软磁盘加密/解密技术的研究

刘惠珍 张 民 陈建中
(北京工业大学计算机学院，北京，100022)

摘 要 简述了磁盘加密解密的主要方法，重点介绍了无缝锁加密技术和特殊常驻程序调用等解密技术原理及实现过程.

关键词 无缝锁，常驻程序，跟踪，键盘
分类号 TP 309

0 引言

磁盘是存储和交换信息的主要工具之一，随着各种计算机成果和应用软件的涌现，人们为了从经济上保护自己的权益，要求存放的信息不会被复制，于是就提出了存储介质信息防止非授权复制的问题，它已成为计算机安全保密技术中的一个重要组成部分.

磁盘加密解密技术主要有 3 方面，即反拷贝、反跟踪和密文技术，数据文件加密可以通过磁盘结构加密技术进行. 我们首先研究了无缝锁加密和伪随机数加密技术，并深入研究了特殊的常驻程序调用和中断服务程序及反跟踪技术，完成了对非标准格式化软磁盘在结构上的 3 种变化(非法磁道和附加磁道，非法扇区，错误的 CRC 校验)进行测试、分析和恢复破解的工具.

1 磁盘加密解密技术方法[1~4]

1.1 常见的磁盘保护方式

1) 更改 ID 值;
2) 多重扇区;
3) 加长磁道;
4) 空白磁道;
5) 附加磁道;
6) 错误的 CRC 校验码;
7) 激光保护;
8) 弱磁扇区;
9) 改写 BIOS;

收稿日期:1998—03—18

10) 无保护(即公用软件和地方许可证)；

11) 硬件保护.

目前硬加密一般可分为采用扩展卡和采用端口(串行口或并行口)加密两种方法．软件加密狗是一种硬件电路，它可以保存用户的有用数据供软件在运行过程中检测，也可以在软件运行过程中进行动态读存取写.

1.2 常见的破解技巧

1.2.1 利用 DOS 命令执行拷贝

这是用 DOS 的 copy 或 diskcopy 命令来拷贝原版磁片，或是利用 PC Tools 相关之功能来完成，只能拷贝毫无保护的程序.

1.2.2 利用拷贝程序执行拷贝

市面上有许多拷贝软件，例如：Locksmith, COPYWRIT, COPY II PC, DISKMACHAMIC 等，这些都是用来对付一些具有保护的磁盘．这些程序对于一些保护不甚严密之磁盘均可复制，但用此类拷贝软件拷贝后之程序在运行时仍需在软盘驱动器中插入一片 key disk(即"钥匙盘)才可正常执行．因此，这种方法称不上真正的破解技术.

1.2.3 用拷贝卡或拷贝机执行拷贝

这种方法几乎能顺利拷贝所有程序，只有少数几种特殊保护方式(例如激光保护磁盘等)无法拷贝．但由于价格昂贵，一般人并不采用此法.

1.2.4 用前人之经验来修改程序

市面上有一些书籍说明如何破解磁盘保护，但一般只告诉读者对一些特定的程序以特定的手法来加以破解．例如：书中常以一些 GAME 作为例子，教读者用 PC Tools 去寻一段机器码，然后修改为某些值，即可破解.

1.2.5 用动态跟踪工具来跟踪程序

通常采用反汇编跟踪工具来分析程序的方法，找出嵌入被保护软件中的识别程序，然后实施解密．常用的软件动态跟踪工具有 Debug 程序等.

2 磁盘加密解密的主要技术与过程分析

2.1 无缝锁加密技术[2, 5, 6, 7]

本系统的加密技术应用了上述的多种方法，如更改 ID 值，非法多重扇区，非法附加磁道，错误 CRC 校验码等，我们不仅将它们有机地揉和在一起，而且还加进了一种性能非常可靠的技术——无缝锁技术.

一条磁道可分为引导部分、扇区部分、结尾部分，而结尾部分作为整个磁道的缓冲部分，在 format 时全部以 4EH 填入，其范围为最后一扇区结束后一直到驱动器检测到索引孔为止．由于磁道是圆的，故在作 format 时一定会有头尾相接的地方，我们称其为接缝．实际上，由于驱动器在存放数据时要经过调制 (modulation)，驱动器的马达运转并非如电子仪器那样精确．由于转速不相同等原因，使得每次格式化产生的接缝处不同，甚至在同一台驱动器上作 format 时，其接缝也不相同．这样我们就可以开发一种程序来检查此接缝即可判断磁盘是否为"原版"．这种保护方法称为"无缝锁"技术、要进行"无缝锁"的保护，

大致可分为以下 3 个阶段.

2.1.1 格式化阶段

此阶段主要为选定 key disk 中的特定磁道来作特殊格式化. 这里我们使用了附加磁道 28H(1.2MB 存储量以上的磁盘选用了 50H 道), 格式化时以"无缝锁"的程序来进行, 也就是说, 在指定 C、H、R、N 之参数时, 设法让保护程序码可以读到此特殊磁道的首尾相接片, 为此我们将 N 值设为 6(经过反复实验与分析, 最终确定对 1.2MB 存储量以上的磁盘应将 N 值设为 7). 在设定特殊参数之前, 先将原来的磁盘参数 (disk parameter)保存起来, 特殊格式化之后, 再将参数还原, 这样就不致于使以后的驱动器存取出现问题.

2.1.2 检查阶段

在进行特殊格式化之后可能在磁盘的首尾相接(即接缝)处并不很稳定, 这时就该重新再格式化一次, 以确保所作的保护程序码在检查此接缝时, 能正确地读出接缝值. 为实现这一目的, 本保护程序设定了一个大循环, 它的循环体是进行一次读取及比较数据, 共执行 100 次, 若每次所读到的数据均相同, 即代表稳定, 若有 1 次或 1 次以上不相同, 就代表不稳定, 需重新格式化. 在每次读取时又给定 3 次机会, 看是否能正确读出接缝数据以及 CRC 是否为我们设定的错误状态. 若能读出就接着进行检查及比较, 如果每次读出的接缝数据均相同, 则重复多试若干次, 以确保其接缝稳定.

2.1.3 合并阶段

设计保护程序的目的是避免修改被保护软件的原始程序, 而直接将一些磁盘检查码加到被保护的软件的执行文件中. DOS 的可执行文件共有两种形式, 一种是.COM 文件, 另一种是.EXE 文件. COM 文件的结构非常简单, 所有文件的内容就是真正的机器码, 不需作任何转换. EXE 文件较为复杂, 除了程序本身的机器码外, 还包含了一堆重要的信息, 它被安置在文件的最开头部分, 我们称其为文件头数据. 这些文件头数据会影响程序的载入及程序的进入点, 并会对一些特定的地址或变量作稍许的更改. 当我们要把额外的程序码附加到 EXE 文件时, 必须要对其文件头数据进行修正, 否则在执行时很可能会出现异常.

具体说来, 合并阶段的主要工作如下: 将保护程序码与被保护程序的执行文件相合并, 但一开始的程序进入点改为此保护程序. 经过处理(即"指纹"识别等工作)之后再把控制权转移至被保护的程序上.

2.2 BIOS 中断服务程序[6~8]

一般而言, PC 的中断服务程序大致可分为两类, 第一类为高层次的 DOS 中断, 第二类为低层次的 BIOS 中断. 一般应用中, 都强调尽量使用高层次的中断服务程序. 由于磁盘的保护及破解本身就是不合法的行为, 故在作保护和破解的过程中无法以调用 DOS 中断服务程序来达到目的. 想要做到保护及破解, 就必须从低层次的 I/O着手. 例如改写 BIOS, 由程序本身直接送出控制信号, 虽然这是一种最强悍的保护及破解方式, 但这样做代价太大. 因此, 既不可使用层次过高的 DOS 中断服务程序, 也不可使用层次过低的改写 DIOS 方式, 那么, 最佳的选择即为 BIOS 中断服务程序.

可以说, BIOS 中断服务程序是位于 DOS 与硬件设备间的一个桥梁, 调用此程序既不用担心系统的相容性, 亦不受 DOS 的约束. 目前的磁盘保护技术, 大致均使用了 BIOS 中断服务程序. 本系统所提供的保护方法即利用了 INT 13H, INT 1EH, INT 40H, INT

60H等，其中由INT 13H及INT 1EH等BIOS中断服务程序来控制驱动器的运行，可以说是磁盘保护及破解的根本核心．我们充分利用了各种BIOS中断服务程序，结合深入的DOS知识与严谨的科学实验，提供了一套加密效果可靠且使用方便的磁盘保护工具．

2.3 磁盘解密的关键技术及应用[2, 6, 7]

前面提到的多种破解技巧，有的破解面窄，有的又代价太高，而理论上，只有追踪程序是最直接且最具威力的方法．但是，这又涉及个人的功力问题，而且追踪程序终究要花上大量宝贵的精力和时间，结果也不尽人意．因此为用户提供解密工具是目前较好的一种方法．当前国内外一些公司已经研制和销售了许多用于解密的高级拷贝和分析工具，这些解密工具大体上可分为3类：①自动型解密工具．它可对加密软盘进行解密分析，依据分析结果自动复制出与源盘相同的加密标记，COPYWRIT、COPY II PC都属于此类工具，但它的适用不够广泛，对于复杂的加密技术显得无能为力，如对无缝锁、激光加密都束手无策；②专用型解密工具．这是用来拷贝特定的加密软件的工具，它与被拷贝对象一一对应．这种解密工具是破译者对某一类加密软件进行详细剖析以后，针对该加密软件编制的专用拷贝工具．但是这种加密软件存在着时效问题，而且，专用型解密软件既然是针对某一类加密软件的，那么它的适用广泛性当然也不会太强；③分析型解密工具．由于它的功能优异，因此加密者和解密者双方都非常关注这种解密工具的发展．解密者利用分析型解密工具可以直接观察和分析加密软盘的加密标记，为用户提供了方便、直观和详细的分析环境．

本系统所提供的解密工具基本属于分析型解密工具类，但它相对于一般的分析型解密工具，又具有界面良好，易学易用等优点．它除了应用常见的破解技巧之外，还提供了一种更好的方法，这就是“利用常驻程序破解软盘的保护技术”．

常驻程序(Terminate and Stay Resident Program, 简称TSR)是一种特殊的类似中断服务程序的程序，当执行一段初始化过程后常驻程序便结束了，但它并不会从存储器中离开，而是留在RAM中，受到操作系统的保护，不会被其它的程序所覆盖．因此，它会占用存储器空间．通常，在常驻程序初始化时，它会更改一些中断向量表的入口，使其指向常驻程序．因此，常驻程序会因某些中断而被触发而去执行某些特定功能．这样它就变成了一个新的中断服务程序，成为操作系统的一部分．若我们能善用常驻程序，则它不仅仅可以随时为我们服务，还可以监督系统中的重要中断．

要达到常驻的功能有两条途径：一是使用INT 27H来结束程序，另一则是使用INT 21H第31H之功能调用来结束．而要使常驻程序不成为“尸体”，就必须使它以某个中段来角发，并考虑是取代旧有的中断服务程序，还是要与其串接．而且一个优良的常驻程序应是可以常驻，还可以被解除常驻的．要将一个常驻程序解除，必须作好3件事：①与常驻程序通连；②还原中断向量；③释放存储器．要与常驻程序连通并不困难，只须将常驻程序串接至一特殊的中断向量，等到要与常驻程序连通时便触发该中断，如此便可与常驻程序相连通．在DOS管理下，60H～67H并未使用，它们专供用户使用，本系统采用了第60H中断作为连通的管道．要还原中断向量，利用25H及35H调用功能即可．唯独释放存储器这部分必须对DOS的管理存储器及其分配原理进行相当深入的剖析才可完成．我们知道，每一个程序(Process)被载入都有2块存储器：环境区及程序区．在程序未用的自由空间，DOS把它并在程序之中．因此在解除常驻程序时，一定要将这2块存储器释放出来．

常驻程序固然能使我们做许多别的程序办不到的事情，但有一个问题需要慎重考虑，否则将导致死机甚至更糟的情形，那就是DOS的不可重入问题．在DOS功能调用中，有一项服务未被公布，即是AH＝34H的调用．执行此功能调用之后，会由ES及BX返回值，而此ES：BX所指向之byte称之为in-dos．每当INT 21H运行时，其值为1，而未运行时，其值为0．因此，我们可在常驻程序初始化时，用AH＝34H执行DOS功能调用，以得到in-dos的地址，并将其保存，而当程序常驻之后，若要使用DOS的功能调用，可先检查此in-dos以确定INT 21H是否正在运行，若是，则不要使用，如此即可避免DOS reentrant之问题．

综上所述，常驻程序使我们能做很多系统不允许或未提供的功能，若我们善用它，它将成为最佳的守门员，可以各种重要的中断上把守，使一些具有保护能力的磁盘无法作怪．本系统利用常驻程序来破解保护可分为两阶段，第一个阶段为"破解"阶段，第二个阶段为"使用"阶段．只有在"破解"的阶段必须使用key disk，而一旦破解之后，就不再需要key disk了．而且，破解后所得的数据均为文件的形态，利用DOS的COPY命令就可拷贝．因此，其保护功能就彻底地被破解了．

2.4 磁盘结构分析与磁盘信息加密解密技术的研究[9, 10]

磁盘扇区是磁盘读写的最小单位，任何文件及磁盘的专用数据都是按扇区分布在磁盘上，分析加密磁盘需要避开DOS所提供的文件读写途径而直接对磁盘指定扇区进行操作．本系统提供了一个扇区读写工具和磁盘分析工具．这两个工具不仅能"读"到并分析出用非法磁道、非法扇区、错误CRC码等方法加密的磁盘，而且对用"无缝锁"方法加密的磁盘还能准确地显示出接缝的位置及接缝值．

一般说来，磁盘防拷贝只是防止磁盘上的某一部分关键的信息或某些特殊的标志被复制．实际上，有时不可能也没有必要做到整块磁盘的信息防拷贝．这就需要防止某些文件被窃取，防止使用某些工具软件直接读取磁盘上的信息．要做到这一点，可以将可执行文件看成数据明文，通过数据加密的各种方法产生密文，存回原文件，使文件按密文的形式存储．使用时先通过解密还原成明文再执行．本系统采用了伪随机数加密法，此法基于相同的初值能得到相同的随机数序列这一事实．其基本思想是：通过某种约定获得一串不重复且是无规律的数，用它来使文件中的字节发生变化，以此实现加密，再用同样的数串使文件中的字节值得到恢复来实现解密．

3 软磁盘加密解密功能和检测[6, 7]

本系统在PC机的DOS下BOYWINDOWS作为开发和使用环境，用C+ +和汇编语言混合编程，系统界面完全模拟WINDOWS的风格，画面美观大方，操作简单易学，容错能力强，还有丰富的联机帮助，即使是非计算机专业的人士也完全能在本系统友好的提示下完成加密解密的工作．本系统开发完成后即进行了大量的功能检测与分析工作，在检测工作中，尤其对本系统提供的软磁盘指纹加密功能和破解功能进行了反复的实验与测试，证明利用本系统提供的软磁盘指纹加密程序制作的钥匙盘性能稳定，效果良好，而且对低密、高密、5寸盘、3寸盘等各种类型的磁盘均适用．而利用本系统提供的解密程序不仅能成功

地破解本系统自身的加密手段，而且对激光保护、针孔保护、弱磁扇区保护以及一些游戏保护等加密方法均能破解，真正实现了既具有强大的破解威力，又方便实用的目标.

4 结束语[9]

磁盘结构的加密解密技术涉及数论、信息论、概率论、电磁学理论、计算复杂性理论等，是一门综合的学科和技术．我们的研究工作还需进一步加深理论，扩充方法，提高水平.

加密解密是矛盾的两个方面，无论是保护措施还是破解方法，都值得计算机专家及管理人员深入研究．而且保护与破解本来就没有永远的赢家，保护再严密的系统终究有其脆弱之处．同样地，再强的攻击手段或破解程序也终究会有更强的保护措施来防止，就此展开的"战争"永不停息.

参 考 文 献

1 王化文．计算机安全保密原理与技术．北京：科学技术出版社，1990

2 软件加密与解密技术及其应用实例专辑．北京：中科院成都计算机应用研究所，1991

3 R A Elbra. Computer Security Handbook. Amervca: NCC Blackwell, 1993

4 K Bhanker. Computer Security Threats & Countermeasures. Amervca: NCC Blackwell, 1992

5 沈永耀，陶铮正．磁盘文件管理与加密原理．北京：中科院希望高级电脑技术公司，1990

6 尹彦芝．C语言常用算法与子程序．北京：清华大学出版社，1991

7 施小龙，葛玉宝．BORLAND C+ +3.1 库函数快速参考．北京：学苑出版社，1992

8 PC Security Issues. Computer and Security. August, 1993. 1～7

9 丁红卫．软件加密技术．北京：北京希望电脑公司，1994

10 林宣雄，谭晓生．磁盘加密与解密实用技术．西安：西安交通大学出版社，1990

Research on the Technical Encryption and Decryption of Disks

Liu Huizhen Zhang Min Chen Jianzhong

(Computer Institute, Beijing Polytechnic University, Beijing, 100022)

Abstract The main method to encrypt and decrypt the floppy disk is dicussed. The theory and implementation of "Checking Slot" and "Terminate and Stay Resident Program" are introduced in particular.

Keywords checking slot, trace, terminate and stay resident program, key disk