ISSN 1000-0054 清华大学学报（自然科学版） 2017 年 第 57 卷 第 1 期 7/20
CN 11-2223/N J Tsinghua Univ (Sci & Technol), 2017, Vol. 57, No. 1 33-38,43

PDF 文件漏洞检测

文伟平[1]， 王永剑[2]， 孟 正[1]

（1. 北京大学 软件与微电子学院，北京 102600；2. 信息网络安全公安部重点实验室，上海 201204）

摘 要：近年来，针对商业组织和政府机构的网络攻击事件层出不穷，高级持续性威胁（APT）攻击时有发生。恶意 PDF 文件是 APT 攻击的重要载体，它通过执行嵌入在文件内部的恶意代码完成攻击过程。查找 PDF 文件自身存在的安全漏洞，检测利用 PDF 漏洞的关键代码如面向返回的编程（ROP）链等，将在根源上对 PDF 恶意代码的传播路径进行阻断，从而更好地应对 PDF 恶意代码的多样性和多变性。该文首先对 PDF 文件格式漏洞的原理和分析方法进行介绍，然后结合 PDF 漏洞分析实例，对漏洞检测规则库进行构建，提出一种基于规则匹配的 PDF 已知漏洞检测方法，接下来描述 ROP 技术的原理，对 ROP 链的检测方法进行分析，最后比较所实现的漏洞检测系统与现有的安全检测工具赛门铁克和 BitDefender 的已知漏洞检测能力，由检测结果可知该系统对已知漏洞的检测能力明显高于同类产品。

关键词：PDF 文件；漏洞检测；规则匹配；面向返回的编程（ROP）链检测

中图分类号：TP309.1 **文献标志码**：A

文章编号：1000-0054(2017)01-0033-06

DOI：10.16511/j.cnki.qhdxxb.2017.21.007

PDF file vulnerability detection

WEN Weiping[1], WANG Yongjian[2], MENG Zheng[1]

(1. School of Software & Microelectronics, Peking University, Beijing 102600, China;
2. Key Laboratory of Information Network Security of Ministry of Public Security, Shanghai 201204, China)

Abstract: Recent years have seen more network attacks on business organizations and government agencies. Advanced persistent threat (APT) attacks are one key example. Malicious PDF files are an important carrier for APT attacks, which complete the attack process by executing malicious code embedded in the file. The security vulnerabilities in PDF files and the key codes in PDF vulnerabilities (such as the ROP chain) are detected to block the propagation path of the PDF malicious code at the root to better deal with the diverse malicious PDF codes. This paper introduces the principle and analysis method for identifying PDF file format vulnerabilities. The vulnerability detection rules are defined with a PDF vulnerability detection method combined with a PDF vulnerability analysis based on rule matching. Next this paper describes the principles of the ROP method and analyzes the ROP chain detection method. Finally, this paper compares this vulnerability detection system with Symantec and BitDefender. The results show that this system more effectively detects vulnerabilities than similar products.

Key words: PDF file; vulnerability detection; rule matching; return-oriented programming (ROP) chain detection

从 2009 年开始，针对商业组织和政府机构的网络攻击事件数量急剧攀升。据卡巴斯基实验室统计，2013 年约有 91%的组织机构遭受网络攻击[1]。这些攻击通常会采用窃取敏感信息、网络钓鱼、监控组织以及扰乱组织运行等方式实施破坏。电子邮件是一种在发送者和接收者之间传递数字信息的有效方法，目前已广泛地被各大组织机构所采用。因此，包含恶意代码的电子邮件附件就成为攻击者进行网络攻击的有效手段。

大多数邮件服务器可以阻止邮件附件中的可执行文件被传递。因此，在最新的网络攻击中，不可执行的文件发挥了越来越重要的作用。F-Secure 公司的报告显示：2010 年第 1 季度，与 Adobe Reader 相关的攻击占全部文档类攻击的 61%，而与 Microsoft Office 相关的攻击只占据 24%。

由于多种常见的 PDF 文件攻击是通过 Adobe Reader 的安全漏洞实施的，PDF 恶意代码也通常是通过漏洞进行传播的，因此查找 PDF 文件自身存在的安全漏洞，检测利用 PDF 漏洞的关键代码如面向返回的编程（ROP）链等，将在根源上对 PDF 恶意代码的传播路径进行阻断，从而更好地应对

收稿日期：2016-01-19
基金项目：信息网络安全公安部重点实验室项目（C14604）
作者简介：文伟平（1976—），男，副教授。
通信作者：王永剑，副研究员，E-mail：wangyongjian@stars.org.cn

PDF 恶意代码的多样性和多变性[2]。

本文提出一种基于规则匹配的针对已知漏洞的 PDF 恶意代码检测技术，用于识别、检测恶意 PDF 文件，保护用户隐私和改善网络安全现状。

1 PDF 文件格式漏洞及其利用方法

1.1 PDF 漏洞

近年来，PDF 文件以其便携性和易用性受到了人们的广泛关注，因此针对该种类型文件的安全漏洞具有较大危害性。PDF 文件格式漏洞[3]以缓冲区溢出为主。缓冲区溢出是一种常见的攻击方式，它向较小的缓冲区中写入较大数据，从而覆盖堆栈的原有信息，并对内存中数据的值进行修改。这样，之前的程序执行流程很有可能会发生改变，使得恶意代码被执行，最终完成对用户主机的控制。

PDF 缓冲区溢出漏洞发生的原因是程序员在编写代码时忽略了对缓冲区的长度检查或者预先分配的内存空间小于实际数据的长度[4]。PDF 缓冲区溢出漏洞可以分为 2 种：堆溢出和栈溢出。堆喷射技术是堆溢出漏洞的一种利用方法，它可以将程序的执行流程转移到嵌入的恶意 Javascript 代码上。堆喷射技术需要使用大量填充有 shellcode 的堆，通过特意构造，可使虚函数表的函数指针跳转入指定的地址空间。攻击者在 shellcode 之前会增加大量的 NOP 指令，从而提高 shellcode 执行的可能性。当函数指针跳转到 NOP 指令时，shellcode 会随后被执行。堆喷射攻击[5]的执行流程如图 1 所示。

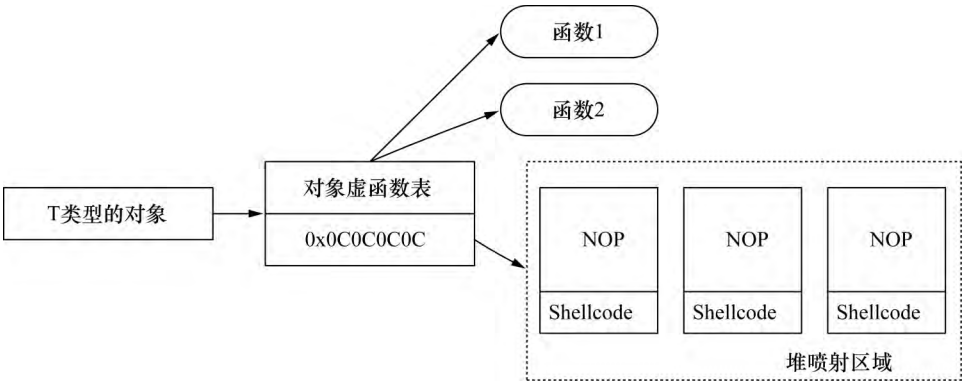

图 1 堆喷射攻击执行流程

1.2 PDF 漏洞利用方法

数据执行保护(DEP)防护机制[4]通过阻止指令在数据区(包括堆、栈、内存池等)上执行，提升了 PDF 漏洞利用的难度。当前，ROP 技术已成为突破 DEP 的最有效方法。ROP 的基本原理是：在栈上对一些指令组合的返回地址进行布置，从而达到执行代码的目的，这些指令组合通常以 ret 指令结尾，这样才能将它们依次执行。尽管指令无法在栈上执行，但可以利用可执行数据区的指令组合完成特定功能。

图 2 描述了由 ROP 链构成的 Shellcode。左半部分表示堆、栈等数据区，右半部分表示可执行代码区。指向可执行代码区的地址构成了数据区中的 Shellcode。这些地址指向的代码片段有一个共同的特点，即都以 ret 指令结尾。这样能够使程序沿着数据区的地址程序，可以有效收回控制权。

典型 ROP 链的特征是：

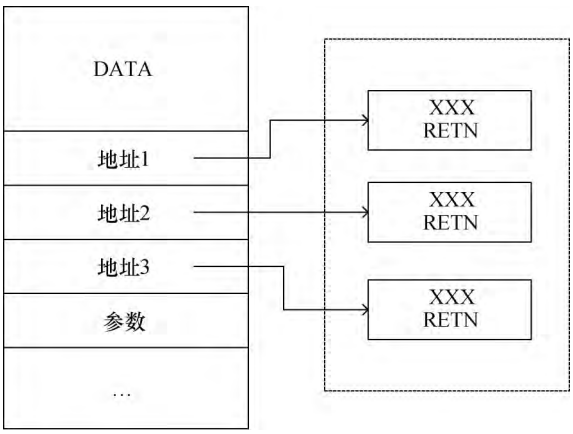

图 2 ROP 链构成的 Shellcode

1)当敏感 API 函数返回后，下一个代码片段会执行，这个代码片段一般不是由 call 指令调用的；

2)每个代码片段包含的指令数量很少，当代码片段执行完毕后，会返回到下一个敏感 API 函数或下一个代码片段。

通常，单纯通过ROP链来实现一个正常Shellcode的全部功能是很困难的。因此，在执行ROP链之前应先调用系统API函数来对内存属性进行修改或分配一段可执行内存，常见的敏感API函数[6]有：

1）VirtualProtect/VirtualProtectEx：使Shellcode所在的堆、栈等区域可执行；

2）VirtualAlloc/VirtualAllocEx：对具有可执行权限的内存进行分配，然后复制Shellcode到这段内存中执行；

3）zwSetInformationProcess：修改KPROCESS结构的_KEXECUTE_OPTIONS中的DEP设置，将DEP关闭；

4）SetProcessDEPPolicy：为DEP设置不同的模式；

5）LoadLibraryA/LoadLibraryW/LoadLibraryEx/LoadLibraryExW：加载动态链接库；

6）HeapAlloc：在指定的堆上分配内存。

2 PDF漏洞检测总体架构

PDF漏洞检测子系统主要包括PDF已知漏洞检测和漏洞利用关键代码检测2个核心模块，其总体架构如图3所示。PDF已知漏洞检测模块涉及漏洞原理分析、漏洞检测规则库构建和基于特征匹配的静态检测等3个流程，漏洞利用关键代码检测模块则主要针对ROP链。ROP链本身是一些指令片段(gadget)，用于突破Windows的内存防护机制DEP，这些片段通常是以ret指令结尾的[7]。对ROP链的检测主要采用堆栈检测、函数调用检测、函数参数检测和动态链接库检测等4种方法。

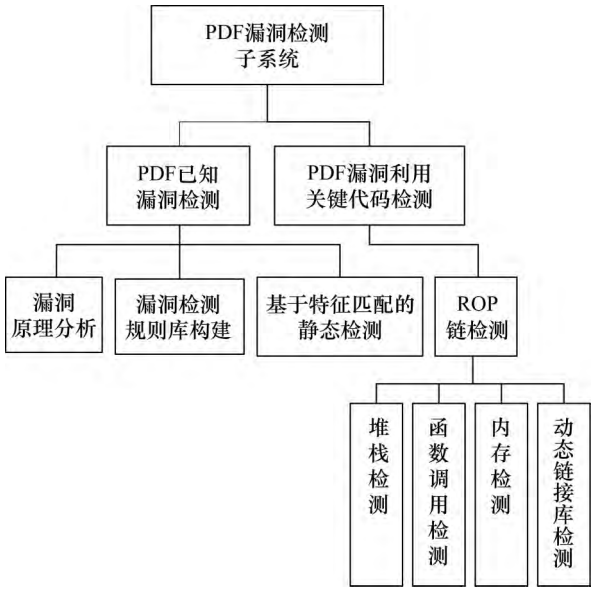

图3 PDF漏洞检测子系统总体架构

3 PDF已知漏洞检测

3.1 PDF漏洞分析

漏洞分析技术指的是对已公开的安全漏洞进行原理分析，通过攻击概念证明(POC)代码触发漏洞，对漏洞场景予以重现并编写漏洞检测规则等。为完成漏洞分析过程，需要在代码中定位漏洞，理清攻击的基本原理，并对漏洞的潜在利用方法进行估计，因此漏洞分析是一项具有较高挑战性的工作。

漏洞分析技术通常包含信息采集、分析调试以及漏洞利用分析等3个阶段，其流程如图4所示。漏洞分析技术为修复漏洞和构建漏洞检测规则库提供了支持。重现漏洞是漏洞分析的重要步骤，只有找到合适的触发条件、触发步骤及受影响软件的版本后，才能稳定地重现漏洞，然后采用调试和跟踪的方法对漏洞进行分析。为重现漏洞，通常需要编写POC代码。

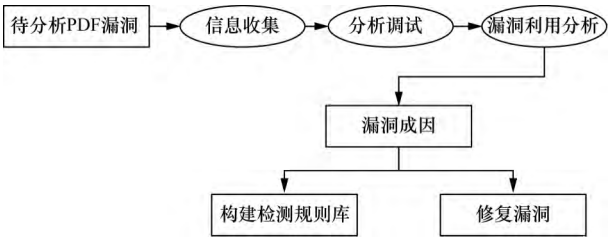

图4 漏洞分析流程

1）信息收集。

对信息的收集是漏洞分析过程的第一个阶段，它主要是在分析调试之前，收集漏洞的相关信息包括漏洞基本信息、文件格式信息和系统状态信息等。

a）收集漏洞基本信息。

对国内外著名的软件厂商网站和漏洞库进行检索，分析由它们发布的漏洞公告，获得漏洞名称、CVE编号、漏洞类型、受影响的产品、漏洞公布时间和漏洞严重等级等信息。

b）解析文件格式信息。

对存在漏洞的应用程序的文件格式进行解析，从而在漏洞分析过程中能够更快地对诱发漏洞的函数、参数和数据对象等进行定位。

c）监测系统状态信息。

观察漏洞触发时的系统状态，对寄存器数据、

堆栈数据以及进程、线程的上下文状态进行监测。

2) 分析调试。

漏洞分析的核心步骤是分析调试，通过信息收集，对触发漏洞的特定数据或字段进行记录，找到它们与漏洞点之间的对应关系。另外，需要采用调试工具对异常信息进行监控，动态跟踪程序在解析特定文件格式时的系统状态，通过回溯法对漏洞的成因和机理进行分析。

a) 使用调试工具。

常见的漏洞分析工具有：虚拟机软件 VMware，文本编辑工具 UltraEdit，静态分析工具 IDA 和动态调试工具 OllyDbg、WinDbg、Immunity Debugger 等。OllyDbg 仅可以调试 Ring3 级的应用程序，它具有丰富的插件和很强的可扩展性，提高了工具的灵活性；而 WinDbg 对 Ring0 级的内核程序和 Ring3 级的应用程序都提供了支持。

b) 跟踪和监测数据流。

数据流指的是程序在运行过程中从输入到输出的一条执行路径，这个路径上的节点覆盖和修改寄存器、内存的方式是应该被关注的，对寄存器和内存的不当处理和非法操作往往是安全漏洞产生的直接原因。对数据流的跟踪和监测可以采用捕获异常和设置断点 2 种方法。

c) 漏洞原理分析。

当漏洞稳定触发后，通过跟踪和监控异常信息，可以得到漏洞点代码(即程序中触发漏洞的代码段)，漏洞点代码通常位于一个函数或方法中，此时可以结合调用栈信息，采用回溯分析的方法对漏洞原理进行分析，最终在样本的文件格式中找到诱发漏洞的数据对象。

在对漏洞原理进行分析的过程中，可以将动态和静态分析工具结合起来，从而提高分析效率。通过动态调试工具对存在漏洞的程序进行加载，然后跟踪程序的执行过程，可以采用单步执行的方式依次执行每一条汇编语句，观察堆栈、寄存器和内存中数据的变化，也可以通过回溯法定位产生溢出的漏洞函数，从而快速剖析漏洞原理。IDA 等静态分析工具能够反汇编存在漏洞的程序，并获得程序的总体结构和完整的反汇编代码，通过对反汇编代码进行阅读和分析，可以进一步理清代码功能，找到代码中的缺陷。静态分析工具主要是用于辅助动态调试工具的[8]。

3) 漏洞利用分析。

漏洞利用分析是在漏洞原理分析的基础上，结合漏洞触发条件，对漏洞的危害程度和可利用程度进行分析，并建立漏洞检测规则的过程。

漏洞利用分析首先需要对漏洞的类型(包括本地权限提升、缓冲区溢出或任意代码执行等)进行确定，然后结合触发漏洞的条件分析漏洞的利用条件，确定是否是特定地址读写或任意地址读写等，最后对漏洞可能造成的危害进行预测[9]。

3.2 PDF 漏洞检测规则库构建

通过对 PDF 漏洞的触发条件和原理进行分析，可以抽取到漏洞特征，进而形成针对单个 PDF 漏洞的检测规则。3 个典型 PDF 文件漏洞的检测规则如表 1 所示。PDF 漏洞检测规则库包含 CVE 编号、受影响的软件和版本以及漏洞检测规则等信息。

表 1 漏洞检测规则库

CVE 编号	受影响的软件和版本	漏洞检测规则
CVE-2011-2096	Adobe Reader 及 Acrobat：8.38.x 9.x(9.4.5 之前)	检测 Universal 3D 字段，如果文件头中定义的数据长度小于 TextureName 的长度加 4，将会触发漏洞
CVE-2011-2097	Adobe Reader 及 Acrobat：8.x(8.3 之前) 9.x(9.4.5 之前) 10.x(10.1 之前)	检测网络数据流，当发现 PDF 文件中存在“/ICCBased”字段时，对 ProfileDescriptionTag 字段(‘desc’)进行查找。若该字段存在，则判断其后偏移 22 字节处的值是否大于 0x7FFFFFFF，若是则触发漏洞
CVE-2011-2098	Adobe Reader 及 Acrobat：8.x(8.3 之前) 9.x(9.4.5 之前) 10.x(10.1 之前)	检测网络数据流，当发现 PDF 文件中存在“/JPXDecode”字段时，对 JP2C box 字段(‘jp2c’)进行查找。若该字段存在，则判断其后偏移 11 字节处的值是否大于 0x3f，若是则触发漏洞

3.3 基于规则匹配的静态检测

基于规则匹配的静态检测方法是将表 2 中描述的检测规则与待查 PDF 样本进行匹配，如果 PDF 样本中有一个或多个数据结构的值命中了规则库中的一条或多条检测规则，那么就判定该样本文件存

在PDF已知漏洞。

基于规则匹配的静态检测方法是以PDF文件解析为前提的，只有将PDF文件中数据结构的类型、名称、偏移量、值和长度等属性准确提取出来，才可以进行下一步的逻辑判断。与PDF漏洞相关的数据结构主要有BMP、IFF、TIFF、PCX、PICT、Universal3D、JPEG和TrueTypeFont等，因此在解析PDF文件本身时，也需要对这些数据结构进行格式解析。

基于规则匹配的静态检测方法流程如图5所示。

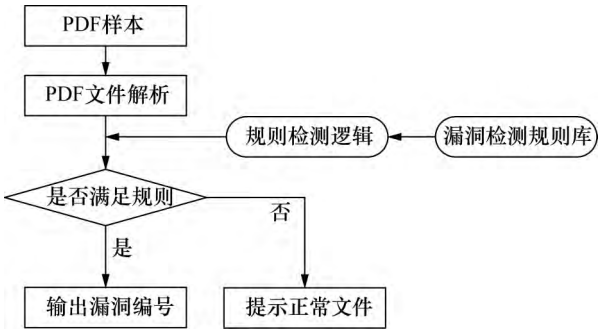

图5 基于规则匹配的静态检测方法流程

对PDF已知漏洞CVE-2011-2437的调试过程、原理和检测规则等进行分析，当(YMax－Ymin＋1)的值大于0xFFFF时，就会触发漏洞。

PDF已知漏洞检测模块可以对19种PDF已知漏洞进行检测，每一种漏洞分别对应一段规则检测代码。

4 PDF漏洞利用关键代码检测

4.1 ROP链检测方法

ROP链检测模块会对节1.2描述的敏感API函数进行inline-hook，它能够直接修改敏感API函数当中的指令，以一个跳转或其他指令来完成挂钩，使敏感API函数在执行之前进行额外的验证。当敏感API函数被调用后，会先跳转至ROP链检测模块的钩子函数上进行检测，之后再恢复程序的正常执行流程。

对敏感API函数挂钩的操作是通过Detours[10]实现的，Detours是Microsoft研发的一个函数库，它可以将任意数据段插入到PE文件中，对dll文件的导入表进行修改，也可以拦截X86主机上的任意Win32 API函数。Detours是在汇编层进行处理的，它能够对目标API函数出口和入口处的汇编指令进行修改。ROP链检测模块流程如图6所示。

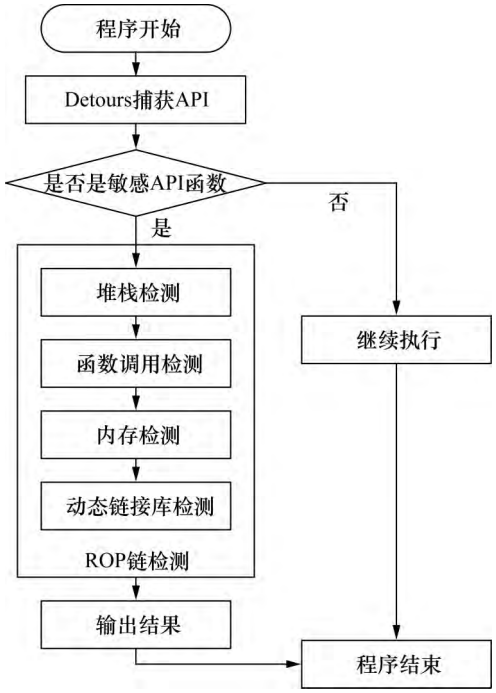

图6 ROP链检测模块流程

ROP链检测有以下4种方法：

1）堆栈检测。

当前一种常见的实现ROP技术的方法是将用户控制的寄存器(该寄存器可能指向用户控制的地址)和栈指针互换，实现该过程的代码片段如下所示：

```
XCHG EAX, ESP
RET
```

对这类攻击的检测方法是当调用VirtualProtect、VirtualAlloc等敏感API函数时，检测栈指针ESP是否位于当前线程栈空间范围，如果不位于该范围，则抛出异常。

堆栈检测方法只是检测当敏感API函数被调用时，ESP指针是否位于栈区域当中，并没有充分考虑ROP链的根本特征，因此ROP的简单变形就可以绕过该检测。为绕过堆栈检测方法，只需通过ROP链在栈区布置API参数，并将ESP重新指向栈区。

2）函数调用检测。

函数调用检测方法对敏感API函数的返回地址进行验证，如果返回地址的上一条指令是call，且call指令的跳转目标是敏感API函数的地址时，那么通过验证。如果返回地址的上一条指令不是call，或call指令的目标跳转地址不是敏感API函数的地址，则认为检测到ROP链。

函数调用检测方法用于过滤敏感API函数的

调用来源，确保目标地址是通过 call 指令进入的，而不是通过 jmp 或 return 指令进入的。call 指令的跳转方式主要有以下 5 种：① call [reg+disp32]，call [loc32]；② call rel；③ call reg，call [reg]；④ call [reg + disp8]；⑤ call [reg1 + reg2 + disp32]。

3）内存检测。

内存检测方法主要针对栈溢出漏洞利用的 ROP 链进行检测。它通过验证传入到敏感 API 函数 VirtualProtect/VirtualProtectEx 中的参数，对 ROP 链进行判断。VirtualProtect/VirtualProtectEx 函数用于对内存页的访问属性进行修改，它的参数有 lpAddress、dwSize 和 flwNewProtect。

内存检测方法首先对第 3 个参数 flwNewProtect 进行检查，如果发现参数 flwNewProtect 中设置了可执行标记位，那么就对参数 lpAddress 进行检查。如果内存[lpAddress，lpaddress + dwSize]位于当前线程的栈空间范围内即 TEB. StackTop < lpAddress && (lpAddress + dwSize) < TEB. StackBottom，那么就认为检测到了 ROP 链。

4）动态链接库检测。

动态链接库检测方法主要为了防止黑客通过执行 ROP 链从远端服务器加载恶意的 dll 文件。该种检测方法对 LoadLibraryW/LoadLibraryA/LoadLibraryEx/LoadLibraryExW 的参数进行检验。

5 PDF 漏洞检测系统测试

PDF 已知漏洞检测模块采用了基于特征匹配的静态检测方法，首先将 PDF 漏洞检测规则库中的检测规则信息采用 C# 语言实现，然后对样本进行检测。如果 PDF 样本中有一个或多个数据结构的值命中了规则库中的一条或多条检测规则，那么就判定该样本文件存在 PDF 已知漏洞。

为实现 PDF 已知漏洞检测功能，需要将与 PDF 漏洞相关的数据结构(包括 BMP、IFF、TIFF、PCX、PICT、Universal3D、JPEG 和 TrueTypeFont 等)的类型、名称、偏移量、值和长度等属性准确提取出来，这主要是由 PDF 文件解析模块完成的。PDF 文件解析的运行结果如图 7 所示。

使用 PDFCheck 对存在漏洞的样本文件“repro. pdf”进行测试，测试结果见图 8，其中显示了漏洞编号和漏洞说明等信息。

对包含 ROP 链的 PDF 样本文件“roptest. pdf”进行测试，测试结果如图 9 所示。

321	Dictionary	/Resour...					249.894 (0x3D026)		
322	Dictionary	/Page				PageObj_322...	224.892 (0x36E7C)		
323	Stream	/Contents				StreamObj_32...	221,378 (0x360C2)	221.441 (0x36101)	3,433 (0xD69)
324	Dictionary	/Names					249.526 (0x3CEB6)		
325	Dictionary	/Names					249.587 (0x3CEF3)		
326	Dictionary	/Names					249.648 (0x3CF30)		
327	Dictionary	/Names					249.708 (0x3CF6C)		
328	Dictionary	/Names					249.770 (0x3CFAA)		
329	Dictionary	/Names					249.832 (0x3CFE8)		
330	Dictionary	/PTEX.I...					228.803 (0x37DC3)		
331	Dictionary	/ExtGSt...					229,068 (0x37ECC)		
332	Dictionary	/Font	/Type1				229,115 (0x37EFB)		
333	Dictionary	/FontDe...					229.544 (0x380A8)		
334	Stream	/FontFile3	/Type1C			StreamObj_33...	229.934 (0x3822E)	230.008 (0x38278)	2.995 (0xBB3)
335	Dictionary	/PTEX.I...					236,474 (0x39BBA)		
336	Dictionary	/ExtGSt...					236,739 (0x39CC3)		
337	Dictionary	/Font	/Type1				236,786 (0x39CF2)		
338	Dictionary	/FontDe...					237,215 (0x39E9F)		

图 7 PDF 文件解析运行结果

解析类型	偏移位置	长度	漏洞类型	说明
Comment	0			Found unknown type -1.7
Error	0	7860		An exception was thrown ...
DefinitelyMalicious	730	6918	CVE_2011_2105	Found CID font with invalid...
Error	0	0		ParsingIncomplete: Trying ...
Error	7862			The prefix of a DataItem w...

图 8 PDF 已知漏洞检测运行结果

图 9 PDF 漏洞利用关键代码检测结果

从可信数据源 VirusTotal repository、Contagio Project 和 Internet and Ben-Gurion University 中选择 200 个存在安全漏洞的 PDF 样本，将本文提出的 PDF 漏洞检测系统 PDFCheck 与安全检测工具赛门铁克、BitDefender 进行比较，结果如表 2 所示。

表 2 PDF 漏洞检测结果比较

工具或模型名称	检出个数	检出率%
PDFCheck	174	87
BitDefender	156	78
赛门铁克	139	69.5

由检测结果可知，PDFCheck 对已知漏洞的检测能力明显高于 BitDefender 和赛门铁克的。

6 结 论

本文提出一种基于规则匹配的 PDF 已知漏洞检测方法，首先对 PDF 文件格式漏洞的原理和分析方法进行介绍，然后结合 PDF 漏洞分析实例，对漏洞检测规则库进行构建，通过规则匹配检测漏洞，接下来描述 ROP 技术的原理，对 ROP 链的检测方法进行分析，最后比较本文实现的漏洞检测系统与现有的安全检测工具赛门铁克、BitDefender 的已知漏洞检测能力，结果表明本文系统对已知漏洞的检测能力明显高于同类产品的。

(下转第 43 页)

WANG Qing. Research on the Routing Technology of Wireless Sensor Networks [D]. Xi'an: Xi Dian University, 2009. (in Chinese)

[5] **崔莉，鞠海玲，苗勇，等。无线传感器网络研究进展** [J]. **计算机研究与发展**, 2005, **42**(1): 163-174.
CUI Li, JU Hailing, MIAO Yong, et al. Research on progress in wireless sensor network [J]. *Computer Research and Development*, 2005, **42**(1): 163-174. (in Chinese)

[6] Pandey A, Tripathi R C. A survey on wireless sensor networks security [J]. *International Journal of Computer Applications*, 2010, **3**(2): 43-49.

[7] Prasad D, Gupta M, Patel R B. A reliable security model irrespective of energy constraints in wireless sensor networks [J]. *International Journal of Advanced Computer Sciences and Applications*, 2011, **2**(4): 2156-5570.

[8] Boujelben M, Youssef H, Mzid R, et al. Self-healing key, distribution schemes for wireless networks: A survey [J]. *The Computer Journal*, 2011, **54**(4): 449-569.

[9] LUO Hanjiang, WU Kaishun, GUO Zhongwen, et al. Ship detection with wireless sensor networks [J]. *IEEE Transactions on Parallel and Distributed Systems*, 2012, **23**(7): 1336-1343.

[10] ZHANG Ting, HE Jingsha, LI Xiaohui, et al. A signcryption-based secure localization scheme in wireless sensor networks [J]. *Physics Procedia*, 2012, **33**: 58-264.

[11] Zhang G H, Poon C C, Zhang Y T. Analysis of using interpulse intervals to generate 128-Bit biometric random binary sequences for securing wireless body sensor networks [J], *IEEE Transactions on Information Technology in Biomedicine*, 2012, **16**(1): 176-182.

[12] **杨峰. 无线传感器网络恶意节点防范技术研究** [D]. **合肥：中国科学技术大学**, 2009.
YANG Feng, Research on Malicious Node Protection Technology in Wireless Sensor Networks [D]. Hefei: University of Science and Technology of China, 2009. (in Chinese)

[13] **欧阳熹. 基于节点信誉的无线传感器网络安全关键技术研究** [D]. **北京：北京邮电大学**, 2013. (in Chinese)
OUYANG Xi. Research on Reputation-based Security Technologies of Wireless Sensor Networks [D]. Beijing: Beijing University of Posts and Telecommunications, 2013. (in Chinese)

[14] **张芹. 无线传感器网络环境下的节点可信技术研究** [D]. **南京：南京邮电大学**, 2011.
ZHANG Qin. Research of Trust Node Technology in Wireless Sensor Network [D]. Nanjing: Nanjing University of Posts and Telecommunications, 2011. (in Chinese)

[15] Wang J, Liu Y, Jiao Y. Building a trusted route in a mobile ad hoc network considering communication reliability and path length [J]. *Journal of Network and Computer Applications*, 2011, **34**(4): 1138-1149.

[16] Conti M, Pietro R D, Mancini L V, et al. Distributed detection of clone attacks in wireless sensor networks [J]. *IEEE Transactions on Dependable and Secure Computing*, 2011, **8**(5): 685-698.

(**上接第** 38 **页**)

参考文献 (References)

[1] Nick Sato. 91% of organisations hit by cyberattacks in 2013 [Z/OL]. [2013-12-10]. http://www.humanipo.com/news/37983/91-of-organisations-hit-by-cyberattacks-in-2013/.

[2] Andy O'Donnell. Tools and Utilities Commonly Used to Hack Computer Systems [Z/OL]. [2013-12-11]. http://netsecurity.about.com/ cs/hackertools/a/aa030504.htm.

[3] **周培和**. PDF **文件格式漏洞挖掘系统的研究及实现** [D]. **成都：电子科技大学**, 2012.
ZHOU Peihe. Research and Implementation of PDF File Format Vulnerability Mining System [D]. Chengdu: University of Electronic Science and Technology of China, 2012. (in Chinese)

[4] Palo Alto Networks. What is an intrusion detection system ids [Z/OL]. [2013-12-11]. https://www.paloaltonetworks.com/resources/learning-center/what-is-an-intrusion-detection-system-ids.html.

[5] **刘磊，王轶骏，薛质. 漏洞利用技术** Heap Spray **检测方法研究** [J]. **信息安全与通信保密**, 2012 (6): 70-72.
LIU Lei, WANG Yijun, XUE Zhi. Research on the detection method of Spray Heap based on vulnerability [J]. *Information Security and Communications Privacy*, 2012 (6): 70-72. (in Chinese)

[6] **王清**. 0day: **软件漏洞分析技术** [M]. **北京：电子工业出版社**, 2008.
WANG Qing. 0day: Software Vulnerability Analysis Technology [M]. Beijing: Publishing House of Electronics Industry, 2008. (in Chinese)

[7] Infosecurity. 91% of APT attacks start with a spear-phishing email [Z/OL]. [2013-12-11]. http://www.Infosecurity-magazine.com/view/29562/91-ofapt-attacks-start-with-a-spearphishing-email/, 2012-11-28.

[8] Vatamanu C, Gavrilut, D, Benchea R. A practical approach on clustering malicious PDF documents [J]. *Journal in Computer Virology*, 2012, **8**(4): 151-163.

[9] Nissima N, Cohena A, Glezerb C, et al. Detection of malicious PDF files and directions for enhancements: A state-of-the art survey [J]. *Computers & Security*, 2015(48): 246-266.

[10] Galen Hunt. Detours [Z/OL]. [2002-01-16]. http://research.microsoft.com/en-us/projects/detours/.