Broadview®
www.broadview.com.cn

安全技术大系

第一线软件加密的卓越实践　数十年软件保护的厚积薄发

软件加密原理与应用

飞天诚信　编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

含光盘1张

安全技术大系

软件加密原理与应用

飞天诚信　编著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书不但由浅入深地讲解了软件保护技术，而且还精选并剖析了一些破解实例，并从一定的角度透视解密者的心态，在多处对照了软件保护与破解的思维方法。主要内容有：软件加密的发展历史、误区、方法，以及与特定语言相关的软件加密技术；破解技术剖析，以及常见的软件加密薄弱环节；PE 技术、实战外壳加密与反脱壳技术（附大量示例源码），并提供了作者自己编写的小工具（加壳工具 PEMaker 等）；调试技术与反调试技术（附大量示例源码）；软件加密技巧与整体方案设计；加密锁分类及其使用技巧（智能卡加密锁）。

本书是作者多年从事软件保护所积累的经验和心得，有很强的实用性，本书主要面向软件开发商、对软件加密和解密有浓厚兴趣的读者。

图书在版编目（CIP）数据

软件加密原理与应用 / 飞天诚信编著. —北京：电子工业出版社，2004.11
（安全技术大系）
ISBN 7-121-00373-2

I. 软… II. 飞… III. ①软件-加密 ②软件-密码-解密译码 IV. TP309.7

中国版本图书馆 CIP 数据核字（2004）第 095708 号

责任编辑：孙学瑛
印　　刷：北京智力达印刷有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
经　　销：各地新华书店
开　　本：787×980　1/16　印张：28.75　字数：572 千字
印　　次：2004 年 11 月第 1 次印刷
印　　数：5000 册　定价：55.00 元（含光盘 1 张）

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

前　言

随着计算机技术的不断发展，面向各应用领域或行业需求的软件不断地孕育而生。但无论哪种优秀的软件，其内部核心的技术往往是该软件的命脉，一旦被他人窃取或被非法复制，由此受到的经济损失是无法估计的。

因特网（Internet）给大家的生活和工作带来了日新月异的变化，同时也为盗版软件在网络上快速传播与流通提供了良好的媒介。因而除了如何有效地通过外在的法律手段打击盗版行为之外，深入学习软件保护技术，增强软件自身抵抗盗版流毒的免疫力也受到越来越多软件开发商的重视。但限于大多数开发商对此方面技术了解的版面性，在实施软件加密的过程中，很少有人能够像分析软件工程一样对软件加密进行系统的分析，周密地计划和设计加密方案，因而使得许多即使应用了一定软件保护技术的程序，仍然能够被解密者轻松破解。

如何避免软件保护方案设计的通病，及如何减少软件加密的薄弱环节成为广大开发商比较困惑的问题之一。并且与软件保护方面相关的专业文章也是非常“罕见”的，虽然网上能够搜索到大量的介绍破解方面的文章，但是要从这些破解的资料中总结出实用的加密心得，对于不精于破解的广大开发商来说仍是一个不小的屏障。

如果说软件保护是防盗版的疫苗，那么软件破解则应算是保护技术病原体，软件保护技术的发展与软件破解技术存在着一种特殊的关联性。本书不但在软件上进行了由浅入深的讲解，而且还精选并剖析了一些破解实例，另外还从一定的角度透视了解密者的心态，并在多处对照了软件保护与破解的思维方法，希望这些内容可以很好地帮助您结合自身产品的技术特点设计出相对完美的软件保护方案。

本书读者对象

本书是我们多年从事软件保护所积累的经验及心得，具有很强的实践性。本书主要是面向软件开发商，以及对软件加密和解密有浓厚兴趣的读者，无论是这一领域的初学者还是有着丰富经验的开发人员，都能够从本书的阅读中受益。

本书的主要内容

- 软件加密的发展历史，软件加密的误区
- 软件加密的方法，与特定语言相关的软件加密技术
- 破解技术剖析及常见的软件加密薄弱环节
- PE 技术、实战外壳加密与反脱壳技术（附大量示例源码）
- 调试技术与反调试技术（附大量示例源码）
- 软件加密技巧与整体方案设计
- 加密锁分类及其使用技巧（智能卡加密锁）

请把您的想法告诉我们

我们虽然不是专业的作家或这个技术领域的绝对权威，但我们希望通过这样一个特殊的窗口来和大家一起交流、学习。北京飞天诚信科技有限公司于 1994 年便步入了软件保护殿堂，多年从业的经历使我们深深地感到，软件保护技术的推广、资源共享远比研究令众多开发商无法自由驾驭的加密工具有效得多。软件保护不能完全靠独辟蹊径来谋求长久的发展，每种保护技术都有其存在的必然道理，虽然本书的内容无法包罗万象，但希望我们的实践经验能够启发您的思维，达到抛砖引玉的作用。本书由多名对软件保护技术有着执著热情及相关经验的飞天诚信在职员工的合力编写。当然，此书的出版更少不了电子工业出版社博文视点资讯有限公司的孙学瑛老师等人的后期工作，事实上在一本书出版的幕后有许多您无法想像的辛劳。

如果您在阅读本书时有任何心得或想法可随时与我们联系，这是对我们工作的最大支持。同时限于作者水平，书中不免有许多错误和疏漏，欢迎您批评指正。如果想了解更多计算安全方面的信息敬请光临我们的网站（http://www.FTsafe.com.cn）。

飞天诚信
2004 年 9 月

目　录

CHAPTER 1

第 1 章　软件加密综述

软件加密，在计算机领域中早已不是一个陌生的词汇。由于软件这种产品是创作者智慧的结晶，其内在的价值是无形的，相对于其外在的（复制、发行的）成本则显得非常低，而软件因其数字产品的特性又使得复制品可以和原品一模一样，所以软件加密就是在创作者被这种问题所困扰的情况下应运而生的。

时至今日，软件加密已经是一个相当大的概念，其方法、手段、内容都包罗万象，但究其根本仍然是创作者希望保护自己的成果而采取的必要措施。软件加密技术是伴随着软件解密技术的发展而发展的，反之亦然。从表面上来看，解密要比加密难度大一些，因为加密者可以自由采取各种手段，而解密者必须通过层层剖析来分析加密者的思路。然而现在的实际情况却是相反的，因为加密过程是由一个人或一家公司设计的方案，这个方案不可能拿出来和别的人或公司去讨论。而加密的产品发行后，面对的是大量解密者的攻击，这些解密者之间可以通过论坛、教程甚至专门的解密工具来交流或传授自己的解密心得。两者相对比，孰优孰劣可想而知。

很多软件开发者对软件加密都有一个错误的认识，他们认为只有不能被破解的加密才是成功的加密。事实上，就我们目前的计算机体系而言，这几乎是一个不可能达成的目标。因为软件最终是要交付给用户去使用的，而解密者就在这些用户之中。软件加密不管如何实现，也必须在使用者的计算机上能够正常执行。理论上来说，加密前的软件和加密后的软件在完成功能上应当是完全相同的，则必然存在某种方法可以在保证功能不变的前提下，把加密的部分从软件本身移除，所需要的仅仅是时间而已。所以严格地讲，如果某种加密技术能够保证在软件的生命周期内不被破解，那么这种加密技术就是成功的。

软件加密技术面临的最大问题就是各自为战。大部分开发者都认为既然是加密技术，当然是知道的人越少越好。即使是同一软件开发公司，软件加密的过程也经常被掌握在个

别人的手中。到因特网上去搜索一下看看，解密的文章、教程等到处都是，而加密的技巧、方法基本没人提及。正如中国有句谚语：“三个臭皮匠，胜过一个诸葛亮”所说的一样，每个人的设计上都会有自己的盲点，只有多交流，才能够提高，这也是本书写作的宗旨。

也许有些开发者会担心，如果把加密技术都说出去了，一旦被解密者看到，不就没有任何秘密而言了吗？实际上并非如此。就多年的加密解密经验来看，很多开发者费尽心思地想出来的加密方法，都是别人早就实现过的，就是因为缺乏交流，还以为是自己所独创的技术，结果软件一拿出去，立刻就被人破解了。其实从解密者的角度来看，加密者就那么几个思维定式，掰手指头都能数得过来。其实这并不是加密者的过错，因为在保护软件这一相同的大前提下，大多数加密者的思维定式都差不多。交流的目的是让开发者了解更多的加密手段。譬如，如果一位开发者知道1000种加密方法，而即使这1000种方法解密者也都知道，则从中选择哪种加密方法就是加密者的权利了。加密者可以从中选择一种或几种加密方法，而解密者要想知道加密者到底使用的是哪些方法就得一点点去分析了。加密者只要评估一下解密者所需要花费时间，比期望的软件生命周期要长一些就行了。这样的加密是可评估可量化的。

软件加密本身只是一种手段，就目前而言虽然是必要的，但往往更加容易引起解密者破解的欲望。最终的方法还是要依靠人们提高知识产权意识，并运用相关的法律武器来保护自己。

1.1 软件加密的发展历史

计算机发展的早期是大、中、小型计算机和工作站所统治的年代。电脑本身就是一种平常人可望而不可及的奢侈品。上面的软件不是随机附带，就是需要专家来安装，软件加密基本是不需要考虑的问题。

软件加密的最早开始时间已经难以考证，但大体上来说是20世纪80年代初期在Commodore64，Amiga这样的游戏机上首先开始的。游戏机和电脑在原理上没有太大的差别，不同的仅仅是设计目的。从现在的眼光来看待那个时期的游戏，无疑是非常简陋的，但作为一种新生的娱乐方式，却很快得到了人们的认可。也有很多人嗅到了这里面的商业气息，开始制作和销售游戏软件。这些游戏软件在开始的时候并没有得到与其他商业软件同样的认同，好玩虽然好玩，但它们不会为你创造价值，很难找到一个说服自己来购买游戏的理由，于是大家把买来的游戏交换着玩。游戏开发商自然不会认同这种想法，于是纷纷出台各种各样的保护手段，这也就导致了最早一代解密者的诞生。

这些最早的破解者基本上都是一些15~20岁左右的年轻人，破解的目的除了为能够玩到更多的游戏外，还希望更多地获得别人敬佩的目光。在那个年代，破解者无疑是非常艰

辛的，因为可以获得的软硬件资料非常有限。学习汇编对他们来说根本不是问题，问题是他们连汇编的资料都很难得到。早期的破解主要都集中在游戏方面，因为只有游戏软件才会加密。

随着 PC 和 DOS 系统的兴起，软件产业得到了迅猛的发展，不但出现了大量的游戏软件，各种各样的商业软件、办公软件也开始出现，而软件加密的传统也被继承了下来。在 DOS 年代的加密基本都是软盘加密，因为软盘是软件流通的惟一载体。软盘加密的原理是在软盘的特殊位置制造一些特殊信息，软件在运行时要检验这些特殊信息，关键的一点是这些特殊信息无法以常规的手段进行复制。此方法加密简单有效，成本低，成为软件开发商很长一段时间内的不二选择。但解密者也很快想到了破解的方法，因为 PC 的软盘控制器并不像 Apple 那么灵活，软件开发商因为无法做出类似 Apple 电脑上那种颇有杀伤力的螺旋磁道之类的加密手段，能做到的无非是应用一些特殊磁道、大扇区、循环扇区之类的技巧。此时，Copyright，Locksmith 等能够拷贝加密软盘的软件也纷纷出炉，软盘加密上的拼杀也日渐白热化。

另外要提一下的是，这个阶段出现过一种密码本加密模式。曾经玩过 DOS 时代游戏的读者可能还有印象，在游戏一开始的时候会弹出一个窗口让你输入密码本中第 xx 页 xx 行 xx 列的字符或符号是什么，而密码本是使用抗复印的低色差的方式印出来的。这种加密模式成本非常低廉，效果也就相对差一些。我们曾经见过很多游戏盘里面直接就有一个 code.txt 的文件，你直接用打印机把这个文件打印出来就是密码本。除了加密效果差之外，正版用户使用不方便也是个很致命的问题，每次启动软件都要查一遍密码本让人很心烦。这种加密模式天生的弱点导致它并没有流行开来。

在国内，有一种新兴的加密方式在这个阶段也开始浮出水面，那就是卡加密。因为最初的 DOS 是英文的，不支持汉字的显示与输入，联想、巨人等公司纷纷组织技术力量来开发汉卡这种产品，因为字库放在卡上的存储器里面，计算机上面的软件自然也就无法离开卡来单独运行。随着计算机速度的加快和存储容量的扩大，原来的汉卡存在的意义已经很小了，这一技术在后期就慢慢转向了作为一种保护软件的方法来使用。因为大多数的解密高手不懂硬件，而硬件复制的成本又相当高，卡加密确有其优势。但这种方式对开发商来说成本也相当高，一般小规模的软件公司是无法投入这么大的成本去生产加密卡的，而且这种加密方案在用户使用的时候要打开用户的计算机来安装加密卡，更是大多数用户无法接受的。这一技术在 Windows 出现的初期就从市场上基本消失了。

在这场矛与盾的较量中，Windows 3.0 的出现让双方都有些手足无措。原有的软盘加密技术大多无法在保护模式下运行，编程机制的变化让大家又重新回到了起跑线上。Windows 3.0/3.1 的时代无论是加密和解密方面的亮点都很少，很多开发者和解密者还沉湎于 DOS 的荣光之中。CD-ROM 的技术也在这个时候渐渐地兴起了，软盘的统治地位已经被逐渐打破了。

不管愿意与否，Windows 95 的出现都让 DOS 时代的开发者们认识到 DOS 时代已经一去不复返了，光盘驱动器逐渐成为了计算机的标准配置，软盘已经逐渐被市场所淘汰。开发者们迫切希望找到一种可以代替原有软盘加密的模式，加密锁的出现正是在这一背景下吸引了开发者的目光。加密锁这一技术在 DOS 时代就有了。这是一种插在计算机打印端口（并口）或鼠标端口（串口）上的小硬件，这个小硬件里面有逻辑电路或存储单元，能够与计算机进行通信。

加密锁的保护机理同加密卡来比是大同小异的，都是通过软件捆绑硬件来实现保护。但加密锁的设计上回避了加密卡的两个致命的缺陷：开发成本太高；用户使用不方便。加密锁在设计上属于需要二次编程的硬件，这样的好处在于把加密锁的大批量生产和开发商的个性化需求有效地结合在一起，整个开发成本平均分摊到多个加密锁的用户头上。另外因为加密锁是安装在计算机外部的硬件，相对加密卡而言要简单得多，不需要专业人员的帮助用户就可以自行安装。所有这些因素导致了加密锁慢慢成为主流的加密解决方案。

加密锁加密的最大问题是其成本问题。对于那些售价较高的商用软件来说可能没什么问题，但对于那些发行量动辄上万的民用类、娱乐类软件来说，加密锁本身的成本就很难被忽略了。所以，光盘加密技术成为这些开发商关注的焦点。光盘加密实际上是软盘加密技术的一种延续，虽然具体的加密技术有所不同，但加密原理同软盘加密是基本一致的，都是以存储载体作为加密介质的，对开发商来说既实用又经济。就目前的技术来看，大多数的光盘加密要求在光盘生产过程中完成，一次性要求的批量很大，不适合小批量的软件生产。另外，光盘这种载体和软盘一样属于易损载体，在用户多次对光盘进行各种操作后，可能会出现划伤，而这张光盘又无法备份。所以一般来说，光盘加密主要是用于发行量大、软件生命周期短的产品。

随着 Windows 98 的逐渐普及，计算机发展也开始进入了互联网时代。这是软件产品极大丰富的时代，各种软件产品基本都能够在网络上找到。当国家和地区的差异不再是软件宣传的限制以后，一种新的销售模式也应运而生，那就是 Shareware（我们常说的共享软件）。其实共享软件概念的诞生由来已久，但直到网络成为人人都可使用的资源之后，共享软件这个名词才被大家所了解。这是一种先用后买的销售模式，一般软件从网络上下载以后就可以直接使用，但会有附加的限制，譬如时间限制或功能限制。当用户在使用过一段时间觉得该软件不错以后，再花钱来购买。

这种销售模式的变化直接导致了软件加密模式的变化，软件注册机制就是在这个阶段成为了共享软件的主流加密手段的。软件注册机制的基本流程就是在用户决定购买软件后，通过汇款或网上支付的方式来购买软件，然后软件开发商会通过网络发给用户一个注册码或注册文件，在用户使用了注册码或注册文件后，已安装的软件就成为正式软件了。

软件注册的加密模式对于开发商来说成本非常低，开发商节省了包装和渠道上的成本，

很容易通过网络跨地区、跨国界地进行软件销售。著名的游戏 DOOM 就是第一个通过这种方式得以成功的典型范例。但这种加密模式最大的问题是无法阻止注册后的用户扩散其完整的产品。因为注册后用户手里的软件就是正版软件了，只要这个用户把注册码之类的注册信息扩散出去，其他人也能够把自己手里面的共享软件变成正版。虽然开发商使用了黑名单等方式来控制，但总的来说，并不是很有效果。

为了改善软件注册机制的注册后无法控制的问题，有人在此基础上提出了许可证加密方式。许可证加密方式是对软件注册机制的一种改良，把原来“一人一码”的方式改为“一机一码”。具体原理就是软件在执行的过程中需要搜集当前运行计算机的特定信息，当用户希望去注册这个软件的时候，开发商要的不是用户给出的个人信息，而是软件自动搜集的使用者的计算机信息，然后再根据当前计算机的信息给出对应的注册码。这种模式能够保证软件用户在拿到注册码后无法进行扩散，因为特定计算机的注册码只对特定的计算机有效，无法在别人的计算机上使用，基本上解决了软件注册后扩散的问题。

但这种加密模式对于正版的注册用户来说也造成了一定的麻烦，因为软件被限定在一台计算机上使用，如果希望把软件换到其他计算机上去用，就需要重新注册，虽然在声明自己是有效用户证明后，不需要再缴纳额外的费用，但一来一回的注册周期是难以避免的。同样即使不更换电脑，对自己当前使用的电脑进行升级也会导致同样的问题。另外，在这种模式下，软件开放商的服务工作也会增加几倍，因为除了购买性的注册外，还有更多的更换设备所导致的注册行为发生。而且针对个人用户来说，似乎没有什么好的方法来阻止他把自己两台电脑上安装的软件都注册一遍，因为他有很合理的借口。

这里要特别说一下 Windows XP 的加密方式。虽然 Windows XP 是一款商业软件，但它也采用了软件许可证的方式来加密，尽管网络上的算号器及各种破解工具很多，但微软通过系统升级这一武器把主动权牢牢地把握在自己的手里，总的来说还算是相当成功的商业加密。但这种加密模式的背后是大量的注册服务器及相关服务人员，外加微软的各种升级服务，这些都是中小规模的软件公司很难去效仿的。

1.2　软件加密方式的确定因素

很多开发者认为软件加密就是保护软件不被盗版就行了，因此在做加密的时候很少或从来没有做过任何形式的加密方案的研究。加密成了软件开发商自己想当然的事情，这样做出来的加密，成功者少，失败者多。我们想在这里给大家分析一下软件加密的方式到底是由哪些因素来决定的。

如图 1-1 所示，我们认为软件的加密方式主要和图 1-1 所示的几个因素有关。下面我们来详细说明一下这几个相关的因素。