文章编号:1000 - 582X(2002)10 - 0121 - 03

计算机软件系统的保护及恢复技术*

姚渝春,李 杰
(重庆大学 职业技术学院,重庆 400030)

摘 要:为了更好地解决大型计算机实验室软件系统的保护和恢复问题,分析了目前所采用的计算机软件系统保护和恢复技术的特点,以及在安全性和稳定性等方面存在的缺陷,从理论和实践两个角度研究了造成这些问题的原因和解决办法,并提出了两条改进途径:一是提高计算机硬件对保护卡的支持程度,特别是要增加 BIOS 对保护卡的直接支持;二是开发新型的主机/终端机计算机系统,利用访问权限保证软件系统的安全。

关键词:计算机;软件系统保护;计算机安全;系统保护卡
中图分类号:TP 311.53 **文献标识码**:A

计算机软件系统保护是计算机系统安全的一个组成部分,事实上,它比计算机系统安全的其它部分如硬件系统保护、计算机网络安全、运行安全等更难以实现。困难的根源不在于技术方面,而在于软件系统的开放性、可操作性需求与安全保护之间的相互矛盾。特别是对于 PC,从硬件角度上讲,不能限制用户对外存储设备的使用;从软件角度来看,现有的操作系统(包括有安全机制的网络操作系统)只能做到限制用户对资源的正常使用,缺少硬件层面的支持,很难防止对软件系统的恶意破坏。单台计算机数据破坏所造成的损失是有限的,但这种事件发生的频率非常高,其损失的总量是相当惊人的。这个问题在一些公用程度较高的计算机上尤为突出,最明显的例子就是高等院校的计算机实验室,无意或故意的破坏行为经常发生,管理人员需耗费大量的时间和精力用于修复和重新安装软件系统,大大降低了计算机的使用效率。由此引出了对计算机软件系统的保护及恢复技术的研究[1]。

1 软件系统保护及恢复技术的现状

对软件系统的保护应考虑两个方面的问题,既要防止对软件系统的非授权修改,又要尽可能少地限制使用者对各种资源的使用。目前的微机及普通的服务器在硬件设计中几乎没有考虑这样的功能,只有一些最简单的保护措施:如通过设置 CMOS 限制对软盘的写、禁止修改硬盘主引导记录等等,靠这些措施来保护软件系统是远远不够的。现有操作系统同样缺乏对软件系统的保护功能,多用户操作系统可以通过设置访问权限一定程度地限制用户对硬盘资源的正常使用,但无法阻止故意的破坏,重新安装系统、删除硬盘分区等操作是不受限制的[2]。因此,保护软件系统必须使用其他方法,目前最常见的办法就是采用系统保护卡(硬保护)和系统保护软件(软保护)。

系统保护卡的工作层面是介于硬件层和操作系统之间,因而有较高的安全性。系统保护软件的工作层面是介于操作系统和应用软件之间,换句话说,只要能阻止计算机从硬盘启动,就能使保护软件失效,因此,其安全性不如硬保护好。系统保护软件与应用程序之间的冲突也是一个大问题。从市场的统计情况来看,系统保护卡的销量要大大高于系统保护软件,后者主要用于笔记本电脑和软件系统比较简单的台式机。

软件系统的恢复与保护是相互关联的,任何保护措施都不是绝对可靠,因此,在进行保护的同时,必须考虑到软件系统的备份及恢复,目前采用得最多的是硬盘克隆技术(Disk Clone)。硬盘克隆在备份数据时与普通的数据备份工具不同,它不但要记录文件内容,还可以记录硬盘主引导记录、分区表、文件分配表等信

* 收稿日期:2002 - 06 - 24
作者简介:姚渝春(1967 -),男,重庆人,重庆大学工程师。主要从事计算机应用技术研究。

息。因此,它最适合于软件系统遭到彻底破坏时的恢复。克隆软件在备份和恢复数据时,可以按逐道逐扇区的方式进行,这种方式可避免因文件系统格式不同造成的不兼容问题。某些网络克隆软件还能以 Client/Server 方式工作,可通过一台服务器一次性的批量恢复多台计算机的软件系统[3]。由于克隆软件强大的功能,在计算机实验室中,它已经成为一个必不可少的工具。经过大量的测试,我们认为 Norton 和 Symantec 两家公司的克隆软件在功能和可靠性上比较突出。此外,目前已经出现了将软件系统保护功能和网络克隆功能合二为一的硬件产品。

某些操作系统也带有系统备份和恢复功能,如 Linux 的"Tar"和 Windows XP 的"系统还原",但这些功能必须是在操作系统可正常启动的前提下才能使用,在软件系统的灾难恢复上,几乎没有价值。

2 系统保护卡的种类、特点及工作原理

我国对微机软件系统保护技术的研究始于 20 世纪 80 年代中后期,从 90 年代初陆续开发出一些基于 DOS 操作系统的系统保护卡和软件,这些产品各有特点,基本原理一般是通过重定向 DOS 的写中断,使得对硬盘的写操作成为"假写",或者干脆限制对硬盘的写操作,以实现对软件系统的保护。但早期的产品有明显的缺陷,一是兼容性差,大部分只能用于 DOS;二是降低系统运行速度和限制对硬件资源的使用;三是不能防止一些高级工具软件对磁盘的分区和格式化,安全性差,这也是最致命的缺陷;四是未考虑数据破坏后的快速恢复问题。近几年来,国内的几家 IT 企业各自研制出了新型的系统保护卡,其中著名的有北京泰利德、海光科技及三茗科技等。新一代的产品在兼容性、稳定性、安全性以及功能上都有明显提高,某些产品除了有保护功能外,还具有网络恢复功能,因而被广泛采用。三茗的产品甚至已经销往像韩国这样 IT 业较为发达的国家[4]。

系统保护卡是一块安装在 PCI 或 ISA 插槽上的扩展设备,其核心部件是一片内置有指令的 ROM 或 FLASH ROM 芯片,芯片的容量一般在 1 ~ 4 MB 之间。

按照插槽类型可将保护卡分为 PCI 和 ISA 两种类型,由于 PCI 设备能自动分配地址和中断号,一般不会出现硬件冲突,而 ISA 类的保护卡可能会与其他 ISA 设备发生地址冲突,需要人工修改设置。目前 ISA 类的保护卡逐渐被 PCI 类所取代。

按照功能可将保护卡分为单一功能的保护卡和多功能保护卡,后者其实就是一块带有 BOOTROM 芯片的网卡,其芯片中除了有网络引导程序外,还有系统保护程序,有些甚至还集成了网络克隆程序和网络管理程序,这类集多种功能于一身的保护卡已经成为当今的主流产品。

虽然生产保护卡的厂商很多,但他们采用的基本都是"假写"原理:计算机加电后,首先进行 BIOS 自检和硬件初始化,然后加载保护卡芯片中的程序,最后才是读取硬盘中的主引导记录和启动操作系统,在操作系统启动之前计算机已经处于保护程序的监控之中。在首次启用保护功能之前,保护卡需对硬盘中现有的数据进行扫描,并将标志信息压缩存贮在虚拟硬盘(硬盘冗余区或者是 Flash ROM 芯片)中。保护以后,用户对硬盘中原有数据的修改并不会被真正地执行,保护软件将所有的修改都映射到虚拟硬盘中。计算机重新启动后,修改的内容将被从虚拟硬盘中清除,硬盘又恢复到原来的状态。

3 系统保护卡的缺陷

作为软件系统保护技术代表性产品的系统保护卡虽然有诸多的优点,但它毕竟是一种"外挂式"设备,并不被硬件和操作系统直接支持,其功能将受到一定程度的制约,甚至会与硬件系统或软件系统发生冲突,其缺陷也是比较突出的。总的来说,系统保护卡存在以下几个方面的问题。

3.1 安全性问题

系统保护卡发挥作用的前提条件是保护卡芯片中的程序必须先于操作系统被启动。因此,大多数保护卡(特别是集成在网卡上的保护卡)都要求将 CMOS 的"Boot First"参数设置为"LAN",强制计算机首先从 BOOTROM 芯片启动,如果将此参数修改,保护卡可能会失效。即使用密码保护 CMOS,用户也可以用两条端口指令轻松地将密码清除,有些版本的 BIOS 甚至还支持禁用网卡,使得这类集成于网卡上的保护卡在故意修改 CMOS 参数后根本无法正常使用。虽然目前大多数保护卡都有自动恢复 CMOS 功能,但如果保护程序未启动,这项功能同样会失效。

要解决这个问题必须取得计算机硬件生产厂商的支持,我们可以设想在 BIOS 自检程序中(而不是保护卡芯片中)加入 CMOS 参数的比较和自动恢复功能,让最

底层的程序来完成这项工作，只有这样才能从根本上解决因 COMS 参数被修改而造成的保护卡失效问题。

3.2 兼容性问题

首先是硬件兼容性问题。为了降低硬件成本，越来越多的计算机主板采用了非 Intel 类的芯片组（如 VIA、SIS 等），并且在操作系统中安装了针对这类芯片组的 IDE 专用驱动程序，这些驱动程序一般都未使用 Windows 建议的统一扩展接口规范，保护卡无法自动识别这类接口，在工作过程中往往会出现冲突，使整个计算机系统只能强制工作在 16 位模式下，降低了系统性能[5]。此外，保护卡一般都不能保护连接在 IDE2 上的硬盘。

其次是对操作系统和文件系统兼容问题。保护卡在使用 FAT16、FAT32 文件格式的 Windows98 中一般都能正常工作，但在使用 NTFS、EXT2 等文件格式的其他操作系统中运行效果不太理想，有时会出现文件存取错误甚至保护失效等问题。此外，保护卡还可能与某些应用程序发生冲突，特别是那些不使用操作系统提供的标准接口而直接与硬件打交道的程序。

以上问题可以通过完善保护卡芯片中的程序来解决。

3.3 其他问题

保护卡在多个方面对计算机产生了不利的影响：首先是占用了硬盘空间，一些生产厂商使用模糊的广告词宣称他们的产品不占用硬盘，这是不可能的。不管是使用压缩、虚拟、冗余还是其他什么技术，只要是需要临时保存的信息量大到一定程度，占用硬盘是不可避免的。当然，随着大容量硬盘的普及，这个问题是可以接受的。其次，保护卡还一定程度地降低了系统的运行速度。此外，保护卡还有诸如长时间使用后产生磁盘错误、限制某些工具软件（特别是磁盘检测工具和加密软件）的使用等问题。以上问题在不改变保护卡工作原理的前提下是难以克服的。

4 对软件系统保护及恢复技术的展望

过去，国际上很多知名的计算机生产厂商对软件系统的保护和恢复技术都没有给予足够的重视，研究这一技术的主要是一些小型配套设备生产商，由于得不到硬件层面的直接支持，这一技术始终局限在“外挂”、“补丁”的范畴。随着教育行业和一些大型公用计算机实验室计算机需求量的迅猛增长，这个问题已经引起了他们的重视。从目前的情况分析，对计算机软件系统保护及恢复技术的研究将主要向以下两个方向发展。

1）增加计算机硬件对保护功能的支持程度。联想集团、方正科技已经开始授权一些保护卡生产企业，针对其产品的特点专门生产特制的保护卡，这只是一个开端。今后，完全可以把保护卡作为一个标准配置集成在主板上。我们可以作如下的技术设想：在 BIOS 中加入软件系统保护程序，使保护功能在计算机硬件检测时就启动；将 CMOS 一分为二，一个用于存储允许操作系统修改的参数（如时间等），一个用于存储不允许操作系统修改的参数，防止软件对保护功能的破坏；在主板上增加一块专门存储硬盘中文件压缩标志信息的大容量快闪芯片等等，要改进保护卡的性能有很多思路。当然，必须在硬件厂商的支持下使用统一的标准。

2）采用主机/终端机系统（Host/Terminal system），即使用一台高性能的主机通过网络连接多台哑终端，终端只包括输入输出和通讯设备，所有的运算和存储都在主机中进行。在 20 世纪 80 年代盛极一时的 VAX 就属于这种类型。由于主机采用了分时操作系统，终端对主机的所有访问都受权限的控制，因此有很高的安全性。但由于受主机运行速度、存储容量、网络带宽等因素的制约，这种类型计算机系统的发展一度停滞不前。现在，计算机硬件性能和网络技术有了很大的提高，制约主机性能的因素都可以克服，重新发展主机/终端机方式的计算机系统是完全可能的。事实上，IBM 等几家公司正着手开发这方面的产品，他们计划将多处理器系统、大容量磁盘阵列、多端口高带宽的通讯系统等新技术应用到新一代的主机上。主机在保障软件系统安全的同时，其性能也大大地提高，它甚至可以为不同的终端用户提供不同的操作系统[6]。这套系统完全可以从根本上解决本文所讨论的公用机房软件系统安全性问题。

参考文献：

[1] 刘荫铭．计算机安全技术[M]．北京：清华大学出版社，2000.
[2] 方刚．计算机机房管理[M]．北京：清华大学出版，2001.
[3] 冯登国．信息安全[M]．北京：国防工业出版社，2000.
[4] 卫恒耀．硬盘数据灾难的恢复[A]．第五界全国计算机应用联合学术论文集[C]．北京：电子工业出版社，1999.364－368.
[5] 李国民．Windows 2000 系统管理员指南[M]．北京：人民邮电出版社，2000.
[6] 张曜．加密解密与网络安全技术[M]．北京：冶金工业出版社，2002.

（下转第 127 页）

[4] 吴丽娜,吴健平.校园房屋管理地理信息系统的设计与实现[J].集美大学学报(自然科学版),2001,6(1):34-38.
[5] 耿安朝.地理信息系统在环境科学领域的开发和应用[J].苏州城建环保学院学报,2000,13(1):17-22.
[6] 朱振卿,朱重宁.汉江流域水污染防治规划 GIS 系统[J].环境科学和技术,2001,96(4):43-46.
[7] 杨华.重庆市国土资源与环境信息系统[D].重庆:重庆师范学院,2000.
[8] 禹雪中,苏德慧等.水环境功能区管理信息系统研究和开发[J].环境科学研究,2000,13(6):49-51.
[9] 徐敬海,李明峰.万维网地理信息系统(WebGIS)的研究[J].江苏测绘,2001,24(3):9-12.

Solid Waste Management Information System Based on GIS in Chongqing

LIN Jian-wei, WANG Li-ao, YUAN Hui, LIU Yuan-yuan, HUANG Beng-sheng
(College of Resource & Environmental Science, Chongqing University, Chongqing 400044, China)

Abstract: The large quantity of MSW (municipal solid waste) and ISW (industrial sold waste) piled up in Chongqing has been threatening ecological environment and water resource. Efficient management is the important guarantee of disposing solid waste. This paper describes the data system of Management Information System of the Solid Waste in Chongqing based on the GIS, construction of information database, overall structure, main functions, etc. Integrating related solid waste technology with computer and geographical system, it can provide the reliable, scientific and convenient management and decision-making support of solid waste in Chongqing. The information system, developed by means of Geographical Information System (GIS) on the basis of a great deal of data and graphs of solid waste of Chongqing, includes six sub-systems as follows: data input sub-system; data query sub-system; database management and maintenance sub-system; database of modal management sub-system; application and output sub-system; system management. This system provides friendly and easy operational interface, and plays a significant role in the disposal and management of solid waste in Chongqing.
Key words: GIS; Solid waste; Management

(责任编辑　姚　飞)

(上接第 123 页)

Software System Protection & Recovery Technology

YAO Yu-chun, LI Jie
(College of Polytechnic, Chongqing University, Chongqing 400030, China)

Abstract: In order to solve the problem of software system protection and recovery in large computer laboratory, this paper analyses the current state of software system protection & recovery technology and it's defects in safety and stability. The reason causing these problems are discussed. Some solution plans are suggested. The authors hold that there have two way to solve these problems completely, one is strengthening the support from hardware, particularly strengthening the support to recover card directly from BIOS, another is developing new Host/Terminal computer system, protecting software system by ARC.
Key words: computer; software system protection; computer system security; recover card

(责任编辑　张　苹)