

基于硬件设备内部指纹的软件锁功能的实现

李志伟, 杨茂兴, 铁跃焕

(空军第一航空学院 航空军械工程系, 河南 信阳 464000)

摘 要: 研究了软件锁常用的实现方法, 提出了利用计算机硬件设备内部指纹信息作为软件钥匙进行身份认证的设计思想. 软件开发时, 将需要随软件分发给用户的硬件设备分别采集其指纹信息并嵌入到程序内部; 软件应用时, 自动检测指定硬件设备的指纹信息, 通过与软件内部嵌入的已知指纹信息进行比较, 实现软件锁的钥匙功能. 实践表明, 该方法设计简单, 使用方便, 可以代替某些专用硬件加密设备, 达到较高强度的身份认证效果.

关键词: 硬件设备; 指纹; 软件锁; 钥匙; 身份认证

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2013)04-0123-04

Implementation of the Software Lock Function Based on Fingerprint within Hardware

LI Zhi-wei, YANG Mao-xing, TIE Yue-huan

(Department of Aviation Ordnance Engineering, The First Aeronautical Institute of Air Force,
Xinyang 464000, China)

Abstract: The common achievement method of software locks is studied, the design idea of identity certification that using the computer hardware internal fingerprint as software key is proposed. When development, the fingerprint information in user's hardware that distributed with the software need to be collected, and must be embedded into the internal program. When application, the fingerprint information in the specified hardware is detected automatically, and compare with the known fingerprint information embedded within the software, the key function of the software lock is realized. Practice shows that this method is designed simple, easy to use and can replace some dedicated hardware encryption devices to achieve higher strength identity certification effect.

Key words: hardware; fingerprint; software lock; key; identity certification

1 引言

长期以来, 软件应用过程中的身份认证一直受到人们的高度重视, 防止非法用户盗用软件或进入系统是身份认证的重要任务. 目前, 最常用的方法是在软件设计或应用过程中对软件加锁, 用户通过授权的钥匙打开软件, 进入系统. 通常情况下, 软件锁功能既可采用设置软件密码的方式实现, 也可采用专用加密设备的方式实现, 还可采用二者混合的方式实现. 随着网络技术应用的普及, 也有很多软件开发者采用广播加密系统实现数据的安全分发和用户授权^[1]. 这些实现方式, 要么软件保护强度不够, 要

么需要支付额外的硬件成本, 给软件开发和应用带来了诸多不便, 为了克服这些缺点, 本文提出了利用计算机自身硬件或常用外部设备内部指纹实现软件锁功能的设计思想, 并进行了实践检验.

2 软件锁常用的实现方法

从根本上讲, 软件锁功能实际上是通过一定的密码体制, 在软件应用过程中将用户提供的密码与系统预先设定的密码进行比较, 达到开启或关闭软件的作用. 通常情况下, 软件锁功能可通过如下三种密码来实现.

2.1 软件密码

软件密码的实现方法主要有两种.

(1)通过程序设计,在程序内部设定用户登录密码,当软件提交给用户时,程序员同时将密码交付给用户.这种方法的优点是只要设置合理,安全性相对较高.缺点是用户不能更改密码,灵活性相对较差,如果密码设置强度不够,也存在被破译的风险.

(2)通过数据文件存储密码,用户可以设置、修改、删除密码.这种方法的优点是密码管理比较灵活,易于移植,易于更改,通常应用于对安全性要求不太高的软件系统.缺点是如果密码数据文件不进行加密处理,或加密强度不够,则密码很容易被非法用户盗取.

2.2 硬件密码

硬件密码是通过固化处理,将密码信息设置到计算机硬件的加密模块上,软件运行时自动调取用户密码,达到开启软件功能的目的.这种加密锁称为硬加密锁.

常用的硬加密锁有插入到计算机主板扩展槽中的加密卡,也有插接到计算机外部接口上的软件狗、USB 钥匙盘等,其密码的产生通常需要采用一定的算法,并将算法程序存储到密码芯片上^[2-3].软件运行时,首先通过相应的接口检测密码锁是否存在,如果存在,读取锁内的密码信息,检查是否与软件设置的内部密码一致,决定是否启动软件.

这种方法的优点是密码的安全性较高,只有软件的开发人员或授权用户才具有密码设置权限,普通用户无需知道密码,只要将密码锁插入到相应的接口,便可开启软件.缺点是需要增加额外的硬件投资,而且如果密码算法设计不合理,还会降低软件的运行性能^[4-5].

2.3 软硬件结合密码

采用软硬件结合方法进行密码设置.软件运行时,通常先检测加密硬件是否存在并验证硬件密码,然后再由用户提供软件密码.这种方式的优点是密码安全性更强,且对多用户管理更加方便.缺点是需要额外的硬件投资.

3 基于硬件设备内部指纹的软件锁设计

3.1 硬件设备内部指纹

目前,对于标准的计算机硬件设备,每个设备在出厂之前都由厂家在其内部“打”上了一个标签,即设备的硬件特征信息,或称为硬件设备的内部指纹,如 CPU ID、声卡 ID、网卡的 MAC 地址、硬盘 ID、U

盘 ID 等.由于这些 ID 号具有身份认证的唯一性和用户不可复制性等优点,因此用它作为计算机软件锁的密码钥匙是非常理想的选择.

由于计算机设备包括固定设备(如 CPU、声卡等)和可移动设备(如移动硬盘、U 盘等),因此作为软件锁密码钥匙的硬件设备也有相应的两种类型,其实现的基本原理完全相同,唯一的区别是:前者固定在计算机内部,软件运行时即可进行检测,不需要额外的人工操作;后者可看作是计算机的外部设备,软件运行时需要将其插入到相应的接口,起到软件加密狗的作用^[6-7].

由此可见,基于硬件设备内部指纹的软件锁设计,主要应当从两个方面进行考虑:一是开发阶段的指纹信息采集,二是应用阶段的指纹信息认证.

3.2 指纹信息采集

软件开发阶段,首先应当根据应用需求,选择合适的硬件设备作为软件钥匙,然后采集相应设备的内部指纹,将其作为软件锁的钥匙存储于指纹数据列表中,并将其嵌入到程序内部.由于该数据列表对用户来说是不透明的,因此具有较好的安全性.

若采用同一种类型的设备作为指纹钥匙,将需要分发给不同用户的所有钥匙设备一一进行指纹检测,并将数据信息存储到同一指纹数据列表中,便于指纹信息的管理.若以普通 U 盘作为软件锁钥匙,则其内部指纹采集流程如图 1 所示.

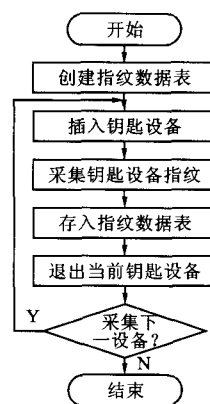


图 1 软件锁钥匙指纹信息采集流程

3.3 指纹信息认证

软件应用时,在客户端计算机上,首先通过软件自身的检测功能采集指定硬件设备的指纹信息,然后将其与软件内嵌的指纹数据表中的信息进行比较,检查是否匹配,如果匹配成功,则通过身份认证,打开软件锁,运行主程序,否则未通过身份认证,终止程序运行.软件锁功能程序设计流程如图 2 所示.

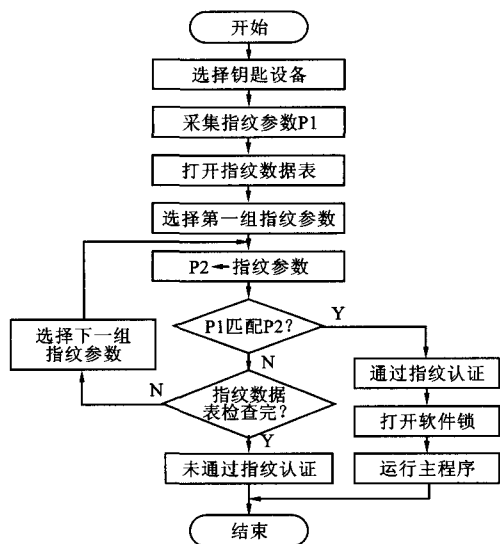


图2 软件锁功能程序设计流程

3.4 说明

通过上述设计过程可以看出,利用硬件设备内部指纹信息实现软件锁功能,应该注意如下问题:

(1) 钥匙设备的选择

通常情况下,对于专人专用的计算机用户终端及应用软件,若采用计算机本身具有的硬件设备(如CPU、网卡、声卡等)作为软件钥匙,可以省去插接外部设备环节。对于多用户计算机终端,为了便于管理和控制,则宜采用可插拔硬件设备作为软件钥匙(如U盘、移动硬盘等)。实践中,可根据具体情况选择合适的硬件设备作为软件钥匙。

(2) 信息采集参数的选择

指纹信息的采集应尽量考虑一些固定不变的信息,如硬盘的物理序列号(即使格式化后仍保持不变),避免采用虽然唯一,但是有可能变化的一些信息,如网络IP地址(与网络地址分配或用户设置有关)、硬盘的逻辑序列号(每次格式化后都不一样)等。

尽量避免选择软件运行时不需要支持的硬件设备。例如,软件运行时不需要网络连接,则可以不把网卡的MAC地址作为认证信息,以免给合法用户造成不便。

(3) 认证强度考虑

必要时,可将同一台计算机上多种设备的指纹信息相互绑定,提高软件身份认证的强度。

4 设备内部指纹信息采集的实现

对于硬件设备内部指纹信息的采集,在进行程序设计时需要考虑对计算机资源和系统底层服务的

操作,具体可以采用多种方法,常见的有:

(1) 利用汇编语言进行程序设计

该方法相对复杂,需要对操作系统的底层操作进行深入了解。

(2) 利用WMI设备管理技术

从Windows 2000开始,操作系统提供了WMI(Windows Management Instrumentation, Windows管理规范)设备管理技术,可以更加便捷地对计算机硬件资源和软件资源进行管理,通过引用WMI类的属性便可对相应管理对象进行操作,实现方法比较简单。

(3) 利用API函数提供的底层服务

在Windows 95以后的32位操作系统中,都提供了丰富的Win32 API(Application Programming Interface,应用程序编程接口)函数,可以执行Windows提供的所有服务。根据不同的功能类别,这些函数分别封装在不同的动态链接库中,通过高级语言调用相应动态链接库中的API函数,可以实现对硬件设备内部指纹信息的采集。

(4) 利用第三方提供的动态链接库

使用方法同(3),只是在系统中通过调用第三方提供的动态链接库实现相应的采集功能。

下面采用<http://www.codefans.net>网站提供的USBPhysic.dll,通过对USB设备内部指纹信息采集说明具体的实现方法^[8]。

动态链接库引用声明:

```
Private Declare Function Init Lib "USBPhysic.dll" (ByVal sUser As String, ByVal sRegCode As String) As Long
```

```
Private Declare Function GetUSBPhysicInfo Lib "USBPhysic.dll" (ByVal diskIndex As Long, ByVal InfoType As Long, ByVal pHddInfo As String) As Long
```

采集子程序样例:

```
Private Sub Command1_Click()
```

```
Dim tDiscs As Long
```

```
Dim sBuffer As String
```

```
Dim iReturn As Long
```

```
Dim PhysicInfo(3) As String
```

```
tDiscs = Init("Mndsoft.com", "C88C-7F7A-725B") 注册名和序列号
```

```
sBuffer = Space(1024) '缓冲区
```

```
iReturn = GetUSBPhysicInfo(0, 0, sBuffer) 'U盘物理序列号
```

U盘物理序列号

```
PhysicInfo(1) = Left(sBuffer, iReturn)
```

```
iReturn = GetUSBPhysicInfo(0, 1, sBuffer) '
```

产品名称

```
PhysicInfo(2) = Left(sBuffer, iReturn)
```

```
iReturn = GetUSBPhysicInfo(0, 2, sBuffer) '
```

制造商

```
PhysicInfo(3) = Left(sBuffer, iReturn)
```

```
End Sub
```

其中,数组 PhysicInfo 用于存储采集到的设备内部指纹信息。

5 验证与分析

基于硬件设备内部指纹信息的软件锁设计,由于利用了 Windows 操作系统的底层服务,将软件设置与硬件指纹进行了绑定,因而这种软件锁功能的实现更加方便,更加安全。

近年来,在面向应用的软件开发中,为了加强对分发到各应用单位软件的管理,采用过将计算机自身硬件设备(如 CPU、网卡)内部指纹作为软件锁钥匙,也采用过将普通外部设备(如 U 盘)内部指纹作为软件钥匙,都收到了理想的应用效果。

实践表明,这种软件锁设计具有如下几个方面的特点:

(1)由于硬件设备指纹信息嵌入到了程序内部,身份认证过程是在程序运行时自动完成的,对于合法用户来说,不需进行任何操作,身份认证更合理,使用更方便。

(2)由于将用户计算机硬件指纹信息与应用软件进行了绑定,提交给用户的最终软件只有检测到经过认证的硬件指纹信息时才能运行,因此即使软件被完整地进行了移植,如果缺少认证硬件的支持也不能运行,最大限度地保护了开发者的知识产权。

(3)由于软件锁指纹信息的设置只对开发者透明,因此更便于对软件的控制与管理,尤其适用于行业专用软件。

(4)由于计算机硬件指纹信息具有全球唯一性,

因此将其作为软件锁钥匙,密码被破译的可能性极小,软件保护强度更高。

6 结束语

基于硬件设备内部指纹信息的软件锁,设计方法简单,通用性强,保护强度高,既不需要专用的加密锁硬件开销,也不需要专用钥匙盘或口令等复杂操作,极大地方便了用户。

该软件锁功能设计既适用于单机版软件,也适用于网络版软件,尤其是行业或部门统一配发的软件系统。软件工程实践中,也可根据具体的应用需求,将计算机硬件设备内部指纹与软件加密算法配合使用,进一步提高钥匙密码的安全性,同时也可以配合用户软件密码设置实现对多用户的管理。

参考文献:

- [1] 邓高明,吴恒旭,张鹏,等.旁路模板在密码芯片指令分析中的应用[J].微电子学与计算机,2011,28(2):140-143.
- [2] 武春岭.基于 RSA 的广播加密方案的研究[J].制造业自动化,2011,33(12):147-149.
- [3] 宋光杰,张明慧,李晶皎.基于硬件加密的嵌入式网络通信的研究[J].电子技术应用,2010,36(1):148-150.
- [4] 周洁,慕德俊,宋利军. IPsec 加密芯片中 AES 加密核的设计与 FPGA 实现[J].测控技术,2011,30(9):60-63.
- [5] 胡向东,魏琴芳.应用密码学[M].北京:电子工业出版社,2011.
- [6] 胡伟,慕德俊,刘航,等.移动硬盘硬件加密的设计与实现[J].计算机工程与应用,2010,46(22):62-64.
- [7] 郝耀辉,刘洪波,郑礼,等.基于 USB 加密锁的软件防盗版方法[J].计算机工程,2010,36(23):119-120.
- [8] 李志伟. VB 环境下基于类的软件复用技术研究[J].计算机工程与设计,2010,31(5):1152-1155.

作者简介:

李志伟 男,(1964—),副教授,CCF 高级会员.研究方向为计算机网络与数据库技术.