Evasión de ASLR y DEP mediante ROP

Erlantz Saenz - Innotec System

@3lr3l

@erlsaenz

Indice

- Exploiting
- Motivación
- DEP
  - Bypass
- ASLR
  - Bypass

Exploiting

- Rama de la seguridad informática
- Aprovechar un fallo para realizar otra acción
- DOS, obtención shell, elevación de privilegios...
- No es reversing
- No es fuzzing

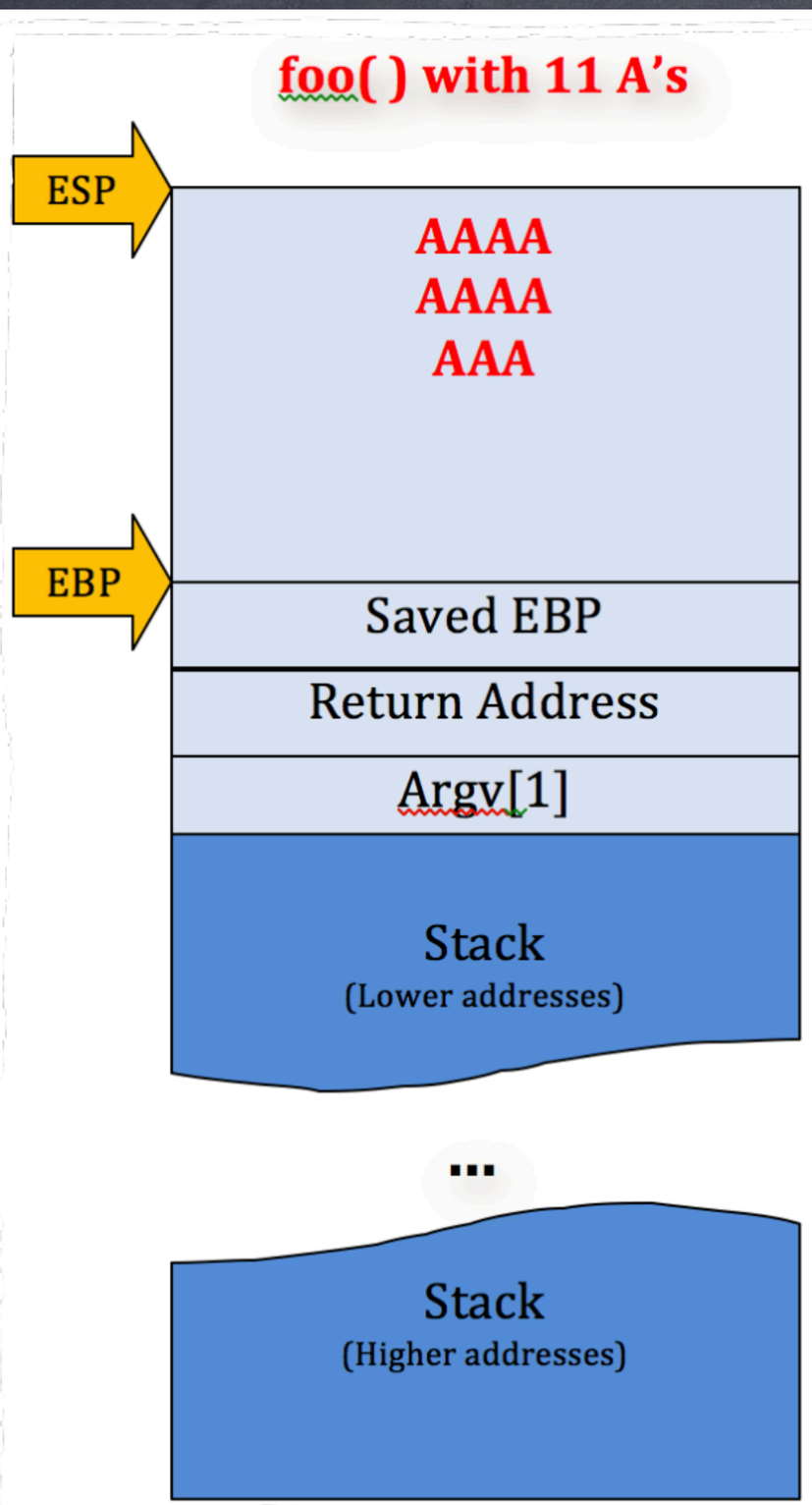
ZERODIUM Payouts for Mobiles*

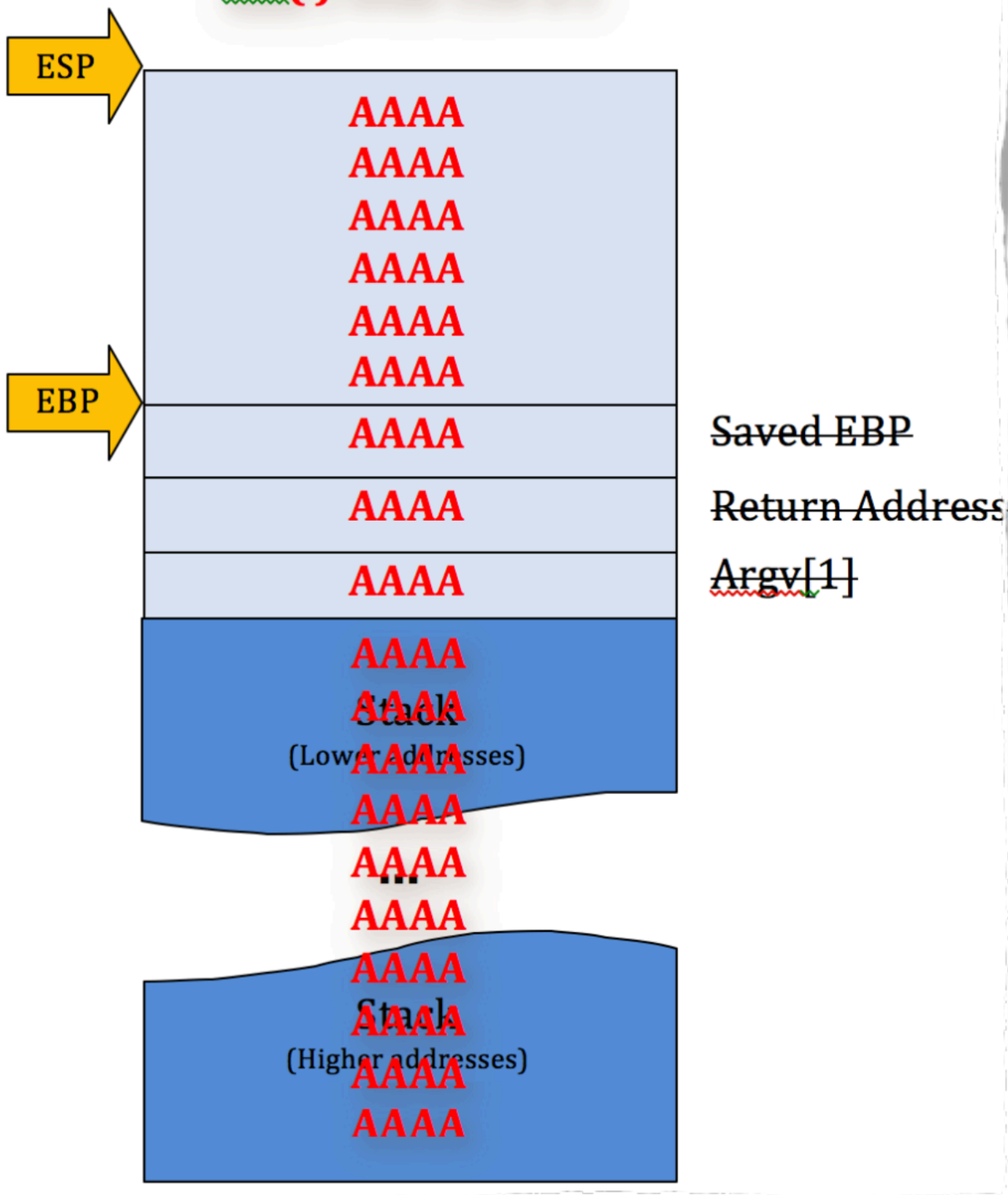
RJB: Remote Jailbreak with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

iOS
Android
Any OS

Up to $1,500,000										1.001 iPhone RJB Zero Click (iOS)
Up to $1,000,000										1.002 iPhone RJB (iOS)
Up to $500,000	2.001 WeChat RCE+LPE (iOS/Android)	2.002 Viber RCE+LPE (iOS/Android)		2.003 FB Messenger RCE+LPE (iOS/Android)	2.004 Signal RCE+LPE (iOS/Android)	2.005 Telegram RCE+LPE (iOS/Android)	2.006 WhatsApp RCE+LPE (iOS/Android)	2.007 iMessage RCE+LPE (iOS)	2.008 SMS/MMS RCE+LPE (iOS/Android)	2.009 Email App RCE+LPE (iOS/Android)
Up to $200,000	3.001 Baseband RCE+LPE (iOS/Android)								4.001 Chrome RCE+SBX (Android)	4.002 Safari RCE+SBX (iOS)
Up to $100,000	5.001 Code Signing Bypass (iOS)	3.002 WiFi RCE+LPE (iOS/Android)		2.010 Media Files RCE (iOS/Android)	2.011 Documents RCE (iOS/Android)	6.001 LPE to Kernel (iOS/Android)	4.003 SBX for Chrome (Android)	4.004 Chrome RCE w/o SBX (Android)	4.005 SBX for Safari (iOS)	4.006 Safari RCE w/o SBX (iOS)
Up to $50,000	5.002 Code Signing Bypass (Android)	5.003 Secure Boot (iOS)	3.003 RCE via MitM (iOS/Android)					6.002 LPE to Root (iOS/Android)	4.007 Chrome UXSS/SOP (iOS/Android)	4.008 Safari UXSS/SOP (iOS)
Up to $25,000	5.004 TrustZone (Android)	5.005 Verified Boot (Android)			6.003 LPE to System (Android)	7.001 ASLR Bypass (iOS/Android)	7.002 kASLR Bypass (iOS/Android)	7.003 Seccomp Bypass (Android)	7.004 RKP Bypass (Android)	7.005 Knox Bypass (Android)
Up to $15,000	9.001 Information Disclosure (iOS/Android)							8.001 Passcode Bypass (iOS)	8.002 Touch ID Bypass (iOS)	8.003 PIN Bypass (Android)

** All payouts are subject to change or cancellation without notice, at the discretion of ZERODIUM. All trademarks are the property of their respective owners.*


foo( ) with 11 A's
ESP
AAAA
AAAA
AAA
EBP
Saved EBP
Return Address
Argv[1]
Stack
(Lower addresses)
...
Stack
(Higher addresses)


foo( ) with 150 A's
ESP
AAAA
AAAA
AAAA
AAAA
AAAA
AAAA
EBP
AAAA
Saved EBP
AAAA
Return Address
AAAA
Argv[1]
Stack
(Lower addresses)
...
Stack
(Higher addresses)

DEP

- Data Execution Prevention
- Impide la ejecución de código en el stack

DEP

Immunity Debugger - RM2MP3Converter.exe - [CPU - main thread]

File View Debug Plugins ImmLib Options Window Help Jobs

l e m t w h c P k b z r ... s ? Code auditor and software assessme

```
0015F614  CC          INT3
0015F615  CC          INT3
0015F616  CC          INT3
0015F617  CC          INT3
0015F618  CC          INT3
0015F619  CC          INT3
0015F61A  CC          INT3
0015F61B  CC          INT3
0015F61C  CC          INT3
0015F61D  CC          INT3
0015F61E  CC          INT3
0015F61F  CC          INT3
0015F620  CC          INT3
0015F621  CC          INT3
0015F622  CC          INT3
0015F623  CC          INT3
0015F624  CC          INT3
0015F625  CC          INT3
0015F626  CC          INT3
0015F627  CC          INT3
0015F628  CC          INT3
0015F629  CC          INT3
0015F62A  CC          INT3
0015F62B  CC          INT3
0015F62C  CC          INT3
```

```
Registers (FPU)
EAX 00000001
ECX 7720387A ntdll.7720387A
EDX 02270578
EBX 00164A1C
ESP 0015F614
EBP 005C2E58 ASCII "C:\Users\corelan_h3ku\Des
ESI 76412960 msvcrt.76412960
EDI 00008A0E

EIP 0015F614

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 0  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 7EFDD000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00010206 (NO,NB,NE,A,NS,PE,GE,G)

ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
```

```
Address   Hex dump                ASCII
00446000  00 00 00 00 31 7A 43 00  ....1zC.
00446008  30 54 40 00 80 54 40 00  0T@.ÇT@.
00446010  00 56 40 00 30 57 40 00  .V@.0W@.
00446018  80 3F 41 00 60 C4 42 00  Ç?A.'-B.
00446020  F0 C4 42 00 10 5D 43 00  ≡-B.▶]C.
00446028  90 60 43 00 00 00 00 00  -`C.....
00446030  00 00 00 00 00 00 00 00  ........
00446038  00 00 00 00 00 00 00 00  ........
00446040  53 65 6C 65 63 74 20 74  Select t
00446048  68 65 20 44 69 72 65 63  he Direc
00446050  74 6F 72 79 20 79 6F 75  tory you
00446058  20 77 69 73 68 20 74 6F   wish to
00446060  20 6F 75 74 70 75 74 2E   output.
```

```
0015F614  CCCCCCCC  ╠╠╠╠
0015F618  CCCCCCCC  ╠╠╠╠
0015F61C  CCCCCCCC  ╠╠╠╠
0015F620  CCCCCCCC  ╠╠╠╠
0015F624  CCCCCCCC  ╠╠╠╠
0015F628  CCCCCCCC  ╠╠╠╠
0015F62C  CCCCCCCC  ╠╠╠╠
0015F630  CCCCCCCC  ╠╠╠╠
0015F634  CCCCCCCC  ╠╠╠╠
0015F638  CCCCCCCC  ╠╠╠╠
0015F63C  CCCCCCCC  ╠╠╠╠
0015F640  CCCCCCCC  ╠╠╠╠
0015F644  CCCCCCCC  ╠╠╠╠
0015F648  CCCCCCCC  ╠╠╠╠
```

```
!mona jmp -r esp
```

```
[17:17:31] Access violation when executing [0015F614] - use Shift+F7/F8/F9 to pass
```

Paused

Bypass DEP

- ROP - Code reuse -> Uso de gadgets

API / OS	XP SP2	XP SP3	Vista SP0	Vista SP1	Windows 7	Windows 2003 SP1	Windows 2008
VirtualAlloc	yes	yes	yes	yes	yes	yes	yes
HeapCreate	yes	yes	yes	yes	yes	yes	yes
SetProcessDEPPolicy	no (1)	yes	no (1)	yes	no (2)	no (1)	yes
NtSetInformationProcess	yes	yes	yes	no (2)	no (2)	yes	no (2)
VirtualProtect	yes	yes	yes	yes	yes	yes	yes
WriteProcessMemory	yes	yes	yes	yes	yes	yes	yes

Fuente: https://www.corelan.be/index.php/2010/06/16/exploit-writing-tutorial-part-10-chaining-dep-with-rop-the-rubikstm-cube/

ASLR

- Address Space Layout Randomization
- Protección a la hora de compilar
- Evita la predicción de direcciones de memoria

ASLR

```
76070000 Modules C:\Windows\syswow64\comdlg32.dll
76150000 Modules C:\Windows\syswow64\GDI32.dll
761E0000 Modules C:\Windows\syswow64\LPK.dll
76200000 Modules C:\Windows\syswow64\kernel32.dll
76370000 Modules C:\Windows\syswow64\SHLWAPI.dll
76420000 Modules C:\Windows\syswow64\msvcrt.dll
76430000 Modules C:\Windows\syswow64\NSI.dll
76480000 Modules C:\Windows\syswow64\WLDAP32.dll
76680000 Modules C:\Windows\syswow64\iertutil.dll
768D0000 Modules C:\Windows\syswow64\ole32.dll
```

```
76FC0000 Modules C:\Windows\syswow64\WS2_32.dll
77120000 Modules C:\Windows\syswow64\MSCTF.dll
772D0000 Modules C:\Windows\syswow64\USP10.dll
77380000 Modules C:\Windows\syswow64\comdlg32.dll
773D0000 Modules C:\Windows\SysWOW64\sechost.dll
77520000 Modules C:\Windows\syswow64\msvcrt.dll
77720000 Modules C:\Windows\syswow64\RPCRT4.dll
77C10000 Modules C:\Windows\system32\IMM32.DLL
```

ASLR

```
00400000 Modules C:\Program Files (x86)\Easy RM to MP3 Converter\RM2MP3Converter.exe
01FD0000 Modules C:\Program Files (x86)\Easy RM to MP3 Converter\MSRMfilter01.dll
02070000 Modules C:\Program Files (x86)\Easy RM to MP3 Converter\wmatimer.dll
02250000 Modules C:\Program Files (x86)\Easy RM to MP3 Converter\MSLog.dll
034E0000 Modules C:\Program Files (x86)\Easy RM to MP3 Converter\MSRMCcodec00.dll
10000000 Modules C:\Program Files (x86)\Easy RM to MP3 Converter\MSRMfilter03.dll
```

```
00260000 Modules C:\Program Files (x86)\Easy RM to MP3 Converter\MSRMCcodec01.dll
00280000 Modules C:\Program Files (x86)\Easy RM to MP3 Converter\MSRMfilter02.dll
00400000 Modules C:\Program Files (x86)\Easy RM to MP3 Converter\RM2MP3Converter.exe
02060000 Modules C:\Program Files (x86)\Easy RM to MP3 Converter\MSRMfilter01.dll
035E0000 Modules C:\Program Files (x86)\Easy RM to MP3 Converter\MSRMCcodec00.dll
10000000 Modules C:\Program Files (x86)\Easy RM to MP3 Converter\MSRMfilter03.dll
```

Bypass ASLR

- Evitar el uso de ASLR
- Sobre-escritura parcial de la dirección
- Fuerza bruta sobre la dirección
- Leak de memoria

Rebase	SafeSEH	ASLR	NXCompat	OS Dll	Version, Modulename & Path
True	True	True	True	True	7.0.7600.16385 [MSVCP60.dll] (C:\Windows\system32\MSVCP60.dll)
True	True	True	True	True	6.1.7600.16385 [WINMM.dll] (C:\Windows\system32\WINMM.dll)
True	True	True	True	True	6.1.7600.16385 [profapi.dll] (C:\Windows\system32\profapi.dll)
True	True	True	True	True	8.00.7600.16385 [urlmon.dll] (C:\Windows\syswow64\urlmon.dll)
False	False	False	False	False	2.7.3.700 [RM2MP3Converter.exe] (C:\Program Files (x86)\Easy RM to MP3
True	True	True	True	True	6.1.7600.16385 [IphlpapI.DLL] (C:\Windows\System32\IphlpapI.DLL)
True	True	True	True	True	6.1.7600.16385 [CRYPT32.dll] (C:\Windows\syswow64\CRYPT32.dll)
True	True	True	True	True	6.1.7601.17514 [MSASN1.dll] (C:\Windows\syswow64\MSASN1.dll)
True	True	True	True	True	6.1.7600.16385 [wship6.dll] (C:\Windows\System32\wship6.dll)
True	True	True	True	True	6.1.7600.16385 [kernel32.dll] (C:\Windows\syswow64\kernel32.dll)
True	True	True	True	True	7.0.7600.16385 [msvcrt.dll] (C:\Windows\syswow64\msvcrt.dll)