

(19) 中华人民共和国国家知识产权局



(12) 发明专利申请

(10) 申请公布号 CN 105160240 A

(43) 申请公布日 2015. 12. 16

(21) 申请号 201510428995. 6

(51) Int. Cl.

(22) 申请日 2012. 09. 20

G06F 21/46(2013. 01)

(62) 分案原申请数据

201210353634. 6 2012. 09. 20

(71) 申请人 北京奇虎科技有限公司

地址 100088 北京市西城区新街口外大街
28 号 D 座 112 室(德胜园区)

申请人 奇智软件(北京)有限公司

(72) 发明人 邓振波 苏云琳 黄鉴廷 燕晓龙

(74) 专利代理机构 北京润泽恒知识产权代理有
限公司 11319

代理人 苏培华

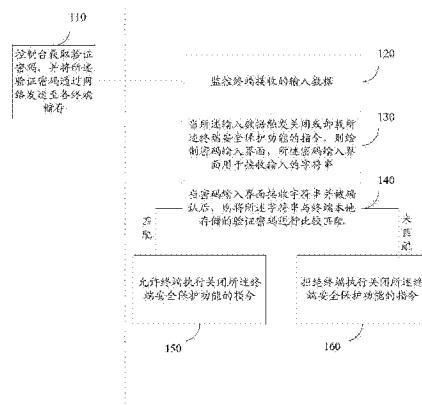
权利要求书2页 说明书12页 附图4页

(54) 发明名称

一种终端密码保护方法和装置

(57) 摘要

本申请提供了及一种终端密码保护方法和系统,涉及计算机技术领域。所述方法包括:控制台获取验证密码,并将所述验证密码通过网络发送至各终端储存;在存储所述验证密码后的终端,进行密码保护的过程包括:监控终端接收的输入数据;当所述输入数据触发关闭或卸载所述终端安全保护功能的指令,则绘制密码输入界面,所述密码输入界面用于接收输入的字符串;当密码输入界面接收字符串并被确认后,则将所述字符串与终端本地存储的验证密码进行比较匹配;如果匹配,则允许终端执行关闭所述终端安全保护功能的指令;反之,则拒绝终端执行关闭所述终端安全保护功能的指令。可以更方便的管理和把控局域网内终端的安全保护模块,提高了局域网信息安全性。



1. 一种终端密码保护的方法,包括:

控制台获取验证密码,并将所述验证密码通过网络发送至各终端储存;

在存储所述验证密码后的终端,进行密码保护的过程包括:

监控终端接收的输入数据;

当所述输入数据触发关闭或卸载所述终端安全保护功能的指令,则绘制密码输入界面,所述密码输入界面用于接收输入的字符串;

当密码输入界面接收字符串并被确认后,则将所述字符串与终端本地存储的验证密码进行比较匹配;

如果匹配上,则允许终端执行关闭所述终端安全保护功能的指令;

如果未匹配上,则拒绝终端执行关闭所述终端安全保护功能的指令。

2. 根据权利要求 1 所述的方法,在所述字符串与本地存储的验证密码匹配上之后,允许终端执行关闭或卸载所述终端安全保护功能的指令之前还包括:

所述终端将所述字符串发送至控制台;

控制台将所述字符串与本地存储的验证密码进行比较匹配。

3. 根据权利要求 1 或 2 所述的方法,所述控制台获取验证密码,并将所述验证密码通过网络发送至各终端储存包括:

控制台采用加密算法将所述验证密码进行数字签名;

将所述进行数字签名后的验证密码通过网络发送至各终端。

4. 根据权利要求 3 所述的方法,所述当密码输入界面接收字符串并被确认后,则将所述字符串与终端本地存储的验证密码进行比较匹配包括:

将所述字符串采用所述加密算法对字符串进行数字签名;

将进行数字签名后的字符串与所述进行数字签名后的验证密码进行比较匹配。

5. 根据权利要求 1 所述的方法,还包括:

预置动态链接库;当所述输入数据触发关闭所述终端安全保护功能的指令后,调用所述动态链接库执行触发关闭所述终端安全保护功能的指令后的步骤。

6. 根据权利要求 1 所述的方法,还包括:

在安全保护功能对应安全保护模块的可执行白名单中,预置第一卸载程序;所述初始卸载程序为当所述输入数据触发卸载所述终端安全保护功能的指令时启用;

进一步的,所述如果匹配上,则允许终端执行关闭所述终端安全保护功能的指令包括:

第一卸载程序调用安全保护功能对应的安全保护模块的原始卸载程序进行卸载。

7. 一种终端密码保护的方法,包括:

控制台获取并存储验证密码;

在控制台控制的终端,进行密码保护的过程包括:

监控终端接收的输入数据;

当所述输入数据触发关闭或卸载所述终端安全保护功能的指令,则绘制密码输入界面,所述密码输入界面用于接收输入的字符串;

所述终端将所述字符串发送至控制台;

控制台将所述字符串与本地存储的验证密码进行比较匹配;

如果匹配上，则允许终端执行关闭所述终端安全保护功能的指令；
如果未匹配上，则拒绝终端执行关闭所述终端安全保护功能的指令。

8. 一种终端密码保护的系统，包括：

控制台和各终端；

所述控制台包括：

验证密码发送模块，用于控制台获取验证密码，并将所述验证密码通过网络发送至各终端储存；

所述每个终端包括：

输入监控模块，用于监控终端接收的输入数据；

启动模块，用于当所述输入数据触发关闭所述终端安全保护功能的指令，则绘制密码输入界面，所述密码输入界面用于接收用户输入的字符串；

第一匹配模块，用于当密码输入界面接收字符串并被确认后，则将所述字符串与终端本地存储的验证密码进行比较匹配；

允许模块，用于如果匹配上，则允许终端执行关闭或卸载所述终端安全保护功能的指令；

拒绝模块，用于如果未匹配上，则拒绝终端执行关闭或卸载所述终端安全保护功能的指令。

9. 根据权利要求 1 所述的系统，

在每个终端中，在所述允许模块之前还包括：字符串发送模块，所述终端将所述字符串发送至控制台；

所述控制台还包括：

第二匹配模块，用于控制台将所述字符串与本地存储的验证密码进行比较匹配。

10. 一种终端密码保护的系统，包括：

控制台和各终端；

所述控制台包括：

验证密码接收模块，用于控制台获取并存储验证密码；

匹配模块，用于控制台将所述字符串与本地存储的验证密码进行比较匹配；

所述每个终端包括：

输入监控模块，用于监控终端接收的输入数据；

启动模块，用于当所述输入数据触发关闭所述终端安全保护功能的指令，则绘制密码输入界面，所述密码输入界面用于接收用户输入的字符串；

字符串发送模块，所述终端将所述字符串发送至控制台；

允许模块，用于如果匹配上，允许终端执行关闭所述终端安全保护功能的指令；

拒绝模块，用于如果未匹配上，拒绝终端执行关闭所述终端安全保护功能的指令。

一种终端密码保护方法和装置

技术领域

[0001] 本申请涉及计算机技术领域，特别是涉及一种终端密码保护方法和系统。

背景技术

[0002] 计算机网络，是指将地理位置不同的具有独立功能的多台计算机及其外部设备，通过通信线路连接起来，在网络操作系统，网络管理软件及网络通信协议的管理和协调下，实现资源共享和信息传递的计算机系统。而企业或者机构为了保证其局域网中计算机的信息安全，需要采用控制台对终端的安全软件进行统一控制，比如漏洞修复、木马查杀等等。

[0003] 现有技术中，终端可以任意将由控制台控制的安全软件进行退出或者卸载等动作，而对于企业等局域网的信息安全来说，如果终端可以随意退出、卸载与控制台交互的安全软件，则无法保证控制台对网内所有终端的控制，从而无法保证企业等局域网的信息安全。

发明内容

[0004] 鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决上述问题的一种终端密码保护系统和相应的一种终端密码保护方法。

[0005] 依据本发明的一个方面，提供了一种终端密码保护的方法，包括：

[0006] 控制台获取验证密码，并将所述验证密码通过网络发送至各终端储存；

[0007] 在存储所述验证密码后的终端，进行密码保护的过程包括：

[0008] 监控终端接收的输入数据；

[0009] 当所述输入数据触发关闭或卸载所述终端安全保护功能的指令，则绘制密码输入界面，所述密码输入界面用于接收输入的字符串；

[0010] 当密码输入界面接收字符串并被确认后，则将所述字符串与终端本地存储的验证密码进行比较匹配；

[0011] 如果匹配上，则允许终端执行关闭所述终端安全保护功能的指令；

[0012] 如果未匹配上，则拒绝终端执行关闭所述终端安全保护功能的指令。

[0013] 可选的，在所述字符串与本地存储的验证密码匹配上之后，允许终端执行关闭或卸载所述终端安全保护功能的指令之前还包括：

[0014] 所述终端将所述字符串发送至控制台；

[0015] 控制台将所述字符串与本地存储的验证密码进行比较匹配。

[0016] 可选的，所述控制台获取验证密码，并将所述验证密码通过网络发送至各终端储存包括：

[0017] 控制台采用加密算法将所述验证密码进行数字签名；

[0018] 将所述进行数字签名后的验证密码通过网络发送至各终端。

[0019] 可选的，所述当密码输入界面接收字符串并被确认后，则将所述字符串与终端本地存储的验证密码进行比较匹配包括：

- [0020] 将所述字符串采用所述加密算法对字符串进行数字签名；
- [0021] 将进行数字签名后的字符串与所述进行数字签名后的验证密码进行比较匹配。
- [0022] 可选的,还包括：
- [0023] 预置动态链接库;当所述输入数据触发关闭所述终端安全保护功能的指令后,调用所述动态链接库执行触发关闭所述终端安全保护功能的指令后的步骤。
- [0024] 可选的,还包括：
- [0025] 在安全保护功能对应安全保护模块的可执行白名单中,预置第一卸载程序;所述初始卸载程序为当所述输入数据触发卸载所述终端安全保护功能的指令时启用;
- [0026] 进一步的,所述如果匹配上,则允许终端执行关闭所述终端安全保护功能的指令包括：
- [0027] 第一卸载程序调用安全保护功能对应的安全保护模块的原始卸载程序进行卸载。
- [0028] 根据本发明的另一个方面,还提供了一种终端密码保护的方法,包括：
- [0029] 控制台获取并存储验证密码；
- [0030] 在控制台控制的终端,进行密码保护的过程包括：
- [0031] 监控终端接收的输入数据；
- [0032] 当所述输入数据触发关闭或卸载所述终端安全保护功能的指令,则绘制密码输入界面,所述密码输入界面用于接收输入的字符串；
- [0033] 所述终端将所述字符串发送至控制台；
- [0034] 控制台将所述字符串与本地存储的验证密码进行比较匹配；
- [0035] 如果匹配上,则允许终端执行关闭所述终端安全保护功能的指令；
- [0036] 如果未匹配上,则拒绝终端执行关闭所述终端安全保护功能的指令。
- [0037] 相应的,还提供了一种终端密码保护的系统,包括：
- [0038] 控制台和各终端；
- [0039] 所述控制台包括：
- [0040] 验证密码发送模块,用于控制台获取验证密码,并将所述验证密码通过网络发送至各终端储存；
- [0041] 所述每个终端包括：
- [0042] 输入监控模块,用于监控终端接收的输入数据；
- [0043] 启动模块,用于当所述输入数据触发关闭所述终端安全保护功能的指令,则绘制密码输入界面,所述密码输入界面用于接收用户输入的字符串；
- [0044] 第一匹配模块,用于当密码输入界面接收字符串并被确认后,则将所述字符串与终端本地存储的验证密码进行比较匹配；
- [0045] 允许模块,用于如果匹配上,则允许终端执行关闭或卸载所述终端安全保护功能的指令；
- [0046] 拒绝模块,用于如果未匹配上,则拒绝终端执行关闭或卸载所述终端安全保护功能的指令。
- [0047] 可选的,可选的,在每个终端中,在所述允许模块之前还包括:字符串发送模块,所述终端将所述字符串发送至控制台；
- [0048] 所述控制台还包括：

- [0049] 第二匹配模块,用于控制台将所述字符串与本地存储的验证密码进行比较匹配。
- [0050] 可选的,所述验证密码发送模块包括:
- [0051] 第一加密模块,用于控制台采用加密算法将所述验证密码进行数字签名;
- [0052] 第一发送模块,用于将所述进行数字签名后的验证密码通过网络发送至各终端。
- [0053] 可选的,所述第一匹配模块包括:
- [0054] 第二加密模块,用于将所述字符串采用所述加密算法对字符串进行数字签名;
- [0055] 第三匹配模块,用于将进行数字签名后的字符串与所述进行数字签名后的验证密码进行比较匹配。
- [0056] 可选的,还包括:
- [0057] 第一预置模块,用于预置动态链接库;当所述输入数据触发关闭所述终端安全保护功能的指令后,调用所述动态链接库执行触发关闭所述终端安全保护功能的指令后的步骤。
- [0058] 可选的,还包括:
- [0059] 第二预置模块,用于在安全保护功能对应安全保护模块的可执行白名单中,预置第一卸载程序;所述初始卸载程序为当所述输入数据触发卸载所述终端安全保护功能的指令时启用;
- [0060] 进一步的,所述允许模块包括:
- [0061] 第一卸载模块,用于第一卸载程序调用安全保护功能对应的安全保护模块的原始卸载程序进行卸载。
- [0062] 相应的,还提供了一种终端密码保护的系统,包括:
- [0063] 控制台和各终端;
- [0064] 所述控制台包括:
- [0065] 验证密码接收模块,用于控制台获取并存储验证密码;
- [0066] 匹配模块,用于控制台将所述字符串与本地存储的验证密码进行比较匹配;
- [0067] 所述每个终端包括:
- [0068] 输入监控模块,用于监控终端接收的输入数据;
- [0069] 启动模块,用于当所述输入数据触发关闭所述终端安全保护功能的指令,则绘制密码输入界面,所述密码输入界面用于接收用户输入的字符串;
- [0070] 字符串发送模块,所述终端将所述字符串发送至控制台;
- [0071] 允许模块,用于如果匹配上,允许终端执行关闭所述终端安全保护功能的指令;
- [0072] 拒绝模块,用于如果未匹配上,拒绝终端执行关闭所述终端安全保护功能的指令。
- [0073] 根据本发明的一种终端密码保护方法可以使终端在关闭或者卸载其具有安全保护功能的安全保护模块的操作时,由控制台统一管控终端的该操作行为,需要终端输入与由控制台控制的验证密码相应的解锁密码,才能进行前述操作,由此解决了终端可以任意将由控制台控制的安全软件进行退出或者卸载等动作,而对于企业等局域网的信息安全来说,如果终端可以随意退出、卸载与控制台交互的安全软件,则无法保证控制台对网内所有终端的控制,从而无法保证企业等局域网的信息安全的问题,取得了对于企业等局域网的信息安全来说,可以更方便的管理和把控局域网内终端的安全保护模块,提高了局域网信息安全性有益效果。

[0074] 上述说明仅是本发明技术方案的概述,为了能够更清楚了解本发明的技术手段,而可依照说明书的内容予以实施,并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂,以下特举本发明的具体实施方式

附图说明

[0075] 通过阅读下文优选实施方式的详细描述,各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的,而并不认为是对本发明的限制。而且在整个附图中,用相同的参考符号表示相同的部件。在附图中:

[0076] 图 1 示出了根据本发明一个实施例的一种终端密码保护的方法实施例一的流程示意图;

[0077] 图 2 示出了根据本发明一个实施例的一种终端密码保护的方法实施例二的流程示意图;

[0078] 图 3 示出了根据本发明一个实施例的一种终端密码保护的系统实施例一的流程示意图;

[0079] 图 4 示出了根据本发明一个实施例的一种终端密码保护的系统实施例二的流程示意图。

具体实施方式

[0080] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例,然而应当理解,可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反,提供这些实施例是为了能够更透彻地理解本公开,并且能够将本公开的范围完整的传达给本领域的技术人员。

[0081] 参照图 1,其示出了一种终端密码保护的方法实施例一的流程示意图,具体可以包括:

[0082] 步骤 110,控制台获取验证密码,并将所述验证密码通过网络发送至各终端储存;

[0083] 在本发明实施例中,包括控制台和各个终端,控制台可用于控制终端的安全保护模块,比如控制终端进行病毒库升级,修复漏洞,清理插件等安全功能。而在本申请中控制台可控制终端,使其不能随意关闭或者卸载终端的安全保护模块(比如杀毒软件),即控制终端不能随意关闭或者卸载其具有安全保护功能的模块。

[0084] 在本实施例中,控制台接收用户输入的验证密码,比如 123456,然后将该验证密码通过其所在网络发送至各终端,在实际中由于控制台与终端处于一封闭的局域网中,控制台可通过局域网将所述验证密码发送至终端。

[0085] 而终端在接收到所述验证密码并进行存储后,即可进入终端密码保护的过程,在终端接收到所述验证密码后可将该验证密码保存至本地在安全保护功能对应安全保护模块目录(比如杀毒软件所在目录)的 ini 文件,以便后续调用。

[0086] 可选的,在所述控制台获取验证密码,并将所述验证密码通过网络发送至各终端储存包括:

[0087] 步骤 S111,控制台采用加密算法将所述验证密码进行数字签名;

[0088] 步骤 S112,将所述进行数字签名后的验证密码通过网络发送至各终端。

[0089] 比如控制台将接收到的验证密码进行数字签名,比如对接收到的验证密码进行 MD5(Message Digest Algorithm MD5,中文名为消息摘要算法第五版)运算,然后将运算后的 MD5 值发送至终端。

[0090] 而相应的,终端则将控制台发送的数字签名后的验证密码进行存储,比如前述 MD5 值。

[0091] 在存储所述验证密码后的终端,进行密码保护的过程包括:

[0092] 步骤 120,监控终端接收的输入数据;

[0093] 对于各个终端来说,可监控其各种鼠标或键盘的输入数据,以便监控用户的鼠标或者键盘操作是否为关闭或者卸载终端的安全保护模块的操作,即用户进行的鼠标或者键盘操作是否触发关闭或卸载所述终端安全保护功能的指令。

[0094] 另外,对于触摸系统来说,则可监控用户进行触动输入的数据。

[0095] 当然对于其他输入形式,本申请也可对其进行监控。

[0096] 步骤 130,当所述输入数据触发关闭或卸载所述终端安全保护功能的指令,则绘制密码输入界面,所述密码输入界面用于接收输入的字符串;

[0097] 比如,鼠标点击退出安全保护模块的 UI(User Interface,用户界面)窗口,即触发关闭终端安全保护功能的指令;鼠标点击卸载安全保护模块的 UI(User Interface,用户界面)窗口,即触发卸载终端安全保护功能的指令,那么此时先进入密码校验过程,即首先绘制密码输入界面,以接收终端用户输入的密码。

[0098] 还比如用户通过触摸屏点击退出完全保护模块,也触发关闭或卸载所述终端安全保护功能的指令,那么绘制密码输入界面。

[0099] 步骤 140,当密码输入界面接收字符串并被确认后,则将所述字符串与终端本地存储的验证密码进行比较匹配;如果匹配上,则进入步骤 150;如果未匹配上,则转入步骤 160;

[0100] 当终端用户在密码输入界面输入待验的字符串并确认后,系统则调用前述的校验密码,将终端用户输入的待验的字符串与终端存储的校验密码进行比较匹配。比如前述终端将验证密码存储与本地目录的 ini 文件中,那么终端接收到终端用户输入的字符串并被终端用户确认输入后,提取 ini 文件中的验证密码,与所述待验证的字符串进行比较匹配;如果匹配上,则进入步骤 150,如果未匹配上则进入步骤 160。

[0101] 在前述步骤 S111 和步骤 S112 的基础之上,所述当密码输入界面接收字符串并被确认后,则将所述字符串与终端本地存储的验证密码进行比较匹配包括:

[0102] 步骤 S141,将所述字符串采用所述加密算法对字符串进行数字签名;

[0103] 步骤 S142,将进行数字签名后的字符串与所述进行数字签名后的验证密码进行比较匹配。

[0104] 比如终端对用户输入的字符进行 MD5 计算,得到 MD5 值,然后将该 MD5 值与控制台发送到终端进行存储的 MD5 值进行比较匹配,两个 MD5 值相同,则说明匹配上,转入步骤 150,如果 MD5 值不同则说明未匹配上,则转入步骤 160。

[0105] 可选的,在所述字符串与本地存储的验证密码匹配上之后,允许终端执行关闭或卸载所述终端安全保护功能的指令之前还包括:

[0106] 步骤 A11,所述终端将所述字符串发送至控制台;

- [0107] 步骤 A12, 控制台将所述字符串与本地存储的验证密码进行比较匹配。
- [0108] 步骤 A11 和步骤 A12 即将终端接收的字符串再发送至控制台, 与控制台接收的验证密码进行比较匹配。如果匹配上, 则通知终端允许执行关闭所述终端安全保护功能的指令, 即步骤 150; 如果未匹配上, 则通知终端拒绝执行关闭所述终端安全保护功能的指令, 即步骤 160。
- [0109] 对于前述步骤 S111, 那么终端可将用户输入的字符串按相同的加密算法进行数字签名后发送给控制台后, 与控制台中的签名后的验证密码进行匹配; 也可由终端将原字符串发送给控制台, 由控制台对其进行数字签名后, 再与控制台中的签名后的验证密码进行匹配。
- [0110] 步骤 150, 则允许终端执行关闭所述终端安全保护功能的指令;
- [0111] 步骤 160, 则拒绝终端执行关闭所述终端安全保护功能的指令。
- [0112] 在拒绝终端执行关闭所述终端安全保护功能的指令, 还可进入步骤 140, 即可接收用户再次输入的字符串进行匹配过程。
- [0113] 其中进一步的, 如果匹配错误次数超过阈值, 则可禁止用户再次输入字符串。
- [0114] 另外, 在本实施例中, 在本系统执行之前, 在终端还包括:
- [0115] 步骤 S50, 预置动态链接库; 当所述输入数据触发关闭所述终端安全保护功能的指令后, 调用所述动态链接库执行触发关闭所述终端安全保护功能的指令后的步骤。
- [0116] 即预置一个 DLL(Dynamic Link Library, 动态链接库)文件, 在用户的键盘或者鼠标操作触发关闭所述终端安全保护功能的指令, 则调用该 DLL 绘制密码输入界面, 并执行后续步骤 140 至步骤 160。在未匹配上时, 退出该 DLL, 调用安全保护功能对应安全保护模块原有的关闭流程, 并可退出该 DLL。
- [0117] 另外, 在本实施例中, 在本系统执行之前, 在终端还包括:
- [0118] 步骤 S60, 在安全保护功能对应安全保护模块的可执行白名单中, 预置第一卸载程序; 所述初始卸载程序为当所述输入数据触发卸载所述终端安全保护功能的指令时启用;
- [0119] 对于将安全保护功能对应安全保护模块(比如杀毒软件)进行卸载的程序, 需要安全保护模块允许其运行才可允许进行卸载, 那么需要将该卸载程序预置在安全保护模块的可执行白名单中, 在监测到鼠标和 / 或键盘的输入数据触发卸载所述终端安全保护功能的指令才可启用。
- [0120] 即通过第一卸载程序绘制密码输入界面, 接收用户输入的字符串, 并将字符串与本地存储的验证密码进行比较匹配。
- [0121] 进一步的, 所述如果匹配上, 则允许终端执行关闭所述终端安全保护功能的指令包括:
- [0122] 第一卸载程序调用安全保护功能对应的安全保护模块的原始卸载程序进行卸载。
- [0123] 在用户输入的字符串与控制台发送的验证密码匹配上后, 则可通过第一调用程序调用安全保护模块的原有卸载程序进行卸载。
- [0124] 参照图 2, 其示出了本申请一种终端密码保护的方法实施例二的流程示意图, 具体可以包括:
- [0125] 步骤 210, 控制台获取并存储验证密码;
- [0126] 在本实施例中, 可选的, 本步骤还包括:

- [0127] 步骤 B211, 将接收的验证密码采用加密算法进行数字签名后, 再进行存储。
- [0128] 在控制台控制的终端, 进行密码保护的过程包括 :
- [0129] 步骤 220, 监控终端接收的输入数据 ;
- [0130] 步骤 230, 当所述输入数据触发关闭或卸载所述终端安全保护功能的指令, 则绘制密码输入界面, 所述密码输入界面用于接收输入的字符串 ;
- [0131] 步骤 240, 所述终端将所述字符串发送至控制台 ;
- [0132] 在本实施例中, 可选的, 相应与步骤 B211, 还包括 : 步骤 B212, 将字符串采用加密算法进行数字签名后再发送至控制台。
- [0133] 步骤 250, 控制台将所述字符串与本地存储的验证密码进行比较匹配 ;
- [0134] 基于前述可选的步骤 B211 和步骤 B212, 本步骤控制台则将数字签名后的字符串与本地存储的数字签名后的验证密码进行匹配。
- [0135] 另外, 基于步骤 B211, 可选的, 还包括 : 控制台将终端发送的字符串采用所述加密算法进行数字签名 ;
- [0136] 然后再将数字签名后的字符串与本地存储的数字签名后的验证密码进行匹配。
- [0137] 步骤 260, 如果匹配上, 则允许终端执行关闭所述终端安全保护功能的指令 ;
- [0138] 步骤 270, 如果未匹配上, 则拒绝终端执行关闭所述终端安全保护功能的指令。
- [0139] 本实施例与图 1 所述实施例相似步骤原理类似, 在此不在详述。
- [0140] 参照图 3, 其示出了本申请一种终端密码保护的系统实施例一的结构示意图, 具体可以包括 :
- [0141] 控制台 310 和各终端 ;
- [0142] 所述控制台 310 包括 :
- [0143] 验证密码发送模块 311, 用于控制台获取验证密码, 并将所述验证密码通过网络发送至各终端储存 ;
- [0144] 所述每个终端 320 包括 :
- [0145] 输入监控模块 321, 用于监控终端接收的输入数据 ;
- [0146] 启动模块 322, 用于当所述输入数据触发关闭所述终端安全保护功能的指令, 则绘制密码输入界面, 所述密码输入界面用于接收用户输入的字符串 ;
- [0147] 第一匹配模块 323, 用于当密码输入界面接收字符串并被确认后, 则将所述字符串与终端本地存储的验证密码进行比较匹配 ;
- [0148] 允许模块 324, 用于如果匹配上, 则允许终端执行关闭或卸载所述终端安全保护功能的指令 ;
- [0149] 拒绝模块 325, 用于如果未匹配上, 则拒绝终端执行关闭或卸载所述终端安全保护功能的指令。
- [0150] 可选的, 在每个终端中, 在所述允许模块之前还包括 : 字符串发送模块, 所述终端将所述字符串发送至控制台 ;
- [0151] 所述控制台还包括 :
- [0152] 第二匹配模块, 用于控制台将所述字符串与本地存储的验证密码进行比较匹配。
- [0153] 可选的, 所述验证密码发送模块包括 :
- [0154] 第一加密模块, 用于控制台采用加密算法将所述验证密码进行数字签名 ;

- [0155] 第一发送模块,用于将所述进行数字签名后的验证密码通过网络发送至各终端。
- [0156] 可选的,所述第一匹配模块包括:
- [0157] 第二加密模块,用于将所述字符串采用所述加密算法对字符串进行数字签名;
- [0158] 第三匹配模块,用于将进行数字签名后的字符串与所述进行数字签名后的验证密码进行比较匹配。
- [0159] 可选的,还包括:
- [0160] 第一预置模块,用于预置动态链接库;当所述输入数据触发关闭所述终端安全保护功能的指令后,调用所述动态链接库执行触发关闭所述终端安全保护功能的指令后的步骤。
- [0161] 可选的,还包括:
- [0162] 第二预置模块,用于在安全保护功能对应安全保护模块的可执行白名单中,预置第一卸载程序;所述初始卸载程序为当所述输入数据触发卸载所述终端安全保护功能的指令时启用;
- [0163] 进一步的,所述允许模块包括:
- [0164] 第一卸载模块,用于第一卸载程序调用安全保护功能对应的安全保护模块的原始卸载程序进行卸载。
- [0165] 参照图4,其示出了本申请一种终端密码保护的系统实施例二的结构示意图,具体可以包括:
- [0166] 控制台410和各终端;
- [0167] 所述控制台410包括:
- [0168] 验证密码接收模块411,用于控制台获取并存储验证密码;
- [0169] 匹配模块412,用于控制台将所述字符串与本地存储的验证密码进行比较匹配;对于匹配结果,可将其发送至终端。
- [0170] 所述每个终端420包括:
- [0171] 输入监控模块421,用于监控终端接收的输入数据;
- [0172] 启动模块422,用于当所述输入数据触发关闭所述终端安全保护功能的指令,则绘制密码输入界面,所述密码输入界面用于接收用户输入的字符串;
- [0173] 字符串发送模块423,所述终端将所述字符串发送至控制台;
- [0174] 允许模块424,用于如果匹配上,则允许终端执行关闭所述终端安全保护功能的指令;
- [0175] 拒绝模块425,用于如果未匹配上,则拒绝终端执行关闭所述终端安全保护功能的指令。
- [0176] 图3实施例与图1方法实施例对应,图4实施例与图2方法实施例对应,在此不再详述。
- [0177] 在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述,构造这类系统所要求的结构是显而易见的。此外,本发明也不针对任何特定编程语言。应当明白,可以利用各种编程语言实现在此描述的本发明的内容,并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

[0178] 在此处所提供的说明书中,说明了大量具体细节。然而,能够理解,本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中,并未详细示出公知的方法、结构和技术,以便不模糊对本说明书的理解。

[0179] 类似地,应当理解,为了精简本公开并帮助理解各个发明方面中的一个或多个,在上面对本发明的示例性实施例的描述中,本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而,并不应将该公开的方法解释成反映如下意图:即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说,如下面的权利要求书所反映的那样,发明方面在于少于前面公开的单个实施例的所有特征。因此,遵循具体实施方式的权利要求书由此明确地并入该具体实施方式,其中每个权利要求本身都作为本发明的单独实施例。

[0180] 本领域那些技术人员可以理解,可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件,以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和 / 或过程或者单元中的至少一些是相互排斥之外,可以采用任何组合对本说明书(包括伴随的权利要求、摘要和附图)中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述,本说明书(包括伴随的权利要求、摘要和附图)中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0181] 此外,本领域的技术人员能够理解,尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征,但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如,在下面的权利要求书中,所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0182] 本发明的各个部件实施例可以以硬件实现,或者以在一个或者多个处理器上运行的软件模块实现,或者以它们的组合实现。本领域的技术人员应当理解,可以在实践中使用微处理器或者数字信号处理器(DSP)来实现根据本发明实施例的一种终端密码保护设备中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序(例如,计算机程序和计算机程序产品)。这样的实现本发明的程序可以存储在计算机可读介质上,或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到,或者在载体信号上提供,或者以任何其他形式提供。

[0183] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制,并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中,不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中,这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

[0184] 本发明公开了 A1、一种终端密码保护的方法,包括:

- [0185] 控制台获取验证密码，并将所述验证密码通过网络发送至各终端储存；
- [0186] 在存储所述验证密码后的终端，进行密码保护的过程包括：
 - [0187] 监控终端接收的输入数据；
 - [0188] 当所述输入数据触发关闭或卸载所述终端安全保护功能的指令，则绘制密码输入界面，所述密码输入界面用于接收输入的字符串；
 - [0189] 当密码输入界面接收字符串并被确认后，则将所述字符串与终端本地存储的验证密码进行比较匹配；
 - [0190] 如果匹配上，则允许终端执行关闭所述终端安全保护功能的指令；
 - [0191] 如果未匹配上，则拒绝终端执行关闭所述终端安全保护功能的指令。
- [0192] A2、如 A1 所述的方法，在所述字符串与本地存储的验证密码匹配上之后，允许终端执行关闭或卸载所述终端安全保护功能的指令之前还包括：
 - [0193] 所述终端将所述字符串发送至控制台；
 - [0194] 控制台将所述字符串与本地存储的验证密码进行比较匹配。
- [0195] A3、如 A1 或 A2 所述的方法，所述控制台获取验证密码，并将所述验证密码通过网络发送至各终端储存包括：
 - [0196] 控制台采用加密算法将所述验证密码进行数字签名；
 - [0197] 将所述进行数字签名后的验证密码通过网络发送至各终端。
- [0198] A4、如 A3 所述的方法，所述当密码输入界面接收字符串并被确认后，则将所述字符串与终端本地存储的验证密码进行比较匹配包括：
 - [0199] 将所述字符串采用所述加密算法对字符串进行数字签名；
 - [0200] 将进行数字签名后的字符串与所述进行数字签名后的验证密码进行比较匹配。
- [0201] A5、如 A1 所述的方法，还包括：
 - [0202] 预置动态链接库；当所述输入数据触发关闭所述终端安全保护功能的指令后，调用所述动态链接库执行触发关闭所述终端安全保护功能的指令后的步骤。
 - [0203] A6、如 A1 所述的方法，还包括：
 - [0204] 在安全保护功能对应安全保护模块的可执行白名单中，预置第一卸载程序；所述初始卸载程序为当所述输入数据触发卸载所述终端安全保护功能的指令时启用；
 - [0205] 进一步的，所述如果匹配上，则允许终端执行关闭所述终端安全保护功能的指令包括：
 - [0206] 第一卸载程序调用安全保护功能对应的安全保护模块的原始卸载程序进行卸载。
 - [0207] B7、一种终端密码保护的方法，包括：
 - [0208] 控制台获取并存储验证密码；
 - [0209] 在控制台控制的终端，进行密码保护的过程包括：
 - [0210] 监控终端接收的输入数据；
 - [0211] 当所述输入数据触发关闭或卸载所述终端安全保护功能的指令，则绘制密码输入界面，所述密码输入界面用于接收输入的字符串；
 - [0212] 所述终端将所述字符串发送至控制台；
 - [0213] 控制台将所述字符串与本地存储的验证密码进行比较匹配；
 - [0214] 如果匹配上，则允许终端执行关闭所述终端安全保护功能的指令；

- [0215] 如果未匹配上，则拒绝终端执行关闭所述终端安全保护功能的指令。
- [0216] C8、一种终端密码保护的系统，包括：
- [0217] 控制台和各终端；
- [0218] 所述控制台包括：
- [0219] 验证密码发送模块，用于控制台获取验证密码，并将所述验证密码通过网络发送至各终端储存；
- [0220] 所述每个终端包括：
- [0221] 输入监控模块，用于监控终端接收的输入数据；
- [0222] 启动模块，用于当所述输入数据触发关闭所述终端安全保护功能的指令，则绘制密码输入界面，所述密码输入界面用于接收用户输入的字符串；
- [0223] 第一匹配模块，用于当密码输入界面接收字符串并被确认后，则将所述字符串与终端本地存储的验证密码进行比较匹配；
- [0224] 允许模块，用于如果匹配上，则允许终端执行关闭或卸载所述终端安全保护功能的指令；
- [0225] 拒绝模块，用于如果未匹配上，则拒绝终端执行关闭或卸载所述终端安全保护功能的指令。
- [0226] C9、如C1所述的系统，
- [0227] 在每个终端中，在所述允许模块之前还包括：字符串发送模块，所述终端将所述字符串发送至控制台；
- [0228] 所述控制台还包括：
- [0229] 第二匹配模块，用于控制台将所述字符串与本地存储的验证密码进行比较匹配。
- [0230] C10、如C8或C9所述的系统，所述验证密码发送模块包括：
- [0231] 第一加密模块，用于控制台采用加密算法将所述验证密码进行数字签名；
- [0232] 第一发送模块，用于将所述进行数字签名后的验证密码通过网络发送至各终端。
- [0233] C11、如C8所述的系统，所述第一匹配模块包括：
- [0234] 第二加密模块，用于将所述字符串采用所述加密算法对字符串进行数字签名；
- [0235] 第三匹配模块，用于将进行数字签名后的字符串与所述进行数字签名后的验证密码进行比较匹配。
- [0236] C12、如C8所述的系统，还包括：
- [0237] 第一预置模块，用于预置动态链接库；当所述输入数据触发关闭所述终端安全保护功能的指令后，调用所述动态链接库执行触发关闭所述终端安全保护功能的指令后的步骤。
- [0238] C13、如C8所述的系统，还包括：
- [0239] 第二预置模块，用于在安全保护功能对应安全保护模块的可执行白名单中，预置第一卸载程序；所述初始卸载程序为当所述输入数据触发卸载所述终端安全保护功能的指令时启用；
- [0240] 进一步的，所述允许模块包括：
- [0241] 第一卸载模块，用于第一卸载程序调用安全保护功能对应的安全保护模块的原始卸载程序进行卸载。

- [0242] D14、一种终端密码保护的系统,包括:
 - [0243] 控制台和各终端;
 - [0244] 所述控制台包括:
 - [0245] 验证密码接收模块,用于控制台获取并存储验证密码;
 - [0246] 匹配模块,用于控制台将所述字符串与本地存储的验证密码进行比较匹配;
 - [0247] 所述每个终端包括:
 - [0248] 输入监控模块,用于监控终端接收的输入数据;
 - [0249] 启动模块,用于当所述输入数据触发关闭所述终端安全保护功能的指令,则绘制密码输入界面,所述密码输入界面用于接收用户输入的字符串;
 - [0250] 字符串发送模块,所述终端将所述字符串发送至控制台;
 - [0251] 允许模块,用于如果匹配上,允许终端执行关闭所述终端安全保护功能的指令;
 - [0252] 拒绝模块,用于如果未匹配上,拒绝终端执行关闭所述终端安全保护功能的指令。

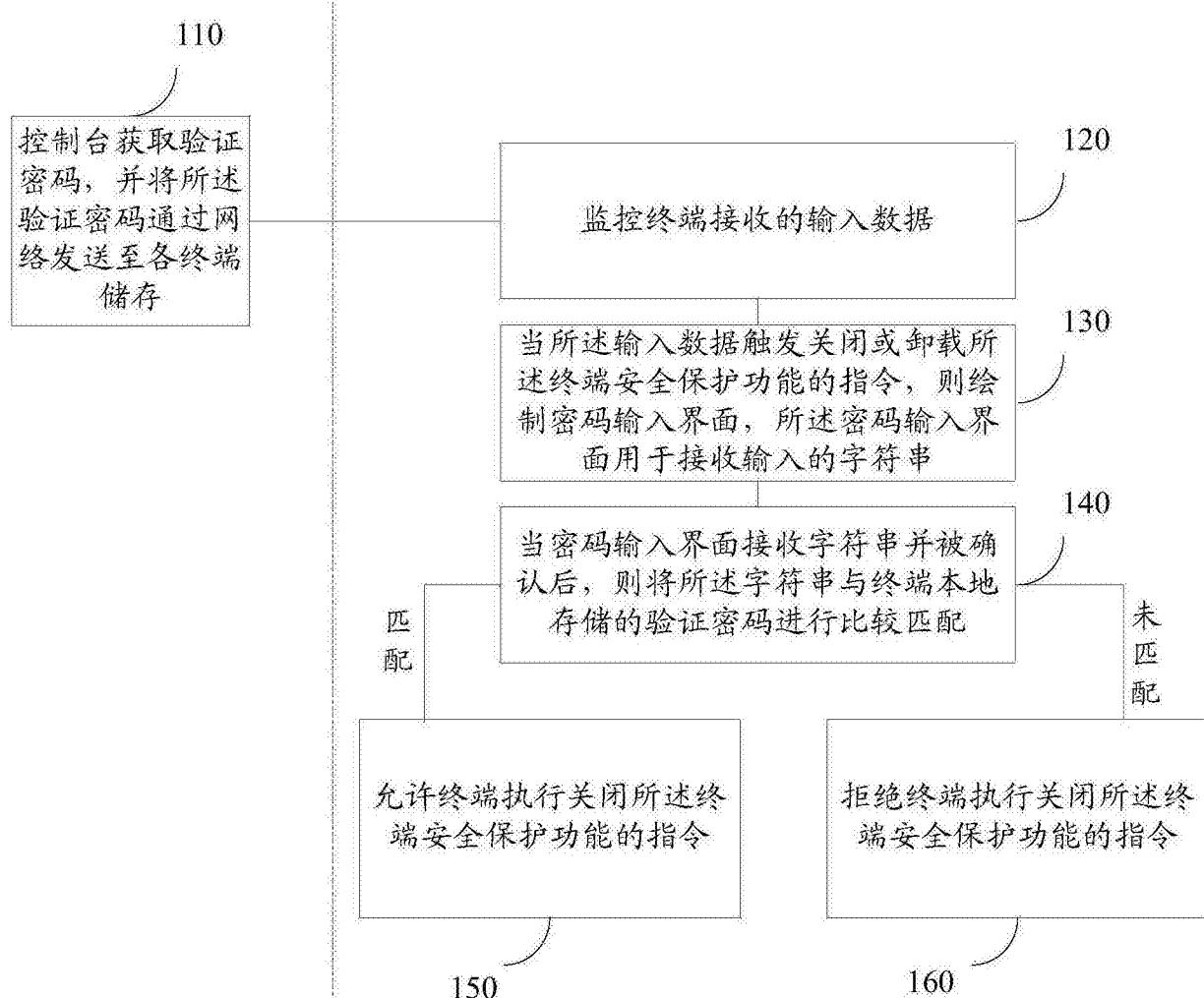


图 1

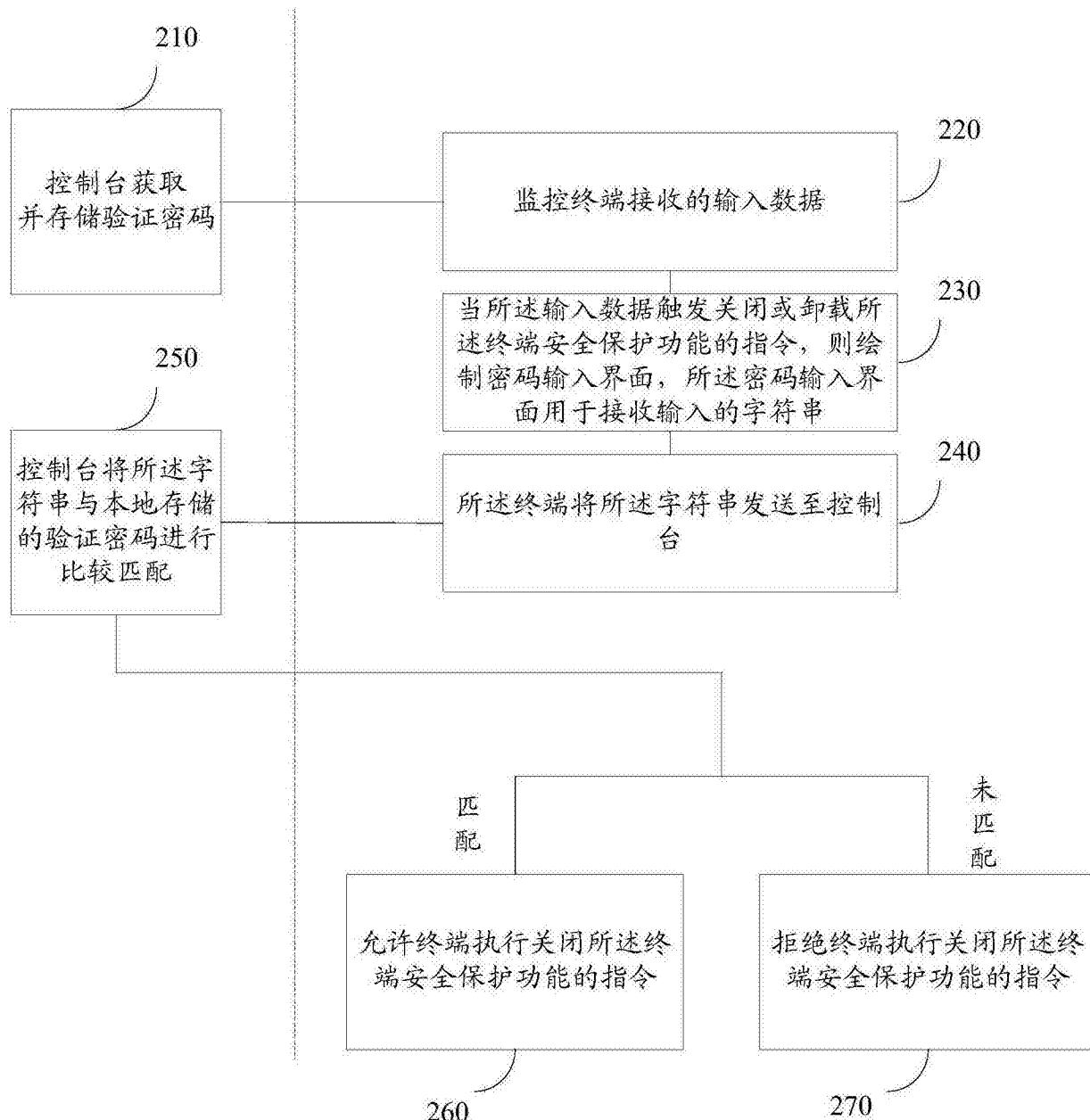


图 2

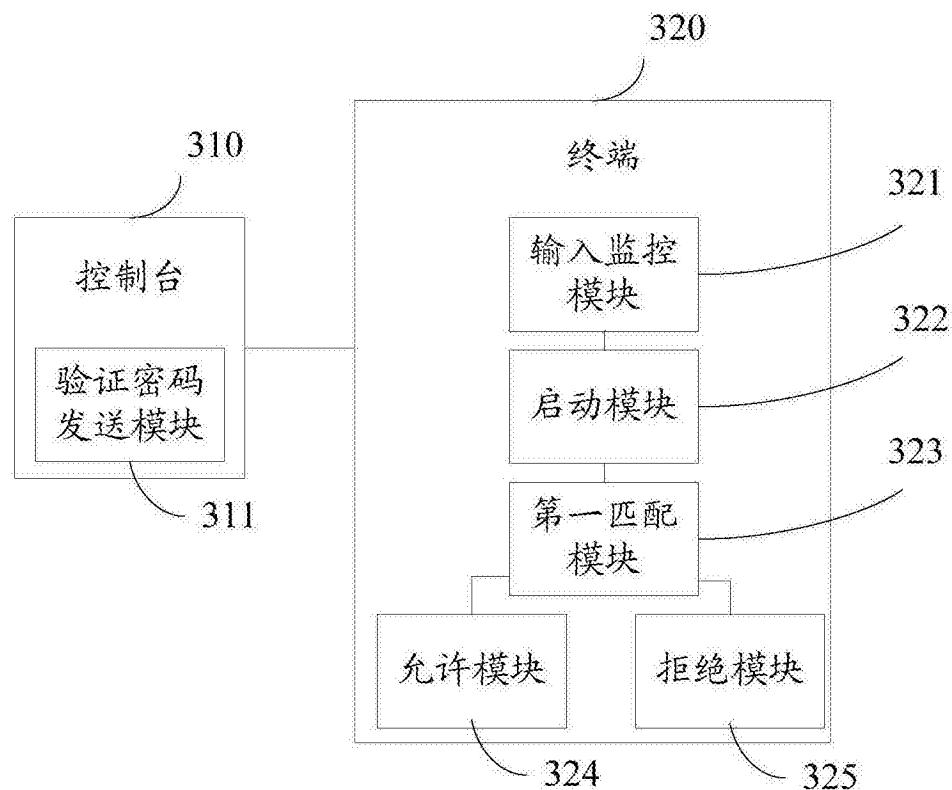


图 3

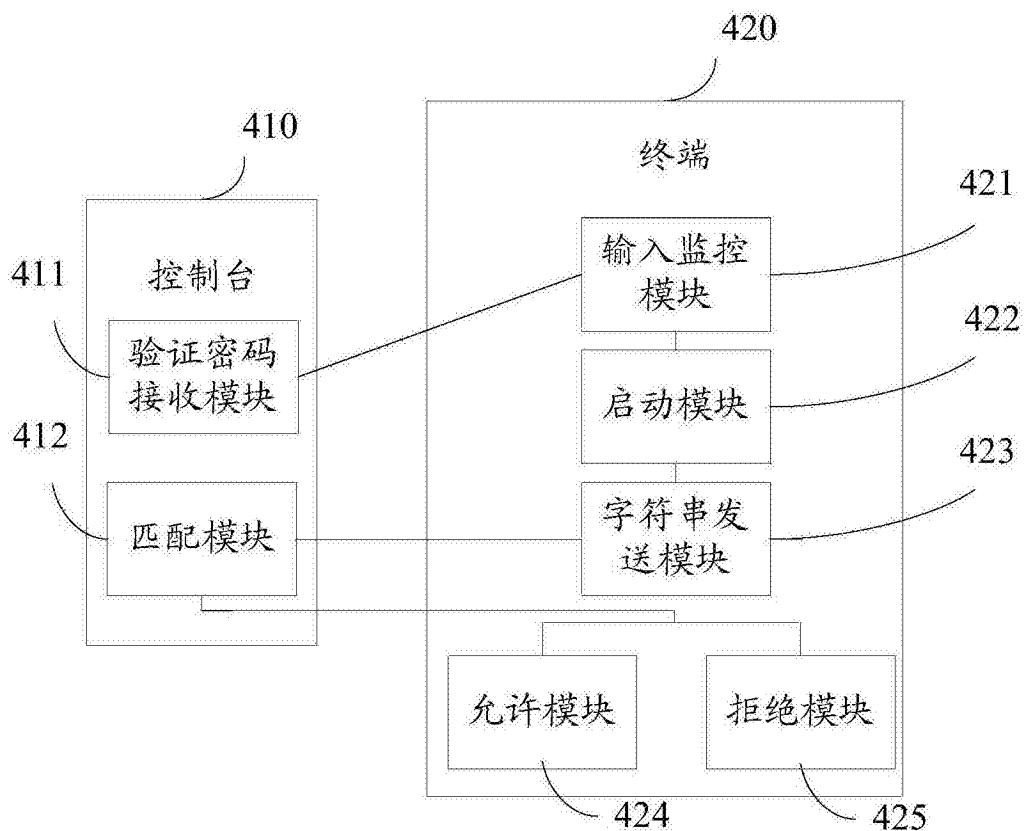


图 4