基于二进制动态翻译的ROP攻击检测方法研究与实现

[第一章 绪论 2](#_Toc537461048)

[1.1 研究背景 2](#_Toc408956174)

[1.2 ROP攻击及防御现状(Ret-to-libc, rop, jop, xop) 3](#_Toc225838643)

[1.3 本文主要研究内容 4](#_Toc1490552290)

[1.3.1 ROP攻击的动态特征提取 4](#_Toc1477718138)

[1.3.2 ROP攻击防御方案与实现 4](#_Toc1871259387)

[1.4 本文组织结构 4](#_Toc1005023963)

[第二章 ROP攻击与防御分析 5](#_Toc283566547)

[2.1 ROP攻击 5](#_Toc1771018586)

[2.2.1 原理 5](#_Toc511241381)

[2.2.2 攻击流程 5](#_Toc79717727)

[2.2.3 变种攻击 6](#_Toc748803773)

[2.2 ROP防御 6](#_Toc1785821585)

[2.2.1 基于随机化 6](#_Toc989055314)

[2.2.2 基于运行时状态监控 7](#_Toc1335109704)

[2.2.3 基于控制流 7](#_Toc1541411541)

[2.3 本章小结 7](#_Toc831051143)

[第三章 二进制动态翻译技术及工具(相关技术PIN\攻击\防御) 7](#_Toc1554256545)

[3.1 二进制动态翻译技术原理 7](#_Toc205995882)

[3.2 PIN框架介绍 7](#_Toc1269503935)

[第四章 常见ROP攻击方法 7](#_Toc500617718)

[4.1 绕过随机化防护 7](#_Toc350578704)

[4.2 调用敏感libc函数 7](#_Toc1090224523)

[4.3 篡改虚函数表/全局偏移量表 7](#_Toc37162414)

[第五章 基于PIN的ROP攻击检测方法与实现 7](#_Toc1521568845)

[5.1 假设 7](#_Toc1195643901)

[5.2 总体设计 7](#_Toc2044542505)

[5.3 系统概述(总体实现) 8](#_Toc2111691605)

[5.4 实现细则 8](#_Toc2098754403)

[5.5 界面实现 9](#_Toc1489179390)

[5.6 实验与评估 9](#_Toc768943937)

[5.7 本章小结 9](#_Toc488731804)

[第六章 总结和展望 9](#_Toc1898135564)

[5.1 总结 9](#_Toc994782580)

[5.2 展望 9](#_Toc1979284094)

[参考文献 9](#_Toc1228370055)

1. **绪论**
   1. 研究背景

如今无论计算机技术发展到何种程度，计算机软件安全永远是人们最为关心的话题，相关的研究总在不断地进展和延续。随着操作系统的更新换代，软件自身的安全性不断提升，针对各种攻击类型，大量防御策略被提出并应用，对软件进行攻击变得越发困难。但是由于操作系统代码量日益增大、复杂度逐步提高，攻击者总能找出系统漏洞，并利用漏洞进行攻击，如图1-1所示，CVE[1]漏洞数量呈现逐年提升的趋势。此外，程序员编程的不规范以及软件安全更新的不及时更是导致软件漏洞被广泛利用。软件漏洞的必然存在，就像一颗定时炸弹，带来了极大的安全隐患。例如勒索病毒WannaCry利用美国国家安全局泄露的危险漏洞“EternalBlue”（永恒之蓝）进行传播，从2018年初到9月中旬，总计对超过200万台终端发起过攻击，攻击次数高达1700万余次，该病毒通过互联网在全球爆发，国内大量高校及企事业单位被攻击。

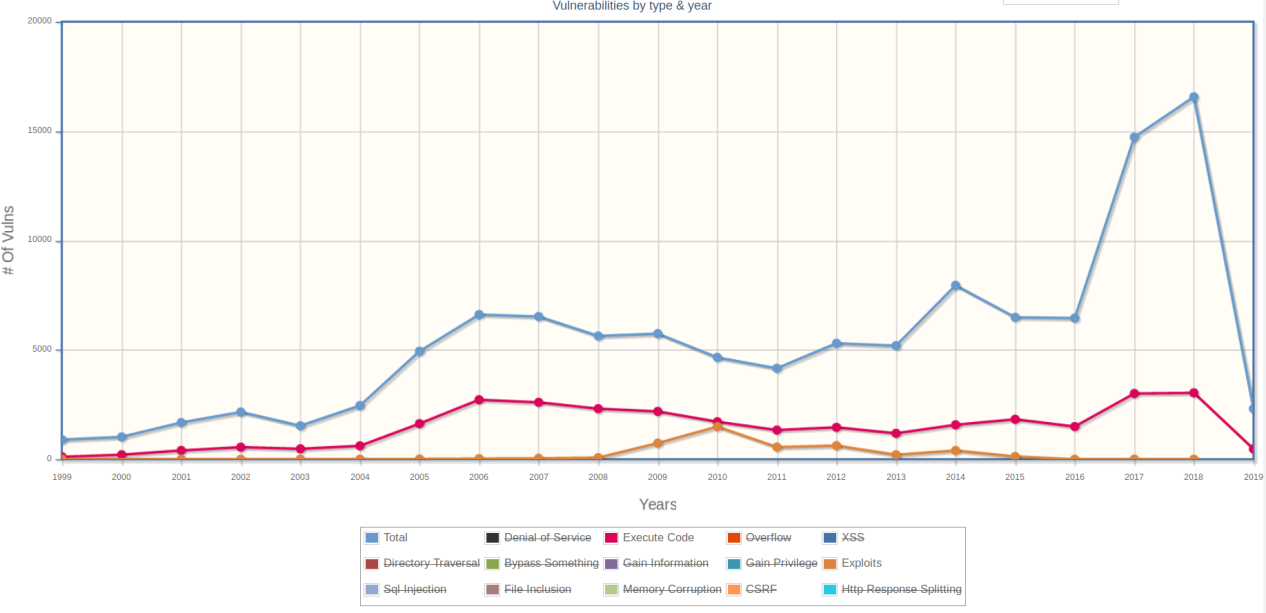


图1-1 近20年CVE漏洞数量

在众多的安全漏洞中，如图1-2，二进制安全占据了半壁江山，其中缓冲区溢出(buffer overflow)是一种常见的漏洞。由于c语言对程序缓冲区边界不进行检测，当攻击者向缓冲区写入过多数据后，缓冲区将溢出。若缓冲区在栈中发生溢出，栈中的函数返回地址将被覆盖，当程序返回时，程序控制流将被攻击者劫持。此外整型溢出、浮点型溢出、格式化字符串、UAF等常见漏洞，均可使攻击者劫持程序控制流。劫持程序控制流，然后执行攻击者构建的攻击代码，是进行攻击的基本流程。早先攻击者将恶意代码注入内存空间，并将控制流劫持至恶意代码，从而达到攻击目的。这些被注入的代码称做shellcode，他们通常是可执行的代码，通过系统调用实现打开shell、更改系统权限、执行程序等恶意行为。

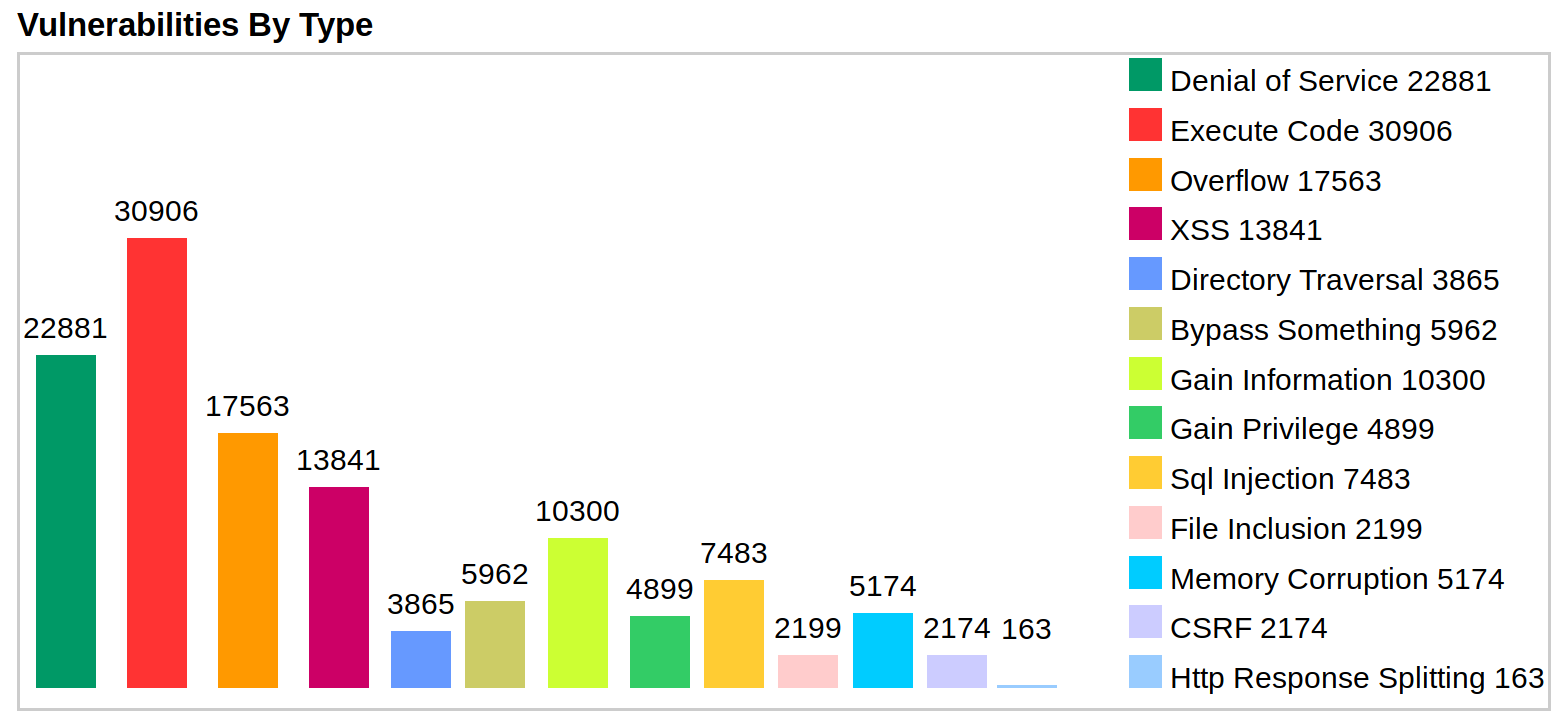


图1-2 近20年各类CVE漏洞数量统计

但是在数据执行保护（DEP）[2]广泛采用后，内存中的所有可写页面均不具有可执行权限。因此，即使攻击者将程序控制流劫持至他们注入的恶意代码，这些代码也无法执行。为了绕过DEP机制实现攻击，攻击者不再注入代码，而是通过利用漏洞进程中的现有的可执行指令来构造恶意行为，即代码复用攻击（CRA）。根据复用的代码类型不同，代码复用攻击主要可分为Return-into-libc和ROP攻击。

* 1. ROP攻击及防御发展现状

1.2.1 ROP攻击发展现状

Return-into-libc[3]是代码复用攻击的一种简单应用，攻击者利用缓冲区溢出漏洞，将栈中的返回地址覆写为某个函数的入口地址，从而使得该函数被执行。复用的函数可以是程序代码段中的函数，也可以是程序所链接的共享库中的函数。攻击者通过修改栈的布局或者寄存器中的数据，构造函数参数，从而实现完整的函数调用，进而实现攻击行为。例如：攻击者复用共享库libc中的system、execve等函数，可执行任意系统命令；复用具有输出功能的函数，如write,puts等，可以获取更多关于程序的信息，比如环境变量、所链接的共享库等；复用具有修改内存功能的函数，如read,malloc等，可以对内存进行任意写操作。

返回导向编程[4]（ROP）是一种常用的代码复用攻击技术，不同于Return-into-libc，攻击者在返回导向编程时，不执行整个函数，而是执行源自各函数片段中的指令序列。这些指令序列称作gadget，具有如下两个基本特点：1.具有一定的功能，如：寄存器相加、加载某值到内存等；2.以ret指令为结尾。攻击者首先搜索可用gadget，然后将各个gadget链接在一起，从而实现一次完整的攻击（详见2.2节）。ROP最初由Shacham[4]提出并应用于x86平台，随后被拓展到其他体系结构[5,6,7,8]。ROP已被证明可实现图灵完备计算[9]。此外，一些允许攻击者使用ROP自动构造任意恶意程序的工具已被开发出[10,11,12,13]。

在目前使用最广的64位x86平台下，被调函数的参数主要保存在寄存器中，因此在一般情况下，攻击者会将Return-into-libc攻击与ROP攻击结合起来，即：进行Return-into-libc攻击时，通过复用一些gadget（如pop rdi）完成函数的参数配置，然后调用函数，进而达到攻击目的。

在x86汇编语言中，call和jmp也能够实现程序控制流的转移，因此将ret指令替换为call指令的Call Oriented Programming(COP)[14]和将ret指令替换为jmp指令的Jump Oriented Programming(JOP)[15]被相继提出。因为传统ROP攻击有着明显的特征，即：使用连续的以ret为结尾的gadget，所以一些防御机制[23,24]识别该特征，对ROP攻击进行防御。上述的变种ROP攻击，不使用或不连续使用以ret指令为结尾的gadget，从而能够绕过这些检测机制。

此外，将Snow[16]还提出了实时ROP，攻击者在程序运行时完成gadget的搜索与链接。Bittau提出了BROP[17]，他指出即使不清楚任何目标服务器的信息，也能够根据服务器返回的内容，搜索gadget并构造攻击。

1.2.2 ROP防御发展现状

针对现有的各种代码复用攻击，研究者提出了几类防御方案：

第一类方案是基于内存地址随机化，通过随机化布局，减少攻击者对内存布局的知晓程度。ASLR[18]是被广泛应用的一种，ASLR在程序共享库、堆栈加载到内存的过程中，为其基址随机增加一个偏移量，从而使攻击者无法准确获取Return-into-libc攻击所需的libc函数地址以及ROP攻击所需的gadget地址。ASLR由于其方法简单，系统开销小，被广泛应用于各Linux操作系统中。ASLR的变种防御相继被提出，随机化粒度也在不断优化[19,20]。

第二类方案是基于程序二进制动态检测技术，通过插桩监测程序运行行为，从而判断程序是否被攻击。Davi[23]等通过构造影子栈，对调用和返回指令进行插桩检测，在函数调用时，将其预期返回地址压入影子栈顶，在函数返回时，将返回地址与栈顶地址作对比，从而阻止非预期的控制流跳转。动态检测技术虽然能获取更多的程序运行时信息，但是也带来了额外的系统开销，使得程序运行放缓。DROP[24]和ROP-Hunt[21]，为了减少额外的系统开销，基于统计学方法，通过设置阈值识别gadget，这些方案虽然性能好，但是不够灵活，防御效果差，容易被攻击者猜到阈值后绕过。

第三类方案是检测程序控制流的完整性，通过监控程序控制流，判断控制流是否按照预期的语义执行，从而防止非预期的代码被复用。Martin[22]等通过构造控制流图(CFG)，确保了语义完整性，但其CFG的生成难以保证准确性。文章[27]中提出了一种基于硬件的完整性保护解决方案。在该方法中，堆栈被分数据栈和专门用于调用和返回的控制栈。CPU采用访问控制机制，不允许用任意数据覆盖控制栈。这有效地防止了ROP攻击，但是，这种方法并不能轻易地移植到常见的复杂指令CPU，如Intel、AMD架构。

还有一些防御方案如CFLocking [25]和G-Free [26]，旨在防御所有类型的ROP攻击，但它们需要用户提供程序源代码，对于一般程序用户而言，程序源代码是难以取得的，因此这些防御方案的应用范围受到了限制。

根据上述的ROP防御思想，本文将使用二进制动态插桩检测框架PIN，提出一种综合方案，应用于ROP攻击的动态防御与检测。

* 1. 二进制动态翻译技术

PIN ... 5.13+

* 1. 本文主要研究内容
     1. ROP攻击特征的动态提取

由于不同程序存在的漏洞类型与数量不同，攻击者攻击的手段多种多样，使用的恶意代码千变万化。众多的不测中，受攻击进程的运行时的异常，却往往具有相同或相似的基本特征。因此，ROP攻击的特征可分为两部分：其一，ROP恶意代码的特征，如：gadget的大小，gadget链的长度；其二，进程运行时的异常，如：控制流被劫持，内存被非预期修改。由于很难预测攻击者使用的恶意代码，本文着重分析众多存在漏洞的进程实例，跟踪这些进程受攻击时的运行时状态，并提取异常信息，最终得到了几类基本的异常特征（详见）。

1.4.2 ROP攻击检测系统的实现

结合ROP恶意代码的特征（详见）与进程运行时的异常特征，本文提出多种检测方案（详见），并通过PIN框架提供的各种实用API实现了对ROP攻击、JOP攻击、return-into-libc攻击的检测与识别。此外，本文实现了基于B/S模式的测试展示界面，系统将根据界面选中的检测方案，对程序进行攻击检测，并在界面中报告检测结果。

、明确判断攻击类型/\*if static else \*/if libc -> ret-to-libc else gadget(rop) if(ret) rop, if )，

* 1. 本文组织结构

第一章 绪论。介绍本文研究背景以及ROP攻击与防御的发展和现状，最后阐述了本文的研究内容。

第二章 ROP攻击与防御分析。详细介绍ROP攻击原理、攻击流程，介绍并分析现有的ROP防御机制的优势与不足。

第三章 常见ROP攻击方法。通过实例介绍常见的ROP攻击方法。

第四章 基于PIN的ROP攻击检测方法。介绍检测工具的总体框架，分析其各部分功能。利用实验验证检测方案的有效性。

第五章 总结和展望。总结本文的工作，分析其中的不足，展望基于二进制插桩检测方法值得改进的地方。

1. **ROP攻击原理与流程**

2.1 ROP攻击

2.2.1 原理

在现代操作系统中，栈被用作函数调用返回的场所。当函数被调用时，操作系统将在栈中分配一块新的内存空间，称作栈帧，栈帧中存储上一个栈帧的栈基址、函数返回地址、局部变量、函数参数等信息。当函数调用发生时，程序控制流会发生转移，即从原函数转移至被调函数。函数调用返回的流程如下：call指令执行后，操作系统将返回地址（call指令的下一条指令地址）压入栈中，然后跳转到call指令的目标地址，执行被调函数，当函数执行结束后，其末尾的ret指令，将栈中的返回地址赋值给指令寄存器ip，程序控制流于是回到原函数。由于函数调用返回的信息存储在栈中，函数调用的过程也伴随着栈帧的切换。以x86汇编语言为例，如图2-1，栈帧的切换流程如下：call指令执行后，程序控制流转移至被调函数，被调函数首先将旧的栈基址压入栈中1，然后设置新的栈基址2，并移动栈指针，开辟新的栈空间3，ret指令执行前，将栈指针指向栈基址4，并恢复保存的栈基址5。其中1-3为栈帧建立过程，4-5为栈帧的销毁过程。

① push ebp

② mov ebp, esp

③ sub esp, 0x8

...

④ mov esp, ebp

⑤ pop ebp

ret

图2-1 x86汇编语言函数栈操作

由于c语言对程序缓冲区边界不进行检测，当攻击者向缓冲区写入过多数据后，缓冲区将溢出。当缓冲区发生溢出后，栈中的返回地址被覆盖，函数返回时指令寄存器ip的值将被攻击者篡改，程序控制流由此被劫持。ROP攻击是将控制流劫持至gadget中的一种代码复用攻击。攻击者将收集到的gadget的地址以及一些必要数据，经过精心编排后写入栈中，覆盖返回地址及其后的区域。通过对栈空间的精心布局，实现一个gadget执行完毕后，跳转至下一个gadget的目的。由此gadget被依次执行，直到达到攻击者目的。

2.2.2 攻击流程

一般情况下，攻击者首先在程序或者程序所链接的共享库的代码段中搜索可用的gadget，随后利用程序存在的漏洞（如：栈溢出），将搜集的gadget地址写入内存空间，并将程序的返回地址覆盖为gadget的地址。如图2-2，攻击者将程序的原返回地址覆盖为返回地址1，并将一些数据以及返回地址2，3写入栈中，返回地址1，2，3分别指向三个不同的gadget。当程序返回时，程序控制流首先被劫持至第一个gadget中，其结尾的ret指令对应返回地址2，当第一个gadget完成一定操作后，程序控制流将转移至下一个gadget。由此，攻击者可以将搜集到的gadget链接起来，进而实现一次完整的攻击。



2.2.3 变种攻击

COP

JOP

混合式ROP

如：检测以ret指令为结尾的的连续短代码序列，jmp将破坏之，



Xor eax,eax

Pop ebx

Inc eax

Pop ecx

stc

jmp ecx

Int 0x80 (再说 expliotdb随便找一个)

2.2 常见ROP攻击方法

2.2.1 绕过随机化防护

通过printf，puts, write等具有输出功能的函数，或者代码中存在的格式化字符串漏洞，将经过随机化后libc中函数地址泄漏，从而获取经过随机化后的libc基址，由此可绕过ASLR防御机制。

...

2.2.2 组合gadget

完成寄存器布局，进行系统调用

2.2.3 调用敏感libc函数

结合ret2libc攻击，调用system，execve等libc函数，进行系统调用，执行系统命令，提升权限。

...

2.2.4 篡改虚函数表/全局偏移量表

虚函数表全局偏移量表（介绍），由于其可以被修改的特性，攻击者可以通过代码中存在的漏洞，对表中的函数指针进行修改。当被修改的函数被调用时，程序控制流将被攻击者劫持。

...

2.3 本章小结

xxx

1. **ROP攻击特征**

3.1 Gadget特征

3.2 运行时特征

3.3 本章小结

1. **ROP攻击检测方法**

4.1 指令特征检测

4.1.1 call-ret指令数检测

4.1.2 连续gadget检测

4.2 完整性检测

4.2.1 调用返回控制流完整性检测

通过调用-返回转移控制流，if-else内部多用jmp转移。

4.2.1 函数指针控制流完整性检测

存在特殊的控制流转移方式，指针，c++虚函数，c语言GOT表

4.3 本章小结

1. **ROP攻击检测实现**

5.1 假设

5.2 总体设计

5.3 系统概述(总体实现)

框架

/\*if static else \*/if libc -> ret-to-libc else gadget(rop) if(ret) rop, if )

## 5.4 实现细则

4.4.1影子栈

有局限，缓冲区溢出，只能检测出通过修改返回地址，然而劫持控制流的方式多种多样，例如uaf,修改got表等，为了弥补影子栈的不足，本文对got进行了防护。见4.4.2

4.4.2 GOT篡改检测器

4.4.3 关键指令计数器

影子栈防御了常见的控制流劫持方法，即：修改程序正常返回地址，未知的新型的控制流劫持方法，应提供另一个层次的防御方式。关键指令计数器，不检测程序返回地址是否正常，而是通过检测程序执行过程中call指令和ret指令执行的次数，判断程序是否被攻击。当rop攻击发生时，ret指令数会远多于call指令数。但是如果攻击者利用COP攻击，手动平衡call与ret的指令数，精心构造rop链，也可以绕过call-ret平衡检测。

4.4.4 阈值检测器

这种方法，通过统计众多ROP攻击中，单个gadget的大小、gadget链的长度，以这两个参数设定阈值，用于区分gadget与正常代码。存在一定机率的误报与漏报。

被攻击标记，置1 -> 检测攻击类型模块

## 5.5界面实现

B/S

5.6 实验与评估

实验环境

过程

结果（表格）

5.7 本章小结

1. **总结和展望**

6.1 总结

6.2 展望

**参考文献**

1. https://www.cvedetails.com/vulnerabilities-by-types.php
2. Data execution prevention. <http://support.microsoft.com/kb/875352/EN-US>
3. Wojtczuk, R.: The advanced return-into-lib(c) exploits: PaX case study. Phrack Mag. 0x0b(0x3a), Phile# 0x04 of 0x0e (2001)
4. Shacham, H.: The geometry of innocent flesh on the bone: return-into-libc without function calls (on the x86). In: Proceedings of the 14th ACM Conference on Computer and Communications Security, pp. 552-561. ACM (2007)
5. Kornau, T.: Return oriented programming for the ARM architecture. Ph.D. thesis, Masters thesis, Ruhr-Universität Bochum (2010)
6. Buchanan, E., Roemer, R., Shacham, H., Savage, S.: When good instructions go bad: generalizing return-oriented programming to risc. In: Proceedings of the 15th ACM Conference on Computer and Communications Security, pp. 27-38. ACM (2008)
7. Checkoway, S., Feldman, A.J., Kantor, B., Halderman, J.A., Felten, E.W., Shacham, H.: Can DREs provide long-lasting security? The case of return-oriented programming and the AVC advantage. In: EVT/WOTE 2009 (2009)
8. Francillon, A., Castelluccia, C.: Code injection attacks on Harvard-architecture devices. In: Proceedings of the 15th ACM Conference on Computer and Communications Security, pp. 15-26. ACM (2008)
9. Tran, M., Etheridge, M., Bletsch, T., Jiang, X., Freeh, V., Ning, P.: On the expressiveness of return-into-libc attacks. In: Sommer, R., Balzarotti, D., Maier, G. (eds.) RAID 2011. LNCS, vol. 6961, pp. 121-141. Springer, Heidelberg (2011). doi:10.1007/978-3-642-23644-0 7
10. Dullien, T., Kornau, T., Weinmann, R.P.: A framework for automated architecture-independent gadget search. In: WOOT (2010)
11. Hund, R., Holz, T., Freiling, F.C.: Return-oriented rootkits: bypassing kernel code integrity protection mechanisms. In: USENIX Security Symposium, pp. 383-398 (2009)
12. Roemer, R.G.: Finding the bad in good code: automated return-oriented programming exploit discovery (2009)
13. Schwartz, E.J., Avgerinos, T., Brumley, D.: Q: Exploit hardening made easy. In: USENIX Security Symposium, pp. 25-41 (2011)
14. Carlini, N., Wagner, D.: ROP is still dangerous: breaking modern defenses. In: 23rd USENIX Security Symposium (USENIX Security 2014), pp. 385-399 (2014)
15. Bletsch, T., Jiang, X., Freeh, V.W., Liang, Z.: Jump-oriented programming: a new class of code-reuse attack. In: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, pp. 30-40. ACM (2011)
16. Kevin Z. Snow, Fabian Monrose, Lucas Davi, Alexandra Dmitrienko, Christopher Liebchen, and A.R. Sadeghi, Just-In-Time Code Reuse: On the Effectiveness of Fine-Grained Address Space Layout Randomization - IEEE Symposium on Security and Privacy, 574-588 (2013)
17. A Bittau, A Belay, A Mashtizadeh, D Mazières, D Boneh - IEEE Symposium on Security and Privacy, 227-242 (2014)
18. PaX Team. <http://pax.grsecurity.net/.>
19. Pappas V , Polychronakis M , Keromytis A D . Transparent ROP exploit mitigation using indirect branch tracing, in 22nd USENIX conference on Security, pages 447-463. (2013)
20. M. Backes and S. Nurnberger. Oxymoron: Making fine-grained memory randomization practical by allowing code sharing. In Proceedings of the 23rd USENIX Security Symposium. (2014)
21. Si, Lu , et al. "ROP-Hunt: Detecting Return-Oriented Programming Attacks in Applications." International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage Springer, Cham. (2016)
22. Pappas, V., Polychronakis, M., Keromytis, A.D.: Transparent ROP exploit mitigation using indirect branch tracing. In: Presented as Part of the 22nd USENIX Security Symposium (USENIX Security 2013), pp. 447-462 (2013)
23. Davi, L., Sadeghi, A.R., Winandy, M.: Ropdefender: adetection tool to defend against return-oriented programming attacks. In: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, pp. 40-51. ACM (2011)
24. Chen, P., Xiao, H., Shen, X., Yin, X., Mao, B., Xie, L.: DROP: detecting returnoriented programming malicious code. In: Prakash, A., Sen Gupta, I. (eds.) ICISS 2009. LNCS, vol. 5905, pp. 163-177. Springer, Heidelberg (2009). doi:10.1007/978-3-642-10772-6 13
25. Bletsch, T., Jiang, X., Freeh, V.: Mitigating code-reuse attacks with control-flow locking. In: Proceedings of the 27th Annual Computer Security Applications Conference, pp. 353-362. ACM (2011)
26. Onarlioglu, K., Bilge, L., Lanzi, A., Balzarotti, D., Kirda, E.: G-free: defeating return-oriented programming through gadget-less binaries. In: Proceedings of the 26th Annual Computer Security Applications Conference, pp. 49-58. ACM (2010)
27. Aurélien Francillon, Daniele Perito, and Claude Castelluccia. Defending embedded systems against control flow attacks. In Proceedings of the 1st Workshop on Secure Execution of Untrusted Code (SecuCode’09), pages 19–26. ACM, 2009.