虚拟机查毒技术的实现

刘勇[1] 邱玲[2]
(1.人工智能四川省重点实验室 四川自贡 643000 2.四川理工学院计算机科学系 四川自贡 643000)

摘 要：近些年，虚拟机技术在反病毒界也被称为通用解密器，已经成为反病毒软件中最引人注目的部分。本文将以32位自含代码虚拟机w32encode的程序结构和流程为例阐述自含代码虚拟机查毒技术的实现问题。
关键词：虚拟机 查毒技术 自含代码
中图分类号：G623.58 文献标识码：A 文章编号：1674-098X(2008)06(c)-0025-02

反计算机病毒作为计算机安全问题的一个重要组成部分已日益受到人们的重视。传统的反病毒软件使用的是基于特征码的静态扫描技术，但这种方法在当今病毒技术迅猛发展的形势下已经起不到很好的作用了。目前形式下主要采用的最新反病毒技术是虚拟机和实时监控技术。

1 虚拟机查毒技术的基础

虚拟机查毒技术即启发式探测未知病毒的反病毒技术。虚拟机技术的主要作用是能够运行一定规则的描述语言。

查毒的虚拟机是一个软件模拟的CPU，它可以取指，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，如此循环反复直到某个特定情况发生以结束工作，这就是虚拟机的基本工作原理和简单流程。

设计虚拟机查毒的目的是为了对付加密变形病毒，虚拟机首先从文件中确定并读取病毒入口处代码，然后以上述工作步骤解释执行病毒头部的解密段，最后在执行完的结果中查找病毒的特征码。这里所谓的“虚拟”，是指染毒文件没有实际执行，只是虚拟机模拟了其真实执行时的效果。

2 自含代码虚拟机(SCCE)

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。SCCE的代码巨大而且速度很慢。然而SCCE对于一个先进的反病毒软件是很有用的。所有指令都在内部被处理，虚拟机可以对每条指令的动作做出非常详细的报告，这些报告和启发式数据以及通用清除模块将相互参照形成一个有效的反毒系统。同时，反病毒程序能够最精确地控制内存和端口的访问，因为它自己处理地址的解码和计算。

3 32位自含代码虚拟机w32encode

32位自含代码虚拟机w32encode由w32encode.cpp,Tw32asm.h,Tw32asm.cpp做为查毒引擎的一部分和其它搜索清除模块联编为Rsengine.dll。

w32encode的工作原理是：它首先设置模拟寄存器组的初始值，初始化执行堆栈指针，然后进入一个循环，解释执行指令缓冲区中的头256条指令，如果循环退出时仍未发现病毒的解密循环则可由此判定非加密变形病毒，若发现了解密循环则调用EncodeInst函数重复执行循环解密过程，将病毒体明文解密到DataSeg1或DataSeg2中。

4 w32encode的工作代码

W32Encode0中总体流程控制部分代码：

```
for (i=0,i<0x100,i++)                    //首先虚拟执行256条指令试图发现病毒循环解密子
    {
      if (InstLoc>=0x280)
    return(0);
      if (InstLoc+ProgSeekOff>=ProgEndOff)
    return(0);                           //以上两条判断语句检查指令位置的合法性
    saveinstloc();                       //存储当前指令在指令缓冲区中的偏移
        HasAddNewInst=0;
      if (!(j=parse()))                  //虚拟执行指令缓冲区中的一条指令
    return(0);                           //遇到不认识的指令时退出循环
    if (j==2)                            //返回值为2 说明发现了解密循环
    break;
    }
  if (i==0x100)                          //执行过256条指令后仍未发现循环则退出
      return(0);
  PreParse=0;
  ProcessInst();
  if (!EncodeInst())                     //调用解密函数重复执行循环解密过程
  return(0);
  Pjmp中判定循环出现部分代码：
  if ((loc>=0)&&(loc<InstLoc))           //若转移后指令指针小于当前指令指针则可能出现循环
  if (!isinstloc(loc))                   //在保存的指令指针数组InstLocArray中查找转移后指
      ......                             令指针值，如发现则可判定循环出现
    else
      {
        ......
    return(2);
返回值2 代表发现了解密循环
  }
```

parse中虚拟执行每条指令的过程较复杂一些：parse会从取得指令缓冲区中取得当前指令的头两个字节并根据它们的值调用相应的指令处理函数。当执行进入特定指令的处理函数中时，首先要通过判断寻址方式确定指令长度并将控制权交给saveinst函数。saveinst在保存该指令的相关信息后会调用真正指令执行函数W32ExecuteInst。这个函数和parse非常相似，它从SaveInstBuf1中取得当前指令的头两个字节并根据它们的值调用相应的指令模拟函数以完成一条指令的执行。相关部分代码如下：

W32ExecuteInst中指令分遣部分代码：

```
if ((c&0xf0)==0x50)
    {if (ExecutePushPop1(c))
// 模拟push和pop
        return(gotonext());
        return(0);
    }
if (c==0x9c)
    {if (ExecutePushf())
// 模拟pushf
        return(gotonext());
        return(0);
    }
if (c==(char)0x9d)
    {if (ExecutePopf())
// 模拟popf
        return(gotonext());
        return(0);
    }
if ((c==0xf)&&((c2&0xbe)==0xbe))
    {if (i=ExecuteMovszx(0))
// 模拟movszx
        return(gotonext());
        return(0);
    }
```

5 结语

目前虚拟机的处理对象主要是文件型病毒，对于引导型病毒、word/excel宏病毒、木马程序在理论上都是可以通过虚拟机来处理的。受病毒在理论上就是不可判定的这一根本前提的制约，尽管虚拟机在

现代信息技术在中医院校发展中的作用

苏传琦
(南京中医药大学 江苏南京 210029)

摘 要：本文从数据库，医院信息系统和多媒体等三方面讨论了现代信息技术在中医院校教学科研中的应用现状。并结合我校工作实际，讨论了现代信息技术在未来发展中能发挥的重要作用。

关键词：信息技术 数据库 多媒体
中图分类号：G64 **文献标识码**：A **文章编号**：1674-098X(2008)06(c)-0026-01

随着计算机技术、网络通信技术、软件技术和数据库技术的快速发展，信息技术已经成为当今中医院校发展的强力助推剂，深深的渗透进中医院校教学、科研的各个方面，成为学校发展与学科建设中不可缺少的一部分。当前，信息技术在中医院校发展中的应用越来越多下面我们重点探讨现代信息技术在中医药院校发展中所起到的作用。

1 数据库与数据挖掘

相对于较为成熟的西药数据库，我国中医药行业数据库建设较晚，起源于20世纪80年代，经过20余年的建设已经取得了初步的成果。到目前为止，国内已经有数10个中医药大学、学院及研究所建设了各种规模不同的、近百个中医药信息数据库，初步实现了中医药信息数字化。

中医药院校作为教学科研的第一线，是数据采集、数据整理、数据信息化的重要力量。通过纸张数字化，分门别类的进入数据库，我们能够很方便对文献数据进行浏览、查询、修改、补充、批注等操作。大大提高了数据使用率，科研效率和教学效果。建成后的数据库将成为一种价值资源，被无数的后来者享用。

尽管中医药现代资料数据库的建设已经具有一定的规模，但是也存在着一些问题。除了重复建设现象严重，持续性建设状态不好外，数据库的应用仅仅停留在查询和统计上，使其价值没有充分发掘是最大问题。因此，如何发掘数据库海量数据中隐含的知识成为了当前人们研究的热点。数据挖掘技术或称KDD(Knowledge Discovery in Database,数据中知识发现)应运而生。所谓数据挖掘，就是从大量的、不完全的、有噪声的、模糊的、随机的数据集中识别有效的、新颖的、潜在有用的以及最终可理解的模式的非平凡过程。数据挖掘技术在西药数据库中的应用较早，中医方面还在转型之中。但是中医药院校目前的课题已经又单纯的使用数据库转向了发掘数据库中隐含的知识。更多的使用到了归纳、抽取、汇总、推导等方法，这就使得数据挖掘技术登上了中医这座舞台。在我国进行的“九五”项目“中药现代化关键问题的基础研究”中开展了“中药复方人工智能信息系统的研究”；国家“973”项目“方剂关键科学问题的基础研究”中也开展了有关方剂基础科学数据的信息处理研究，取得了一定的研究成果。为中医药院校科研成果创新作出了较大的贡献。

2 医院管理信息系统(HIS)

管理信息系统就是利用计算机技术、网络通讯技术和软件技术等开发出来的应用系统，几十年来，管理信息系统广泛应用于医学领域的科研、教育、医疗和生产经营等各个方面，其中较有影响的是医院管理信息系统HIS(Hospital Information System)。

我国卫生部2002年的定义是：医院信息系统是指利用计算机软硬件技术、网络通讯技术等现代化手段，对医院及其所属各部门的人流、物流、财流进行综合管理，对在医疗活动各阶段中产生的数据进行采集、存储、处理、提取、传输、汇总、加工生成各种信息，从而为医院的整体运行提供全面的、自动化的管理及各种服务的信息系统。由于国家卫生部对医院信息化工作的重视，要求三级甲等医院必须配备HIS，目前我国的大中型医院一般都具备规模不一、程度不同的医院信息系统。因此，医院信息系统的体系结构、功能模块、技术特点以及发展趋势等，是医学院校的学生必须熟悉的。在全校范围内开设医学信息为必修课，建设医学信息开放性实验室，能使学生尽早接触和了解到相关的知识，从而在工作中能尽快适应实际环境，做到得心应手。

中医药院校作为中医教育的摇篮，无数的中医药人才在这座温床上茁壮的成长，这无疑是非常重要的一环。培养人才适应社会、医院、企业的需求，是中医药院校发展的根本。医药知识过硬，又懂计算机和网络技术，又有信息分析处理和服务能力的复合型人才无疑成为了抢手的“香饽饽”，不管在哪个行业都能成为学校最佳的形象代言人。毕业生口碑好，就有更多的单位青睐，就业率提高了，就有更多人来报考，学校的规模才会变大。循环效应的好处不言而喻，这其中最为重要的一环就是如何培养学生。撇开中医药专业知识不谈，现代信息技术的教育在其中起着举足轻重的作用。

3 多媒体教学手段的应用

媒体是信息的载体，信息只有通过媒体的传播才能发挥作用。多媒体教学充分利用了各种资源，如录像、CD、DVD等，对它们进行优化组合，得到了更好的信息传递方式，并达到了更佳的传播效果。

应用多媒体教学使学生了解医学实验病例及手术过程更加直观、生动，师生之间的相互交流更加便利，起到了传统教学所起不到的作用。在中医院校应用多媒体教学，还有它自身的教学特点，因为有很多传统经典的教学内容，简单的制作表达不出它的内涵，比如四大经典的内容、医古文、脉象的内容等。中医药网络课程、网络课件、CAI课件不断推出，让教师对多媒体教室的设施和教学资源的合理配置也有了更多的理解，这都将有利推动中医院校教学改革的进程，将会给中医教育观念、思想、方法、内容、手段乃至人才培养模式带来巨大的变革，具有深远的意义。

信息技术已经渗透到中医院校教学与科研的各个方面，有力的促进了中医药现代化的发展。展望未来，这种渗透力度会越来越强，信息技术和中医的融合将改变几千年来中医发长缓慢，中医人才培养困难的局面，给中医药带来革命性的变化。

参考文献

[1] 张福炎，孙志挥.大学计算机信息技术教程[M].南京大学出版社，2007，6.
[2] 施诚，等.医院信息系统教程[M].中国中医药出版社，2007，8.
[3] 杜建强.信息技术在医药领域中的应用[J].计算机与现代化，2005，12.

实践中不断得到发展，但其成功的概率永远不可达到100%。这是惟一的却又是无可奈何的缺憾。

参考文献

[1] William Stallings(美)著 杨明等译.密码编码学与网络安全原理与实践[M].北京：企业管理出版社，2004.
[2] 凌捷.计算机数据安全技术[M].北京：科学出版社，2004.
[3] 杨力平.计算机房罪与防范[M].北京：电子工业出版社，2002.
[4] 李成大，张京，龚茗.计算机信息安全[M].北京：人民邮电出版社，2004.

虚拟机查毒技术的实现

作者： 刘勇， 邱玲
作者单位： 刘勇(人工智能四川省重点实验室,四川自贡,643000)， 邱玲(四川理工学院计算机科学系,四川自贡,643000)
刊名： 科技创新导报
英文刊名： SCIENCE AND TECHNOLOGY INNOVATION HERALD
年，卷(期)： 2008(18)
被引用次数： 1次

参考文献(4条)

1. [美]William Stallings;杨明 密码编码学与网络安全原理与实践 2004
2. 凌捷 计算机数据安全技术 2004
3. 杨力乎 计算机房罪与防范 2002
4. 李成大;张京;龚茗 计算机信息安全 2004

本文读者也读过(7条)

1. 李洪敏.凌荣辉 反病毒引擎技术初探[会议论文]-2003
2. 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)
3. 刘正宏 变形病毒的分析与检测[期刊论文]-网络安全技术与应用2009(5)
4. 彭炎 基于虚拟机的虚拟实验室可编程控制模型研究[学位论文]2003
5. 陈健伟.朱梅.Chen Jianwei.Zhu Mei 计算机病毒与反病毒技术研究[期刊论文]-电脑与电信2006(12)
6. 武炳正.武延军.贺也平.WU Bingzheng.WU Yanjun.HE Yeping 基于虚拟机架构的自修改代码监测技术[期刊论文]-计算机工程与应用2011,47(10)
7. 曾宪伟.张智军.张志.Zeng Xianwei.Zhang Zhijun.Zhang Zhi 基于虚拟机的启发式扫描反病毒技术[期刊论文]-计算机应用与软件2005,22(9)

引证文献(1条)

1. 张智军.覃健诚 虚拟机无人值守自动监护系统研究[期刊论文]-科技创新导报 2011(10)