C and C++ vulnerability exploits and countermeasures

Frank Piessens
(Frank.Piessens@cs.kuleuven.be)

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

• Introduction

• Example attacks
  – Stack-based buffer overflow
  – Heap-based buffer overflow
  – Return-to-libc attacks
  – Data-only attacks

• Example defenses
  – Stack canaries
  – Non-executable data
  – Control-flow integrity
  – Layout randomization

• Conclusion
Introduction

• An *implementation-level software vulnerability* is a bug in a program that can be exploited by an attacker to cause harm.

• Example vulnerabilities:
  – SQL injection vulnerabilities (discussed before)
  – XSS vulnerabilities (discussed before)
  – Buffer overflows and other memory corruption vulnerabilities

• An *attack* is a scenario where an attacker triggers the bug to cause harm.

• A *countermeasure* is a technique to counter attacks.

• These lectures will discuss memory corruption vulnerabilities, common attack techniques, and common countermeasures for them.
Memory corruption vulnerabilities

• Memory corruption vulnerabilities are a class of vulnerabilities relevant for unsafe languages
  – i.e. Languages that do not check whether programs access memory in a correct way
  – 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
Example vulnerable C program

```c
int unsafe( char* a, char* b )
{
    char t[MAX_LEN];
    strcpy( t, a );
    strcat( t, b );
    return strcmp( t, "abc" );
}
```
Introduction

• Attacks that exploit such vulnerabilities can have devastating consequences:
  – E.g. CERT Advisory Feb 2006:
    “The Microsoft Windows Media Player plug-in for browsers other than Internet Explorer contains a buffer overflow, which may allow a remote attacker to execute arbitrary code.” (CVE-2006-005)

• This is one (of the many) examples of a vulnerability that is exploitable by a code injection attack
Background: Memory management in C

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

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

High addresses

Arguments/ Environment
Stack
Unused and Mapped Memory
Heap (dynamic data)
Static Data
Program Code

Low addresses

Stack grows down
Heap grows up

Secappdev 2011
Memory management in C

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

• To do a code injection attack, an attacker must:
  – Find a bug in the program that can break memory safety
  – Find an interesting memory location to overwrite
  – Get attack code in the process memory space
Bugs that can break memory safety

- Writing past the end of an array (*buffer overrun or overflow*)
- Dereference a dangling pointer
- Use of a dangerous API function
  - That internally overflows a buffer
    - E.g. `strcpy()`, `gets()`
  - That is implemented in assembly in an intrinsically unsafe way
    - E.g. `printf()`
Interesting memory locations

• Code addresses or function pointers
  – Return address of a function invocation
  – Function pointers in the virtual function table
  – Program specific function pointers

• Pointers where the attacker can control what is written when the program dereferences the pointer
  – Indirect pointer overwrite: first redirect the pointer to another interesting location, then write the appropriate value
Overview

• Introduction

• Example attacks
  – Stack-based buffer overflow
  – Heap-based buffer overflow
  – Return-to-libc attacks
  – Data-only attacks

• Example defenses
  – Stack canaries
  – Non-executable data
  – Control-flow integrity
  – Layout randomization

• Conclusion
Stack based buffer overflow

• The stack is a memory area used at run time to track function calls and returns
  – 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
Stack based buffer overflow

f0:
  ...
  call f1
  ...

f1:
  buffer[]
  overflow()
  ...

Stack

- Return address f0
- Saved Frame Ptr f0
- Local variables f0
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
Injected Code

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
Stack based buffer overflow

• Shell code strings:

LINUX on Intel:
char shellcode[] =
"\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
"\x89\xf3\x8d\xe0\x88\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xda\x40\xcd"
"\x80\xe8\xdc\xff\xff\xff/bin/sh";

SPARC Solaris:
char shellcode[] =
"\x2d\x0b\xda\x9a\xac\x15\xa1\x6e\x2f\x0b\xdc\xda\x90\x0b\x80\x0e"
"\x92\x03\xa0\x08\x94\x1a\x80\x0a\x03\xa0\x10\xec\x3b\xbf\xf0"
"\xdc\x23\xbf\xf8\xc0\x23\xbf\xfc\x82\x10\x20\x3b\x91\xd0\x20\x08"
"\x90\x1b\xc0\x0f\x82\x10\x20\x01\x91\xd0\x20\x08";
Very simple shell code

- In examples further on, we will use:

<table>
<thead>
<tr>
<th>machine code</th>
<th>assembly-language version of the machine code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oxcd 0x2e</td>
<td>int 0x2e ; system call to the operating system</td>
</tr>
<tr>
<td>0xeb 0xfe</td>
<td>L: jmp L ; a very short, direct infinite loop</td>
</tr>
</tbody>
</table>
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>notes</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>note</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</td>
</tr>
<tr>
<td>0x0012ff48</td>
<td>0x61626f6f</td>
<td>’r’ ’\0’ ’\0’ ’\0’</td>
</tr>
<tr>
<td>0x0012ff44</td>
<td>0x662f2f3a</td>
<td>tmp continues</td>
</tr>
<tr>
<td>0x0012ff40</td>
<td>0x656c6966</td>
<td>’\0’ ’/’ ’/’ ’\0’</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tmp continues</td>
</tr>
<tr>
<td></td>
<td></td>
<td>’:’ ’/’ ’/’ ’/’</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tmp array:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>’f’ ’i’ ’l’ ’e’</td>
</tr>
</tbody>
</table>
Stack based buffer overflow

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

• More information in
  – “Smashing the stack for fun and profit” by Aleph One
Overview

• Introduction

• Example attacks
  – Stack-based buffer overflow
  – Heap-based buffer overflow
  – Return-to-libc attacks
  – Data-only attacks

• Example defenses
  – Stack canaries
  – Non-executable data
  – Control-flow integrity
  – Layout randomization

• Conclusion
Heap based buffer overflow

- 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:
  - Overwriting a function pointer
  - 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_foobar_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 “asdfsdfasdfsdf”.

(c) After a malicious buffer overflow caused by attacker-chosen inputs.
Overwriting heap metadata

• The heap is a memory area where dynamically allocated data is stored
  – 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
  – As a consequence, buffer overruns on the heap can overwrite this management information
  – This enables an “indirect pointer overwrite”-like attack allowing attackers to overwrite arbitrary memory locations

Secappdev 2011
Dlmalloc maintains a doubly linked list of free chunks.

When chunk \( c \) gets unlinked, \( c \)'s backward pointer is written to \( * (\text{forward pointer} + 12) \).

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
Exploiting a buffer overrun

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.
Overview

• Introduction

• Example attacks
  – Stack-based buffer overflow
  – Heap-based buffer overflow
  – Return-to-libc attacks
  – Data-only attacks

• Example defenses
  – Stack canaries
  – Non-executable data
  – Control-flow integrity
  – Layout randomization

• 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

```
Code Memory

| f1   |
|      |
|      |
|      |
|      |
|      |
|      |
|      |
| return |

| f2   |
|      |
|      |
|      |
|      |
|      |
|      |
|      |
| return |

| f3   |
|      |
|      |
|      |
|      |
|      |
|      |
|      |
| return |
```

Stack

```
| Params for f1 |
| Return addr   |
| Params for f2 |
| Return addr   |
| Params for f3 |
| Return addr   |
```

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

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

Secappdev 2011
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

IP

Secappdev 2011
Return-into-libc: overview

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

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

Code Memory
- Return addr

Secappdev 2011
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?
  – Inject the fake stack
    • Easy: this is just data we can put in a buffer
  – 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
  – 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_less-than ; 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>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 ; cmp argument</td>
</tr>
<tr>
<td>0x0012ff34</td>
<td>0x00000001</td>
<td>0x111110c</td>
<td>0x111110c ; len argument</td>
</tr>
<tr>
<td>0x0012ff30</td>
<td>0x0353050</td>
<td>0x111110b</td>
<td>0x111110b ; data argument</td>
</tr>
<tr>
<td>0x0012ff2c</td>
<td>0x401528</td>
<td>0x111110a</td>
<td>0xfeeb2ecd ; return address</td>
</tr>
<tr>
<td>0x0012ff28</td>
<td>0x012ff4c</td>
<td>0x1111109</td>
<td>0x70000000 ; saved base pointer</td>
</tr>
<tr>
<td>0x0012ff24</td>
<td>0x00000000</td>
<td>0x1111108</td>
<td>0x70000000 ; tmp final 4 bytes</td>
</tr>
<tr>
<td>0x0012ff20</td>
<td>0x00000000</td>
<td>0x1111107</td>
<td>0x0000000a ; tmp continues</td>
</tr>
<tr>
<td>0x0012ff1c</td>
<td>0x00000000</td>
<td>0x1111106</td>
<td>0x00003000 ; tmp continues</td>
</tr>
<tr>
<td>0x0012ff18</td>
<td>0x00000000</td>
<td>0x1111105</td>
<td>0x00001000 ; tmp continues</td>
</tr>
<tr>
<td>0x0012ff14</td>
<td>0x00000000</td>
<td>0x1111104</td>
<td>0x70000000 ; tmp continues</td>
</tr>
<tr>
<td>0x0012ff10</td>
<td>0x00000000</td>
<td>0x1111103</td>
<td>0x7c80978e ; tmp continues</td>
</tr>
<tr>
<td>0x0012ff0c</td>
<td>0x00000000</td>
<td>0x1111102</td>
<td>0x7c809a51 ; tmp continues</td>
</tr>
<tr>
<td>0x0012ff08</td>
<td>0x00000000</td>
<td>0x1111101</td>
<td>0x1111101 ; tmp buffer starts</td>
</tr>
<tr>
<td>0x0012ff04</td>
<td>0x00000000</td>
<td>0x00000004</td>
<td>0x00000004 ; memcpy length argument</td>
</tr>
<tr>
<td>0x0012ff00</td>
<td>0x353050</td>
<td>0x00353050</td>
<td>0x00353050 ; memcpy source argument</td>
</tr>
<tr>
<td>0x0012fefe</td>
<td>0x0012ff08</td>
<td>0x0012ff08</td>
<td>0x0012ff08 ; memcpy destination arg.</td>
</tr>
</tbody>
</table>
Unwinding the fake stack

malicious
overflow
contents

Code Memory
VirtualAlloc

InterlockedExchange

return

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
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

InterlockedExchange

return

SP

IP
Unwinding the fake stack

malicious
overflow
contents

Code Memory

VirtualAlloc
.
.
.

return
.
.
.

InterlockedExchange
.
.
.

return
.
.
.

IP

0x7c971649 ; cmp argument
0x1111110c ; len argument
0x1111110b ; 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
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
  .
  .
  .

Secappdev 2011
Unwinding the fake stack

malicious
overflow
contents

VirtualAlloc

.InterlockedExchange

Code Memory

return

SP

IP

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

Secappdev 2011
Overview

• Introduction

• Example attacks
  – Stack-based buffer overflow
  – Heap-based buffer overflow
  – Return-to-libc attacks
  – Data-only attacks

• Example defenses
  – Stack canaries
  – Non-executable data
  – Control-flow integrity
  – Layout randomization

• Conclusion
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:

Stack

<table>
<thead>
<tr>
<th>Hashed password</th>
<th>Password check in login program:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Read loginname</td>
</tr>
<tr>
<td></td>
<td>2. Lookup hashed password</td>
</tr>
<tr>
<td></td>
<td>3. Read password</td>
</tr>
<tr>
<td></td>
<td>4. Check if</td>
</tr>
<tr>
<td></td>
<td>hashed password = hash (password)</td>
</tr>
</tbody>
</table>

...
Unix password attack

Stack

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

• Example attacks
  – Stack-based buffer overflow
  – Heap-based buffer overflow
  – Return-to-libc attacks
  – Data-only attacks

  • Example defenses
    – Stack canaries
    – Non-executable data
    – Control-flow integrity
    – Layout randomization

• Conclusion
Stack canaries

• Basic idea
  – Insert a value right in a stack frame right before the stored base pointer/return address
  – 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

f0:
...
call f1
...

f1:
buffer[]
overflow()
...

Stack

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

f0:
  ...
  call f1
  ...

f1:
  buffer[]
  overflow()
  ...

Stack

Return address f0
Saved Frame Ptr f0
Canary

Arguments f1
Return address f1
Saved Frame Ptr f1
Canary
Stack based buffer overflow

Stack

Return address f0
Saved Frame Ptr f0
Canary
Arguments f1
Overwritten address
Canary
Canary

f0:
  ...
call f1
  ...

f1:
buffer[]
overflow()
  ...

IP
FP
SP
Overview

• Introduction

• Example attacks
  – Stack-based buffer overflow
  – Heap-based buffer overflow
  – Return-to-libc attacks
  – Data-only attacks

• Example defenses
  – Stack canaries
  – Non-executable data
  – Control-flow integrity
  – Layout randomization

• 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 not return-into-libc or data-only attacks
- In addition, this countermeasure may break certain legacy applications
Overview

• Introduction

• Example attacks
  – Stack-based buffer overflow
  – Heap-based buffer overflow
  – Return-to-libc attacks
  – Data-only attacks

• Example defenses
  – Stack canaries
  – Non-executable data
  – Control-flow integrity
  – Layout randomization

• Conclusion
Control-flow integrity

• Most attacks we discussed breaks 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();
    }
}
```
Example CFI with labels

```cpp
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);
}
```
Overview

• Introduction

• Example attacks
  – Stack-based buffer overflow
  – Heap-based buffer overflow
  – Return-to-libc attacks
  – Data-only attacks

• Example defenses
  – Stack canaries
  – Non-executable data
  – Control-flow integrity
  – Layout randomization

• Conclusion
Layout Randomization

- Most attacks rely on precise knowledge of runtime 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>address</td>
<td>contents</td>
</tr>
<tr>
<td>0x0022feac</td>
<td>0x008a13e0</td>
</tr>
<tr>
<td>0x0022fe8a</td>
<td>0x00000001</td>
</tr>
<tr>
<td>0x0022fe4a</td>
<td>0x00a91147</td>
</tr>
<tr>
<td>0x0022fe0a</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>
Overview

• Introduction
• Example attacks
  – Stack-based buffer overflow
  – Heap-based buffer overflow
  – Return-to-libc attacks
  – Data-only attacks
• Example defenses
  – Stack canaries
  – Non-executable data
  – Control-flow integrity
  – Layout randomization
• Conclusion
<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>Stack Canary (D1)</td>
<td>Partial defense</td>
<td>Partial defense</td>
<td>Partial defense</td>
<td>Partial defense</td>
</tr>
<tr>
<td>Non-executable data (D2)</td>
<td>Partial defense</td>
<td>Partial defense</td>
<td>Partial defense</td>
<td>Partial defense</td>
</tr>
<tr>
<td>Control-flow integrity (D3)</td>
<td>Partial defense</td>
<td>Partial defense</td>
<td>Partial defense</td>
<td>Partial defense</td>
</tr>
<tr>
<td>Address space layout randomization (D4)</td>
<td>Partial defense</td>
<td>Partial defense</td>
<td>Partial defense</td>
<td>Partial defense</td>
</tr>
</tbody>
</table>
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
Conclusion

• The “automatic” defenses discussed in this lecture are only one element of securing C software

• Secure software development also entails:
  – Threat modeling: what parts of the program are most likely to be under attack
  – Code review: to detect and eliminate bugs
  – Security testing
Attack exercises

• Exercises
  – Taken from (or based on) Gera’s Insecure Programming Page:
    http://community.corest.com/~gera/InsecureProgramming/
  – For each of the following exercises:
    • Draw the layout of the stack at the point where gets() is executed
    • What input makes the program print out “you win!”?
Attack exercises

• Exercise 1:

```c
#include <stdio.h>
int main() {
    int cookie;
    char buf[80];
    printf("buf: %08x cookie: %08x\n", &buf, &cookie);
    gets(buf);
    if (cookie == 0x41424344)
        printf("you win!\n");
}
```
Attack exercises

• Exercise 2:

```c
#include <stdio.h>
int main() {
    int cookie;
    char buf[80];
    printf("buf: %08x cookie: %08x\n", &buf, &cookie);
    gets(buf);
}
```