基于虚拟机的启发式扫描反病毒技术

曾宪伟 张智军 张 志
(空军工程大学工程学院 陕西 西安 710038)

摘 要 在进行深入分析病毒和正常程序的区别基础上,提出对病毒进行启发扫描分析的观点,并基于虚拟机技术进行了实现。改进手动病毒分析的传统方式,深层理解病毒运行机制,方便了防毒软件的编写,同时对未知病毒的防治也具有深远的意义。

关键词 虚拟机 病毒 启发扫描 指令模拟

HEURISTIC SKILL OF COMPUTER VIRUS ANALYSIS BASED ON VIRTUAL MACHINE

Zeng Xianwei Zhang Zhijun Zhang Zhi
(*Engineering College, Airforce Engineering University, Xi'an Shaanxi 710038, China*)

Abstract A new antivirus theory is presented in this paper. Based on distinguishing between virus and normal programs, the system puts forward a heuristic skill of computer virus analysis and realizes based on virtual machine. It improves the conventional manual methods. Through this way we learn deeply how virus working, it is helpful for designing of antivirus Software, also do well in detecting unknown viruses.

Keywords Virtual machine Virus Heuristic search Instruction simulation

0 引 言

随着个人计算机的日益普及和因特网快速发展,个人计算机系统安全和数据安全受到人们的普遍关注。其中破坏性比较大的就是这里将要讨论到的借助网络传播的计算机病毒,本文将在传统的对已知病毒的分析和研究的手法基础上,使用基于虚拟机的启发扫描手段分析病毒。

1 计算机病毒的传统分析方法

传统分析方法是当拿到一个病毒样本时,不直接运行它,因为它可能是带毒的,而且极可能是未知的,谁也无法查杀的新病毒。程序员会使用 DOS 的 DEBUG 程序分析病毒,现在更多的人选择 SOFT - ICE 一类功能更强大的软件。它们的原理都是单步跟踪执行被调程序的每一个语句,从而获得病毒的特征码。目前的防毒软件主要是通过特征搜索,在收集到的特征库中进行对比查杀病毒,但对于有强大变种加密引擎的病毒就有些力不从心,而且对于特征库中没有的病毒也无能为力。

2 虚拟机分析技术及其实现

虚拟机(VM),在反病毒界也被称为通用解密器。具体的做法是:用程序代码虚拟一个 CPU 来,同样也虚拟 CPU 的各个寄存器,甚至将硬件端口也虚拟出来,用调试程序调人被调的“样本”,将每一个语句放到虚拟环境中执行,这样就可以通过内存和寄存器以及端口的变化来了解程序的执行。这样的一个虚拟环境就是一个虚拟机。

既然虚拟中可以反映程序的任何动态,那么,将病毒放到虚拟机中执行,则病毒的传染动作一定会被反映出来。

虚拟机(例如在 WINNT/2000 环境下运行如 Linux 等其它操作系统),它作为原操作系统下的一个应用程序可以为运行于其上的目标操作系统创建出一部虚拟的机器,目标操作系统就象运行在单独一台真正机器上,丝毫察觉不到自己处于 VM 的控制之下。在 VM 上运行的应用程序认为自己独占整个机器,它们相信自己是从真正的键盘和鼠标获得输入,并从真正的屏幕上输出。稍被加一点限制,它们甚至可以认为自己完全拥有 CPU 和全部内存。图 1 为具体实现框图。

图 1 系统框架图

由此可见,实现虚拟技术关键在于软件虚拟化和硬件虚拟化。通常,虚拟机的设计方案可以采取以下三种之一:自含代码虚拟机(SCCE),缓冲代码虚拟机(BCE),有限代码虚拟机(LCE)。

自含代码虚拟机工作起来像一个真正的 CPU。一条指令取自内存,由 SCCE 解码,并被传送到相应的模拟这条指令的例程,下一条指令则继续这个循环。虚拟机会包含一个例程来对内存/寄存器寻址操作数进行解码,然后还会包括一个用于模拟每个可能在 CPU 上执行的指令的例程集。正如你所想到的,SCCE 的代码会变得无比的巨大而且速度也会很慢。

缓冲代码虚拟机是 SCCE 的一个缩略版,因为相对于 SCCE 它具有较小的尺寸和更快的执行速度。在 BCE 中,一条指令是从内存中取得的,并和一个特殊指令表相比较。如果不是特殊指令,则它被进行简单的解码以求得指令的长度,随后所有这样的指令会被导入到一个可以通用地模拟所有非特殊指令的小过程中。而特殊指令,只占整个指令集的一小部分,则在特定的小处理程序中进行模拟。

LCE 实际上并非一个虚拟机,因为它只简单地跟踪一段代

收稿日期:2004 - 05 - 31。曾宪伟,硕士生,主研领域:电子场与电子波。

码的寄存器内容,也许会提供一个小的被改动的内存地址表,或是调用过的中断之类的东西。选择使用 LCE 而非更大更复杂的系统的原因,在于即使只对极少数指令的支持便可以在解密原始加密病毒的路上走很远,因为病毒仅仅使用了 INTEL 指令集的一小部分来加密其主体。

3 启发式代码扫描技术

传统的反病毒扫描技术是在文件中查找已知病毒的特征码来鉴别是否染毒,是一种静态的过程,仅能查出已知的病毒。为了克服这个缺点,反病毒软件引入了人工智能中的“启发式”(heuristic)搜索技术。启发式指的“自我发现的能力”或“运用某种方式或方法去判定事物的知识和技能,扫描时能够根据某些规则智能地分析程序的代码,从而有可能找到未知的病毒。在具体实现上,启发式扫描技术是相当复杂的,它要能够识别并探测许多可疑的程序代码指令序列,如格式化磁盘类操作,搜索和定位各种可执行程序的操作,实现驻留内存的操作,发现非常的或未公开的系统功能调用的操作。一个运用启发式扫描技术的病毒检测软件,实际上就是以特定方式实现的动态高度器或反编译器,通过对有关指令序列的反编译逐步理解和确定其蕴藏的真正动机。

4 基于虚拟机的反病毒技术的实现

根据上面虚拟机的分析技术,在上面运用启发式代码扫描技术。具体实现原理如下:查毒的虚拟机是一个软件模拟的 CPU,它可以像真正 CPU 一样取指,译码,执行,它可以模拟一段代码在真正 CPU 上运行得到的结果。给定一组机器码序列,虚拟机会自动从中取出第一条指令操作码部分,判断操作码类型和寻址方式以确定该指令长度,然后在相应的函数中执行该指令,并根据执行后的结果确定下条指令的位置。当执行过程中发现可疑的程序代码指令序列时,根据一定的智能规则判断它是否为病毒代码。如果判断为病毒,在执行完的结果中查找并记录病毒的特征码。

具体实现如下:

指令模拟函数:cmp 指令模拟

```
void cmp(int c1,int c2)
 {
char FlgReg;
__asm  {
mov eax,c1//取得第一个操作数
mov ecx,c2//取得第二个操作数
cmp eax,ecx//比较
lahf//将比较后的标志结果装入 ah
mov FlgReg,ah//保存结果在局部变量 FlgReg 中
}
FlagReg = FlgReg;//保存结果在全局变量 FlagReg 中
} //其他指令模拟类似
```

总体流程控制代码:

```
for(i=0;i<256;i++)//首先虚拟执行 256 条指令试图发现病毒循环解密子
 {
  if(FindVirusDecrypt == TRUE)
  break;
}
if( i ==256)
  return(0);//没发现病毒解密子
if(!EncodeVirus())
  return(0);//调用解密函数重复执行循环解密过程
  switch(ExeEncode())//模拟执行解密后代码,并进行智能判断
  {
    case 1;
      break;
    ..........
  } //判断存在病毒后,捕捉特征码;
```

5 结 论

启发式代码分析技术代表着未来反病毒技术发展的必然趋势,即具备某种人工智能特点的反病毒技术,展示了一种通用的病毒检测技术和产品应用的可能性。虚拟机为启发式扫描的实现提供了一个基础,而启发式扫描是在虚拟机上进行病毒分析判定的具体手段。与在模式识别中的过程类似,虚拟机解码病毒并提供特征素材,而启发式扫描方法则进行特征的分类。对于新的病毒码具有智能学习并且记忆的功能,为未来的一般性防毒杀毒技术奠定基础。

参 考 文 献

[1] 陆麟,WINDOWS9X 文件读写 Internal,2001.

[2] David A. Solomon,Inside Windows NT,1998,5.

[3] Matt Pietrek,Windows 95 System Programming Secrets,1996,3.

[4] Prasad Dabak,Sandeep Phadke,Milind Borate,Undocumented Windows NT,1999,10.

[5] Vavid A. Solomon,Mark Russinovich,Inside Microsoft Windows 2000,2000,10.

[6] Walter Oney,System Programming for Windows 95,1996,3.

[7] Walter Oney,Programming the Windows Driver Model,1999.

(上接第 60 页)

(6) 抽取记录模块逐行读取源表记录,再通过数据装配模块,把装配好的 SQL 插入命令提交相应的 DBMS 执行,完成记录到目标表的数据转换。

4 结束语

通用数据转换工具从应用系统角度实现多平台数据环境和异构数据库环境管理信息系统的集成,从数据库角度则实现本地数据库、远程数据库乃至数据库仓库的全面集成。本文就有关数据转换和异构数据集成进行了初步的探讨,尤其是开发的通用数据转换工具,具有一定的使用性和通用性。今后需对系统的功能进行扩展,实现更加复杂的转换功能。

参 考 文 献

[1] 柯建勋、张涛,PowerBuilder8.0 进阶篇[M],北京:清华大学出版社,2002.

[2] 梁鹰、罗伟其,“异构数据库的数据转换在大型信息系统中的实现[J]”,《计算机工程与应用》,2000,(9):103~105.

[3] 陈继东,“异构数据源数据转换工具的设计与实现[J]”,《计算机科学》,2002,29(8):206~208.

[4] 王胜德、杨学强,“利用 DTS 实现异构数据库的数据交换[J]”,《计算机应用》,2003,23(7):132~134.

基于虚拟机的启发式扫描反病毒技术

作者： 曾宪伟， 张智军， 张志， Zeng Xianwei， Zhang Zhijun， Zhang Zhi
作者单位： 空军工程大学工程学院,陕西,西安,710038
刊名： 计算机应用与软件 ISTIC
英文刊名： COMPUTER APPLICATIONS AND SOFTWARE
年，卷(期)： 2005,22(9)
被引用次数： 10次

参考文献(7条)

1. 陆麟 WINDOWS9X文件读写Internal 2001
2. David A Solomon 1998
3. Matt Pietrek Windows 95 System Programming Secrets 1996
4. Prasad Dabak Sandeep Phadke,Milind Borate 1999
5. Vavid A Solomon Mark Russinovich 2000
6. Walter Oney System Programming for Windows 95 1996
7. Walter Oney Programming the Windows Driver Model 1999

本文读者也读过(10条)

1. 王振海.王海峰.WANG Zhen-hai.WANG Hai-feng 基于多态病毒行为的启发式扫描检测引擎的研究[期刊论文]-实验室研究与探索2006,25(9)
2. 刘勇.邱玲 虚拟机查毒技术的实现[期刊论文]-科技创新导报2008(18)
3. 彭安杰.Peng Anjie 虚拟机在反病毒实验中的应用[期刊论文]-计算机光盘软件与应用2010(7)
4. 谭云松.Tan Yunsong 一种启发式反病毒技术的研究[期刊论文]-网络安全技术与应用2006(11)
5. 王振海.王海峰.Wang,Zhenhai.Wang,Haifeng 针对多态病毒的反病毒检测引擎的研究[期刊论文]-微计算机信息2006,22(27)
6. 孙伟.冯萍.SUN Wei.FENG Ping 一种启发式宏病毒扫描技术[期刊论文]-长春大学学报（自然科学版）2007,17(1)
7. 张青霞.杨吉峰 二进制病毒的启发式扫描技术[期刊论文]-农业网络信息2006(8)
8. 崔鹏.CUI Peng 基于语义的启发式病毒检测引擎研究[期刊论文]-常熟理工学院学报2008,22(10)
9. 崔鹏.CUI Peng 基于形式化语义的启发式病毒检测引擎研究[期刊论文]-辽东学院学报（自然科学版）2008,15(3)
10. 单长虹.张焕国.孟庆树.彭国军 一种启发式木马查杀模型的设计与分析[期刊论文]-计算机工程与应用2004,40(20)

引证文献(10条)

1. 霍珊 数据挖掘在计算机病毒中的应用[期刊论文]-才智 2011(36)
2. 崔鹏 基于形式化语义的启发式病毒检测引擎研究[期刊论文]-辽东学院学报（自然科学版） 2008(3)
3. 崔鹏 基于语义的启发式病毒检测引擎研究[期刊论文]-常熟理工学院学报 2008(10)
4. 谭云松 一种启发式反病毒技术的研究[期刊论文]-网络安全技术与应用 2006(11)
5. 王振海.王海峰 基于多态病毒行为的启发式扫描检测引擎的研究[期刊论文]-实验室研究与探索 2006(9)
6. 张永超.张磊.张权.唐朝京 反病毒虚拟机的缺陷及其改进[期刊论文]-信息安全与通信保密 2011(9)
7. 王平 基于虚拟机技术的DCS仿真系统设计与实现[期刊论文]-微型机与应用 2010(7)
8. 陈志峰.张申生.张熙哲 基于虚拟机技术的密码系统的研究与实现[期刊论文]-计算机应用与软件 2009(3)
9. 顾兴杰 嵌入式系统动态加载引擎的研究[学位论文]硕士 2006
10. 王春东.魏俊锋 基于OAP板卡的网关防病毒技术研究[期刊论文]-数字技术与应用 2011(11)