(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106973054 B
(45)授权公告日 2021.03.30

(21)申请号 201710195967.3
(22)申请日 2017.03.29
(65)同一申请的已公布的文献号
申请公布号 CN 106973054 A
(43)申请公布日 2017.07.21
(73)专利权人 山东超越数控电子有限公司
地址 250104 山东省济南市高新区孙村镇科航路2877号
(72)发明人 冯磊 王晓明 朱书杉
(74)专利代理机构 北京连和连知识产权代理有限公司 11278
代理人 杨帆
(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 102315942 A,2012.01.11
CN 105426734 A,2016.03.23
CN 101771535 A,2010.07.07
CN 106127016 A,2016.11.16

审查员 王黎明

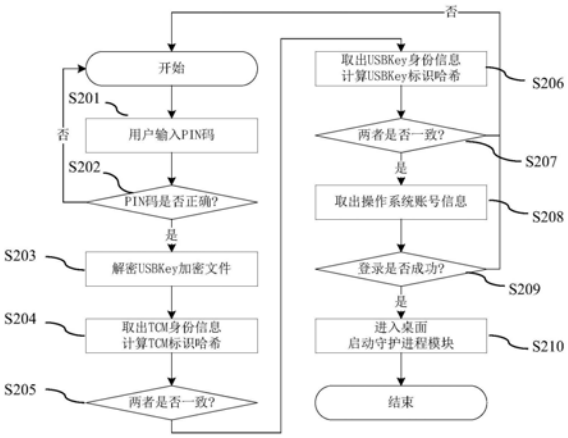
权利要求书2页 说明书4页 附图2页

(54)发明名称

一种基于可信平台的操作系统登录认证方法和系统

(57)摘要

本发明提供一种基于可信平台的操作系统登录认证方法，该方法包括以下步骤：注册USBKey并将USBKey和可信平台的TCM绑定、进行USBKey和TCM之间的双向认证以实现登录操作系统、以及实时监测USBKey是否存在。本发明还提供了一种基于可信平台的操作系统登录认证系统。本发明具有双向认证、安全性高的特点。



CN 106973054 B

1.一种基于可信平台的操作系统登录认证方法,其特征在于,所述方法包括以下步骤:

步骤一:将USBKey和可信平台的TCM彼此互相绑定;

步骤二:登录认证模块利用所述USBKey的身份标识和所述TCM的身份标识进行所述USBKey和所述TCM之间的双向认证以登录所述操作系统;

所述步骤一中的所述绑定包括以下步骤:

步骤1:分别初始化所述USBKey和所述TCM,且所述USBKey和所述TCM均未双向绑定;

步骤2:将所述USBKey的唯一标识的哈希值传送到所述TCM中;

步骤3:所述TCM接收到所述USBKey的唯一标识的所述哈希值后,将其保存在所述TCM中;然后,将所述TCM的唯一标识的哈希值传送到所述USBKey并保存在所述USBKey中;

所述步骤二包括以下步骤:

步骤1:待认证的USBKey验证用户输入的PIN码,若错误,阻止登陆;若正确,进入步骤2;

步骤2:读取所述待认证的USBKey的加密文件并解密所述加密文件,获取待认证的TCM身份信息,根据所述待认证的TCM身份信息计算出所述待认证的TCM的哈希值HTCM-待认证;

步骤3:获取所述可信平台的TCM唯一标识的哈希值HTCM,将所述HTCM-待认证与所述HTCM进行比较,若一致,进入步骤4,若不一致,中止登陆认证过程;

步骤4:根据待认证的USBKey的身份信息获取所述待认证的USBKey的哈希值HUSBKey-待认证,获取所述可信平台的TCM中存储的USBKey的唯一标识的哈希值HUSBKey,将所述HUSBKey-待认证与所述HUSBKey进行比较,若比较一致,则绑定关系正确,进入步骤5,若不一致,中止登陆认证过程;

步骤5:验证所述待认证的USBKey解密文件中的账户信息,若正确,登陆认证成功,若错误,登陆认证失败,返回登录界面;

所述方法进一步包括实时监测所述USBKey是否存在,若所述USBKey被拔出,则立刻锁定所述操作系统;若所述USBKey一直存在,则所述操作系统可被操作;其中,所述实时监测包括监听所述USBKey的拔插事件和检测所述USBKey。

2.根据权利要求1所述的基于可信平台的操作系统登录认证方法,其特征在于,在所述绑定之前进一步包括注册USBKey的步骤:输入用户名、密码、新的PIN码和旧的PIN码。

3.根据权利要求1所述的基于可信平台的操作系统登录认证方法,其特征在于,所述哈希值通过散列函数计算而获得。

4.根据权利要求1所述的基于可信平台的操作系统登录认证方法,其特征在于,所述账户信息进一步包含用户名、密码。

5.一种基于可信平台的操作系统登录认证系统,其特征在于,所述系统包含注册管理模块、与所述注册管理模块通信地连接的登录认证模块、以及与所述注册管理模块和所述登录认证模块通信地连接的守护进程模块,其中,

所述注册管理模块用于完成USBKey的注册,以及建立所述USBKey和TCM的双向绑定关系;其中,建立所述USBKey和TCM的双向绑定关系包括:

步骤1:分别初始化所述USBKey和所述TCM,且所述USBKey和所述TCM均未双向绑定;

步骤2:将所述USBKey的唯一标识的哈希值传送到所述TCM中;

步骤3:所述TCM接收到所述USBKey的唯一标识的所述哈希值后,将其保存在所述TCM中;然后,将所述TCM的唯一标识的哈希值传送到所述USBKey并保存在所述USBKey中;

所述登录认证模块用于完成所述USBKey和所述TCM之间的双向认证，从而实现登录所述操作系统；

所述守护进程模块用于实时监测所述USBKey是否存在，若所述USBKey被拔出，则立刻锁定所述操作系统；

其中，所述登录认证模块用于完成所述USBKey和所述TCM之间的双向认证，从而实现登录所述操作系统具体包括：

步骤1：待认证的USBKey验证用户输入的PIN码，若错误，阻止登陆；若正确，进入步骤2；

步骤2：读取所述待认证的USBKey的加密文件并解密所述加密文件，获取待认证的TCM身份信息，根据所述待认证的TCM身份信息计算出所述待认证的TCM的哈希值HTCM-待认证；

步骤3：获取所述可信平台的TCM唯一标识的哈希值HTCM，将所述HTCM-待认证与所述HTCM进行比较，若一致，进入步骤4，若不一致，中止登陆认证过程；

步骤4：根据待认证的USBKey的身份信息获取所述待认证的USBKey的哈希值HUSBKey-待认证，获取所述可信平台的TCM中存储的USBKey的唯一标识的哈希值HUSBKey，将所述HUSBKey-待认证与所述HUSBKey进行比较，若比较一致，则绑定关系正确，进入步骤5，若不一致，中止登陆认证过程；

步骤5：验证所述待认证的USBKey解密文件中的账户信息，若正确，登陆认证成功，若错误，登陆认证失败，返回登录界面；

所述系统进一步包括实时监测所述USBKey是否存在，若所述USBKey被拔出，则立刻锁定所述操作系统；若所述USBKey一直存在，则所述操作系统可被操作；其中，所述实时监测包括监听所述USBKey的拔插事件和检测所述USBKey。

6.一种计算机可读存储介质，其上存储有计算机程序，用于实现基于可信平台的操作系统的登录认证，其特征在于，所述程序被处理器执行时实现权利要求1所述的方法的步骤。

一种基于可信平台的操作系统登录认证方法和系统

技术领域

[0001] 本发明涉及信息安全技术领域，并且更具体地涉及一种基于可信平台的操作系统登录认证方法和系统。

背景技术

[0002] 随着国产处理器的硬件性能的提升，国家对研制自主可控的国产计算机越来越重视。硬件方面，目前我国拥有多种自主研制的CPU(中央处理器(Central Processing Unit))(例如，龙芯、飞腾、申威)，也拥有研制相应主板的核心技术和成熟工艺，更兼有TCM(Trusted Cryptography Module，可信密码模块)这一核心国家安全可信部件。另外，一些计算机的其他部件(如内存、硬盘)也早已国产化。软件方面，已有自主研制的BIOS(基本输入输出系统(Basic Input Output System))(例如，昆仑固件)。以中标麒麟为首的国产操作系统提供了windows的替代品，其上的国产软件也逐渐丰富起来。

[0003] 虽然自主可控的软硬件平台杜绝了Intel x86系列计算机的安全后门，但是我国的计算机安全防护技术仍然十分薄弱。以可信技术为支撑的安全可控软硬件技术正逐步发展起来，已成为我国个人终端抵御外界入侵的天然屏障。

[0004] 主流计算机操作系统主要是Uinx/Linux操作系统和Windows操作系统，但是两者采用的用户登录认证方式并不相同。其中Uinx/Linux操作系统的用户登录认证方式采用账号/口令的方案，用户提供正确的账号和口令后，系统才能确定他的合法身份。而Windows操作系统的本地登录主要采用交互式身份认证过程。两者都存在确认用户身份的口令简单、单向鉴别的不安全因素。

发明内容

[0005] 针对上述现有技术中存在的问题，本发明的目的在于提供一种基于可信平台的操作系统登录认证方法和系统，基于可信计算平台，利用TCM的身份标识和USBKey的身份标识实现双向身份认证，大大提高了操作系统登录认证的安全性。

[0006] 为了实现上述目的，本发明采用的技术方案如下：

[0007] 一种基于可信平台的操作系统登录认证方法，方法包括以下步骤：

[0008] 步骤一：将USBKey和可信平台的TCM彼此互相绑定；

[0009] 步骤二：利用USBKey的身份标识和TCM的身份标识进行USBKey和TCM之间的双向认证以登录操作系统。

[0010] 进一步地，方法进一步包括实时监测USBKey是否存在，若USBKey被拔出，则立刻锁定操作系统；若USBKey一直存在，则操作系统可被操作。

[0011] 进一步地，步骤一中的绑定包括以下步骤：

[0012] 步骤1：分别初始化USBKey和TCM；

[0013] 步骤2：将USBKey的唯一标识的哈希值传送到TCM中；

[0014] 步骤3：TCM接收到USBKey的唯一标识的哈希值后，将其保存在TCM中；然后，将TCM

的唯一标识的哈希值传送到USBKey并保存在USBKey中。

[0015] 进一步地，在绑定之前进一步包括注册USBKey的步骤：输入用户名、密码、新的PIN码和旧的PIN码。

[0016] 进一步地，哈希值通过散列函数计算而获得。

[0017] 进一步地，步骤二包括以下步骤：

[0018] 步骤1：待认证的USBKey验证用户输入的PIN码，若错误，阻止登陆；若正确，进入步骤2；

[0019] 步骤2：读取待认证的USBKey的加密文件并解密加密文件，获取待认证的TCM身份信息，根据待认证的TCM身份信息计算出待认证的TCM的哈希值$H_{TCM-待认证}$；

[0020] 步骤3：获取可信平台的TCM唯一标识的哈希值H_{TCM}，将$H_{TCM-待认证}$与H_{TCM}进行比较，若一致，进入步骤4，若不一致，中止登陆认证过程；

[0021] 步骤4：根据待认证的USBKey的身份信息获取待认证的USBKey的哈希值$H_{USBKey-待认证}$，获取可信平台的TCM中存储的USBKey的唯一标识的哈希值H_{USBKey}，将$H_{USBKey-待认证}$与H_{USBKey}进行比较，若比较一致，则绑定关系正确，进入步骤5，若不一致，中止登陆认证过程；

[0022] 步骤5：验证待认证的USBKey解密文件中的账户信息，若正确，登陆认证成功，若错误，登陆认证失败，返回登录界面。

[0023] 进一步地，账户信息进一步包含用户名、密码。

[0024] 进一步地，实时监测包括监听USBKey的拔插事件和检测USBKey。

[0025] 根据本发明，还提供一种基于可信平台的操作系统登录认证系统，系统包含注册管理模块、与注册管理模块通信地连接的登录认证模块、以及与注册管理模块和登录认证模块通信地连接的守护进程模块，其中，

[0026] 注册管理模块用于完成USBKey的注册，以及建立USBKey和TCM的双向绑定关系；

[0027] 登录认证模块用于完成USBKey和TCM之间的双向认证，从而实现登录操作系统；

[0028] 守护进程模块用于实时监测USBKey是否存在，若USBKey被拔出，则立刻锁定操作系统。

[0029] 根据本发明，还提供一种计算机可读存储介质，其上存储有计算机程序(指令)，用于实现基于可信平台的操作系统的登录认证，所述程序(指令)被处理器执行以实现基于可信平台的操作系统登录认证方法的步骤。

[0030] 本发明基于安全可信技术开发，利用TCM和USBKey关键硬件，实时监测USBKey的存在，实现了登录操作系统的双向身份认证，大大提高了操作系统的安全性。

附图说明

[0031] 图1为根据本发明的一个实施例的注册管理处理流程图；

[0032] 图2为根据本发明的另一个实施例的登录认证处理流程图；

[0033] 图3为根据本发明的另一个实施例的基于可信平台的操作系统登录认证系统的结构示意图。

具体实施方式

[0034] 为了使本发明的目的、技术方案及优点更加清楚明白，下面结合附图，对本发明进

行进一步详细说明。应当理解，此处所描述的具体实施例仅用以解释本发明，并不用于限定本发明。

[0035] 图1示出了根据本发明一个实施例的注册管理处理流程图，过程开始于框S101。在框S101，在要绑定USBKey和可信平台的TCM的计算机上，用户首先输入操作系统的账号信息(例如，用户名、密码等)，然后输入新的PIN码、旧的PIN码(其目的是防止恶意注册)，并将一个经过初始化的USBKey连接到计算机终端，过程前进到框S102。在框S102，判断输入的旧的PIN码是否正确，如果输入的旧的PIN码不正确，过程结束，如果输入的旧的PIN码正确，过程前进到框S103。在框S103，将输入的用户名和密码保存到USBKey的加密文件中，过程前进到框S104。在框S104，连接到计算机终端的USBKey从可信计算平台的TCM(已初始化TCM)获取TCM的唯一标识的哈希值，并将该哈希值保存在USBKey的加密文件中，该哈希值通过散列函数从TCM的唯一标识计算而获得，过程前进到框S105。在框S105，USBKey将自己的唯一标识的哈希值传送到TCM并保存在TCM的flash区域中，至此，完成了USBKey和TCM的彼此相互绑定，其他非法的USBKey无法通过双向认证。首次绑定过程结束。本领域技术人员应当理解的是绑定的前提条件是：USBKey、TCM均被软件初始化，且尚未双向绑定。

[0036] 图2示出了根据本发明的另一个示例的登录认证处理流程图，过程开始于框S201。在框S201，用户通过登录界面输入PIN码，过程前进到框S202。在框S202，登录认证模块会将PIN码传送到待认证的USBKey，待认证的USBKey验证PIN码的正确性，若PIN码错误，则登录认证模块将阻止用户登录系统，否则，过程前进到框S203。在框S203，登录认证模块从待认证的USBKey中读取加密文件，并解密该加密文件，过程前进到框S204。在框S204，待认证的USBKey从经过解密的文件中获取操作系统的账号、密码、待认证的TCM身份信息等，并根据待认证的TCM身份信息中的信息计算待认证的TCM的哈希值$H_{TCM-待认证}$，过程前进到框S205。在框S205，获取可信平台的TCM唯一标识的哈希值H_{TCM}，将$H_{TCM-待认证}$与H_{TCM}进行比较，如果二者不一致，则过程结束，如果二者一致，则过程前进到框S206。在框S206，根据待认证的USBKey的身份信息获取待认证的USBKey的哈希值$H_{USBKey-待认证}$，获取可信平台的TCM中存储的USBKey的唯一标识的哈希值H_{USBKey}，过程前进到框S207。在框S207，将$H_{USBKey-待认证}$与H_{USBKey}进行比较，如果二者不一致，则过程结束，如果二者一致，则过程前进到框S208。在框S208，登录认证模块使用从框S204中获取的操作系统的账号和密码，尝试登录操作系统，过程前进到框S209。在框S209，用户名和密码的正确性由操作系统来完成，如果不正确，则过程结束，如果正确，过程前进到框S210。在框S210，进入操作系统的桌面环境并启动守护进程模块。至此，登陆认证过程结束。

[0037] 图3示出了根据本发明的另一个实施例的基于可信平台的操作系统登录认证系统的结构示意图。如图3所示，该系统包含注册管理模块、登录认证模块和守护进程模块，其中登录认证模块与注册管理模块通信地连接，守护进程模块与注册管理模块和登录认证模块各自通信地连接。注册管理模块用于完成USBKey的注册，以及建立USBKey和TCM的彼此双向绑定关系；登录认证模块用于完成USBKey和TCM之间的双向认证从而实现登录操作系统；守护进程模块用于实时监测USBKey是否存在，一旦监测到USBKey被拔出，则立刻锁定操作系统的桌面环境，若监测到USBKey一直存在，则操作系统的桌面环境一直处于激活状态，换句话说，如果监测到USBKey一直存在，则操作系统的桌面环境一直可以被操作。

[0038] 关于这里所述的过程、系统、方法等，应理解的是虽然这样的过程等的步骤描述为

按照一定的顺序排列发生，但这样的过程可以采用以这里描述的顺序之外的顺序完成的描述的步骤实施操作。进一步应该理解的是，某些步骤可以同时执行，可以添加其他步骤，或者可以省略这里所述的某些步骤。换言之，这里的过程的描述提供用于说明某些实施例的目的，并且不应该以任何方式解释为限制要求保护的发明。

[0039] 相应地，应理解的是上面的描述的目的是说明而不是限制。在阅读上面的描述时，除了提供的示例外许多实施例和应用都是显而易见的。本发明的范围应参照所附权利要求以及与权利要求所要求的权利等效的全部范围而确定，而不是参照上面的说明而确定。可以预期的是这里所讨论的领域将出现进一步的发展，并且所公开的系统和方法将可以结合到这样的未来的实施例中。总之，应理解的是本发明能够进行修正和变化。

[0040] 还应当理解的是，任何所述的过程或所述过程中的步骤可以与其它公开的过程或步骤组合以形成本公开范围内的结构。本文公开的示例性结构、和过程是为了说明的目的，而不应被解释为限制。

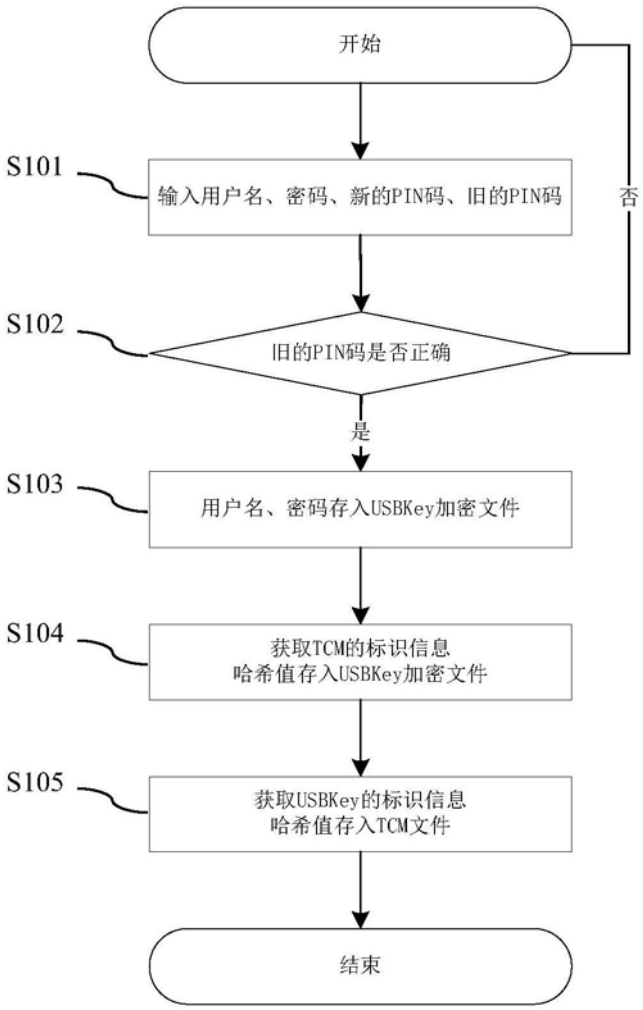

开始
S101
输入用户名、密码、新的PIN码、旧的PIN码
S102
旧的PIN码是否正确
否
是
S103
用户名、密码存入USBKey加密文件
S104
获取TCM的标识信息
哈希值存入USBKey加密文件
S105
获取USBKey的标识信息
哈希值存入TCM文件
结束

图1

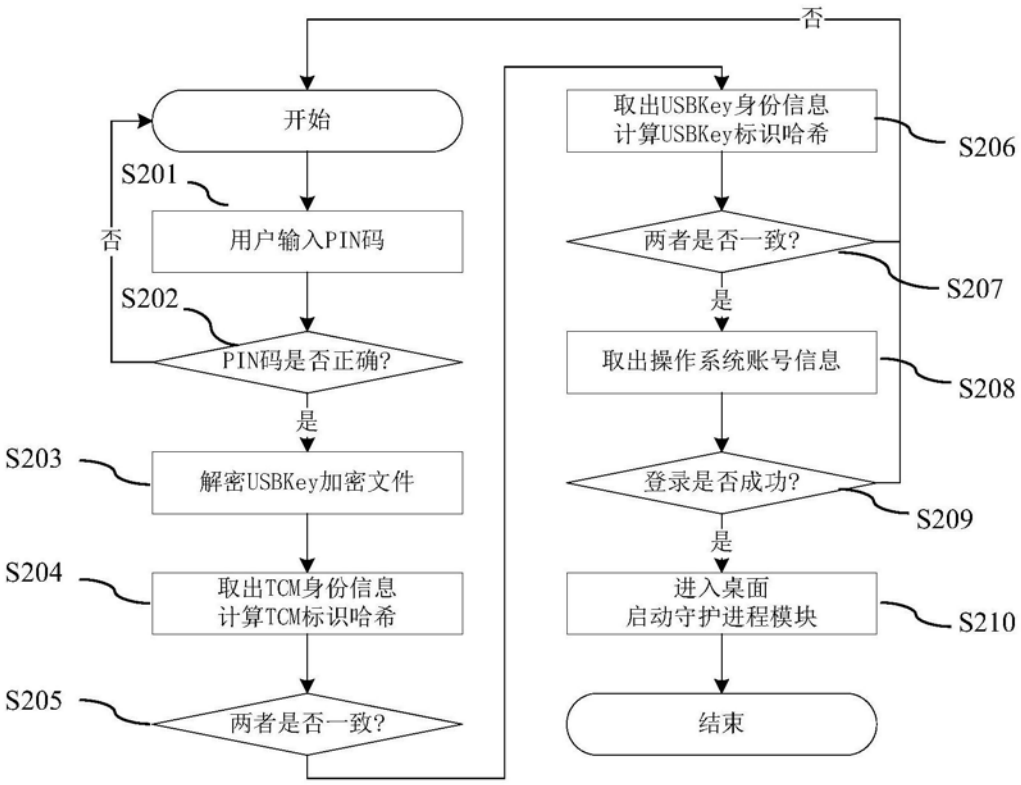

开始
S201
用户输入PIN码
否
S202
PIN码是否正确?
是
S203
解密USBKey加密文件
S204
取出TCM身份信息
计算TCM标识哈希
S205
两者是否一致?
否
取出USBKey身份信息
计算USBKey标识哈希
S206
两者是否一致?
S207
是
取出操作系统账号信息
S208
登录是否成功?
S209
是
进入桌面
启动守护进程模块
S210
结束

图2

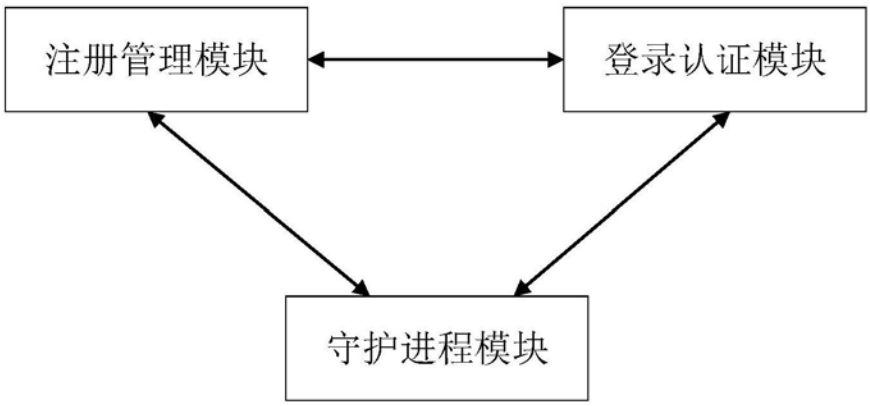

注册管理模块
登录认证模块
守护进程模块

图3