Review OS (Buffer Overflow)

CS461 / ECE422 – UIUC Spring 2018

By Kaishen Wang

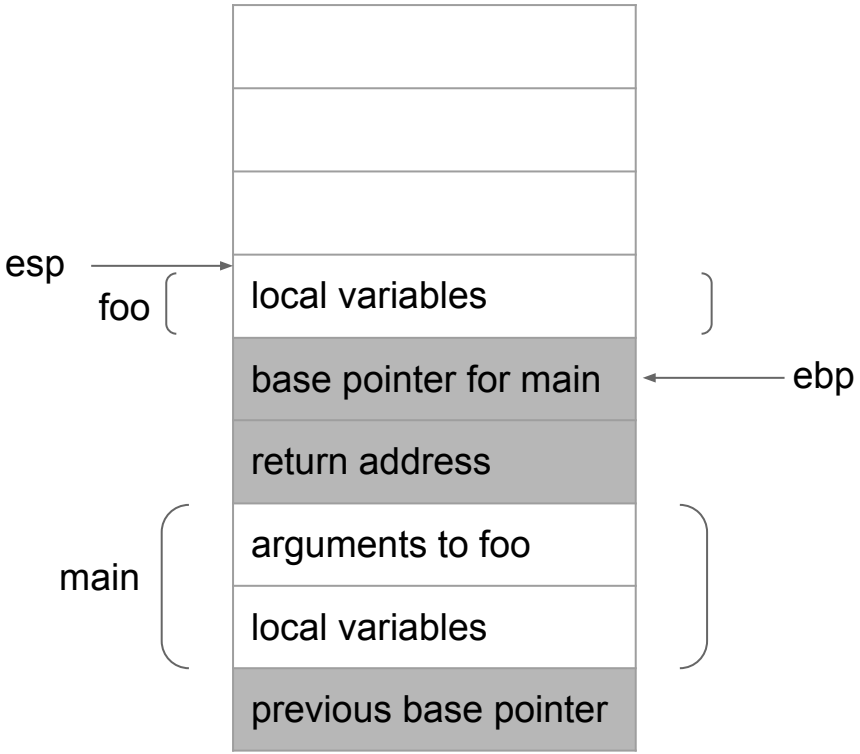
Outline

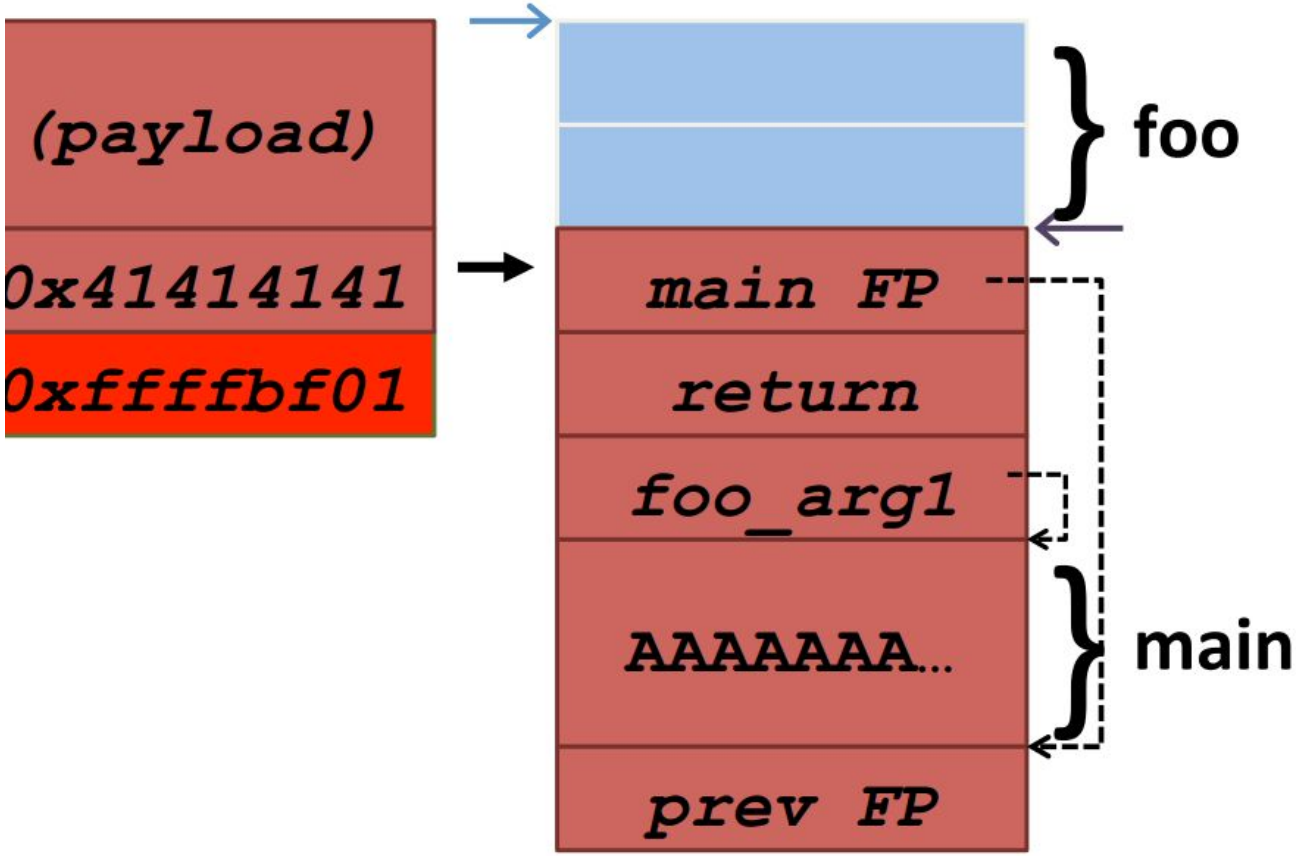
- General Idea
- Defense
- Other attacks
- Tips for midterm

Stack Frame

example: *main* calls *foo*

1. Do stuff in *main*
2. Set up arguments to call *foo*
3. Set up stack frame for *foo*
4. Do stuff in *foo*




(payload)
0x41414141
0xffffbf01
main FP
return
foo_arg1
AAAAAAA…
prev FP
foo
main

What to do?

Bounds checking:

strcpy, gets, strncpy

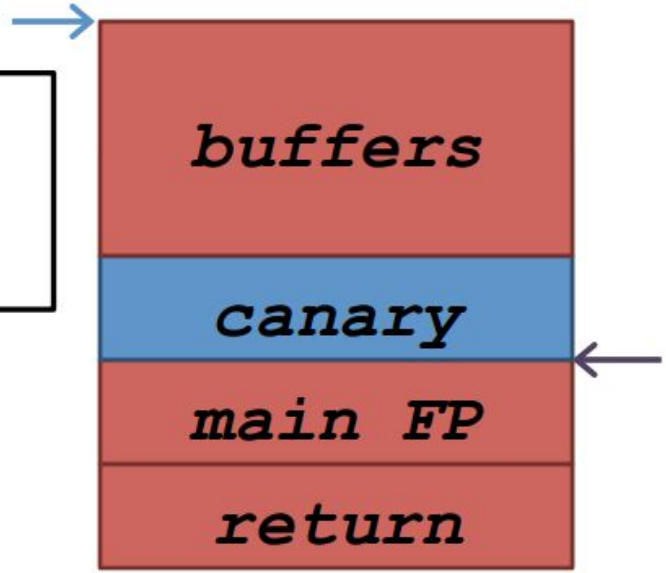
Defenses

Stack Canary

Stack canaries

```
# on function call:

canary = secret
```



Defenses

Stack Canary

DEP

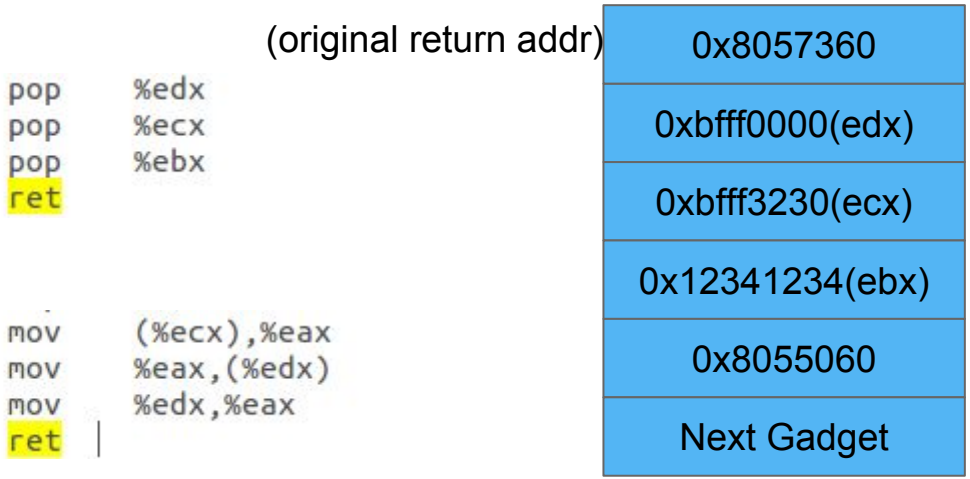
No eXecute (aka W^X aka DEP aka…)

- Mark pages as EITHER
  - Read/write (stack/heap)
  - Executable (.text/code segments)
  - (never both)
- Requires hardware support
- Attacker cannot return to stack

Return-Oriented Programming

```
8057360:      5a                pop    %edx
8057361:      59                pop    %ecx
8057362:      5b                pop    %ebx
8057363:      c3                ret
```

```
8055060:      8b 01             mov    (%ecx),%eax
8055062:      89 02             mov    %eax,(%edx)
8055064:      89 d0             mov    %edx,%eax
8055066:      c3                ret
```



Defenses

Stack Canary

DEP

ASLR

Address Space Layout Randomization

- Virtual Address Space: 4GB+
- Stack/code size: ~10 MB
- Randomize offsets

Some other attacks:

Integer overflow

```
void foo(int *array, int len) {
  int *buf;
  buf = malloc(len * sizeof(int));
  if (!buf)
     return;

  int i;
  for (i=0; i<len; i++) {
     buf[i] = array[i];
  }
}
```

1.2.11 Format String Attack

%n

Proto-answer: print malicious_code + padding + ADDR1 + ADDR2 + “%00000x%04$hn%00000x%05$hn”

Tips for reviewing midterm (for MP1 related question):

When looking at MP1, make sure

- you are familiarize with all the calling conventions
- you understand the approach to all problems
- you understand and be able to write the assembly code

When looking at previous midterms, make sure

- you know the answers to all questions