Low-level Software Security: Attacks and Countermeasures

Prof. Frank PIESSENS

These slides are based on the paper: “Low-level Software Security by Example” by Erlingsson, Younan and Piessens
Overview

• Introduction
• The attacker-defender race
  o Attack 1: Stack-based buffer overflow
  o Defense 1: Stack canaries
  o Attack 2: Heap-based buffer overflow
  o Defense 2: Non-executable data
  o Attack 3: Return-to-libc attacks
  o Defense 3: Layout randomization
• Advanced attacks and defenses
• Other defenses
• Conclusion
Introduction

• *Memory corruption vulnerabilities* are a class of vulnerabilities relevant for *unsafe* languages
  o i.e. Languages that do not check whether programs access memory in a correct way
  o Hence buggy programs may mess up parts of memory used by the language run-time

• In these lectures we will focus on memory corruption vulnerabilities in C programs
  o These can have *devastating* consequences
Example vulnerable C program

```c
#include <stdio.h>
int main() {
    int cookie = 0;
    char buf[80];
    gets(buf); // reads chars until EOL
    if (cookie == 0x41424344) {
        printf("you win!\n");
    }
}
```
Example vulnerable C program

```c
#include <stdio.h>

int main() {
    int cookie;
    char buf[80];
    gets(buf);  // reads chars until EOL
}
```
Background:
Memory management in C

• Memory can be allocated in many ways in C
  o Automatic (local variables in functions)
  o Static (global variables)
  o Dynamic (malloc and new)

• Programmer is responsible for:
  o Appropriate use of allocated memory
    • E.g. bounds checks, type checks, …
  o Correct de-allocation of memory
### Process memory layout

<table>
<thead>
<tr>
<th>High addresses</th>
<th>Low addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Program Code</strong></td>
<td><strong>Arguments/ Environment</strong></td>
</tr>
<tr>
<td><strong>Stack</strong></td>
<td><strong>Unused and Mapped Memory</strong></td>
</tr>
<tr>
<td><strong>Heap (dynamic data)</strong></td>
<td><strong>Static Data</strong></td>
</tr>
</tbody>
</table>

Stack grows down

Heap grows up
Memory management in C

• Memory management is very error-prone
• Some typical bugs:
  o Writing past the bound of an array
  o Dangling pointers
  o Double freeing
  o Memory leaks
• For efficiency, practical C implementations don’t detect such bugs at run time
  o The language definition states that behavior of a buggy program is *undefined*
Overview

• Introduction

• The attacker-defender race
  o Attack 1: Stack-based buffer overflow
  o Defense 1: Stack canaries
  o Attack 2: Heap-based buffer overflow
  o Defense 2: Non-executable data
  o Attack 3: Return-to-libc attacks
  o Defense 3: Layout randomization

• Advanced attacks and defenses

• Other defenses

• Conclusion
Stack based buffer overflow

• The stack is a memory area used at run time to track function calls and returns
  o Per call, an activation record or stack frame is pushed on the stack, containing:
    • Actual parameters, return address, automatically allocated local variables, …

• As a consequence, if a local buffer variable can be overflowed, there are interesting memory locations to overwrite nearby
  o The simplest attack is to overwrite the return address so that it points to attacker-chosen code (shellcode)
Stack based buffer overflow

```
Stack

Return address f0
Saved Frame Ptr f0
Local variables f0
```

```
f0:
  ...
  call f1
  ...

f1:
  buffer[]
  overflow()
  ...
```
Stack based buffer overflow

Stack

- Return address f0
- Saved Frame Ptr f0
- Local variables f0
- Arguments f1
- Return address f1
- Saved Frame Ptr f1
- Space for buffer

f0:

... call f1
...

f1:

buffer[]
overflow()
...

IP

FP

SP
Stack based buffer overflow

f0:
  ...
call f1
  ...

f1:
buffer[]
overflow()
  ...

Stack

Return address f0
Saved Frame Ptr f0
Local variables f0
Arguments f1
Overwritten address
Injected Code
Side-note: endianness

- Intel processors are *little-endian*

<table>
<thead>
<tr>
<th>Register Contents</th>
<th>Memory Contents</th>
<th>Register Contents</th>
<th>Memory Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>0A0B0C0D</td>
<td>...</td>
<td>0A0B0C0D</td>
<td>...</td>
</tr>
<tr>
<td>Little-endian</td>
<td></td>
<td>Big-endian</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Location</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x1000</td>
<td>0x03</td>
</tr>
<tr>
<td>0x1004</td>
<td>0x02</td>
</tr>
<tr>
<td>0x1008</td>
<td>0x01</td>
</tr>
<tr>
<td>0x1010</td>
<td>0x00</td>
</tr>
<tr>
<td>0x0f</td>
<td>0x0e</td>
</tr>
<tr>
<td>0x0d</td>
<td>0x0c</td>
</tr>
<tr>
<td>0x0b</td>
<td>0x0a</td>
</tr>
<tr>
<td>0x09</td>
<td>0x08</td>
</tr>
<tr>
<td>0x07</td>
<td>0x06</td>
</tr>
<tr>
<td>0x05</td>
<td>0x04</td>
</tr>
</tbody>
</table>
Very simple shell code

- In examples further on, we will use:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0xcd 0x2e</td>
<td>int 0x2e</td>
<td>system call to the operating system</td>
</tr>
<tr>
<td>0xeb 0xfe</td>
<td>L: jmp L</td>
<td>a very short, direct infinite loop</td>
</tr>
</tbody>
</table>

- Real shell-code is only slightly longer:

  LINUX on Intel:
  ```c
  char shellcode[] =
  "\xeb\x1f\xe89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
  "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
  "\x80\xe8\xdc\xff\xff\xff/bin/sh";
  ```
Stack based buffer overflow

• Example vulnerable program:

```c
int is_file_foobar( char* one, char* two )
{
    // must have strlen(one) + strlen(two) < MAX_LEN
    char tmp[MAX_LEN];
    strcpy( tmp, one );
    strcat( tmp, two );
    return strcmp( tmp, "file://foobar" );
}
```
Stack based buffer overflow

• Or alternatively:

```c
int is_file_foobar_using_loops( char* one, char* two )
{
    // must have strlen(one) + strlen(two) < MAX_LEN
    char tmp[MAX_LEN];
    char* b = tmp;
    for( ; *one != '\0'; ++one, ++b ) *b = *one;
    for( ; *two != '\0'; ++two, ++b ) *b = *two;
    *b = '\0';
    return strcmp( tmp, "file://foobar" );
}
```
Stack based buffer overflow

- Snapshot of the stack before the return:

<table>
<thead>
<tr>
<th>address</th>
<th>content</th>
<th>comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0012ff5c</td>
<td>0x00353037</td>
<td>argument two pointer</td>
</tr>
<tr>
<td>0x0012ff58</td>
<td>0x0035302f</td>
<td>argument one pointer</td>
</tr>
<tr>
<td>0x0012ff54</td>
<td>0x00401263</td>
<td>return address</td>
</tr>
<tr>
<td>0x0012ff50</td>
<td>0x0012ff7c</td>
<td>saved base pointer</td>
</tr>
<tr>
<td>0x0012ff4c</td>
<td>0x00000072</td>
<td>tmp continues \r \0 \0 \0</td>
</tr>
<tr>
<td>0x0012ff48</td>
<td>0x61626f6f</td>
<td>tmp continues o o b a</td>
</tr>
<tr>
<td>0x0012ff44</td>
<td>0x662f2f3a</td>
<td>tmp continues : / / f</td>
</tr>
<tr>
<td>0x0012ff40</td>
<td>0x656c6966</td>
<td>tmp array: f i l e</td>
</tr>
</tbody>
</table>
Stack based buffer overflow

• Snapshot of the stack before the return:

<table>
<thead>
<tr>
<th>address</th>
<th>content</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0012ff5c</td>
<td>0x00353037</td>
<td></td>
</tr>
<tr>
<td>0x0012ff58</td>
<td>0x0035302f</td>
<td></td>
</tr>
<tr>
<td>0x0012ff54</td>
<td>0x00401263</td>
<td></td>
</tr>
<tr>
<td>0x0012ff50</td>
<td>0x0012ff7c</td>
<td></td>
</tr>
<tr>
<td>0x0012ff4c</td>
<td>0x00000072</td>
<td></td>
</tr>
<tr>
<td>0x0012ff48</td>
<td>0x61626f6f</td>
<td></td>
</tr>
<tr>
<td>0x0012ff44</td>
<td>0x662f2f3a</td>
<td></td>
</tr>
<tr>
<td>0x0012ff40</td>
<td>0x656c6966</td>
<td></td>
</tr>
</tbody>
</table>

; argument two pointer
; argument one pointer
; return address
; saved base pointer
; tmp continues 'r' '
; tmp continues 'o' 'o' 'b' 'a'
; tmp continues ':' '/ ' '/ ' 'f'
; tmp array: 'f' 'i' 'l' 'e'
Stack based buffer overflow

- Snapshot of the stack before the return:

<table>
<thead>
<tr>
<th>address</th>
<th>content</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0012ff5c</td>
<td>0x00353037 ; argument two pointer</td>
</tr>
<tr>
<td>0x0012ff58</td>
<td>0x0035302f ; argument one pointer</td>
</tr>
<tr>
<td>0x0012ff54</td>
<td>0x0012ff4c ; return address</td>
</tr>
<tr>
<td>0x0012ff50</td>
<td>0x66666666 ; saved base pointer</td>
</tr>
<tr>
<td>0x0012ff4c</td>
<td>0xfeeb2ecd ; tmp continues</td>
</tr>
<tr>
<td>0x0012ff48</td>
<td>0x66666666 ; tmp continues</td>
</tr>
<tr>
<td>0x0012ff44</td>
<td>0x66 2f2f3a ; tmp continues</td>
</tr>
<tr>
<td>0x0012ff40</td>
<td>0x656c6966 ; tmp array: 'f' 'i' 'l' 'e'</td>
</tr>
</tbody>
</table>
Stack based buffer overflow

• Lots of details to get right before it works:
  o No nulls in (character-)strings
  o Filling in the correct return address:
    • Fake return address must be precisely positioned
    • Attacker might not know the address of his own string
  o Other overwritten data must not be used before return from function
  o ...

• More information in
  o “Smashing the stack for fun and profit” by Aleph One
Exploitation challenge (from the SYSSEC 10K challenge)

```c
char gWelcome [] = "Welcome to our system! ";

void echo (int fd)
{
    int len;
    char name [64], reply [128];

    len = strlen (gWelcome);
    memcp (reply, gWelcome, len); /* copy the welcome string to reply */

    write_to_socket (fd, "Type your name: "); /* prompt client for name */
    read (fd, name, 128); /* read name from socket */

    /* copy the name into the reply buffer (starting at offset len, so
     * that we won't overwrite the welcome message we copied earlier). */
    memcp (reply+len, name, 64);

    write (fd, reply, len + 64); /* now send full welcome message to client */
    return;
}

void server (int sockfd) { /* just call echo() in an endless loop */
    while (1)
        echo (socketfd);
}
Exploitation challenge (from the SYSSEC 10K challenge)

```c
char gWelcome[] = "Welcome to our system! ";

void echo (int fd)
{
    int len;
    char name[64], reply[128];

    len = strlen(gWelcome);
    memcpy(reply, gWelcome, len);

    write_to_socket(fd, "Type your name: ");
    read(fd, name, 128);

    memcpy(reply+len, name, 64);

    write(fd, reply, len + 64);
    return;
}

void server (int socketfd) {
    while (1)
        echo(socketfd);
}
```
Overview

• Introduction

• The attacker-defender race
  o Attack 1: Stack-based buffer overflow
  o Defense 1: Stack canaries
  o Attack 2: Heap-based buffer overflow
  o Defense 2: Non-executable data
  o Attack 3: Return-to-libc attacks
  o Defense 3: Layout randomization

• Advanced attacks and defenses

• Other defenses

• Conclusion
Stack canaries

• Basic idea
  o Insert a value right in a stack frame right before the stored base pointer/return address
  o Verify on return from a function that this value was not modified
• The inserted value is called a canary, after the coal mine canaries
Stack canaries

```assembly
f0:
  ...
  call f1
  ...

f1:
  buffer[]
  overflow()
  ...
```

Stack

- Return address f0
- Saved Frame Ptr f0
- Canary
Stack based buffer overflow

```
1. f0:
   ...  
call f1
   ...  

2. f1:
   buffer[]
   overflow()
   ...
```

**Stack Diagram:**
- Return address f0
- Saved Frame Ptr f0
- Canary
- Arguments f1
- Return address f1
- Saved Frame Ptr f1
- Canary
Stack based buffer overflow

```plaintext
f0:
  ...
  call f1
  ...

f1:
  buffer[]
  overflow()
  ...
```

Stack:
- Return address f0
- Saved Frame Ptr f0
- Canary
- Arguments f1
- Overwritten address
- Canary

IP ➔ SP ➔ FP
Exploitation challenge (from the SYSSEC 10K challenge)

```c
char gWelcome [] = "Welcome to our system! ";

void echo (int fd)
{
    int len;
    char name [64], reply [128];

    len = strlen (gWelcome);
    memcpy (reply, gWelcome, len); /* copy the welcome string to reply */

    write_to_socket (fd, "Type your name: "); /* prompt client for name */
    read (fd, name, 128); /* read name from socket */

    /* copy the name into the reply buffer (starting at offset len, so *
     * that we won't overwrite the welcome message we copied earlier). */
    memcpy (reply+len, name, 64);

    write (fd, reply, len + 64); /* now send full welcome message to client */
    return;
}

void server (int sockfd) { /* just call echo() in an endless loop */
    while (1)
        echo (socketfd);
}
```
Exploitation challenge (from the SYSSEC 10K challenge)

```c
char gWelcome [] = "Welcome to our system! ";

void echo (int fd)
{
    int len;
    char name [64], reply [128];

    len = strlen (gWelcome);
    memcpy (reply, gWelcome, len);

    write_to_socket (fd, "Type your name: ");
    read (fd, name, 128);

    memcpy (reply+len, name, 64);

    write (fd, reply, len + 64);
    return;
}

void server (int socketfd) {
    while (1)
        echo (socketfd);
}
```
Overview

• Introduction
• The attacker-defender race
  o Attack 1: Stack-based buffer overflow
  o Defense 1: Stack canaries
  o Attack 2: Heap-based buffer overflow
  o Defense 2: Non-executable data
  o Attack 3: Return-to-libc attacks
  o Defense 3: Layout randomization
• Advanced attacks and defenses
• Other defenses
• Conclusion
Heap based buffer overflow

• Stack canaries only protect the stack, but there are also buffers on the heap
• If a program contains a buffer overflow vulnerability for a buffer allocated on the heap, there is no return address nearby
• So attacking a heap based vulnerability requires the attacker to overwrite other code pointers
• We look at two examples:
  o Overwriting a function pointer
  o Overwriting heap metadata
Overwriting a function pointer

• Example vulnerable program:

```c
typedef struct _vulnerable_struct
{
    char buff[MAX_LEN];
    int (*cmp)(char*,char*);
} vulnerable;

int is_file_foo_bar_using_heap( vulnerable* s, char* one, char* two )
{
    // must have strlen(one) + strlen(two) < MAX_LEN
    strcpy( s->buff, one );
    strcat( s->buff, two );
    return s->cmp( s->buff, "file://foobar" );
}
```
Overwriting a function pointer

• And what happens on overflow:

(a) A structure holding “file:///foobar” and a pointer to the strcmp function.

(b) After a buffer overflow caused by the inputs “file://” and “asdfasdfasdf”.

(c) After a malicious buffer overflow caused by attacker-chosen inputs.
Overview

• Introduction

• The attacker-defender race
  o Attack 1: Stack-based buffer overflow
  o Defense 1: Stack canaries
  o Attack 2: Heap-based buffer overflow
  o Defense 2: Non-executable data
  o Attack 3: Return-to-libc attacks
  o Defense 3: Layout randomization

• Advanced attacks and defenses

• Other defenses

• Conclusion
Non-executable data

• Direct code injection attacks at some point execute data
• Most programs never need to do this
• Hence, a simple countermeasure is to mark data memory (stack, heap, ...) as non-executable
• This counters direct code injection
• But this countermeasure may break certain legacy applications
• How would you break this?
Overview

• Introduction
• The attacker-defender race
  - Attack 1: Stack-based buffer overflow
  - Defense 1: Stack canaries
  - Attack 2: Heap-based buffer overflow
  - Defense 2: Non-executable data
  - Attack 3: Return-to-libc attacks
  - Defense 3: Layout randomization
• Advanced attacks and defenses
• Other defenses
• Conclusion
Return-into-libc

- *Direct code injection*, where an attacker injects code as data is not always feasible
  - E.g. When certain countermeasures are active
- *Indirect code injection* attacks will drive the execution of the program by manipulating the stack
- This makes it possible to execute fractions of code present in memory
  - Usually, interesting code is available, e.g. libc
Return-into-libc: overview

Stack

- Params for f1
- Return addr
- Params for f2
- Return addr
- Params for f3
- Return addr

Code Memory

- f1
  - return
- f2
  - return
- f3
  - return

SP

IP
Return-into-libc: overview

Stack

- Params for f1
- Return addr
- Params for f2
- Return addr
- Params for f3
- Return addr

Code Memory

- f1
  - return
- f2
  - return
- f3
  - return

SP

IP
Return-into-libc: overview

Stack
- Params for f1
- Return addr
- Params for f2
- Return addr
- Params for f3
- Return addr

Code Memory
- f1
  - return
- f2
  - return
- f3
  - return

IP
SP
Return-into-libc: overview

Stack

Params for f1

Return addr

Params for f2

Return addr

Params for f3

Return addr

Code Memory

f1

return

f2

return

f3

return

return

return

SP

IP
Return-into-libc: overview
Return-into-libc: overview

Stack
- Params for f1
- Return addr
- Params for f2
- Return addr

Code Memory
- f1
  - return
- f2
  - return
- f3
  - return
  - return

SP

IP
Return-into-libc: overview

Stack

- Params for f1
- Return addr

Code Memory

- IP
- f1
  - return
- f2
  - return
- f3
  - return
  - return
Return-to-libc

• What do we need to make this work?
  o Inject the fake stack
    • Easy: this is just data we can put in a buffer
  o Make the stack pointer point to the fake stack right before a return instruction is executed
    • We will show an example where this is done by jumping to a trampoline
  o Then we make the stack execute existing functions to do a direct code injection
    • But we could do other useful stuff without direct code injection
Vulnerable program

```c
int median( int* data, int len, void* cmp )
{
    // must have 0 < len <= MAX_INTS
    int tmp[MAX_INTS];
    memcpy( tmp, data, len*sizeof(int) );  // copy the input integers
    qsort( tmp, len, sizeof(int), cmp );  // sort the local copy
    return tmp[len/2];  // median is in the middle
}
```
The trampoline

Assembly code of qsort:

... push edi ; push second argument to be compared onto the stack
push ebx ; push the first argument onto the stack
call [esp+comp_fp] ; call comparison function, indirectly through a pointer
add esp, 8 ; remove the two arguments from the stack
test eax, eax ; check the comparison result
jle label_lessthan ; branch on that result
...

Trampoline code

<table>
<thead>
<tr>
<th>address</th>
<th>machine code</th>
<th>assembly-language version of the machine code</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x7c971649</td>
<td>0x8b 0xe3</td>
<td>mov esp, ebx ; change the stack location to ebx</td>
</tr>
<tr>
<td>0x7c97164b</td>
<td>0x5b</td>
<td>pop ebx ; pop ebx from the new stack</td>
</tr>
<tr>
<td>0x7c97164c</td>
<td>0xc3</td>
<td>ret ; return based on the new stack</td>
</tr>
</tbody>
</table>
## Launching the attack

<table>
<thead>
<tr>
<th>stack address</th>
<th>normal stack contents</th>
<th>benign stack overflow contents</th>
<th>malicious stack overflow contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0012ff38</td>
<td>0x004013e0</td>
<td>0x1111110d</td>
<td>0x7c971649</td>
</tr>
<tr>
<td>0x0012ff34</td>
<td>0x00000001</td>
<td>0x1111110c</td>
<td>0x1111110c</td>
</tr>
<tr>
<td>0x0012ff30</td>
<td>0x00353050</td>
<td>0x1111110b</td>
<td>0x1111110b</td>
</tr>
<tr>
<td>0x0012ff2c</td>
<td>0x00401528</td>
<td>0x1111110a</td>
<td>0xfeeb2ecd</td>
</tr>
<tr>
<td>0x0012ff28</td>
<td>0x0012ff4c</td>
<td>0x11111109</td>
<td>0x70000000</td>
</tr>
<tr>
<td>0x0012ff24</td>
<td>0x00000000</td>
<td>0x11111108</td>
<td>0x70000000</td>
</tr>
<tr>
<td>0x0012ff20</td>
<td>0x00000000</td>
<td>0x11111107</td>
<td>0x00000040</td>
</tr>
<tr>
<td>0x0012ff1c</td>
<td>0x00000000</td>
<td>0x11111106</td>
<td>0x00003000</td>
</tr>
<tr>
<td>0x0012ff18</td>
<td>0x00000000</td>
<td>0x11111105</td>
<td>0x0001000</td>
</tr>
<tr>
<td>0x0012ff14</td>
<td>0x00000000</td>
<td>0x11111104</td>
<td>0x70000000</td>
</tr>
<tr>
<td>0x0012ff10</td>
<td>0x00000000</td>
<td>0x11111103</td>
<td>0x7c80978e</td>
</tr>
<tr>
<td>0x0012ff0c</td>
<td>0x00000000</td>
<td>0x11111102</td>
<td>0x7c809a51</td>
</tr>
<tr>
<td>0x0012ff08</td>
<td>0x00000000</td>
<td>0x11111101</td>
<td>0x11111101</td>
</tr>
<tr>
<td>0x0012ff04</td>
<td>0x00000000</td>
<td>0x11111101</td>
<td>0x11111101</td>
</tr>
<tr>
<td>0x0012ff00</td>
<td>0x00353050</td>
<td>0x00353050</td>
<td>0x00353050</td>
</tr>
<tr>
<td>0x0012ff0e</td>
<td>0x0012ff08</td>
<td>0x0012ff08</td>
<td>0x0012ff08</td>
</tr>
</tbody>
</table>
Unwinding the fake stack

malicious overflow contents
0x7c971649 ; cmp argument
0x11111110c ; len argument
0x11111110b ; data argument
0xfeeb2ecd ; return address
0x70000000 ; saved base pointer
0x70000000 ; tmp final 4 bytes
0x00000040 ; tmp continues
0x00003000 ; tmp continues
0x00001000 ; tmp continues
0x70000000 ; tmp continues
0x7c80978e ; tmp continues
0x7c809a51 ; tmp continues
0x11111101 ; tmp buffer starts

Code Memory

VirtualAlloc

return

InterlockedExchange

return
Unwinding the fake stack

malicious
overflow
contents

0x7c971649 ; cmp argument
0x1111110c ; len argument
0x1111111b ; data argument
0xfeeb2ecd ; return address
0x70000000 ; saved base pointer
0x70000000 ; tmp final 4 bytes
0x00000040 ; tmp continues
0x00003000 ; tmp continues
0x00010000 ; tmp continues
0x70000000 ; tmp continues
0x7c80978e ; tmp continues
0x7c809a51 ; tmp continues
0x11111101 ; tmp buffer starts

Code Memory

IP

VirtualAlloc
•
•
return

InterlockedExchange
•
•
return

•
Unwinding the fake stack

malicious
overflow
contents
0x7c971649 ; cmp argument
0x11111110c ; len argument
0x11111110b ; data argument
0xfeeb2ecd ; return address
0x70000000 ; saved base pointer
**0x70000000** ; tmp final 4 bytes
0x00000040 ; tmp continues
0x00003000 ; tmp continues
0x00001000 ; tmp continues
0x70000000 ; tmp continues
**0x7c80978e** ; tmp continues
**0x7c809a51** ; tmp continues
0x111111101 ; tmp buffer starts

Code Memory

VirtualAlloc
- return
- 
- 

InterlockedExchange
return
- 
- 

SP

IP
Unwinding the fake stack

malicious
overflow
contents

0x7c971649 ; cmp argument
0x1111110c ; len argument
0x1111111b ; data argument
0xfeeb2ecd ; return address
0x70000000 ; saved base pointer
0x70000000 ; tmp final 4 bytes
0x00000040 ; tmp continues
0x00003000 ; tmp continues
0x0001000 ; tmp continues
0x70000000 ; tmp continues
0x7c80978e ; tmp continues
0x7c809a51 ; tmp continues
0x11111101 ; tmp buffer starts

Code Memory

VirtualAlloc

. .
return

. .

InterlockedExchange

return

. .
Unwinding the fake stack

malicious
overflow
contents
0x7c971649 ; cmp argument
0x11111110c ; len argument
0x11111110b ; data argument
0xfeeb2ecd ; return address
0x70000000 ; saved base pointer
0x70000000 ; tmp final 4 bytes
0x00000040 ; tmp continues
0x00003000 ; tmp continues
0x00001000 ; tmp continues
0x70000000 ; tmp continues
0x7c80978e ; tmp continues
0x7c809a51 ; tmp continues
0x11111101 ; tmp buffer starts

Code Memory

VirtualAlloc
.
.
return
.
.
.
.
.
.
.
InterlockedExchange
.
.
.
.
return
.
.
.
.
.
.
.

SP

IP
char gWelcome [] = "Welcome to our system! ";

void echo (int fd)
{
    int len;
    char name [64], reply [128];

    len = strlen (gWelcome);
    memcpy (reply, gWelcome, len); /* copy the welcome string to reply */

    write_to_socket (fd, "Type your name: "); /* prompt client for name */
    read (fd, name, 128); /* read name from socket */

    /* copy the name into the reply buffer (starting at offset len, so
     * that we won't overwrite the welcome message we copied earlier). */
    memcpy (reply+len, name, 64);

    write (fd, reply, len + 64); /* now send full welcome message to client */
    return;
}

void server (int sockfd) { /* just call echo() in an endless loop */
    while (1)
        echo (socketfd);
Exploitation challenge (from the SYSSEC 10K challenge)

```c
char gWelcome [] = "Welcome to our system! \n/

void echo (int fd)
{
    int len;
    char name [64], reply [128];

    len = strlen (gWelcome);
    memcpy (reply, gWelcome, len);

    write_to_socket (fd, "Type your name: ");
    read (fd, name, 128);

    memcpy (reply+len, name, 64);

    write (fd, reply, len + 64);
    return;
}

void server (int sockfd) {
    while (1)
        echo (socketfd);
}
```
Overview

• Introduction
• The attacker-defender race
  o Attack 1: Stack-based buffer overflow
  o Defense 1: Stack canaries
  o Attack 2: Heap-based buffer overflow
  o Defense 2: Non-executable data
  o Attack 3: Return-to-libc attacks
  o Defense 3: Layout randomization
• Advanced attacks and defenses
• Other defenses
• Conclusion
Layout Randomization

- Most attacks rely on precise knowledge of run time memory addresses
- Introducing artificial variation in these addresses significantly raises the bar for attackers
- Such address space layout randomization (ASLR) is a cheap and effective countermeasure
### Example

<table>
<thead>
<tr>
<th>Stack One</th>
<th>Stack Two</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td><strong>Contents</strong></td>
</tr>
<tr>
<td>0x0022feac</td>
<td>0x008a13e0</td>
</tr>
<tr>
<td>0x0022fea8</td>
<td>0x00000001</td>
</tr>
<tr>
<td>0x0022fea4</td>
<td>0x00a91147</td>
</tr>
<tr>
<td>0x0022fea0</td>
<td>0x008a1528</td>
</tr>
<tr>
<td>0x0022fe9c</td>
<td>0x0022fec8</td>
</tr>
<tr>
<td>0x0022fe98</td>
<td>0x00000000</td>
</tr>
<tr>
<td>0x0022fe94</td>
<td>0x00000000</td>
</tr>
<tr>
<td>0x0022fe90</td>
<td>0x00000000</td>
</tr>
<tr>
<td>0x0022fe8c</td>
<td>0x00000000</td>
</tr>
<tr>
<td>0x0022fe88</td>
<td>0x00000000</td>
</tr>
<tr>
<td>0x0022fe84</td>
<td>0x00000000</td>
</tr>
<tr>
<td>0x0022fe80</td>
<td>0x00000000</td>
</tr>
<tr>
<td>0x0022fe7c</td>
<td>0x00000000</td>
</tr>
<tr>
<td>0x0022fe78</td>
<td>0x00000004</td>
</tr>
<tr>
<td>0x0022fe74</td>
<td>0x00a91147</td>
</tr>
<tr>
<td>0x0022fe70</td>
<td>0x0022fe8c</td>
</tr>
</tbody>
</table>
```c
char gWelcome[] = "Welcome to our system! ";

void echo (int fd) {
    int len;
    char name[64], reply[128];

    len = strlen(gWelcome);
    memcpys(reply, gWelcome, len); /* copy the welcome string to reply */

    write_to_socket(fd, "Type your name: "); /* prompt client for name */
    read(fd, name, 128); /* read name from socket */

    /* copy the name into the reply buffer (starting at offset len, so
     * that we won't overwrite the welcome message we copied earlier). */
    memcpys(reply+len, name, 64);

    write(fd, reply, len + 64); /* now send full welcome message to client */
    return;
}

void server (int sockfd) { /* just call echo() in an endless loop */
    while (1)
        echo(sockfd);
} 60
```
Exploitation challenge (from the SYSSEC 10K challenge)

```c
char gWelcome [] = "Welcome to our system! ";

void echo (int fd)
{
    int len;
    char name [64], reply [128];

    len = strlen (gWelcome);
    memcpy (reply, gWelcome, len);

    write_to_socket (fd, "Type your name: ");
    read (fd, name, 128);

    memcpy (reply+len, name, 64);

    write (fd, reply, len + 64);
    return;
}

void server (int socketfd) {
    while (1)
        echo (socketfd);
}
```
Overview

• Introduction

• The attacker-defender race
  o Attack 1: Stack-based buffer overflow
  o Defense 1: Stack canaries
  o Attack 2: Heap-based buffer overflow
  o Defense 2: Non-executable data
  o Attack 3: Return-to-libc attacks
  o Defense 3: Layout randomization

• Advanced attacks and defenses

• Other defenses

• Conclusion
Advanced defense: Control Flow Integrity
Control-flow integrity

- Most attacks we discussed break the control flow as it is encoded in the source program
  - E.g. At the source code level, one always expects a function to return to its call site
- The idea of control-flow integrity is to instrument the code to check the “sanity” of the control-flow at runtime
Example CFI at the source level

• The following code explicitly checks whether the cmp function pointer points to one of two known functions:

```c
int is_file_foobar_using_heap( vulnerable* s, char* one, char* two )
{
    // ... elided code ...
    if( (s->cmp == strcmp) || (s->cmp == stricmp) ) {
        return s->cmp( s->buff, "file://foobar" );
    } else {
        return report_memory_corruption_error();
    }
}
```
bool lt(int x, int y) {
    return x < y;
}
bool gt(int x, int y) {
    return x > y;
}
sort2(int a[], int b[], int len) {
    sort(a, len, lt);
    sort(b, len, gt);
}
Advanced attack: overwriting heap metadata and indirect pointer overwrite
Overwriting heap metadata

• The heap is a memory area where dynamically allocated data is stored
  o Typically managed by a memory allocation library that offers functionality to allocate and free chunks of memory (in C: malloc() and free() calls)

• Most memory allocation libraries store management information in-band
  o As a consequence, buffer overruns on the heap can overwrite this management information
  o This enables an “indirect pointer overwrite”-like attack allowing attackers to overwrite arbitrary memory locations
Heap management in dlmalloc

Dlmalloc maintains a doubly linked list of free chunks

When chunk c gets unlinked, c’s backward pointer is written to *(forward pointer+12)

Or: green value is written 12 bytes above where red value points
Exploiting a buffer overrun

Green value is written 12 bytes above where red value points

A buffer overrun in d can overwrite the red and green values

• Make Green point to injected code
• Make Red point 12 bytes below a function return address

Top Heap grows with brk()
Exploiting a buffer overrun

Top Heap grows with brk()

Green value is written 12 bytes above where red value points

Net result is that the return address points to the injected code
Indirect pointer overwrite

- This technique of overwriting a pointer that is later dereferenced for writing is called *indirect pointer overwrite*
- This is a broadly useful attack technique, as it allows to selectively change memory contents
- A program is vulnerable if:
  - It contains a bug that allows overwriting a pointer value
  - This pointer value is later dereferenced for writing
  - And the value written is under control of the attacker
Advanced(?) attack: data-only attacks
Data-only attacks

- These attacks proceed by changing only data of the program under attack.
- Depending on the program under attack, this can result in interesting exploits.
- We discuss two examples:
  - The unix password attack
  - Overwriting the environment table
Unix password attack

- Old implementations of login program looked like this:

<table>
<thead>
<tr>
<th>Stack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hashed password</td>
</tr>
<tr>
<td>password</td>
</tr>
</tbody>
</table>

Password check in login program:
1. Read loginname
2. Lookup hashed password
3. Read password
4. Check if
   hashed password = hash (password)
Unix password attack

Password check in login program:
1. Read loginname
2. Lookup hashed password
3. Read password
4. Check if
   hashed password = hash(password)

ATTACK: type in a password of the form pw || hash(pw)
void run_command_with_argument( pairs* data, int offset, int value )
{
    // must have offset be a valid index into data
    char cmd[MAX_LEN];
data[offset].argument = value;
{
    char valuestring[MAX_LEN];
    itoa( value, valuestring, 10 );
    strcpy( cmd, getenv("SAFECOMMAND") );
    strcat( cmd, " " );
    strcat( cmd, valuestring );
}
data[offset].result = system( cmd );
}
Overview

• Introduction
• The attacker-defender race
  o Attack 1: Stack-based buffer overflow
  o Defense 1: Stack canaries
  o Attack 2: Heap-based buffer overflow
  o Defense 2: Non-executable data
  o Attack 3: Return-to-libc attacks
  o Defense 3: Layout randomization
• Advanced attacks and defenses
• Other defenses
• Conclusion
# Overview of automatic defenses

<table>
<thead>
<tr>
<th></th>
<th>Return address corruption (A1)</th>
<th>Heap function pointer corruption (A2)</th>
<th>Jump-to-libc (A3)</th>
<th>Non-control data (A4)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Stack Canary (D1)</strong></td>
<td>Partial defense</td>
<td>Partial defense</td>
<td>Partial defense</td>
<td>Partial defense</td>
</tr>
<tr>
<td><strong>Non-executable data (D2)</strong></td>
<td>Partial defense</td>
<td>Partial defense</td>
<td>Partial defense</td>
<td>Partial defense</td>
</tr>
<tr>
<td><strong>Control-flow integrity (D3)</strong></td>
<td>Partial defense</td>
<td>Partial defense</td>
<td>Partial defense</td>
<td>Partial defense</td>
</tr>
<tr>
<td><strong>Address space layout randomization (D4)</strong></td>
<td>Partial defense</td>
<td>Partial defense</td>
<td>Partial defense</td>
<td>Partial defense</td>
</tr>
</tbody>
</table>
Need for other defenses

• The “automatic” defenses discussed in this lecture are only one element of securing C software
• Instead of preventing / detecting exploitation of the vulnerabilities at run time, one can:
  o Prevent the introduction of vulnerabilities in the code
  o Detect and eliminate the vulnerabilities at development time
  o Detect and eliminate the vulnerabilities with testing
Preventing introduction

• Safe programming languages such as Java / C# take memory management out of the programmer’s hands
• This makes it impossible to introduce exploitable memory safety vulnerabilities
  o They can still be “exploited” for denial-of-service purposes
  o Exploitable vulnerabilities can still be present in native parts of the application
Detect and eliminate vulnerabilities

• Code review
• Static analysis tools:
  o Simple “grep”-like tools that detect unsafe functions
  o Advanced heuristic tools that have false positives and false negatives
  o Sound tools that require significant programmer effort to annotate the program
• Testing tools:
  o Fuzz testing
  o Directed fuzz-testing / symbolic execution
Overview

• Introduction

• The attacker-defender race
  o Attack 1: Stack-based buffer overflow
  o Defense 1: Stack canaries
  o Attack 2: Heap-based buffer overflow
  o Defense 2: Non-executable data
  o Attack 3: Return-to-libc attacks
  o Defense 3: Layout randomization

• Advanced attacks and defenses

• Other defenses

• Conclusion
Conclusion

• The design of attacks and countermeasures has led to an arms race between attackers and defenders

• While significant hardening of the execution of C-like languages is possible, the use of safe languages like Java / C# is from the point of view of security preferable