文章编号:1006－7329(2000)02－0092－03

软件加密的防拷贝和防数字仿真*

李济民， 李化民
(重庆建筑大学 管理学院，重庆 400045)

摘要:对软件加密解密基本技术和方法分析的基础上，提出组合加密防拷贝，动态密钥读取防仿真两种方法。这两种方法的联合应用可以有效防止现有各种拷贝工具和数字仿真软件对软件产品的攻击。

关 键 词:数字仿真;动态密钥读取;组合加密;磁道接缝指纹
中图分类号:TP311.56 **文献标识码**:A

概述

如何防止软件产品被非法拷贝、剽窃和修改，是软件开发人员一直比较关心的问题，在计算机领域，这也是一个重要的研究课题。软件加密的基本方法是在介质上制作密钥，然后在保护软件中嵌入密钥识别程序，软件运行时，先运行识别程序，如果识别到正确的密钥，软件正常运行，否则死机或退出。因此，软件解密通常有三种途径，一是直接拷贝存放在介质中的保护软件及其密钥盘；其二是对保护软件的源代码做静态分析，找到并修改保护软件的识别程序，使复制的软件能正常运行；其三是对保护软件进行动态跟踪，寻找并修改识别程序。三种方法中，后两种方法特别是动态跟踪较为困难，要求解密者具有扎实的计算机技术基本功，而且费时费事，一般的解密者难以做到。第一种方法虽然简单，但随着各种防拷贝技术的出现，现有的拷贝工具要复制一张与源盘和密钥盘完全相同的复制盘越来越困难。

近年来出现的软件解密的数字仿真技术，一反过去解密的基本思路，用仿真密钥数据的方法，轻易破解了不少加密强度甚高的商品软件。这种解密方法的基本思路是这样的：不管用什么方法加密，识别程序必然与存放密钥数据的外设进行数据交换。首先运行仿真软件，让其常驻内存，然后运行正版软件。仿真软件监控正版软件的运行，当发现正版软件与外设交换数据，马上截获这些数据，并记录下该时点正版软件的运行现场。让正版软件反复运行几次，仿真软件即可记录下正版软件与外设交换的全部数据包括密钥数据以及运行时点的现场，退出正版软件，用仿真软件根据截获的数据和运行现场制作可运行的仿真程序(有的仿真软件分别制作成数据文件和仿真程序两个文件)，此仿真程序就相当于正版软件的钥匙盘。以后每次运行正版软件的复制版本时，首先运行仿真程序，使其常驻内存，然后运行复制软件，仿真程序监控软件运行，一旦发现识别程序从外设读取密钥数据，屏蔽读取操作，取出仿真程序内部或仿真数据文件中与当前时点运行现场匹配的数据，使识别程序误判为读到了正常的密钥数据，开始正常运行。用这种方法不仅能破解软加密，也能破解软件狗之类的硬加密。

对于一般的计算机用户，如果手中有一套强力拷贝工具或解密用的数字仿真软件，不需要什么特别的技术，就能对很多软件进行解密，因此，防拷贝和防数字仿真，是软件加密的最基本的技术。本文介绍软件加密的一般方法的同时，介绍了我们在开发工程造价管理系统商品软件过程中探索和使用的一些特殊技术，有效地防止了现有各种拷贝工具和数字仿真软件对软件产品的攻击。

* 收稿日期:2000－01－31
作者简介:李济民(1948－)，男，四川大竹人，副教授，硕士，主要从事土木工程、计算机科学研究。

1　软件防拷贝的基本方法

软件防拷贝的方法分为两类,一类叫硬加密,一类叫软加密。所谓硬加密,就是把密钥放在计算机的专用电路中,例如前一段时间市面上流行的汉卡,现在流行的软件狗等。前者把密钥放在计算机主板的插口槽内的插板电路中,后者把密钥放在插入计算机打印口的软件狗电路中。所谓软加密,就是把密钥放在软磁盘上,制成钥匙盘。为了防止钥匙盘被非法复制,对钥匙盘要进行各种处理,其中的一个方法就是用硬件设备在磁盘上制作一个永久性的无法复制的硬标志,然后在保护软件中加一段此硬标志的识别程序。例如激光加密法,电磁加密法,掩膜加密法等就是采用的这种方法;另外一种方法是对软磁盘的一些磁道和扇区进行特殊格式化,把密钥放在经过特殊格式化的磁道和扇区中,例如额外扇区法,超级扇区法,未格式化扇区法,额外磁道法,异常 ID 法,磁道接缝指纹法等。上面这几种软件加密方法中,硬加密和制作软盘硬标志需要专用的硬件设备,有的设备还十分昂贵,一般的加密人员难以实现,而用磁盘特殊格式化的方法加密,只需用一般计算机都拥有的普通软盘驱动器即可进行,而且能够制作出无法拷贝的软指纹,因此用这种方法加密仍然较为普遍。

以下结合自己在软件开发中进行软件加密的实际经验,提出组合加密防拷贝,动态密钥读取防仿真两种方法。这两种方法的联合应用有效地保护了软件产品的安全。

2　组合加密法防拷贝

上面介绍的特殊格式化加密的各种方法中,有的已被一些新开发的拷贝工具攻破,有的现有拷贝工具还无能为力,例如磁道接缝指纹法。如果把这些方法组合在一起,发挥它们各自的优势,在提高防拷贝的能力方面是大有可为的。这里介绍一种把额外扇区法和磁道接缝指纹法组合在一起的方法。

目前常用的软盘是 3.5 英寸软磁盘,正常格式化后有 80 条磁道,每条磁道 18 个扇区,每个扇区可存放 512 个字节的数据。磁道呈园形,它被分成 3 个区域:前置区,数据区,后置区。前置区主要用于缓冲,防止索引传感器位置误差影响互换性;数据区就是存放数据的区域,它被分成 18 个扇区;后置区位于磁道最后一个扇区的后面,它是连接最后一个扇区和下一个索引脉冲前沿的间隔。磁盘格式化时,由于磁盘转速存在波动,因此,后置区的长度以及它的每个字节的内容都是随机的,即使是同一张磁盘,在同一个软盘驱动器上前后格式化两次,同一磁道的后置区两次格式化的长度以及它的每个字节的内容都不相同。利用这一特性,把这种磁道接缝数据做成指纹密钥,目前的各种拷贝软件包括拷贝机也无法拷贝这些指纹。

修改磁盘基数表,把某磁道例如 79 磁道特殊格式化成 19 扇区,计算出磁道接缝数据的和,此和数称为磁道接缝指纹,把此指纹作为 79 磁道的密钥,存放在 19 扇区的某一字节中,一般拷贝软件无法拷贝到 19 扇区的数据。在保护软件中插入一段识别程序,识别程序中有一段读取磁道接缝数据和 19 扇区指纹的代码,对磁道接缝数据求和,将和数与存放在 19 扇区的指纹比较,如果一致,此盘是原盘,否则是复制盘。用这种方法制成的钥匙盘,虽然某些拷贝工具能够成功拷贝其 19 扇区的指纹,但拷贝不了磁道的接缝数据,因此,复制盘的 79 磁道的接缝数据与原盘的 79 磁道的接缝数据肯定不一样,其和数与存放在 19 扇区的指纹不可能匹配。

3 动态密钥读取法防数字仿真

用上面介绍的方法虽然能够防拷贝，但无法抵抗解密软件的数字仿真。下面介绍的动态密钥读取法可以解决这个问题。这种方法的基本思路是，把不同的密钥放在多个磁道或多个扇区里，识别程序随机动态地读取某一磁道或某一扇区的密钥，仿真软件虽然能够仿真某一磁道或某一扇区的数据和密钥，但由于每次运行时识别程序随机动态地读取不同磁道或不同扇区的数据，在大多数情况下，用仿真软件制作的复制盘不能正常运行。现在把上面介绍的防拷贝的方法和这种思路结合在一起，用上面的方法特殊格式化六条磁道，磁道编号从 74 磁道到 79 磁道，仍然把每条磁道的接缝指纹放在其 19 扇区里，软件运行时，识别程序随机读取这六条磁道的某一磁道的接缝数据和其存放在 19 扇区里的指纹，计算接缝数据的和并与指纹比较，匹配即正常运行。仿真软件能够检测到这些数据和指纹并记录在案，据此制作出仿真程序，但软件下一次运行时，如果识别程序读取另一条磁道，由于仿真软件没有仿真到这些数据，必然被识别程序诊断出复制盘。

有的解密仿真软件为了对付这种动态密钥读取方法，在制作仿真程序时，采用多次运行正版软件的方法，希望检测到所有的磁道或扇区数据。为了对付这种仿真方法，可以采用如下的算法，把一小时划为六段（因为总共有六条加密磁道），在某一时段内，不管正版软件运行多少次，识别程序总是按照一种与时间有关的算法选择一条磁道，因此在某个时段内，总是读取同一条磁道，仿真软件不可能检测到所有磁道。显然，用这种动态读取磁道的方法，加密磁道越多，被仿真的可能性越小。用这种方法的缺点是，加密磁道占用磁盘空间太大，如果采用动态读取扇区的方法，可以少占用磁盘空间。

参考文献：

[1] 杨迈．软件加密/解密反跟踪实用技术(M)．西安：西安电子科技大学出版社，1993

Anti-Copy and Anti-Digital Simulation in Software Security Key

LI Ji-min, *LI Hua-min*

(Faculty of Management, Chongqing Jianzhu University, 400045, China)

Abstract: This paper discussed the basic technique of setting security key and produced group security key to anti—copy and dynamic reading security key to anti digital simulation. These two methods can prevent effectively the software from attacking.

Keywords: digital simulation; dynamic security key; group security key; track fingerprint