IBM PC 微型计算机

软件加密/解密反跟踪实用技术

杨 迈 李 卫 郑自修

西安电子科技大学出版社

IBM PC 微型计算机

软件加密/解密及反跟踪实用技术

杨 迈 李 卫 郑自修 编著

西安电子科技大学出版社

1993

(陕) 新登字 010 号

内 容 简 介

本书全面介绍了目前国内外在 IBM PC 系列微型计算机上对磁盘软件进行加密/解密的实用方法，并介绍了反动态跟踪原理和一些典型的方法，其中有一些是作者新近研究出来的新方法，目前的破解工具对它们无效。考虑到单板机的应用前景日益广阔，本书辟出一章，专讲单板机的加密技术和反动态跟踪技术。

读者根据自己所编软件的特点，利用本书提供的方法和程序实例，很容易对自己开发的软件产品实施加密保护。

本书适合计算机软硬件开发人员、从事软件加密/解密的工程技术人员及对此内容感兴趣的各类教师和学生阅读参考，也可用作有关培训班的教材。

IBM PC 微型计算机
软件加密/解密及反跟踪实用技术
杨 迈 李 卫 郑自修 编著
责任编辑 徐德源

西安电子科技大学出版社出版发行
陕西省军区西安长城印刷分厂印刷
新华书店经销
开本 787×1 092 1/16 印张 17 8/16 字数 410 千字
1991 年 12 月第 1 版 1993 年 4 月第 2 次印刷 印数 5 001—15 000

ISBN7—5606—0160—X/TP・0060 定价：12.00 元

序

计算机软件产权的保护问题一直是计算机技术领域内非常受到重视但又极难解决的一个问题。软件生产者和经销者为了保护自己的权益，对其出售的产品进行加密以防止无偿复制和无限制的无偿扩散。但是多年来的事实证明，任一种加密措施出现之后，随之就会出现相应的解密方法。加密与解密之争日趋激烈，难解难分。在这种形势下，愈来愈多的人希望对已有的加密技术和其相应的解密方法有一些深入的了解以便借鉴以往的经验教训研究出更新更好的加密技术，从而使软件的产权保护措施从技术的角度来说达到一个更加有效的地步。

杨迈等同志多年来利用业余时间对此问题进行了比较深入广泛的探索，收集了比较丰富的资料并加以整理归纳，比较系统且详细地介绍了已收集到的加密技术和解密方法。同时，作者还根据自己探索的心得对“电磁软盘加密技术”进行了改进(见§5.4)，并自行设计了一些加密方法，其中有代表性的如：磁道接缝软指纹加密技术(见§5.8)和第九章所介绍的“基于内存保护的加密系统”，这些方法均经过实践考查，证明是比较有效的。作者的目的在于与同行们互相交流、切磋，以期为软件加密技术的提高作出一些有益的工作。全书叙述清晰，注重实用，并附了一些较有实用价值的实例。读者可以通过本书对加密和解密的一些技术和方法得到较细致的了解并从中领会出一些原理和技巧，为进一步研究出新的更有效的加密技术从思路上得到一点启发。

我相信，本书的出版发行将能够对我国计算机软件的加密水平的提高有所帮助。

西安交通大学　**胡正家教授**

1991. 11. 15

前　言

随着计算机的广泛应用和日益普及，在当今世界范围内，计算机已经越来越深入到人们的日常生产、生活、娱乐、等各个领域中。做为发挥计算机功能的软件，无论在质量上还是在数量上都迅猛地发展着。软件产品是一种知识密集的特殊产品，生产一个软件产品需要大量的人力和物力，生产难度大，成本高，周期快。但是，软件产品的复制却相当容易。这就导致了非法复制、盗窃软件之风的泛滥。在这种形势下，软件的研制者和销售商为了保护自己的权益不被侵犯，除了法律手段外，还须依靠技术手段来实现。目前，软件加密技术蓬勃兴起，不管采用那种软件加密手段，其目的都是为了保护软件的安全，不使之被非法拷贝、篡改。从有效程度角度来看，没有绝对能保证软件安全无虞的方法，而只能保证其在一定的时间内不被破解。因为破解一个软件也是一件很费力的工作，而且需要有较高的技术水平和丰富的实践经验。如果破解软件本身的代价已超过购买软件的代价，那么实际上就已经达到了软件加密的效果。

其实，软件加密的指导思想是在软件系统原盘上产生这样一种信息，这种信息既是软件系统中各可执行程序在运行中必须引用的，又是各种文件复制命令或软盘复制软件所无法正确复制的。于是，该软件系统的运行完全依赖于售给用户的原系统软件软盘。

软件加密的目的在于保护存放在磁盘上的软件不会被非法复制，也就是说，对于磁盘有较高的存取能力，即能够在磁盘上写入和读出拷贝软件无法正确复制的信息的能力。一种好的加密方法往往能在很长一段时间里防止软件的非法复制，从而较好地保护了软件开发者与销售者的合法权益和经济效益。软件加密技术通常可分为硬加密技术和软加密技术两类。

硬加密技术的指导思想是：在磁盘(通常是软盘)上作某种特殊的标记，在复制这种磁盘时，其上的特殊标记是拷贝软件不易识别和复制的，从而使拷贝所得的复制磁盘上的软件无法运行。硬加密技术是软件保护技术的核心基础，没有性能良好的硬加密技术，就无法抗衡高级解密拷贝程序的复制，从而无法保护自己的软件不被非法复制。根据这种特殊标记的性质又可分为硬标记和软标记两类。

硬加密技术可以防止软件被非法复制，但是，若加密处理过的软盘不做解密处理的话，其加密硬标记利用常规的方法也是读不出来的。换句话说，不经过识别程序进行解密处理，加密处理过的软盘也不能正常运行。然而，识别程序本身就是一个最忠实的“告密者”，它将把你采取的加密措施毫不保留地告诉破译者。破译者若知道了你采取的加密措施，就可以很快地破译你的加密软盘。

本书的作者一直从事计算机方面的研究开发工作，对于 IBM PC 微型计算机上软件的加密，具有丰富的经验和独到的方法。在本书中，作者就 IBM PC 微型计算机上磁盘软件加密/解密的基本原理和方法进行了介绍，并详细介绍了作者在实际应用中较为有效的几种加密和反动态跟踪的方法。这些方法各有其特点。作者希望通过这本书，能与广大计算机同行共同交流 IBM PC 微型计算机加密及反动态跟踪的经验和方法，为研制更加有效的加密技术而共同努力，从而从技术上防止软件被非法复制，促进软件版权法的实施。

中华人民共和国国家教委工科计算机基础课程教学指导委员会主任委员、机电部计算机教材委员会副主任委员、西安交通大学计算机科学与工程系胡正家教授在百忙中审阅了本书，并提出了许多宝贵意见，我们在此表示衷心的感谢。本书的编写还得到张书凯、徐峰、刘坚、史晴旻等同志的大力支持与帮助，我们在此一并致谢。由于编者水平和经验有限，缺点和错误在所难免，敬请各位专家同行批评指正。

编著者

一九九一年十月于西安交通大学

◀ 目　录 ▶

第一部分　加密/解密所需了解的磁盘技术细节

第二部分 加密/解密及反跟踪实用技术

第一部分

加密/解密所需了解的磁盘技术细节

第一章 绪 论

§1.1 计算机安全与软件权益

所谓计算机安全，是指对计算机系统的硬件、软件、数据等加以严密的保护，使之不因偶然的和/或恶意的原因而遭到破坏、更改、泄漏，保证计算机系统的正常运行。计算机安全主要包括以下几个方面的内容：

1. 实体安全(Physical Security)

实体安全是指计算机系统的全部硬件及计算机辅属设备的安全。包括计算机房地理环境的选择、建筑结构、布局、各种防火、防盗措施及手段等。

2. 软件安全(Software Security)

软件安全是指软件的防复制、防篡改、防非法执行等。软件安全是计算机安全学目前研究得最为薄弱的环节。软件的安全性如何证明，如何测试，运行中的软件如何保证是未被篡改过的，一但篡改，又如何能立即被发现，如何有效地防止复制等问题，都是软件安全研究尚需急待解决的问题。

3. 数据安全(Data Security)

数据安全是指计算机中的数据不被非法读出、更改、删除等。它是计算机安全的关键。几乎所有的计算机犯罪，都是以对数据的非法操作而达到目的的。由于在计算机内部，软件和数据的存储方式基本是一样的，所以软件安全与数据安全在技术上有着许多共同之处。

4. 运行安全(Operating Security)

运行安全主要是指计算机系统在投入运行之后，工作人员对机器的使用、维护等安全措施。运行安全主要取决于工作人员的责任心、维护能力和健全合理的运行管理制度等。

对于计算机安全的研究，已成为当前计算机科学的一个十分重要的课题。正像许多计算机专家指出的一样：计算机系统如果没有确保其安全的体系与机制，将是一个非常危险的系统。计算机安全已作为一门边沿学科而逐渐形成。计算机安全学研究的内容包括：计算机安全技术、计算机安全管理与保卫、计算机产品安全、计算机犯罪与侦察、计算机安全法律、计算机安全监察、计算机安全理论与政策等。

软件安全的另一方面，是确保软件研制者的权益免受侵害。一个软件的开发，有时往往要花费巨资，并付出若干人年的艰辛劳动，软件本身也是研制者的智慧与心血的结晶。如果软件可以轻而易举地被别人复制或仿制，研制者不能得到应有的报酬，这将是对软件研

制者合法权益的严重损害，也将大大地阻碍软件产品与软件市场的发展，进而也极大地限制了计算机的应用与发展。对于软件权益的保护，既要依赖于国家的立法保障，软件本身也要具有防复制，防跟踪等自我保护措施，这也是十分必要的技术保护措施。目前，尽管世界各国大都制订了软件保护法，但由于这一问题所涉及的范围较广，监察困难，所以仅靠立法的收效是有限的。因此开展这方面的研究，对于保障软件研制者的权益，加速软件技术的发展，提高计算机的应用水平，都有着重要的意义。

§1.2 计算机软件的自我保护

1.2.1 软件保护的基本任务

利用软件技术对程序和数据实行安全保护，其主要任务是：

1. 对数据保护

(1) 防止对数据的非法访问。

(2) 防止对数据的非法修改。

(3) 防止对数据的非法截获。

(4) 防止由于误操作对数据的破坏。

这里所谓的“非法”，是指未经授权的不合法操作。对数据的保护，是保证计算机安全、防止计算机犯罪和防止盗窃机密信息的关键。

2. 对程序保护

(1) 防止对程序的非法执行。

(2) 防止对程序的非法修改。

(3) 防止对程序的非法拷贝。

(4) 防止对程序的动态跟踪。

防止对程序的非法执行和修改，也是出于安全防范的目的。防止对程序的非法复制和动态跟踪，目的在于保护软件研制者的合法权益。

对程序和数据是否有必要加以保护，实行多么严密的保护，应取决于程序和数据的重要性。因为不管采用何种方式的保护，都要增加计算机的时空开销并以人力、财力为代价。保护的严密程度，与采用的保护措施、技术等有关，但一般也与付出的代价成正比，因此应权衡利弊。权衡的标准是，可能遭受的损失与保护所需花费的比。

1.2.2 软件保护的基本方法

利用软件手段实现对软件(包括程序和数据等)的保护，其方法是多种多样的，但每一方法都有一定的适应范围和局限性。所以在一个系统中往往需要采用多种保护手段，实行层层把关。由于系统的不同，如网络系统，分布系统等共享性很强，并要考虑对通信提供保护等情况，故问题将会变得更为复杂。

下面介绍几种常用的软件保护方法。

一、数据加密

将数据按照一定的密码算法加工成密文，使不掌握密钥的人无法识别，以达到对数据

保密的目的。数据加密尤其会使企图截获信息的攻击者难以真正了解到实际内容。

二、身份鉴别

身份鉴别的基本方法是由计算机识别要使用计算机的人是否为合法用户。如果是合法用户，系统将允许他进行操作，否则予以拒绝、使其无法进入系统而不能对系统做任何操作。由于这种方法可以将非法用户拒之门外，所以它对程序和数据都可提供保护。

身份鉴别的手段是多样的，现就常用的几种介绍如下。

1. 物理特征鉴别

物理特征鉴别由计算机系统识别用户个人的某些特征，像指纹、声波、相貌、签名笔迹等具有唯一性特征的信息。这种方法在理论上是最可靠的，但在实际中还存在一定的问题，如代价较高，技术也不甚成熟，且有些物理特征还会发生变化等，所以一般系统很难采用。

2. 特殊证件鉴别

特殊证件鉴别将表示用户身份的信息记录在卡片上，卡片上的信息应不能由人直接读出或写入，但可由计算机读出和写入。计算机读出卡片上的信息，与原存的表示用户身份的信息作比较，以此识别是否为合法用户。这种方法在银行系统中应用很多，如金融信用卡，现金存取卡等。早先的卡多采用磁卡，以磁记录方式记入用户的身份及其他信息。这种卡的缺点是易被复制或改写。近年来出现的集成电路卡(IC 卡，或称芯片卡 Chip—Card)可克服上述缺点。IC 卡内有存储器和(或)CPU，存储器的容量远较磁卡大，读出也极为方便，由于卡内有 CPU，所以本身就可以实施多种安全控制，加之使用方便，灵活，所以目前认为是最为理想的一种卡。

3. 口令字鉴别

口令字鉴别口令字(Pass Word)识别是一种简单易行的方法，也是目前较为普遍采用的一种方法。这种方法的基本思想是给每个用户设一口令字，口令字只有计算机和用户本人知道。用户上机时，系统首先运行识别软件，要求用户回答口令，用户打入口令后，机器对这一口令进行验证(与机内原存的比较)，以此鉴别是否为合法用户。

利用口令字实现软件保护，可用于多用户终端联机、工作站入网、某一具体应用软件的运行、硬盘的使用、子目录的进入，以及数据文件的打开等多种场合。根据应用环境和要求的保密程度不同，口令字的具体实现方法也有所不同。现将几种常用的方法介绍如下。

(1) 直接核实。直接核实将约定的口令字(PW)作为常数写入程序或建一口令字文件(PF)，当用户回答口令字 PW′后，检查 PW′＝PW 或是 PW′ ∈PW。这种方法实现起来较为简便，但保密性能相对较差。因为稍有计算机知识的人可以通过系统软件在机器中直接找到 PW 或 PF。下面介绍的几种方法可克服上述缺点。

(2) 单向函数法。单向函数是指具有下述特点的函数：

①对于任意给定的自变量 X，可以很容易地求出 Y＝F(X)。

②对于所有的 Y 值，不可能求出自变量 X。

由此可见，单向函数是一种不可逆函数。将用户的口令字 PW 代入单向函数，计算求出 F(PW)并存于机器内，每当用户打入口令字 PW′ 时计算 F (PW′)，通过判断 F(PW′)＝F(PW)，就可鉴别是否为合法用户。

由于单向函数的不可逆性，破译者即使在机器内查到 F(PW)，但他却无法由 F(PW)推

算出 PW。利用单向函数加密，其保密性能显然优于直接核对法。但该方法如果用在远程终端或网络工作站上，就有可能被攻击者通过窃听手段了解到口令字 PW。下面给出两种可对付窃听的口令字识别法。

(3) 加入变量的口令字

为了对付攻击者的窃听，在口令字中加入变量，即一个口令字由口令 P 和变量 Ti(i 表示口令字使用次数)两部分组成。在打入口令字时，Ti 每次按约定的规律(如递增)变化，并对 P 和 Ti 用公开钥密码加密后再作为口令打入机器。机器对接收到的口令字 $PW'=P'+Ti'$ 利用密钥解密，再经单向函数计算后与原存口令字比较。正确的口令字 P 内容与原来相同，Ti 的值应大于 Ti－1。识别后若是合法用户，机器还将记录本次的 Ti 值。

可以看出，在口令字中加入变量 Ti 后，使得用户每次回答的口令字都不同，监听到的口令字又经过了加密处理，就使得攻击者无法知道 P 和 Ti 的明文，也无法推测出 Ti 的当前值和变化规律。同时采用了单向函数，也克服了直接核对法的弊端。

(4) 采用数据签名的口令字

该方法基于密码学中的数据签名原理。用户将变量 Ti(变化规律可同③)和签名后的 D(Ti)以及用户名 U_A(表示 A 用户)组成的口令字(Ti, D_A(Ti), U_A)打入机器，机器将验证签名得到的 $Ti'=E_{\hat{A}}(D_A(Ti))$ 与 Ti 比较，若 $Ti'=Ti>Ti-1$ 则认为是合法的 A 用户。由于签名用的密钥 D_A 是保密的，所以即使攻击者窃听到 Ti，但无法形成 D_A(Ti)。这样也同样可以对付窃听和直接核对的攻击。

利用口令字鉴别用户身份，无论采用何种口令字方式，都无法解决用户自己泄漏口令字而造成的失密问题。所以用户的责任心才是保障系统安全的关键。另一方面，许多用户都喜欢以自己的姓名或部门名称、软件名称的拼音或英文缩写作为口令，这就会使入侵者方便地猜测出口令。口令字的长度与保密性有很大的关系，猜中一个口令字的平均时间为

$$T=\frac{1}{2}C^L\cdot t$$

其中 C 表示口令中可使用的符号个数，L 是口令长度，t 是鉴别一次口令所需的时间。当然，如果在鉴别口令字的软件中设计一控制非法用户对回答口令次数的限制(如 3 次口令不对时拒绝再打入口令)，这对于防止以试凑法和猜测法攻击系统是很有帮助的。

三、访问控制

访问控制是对不同用户访问某一(些)程序和数据的权利限定。一般用在网络和多用户系统对共享文件的访问保护上。

访问控制的权限主要有以下 8 种类型：

(1) 读(R)。拥有此权利的用户，只可读取指定范围内的信息。

(2) 写(W)。允许用户在指定范围内写入和修改信息。

(3) 读、写(R,W)。具有读、写两种权利。

(4) 读、写、建(R，W，C)。除具有读的权利外，还可在指定区域建立或删除文件。

(5) 私用(PRIV)。网络中(如 3+网)，只允许该目录的拥有者访问。

(6) 执行(E)。可执行指定范围内的程序。

(7) 迁移(M)。可在指定的范围内移动信息的存放位置。例如在虚拟存储系统中移动信息的存储页面等。

(8) 存在证实(EV)。限定用户只能在指定区域内证实某种信息是否存在。

给什么用户授于何种访问权限的方案称为控制策略。控制策略的确定，应遵循的原则是“需者方知”(the need—to—know)。例如一个人事档案数据库，人事部门可拥有读、写(R、W)权利，而对上级主管领导则只应赋予读(R)权利。再比如一个学生成绩数据库，对任一授课教员，他只有权利读、写自己所任课成绩的数据项，而对其他数据项，最多只赋予他读的权利。

四、移动控制

移动控制的目的在于避免某一用户 A 把不允许另一用户 B 使用区域内的信息，移到了允许 B 使用的区域，以便不使 B 有机会非法地访问这一信息。移动控制也可以消除由于用户的误操作而移动了信息所产生的不安全因素。

五、推断控制

给用户规定访问权限后，有些信息虽然不能直接被某用户访问到，但他可以通过几次如投影等运算后再进行逻辑推理而得到。推断控制就是要防止这种情况的发生。实现逻辑推断控制，应对各数据项的属性及相互间的关系作仔细地分析，正确地限制访问数据集合的最大、最小体积，两次访问数据集合的交集体积。

六、防拷贝加密与反动态跟踪

利用软件保护技术防止对软件的非法复制与仿制，是软件开发者对自身利益的一种保护，同时也可防止某些方式的计算机犯罪。Oded Goldreich 在“软件的保护理论”一文中提出，软件的保护在于“所出售的程序是买主可以执行的，但他却不能复制或分配给其他用户”。防复制应确保不存在任何一种能生产可供执行的软件拷贝的有效方法。防分配应确保非法复制者万一成功地对软件进行了复制，但他不能在法庭上证明软件是他设计的。本书的第五、六、七、八、九章将重点介绍软件的防复制与反动态跟踪技术，这里不再讨论。

可以说不管采用什么样的软件保护技术与措施，都很难保证系统的绝对安全。采用硬、软件结合的保护方法，有时会取得更好的效果。需要强调的是，从事系统开发和使用者的职业道德、工作责任心等，也是保证系统安全的关键因素。

第二章　磁盘的组织结构及磁盘技术细节

美国 IBM 公司在 1981 年里推出了 IBM 个人计算机(即 PC 机)，并获得了巨大的成功。IBM PC 的用户越来越多，众多的软硬件开发者开始为 IBM PC 生产更多的产品。为了配合这种努力，IBM 公司提供了有关 IBM PC 机及其操作系统的技术文档。PC 引进了一个新的操作系统，即 Microsoft 磁盘操作系统(MS－DOS)或 IBM 销售的 IBM 个人计算机操作系统(PC-DOS)。本书中的 DOS 这个名词将用来代表这两个操作系统中的任一版本。DOS 被设计用于提供基本的磁盘和数据文件管理功能，也用来提供显示、打印和异步通信的有限支持。所有各种计算机，无论大小，都要有存储设备。在小型计算机前期，数据是被频繁地记录在磁带上的。然而，在磁带上处理数据必须严格按顺序进行。在小型计算机上，作为外存，磁盘基本取代了磁带。磁盘与磁带相比具有一个极其重要的优点，即它可分成能独立写入或读出的数据块。随着个人计算机 IBM/XT 的问世，另外一种存储介质硬盘流行起来。硬盘不同于前面的磁带和软盘，它是不可移动的、固定的、大容量、读写非常快的一种外部存储设备。本章着重介绍 5.25 英寸* 磁盘机的结构特点与工作原理，磁盘机的技术参数和指标，还要介绍 DOS 磁盘分区、文件分配表、文件目录表和磁盘参数表等 DOS 文件的管理机制。

§2.1　磁盘及其结构

本世纪 70 年代以来，磁盘机开始向高密度、大容量、小型化、高可靠性、低价格以及快速存取的方向迅猛发展。目前，在微型计算机中使用最多的是 5.25 英寸* 磁盘机。所有磁盘，无论软盘还是硬盘，它们的构成方式都是一样的。磁盘的表面由一系列同心圆组成，每个同心圆称为磁道。磁道沿径向分成很多扇区。一个完整的磁盘机是由磁头、盘片、控制电路及驱动部件等组成的。

2.1.1　驱动器

磁盘驱动器可分为软盘驱动器和温氏硬盘驱动器。DOS 最多可支持 26 个磁盘驱动器，这是由于 DOS 赋给每个磁盘驱动器一个英文字母的缘故。

5.25 英寸* 软盘驱动器种类繁多，其电路各异。主机通过软盘控制器实现对它的控制。大多数驱动器接口信号均相同，可以互换。尽管驱动器电路各种各样，但它们都必须实现

---

* 1 英寸＝2.54cm