第33卷 第12期 计 算 机 工 程 2007年6月
Vol.33 No.12 Computer Engineering June 2007
·安全技术· 文章编号：1000—3428(2007)12—0183—02 文献标识码：A 中图分类号：TP311

基于动态注册码的软件加密保护

孙永清[1]，顾雨捷[2]，赵 戈[1]
(1. 公安部第三研究所，上海 200031；2. 浙江工业大学信息工程学院，杭州 310032)

摘 要：设计了一套基于动态注册码的软件保护方法，该方法采用了提取计算机指纹信息并添加附加码作为特征信息的做法，运用公开成熟的 MD5 算法进行加密处理，并用 VC++编写程序进行检验，在程序编写过程中充分考虑安全性，并通过一系列手段进一步提高其安全性。

关键词：动态注册码；计算机指纹信息；MD5 算法；附加码

Software Encryption and Protection Based on Dynamic Register Code

SUN Yongqing[1], GU Yujie[2], ZHAO Ge[1]
(1. The 3rd Research Institute of Ministry of Public Security, Shanghai 200031;
2. School of Information Engineering, Zhejiang University of Technology, Hangzhou 310032)

【Abstract】 A method about how to protect software is designed, which is based on dynamic register code. In the method, computer fingerprint is drawn and additional information is added, and the two are combined to be as characteristic information. Then MD5 algorithm is used to encrypt. The procedure is realized with VC++. Security is considered fully and some methods are adopted to enhance security.

【Key words】 Dynamic register code; Computer fingerprint; Message-digest algorithm 5; Additional code

1 常见的加密方法

软件的加密方法多种多样，根据软件保护方法可分为依赖硬件的硬加密方法和不依赖硬件的软加密方法[1]。

硬加密方法是将加密信息固化在硬件上，如软件狗，软件在每次启动时，先检测硬件上的相应信息，如果通过检测，则启动软件系统，否则不能正常启动软件系统。通过这种方法实现软件的合法使用，一般认为硬加密方法成本高，但安全性高。对于考虑成本或者有特殊应用要求的软件，硬加密有时候并不适合。

软加密最大优势在于极低的加密成本，用软件方法不依靠特殊硬件来实现对软件的加密，通过在软件中插入加密模块来保证软件不被非法使用，主要有密码表法、软件自校验法、钥匙盘法[2]，前 2 种方法是早期软件保护做法，对软件的保护作用较弱，第 3 种方法不能限制软件在多台计算机上安装，现在这 3 种方法已经不太常用。

现在常用的是第 4 种方法，这种方法是用户软件安装完毕后需要向软件开发商申请许可证才可以不受限制地使用软件的许可证方法，这种许可证方法采用基于动态注册码的软件加密方法实现。本文主要讨论这种实现方法。

2 基于动态注册码的软件加密方法

2.1 设计思想和特点

基于动态注册码的软件加密方法过程为软件在使用过程中获取用户计算机系统已经存在的某些特征信息，比如CPU ID、BIOS信息、硬盘序列号、硬盘分区信息等能够将任意 2 台机器区分开来，这些信息被称为计算机指纹[3]。将指纹信息经过一定的处理后生成机器码，用户需将此机器码以电话、传真或者Email等方式告诉软件开发商，软件开发商在收到此信息确认此用户为合法用户，则将根据机器码生成的软件注册码告诉用户，用户在软件中输入此注册码，软件校验此注册码合法后即可正常使用软件。

由于注册码是根据计算机指纹信息(几乎是唯一的)动态生成的，因此这种方法可以确保软件只在一台机器上使用，具有一定的使用价值。

2.2 程序实现

本文在 Windows 操作系统(Win2000 和 Windows XP)中使用 C++实现了动态注册码的加密保护。

2.2.1 计算机指纹信息提取

本加密方法采用计算机硬盘序列号和网卡 MAC 地址作为计算机指纹信息，获取硬盘序列号和网卡物理地址的方法虽然可以通过专用软件获取，但是在制作加密程序和软件安装时不够方便，理想的加密程序应该本身具有提取计算机指纹信息的功能，而且软件每次运行时先提取计算机指纹信息，然后通过加密算法验证软件使用的合法性。

获取硬盘序列号通过 Windows API 函数 DeviceIoControl 来获取硬盘信息，得到的信息经过转换后就可以得到硬盘序列号，每一块硬盘序列号都是唯一的。下面是部分代码：

```
if (DeviceIoControl (hScsiDriveIOCTL, IOCTL_SCSI_
MINIPORT,
        buffer,
        sizeof (SRB_IO_CONTROL) +
        sizeof (SENDCMDINPARAMS) - 1,
        buffer,
        sizeof (SRB_IO_CONTROL) + SENDIDLENGTH,
```

作者简介：孙永清(1976－)，男，硕士，主研方向：计算机信息安全；顾雨捷，硕士生；赵 戈，硕士

收稿日期：2006-09-04 **E-mail：**yqsun@trimps.ac.cn

```
            &dummy, NULL))
    {
            SENDCMDOUTPARAMS *pOut =
                (SENDCMDOUTPARAMS *) (buffer + sizeof
(SRB_IO_CONTROL));
            IDSECTOR *pId = (IDSECTOR *) (pOut -> bBuffer);
            if (pId -> sModelNumber [0])
            {
                DWORD diskdata [256];
                int ijk = 0;
                USHORT *pIdSector = (USHORT *) pId;
                for (ijk = 0; ijk < 256; ijk++)
                    diskdata [ijk] = pIdSector [ijk];
                PrintIdeInfo (controller * 2 + drive, diskdata);
                done = TRUE;
              }
    }
```

获取网卡 MAC 地址要首先对选定的网卡发送一个 NCBRESET 命令，进行初始化后，通过 Netbios 函数发送 NCBASTAT 命令获取到网卡信息，最后经过转换，得到 MAC 地址。

把硬盘序列号和网卡 MAC 地址进行组合(本文只是简单叠加)就提取到了所需要的计算机指纹信息。

2.2.2 附加码策略

简单的提取计算机指纹在安全性方面是不够的，如果对计算机指纹信息不加处理，那么破解者就可以猜出提取的是哪些特征信息，使用公开的算法经过简单的验证后就会得到注册码。

为了避免这个问题，通常需要把提取到的计算机指纹信息进行处理后再生成注册码，附加码策略就可以解决这个问题。这种策略是在软件代码中包含一个软件开发者定义的字符串，开发者自己保存了一个附加码表，不同用户得到的附加码可能是相同的，也可能不同，附加码与计算机指纹信息组合得到了新的计算机特征码，使用加密算法对这个特征码进行加密得到注册码。

附加码策略的使用如图 1 所示。

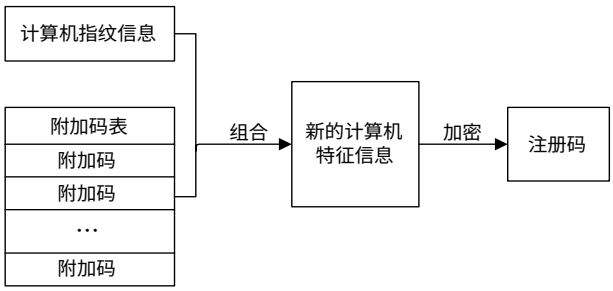

图 1 附加码策略

2.2.3 程序实现

动态注册码的生成采用信息-摘要算法(message-digest algorithm 5，MD5)加密算法[4]。MD5 算法基于不可逆的字符串变换算法，20 世纪 90 年代初由麻省理工大学计算机科学实验室和RSA Data Security Inc.的Ronald L. Rivest开发出来，经MD2、MD3 和MD4 发展而来。它的作用是让大容量信息在用数字签名软件签署私人密钥前被“压缩”成一种保密的格式(即把一个任意长度的字节串变换成一定长的大整数)，产生了唯一的MD5 信息摘要。这个算法被广泛应用在加密、解密以及数字签名技术上，具有很高的安全性。用MFC编写的注册码生成器如图 2 所示。

图 2 动态注册码生成器

2.3 安全性

软件保护的安全性涉及到许多方面，包括反调试、反跟踪技术以及反静态分析技术等。但是就软件加密的安全性而言，安全性取决于两个方面：

(1)算法的安全性；

(2)特征码提取的难易程度。

动态注册码基于安全的公开算法，同时采用了动态提取特征码的方法，因而具有了较高的安全性。

此外，为了提高加密的安全性，在程序设计时做到了以下 4 点：

(1)附加码在程序中进行了简单的替换，这样就不能根据可执行程序直接分析出附加码的明文；

(2)将生成注册码的代码和检测注册码是否合法的代码分开，这样就不可能通过简单地判断系统调用来获得注册码；

(3)生成的注册码不存放一个数组中，而是分散存放，破解者就很难通过分析内存获得注册码；

(4)检测注册码时，加入了一些无用的运算，通过误导破解者来加大破解难度。

3 结束语

对软件加密而言，没有绝对安全的加密方法，当破解软件的代价大于通过正当途径获得合法版权软件的代价时，就可以认为这种加密方法是安全的。

对于软件开发者而言，应该灵活地应用软件加密技术，在允许的范围内尽量提高软件的保护强度。

参考文献

1 佟晓筠, 王 外翥, 杜 宇, 等. 基于软件安全混合加密技术的研究[J]. 计算机工程, 2004, 30(23): 98-100.

2 冯能山. 应用软件加密钥匙盘的一种实现方法[J]. 计算机应用与软件, 2005, 22(9):123-124.

3 鞠斌山, 邱晓凤, 张文东. 利用计算机指纹实现软件加密原理与方法[J]. 青岛大学学报(自然科学版), 2005, 18(3): 63-66.

4 汤 惟. 密码学与网络安全技术基础[M]. 北京: 机械工业出版社, 2004.

5 孙文乾. 浅谈软件加密技术[J]. 河池师专学报(自然科学版), 2002, 22(2): 60-62.