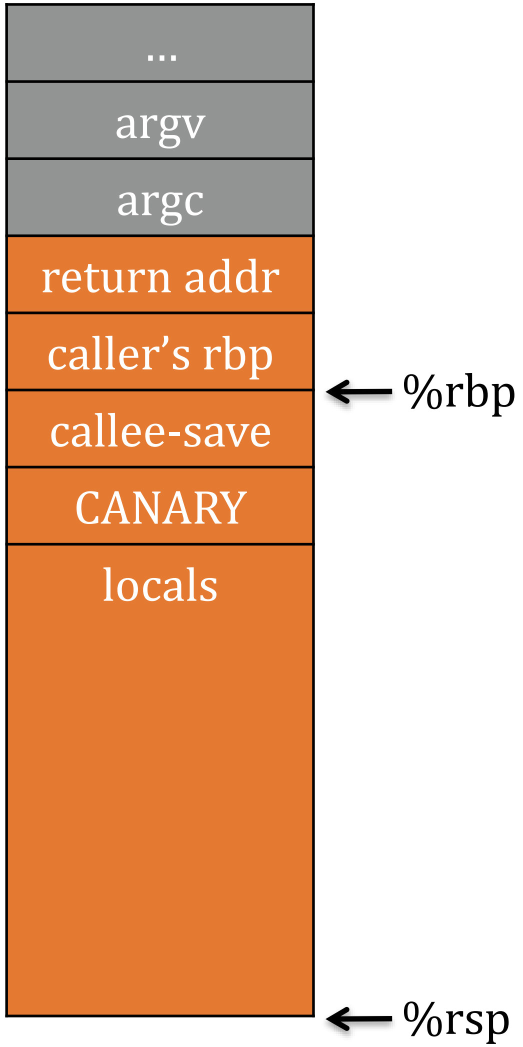


Defenses

StackGuard [Cowen et al. 1998]

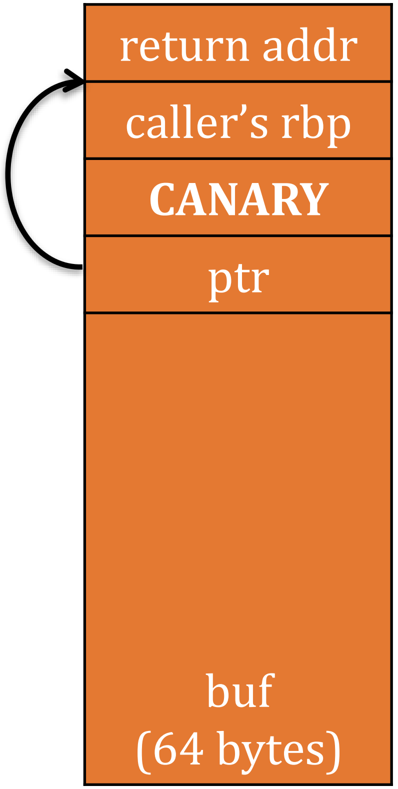
Key idea: insert a unique identifier ("canary") just below the saved return address

- Function prologue inserts a random value below callee-save registers, above locals
- Epilogue checks the value before returning
- Terminate if the canary doesn't match!



Data Pointer Subterfuge

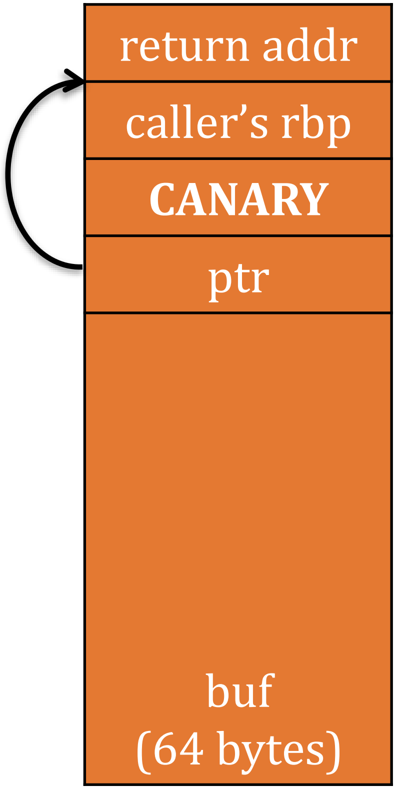
```
int *ptr;
char buf[64];
memcpy(buf, user1);
*ptr = user2;
```



Data Pointer Subterfuge

```
int *ptr;
char buf[64];
memcpy(buf, user1);
*ptr = user2;
```

First overwrite *ptr* to point to saved return address

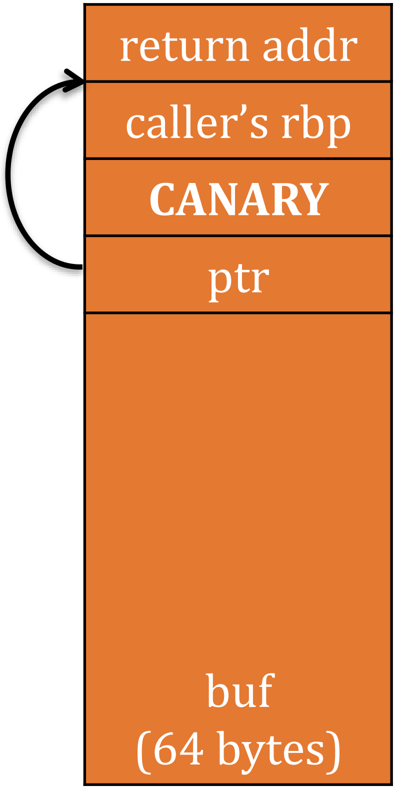


Data Pointer Subterfuge

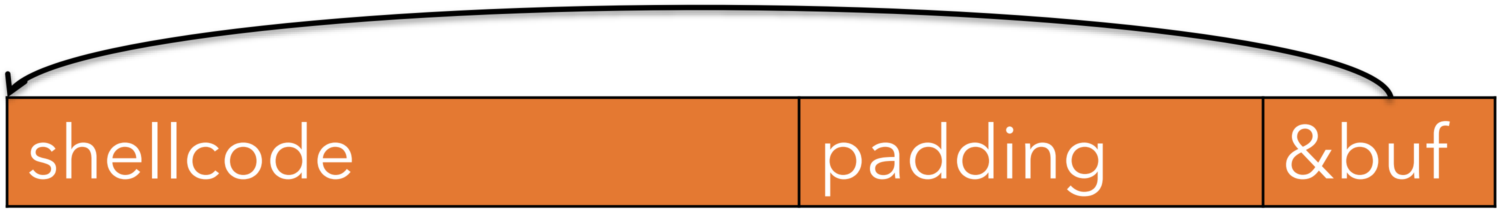
```
int *ptr;
char buf[64];
memcpy(buf, user1);
*ptr = user2;
```

First overwrite *ptr* to point to saved return address

Then modify return address via *ptr*



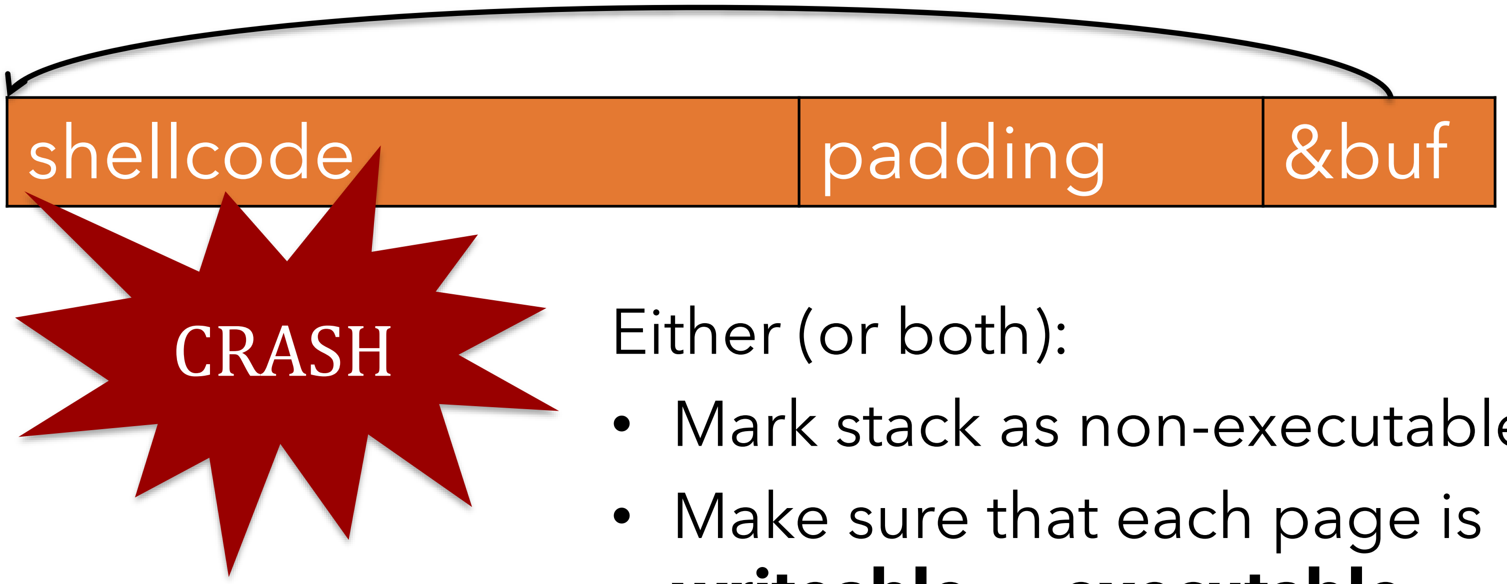
Memory protection



Either (or both):

- Mark stack as non-executable
- Make sure that each page is **writeable** *or* **executable**, exclusively

Memory protection



Either (or both):

- Mark stack as non-executable
- Make sure that each page is **writeable** *or* **executable**, exclusively

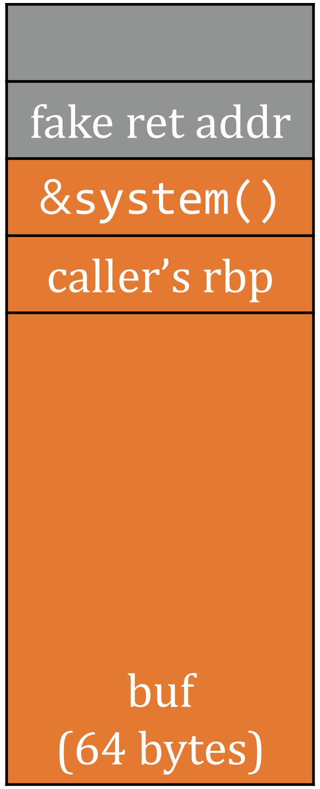
Bypassing memory protection

Set return address to code that's already marked executable!

Fertile ground: libc

- More difficult with register-based calling conventions
- Typically done via register-loading "gadgets"

Main point: no injected code



Layout randomization (ASLR)

Recall: Our exploit needs a concrete address

True of both stack-based and return-to-libc:

- Location of shell code
- Library addresses, gadget offsets

Vulnerability (partially) due to fixed memory layout

Solution: Randomize the layout!

ASLR

Base address a

Program

- Code
- Uninitialized data
- Initialized data

Base address b

Mapped

- Heap
- Dynamic libraries
- Thread stacks
- Shared Memory

Base address c

Stack

- Main stack

ASLR

a + 16 bit rand r_1 | **b + 16 bit rand r_2** | **c + 24 bit rand r_3**

Program

- Code
- Uninitialized data
- Initialized data

Mapped

- Heap
- Dynamic libraries
- Thread stacks
- Shared Memory

Stack

- Main stack

How to attack ASLR

Attack

- **Brute Force**
- **Non-randomized memory**
  - ret2text
  - Func ptr
- **Stack Juggling**
  - ret2ret
  - ret2pop
- **GOT Hijacking**
  - ret2got

Recap

Memory safety (esp. buffer overflow) issues cause vulnerability

There are a wide range of *heuristic* defenses

- Canaries → pointer subterfuge
- Memory protection → return-to-libc
- ASLR → pick your favorite attack

Why not just enforce memory safety?

Basic Example, revisited

```
int main(int argc, char **argv) {
    char buf[64];
    fgets(buf, 64, stdin);
}
```

How do we know that this is actually safe?

```
char* fgets(char* s, int n, FILE *iop) {
    register int c;
    register char* cs;
    cs = s;
    while(--n > 0 && (c = getc(iop)) != EOF)
    {
        if((*cs++ = c) == '\n')
        break;
    }

    *cs = '\0';
    return (c == EOF && cs == s) ? NULL : s;
}
```

How do we know that *this* is actually safe?

Basic Example, revisited

```
char* fgets(char* s, int n, FILE *iop)
//@requires 0 <= n && 0 < s
{
    register int c;
    register char* cs;
    cs = s;
    while(--n > 0 && (c = getc(iop)) != EOF)
    //@loop_invariant 0 < cs && cs – s <= n
    {
        if((*cs++ = c) == '\n')
        break;
    }

    *cs = '\0';
    return (c == EOF && cs == s) ? NULL : s;
}
```