浙江科技学院学报,第 22 卷第 4 期,2010 年 8 月
Journal of Zhejiang University of Science and Technology
Vol. 22 No. 4, Aug. 2010

DOI: 10.3969/j.issn.1671-8798.2010.04.007

一种基于“一机一码”的软件激活序列号生成方案

许　旭,潘志刚
(浙江科技学院 信息与电子工程学院,杭州 310023)

摘　要:激活码是软件安全保护、验证软件授权合法性的重要手段,对保护软件版权、防止盗版均具有非常重要的意义。为此,在对现有软件激活机制研究的基础上,给出了一种通过提取并组合用户机器 CPU 特征值、随机函数及系统时间,来完成特征码采集和激活 ID 生成;并采用 MD5 加密算法生成软件激活序列号的设计实现方案。该方案在实践中已做过初步尝试,能够实现构造机器唯一标识,生成激活序列号,有效保证软件的安全,具有一定的使用和推广价值。

关键词:软件保护;序列号;唯一标识
中图分类号:TP311.52　　**文献标识码**:A　　**文章编号**:1671-8798(2010)04-0273-05

Solution to creating software activation serial number based on “current hardware ID for current machine”

XU Xu, PAN Zhi-gang
(School of Information and Electronic Engineering, Zhejiang University of Science and Technology, Hangzhou 310023, China)

Abstract: As an important measure for software safety security and software authority validity, an authority code is significant for software copyright protection and anti-piracy. Based on the previous research of software activations, the use of MD5 encryption algorithm to generate the serial number of software activation is now realized. By extracting and combining user PC CPU eigenvalue, random functions and system time, we manage to complete attribute code collection and authority ID creation, as well as create software activation serial numbers implementing MD5 encryption algorithm. This solution can enable the only identity for a machine, and thus preserve software safety, featuring practical and promotional value.

Key words: software security; serial number; the only identity

收稿日期:2010-03-11
基金项目:浙江省大学生科技创新活动计划(新苗人才计划)项目(团浙联(2010)15 号)
作者简介:许　旭(1987—　),男,湖南岳阳人,计算机科学与技术专业本科生。
通讯作者:潘志刚,讲师,硕士研究生,主要从事软件工程、信息系统和监控系统研究。

随着经济技术的飞速发展,软件作为辅助工具已经深入到了无线通信、数据卡等各行各业当中。软件产品是软件设计者和软件编程人员智慧的结晶,因而,保护软件产品的版权,防止软件产品被盗版,具有很重要的现实意义[1-3]。目前,国内已经开展了通过增加后续服务、增加软件狗、设定激活软件、限定 IP 等方法来从根本上打击盗版[4]。

对软件开发商而言,很多商家选择使用设备特征码及激活码来验证其软件授权合法性。理想的特征码应该是提取设备的唯一性标识,软件运行在不同的硬件上,将会读到不同的特征码,根据不同的特征码生成激活码,保证一个确定的激活码只会对应一个特征码,从而保证激活的唯一性,防止软件盗版[5]。

在对现有激活机制研究的基础上,本文给出了一种基于"一机一码"的软件激活序列号生成方案,该方案采用组合用户机器硬件特征值、随机函数及系统时间来采集特征码,根据得到的特征码生成激活 ID;并利用自定的加密规则和 MD5 加密算法相结合,生成激活序列号。在用户使用激活软件后,把激活信息永久保存到注册表,在每次启动被激活软件时先到注册表中寻找激活信息,并进行激活信息匹配。该方案采用 C++、MFC 作为编程工具,实现了构造机器唯一标识,生成激活序列号,以有效保证软件的安全。

1 软件激活简介

1.1 激活机制

尽管不同的软件厂商有不同的实现方式,但目前大家采用的激活机制的原理还是相通的:根据用户的硬件配置为每个用户生成一个唯一的激活代码。激活代码可以是一个单一数值,也可以是几个数值的组合。例如,Microsoft 公司通常提供单一的组合值,而 Macrovision 公司(该公司生产著名的 DRM 产品 SafeCast)会发给用户 2 个数值:一个系列号和一个根据硬件生成的数字。用户的配置信息会通过 Internet(或者电话)发送到软件公司的激活服务器,服务器会把收到的数值保存到数据库,然后把唯一的激活代码发回给用户,用户用这个激活代码就可以解锁软件产品[6]。

1.2 激活算法

软件激活码合法性的验证过程,其实就是验证用户相关信息和序列号之间的换算关系是否正确的过程。构造机器唯一标识码是产生激活 ID 和激活序列号的第一步,同时也是控制软件不被盗版的重要的一步。通过构造机器唯一标识,可以保证每台机器获取的激活 ID 唯一,杜绝 2 台机器使用同一个激活 ID 进行激活,减少软件盗版的可能。

现有的激活机制一般是采集机器的唯一标识,但是机器的很多硬件唯一标识并不能直接满足软件激活序列号所要求的唯一性。例如网卡,如果仅仅是通过获取网卡的 MAC 地址来生成激活序列号,可能会造成如下问题:一是用户激活后修改了计算机的 MAC 地址,原有的激活状态就可能不存在,需要重新激活;二是用户未激活,可通过把未激活机器的 MAC 地址修改成已激活机器的 MAC 地址,从而采用已激活用户的激活 ID 和激活序列号正常使用未经授权的软件,造成软件盗版;三是如果用户没有网卡,可能造成无法激活的情况。此外,同生产批次、同型号的机器设备其机器标识可能是相同的,难以满足要求。基于以上考虑和计算机 CPU 寿命较长、是计算机不可缺少的硬件,笔者采用如下激活生成方案:

$$\text{激活 ID}=F1(\text{CPUID},\text{时间},\text{随机数})$$

$$\text{激活序列号}=F2(F_{MD5}(\text{激活 ID}))$$

此处,$F1$、$F2$ 是 2 个不同的算法函数。程序读取 CPU 的 ID 并加以随机数和时间因素,利用 $F1$ 生成激活 ID。CPU ID 虽然不是机器唯一标识,但是加上时间和随机数就可以使之变成唯一标识。生成激活 ID 后对它进行 MD5 加密,可以实现信息的隐藏,然后对隐藏信息利用 $F2$ 算法转换成需要的格式,作为激活序列号。

2 软件结构设计

该软件分为 4 个主要模块,分别为获取机器唯一标识、计算激活 ID、计算 MD5 编码和计算激活序列

号。其中计算 MD5 编码模块还可以细分为 GetMD5OfString 模块。具体软件结构图如图 1 所示。

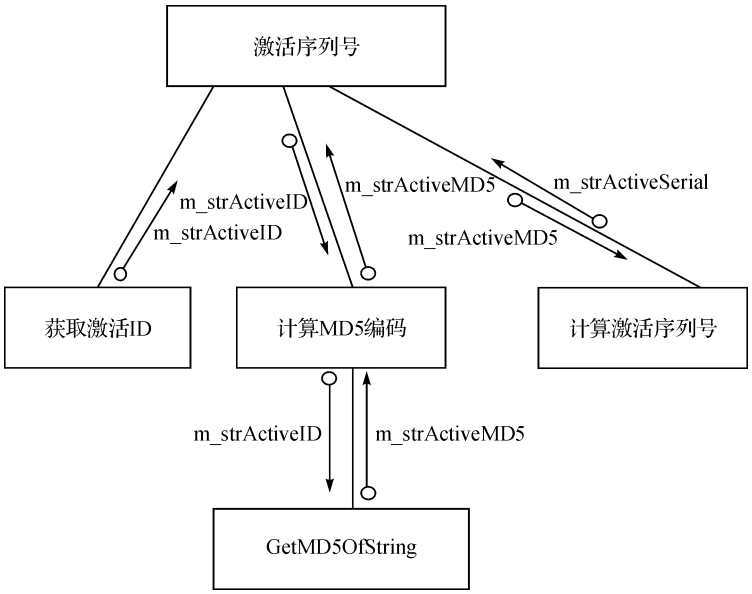

图 1　软件结构图

Fig. 1　Software chart

3　软件实现

3.1　特征码采集

机器唯一标识码的构造采用如下方法：程序首先获取 CPU 的 ID，然后使用 CTime 类的 GetCurrentTime 函数获取当前时间，接着用当前时间的年份构造一个当年元旦 0 时 0 分 0 秒的时间，使用 CTimeSpan 类存储 2 个时间差，用获得的 CPU ID 加上时间差的秒数，用 srand 函数初始化随机数发生器，产生一个随机数，与之前产生的 ID 相加，作为激活 ID。具体代码如下：

```
CTime CurrentTime=CTime::GetCurrentTime();//获取当前时间
int year=CurrentTime.GetYear();//获取当前时间的年份
CTime CurrentYear(year,1,1,0,0,0);//利用当前年份构造一个当年元旦 0 点 0 分 0 秒的时间
CTimeSpan TimeDiff=CurrentTime-CurrentYear;//计算当前时间与元旦的时间差
iCpuID+=TimeDiff.GetSeconds();//CPU 的 ID 号加上当前时间的秒数(粗略)
srand((unsigned)time(NULL));//初始化随机数发生器
iCpuID+=rand();//获取随机数,并把开始于时间关联的 ID 号与随机数相加
```

3.2　自定规则加密

采集特征码并产生 MD5 编码，需要采用自定规则对获得的数据进行加密。该规则的实现具有很大的灵活性，加密规则有很多种，但为了安全起见，采用自定义的加密规则，可以有效地减少软件被破解的可能。

采用自定义加密规则隐藏获取激活 ID 时，笔者采用如下自定加密规则：第 1 位乘 11 对 10 取模，第 2 位乘 9 对 10 取模，第 3 位乘 7 对 10 取模，第 4 位乘 5 对 10 取模，第 5 位乘 3 对 10 取模，第 6 位加 2 对 10 取模，第 7 位加 4 对 10 取模，第 8 位加 6 对 10 取模，第 9 位加 8 对 10 取模，第 10 位减 11 对 10 取模。然后把 10 位数据连接成一个字符串，返回到编辑框中，作为激活 ID。主要代码如下：

```
i1=(iCpuID%10*11)%10;//第 1 位乘 11 对 10 取模
iCpuID/=10;
i2=(iCpuID%10*9)%10;//第 2 位乘 9 对 10 取模
iCpuID/=10;
```

```
i3=(iCpuID%10*7)%10;//第 3 位乘 7 对 10 取模
iCpuID/=10;
i4=(iCpuID%10*5)%10;//第 4 位乘 5 对 10 取模
iCpuID/=10;
```

产生 MD5 编码后，笔者采用如下规则进行加密：对于 32 位的 MD5 编码，第 1 位和第 17 位一组，第 2 位和第 18 位一组，依此类推，一直到第 16 位与第 32 位一组。把每组的 2 个字母 ASCII 码值进行相加，然后除以 2。根据 ASCII 码表，如果字母在 0－9、A－Z 或 a－z 中，则不处理；如果字母在 9－A 中，则对求出的字母的 ASCII 值加上 A 的 ASCII 码值减去 9 的 ASCII 值；如果字母在 Z－a 中，则对求出的字母的 ASCII 值加上 a 的 ASCII 码值减去 Z 的 ASCII 值。求出 16 个字母后，第 1 位和第 16 位的字母计算产生的结果作为激活序列号的第 1 位，第 2 位和第 17 位字母计算产生的结果作为激活序列号的第 2 位，一直到第 16 位。以 4 个字母为一组，在每组中间加上“－”分隔。然后连接成一个字符串，返回到编辑框中，作为激活序列号。主要代码如下：

```
for (int i=0;i<16;i++)
{
  ActiveSerial[i]=(char)(((int)m_strActiveMD5[i]+(int)m_strActiveMD5[i+16])/2);
  if (ActiveSerial[i]>'9'&&ActiveSerial[i]<'A')
  {
    ActiveSerial[i]=ActiveSerial[i]+'A'-'9';
  }
  if (ActiveSerial[i]>'Z'&&ActiveSerial[i]<'a')
  {
    ActiveSerial[i]=ActiveSerial[i]+'a'-'Z';
  }
}
```

3.3 MD5 加密

获得激活 ID 后，需要对激活 ID 进行 MD5 加密，以实现对信息的隐藏。通过 MD5 加密，可以获得原始信息的信息摘要，防止侵权者利用激活序列号计算出激活 ID，保护软件安全。实现过程如下：用 Init 函数初始化 MD5 常量并计算追加长度，Append 函数对原始信息进行补位，将原始信息长度附加在补位后的数据后面，用循环将原始信息以 64 字节为一组拆分。返回时把激活序列号中的小写字母变成大写。主要代码如下：

```
Init();//初始化 MD5 所需常量
Append(InputMessage.length());//计算追加长度
for(int i=0;i<m_AppendByte;i++)//对原始信息进行补位
{
  if(i==0) InputMessage+=(unsigned char)0x80;
  else InputMessage+=(unsigned char)0x0;
}
//将原始信息长度附加在补位后的数据后面
for(int i=0;i<8;i++) InputMessage+=m_MsgLen[i];
unsigned char x[64]={0};//位块数组
//循环，将原始信息以 64 字节为一组拆分进行处理
for(int i=0,Index=-1;i<InputMessage.length();i++)
```

```
{
  x[++Index]=InputMessage[i];
  if(Index==63)
  {
    Index=-1;
    Transform(x);
  }
}
```

3.4　通过软件版权人再加密实现与待激活软件配合使用

软件版权人再加密是在产生激活序列号的情况下，在输入激活序列号时，人为地加入一个加密规则，这个规则可以很简单，往往只有软件著作权持有人或其授权人知道，是一个看不见的规则。例如在输入激活序列号时，用由激活软件生成的激活序列号去激活待激活软件是无效的，必须将计算出的激活序列号第 2 位和第 8 位互换之后才能有效激活。这个只存在于软件作者脑海中的规则，主要用来防止激活码生成软件本身被拷贝盗版的情况下，依然能有效减少软件被破解的可能，加强软件的安全。

笔者此处采用如下规则：除去“－”字符，把激活软件生成的 16 位激活码的第 4 位字符 ASCII 值加上 2，如果加上 2 后不是一个类似 0－9，a－z，A－Z 之类的字符，在各自界定字符如 0－9、a－z 和 A－Z 范围内循环。例如字符 y，加上 2 后，就变为 a；字符 9，加上 2 后，变为字符 1。依次类推。第 13 位减去 3，如果出现与第 4 位类似情况，用相同的方法处理。激活码生成软件配合待激活软件使用效果如图 2 和图 3 所示。

图 2　未经过二次加密，激活失败图

Fig. 2　Without second encryption, activation failed

图 3　经过二次加密，激活成功图

Fig. 3　After second encryption, activation succeeded

4　结　语

本文介绍了一种软件激活机制，设计并开发了一款激活软件，该软件经过多次测试，能与多种语言编写的普通软件配合使用，并且结果正确，效率高，能够达到防止软件盗版，控制软件随意传播的目的。

参考文献：

[1]　凯立德欣技术(深圳)有限公司. 一种导航设备激活方法、导航设备激活中心和导航设备：中国，200810068443. 9[P]，2008-12-03.

[2]　e2 因特莱科迪伏有限公司. 激活码的产生与关联：中国，200710108785. 4[P]. 2007-12-26.

[3]　北京深思洛克软件技术股份有限公司. 一种远程激活软件的方法：中国，200810105873. 3[P]. 2009-04-08.

[4]　伍瑞姝. 软件盗版问题分析与反盗版策略探讨[J]. 商业经济，2009(12)：71-72.

[5]　凯立德欣技术(深圳)有限公司. 一种软件激活方法及系统：中国，200810067031. 3[P]. 2008-10-01.

[6]　佚名. 软件激活 FAQ[J]. 个人电脑，2004(1)：202-203.