2017Fall:Software Security

Lecture 5 : Practical Control Flow Hijack Defense: StackGuard, DEP, and ASLR

Bing Mao

maobing@nju.edu.cn

Department of Computer Science

Outline

- Background
  - Control Flow Hijack
  - Control Flow Hijack Defense
  - Canary Defense
  - StackGuard
  - StackGuard Weakness
  - DiffGuard
  - Polymorphic Canary
- Data Execution Prevention
  - Definition
  - DEP Scorecard
  - Return-to-libc Attack
- ASLR
  - ASLR Randomization
  - ASLR

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Background
Control Flow Hijack

Occurs when an attacker **gains** control of

the instruction pointer

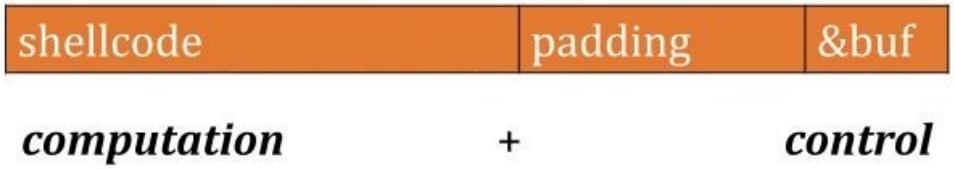
A few common hijack methods

1. buffer overflows
2. heap overflow
3. format string attacks

Credit: a portion of the slides in this lecture are compiled from Dr. David Brumley and also from book CSAPP

Background
3 Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Background
Control Flow Hijack



1. Leveraging memory corruption **vulnerabilities**
2. Crafting special input (**exploit**):
   - Performing certain **computation**
   - Gaining the **control** of the program

Same principle, different mechanism

1. Code injection
2. Return-to-libc
3. Return-oriented programming (ROP)

Background
4 Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Background
Control Flow Hijack Defense

Vulnerabilities (bugs) are the root cause of hijacks

1. Identify vulnerabilities with analysis tools (before attackers)
2. Prove program correctness

Mitigation Techniques:

1. Canaries – StackGuard
2. Data Execution Prevention (DEP) /No eXecute (NX)
3. Address Space Layout Randomization (ASLR)

Background
Control Flow Hijack
5 Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Background
Control Flow Hijack
6 Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Proposed defense scorecard:

Aspect	Defense
Performance	Smaller impact is better
Deployment	Can everyone easiliy use it
Compatibility	Does not break libraries
Safety Guarantee	Completely secure to easy to bypass

Canary-Based Protection
Canary Defense

Background
Control Flow Hijack
Control Flow Hijack Defense
7 Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

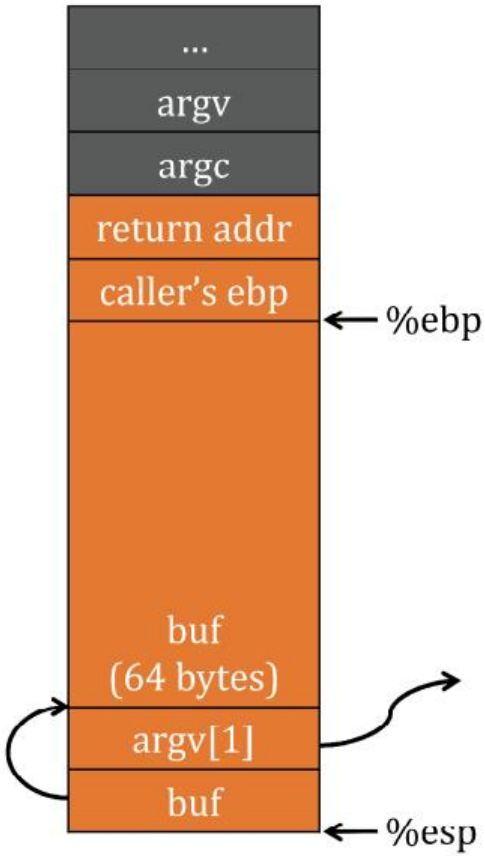
Wikipedia: "the historic practice of using canaries in coal mines, since they would be affected by toxic gases earlier than the miners, thus providing a biological warning system."

Canary / Stack Cookies

Canary-Based Protection
Canary Defense

"A"x68 . " \xEF \xBE \xAD\xDE"

```
#include<string.h>
int main(int argc, char **argv) {
    char buf[64];
    strcpy(buf, argv[1]);
}

Dump of assembler code for function main:
   0x080483e4 <+0>:  push   %ebp
   0x080483e5 <+1>:  mov    %esp,%ebp
   0x080483e7 <+3>:  sub    $72,%esp
   0x080483ea <+6>:  mov    12(%ebp),%eax
   0x080483ed <+9>:  mov    4(%eax),%eax
   0x080483f0 <+12>: mov    %eax,4(%esp)
   0x080483f4 <+16>: lea    -64(%ebp),%eax
   0x080483f7 <+19>: mov    %eax,(%esp)
   0x080483fa <+22>: call   0x8048300 <strcpy@plt>
   0x080483ff <+27>: leave
   0x08048400 <+28>: ret
```



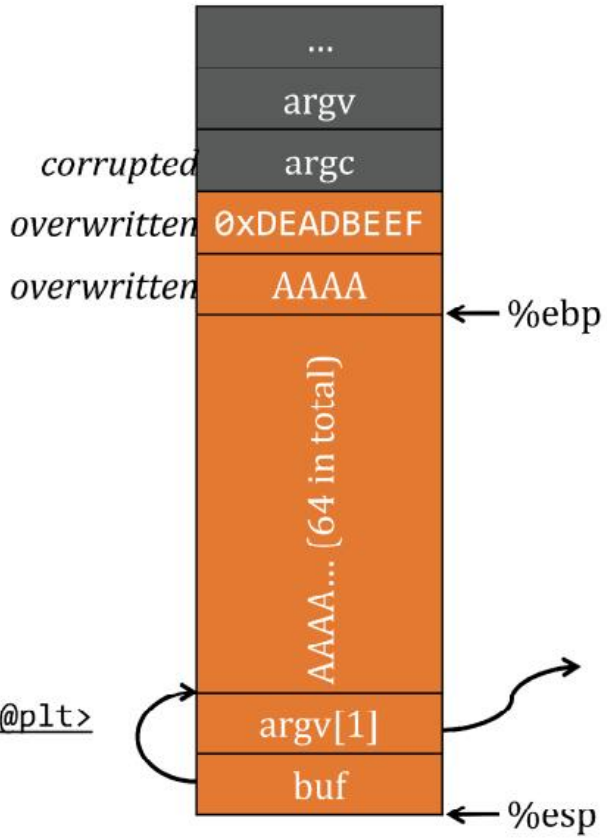
Background
Control Flow Hijack
Control Flow Hijack Defense
8 Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Canary-Based Protection
Canary Defense

"A"x68 . " \xEF \xBE \xAD\xDE"

```
#include<string.h>
int main(int argc, char **argv) {
    char buf[64];
    strcpy(buf, argv[1]);
}
```

```
Dump of assembler code for function main:
   0x080483e4 <+0>:  push   %ebp
   0x080483e5 <+1>:  mov    %esp,%ebp
   0x080483e7 <+3>:  sub    $72,%esp
   0x080483ea <+6>:  mov    12(%ebp),%eax
   0x080483ed <+9>:  mov    4(%eax),%eax
   0x080483f0 <+12>: mov    %eax,4(%esp)
   0x080483f4 <+16>: lea    -64(%ebp),%eax
   0x080483f7 <+19>: mov    %eax,(%esp)
   0x080483fa <+22>: call   0x8048300 <strcpy@plt>
   0x080483ff <+27>: leave
   0x08048400 <+28>: ret
```

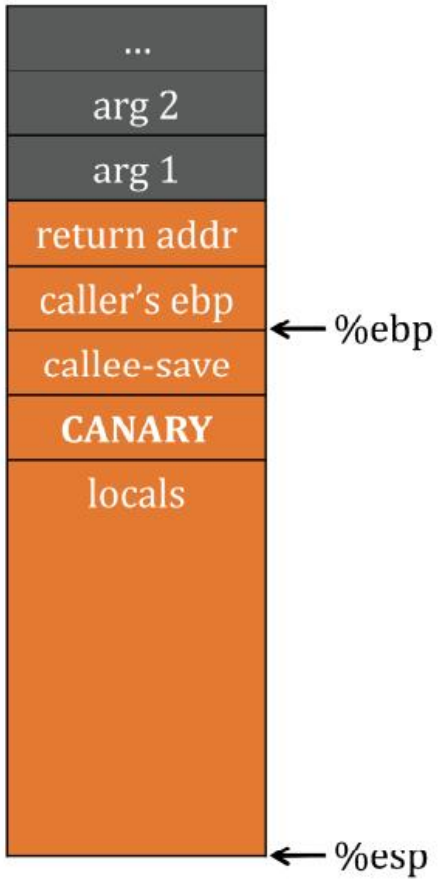


Background
Control Flow Hijack
Control Flow Hijack Defense
9 Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Canary-Based Protection
StackGuard

Idea:

- prologue introduces a ***canary word*** between return addr and locals

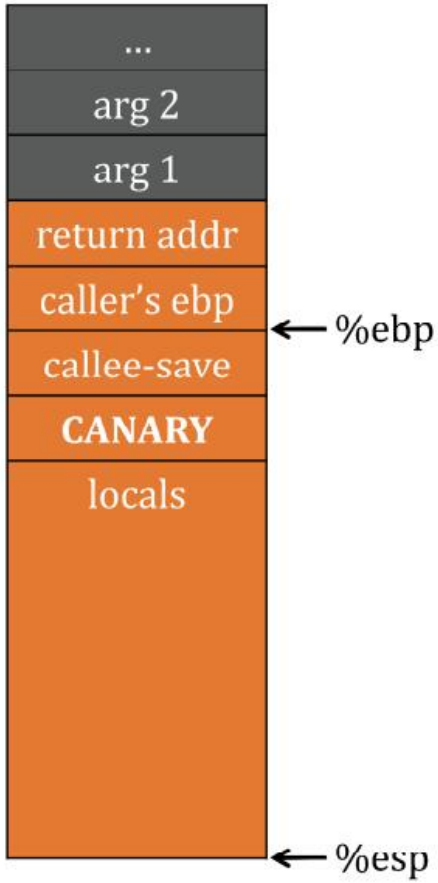


Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
10 StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Canary-Based Protection
StackGuard

Idea:

- prologue introduces a ***canary word*** between return addr and locals
- epilogue checks canary before function returns



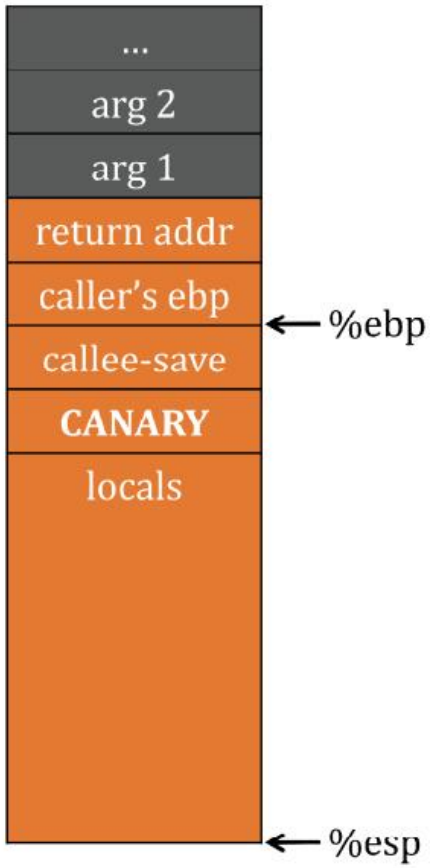
Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
11 StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Canary-Based Protection
StackGuard

Idea:

- prologue introduces a ***canary word*** between return addr and locals
- epilogue checks canary before function returns

Wrong Canary => Overflow



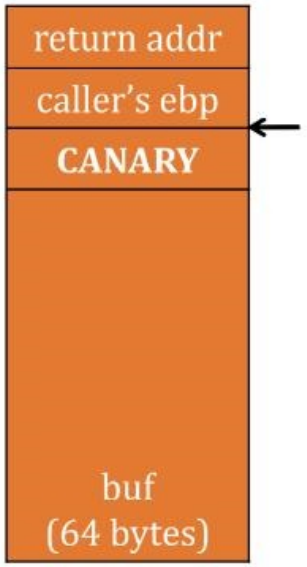
Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
12 StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Canary-Based Protection
StackGuard

gcc Stack-Smashing Protector

```
Dump of assembler code for function main:
   0x08048440 <+0>:  push   %ebp
   0x08048441 <+1>:  mov    %esp,%ebp
   0x08048443 <+3>:  sub    $76,%esp
   0x08048446 <+6>:  mov    %gs:20,%eax
   0x0804844c <+12>: mov    %eax,-4(%ebp)
   0x0804844f <+15>: xor    %eax,%eax
   0x08048451 <+17>: mov    12(%ebp),%eax
   0x08048454 <+20>: mov    4(%eax),%eax
   0x08048457 <+23>: mov    %eax,4(%esp)
   0x0804845b <+27>: lea    -68(%ebp),%eax
   0x0804845e <+30>: mov    %eax,(%esp)
   0x08048461 <+33>: call   0x8048350 <strcpy@plt>
   0x08048466 <+38>: mov    -4(%ebp),%edx
   0x08048469 <+41>: xor    %gs:20,%edx
   0x08048470 <+48>: je     0x8048477 <main+55>
   0x08048472 <+50>: call   0x8048340 <__stack_chk_fail@plt>
   0x08048477 <+55>: leave
   0x08048478 <+56>: ret
```

Compiled with v4.6.1:
`gcc -fstack-protector -O1 …`

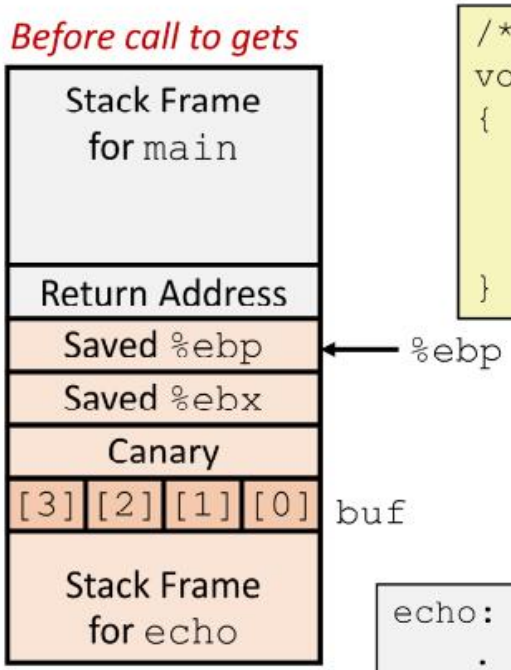


18

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
13 StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
14 StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Setting up canary



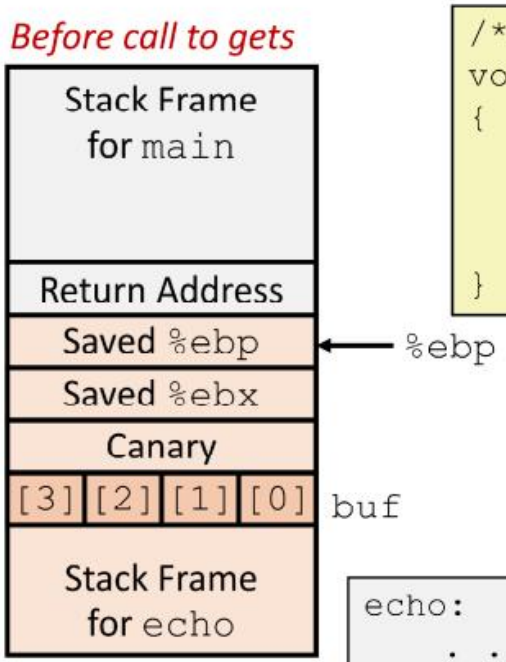

```
/* Echo Line */
void echo()
{
    char buf[4];  /* Way too small! */
    gets(buf);
    puts(buf);
}
```

%ebp

```
echo:
    . . .
    movl    %gs:20, %eax     # Get canary
    movl    %eax, -8(%ebp)   # Put on stack
    xorl    %eax, %eax       # Erase canary
    . . .
```

Canary-Based Protection
StackGuard

Checking canary




```
/* Echo Line */
void echo()
{
    char buf[4];  /* Way too small! */
    gets(buf);
    puts(buf);
}
```

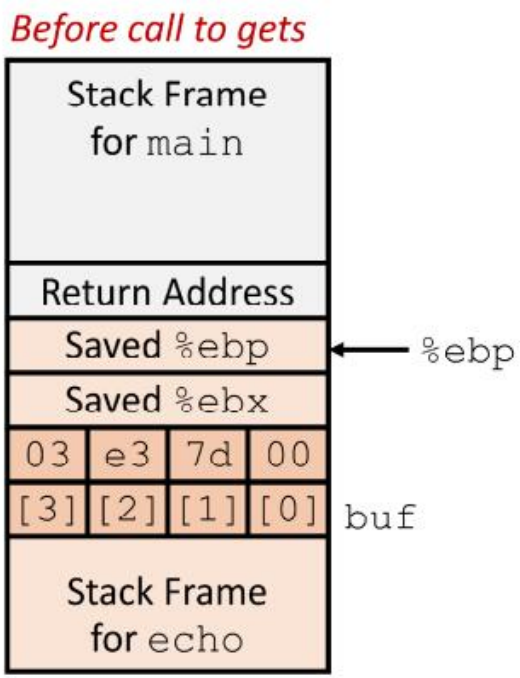
```
echo:
    . . .
    movl    -8(%ebp), %eax    # Retrieve from stack
    xorl    %gs:20, %eax      # Compare with Canary
    je      .L24              # Same: skip ahead
    call    __stack_chk_fail  # ERROR
.L24:
    . . .
```

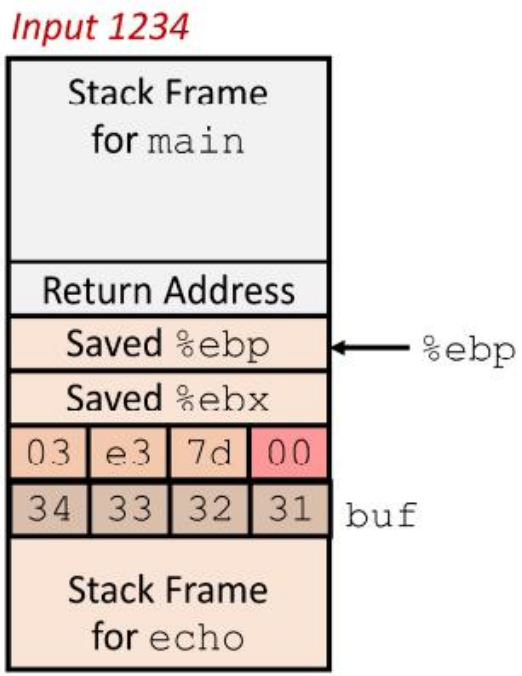
Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
15 StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Canary-Based Protection
StackGuard

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
16 StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Canary example






```
(gdb) break echo
(gdb) run
(gdb) stepi 3
(gdb) print /x *((unsigned *) $ebp - 2)
$1 = 0x3e37d00
```

Benign corruption!
(allows programmers to make silent off-by-one errors)

Canary-Based Protection
StackGuard

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
17 StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Glibc
- Genarate random canary
- Exception handing function

```
#0  security_init () at rtld.c:854
// 相当于glibc/dynamic-linker的main
#1  dl_main () at rtld.c:1818
#2  _dl_sysdep_start () at ../elf/dl-sysdep.c:249
#3  _dl_start_final () at rtld.c:331
#4  _dl_start () at rtld.c:557
// glibc/dynamic-linker入口
#5  _start () from /lib/ld-linux.so.2
```


调用栈

Canary-Based Protection
StackGuard

```
static void security_init (void)
{
                        ...
  /* Set up the stack checker's canary.  */
  uintptr_t stack_chk_guard = _dl_setup_stack_chk_guard (_dl_random);
  #ifdef THREAD_SET_STACK_GUARD
  THREAD_SET_STACK_GUARD (stack_chk_guard);
                        ...
}
```


Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
18 StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Canary-Based Protection
StackGuard

```
static inline uintptr_t __attribute__ ((always_inline)) _dl_setup_stack_chk_guard (void){
  uintptr_t ret;
  #ifdef ENABLE_STACKGUARD_RANDOMIZE
  int fd = __open ("/dev/urandom", O_RDONLY);
  if (fd >= 0) {
          ssize_t reslen = __read (fd, &ret, sizeof (ret));
          __close (fd);
          if (reslen == (ssize_t) sizeof (ret))
                  return ret;
  }
  #endif
  ret = 0;
  unsigned char *p = (unsigned char *) &ret;
  p[sizeof (ret) - 1] = 255;
  p[sizeof (ret) - 2] = '\n';
  return ret;
}
```


Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
19 StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Canary-Based Protection
StackGuard

Glibc
- Genarate random canary
- Exception handing function

glibc-2.19/debug/stack_chk_fail.c

```
#line 24
void
__attribute__ ((noreturn))
__stack_chk_fail (void)
{
  __fortify_fail ("stack smashing detected");
}
```

```
zwp@ubuntu:~/Desktop$ ./demo b.txt
Welcome to seclab!
*** stack smashing detected ***: ./demo terminated
```

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
20 StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Canary-Based Protection
StackGuard

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
21 StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Canary Should be HARD to Forge:

Random Canary

- 4 random bytes chosen at load time
- stored in a guarded page
- need good randomness

Random XOR canaries

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
22 StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

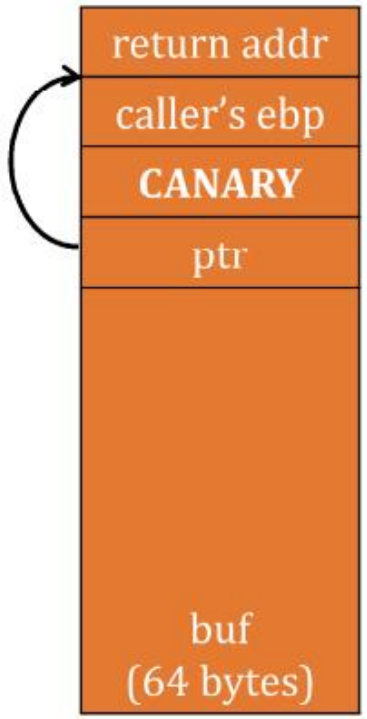
Canary scorecard

Aspect	Defense
Performance	Several instructions per function Time: a few percetange on average Size: can optimize away in safe functions
Deployment	Recompile sufficies; no code change
Compatibility	Perfect – invisible to outside
Safety Guarantee	Not really ...

Bypass: Data Pointer Subterfuge

Overwrite a data pointer *first*...

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



Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
23 StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Canary-Based Protection
StackGuard Weakness

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
24 StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Check does ***not*** happen until epilogue…

- func ptr subterfuge
- C++ vtable hijack
- exception handler hijack
- …

Canary-Based Protection
StackGuard Weakness

Check does ***not*** happen until epilogue…

- func ptr subterfuge } PointGuard
- C++ vtable hijack
- exception handler hijack } SafeSEH SEHOP
- …

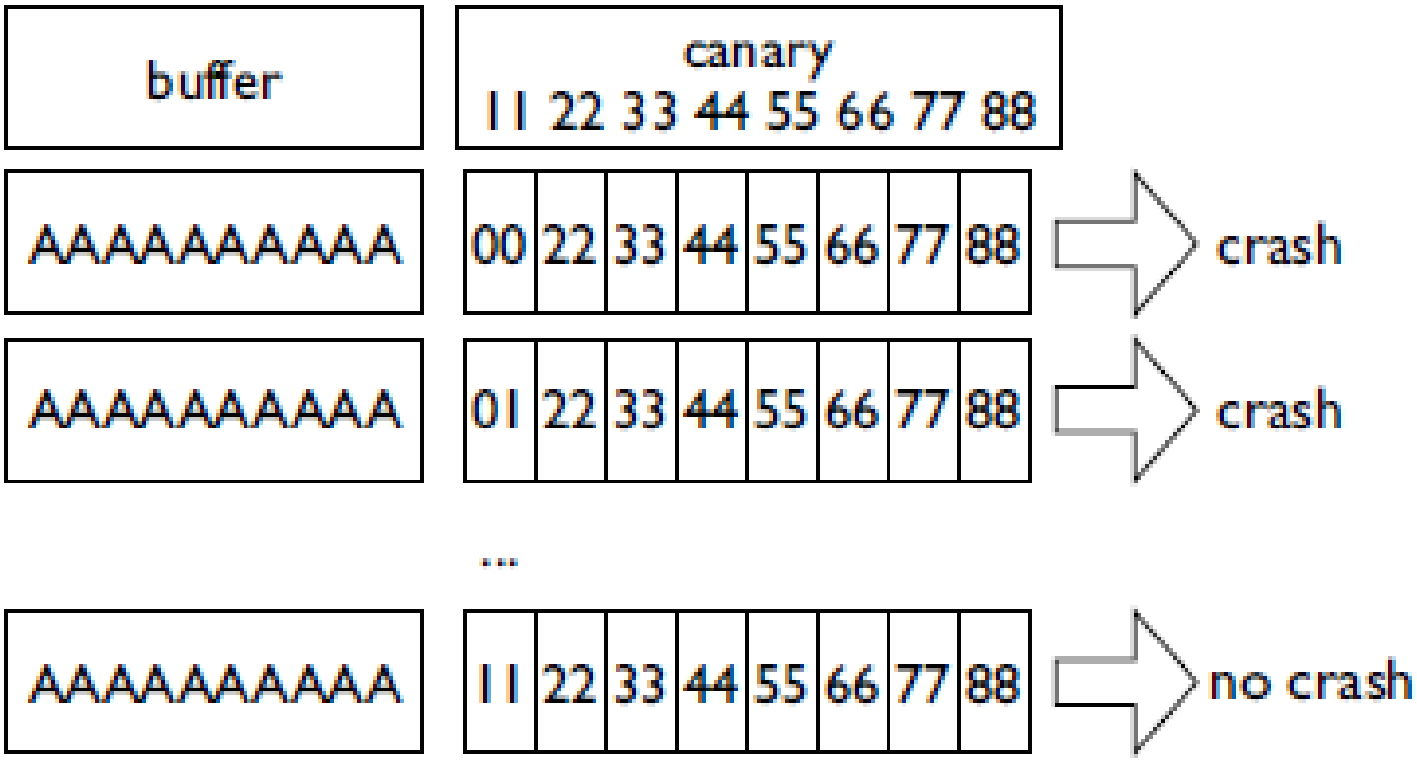
Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
25 StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Hacking Blind

- The situation is common in C/S mode, that the server forks a child process to service for client and the service restarts after a crash.
- All the children processes inherit/share the same memory layout from the parent process.
- The attacker can try in bounded time all the possible values of canary(for SSP) and memory layout(for ASLR) until the correct ones are found.

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
26 DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Canary-Based Protection
DiffGuard



Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
27 DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Canary-Based Protection
DiffGuard

A straight method is to update the canary when the parent server forks the child process.

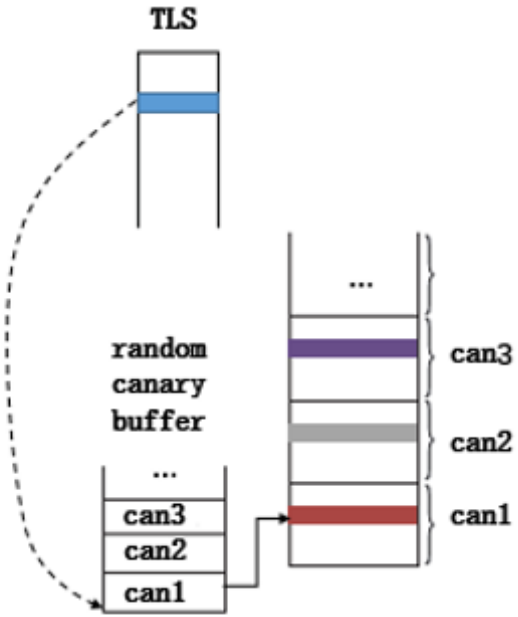
Any question?

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
28 DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

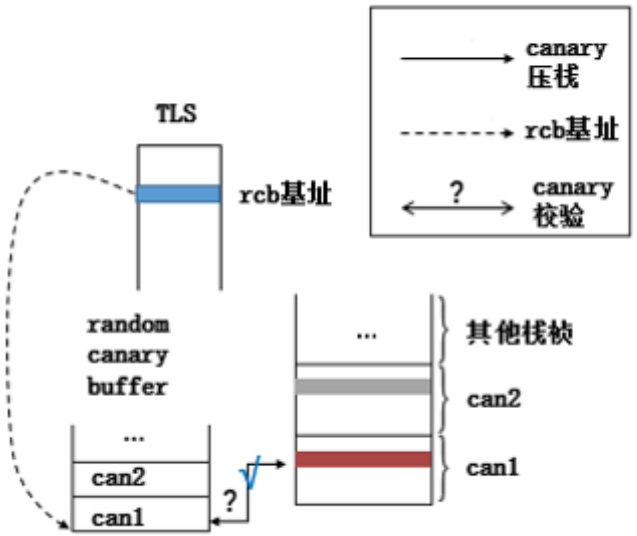
Canary-Based Protection
DiffGuard

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
29 DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

DiffGuard-普通程序



(a)rcb中的canary在函数调用时，逐一压到对应栈帧

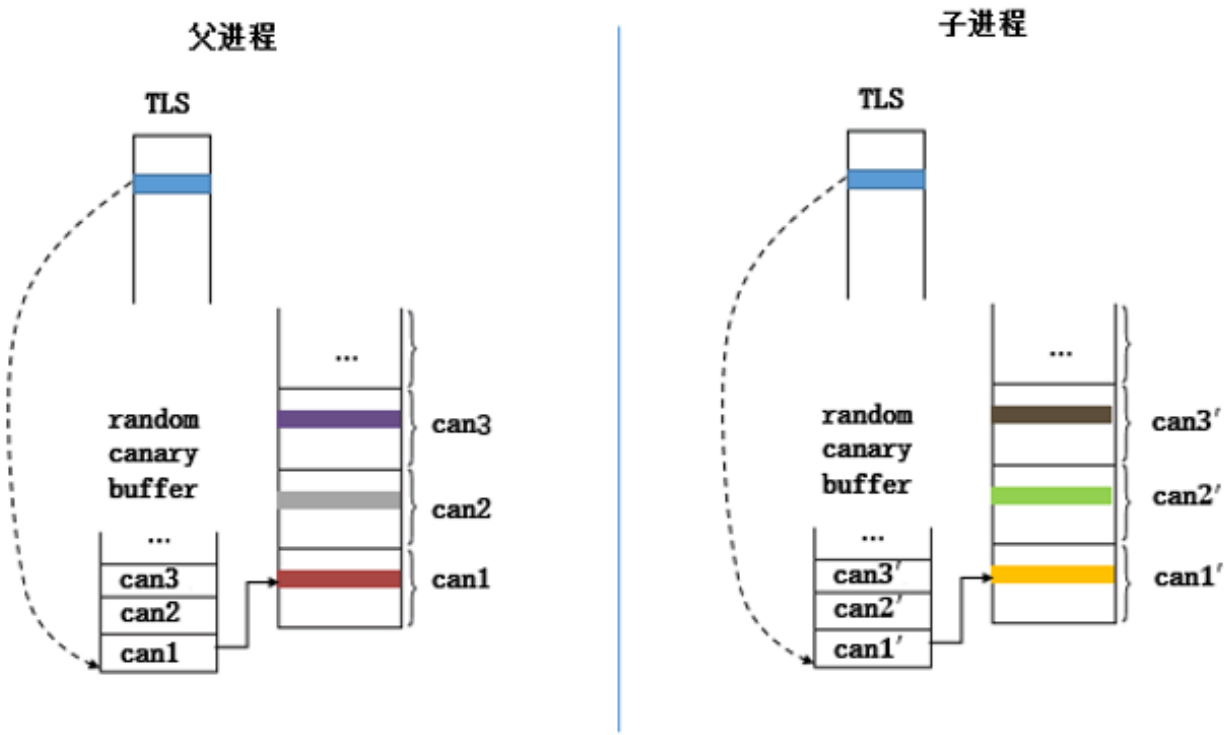


(b)函数调用结束时，检查canary是否被篡改

Canary-Based Protection
DiffGuard

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
30 DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

DiffGuard-Forking Program

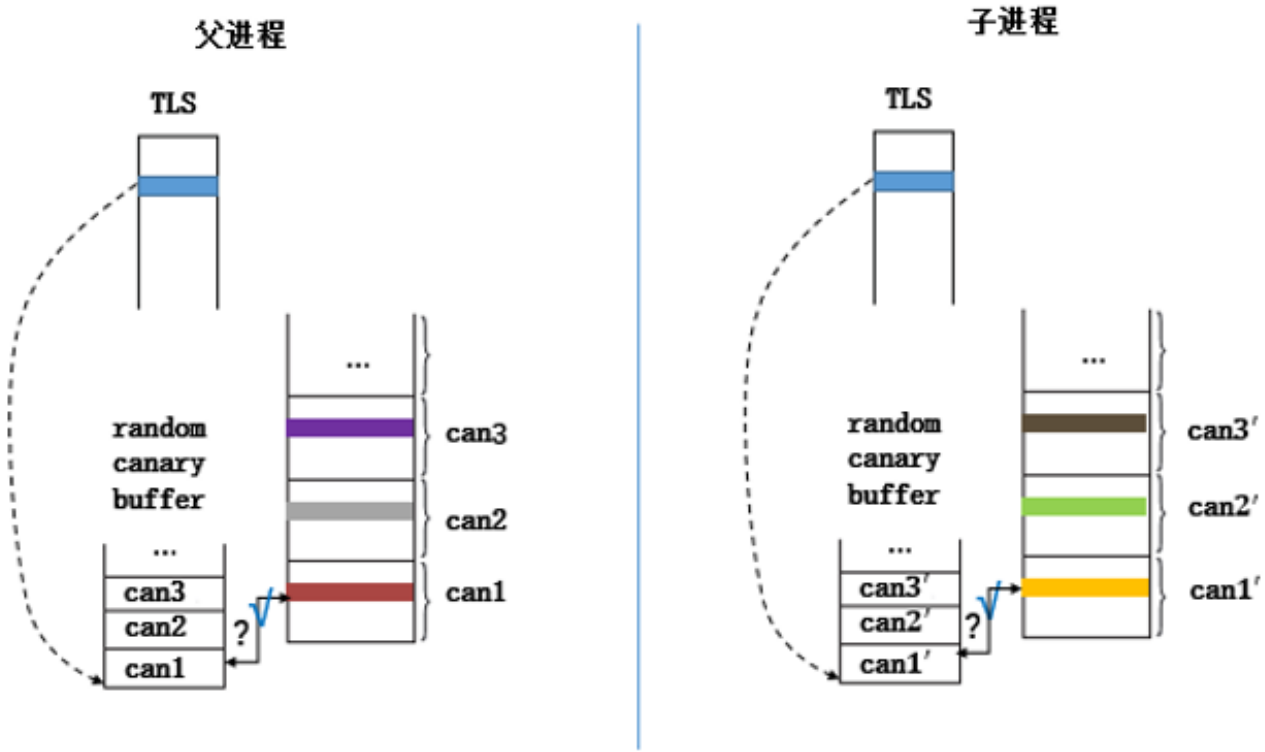


(c)当fork函数调用时，更新rcb中canary的值

Canary-Based Protection
DiffGuard

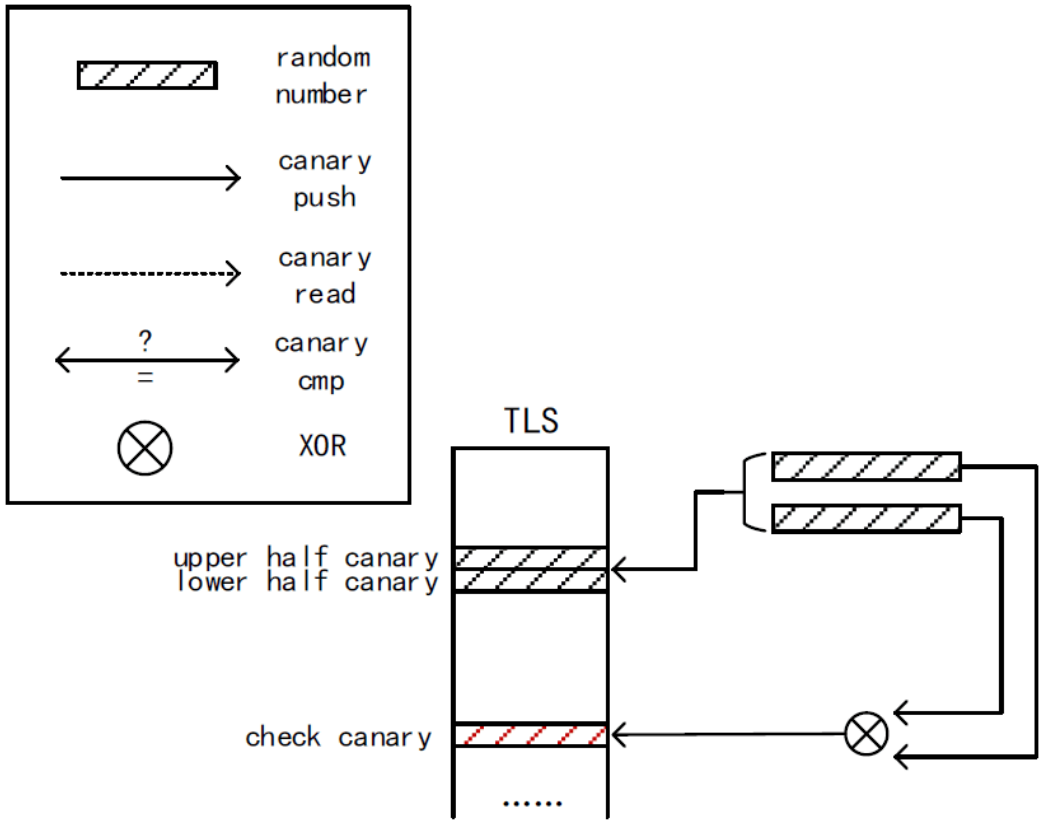
Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
31 DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

DiffGuard-Forking Program



(d)父进程与子进程拥有各自的rcb，在函数调用结束时，校验canary是否被篡改

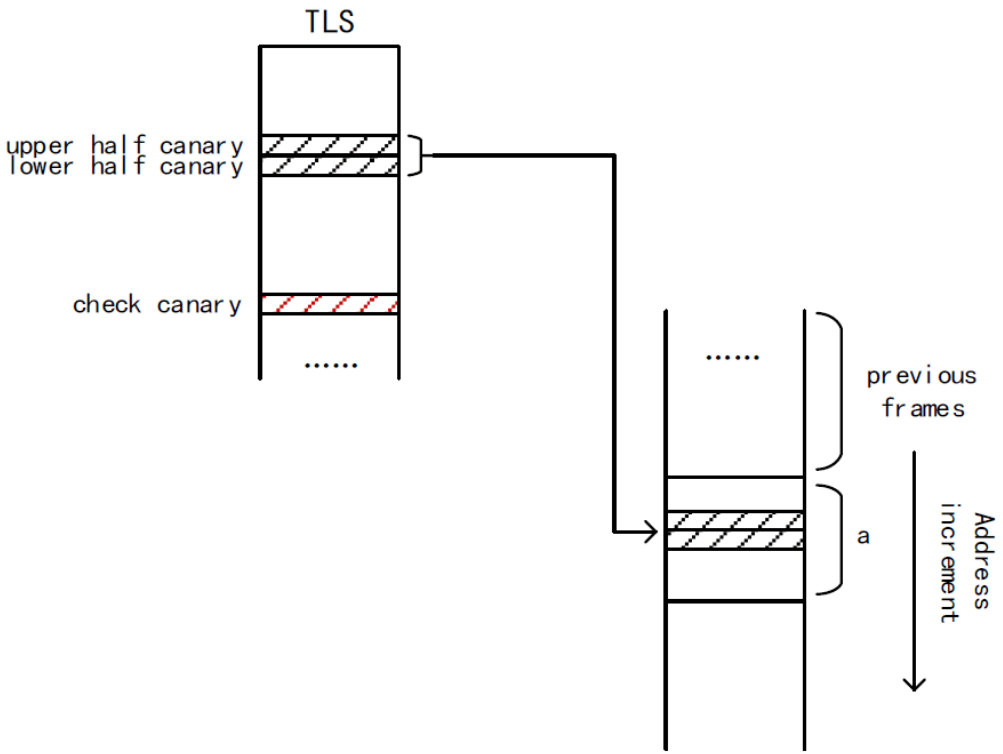
Canary-Based Protection
Polymorphic Canary



(a) Initialization of the canary in the TLS.

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
32 Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

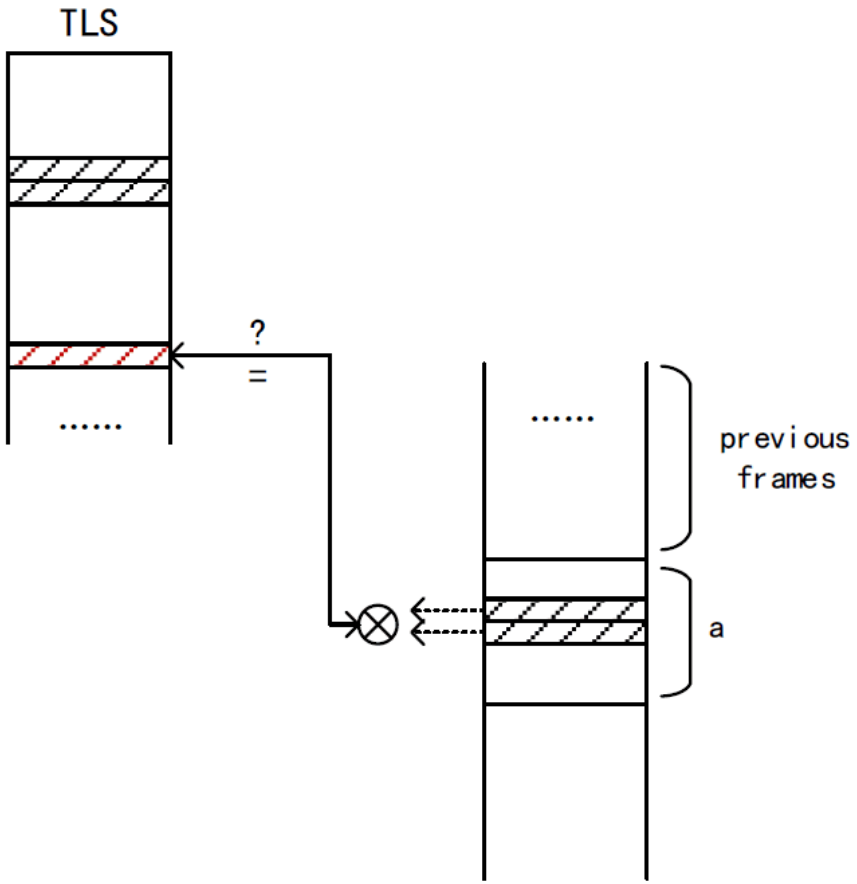
Canary-Based Protection
Polymorphic Canary



(b) Loading of Canary in function prologue.

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
33 Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

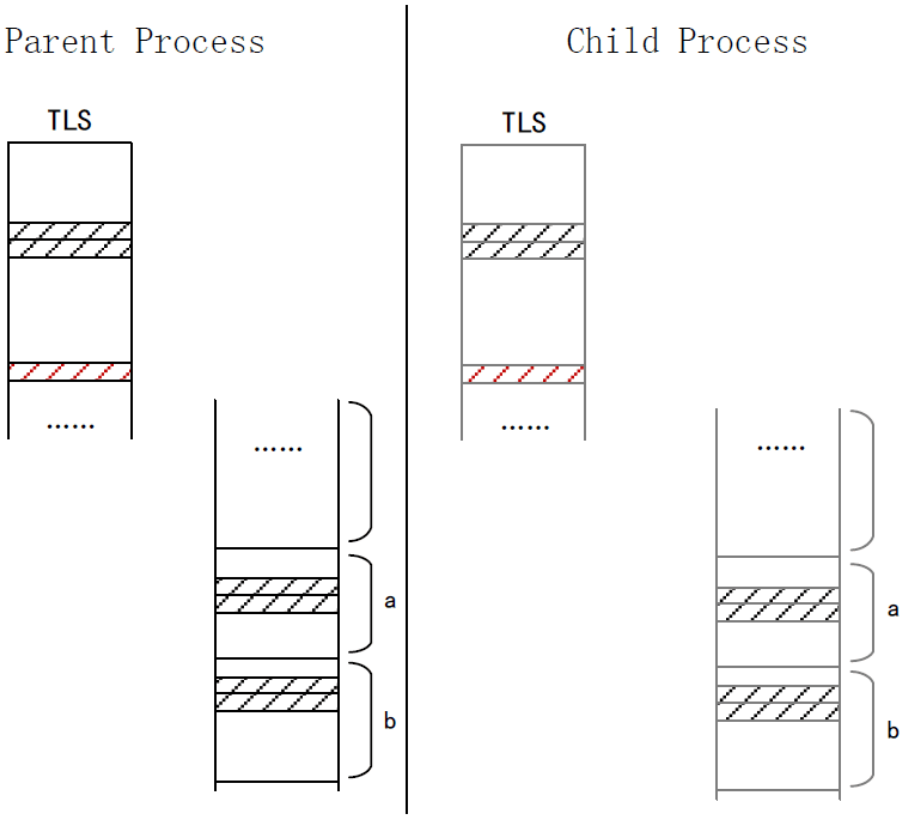
Canary-Based Protection
Polymorphic Canary



(c) Verification of canary in function epilogue.

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
34 Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

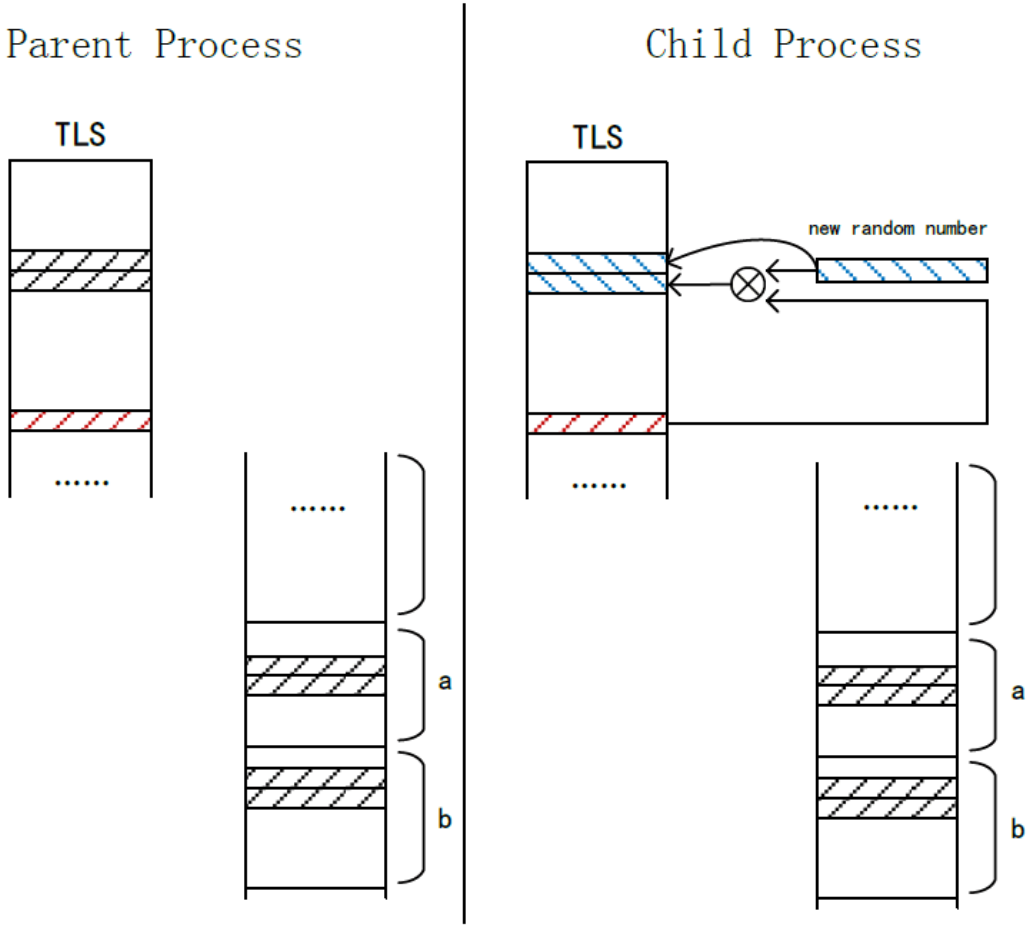
Canary-Based Protection
Polymorphic Canary



(d) The forked (child) process is a copy of the parent.

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
35 Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

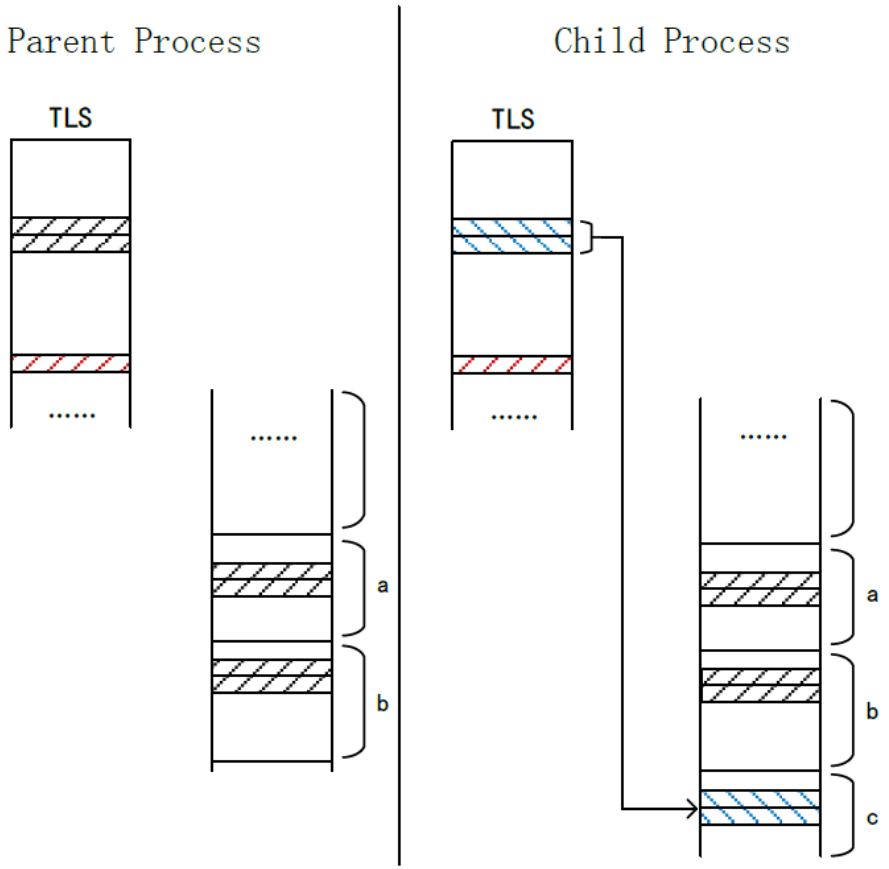
Canary-Based Protection
Polymorphic Canary



(a) Updating of canary in the child process.

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
36 Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

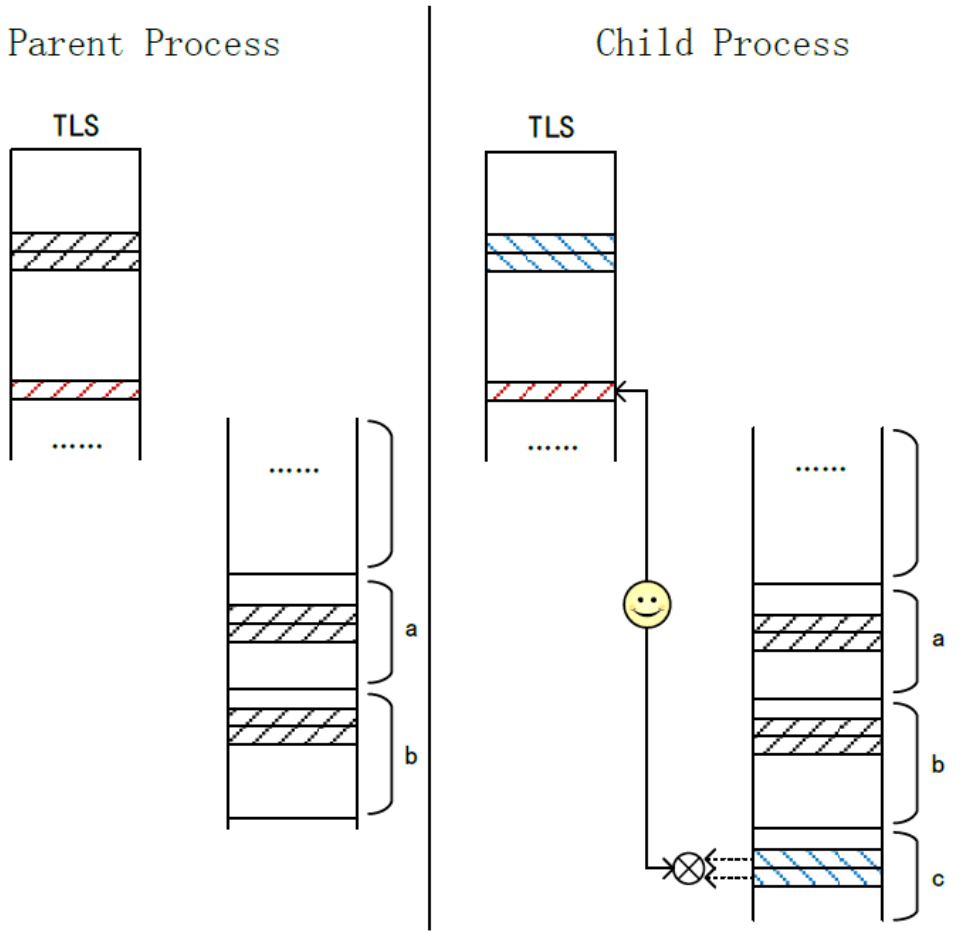
Canary-Based Protection
Polymorphic Canary



(b) Loading of canary in stack frame generated by child-process.

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
37 Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Canary-Based Protection
Polymorphic Canary

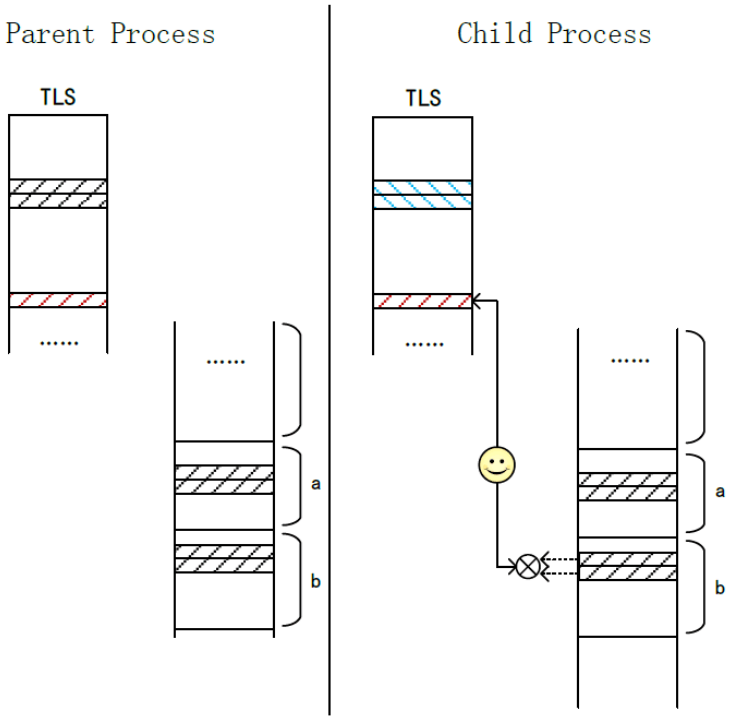


(c) Verification of canary in child-process's stack frame.

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
38 Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Canary-Based Protection
Polymorphic Canary

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
39 Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR



(d) Verification of canary when execution reaches frames inherited from the parent.

Canary-Based Protection
Polymorphic Canary

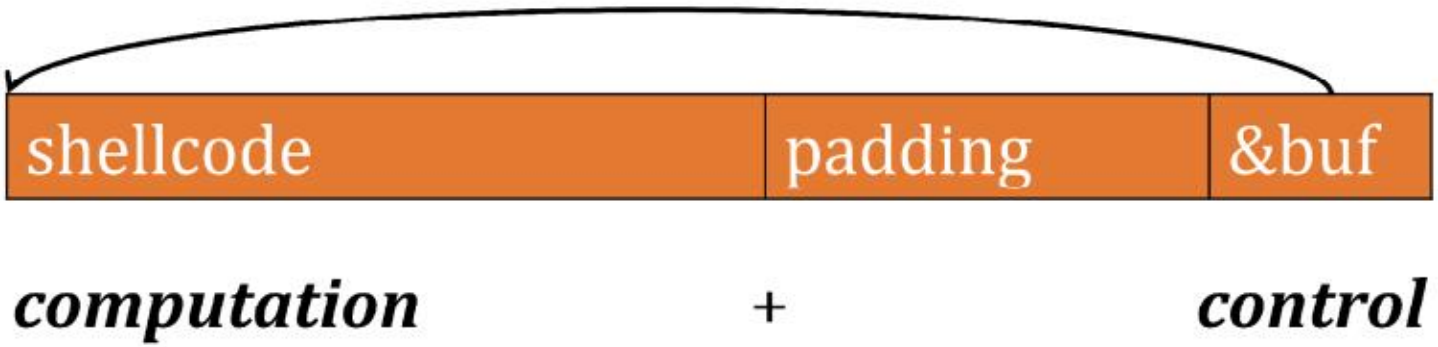
```
;function prologue
55                      push   %rbp
48 89 e5                mov    %rsp,%rbp
48 83 ec 10             sub    $0x10,%rsp
64 48 8b 04 25 a8 02    mov    %fs:0x2a8,%rax
00 00
48 89 45 f8             mov    %rax,-0x8(%rbp)
64 48 8b 04 25 b0 02    mov    %fs:0x2b0,%rax
00 00
48 89 45 f0             mov    %rax,-0x10(%rbp)

        ......
;canary check
48 8b 55 f8             mov    -0x8(%rbp),%rdx
48 8b 7d f0             mov    -0x10(%rbp),%rdx
48 31 fa                xor    %rdi,%rdx
64 48 33 14 25 a0 02    xor    %fs:0x2a0,%rdx
00 00
74 09                   je     Label
e8 80 fd ff ff          callq <__stack_chk_fail@plt>
                        Label:
c9                      leaveq
c3                      retq
```


Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
40 Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Data Execution Prevention

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
41 Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

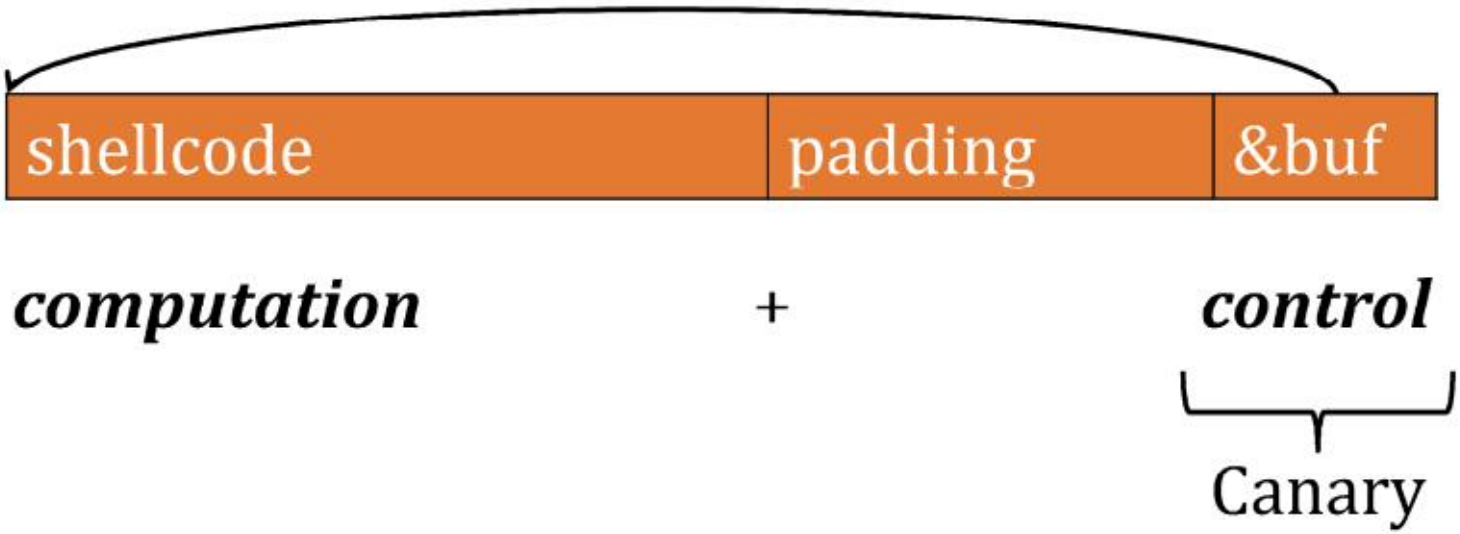
How to defeat exploits



Data Execution Prevention

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
42 Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

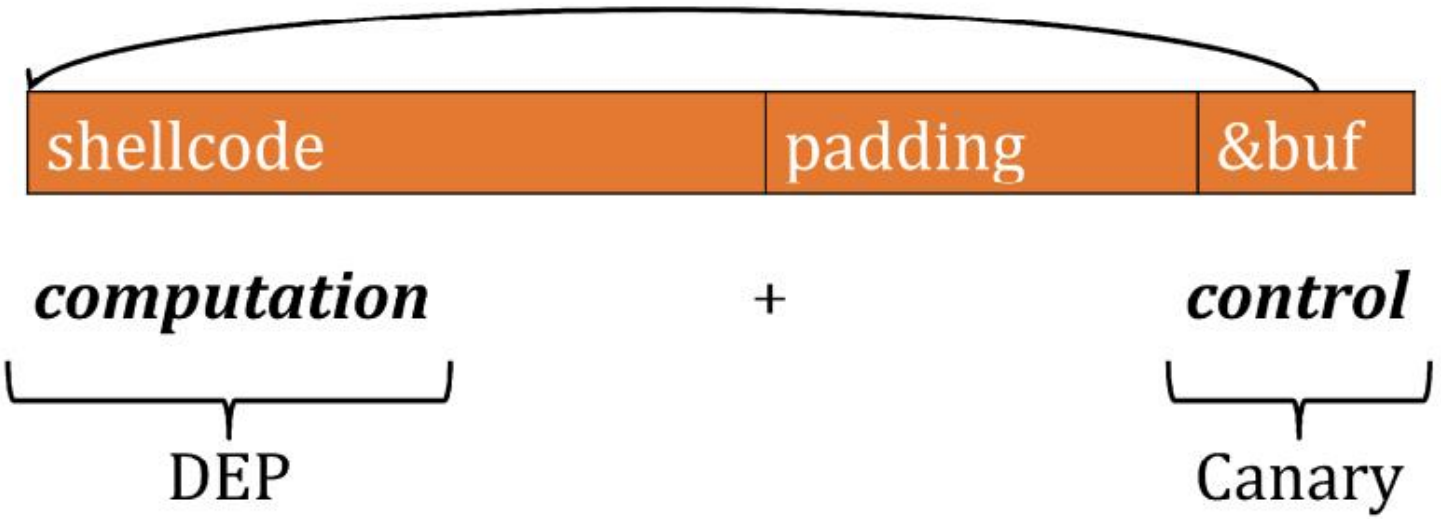
How to defeat exploits



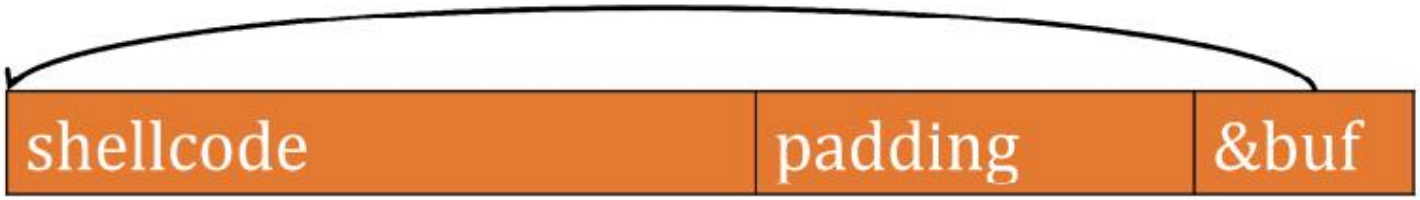
Data Execution Prevention

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
43 Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

How to defeat exploits



Data Execution Prevention
Definition



Mark stack as non-executable using NX bit

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
44 Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Data Execution Prevention
Definition

Mark stack as non-executable using NX bit

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
45 Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Data Execution Prevention
Definition

Mark stack as non-executable using NX bit

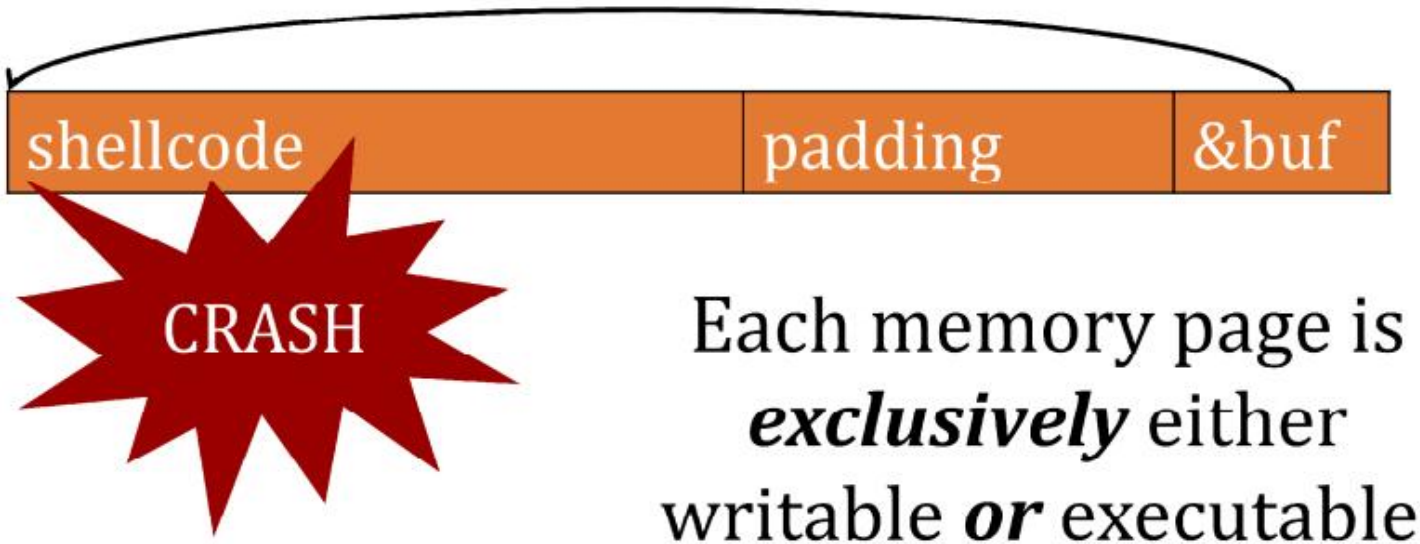
(still a Denial-of-Service attack!)

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
46 Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Data Execution Prevention
Definition

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
47 Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

W ^ X



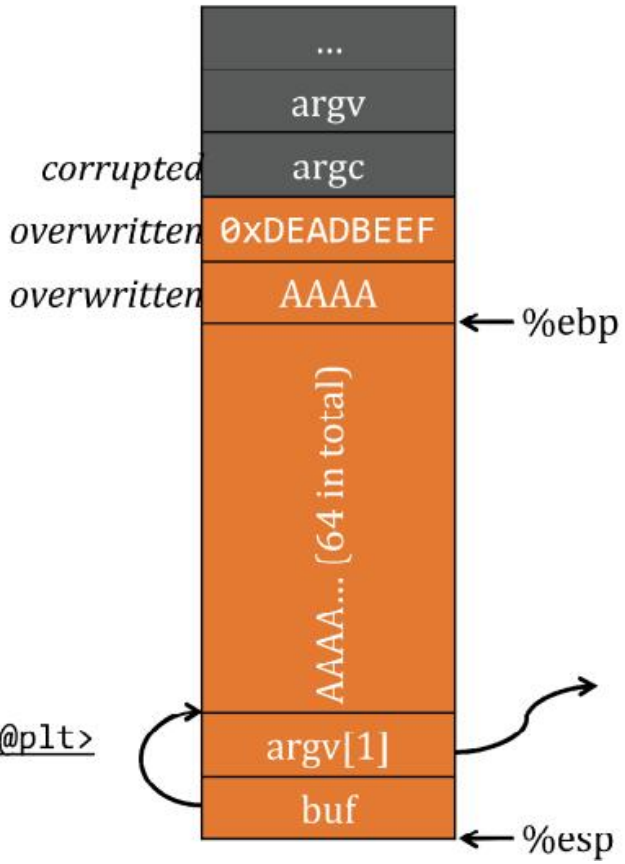
Each memory page is ***exclusively*** either writable ***or*** executable.

(still a Denial-of-Service attack!)

Data Execution Prevention
Definition

"A"x68 . " \xEF \xBE \xAD\xDE"(cannot be executed)

```
#include<string.h>
int main(int argc, char **argv) {
    char buf[64];
    strcpy(buf, argv[1]);
}

Dump of assembler code for function main:
   0x080483e4 <+0>:  push   %ebp
   0x080483e5 <+1>:  mov    %esp,%ebp
   0x080483e7 <+3>:  sub    $72,%esp
   0x080483ea <+6>:  mov    12(%ebp),%eax
   0x080483ed <+9>:  mov    4(%eax),%eax
   0x080483f0 <+12>: mov    %eax,4(%esp)
   0x080483f4 <+16>: lea    -64(%ebp),%eax
   0x080483f7 <+19>: mov    %eax,(%esp)
   0x080483fa <+22>: call   0x8048300 <strcpy@plt>
   0x080483ff <+27>: leave
   0x08048400 <+28>: ret
```



Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
48
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
49 DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

DEP scorecard

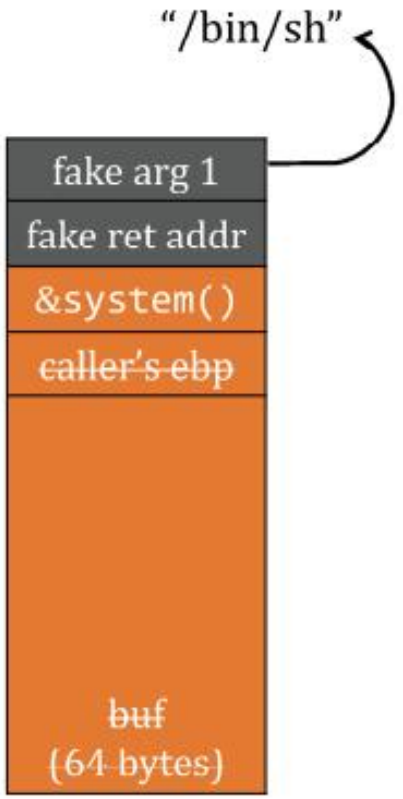
Aspect	DEP
Performance	With hardware support: no impact Otherwise: reported to bel <1% in PaX
Deployment	Kernel support (common on all platforms) Modules opt-in (less frequent in Windows)
Compatibility	Can break ligitimate programs JIT compilers; unpackers
Safety Guarantee	Code injected to NX pages never execugted But code injection may not be necessary ...

Data Execution Prevention
Return-to-libc Attack

Overwrite return address by address of a libc function

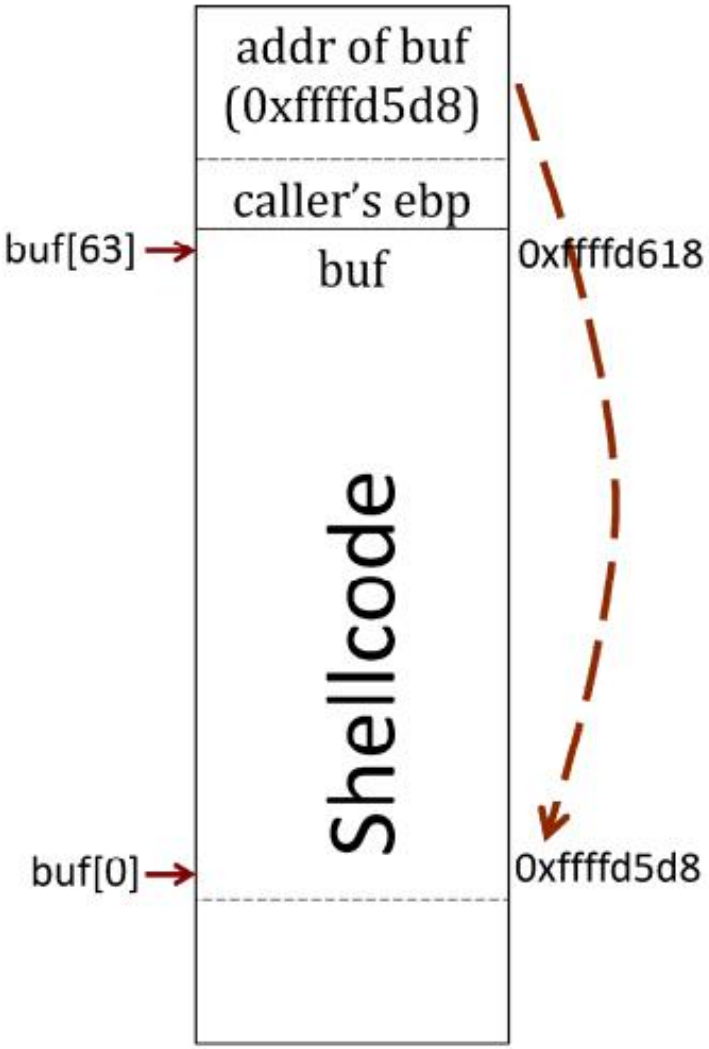
- setup fake return address and argument(s)
- `ret` will "call" libc function

No injected code!



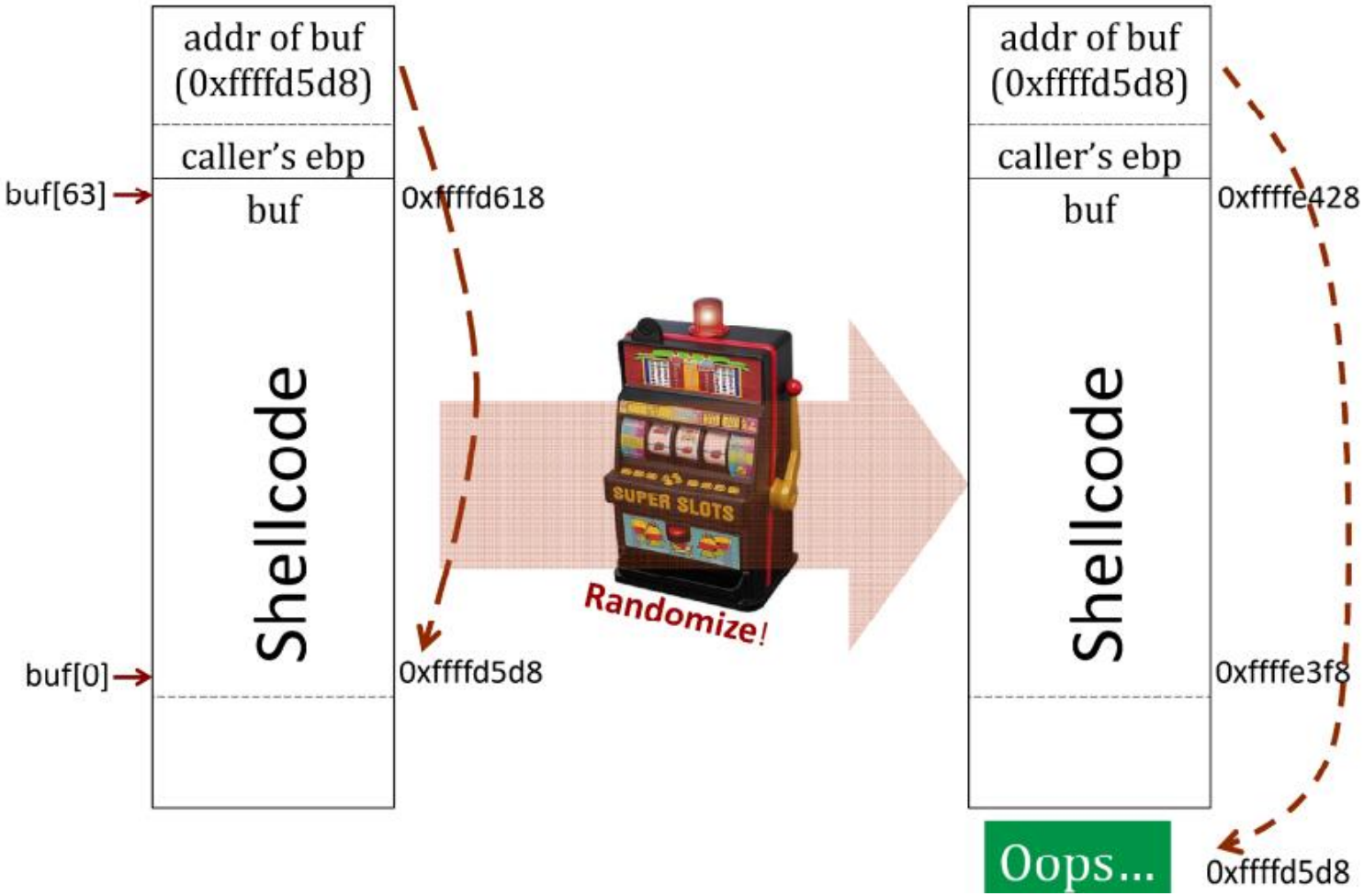
Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
50 Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

ASLR



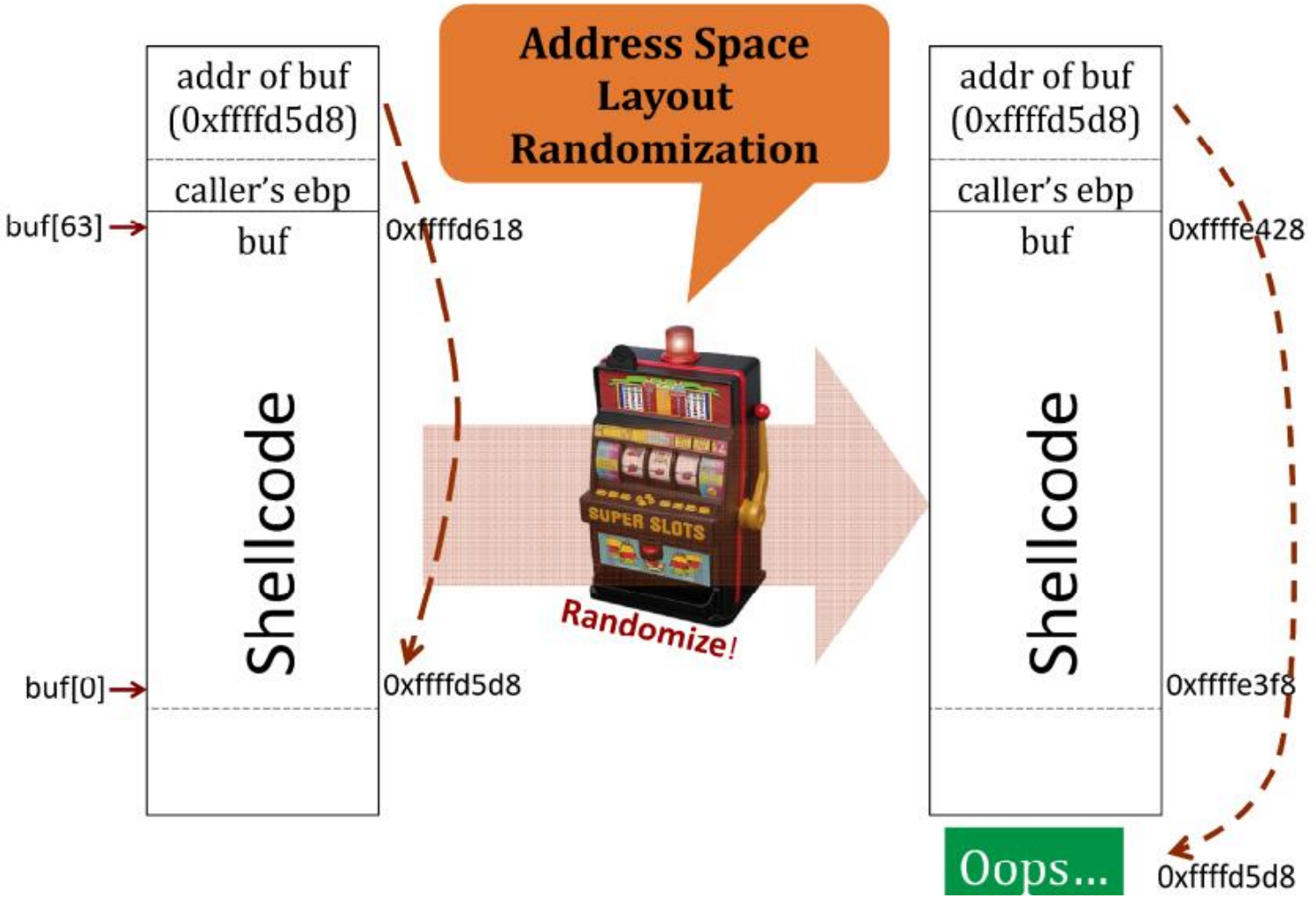
Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
51 ASLR
ASLR Randomization
ASLR

ASLR



Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
52 ASLR
ASLR Randomization
ASLR

ASLR



Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
53 ASLR
ASLR Randomization
ASLR

ASLR

Traditional exploits need precise address

- Stack-based overflows: location of shellcode
- Return-to-libc: library address
- Program: program's memory layout is fixed
  - stack, heap, libraries, etc
- Solution: randomize address of each region

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
54 ASLR
ASLR Randomization
ASLR

ASLR

Running cat twice

- Run 1

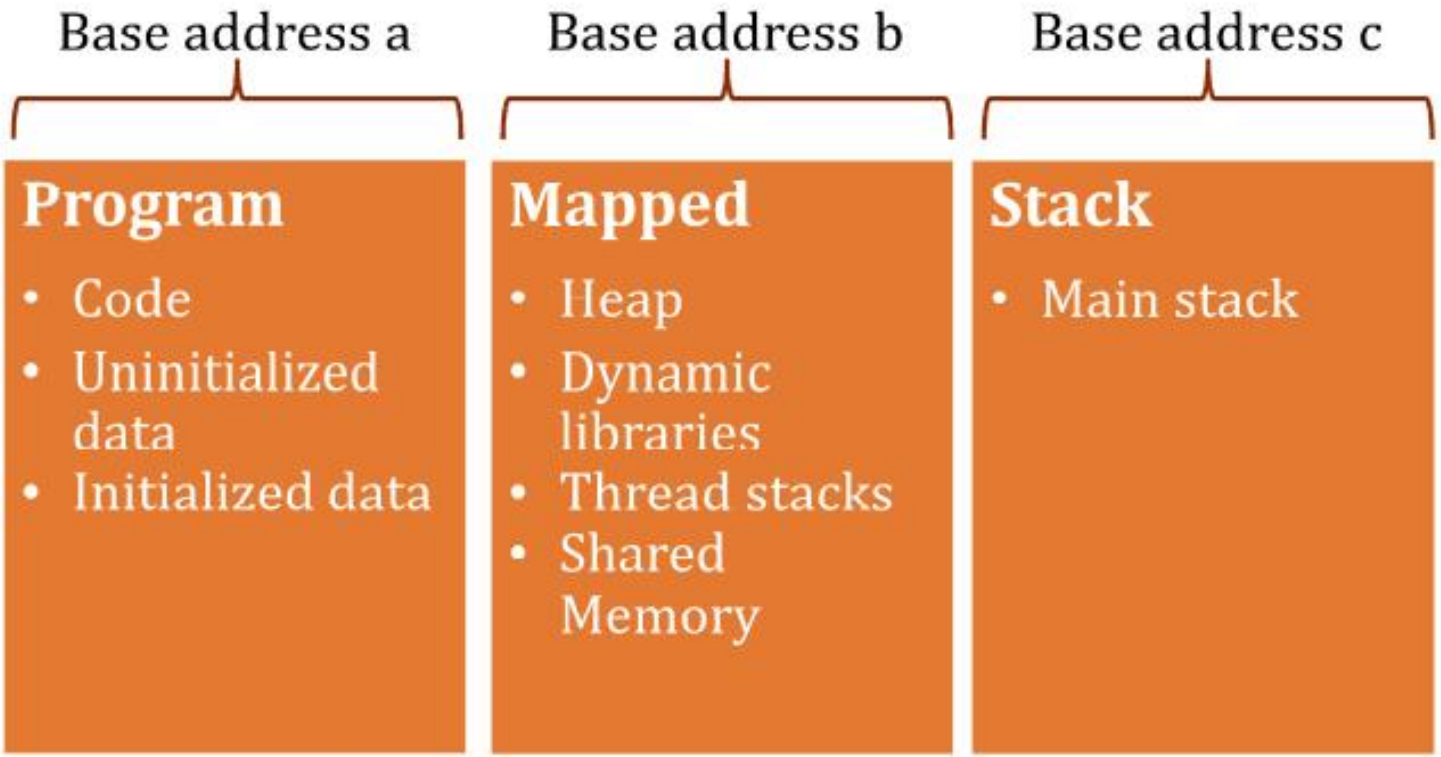
```
exploit:~# cat /proc/self/maps | egrep '(libc|heap|stack)'
082ac000-082cd000 rw-p 082ac000 00:00 0          [heap]
b7dfe000-b7f53000 r-xp 00000000 08:01 1750463    /lib/i686/cmov/libc-2.7.so
b7f53000-b7f54000 r--p 00155000 08:01 1750463    /lib/i686/cmov/libc-2.7.so
b7f54000-b7f56000 rw-p 00156000 08:01 1750463    /lib/i686/cmov/libc-2.7.so
bf966000-bf97b000 rw-p bffeb000 00:00 0          [stack]
```

- Run 2

```
exploit:~# cat /proc/self/maps | egrep '(libc|heap|stack)'
086e8000-08709000 rw-p 086e8000 00:00 0          [heap]
b7d9a000-b7eef000 r-xp 00000000 08:01 1750463    /lib/i686/cmov/libc-2.7.so
b7eef000-b7ef0000 r--p 00155000 08:01 1750463    /lib/i686/cmov/libc-2.7.so
b7ef0000-b7ef2000 rw-p 00156000 08:01 1750463    /lib/i686/cmov/libc-2.7.so
bf902000-bf917000 rw-p bffeb000 00:00 0          [stack]
```

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
55 ASLR
ASLR Randomization
ASLR

ASLR
ASLR Randomization



Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

Background
Control Flow Hijack
Control Flow Hijack Defense
Canary Defense
StackGuard
StackGuard Weakness
DiffGuard
Polymorphic Canary
Data Execution Prevention
Definition
DEP Scorecard
Return-to-libc Attack
ASLR
ASLR Randomization
ASLR

ASLR scorecard

Aspect	ASLR
Performance	Excellent — ramdomize once at load time
Deployment	Turn on kernel support No recompilation necessary
Compatibility	Transpartent to safe apps (Position independent)
Safety Guarantee	Not good on x32, much better on x64 But code injection may not be necessary ...