



(12) 发明专利申请

(10) 申请公布号 CN 114553609 A

(43) 申请公布日 2022. 05. 27

(21) 申请号 202210444037.8

(22) 申请日 2022.04.24

(71) 申请人 北京圣博润高新技术股份有限公司
地址 100089 北京市海淀区知春路56号西
区64楼第七层711房间

(72) 发明人 黄勇 操飞飞 王霄 于洋
王志彪

(51) Int.Cl.
H04L 9/40 (2022.01)

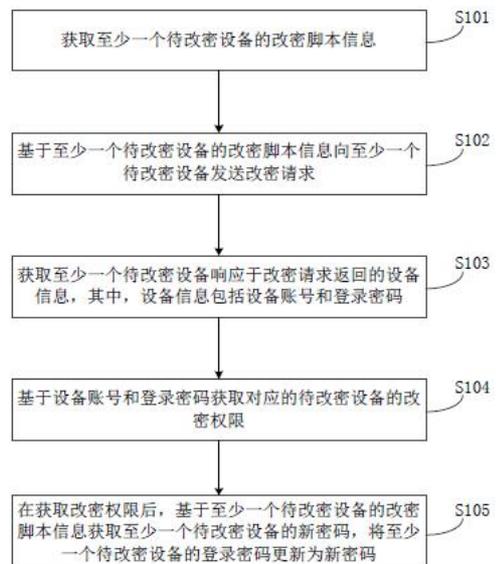
权利要求书2页 说明书7页 附图2页

(54) 发明名称

基于Linux的远程设备账号改密方法、装置、设备及介质

(57) 摘要

本申请涉及一种基于Linux的远程设备账号改密方法、装置、设备及介质,应用于信息安全技术领域,其方法包括:获取至少一个待改密设备的改密脚本信息;基于所述至少一个待改密设备的改密脚本信息向所述至少一个待改密设备发送改密请求;获取所述至少一个待改密设备响应于所述改密请求返回的设备信息,其中,所述设备信息包括设备账号和登录密码;基于所述设备账号和所述登录密码获取对应的待改密设备的改密权限;在获取改密权限后,基于所述至少一个待改密设备的改密脚本信息获取所述至少一个待改密设备的新密码,将所述至少一个待改密设备的登录密码更新为所述新密码。本申请具有提高密码的修改效率的效果。



1. 一种基于Linux的远程设备账号改密方法,其特征在于,包括:
 - 获取至少一个待改密设备的改密脚本信息;
 - 基于所述至少一个待改密设备的改密脚本信息向所述至少一个待改密设备发送改密请求;
 - 获取所述至少一个待改密设备响应于所述改密请求返回的设备信息,其中,所述设备信息包括设备账号和登录密码;
 - 基于所述设备账号和所述登录密码获取对应的待改密设备的改密权限;
 - 在获取改密权限后,基于所述至少一个待改密设备的改密脚本信息获取所述至少一个待改密设备的新密码,将所述至少一个待改密设备的登录密码更新为所述新密码。
2. 根据权利要求1所述的方法,其特征在于,所述改密脚本信息包括请求发送方式;所述基于所述至少一个待改密设备的改密脚本信息向所述至少一个待改密设备发送改密请求包括:
 - 若所述请求发送方式为手动发送,则响应于管理员的发送指令,向所述至少一个待改密设备发送改密请求;
 - 若所述请求发送方式为自动发送,则获取预设改密周期,并基于所述预设改密周期向所述至少一个待改密设备发送改密请求。
3. 根据权利要求2所述的方法,其特征在于,在所述获取所述至少一个待改密设备返回的设备信息之前,还包括:
 - 接收所述至少一个待改密设备返回的响应信息;
 - 若所述响应信息包含改密允许信息,则执行所述获取所述至少一个待改密设备返回的设备信息的步骤。
4. 根据权利要求1至3任一项所述的方法,其特征在于,所述改密脚本信息包括密码生成规则;所述基于所述至少一个待改密设备的改密脚本信息获取所述至少一个待改密设备的新密码包括:
 - 基于所述密码生成规则生成所述新密码。
5. 根据权利要求1所述的方法,其特征在于,所述获取至少一个待改密设备的改密脚本信息包括:
 - 获取所述至少一个待改密设备的远程协议;
 - 基于所述远程协议配置所述改密脚本信息;
 - 绑定与配置后的改密脚本信息匹配的所述至少一个待改密设备,并生成脚本绑定信息。
6. 根据权利要求5所述的方法,其特征在于,所述基于所述至少一个待改密设备的改密脚本信息向所述至少一个待改密设备发送改密请求包括:
 - 通过Redis监听所述脚本绑定信息,则允许向所述至少一个改密设备发送改密请求。
7. 根据权利要求1所述的方法,其特征在于,在所述将所述新密码更新为所述至少一个待改密设备的登录密码之后,还包括:
 - 生成并发送包含所述新密码的提示信息,所述提示信息用于提示所述待改密设备的使用者改密成功。
8. 一种基于Linux的远程设备账号改密装置,其特征在于,包括:

脚本获取模块,用于获取至少一个待改密设备的改密脚本信息;

改密请求模块,用于基于所述至少一个待改密设备的改密脚本信息向所述至少一个待改密设备发送改密请求;

信息获取模块,用于获取所述至少一个待改密设备响应于所述改密请求返回的设备信息,其中,所述设备信息包括设备账号和登录密码;

账号登录模块,用于基于所述设备账号和所述登录密码获取对应的待改密设备的改密权限;

密码修改模块,用于在获取改密权限后,基于所述至少一个待改密设备的改密脚本信息获取所述至少一个待改密设备的新密码,将所述至少一个待改密设备的登录密码更新为所述新密码。

9. 一种电子设备,其特征在于,包括存储器和处理器,所述存储器上存储有能够被所述处理器加载并执行如权利要求1至7中任一种所述的基于Linux的远程设备账号改密方法的计算机程序。

10. 一种计算机可读存储介质,其特征在于,存储有能够被处理器加载并执行如权利要求1至7中任一种所述的基于Linux的远程设备账号改密方法的计算机程序。

基于Linux的远程设备账号改密方法、装置、设备及介质

技术领域

[0001] 本申请涉及信息安全的技术领域,尤其是涉及一种基于Linux的远程设备账号改密方法、装置、设备及介质。

背景技术

[0002] 在使用Linux系统对远程设备的进行改密时,在客户端登录PAM账号,并通过Telnet协议或者SSH协议或者RDP协议连接待改密设备,从而对远程设备进行改密。

[0003] 但传统的远程设备改密一般需要管理员手动对每一个待改密账号进行改密,由于账号数量庞大,管理员手动改密耗时长并且效率低。

发明内容

[0004] 为了提高密码的修改效率,本申请提供一种基于Linux的远程设备账号改密方法、装置、设备及介质。

[0005] 第一方面,本申请提供一种基于Linux的远程设备账号改密方法,采用如下的技术方案:

一种基于Linux的远程设备账号改密方法,包括:

获取至少一个待改密设备的改密脚本信息;

基于所述至少一个待改密设备的改密脚本信息向所述至少一个待改密设备发送改密请求;

获取所述至少一个待改密设备响应于所述改密请求返回的设备信息,其中,所述设备信息包括设备账号和登录密码;

基于所述设备账号和所述登录密码获取对应的待改密设备的改密权限;

在获取改密权限后,基于所述至少一个待改密设备的改密脚本信息获取所述至少一个待改密设备的新密码,将所述至少一个待改密设备的登录密码更新为所述新密码。

[0006] 通过采用上述技术方案,同时向多个待改密设备发送改密请求,并同时登陆多个待改密设备,基于改密脚本信息修改多个待改密设备的登录密码,达到对多个待改密设备批量改密的效果,从而提高密码的修改效率。

[0007] 可选的,所述改密脚本信息包括请求发送方式;所述基于所述至少一个待改密设备的改密脚本信息向所述至少一个待改密设备发送改密请求包括:

若所述请求发送方式为手动发送,则响应于管理员的发送指令,向所述至少一个待改密设备发送改密请求;

若所述请求发送方式为自动发送,则获取预设改密周期,并基于所述预设改密周期向所述至少一个待改密设备发送改密请求。

[0008] 可选的,在所述获取所述至少一个待改密设备返回的设备信息之前,还包括:

接收所述至少一个待改密设备返回的响应信息;

若所述响应信息包含改密允许信息,则执行所述获取所述至少一个待改密设备返

回的设备信息的步骤。

[0009] 可选的,所述改密脚本信息包括密码生成规则;所述基于所述至少一个待改密设备的改密脚本信息获取所述至少一个待改密设备的新密码包括:

基于所述密码生成规则生成所述新密码。

[0010] 可选的,所述获取至少一个待改密设备的改密脚本信息包括:

获取所述至少一个待改密设备的远程协议;

基于所述远程协议配置所述改密脚本信息;

绑定与配置后的改密脚本信息匹配的所述至少一个待改密设备,并生成脚本绑定信息。

[0011] 可选的,所述基于所述至少一个待改密设备的改密脚本信息向所述至少一个待改密设备发送改密请求包括:

通过Redis监听所述脚本绑定信息,则允许向所述至少一个改密设备发送改密请求。

[0012] 可选的,在所述将所述新密码更新为所述至少一个待改密设备的登录密码之后,还包括:

生成并发送包含所述新密码的提示信息,所述提示信息用于提示所述待改密设备的使用者改密成功。

[0013] 第二方面,本申请提供一种基于Linux的远程设备账号改密装置,采用如下的技术方案:

一种基于Linux的远程设备账号改密装置,包括:

脚本获取模块,用于获取至少一个待改密设备的改密脚本信息;

改密请求模块,用于基于所述至少一个待改密设备的改密脚本信息向所述至少一个待改密设备发送改密请求;

信息获取模块,用于获取所述至少一个待改密设备响应于所述改密请求返回的设备信息,其中,所述设备信息包括设备账号和登录密码;

账号登录模块,用于基于所述设备账号和所述登录密码获取对应的待改密设备的改密权限;

密码修改模块,用于在获取改密权限后,基于所述至少一个待改密设备的改密脚本信息获取所述至少一个待改密设备的新密码,将所述至少一个待改密设备的登录密码更新为所述新密码。

[0014] 通过采用上述技术方案,同时向多个待改密设备发送改密请求,并同时登陆多个待改密设备,基于改密脚本信息修改多个待改密设备的登录密码,达到对多个待改密设备批量改密的效果,从而提高密码的修改效率。

[0015] 第三方面,本申请提供一种电子设备,采用如下的技术方案:

一种电子设备,包括存储器和处理器,所述存储器上存储有能够被处理器加载并执行第一方面任一项所述的基于Linux的远程设备账号改密方法的计算机程序。

[0016] 第四方面,本申请提供一种计算机可读存储介质,采用如下的技术方案:

一种计算机可读存储介质,存储有能够被处理器加载并执行第一方面任一项所述的基于Linux的远程设备账号改密方法的计算机程序。

附图说明

[0017] 图1是本申请实施例提供的一种基于Linux的远程设备账号改密方法的流程示意图。

[0018] 图2是申请实施例提供的一种基于Linux的远程设备账号改密装置的结构框图。

[0019] 图3是本申请实施例提供的基于Linux的远程设备账号改密设备的结构框图。

具体实施方式

[0020] 以下结合附图对本申请作进一步详细说明。

[0021] 在本实施例中,管理员使用Linux系统在浏览器中登录PAM系统账号,即登录改密特权账号,基于特权账号对远程设备进行批量改密。

[0022] 图1为本申请实施例提供的一种基于Linux的远程设备账号改密方法的流程示意图。

[0023] 如图1所示,该方法主要流程描述如下(步骤S101~S104):

步骤S101,获取至少一个待改密设备的改密脚本信息。

[0024] 在步骤S101之前,获取至少一个待改密设备的远程协议;基于远程协议配置改密脚本信息;绑定与配置后的改密脚本信息匹配的至少一个待改密设备,并生成脚本绑定信息。

[0025] 其中,远程协议包括SSH协议、Telnet协议和RDP协议,不同的待改密设备使用的远程协议不同,但所使用的改密脚本只有一个,因此,需要根据待改密设备所使用的远程协议配置改密脚本信息,需要说明的是,待改密设备需要使用其中至少一种远程协议。

[0026] 在本实施例中,通过Redis监听脚本绑定信息,则允许向至少一个改密设备发送改密请求。

[0027] 其中,在脚本配置结束并且与至少一个带改密设备绑定后才可以发送改密请求。

[0028] 针对步骤S101,改密脚本信息包括请求发送方式,其中,请求发送方式包括手动发送和自动发送;

在本实施例中,若请求发送方式为手动发送,则响应于管理员的发送指令,向至少一个待改密设备发送改密请求;

其中,手动发送即为根据改密需求,管理员点击改密按钮或者编辑改密指令从而触发改密请求发送机制,从而向至少一个待改密设备发送改密请求,具体的手动请求发送方式在此不做具体限定。

[0029] 在本实施例中,若请求发送方式为自动发送,则获取预设改密周期,并基于预设改密周期向至少一个待改密设备发送改密请求。

[0030] 其中,预设改密周期为达到固定天数时自动触发改密请求机制,预设改密周期根据实际需求可以设置为几天、几周或者几个月,预设改密时间为达到固定时间时自动触发改密请求机制,预设改密周期和预设改密时间需要同时设置,即达到固定天数的固定时间时才会自动触发改密请求机制。例如,预设改密周期设置为20天,预设改密时间为晚上11点,上次改密时间为本月5号,则本次改密请求将在本月25号晚上11点钟发出。需要说明的是,相邻两次请求发送方式可选择不同的请求发送方式,两种请求发送方式之间互不影响,并且具体的预设改密周期和预设改密时间需要根据实际需求自行设定,在此不做具体限

定。

[0031] 步骤S102,基于至少一个待改密设备的改密脚本信息向至少一个待改密设备发送改密请求。

[0032] 步骤S103,获取至少一个待改密设备响应于改密请求返回的设备信息,其中,设备信息包括设备账号和登录密码。

[0033] 针对步骤S103,接收至少一个待改密设备返回的响应信息;若响应信息包含改密允许信息,则获取相应信息中的设备信息。接收至少一个待改密设备返回的响应信息;若响应信息包含改密允许信息,则执行步骤S103。

[0034] 在本实施例中,待改密设备在接收到改密请求后,向改密服务器发送响应信息,即是否同意改密,同意改密则为改密允许信息,不同意改密则为改密拒绝信息。若改密设备返回改密允许信息,则待改密设备向改密服务器发送包含设备账号和登录密码的设备信息,若改密设备返回改密禁止信息,则中止对该待改密设备的改密操作。

[0035] 步骤S104,基于设备账号和登录密码获取对应的待改密设备的改密权限。

[0036] 在本实施例中,通过待改密设备的设备账号和登录密码登录待改密设备,从而获得改密权限,当设备账号与登录密码不匹配或者登录密码出现错误时,无法登录该待改密设备,若无法登录待改密设备则无法获得改密权限。此时,待改密设备向改密服务器发送登录错误信息,改密服务器接受到登录错误信息后将登录错误信息反馈给管理员并停止对该待改密设备的改密操作。

[0037] 步骤S105,在获取改密权限后,基于至少一个待改密设备的改密脚本信息获取至少一个待改密设备的新密码,将至少一个待改密设备的登录密码更新为新密码。

[0038] 在本实施例中,成功登录待改密设备并获得改密权限后,获取本次改密使用的新密码,将新密码替换初始登录密码成为新的登录密码。其中,多个待改密设备的新密码可以为相同的密码也可以为不同的密码,例如,本次的待改密设备为10个,可以本次的10个待改密设备的密码一致,也可以本次的10个待改密设备每个设备拥有不同于其他9个待改密设备的新密码,还可以将本次的10个待改密设备按一定的规则进行分组,每个小组内的待改密设备使用相同的新密码,具体的新密码分配规则需要管理员根据实际需求自行设置,在此不做具体限定。

[0039] 针对步骤S105,改密脚本信息包括密码生成规则,基于密码生成规则生成新密码。

[0040] 密码生成规则由管理员根据设备情况自行设定,密码生成规则可以为大写字母、小写字母、数字和符号按照预设的字符长度自由组合,并且生成的密码需要包含大写字母、小写字母、数字和符号中的至少两种,字符不可作为密码的首位,例如,需要生成字符长度为10个字符,则生成的密码可以为LIN258ux**、ZZZZ256347、72hub*129f等。密码生成规则还可以为大写字母、小写字母、数字和符号中的任意三种,每种都按照固定的字符长度自由组合,例如,大写字母的字符长度为3、小写字母的字符长度为4、数字的字符长度为4、符号的字符长度为2,则生成的密码可以为H23U*I*56、h1256HI4Lin、LINux**ss等。需要说明的是,密码生成规则包括但不限于上述方法,在此不做具体限定。

[0041] 在密码修改结束之后,生成并发送包含新密码的提示信息,提示信息用于提示待改密设备的使用者改密成功。

[0042] 在本实施例中,在改密之后存在改密失败的情况,当改密失败时,返回改密错误信

息,管理员根据需要多改密失败的待改密设备进行处理,可以选择继续改密也可以选择手动改密还可以为进入等待队列,等待下次改密。当改密成功时,返回改密正确信息,获取待改密设备的使用者的联系信息,联系信息可以为使用者的电话号码也可以为使用者的邮箱,将修改的新密码以短信的形式或者邮件的形式发送给使用者,具体的联系信息和通知方式在此不做具体限定。

[0043] 在本实施例中,远程设备为计算机、中继器、集线器等,在此不做具体限定。

[0044] 图2为申请实施例提供的一种基于Linux的远程设备账号改密装置200的结构框图。

[0045] 如图2所示,基于Linux的远程设备账号改密装置200主要包括:

脚本获取模块201,用于获取至少一个待改密设备的改密脚本信息;

改密请求模块202,用于基于至少一个待改密设备的改密脚本信息向至少一个待改密设备发送改密请求;

信息获取模块203,用于获取至少一个待改密设备响应于改密请求返回的设备信息,其中,设备信息包括设备账号和登录密码;

账号登录模块204,用于基于设备账号和登录密码获取对应的待改密设备的改密权限;

密码修改模块205,用于在获取改密权限后,基于至少一个待改密设备的改密脚本信息获取至少一个待改密设备的新密码,将至少一个待改密设备的登录密码更新为新密码。

[0046] 作为本实施例的一种可选实施方式,脚本获取模块201具体用于若请求发送方式为手动发送,则响应于管理员的发送指令,向至少一个待改密设备发送改密请求;若请求发送方式为自动发送,则获取预设改密周期,并基于预设改密周期向至少一个待改密设备发送改密请求。

[0047] 作为本实施例的一种可选实施方式,该基于Linux的远程设备账号改密装置200还包括:

信息接收模块,用于接收至少一个待改密设备返回的响应信息;

若响应信息包含改密允许信息,则执行获取至少一个待改密设备返回的设备信息的步骤。

[0048] 作为本实施例的一种可选实施方式,密码修改模块205具体用于基于密码生成规则生成新密码。

[0049] 作为本实施例的一种可选实施方式,脚本获取模块201具体用于获取至少一个待改密设备的远程协议;基于远程协议配置改密脚本信息;绑定与配置后的改密脚本信息匹配的至少一个待改密设备,并生成脚本绑定信息。

[0050] 作为本实施例的一种可选实施方式,改密请求模块202具体用于通过Redis监听脚本绑定信息,则允许向至少一个改密设备发送改密请求。

[0051] 作为本实施例的一种可选实施方式,该基于Linux的远程设备账号改密装置200还包括:

密码提示模块,用于生成并发送包含新密码的提示信息,提示信息用于提示待改密设备的使用者改密成功。

[0052] 在一个例子中,以上任一装置中的模块可以是配置成实施以上方法的一个或多个集成电路,例如:一个或多个专用集成电路(application specific integrated circuit,ASIC),或,一个或多个数字信号处理器(digital signal processor,DSP),或,一个或者多个现场可编程门阵列(field programmable gate array,FPGA),或这些集成电路形式中至少两种的组合。

[0053] 再如,当装置中的模块可以通过处理元件调度程序的形式实现时,该处理元件可以是通用处理器,例如中央处理器(central processing unit,CPU)或其它可以调用程序的处理器。再如,这些模块可以集成在一起,以片上系统(system-on-a-chip,SOC)的形式实现。

[0054] 所属领域的技术人员可以清楚地了解到,为描述的方便和简洁,上述描述的装置和模块的具体工作过程,可以参考前述方法实施例中的对应过程,在此不再赘述。

[0055] 图3为本申请实施例提供的电子设备300的结构框图。

[0056] 如图3所示,电子设备300包括处理器301和存储器302,还可以进一步包括信息输入/信息输出(I/O)接口303、通信组件304中的一种或多种以及通信总线305。

[0057] 其中,处理器301用于控制电子设备300的整体操作,以完成上述的基于Linux的远程设备账号改密方法的全部或部分步骤;存储器302用于存储各种类型的数据以支持在电子设备300的操作,这些数据例如可以包括用于在该电子设备300上操作的任何应用程序或方法的指令,以及应用程序相关的数据。该存储器302可以由任何类型的易失性或非易失性存储设备或者它们的组合实现,例如静态随机存取存储器(Static Random Access Memory,SRAM)、电可擦除可编程只读存储器(Electrically Erasable Programmable Read-Only Memory,EEPROM)、可擦除可编程只读存储器(Erasable Programmable Read-Only Memory,EPROM)、可编程只读存储器(Programmable Read-Only Memory,PROM)、只读存储器(Read-Only Memory,ROM)、磁存储器、快闪存储器、磁盘或光盘中的一种或多种。

[0058] I/O接口303为处理器301和其他接口模块之间提供接口,上述其他接口模块可以是键盘,鼠标,按钮等。这些按钮可以是虚拟按钮或者实体按钮。通信组件304用于电子设备300与其他设备之间进行有线或无线通信。无线通信,例如Wi-Fi,蓝牙,近场通信(Near Field Communication,简称NFC),2G、3G或4G,或它们中的一种或几种的组合,因此相应的该通信组件104可以包括:Wi-Fi部件,蓝牙部件,NFC部件。

[0059] 电子设备300可以被一个或多个应用专用集成电路(Application Specific Integrated Circuit,简称ASIC)、数字信号处理器(Digital Signal Processor,简称DSP)、数字信号处理设备(Digital Signal Processing Device,简称DSPD)、可编程逻辑器件(Programmable Logic Device,简称PLD)、现场可编程门阵列(Field Programmable Gate Array,简称FPGA)、控制器、微控制器、微处理器或其他电子元件实现,用于执行上述实施例给出的基于Linux的远程设备账号改密方法。

[0060] 通信总线305可包括一通路,在上述组件之间传送信息。通信总线305可以是PCI(Peripheral Component Interconnect,外设部件互连标准)总线或EISA(Extended Industry Standard Architecture,扩展工业标准结构)总线等。通信总线305可以分为地址总线、数据总线、控制总线等。

[0061] 电子设备300可以包括但不限于移动电话、笔记本电脑、数字广播接收器、PDA(个

人数字助理)、PAD(平板电脑)、PMP(便携式多媒体播放器)、车载终端(例如车载导航终端)等等的移动终端以及诸如数字TV、台式计算机等等的固定终端,还可以为服务器等。

[0062] 本申请还提供一种计算机可读存储介质,计算机可读存储介质上存储有计算机程序,计算机程序被处理器执行时实现上述的基于Linux的远程设备账号改密方法的步骤。

[0063] 该计算机可读存储介质可以包括:U盘、移动硬盘、只读存储器(Read-Only Memory,ROM)、随机存取存储器(Random Access Memory,RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0064] 术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、物品或者设备所固有的要素。

[0065] 以上描述仅为本申请的较佳实施例以及对所运用技术原理的说明。本领域技术人员应当理解,本申请中所涉及的应用范围,并不限于上述技术特征的特定组合而成的技术方案,同时也应涵盖在不脱离前述申请构思的情况下,由上述技术特征或其等同特征进行任意组合而形成的其它技术方案。例如上述特征与本申请中申请的(但不限于)具有类似功能的技术特征进行互相替换而形成的技术方案。

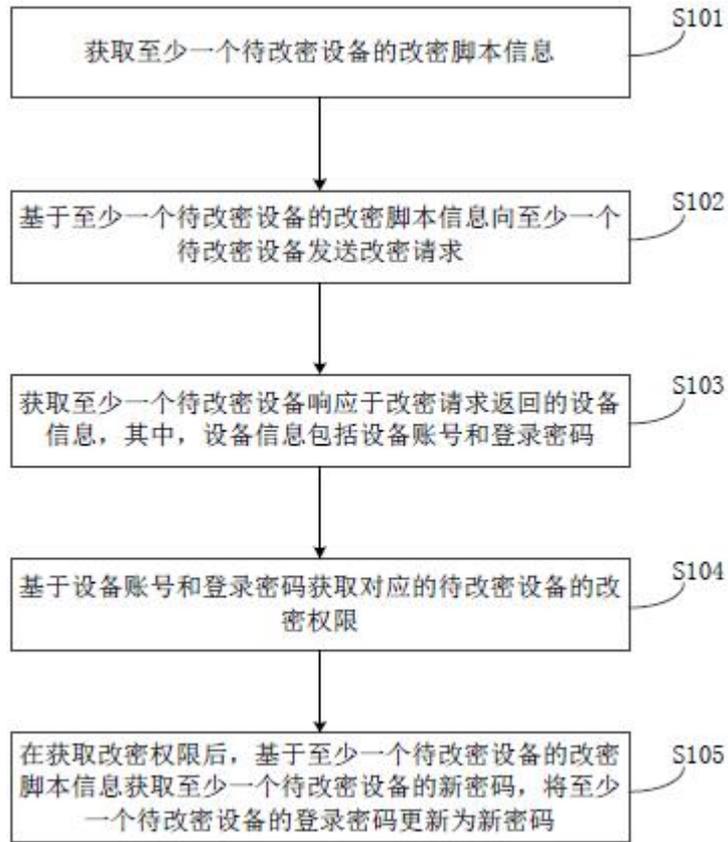


图1

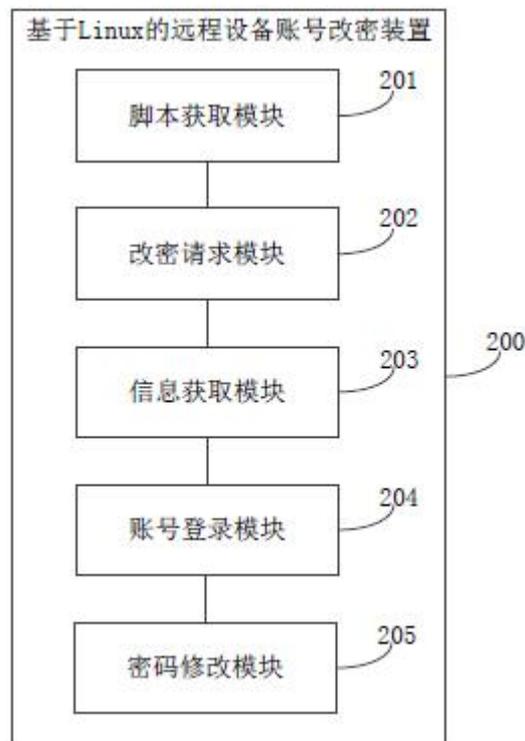


图2

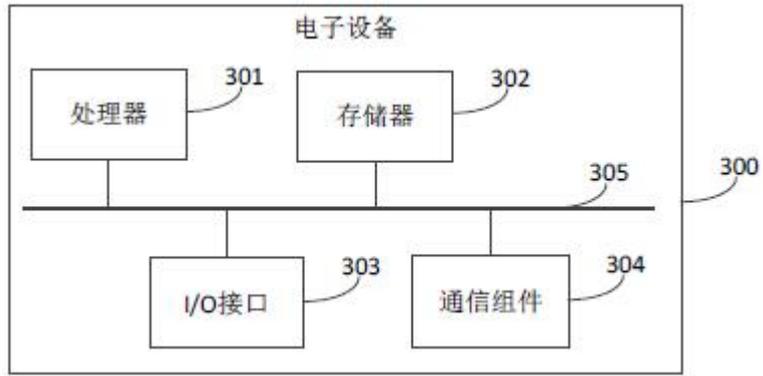


图3