病毒检测技术的研究与 0.5 级环

朱俚治
(南京航空航天大学 信息中心,江苏 南京 210016)

摘 要:检测病毒是清除病毒的第一步,它是维护系统安全的关键技术之一。在描述了由比较法和校验和法组成的综合检测法后,设计了一种消除病毒的算法。为了支持比较法,提出原始文件概念,在环保护特权规则的基础之上,提出 0.5 级环方法,并给出了存储原始文件的逻辑空间和写操作的环境。文中还对建立原始文件的必要性、原始文件集的组成原则进行了讨论,并描述了原始文件的硬件保护方法,且给出了逻辑示意图。文中试图为网络安全提供一种新的研究思路。

关键词:病毒;检测;环保护
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2012)09-0225-03

Research on Detecting Virus and 0.5 Level Ring

ZHU Li-zhi
(Information Center, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

Abstract: Detecting virus is the first step, it is one of the key techniques of maintaining systems safety. After describing comprehensive detection method that is composed of comparing method and checking sum method, a kiss virus algorithm is designed. To support comparing method, primitive file is proposed. The 0.5 level ring is proposed based on the privileged regulation of ring protection, and the logical space of storing primitive files and the environment of write operation are given. Additionally, the necessity of setting primitive file and the principles of building primitive file set are discussed, and the protecting way with hardware is described, the logical sketch is given. It attempts to provide a new thinking for the research of network security.

Key words: virus; detecting; ring protection

0 引 言

病毒是一种具有智能和自身隐藏技术的特殊程序。当病毒进入到计算机后,就寄生在应用程序或系统程序中。当感染了病毒的程序得到运行,就可能出现传播病毒、破坏正常程序、不断消耗有限的资源等情形。此时,计算机系统就受到了严重的威胁。因此,为了用户程序和系统程序能够正常地运行,必须清除病毒。检测病毒,即检查并测定病毒隐藏在何处,是清除病毒的首要任务。目前,识别恶意代码主要从其特征行为进行研究[1~3];防御病毒策略的研究在网络和操作系统两方面进行[4~6],这体现了人们想从传播途径和计算机系统方面根治病毒的愿望;检测病毒主要采用了数学方法[7~9]、仿生和智能方法[10~13]。在防治病毒方面虽然取得了很多成果,但对病毒进行检测是关键的首要步骤。文件内容被改变是文件感染病毒的基本特征。文中以文件是否被改变为基准,讨论基于比较法判别文件感染病毒的可能性,并重点研究原始文件的保护方式。

收稿日期:2012-01-20;**修回日期**:2012-04-23
基金项目:国家"863"高技术发展计划项目(2009AA043303);软件开发环境国家重点实验室开放课题(SKLSDE-2011KF-04);
作者简介:朱俚治(1980-),男,助理工程师,研究方向为计算机网络和信息安全。

1 病毒检测和消除的基本算法

目前有比较法、校验和法、行为检测法等多种病毒的检测方法。尽管比较法和校验和法不属智能型病毒检测方法,但它们简单可靠,是检测方法中的经典之作。采用校验和法时,需要假设有一个未被病毒感染的原始文件 A 存在,这才能用被检测文件 B 的校验和与 A 进行比较。若校验和不等,则表明 B 已被破坏,它可能被感染病毒;若校验和相等,只能说明 B 未被感染病毒的可能性较大,但不能表明 B 未被感染病毒。因此,校验和法只能作为检测文件的原始程度。

采用比较法可以检测文件 B 与 A 是否相同,并可以将不同之处给以定位,为后续的清除病毒程序提供了便利。与校验和法一样,采用比较法时需要原始文件 A。

校验和法的优点是速度快、简单;比较法的优点是准确、可定位。在设计实用的病毒检测算法时,往往是

将比较法和校验和法结合在一起,形成具有一定智能的检测手段,这种基本的综合算法如图 1 所示。该方法能较为快捷地决定对被检测文件是否需要按有病毒的方式进行处理。

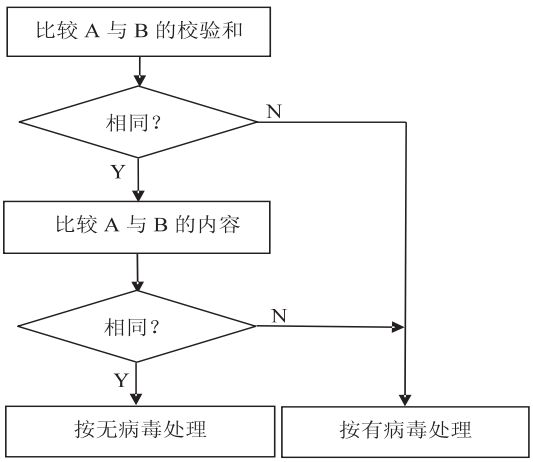

图 1 综合检测法

在综合检测过程中,对疑似感染文件可以采用以下算法处理。

Step1:原始文件的长度→计数器 A,原始文件首地址→指针 A,被检测文件首地址→指针 D,被检测文件的长度→计数器 D,缓冲区首地址→指针 B;

Step2:if ((指针 A))-((指针 D))≠0,转 Step5;

Step3:((指针 A)) → (指针 B),(指针 A)+1 → (指针 A),(指针 B)+1 → (指针 B);

Step4:if (计数器 A)-1 → 计数器 A=0, 结束;

Step5:if (计数器 D) -1→计数器 D=0, then 提示无法消除病毒,并建议删除该文件,结束, else 转 Step2。

如果在 Step4 结束,被检测文件的病毒就被去除了。

从上述的基本算法中可以看出:保护原始文件(含系统程序和应用程序),使其不被更改,是采用比较法的根本前提。

2 原始文件的保护

原始文件是指未被病毒感染的只读文件。计算机系统中的文件都是存储在存储器中,为了使已保存在存储器中的原始文件不受破坏,只要限制存储器的写操作,就能达到目的。例如,将原始文件保存在只读光盘或 ROM 中,就能很好地保护原始文件。然而,这样又缺乏对存储器操作的灵活性。下面讨论一种新的保护方法。

2.1 环保护法

程序可以划分为系统程序和应用型程序,一般来讲,它们都储存在磁盘上。从系统的安全看,系统程序属于计算机系统的核心,一旦系统程序感染了病毒,就可能给计算机系统带来灾难性后果,病毒发作就会使得系统崩溃。目前,常采用环形保护法,尽量使系统程序免遭破坏。环保护采用特权级别对系统程序与应用程序之间的隔离,级别越小,拥有的访问权限越高,即程序拥有的权限随着所在环的级别递增而逐级递减。特权规则主要有两条:级别 n 的数据只能由不大于 n 的特权级进行访问;具有 n 级别的程序只能由不小于 n 的级别的程序调用。Intel 等著名公司支持环形保护,图 2 是 32 位微处理器的特权保护。

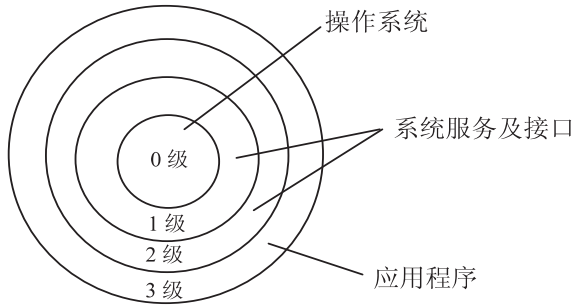

图 2 intel32 位微处理器的 4 级环保护

图 2 中的操作系统、系统服务及接口、应用程序都是能够运行的程序。而原始文件在一般情形下不能进行写操作,这是为了防止病毒感染;而在确定某一文件为原始文件时,却又要写入磁盘。因此,利用环形保护,需要为原始文件的集合开辟一个逻辑空间,并确定写操作时的环境。

2.2 0.5 级环

由于原始文件应能够被操作系统管理,即它们的特权级要低于操作系统;又由于原始文件能由比它特权级低的程序读出,所以原始文件的特权级应在图 2 所示的操作系统和其它部分之间。图 3 是以图 2 为基础,在 0 级和 1 级之间设置存放原始文件集合的逻辑空间——0.5 级环的环保护示意。

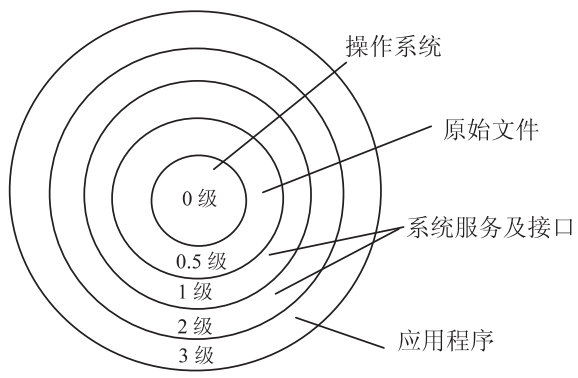

图 3 含原始文件的环保护逻辑示意

再从特权规则分析,由于 0.5>0,所以 0.5 级环能以数据形式被操作系统访问,换言之,操作系统对它们可读可写。由于 0.5<1,所以 0.5 级环内的文件能以程序形式被系统服务及接口和应用程序访问,即只能

读。可知,0.5 级环只能被操作系统进行写操作。进一步讲,只要操作系统不被病毒感染,存储在 0.5 环的原始文件是无法感染病毒的。因此,设置 0.5 环,对于原始文件免受病毒感染是必要的,也是有效的。

下面讨论写入 0.5 环的环境。当确定某一文件为原始文件时,为了避免在写入 0.5 环的过程中被病毒感染,必须采取合适的措施,主要步骤和理由如下:

(1)断开计算机网络,防止网络病毒的侵入;

(2)关闭所有正在运行的程序(不含操作系统),预防已侵入病毒发作;

(3)关闭硬中断,防止由时钟中断或引发已隐藏的病毒发作。

总之,在净化环境中,将原始文件写入 0.5 环才是安全的。

2.3　进一步的讨论

(1)建立原始文件的必要性。

前面已论述:采用比较法必须有原始文件。那么,在具体应用中直接使用原始文件是否可行呢? 从防病毒的角度看,回答是否定的,其原因是比较复杂的。但主要理由有两点:

①从操作系统角度看,欲运行在磁盘上的程序要经历一个过程。如图 4 所示,运行程序 A,必须先使其先成为作业并处于保持状态;作业进入主存储器后成为进程,处于准备状态;当得到 CPU 访问,进程就处于运行状态;当进程的运行结束后就退出主存又成为作业,处于终止状态,并在适当的时候再使它成为程序(存储于磁盘)。因此,回写磁盘的程序有可能与成为作业前的程序不同,这是因为在正常运行时产生变化(如改变了数据),或由病毒作用时改变了程序。

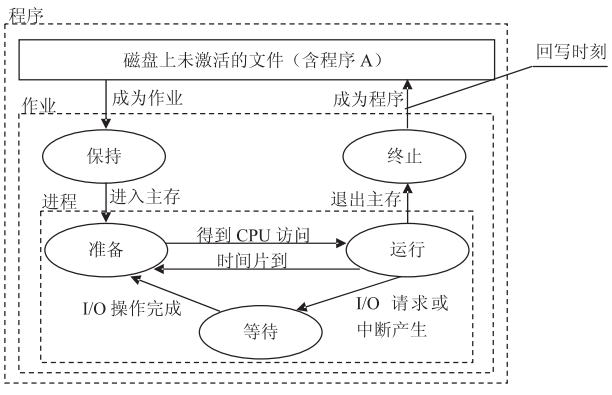

图 4　程序运行过程示意

② 从虚拟存储器角度看,在分配给程序 A 的主存空间完全占用时要调用不在主存的信息,此时只能将主存中暂不需用的信息送回磁盘原处。与①同样的原因,送回的信息有可能与原先的不同。

综上所述,建立标本式的原始文件,对于采用比较法抗病毒是必要的。

(2)原始文件集的组成原则。

显然,采用原始文件方法,就要有副本,这肯定会大量占用存储资源。为了既能有效地检测病毒,又能相对较少地占用存储空间,必须选择少数文件作原始文件,选择原则大致如下:

①是可以运行的代码文件和重要数据;

②是工具软件;

③是经常使用的程序。

对于一般的纯数据文件,如 doc 文档、xls 文档等,不必作为原始文件。

(3)操作系统自身如何抗病毒。

采用 0.5 级环和原始文件方法的前提是操作系统安全、可信。因此保护操作系统是头等主要的。尽管环保护能提供较好的机制,但采用代码只读策略会更有效。如将操作系统的代码和数据分离,将代码存放于只读光盘。这样就可以消除被病毒感染的风险。

(4)原始文件的硬件保护方法。

随着硬件价格的急剧下降,采用 Flash 储存器存放原始文件已成为可能,在抗病毒方面其效果更佳。Flash 是一种具有记忆功能和快速擦除功能的只读储存器,写入信息时需要采取特殊措施,即除了 WE(写)引脚正常工作外,还必须使得引脚 Vpp 始终处于供电状态。图 5 给出了作为原始文件存储空间的 Flash 存储器的简单逻辑设计示意。

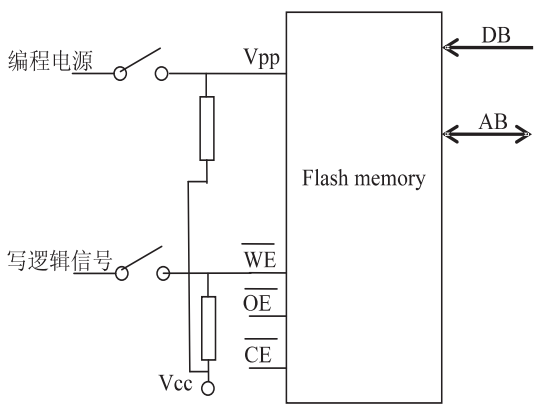

图 5　用于原始文件 Flash 存储器的逻辑设计示意

正常工作时,图中的开关处于断开状态,这就从物理上完全避免了对 Flash 的写入,从而彻底杜绝病毒的感染。在需要写入时,必须符合 2.2 所讨论的写入 0.5 环的环境,并采用非编程方式,使得开关闭合,然后启动写程序。在 Flash 写操作完成后,再使开关处于断开状态。

3　结束语

文中探讨了检测病毒的一些基本方法,讨论了原始文件的必要性、原始文件的组成原则和原始文件的

(下转第 231 页)

保障网络的安全性。

4　结束语

针对目前无线传感器网络安全技术处于静态预置安全措施被动防守、动态防护能力不强的问题,文中设计了面向主动防御的 WSN 安全框架,给出了面向未来的弹性的主动防御安防模式。今后研究的重点是进一步强化入侵预测和响应模块的细节。

参考文献:

[1] 孙利民. 无线传感器网络[M]. 北京:清华大学出版社,2005.

[2] Perrig A,Szewczy R. SPINS:Security Protocols for Sensor Networks[C]//Mobile Computing and Networking. Rome,Italy:[s. n.],2001.

[3] Karlof C,Sastry N,Wagner D. TinySec:A Link Layer Security Architecture for Wireless Sensor Networks[C]//Proc. of the 2nd ACM Conference on Embedded Networked Sensor Systems. Baltimore,USA:ACM,2004.

[4] Park T,Shin K G. LiSP:A Lightweight Security Protocol for Wireless Sensor Networks[J]. ACM Transactions on Embedded Computing Systems,2004,3(3):86-88.

[5] 苏　忠,林　闯,封富君,等. 无线传感器网络密钥管理的方案和协议[J]. Journal of Software,2007,18(5):1219-1221.

[6] 李少衡,张　琨,王翠荣. 无线传感器网络中的一种安全高效的路由协议[J]. 北京化工大学学报,2007,34(Sup):117-118.

[7] Lazos U,Poovendran R. SeRLoc: robust localization for wireless sensor network[J]. ACM Transactions on Sensor Networks,2005,1(1):73-100.

[8] Elson J,Girod L,Estrin D. Fine Grained Network Time Synchronization Using Reference Broadcasts[C]//Operating Systems Design and Implementation. New York,NY, USA:ACM,2002.

[9] Przydatek B,Song D X,Perrig A. SIA: secure information aggregation in sensor networks[J]. Special Issue on Security of Ad-hoc and Sensor Networks,2007,15(1):69-102.

[10] Deng J,Han R,Mishra S. Secure Code Distribution in Dynamically Programmable Wireless Sensor Networks[C]//Proceedings of the 5th international conference on information processing in sensor networks. New York,NY,USA:ACM,2006.

[11] Jeong J,Culler D. Incremental Network Programming for Wireless Sensors[C]//Proc. of the First IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks. Santa Clara,CA,USA:[s. n.],2004.

[12] Tirkawi F,Fischer S. Remote Interaction Tool for Wireless Sensor Networks[C]//3rd IEEE International Symposium on Wireless Pervasive Computing. [s. l.]:[s. n.],2008.

(上接第 227 页)

保存方法。文中提出了 0.5 级环方法,并给出了写入环境;0.5 级环的可信度依赖于操作系统的安全,文中对操作系统本身如何抗病毒也进行了设想;实现 0.5 级环的最佳方法应是在设计操作系统时就将其考虑,使它成为操作系统的一个基本功能。顺便指出,2.3 节所讨论的原始文件若已在磁盘或 Flash 存储器中,在一定的条件下,是不需要回写的。

在进行病毒检测的研究同时,笔者也注意到综合化和智能化的杀毒技术的进展,这是一个值得研究的重要方向。

参考文献:

[1] 刘巍伟,石　勇,郭　煜,等. 一种基于综合行为特征的恶意代码识别方法[J]. 电子学报,2009,37(4): 696-700.

[2] 左黎明,刘二根,徐保根,等. 恶意代码族群特征提取与分析技术[J]. 华中科技大学学报(自然科学版), 2010,38(4):46-49.

[3] 刘　磊,邵　堃. 恶意代码行为分析技术研究与应用[D]. 合肥:合肥工业大学,2009.

[4] Geer D. Behavior-based security become the main-stream of network security[J]. Computer,2006,39(3):14-17.

[5] 李　明,范明钰. 基于网络行为分析的未知恶意代码检测系统的研究与实现[D]. 成都:电子科技大学,2009.

[6] 周　冲,张琼声. 操作系统病毒防御策略的研究[D]. 北京:中国石油大学,2009.

[7] Christodorescu M,Jha S. Static analysis of execut-ables to detect malicious patterns[C] //Proceedings of the 12th USENIX Security Symposium. [s. l.]:[s. n.],2003:169-186.

[8] Karnik A,Goswami S,Guha R. Detecting obfuscated viru-ses using cosine similarity analysis[C]//Proceedings of the 1st Asia International Conference on Modeling and Simulation. Phuket Thailand:[s. n.],2007:165-170.

[9] 张波云,殷建平,唐文胜,等. 基于模糊模式识别的未知病毒检测[J]. 计算机应用,2005,25(9):2050-2053.

[10] 王　维,张鹏涛,谭　营,等. 一种基于人工免疫和代码相关性的计算机病毒特征提取方法[J]. 计算机学报,2011,34(2):204-215.

[11] 洪群业,唐学文. 基于分类的未知 PE 病毒检测技术的研究[D]. 重庆:重庆大学,2010.

[12] 张　勇,张卫民,欧庆于. 基于主动学习的计算机病毒检测方法研究[J]. 计算机与数字工程,2011,39(11):89-93.

[13] 庄蔚蔚,姜青山. 基于增量学习关联分类规则的病毒检测方法研究[D]. 厦门:厦门大学,2009.

病毒检测技术的研究与0.5级环

作者： 朱俚治
作者单位： 南京航空航天大学 信息中心,江苏 南京 210016
刊名： 计算机技术与发展
英文刊名： Computer Technology and Development
年，卷(期)： 2012(9)

参考文献(12条)

1. Hollerer T H;Feiner S K Mobile augmented reality 2004

2. Wikipedia Augmented reality 2009

3. 彭志宇;李善平 移动环境下LBS位置隐私保护[期刊论文]-电子与信息学报 2011(05)

4. Mokbel M F;Chow C Y;Aref W G The newCasper:query processing for location services without compromising privacy 2006

5. Gedik B;Liu L Protecting location privacy with personalized k-anonymity:architecture and algorithms 2008(01)

6. Gruteser M;Grunwald D Anonymous usage of location based services through spatial and temporal cloaking 2003

7. Kido H;Yanagisawa Y;Satoh T Protection of location privacy using dummies for location-based services 2005

8. 潘晓;肖珍;孟小峰 位置隐私研究综述[期刊论文]-计算机科学与探索 2007(03)

9. 王平水;马钦娟 隐私保护K-匿名算法研究[期刊论文]-计算机工程与应用 2011(28)

10. Machanavajjhala A;Gehrke J;Kifer D L-diversity:privacy beyond k-anonymity 2006

11. Mohalsen A;Hong D;Nyang D Privacy in location based services:primitives toward the solution 2008

12. Aryan A;Singh S Securing Location Privacy in Augmented Reality 2010