(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 107147801 A
(43)申请公布日 2017.09.08

(21)申请号 201710421682.7

(22)申请日 2017.06.06

(71)申请人 华东交通大学
地址 330013 江西省南昌市青山湖区双港东路808号

(72)发明人 姜楠 周洁 汤兆平 张恒 万涛 徐炜新 许东 万朔

(74)专利代理机构 深圳市智圈知识产权代理事务所(普通合伙) 44351
代理人 周宇波

(51)Int.Cl.
H04M 1/725(2006.01)
G08B 21/24(2006.01)

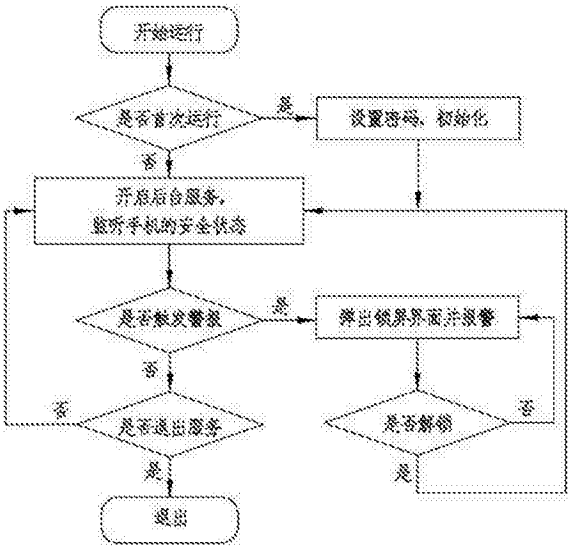
权利要求书2页 说明书5页 附图2页

(54)发明名称

基于USB接口附件的安卓手机防盗方法及系统

(57)摘要

本发明涉及一种基于USB接口附件的安卓手机防盗方法，应用于安卓手机防盗系统中，以实现安卓手机的防盗。该方法包括步骤：提示用户进行安全设置，并初始化安卓手机防盗系统；提示用户在USB接口内插入适配的附件，并根据USB接口内附件的插拔情况监听手机的安全状态；当检测到USB接口内的附件被拔出，则判断手机被盗，弹出锁屏界面并控制手机发出报警信息；以及持续监控手机锁屏状态，若判断手机已被解锁，则继续监听手机的安全状态；若判断手机未解锁，则认为手机仍处于被盗状态，控制所述手机持续发出报警信息。上述的基于USB接口附件的安卓手机防盗方法较为主动且有效。



CN 107147801 A

1.一种基于USB接口附件的安卓手机防盗方法,应用于安卓手机防盗系统中,以实现安卓手机的防盗;其特征在于,该方法包括步骤:

提示用户进行安全设置,并初始化安卓手机防盗系统;

提示用户在USB接口内插入适配的附件,并根据USB接口内附件的插拔情况监听手机的安全状态;

当检测到USB接口内的附件被拔出,则判断手机被盗,弹出锁屏界面并控制手机发出报警信息;以及

持续监控手机锁屏状态,若判断手机已被解锁,则继续监听手机的安全状态;若判断手机未解锁,则认为手机仍处于被盗状态,控制所述手机持续发出报警信息。

2.如权利要求1所述的方法,其特征在于,提示用户进行安全设置时,提示用户输入密码,并通过消息摘要算法第五版(MD5)加密算法对密码进行加密,将密码分组级联后生成一个128位的散列值,然后利用安卓系统的Sharedpreference存储将散列值存储在手机的只读存储器(ROM)中。

3.如权利要求1所述的方法,其特征在于,监听手机的安全状态时,开启后台服务监听手机状态。

4.如权利要求3所述的方法,其特征在于,采用安卓系统的本地服务来保持常驻后台防盗。

5.如权利要求3所述的方法,其特征在于,监听手机的安全状态时,在安卓系统的系统服务中利用安卓系统的广播机制注册监听USB接口状态的广播地址(Broadcast),若广播内接收到的内容是BATTERY_STATUS_CHARGING时,认为USB接口内插有适配的附件;若广播内接收到的内容是BATTERY_STATUS_DISCHARGING,则认为该附件被拔出。

6.如权利要求1所述的方法,其特征在于,控制手机发出报警信息时,报警信息可以包括如下报警方式的任一种或多种的组合:手机屏幕闪烁、手机响铃、手机震动、手机语音播报、手机电筒闪烁。

7.如权利要求1所述的方法,其特征在于,还包括步骤:判断手机处于被盗状态时锁定手机;在提示用户进行安全设置后,申请手机的SYSTEM_ALERT_WINDOW的权限,以便在手机被盗时锁定手机。

8.如权利要求1所述的方法,其特征在于,还包括步骤:监控系统服务状态,若用户停止运行所述安卓手机防盗系统,则关闭服务并退出,若用户未停止运行所述安卓手机防盗系统,则继续监听手机状态。

9.如权利要求8所述的方法,其特征在于,若判断用户在预设的时间段之内点击了两次返回按键,则认为用户需要停止运行所述安卓手机防盗系统。

10.一种基于USB接口附件的安卓手机防盗系统,用于执行权利要求1～9中任一项的基于USB接口附件的安卓手机防盗方法,其特征在于,所述安卓手机防盗系统包括:

安全设置模块,用于提示用户进行安全设置,并初始化所述安卓手机防盗系统;

状态监听模块,用于提示用户在USB接口内插入适配的附件,并根据USB接口内附件的插拔情况监听手机的安全状态;还用于在检测到USB接口内的附件被拔出时,判断手机处于被盗状态;

警报模块,用于在所述状态监听模块判断手机被盗时,控制手机发出报警信息;以及

用户交互模块，用于在所述状态监听模块判断手机被盗时，弹出锁屏界面；还用于持续监控手机锁屏状态，若判断手机已被解锁，则允许所述状态监听模块继续监听手机的安全状态；若判断手机未解锁，则允许所述警报模块还用于控制所述手机持续发出报警信息。

基于USB接口附件的安卓手机防盗方法及系统

技术领域

[0001] 本发明涉及移动通信装置防盗领域，尤其涉及一种基于USB接口附件的安卓手机防盗方法及系统。

背景技术

[0002] 在手机的防盗软件方面，现有防盗软件功能十分复杂。例如，采用360手机安全卫士，用户可以通过发送包含防盗密码的短信到绑定的手机，从而实现震动报警、获取手机新号码、远程锁定和拍照上传等功能，非常方便。虽然用户通过手机防盗软件在手机被盗之后能够快速找到使用手机的新的电话号码和位置，但是手机防盗的意义不是很大，手机被盗事件仍然得不到遏制。一方面，手机被盗之后就被快速地送到二手市场，二手市场通过格式化硬盘或破解程序刷机等方法能够清除自带和安装的手机防盗软件，让手机防盗软件形同虚设。

发明内容

[0003] 本发明实施例的目的在于提供一种基于USB接口附件的安卓手机防盗方法及系统，用于解决上述技术问题。

[0004] 一种基于USB接口附件的安卓手机防盗方法，应用于安卓手机防盗系统中，以实现安卓手机的防盗。该方法包括步骤：提示用户进行安全设置，并初始化安卓手机防盗系统；提示用户在USB接口内插入适配的附件，并根据USB接口内附件的插拔情况监听手机的安全状态；当检测到USB接口内的附件被拔出，则判断手机被盗，弹出锁屏界面并控制手机发出报警信息；以及持续监控手机锁屏状态，若判断手机已被解锁，则继续监听手机的安全状态；若判断手机未解锁，则认为手机仍处于被盗状态，控制所述手机持续发出报警信息。

[0005] 在其中一种实施方式中，提示用户进行安全设置时，提示用户输入密码，并通过消息摘要算法第五版(MD5)加密算法对密码进行加密，将密码分组级联后生成一个128位的散列值，然后利用安卓系统的Sharedpreference存储将散列值存储在手机的只读存储器(ROM)中。

[0006] 在其中一种实施方式中，监听手机的安全状态时，开启后台服务监听手机状态。

[0007] 在其中一种实施方式中，采用安卓系统的本地服务来保持常驻后台防盗。

[0008] 在其中一种实施方式中，监听手机的安全状态时，在安卓系统的系统服务中利用安卓系统的广播机制注册监听USB接口状态的广播地址(Broadcast)，若广播内接收到的内容是BATTERY_STATUS_CHARGING时，认为USB接口内插有适配的附件；若广播内接收到的内容是BATTERY_STATUS_DISCHARGING，则认为该附件被拔出。

[0009] 在其中一种实施方式中，控制手机发出报警信息时，报警信息可以包括如下报警方式的任一种或多种的组合：手机屏幕闪烁、手机响铃、手机震动、手机语音播报、手机电筒闪烁。

[0010] 在其中一种实施方式中，所述方法还包括步骤：判断手机处于被盗状态时锁定手

机;在提示用户进行安全设置后,申请手机的SYSTEM_ALERT_WINDOW的权限,以便在手机被盗时锁定手机。

[0011] 在其中一种实施方式中,所述方法还包括步骤:监控系统服务状态,若用户停止运行所述安卓手机防盗系统,则关闭服务并退出,若用户未停止运行所述安卓手机防盗系统,则继续监听手机状态。

[0012] 在其中一种实施方式中,若判断用户在预设的时间段之内点击了两次返回按键,则认为用户需要停止运行所述安卓手机防盗系统。

[0013] 一种基于USB接口附件的安卓手机防盗系统,用于执行权利要求1～9中任一项的基于USB接口附件的安卓手机防盗方法,所述安卓手机防盗系统包括:安全设置模块,用于提示用户进行安全设置,并初始化所述安卓手机防盗系统;状态监听模块,用于提示用户在USB接口内插入适配的附件,并根据USB接口内附件的插拔情况监听手机的安全状态;还用于在检测到USB接口内的附件被拔出时,判断手机处于被盗状态;警报模块,用于在所述状态监听模块判断手机被盗时,控制手机发出报警信息;以及用户交互模块,用于在所述状态监听模块判断手机被盗时,弹出锁屏界面;还用于持续监控手机锁屏状态,若判断手机已被解锁,则允许所述状态监听模块继续监听手机的安全状态;若判断手机未解锁,则允许所述警报模块还用于控制所述手机持续发出报警信息。

[0014] 相对于现有技术,本发明实施例提供的基于USB接口附件的安卓手机防盗方法,其应用在安卓手机防盗系统中,通过实时地监控USB接口内附件的插拔状态,能够实时地监控安卓手机的安全状态,并在判断手机被盗时发出警报,为用户提供了较为主动的手机防盗模式,能够实现有效的手机防盗。。

附图说明

[0015] 为了更清楚地说明本发明的技术方案,下面将对实施方式中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明的一些实施方式,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0016] 图1是本发明实施例提供的基于USB接口附件的安卓手机防盗方法的流程示意图;

[0017] 图2是本发明实施例提供的安卓手机防盗系统的功能模块示意图。

具体实施方式

[0018] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0019] 请参阅图1及图2,本发明实施方式提供一种基于USB接口附件的安卓手机防盗方法,该方法应用于如图2所示的安卓手机防盗系统S1中,用于实时地监控手机USB接口内附件的插拔的状态以判断手机是否被盗,并在判断手机被盗时向用户发出警报,从而对手机提供较为主动的防盗保护。上述的USB接口内的附件应当为适配于手机的USB接口的外接装置,包括但不限于数据线、电源线等。

[0020] 具体而言,所述安卓手机防盗系统S1包括安全设置模块101、状态监听模块103、警

报模块105以及交互模块107。所述安全设置模块101用于设置或/及存储用户的安全信息，如用户名及密码等；所述状态监听模块103用于监听手机的实时状态，并判断用户手机是否被盗；所述警报模块105用于在用户手机被盗时控制手机发出警报，以提醒用户注意；所述交互模块107用于为用户提供人机交互界面。上述的安卓手机防盗系统S1运行于安卓操作系统上。

[0021] 所述基于USB接口附件的安卓手机防盗方法，应用于上述的安卓手机防盗系统S1，具体包括如下步骤：

[0022] 步骤S101：用户进行安全设置，并初始化安卓手机防盗系统S1。具体地，在用户启动所述安卓手机防盗系统S1时，所述安全设置模块101判断用户是否首次运行安卓手机防盗系统S1，若是，则提示用户设置密码并初始化所述安卓手机防盗系统S1。具体在本实施方式中，当用户首次启动所述安卓手机防盗系统S1时，所述安卓手机防盗系统S1的安全设置模块101控制手机弹出一个对话框，请用户输入账号和密码，然后存储账号和密码，从而保护所述安卓手机防盗系统S1不受外人的恶意操作。

[0023] 进一步地，为了提高所述安卓手机防盗系统S1的安全性，所述安全设置模块101在存储上述密码时，通过消息摘要算法第五版(MD5)加密算法对密码进行加密，将密码分组级联后生成一个128位的散列值，然后利用安卓系统的Sharedpreference存储将散列值存储在手机的只读存储器(ROM)中。当需要进行匹配密码的时候，只需要将输入的新密码进行MD5加密，然后从ROM中读取存储的散列值，将两者进行比较即可。

[0024] 步骤S103：监听手机的安全状态。具体地，所述状态监听模块103启动并监听手机的状态。具体在本实施方式中，当用户在手机上运行所述安卓手机防盗系统S1时，其手机的USB接口内应插有适配的附件，如USB接口内插有电源线或者数据线等，所述状态监听模块103通过监听手机的USB接口内附件的插拔状态来实时监听并判断手机是否被盗。为了保证用户运行所述安卓手机防盗系统S1时其手机的USB接口内插有附件，所述安卓手机防盗系统S1的状态监听模块103还用于控制手机向用户发出“请先插入附件”的提示，当用户在USB接口内插入附件后，所述状态监听模块103开始正常监听手机的安全状态。

[0025] 进一步地，所述安卓手机防盗系统S1能够开启后台服务监听手机状态，以便用户在开启手机防盗服务时能够利用手机处理其他事务。

[0026] 具体在本实施方式中，当用户选择将所述安卓手机防盗系统S1保持在后台运行时，所述安卓手机防盗系统S1使用安卓系统的系统服务(Service)机制，实现防盗服务常驻后台的功能。应当了解的是，Service服务是安卓系统中最常用到的四大部件之一，安卓支持Service服务的主要目的有两个，一是为了简化常驻后台的任务的实现，二是在同一台设备当中实现跨进程的远程信息通信。Service服务有两种常用的使用方式：本地服务(Local Service)与远程服务(Remote Service)。本地服务只支持同一进程内进行内部的访问，远程服务可通过安卓接口定义语言(Android Interface Definition Language,AIDL)技术进行跨进程的访问。Service服务可以通过Context.startService()和Context.bindService()进行启动，一般本地服务可使用其中一种方法启动。具体在本发明实施方式中，所述安卓手机防盗系统S1采用本地服务来保持常驻后台的防盗功能。

[0027] 步骤S105：判断手机状态是否触发警报，若是，则执行步骤S107，若否，则执行步骤S101。具体地，所述状态监听模块103持续监听手机的USB接口的插拔状态，并根据USB接口

的状态判断手机是否被盗，若所述状态监听模块103判断手机USB接口内附件被拔出时，则认为手机已经被盗而触发警报。

[0028] 具体在本实施方式中，当用户在手机上运行所述安卓手机防盗系统S1时，所述USB接口内应插有适配的附件，若所述状态监听模块103监控到该附件被拔出，则认为手机被盗，并触发警报。具体而言，当所述安卓手机防盗系统S1在后台运行时，为顺利实现后台防盗且在判断手机被盗时顺利发出警报信息，所述安卓手机防盗系统S1能够在安卓系统的系统服务(Service)中利用安卓系统的广播机制注册监听USB接口状态的广播地址(Broadcast)。当广播内接收到的内容是BATTERY_STATUS_CHARGING的时候，表示USB接口内插有适配的附件；若广播内接收到的内容是BATTERY_STATUS_DISCHARGING，则表示该附件被拔出。

[0029] 步骤S107：弹出锁屏界面并控制手机发出报警信息。具体地，所述用户交互模块107控制手机弹出锁屏界面，所述警报模块105控制所述手机发出报警信息，以提醒用户注意手机。该报警信息可以包括如下报警方式的任一种或多种的组合：手机屏幕闪烁、手机响铃、手机震动、手机语音播报、手机电筒闪烁等。

[0030] 具体在本实施方式中，所述警报模块105控制所述手机以震动及响铃的形式发出报警信息。所述安卓手机防盗系统S1通过预先获取手机震动权限：android.permission.VIBRATE，来发出震动警报；所述安卓手机防盗系统S1获取权限后通过getSystemService(Context.VIBRATOR_SERVICE)获取安卓系统的震动应用程序编程接口(Application Programming Interface，API)，然后设置震动频率，发出震动；同时通过getSystemService(Context.AUDIO_SERVICE)获取安卓系统的多媒体API，然后通过该API调用事先准备好的手机报警铃声，将手机外放音量调至最大，发出报警。

[0031] 所述安卓手机防盗系统S1通过悬浮窗的形式实现弹出锁屏界面，即，使用一个能占满整个屏幕的自定义组合控件来实现锁住屏幕的功能。所述安卓手机防盗系统S1能够获取整个手机屏幕的宽度和高度，通过安卓系统的Sharedpreference存储将参数存储到手机中，当所述状态监听模块103检测到手机被盗的时候，所述用户交互模块107执行锁住屏幕的代码，也就是执行弹出悬浮窗的代码。悬浮窗内最上方是一个文本显示区域(TextView)，用来显示“请解锁”的提醒，下方是一个输入框(EditText)，该输入框用来输入解锁密码，输入框下方就是一个九宫格，显示0-9十个数字，每一个数字都是由按键组成，还有一个撤销按键，用来撤销用户输错的密码。当所述状态监听模块103判断手机被盗时，所述用户交互模块107会通过WindowManager.addView(contentView,params)来弹出对话框，若想撤销对话框，只能在悬浮窗中输入正确的密码，否则悬浮窗会一直占据整个屏幕。当用户输入了正确的密码，所述用户交互模块107就会通过WindowManager.removeView(contentView)来撤销悬浮窗。

[0032] 进一步地，若所述状态监听模块103判断手机处于被盗状态，则锁定手机，具体在本发明实施方式中，所述安卓手机防盗系统S1的安全设置模块101在用户设定账号密码后，会申请用户手动开启SYSTEM_ALERT_WINDOW的权限，以便在手机被盗时锁定手机。

[0033] 步骤S109：监控手机锁屏状态，若用户已解锁，则所述状态监听模块103继续监听手机状态，若用户未解锁，则认为手机仍处于被盗状态，所述警报模块105控制所述手机持续发出报警信息。具体地，所述用户交互模块107用于监控手机锁屏状态。

[0034] 步骤S111：监控系统服务状态，若用户停止运行所述安卓手机防盗系统，则关闭服务并退出，若用户未停止运行所述安卓手机防盗系统，则所述状态监听模块103继续监听手机状态。具体而言，用户操作所述安卓手机防盗系统S1时，若所述用户交互模块107判断用户在预设的时间段之内点击了两次返回按键，则认为用户需要停止运行所述安卓手机防盗系统。在本实施方式中，所述预设的时间段为两秒。可以理解，在其他的实施方式中，所述预设的时间段可以为一秒、两秒、三秒、四秒等等。

[0035] 本发明实施例提供的基于USB接口附件的安卓手机防盗方法，其应用在安卓手机防盗系统中，通过实时地监控USB接口内附件的插拔状态，能够实时地监控安卓手机的安全状态，并在判断手机被盗时发出警报，为用户提供了较为主动的手机防盗模式，能够实现有效的手机防盗。

[0036] 最后应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不驱使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

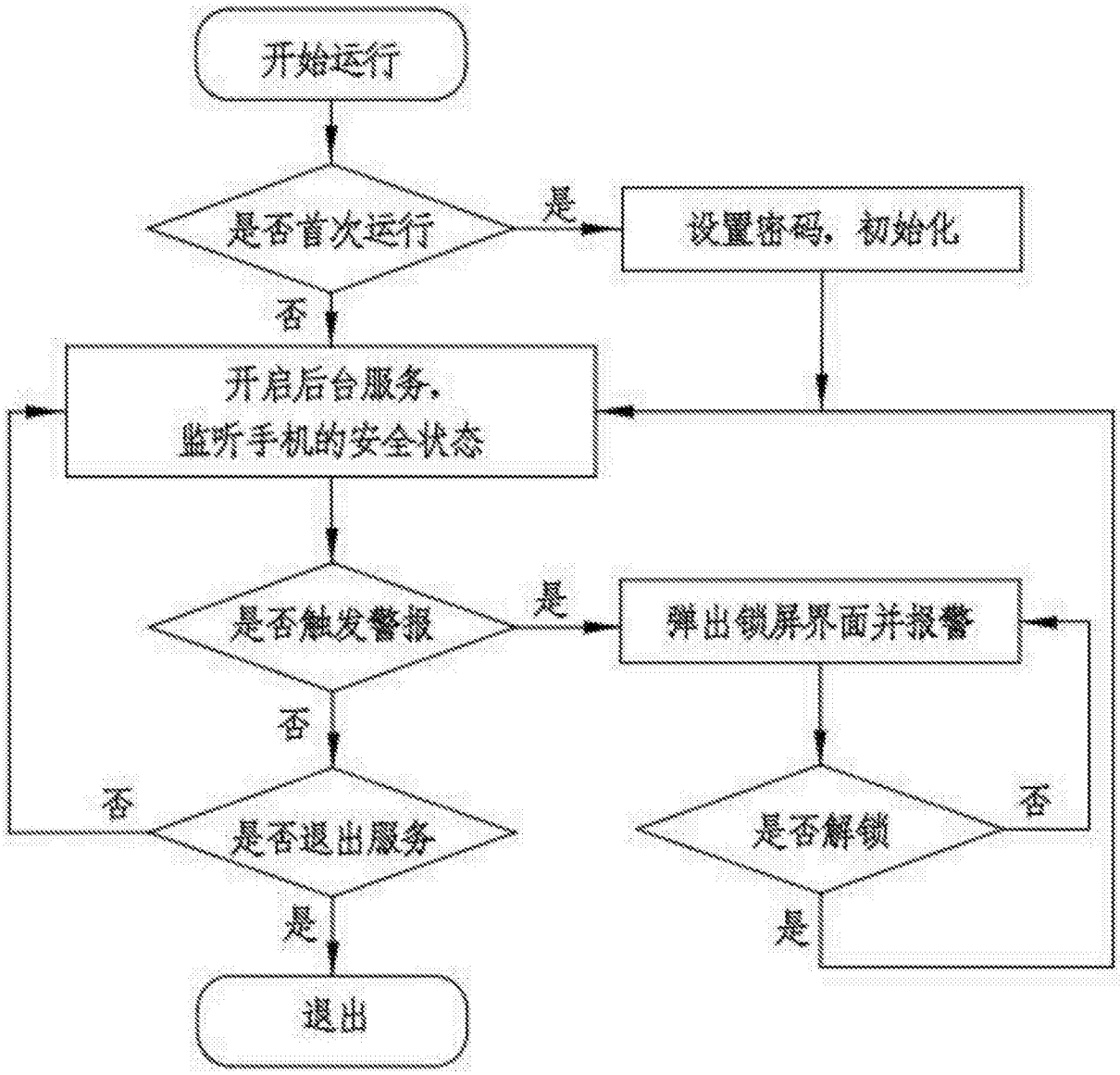

开始运行
是否首次运行
是
设置密码，初始化
否
开启后台服务，
监听手机的安全状态
是否触发警报
是
弹出锁屏界面并报警
否
否
是否退出服务
否
是否解锁
是
是
退出

图1

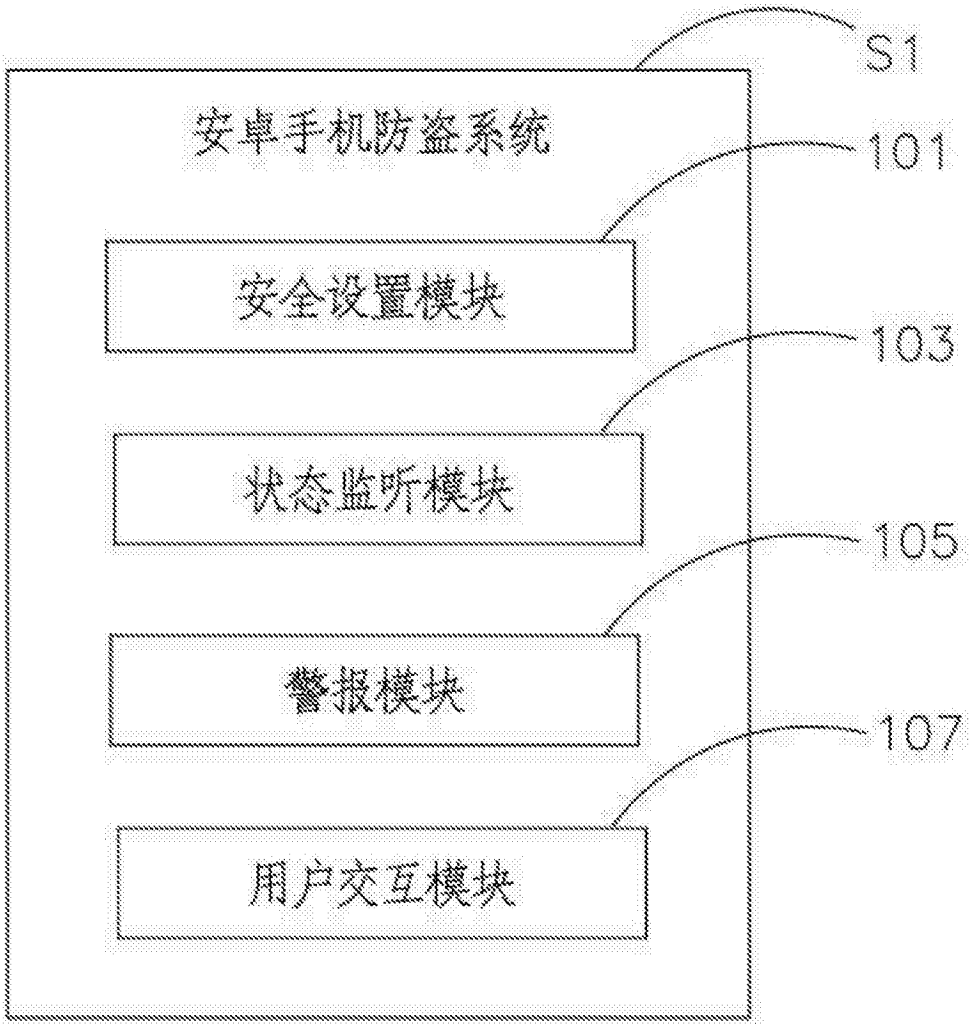


图2