



(12)发明专利

(10)授权公告号 CN 105975320 B

(45)授权公告日 2020.03.17

(21)申请号 201610365524.X

G06F 21/51(2013.01)

(22)申请日 2016.05.26

(56)对比文件

(65)同一申请的已公布的文献号

申请公布号 CN 105975320 A

CN 103577757 A,2014.02.12,

CN 103279706 A,2013.09.04,

US 2014096246 A1,2014.04.03,

(43)申请公布日 2016.09.28

审查员 张楚湖

(73)专利权人 宇龙计算机通信科技(深圳)有限公司

地址 518057 广东省深圳市南山区高新技术产业园(北区)梦溪道2号

(72)发明人 吴安峻 杨佳佳 叶瑞权

(74)专利代理机构 广州三环专利商标代理有限公司 44202

代理人 郝传鑫 熊永强

(51)Int.Cl.

G06F 8/61(2018.01)

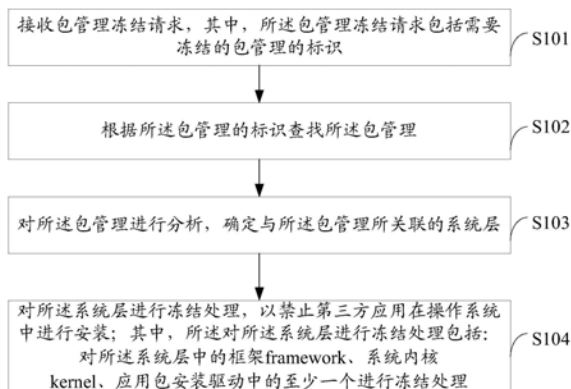
权利要求书2页 说明书11页 附图4页

(54)发明名称

一种第三方应用禁止安装的方法、装置以及终端

(57)摘要

本发明实施例提供了一种第三方应用禁止安装的方法、装置以及终端,其中,所述方法包括:接收包括有需要冻结的包管理的标识的包管理冻结请求;根据所述包管理的标识查找所述包管理;对所述包管理进行分析,确定与所述包管理所关联的系统层;对所述系统层进行冻结处理,以禁止第三方应用在操作系统中进行安装;其中,所述对所述系统层进行冻结处理包括:对所述系统层中的框架framework、系统核心kernel、应用包安装驱动中的至少一个进行冻结处理。采用本发明,可通过对与包管理相关联的系统层进行冻结,以禁止第三方应用程序安装,达到保护终端操作系统的目的,提升了终端使用的安全性。



1. 一种第三方应用禁止安装的方法,其特征在于,所述方法包括:

接收到触发终端系统启动的操作后,识别系统目录并进行扫描,以完成所述终端系统仅在初始化安装系统应用基础上的启动,所述初始化安装系统应用为在接收到所述触发终端系统启动的操作之前已完成安装的系统应用;

接收包管理冻结请求,其中,所述包管理冻结请求包括需要冻结的包管理的标识;

根据所述包管理的标识查找所述包管理;

对所述包管理进行分析,确定与所述包管理所关联的系统层;

对所述系统层进行冻结处理,以禁止第三方应用在操作系统中进行安装;

其中,所述对所述系统层进行冻结处理包括:对所述系统层中的框架、系统内核、应用包安装驱动中的至少一个进行冻结处理。

2. 如权利要求1所述的方法,其特征在于,所述对所述系统层中的框架进行冻结处理,包括:

对所述系统层中的框架进行分析,确定与所述框架对应的应用包安装进程和/或应用包安装服务;

对所确定的所述应用包安装进程和/或所述应用包安装服务进行冻结处理。

3. 如权利要求1所述的方法,其特征在于,还包括:

检测并获取当前处于后台运行的应用程序;

对与所述后台运行的应用程序关联的程序运行服务、程序运行进程、程序运行广播接收器中的至少一个进行冻结处理,以便停止运行所述后台运行的应用程序。

4. 如权利要求1-3中任意一项所述的方法,其特征在于,还包括:

接收用于对冻结处理后的所述系统层进行解冻处理的包管理解冻请求;

根据所述包管理解冻请求的指示对所述冻结处理后的系统层进行解冻处理,以允许所述第三方应用在所述操作系统中进行安装。

5. 如权利要求1所述的方法,其特征在于,所述对所述系统层中的框架进行冻结处理,包括:

对所述系统层中的框架进行分析,确定与所述框架对应的应用包安装进程和/或应用包安装服务;

确定调用所述应用包安装进程和/或应用包安装服务的模块;

对调用所述应用包安装进程和/或应用包安装服务的模块进行冻结处理。

6. 一种第三方应用禁止安装的装置,其特征在于,所述装置包括:

第一接收模块,用于在接收到触发终端系统启动的操作后,识别系统目录并进行扫描,以完成所述终端系统仅在初始化安装系统应用基础上的启动,所述初始化安装系统应用为在接收到所述触发终端系统启动的操作之前已完成安装的系统应用;

所述第一接收模块,还用于接收包管理冻结请求,其中,所述包管理冻结请求包括需要冻结的包管理的标识;

查找模块,用于根据所述包管理的标识查找所述包管理;

确定模块,用于对所述包管理进行分析,确定与所述包管理所关联的系统层;

冻结模块,用于对所述系统层进行冻结处理,以禁止第三方应用在操作系统中进行安装;其中,所述对所述系统层进行冻结处理包括:对所述系统层中的框架、系统内核、应用包

安装驱动中的至少一个进行冻结处理。

7. 如权利要求6所述的装置,其特征在于,

所述冻结模块,具体用于对所述系统层中的框架进行分析,确定与所述框架对应的应用包安装进程和/或应用包安装服务;对所确定的所述应用包安装进程和/或所述应用包安装服务进行冻结处理。

8. 如权利要求6所述的装置,其特征在于,所述装置还包括:

发送模块,用于当检测到所述第三方应用要被安装时,发送用于提示所述操作系统禁止安装所述第三方应用的提示信息,停止所述第三方应用的安装。

9. 如权利要求6所述的装置,其特征在于,所述装置还包括:

检测模块,用于检测并获取当前处于后台运行的应用程序;

所述冻结模块,还用于对与所述后台运行的应用程序关联的程序运行服务、程序运行进程、程序运行广播接收器中的至少一个进行冻结处理,以便停止运行所述后台运行的应用程序。

10. 如权利要求6-9中任意一项所述的装置,其特征在于,所述装置还包括:

第二接收模块,用于接收用于对冻结处理后的所述系统层进行解冻处理的包管理解冻请求;

解冻模块,用于根据所述包管理解冻请求的指示对所述冻结处理后的系统层进行解冻处理,以允许所述第三方应用在该所述操作系统中进行安装。

11. 一种终端,其特征在于,所述终端包括如权利要求6至10中任意一项所述的第三方应用禁止安装的装置。

## 一种第三方应用禁止安装的方法、装置以及终端

### 技术领域

[0001] 本发明涉及终端技术领域,尤其涉及一种第三方应用禁止安装的方法、装置以及终端。

### 背景技术

[0002] 目前,现有的冻结方案中一般都是对终端中已安装的应用进行冻结,限制所述已安装的应用访问系统资源,使其不被启用运行。如用户可以将不常用的应用程序安装包APK(Android Package,简称APK)、第三方应用、部分系统应用等进行冻结,使得冻结之后的各个应用不再被再次启用运行、不再占用系统资源,提升系统的运行速度。如果想要重新启动所述冻结之后的某个应用,就需要将此应用进行解冻处理,解冻后的该应用能够获取到相应的系统资源,从而达到能够正常运行的目的。

[0003] 然而在实践中发现,基于上述现有的冻结方案,仍然有一些第三方恶意应用软件能够在系统不知情的情况下被自动安装,或者在安装部分应用软件时会自动捆绑安装一些用户不需要的APK来抢占系统资源,延缓系统运行速度,甚至造成用户隐私信息泄露等,降低了终端使用的安全性。

### 发明内容

[0004] 本发明实施例所要解决的技术问题在于,提供一种第三方应用禁止安装的方法、装置以及终端,可通过对包管理进行冻结来禁止第三方应用程序安装,达到了保护终端操作系统的目的,提升了终端使用的安全性。

[0005] 一方面,本发明实施例公开提供了一种第三方应用禁止安装的方法,所述方法包括:

[0006] 接收包管理冻结请求,其中,所述包管理冻结请求包括需要冻结的包管理的标识;

[0007] 根据所述包管理的标识查找所述包管理;

[0008] 对所述包管理进行分析,确定与所述包管理所关联的系统层;

[0009] 对所述系统层进行冻结处理,以禁止第三方应用在操作系统中进行安装;

[0010] 其中,所述对所述系统层进行冻结处理包括:对所述系统层中的框架、系统内核、应用包安装驱动中的至少一个进行冻结处理。

[0011] 其中可选地,所述对所述包管理所关联的框架进行冻结处理,包括:

[0012] 对所述系统层中的框架进行分析,确定与所述框架对应的应用包安装进程和/或应用包安装服务;

[0013] 对所确定的所述应用包安装进程和/或所述应用包安装服务进行冻结处理。

[0014] 其中可选地,所述方法还包括:

[0015] 当检测到所述第三方应用要被安装时,发送用于提示所述操作系统禁止安装所述第三方应用的提示信息,停止所述第三方应用的安装。

[0016] 其中可选地,所述方法还包括:

- [0017] 检测并获取当前处于后台运行的应用程序；
- [0018] 对与所述后台运行的应用程序关联的程序运行服务、程序运行进程、程序运行广播接收器中的至少一个进行冻结处理，以便停止运行所述后台运行的应用程序。
- [0019] 其中可选地，所述方法还包括：
- [0020] 接收用于对冻结处理后的所述系统层进行解冻处理的包管理解冻请求；
- [0021] 根据所述包管理解冻请求的指示对所述冻结处理后的系统层进行解冻处理，以允许所述第三方应用在所述操作系统中进行安装。
- [0022] 另一方面，本发明实施例还公开提供了一种第三方应用禁止安装的装置，所述装置包括：
- [0023] 第一接收模块，用于接收包管理冻结请求，其中，所述包管理冻结请求包括需要冻结的包管理的标识；
- [0024] 查找模块，用于根据所述包管理的标识查找所述包管理；
- [0025] 确定模块，用于对所述包管理进行分析，确定与所述包管理所关联的系统层；
- [0026] 冻结模块，用于对所述系统层进行冻结处理，以禁止第三方应用在操作系统中进行安装；其中，所述对所述系统层进行冻结处理包括：对所述系统层中的框架、系统内核、应用包安装驱动中的至少一个进行冻结处理。
- [0027] 其中可选地，
- [0028] 所述冻结模块，具体用于对所述系统层中的框架进行分析，确定与所述框架对应的应用包安装进程和/或应用包安装服务；对所确定的所述应用包安装进程和/或所述应用包安装服务进行冻结处理。
- [0029] 其中可选地，所述装置还包括：
- [0030] 发送模块，用于当检测到所述第三方应用要被安装时，发送用于提示所述操作系统禁止安装所述第三方应用的提示信息，停止所述第三方应用的安装。
- [0031] 其中可选地，所述装置还包括：
- [0032] 检测模块，用于检测并获取当前处于后台运行的应用程序；
- [0033] 所述冻结模块，还用于对与所述后台运行的应用程序关联的程序运行服务、程序运行进程、程序运行广播接收器中的至少一个进行冻结处理，以便停止运行所述后台运行的应用程序。
- [0034] 其中可选地，所述装置还包括：
- [0035] 第二接收模块，用于接收用于对冻结处理后的所述系统层进行解冻处理的包管理解冻请求；
- [0036] 解冻模块，用于根据所述包管理解冻请求的指示对所述冻结处理后的系统层进行解冻处理，以允许所述第三方应用在所述操作系统中进行安装。
- [0037] 再一方面，本发明实施例还公开提供了一种终端，所述终端包括上述的第三方应用禁止安装的装置。
- [0038] 本发明实施例可通过接收包括有需要冻结的包管理的标识的包管理冻结请求，并根据所述包管理的标识查找所述包管理，接着对所述包管理进行分析，确定与所述包管理所关联的系统层，最后对所述系统层进行冻结处理，以禁止第三方应用在操作系统中进行安装，其中，所述对所述系统层进行冻结处理包括：对所述系统层中的框架framework、系统

内核kernel、应用包安装驱动中的至少一个进行冻结处理。这样可通过对系统层中的框架framework、系统内核kernel、应用包安装驱动中的至少一个进行冻结处理,来阻止第三方应用的安装,达到保护终端操作系统的目的,从而提升了终端使用的安全性。

### 附图说明

[0039] 为了更清楚地说明本发明实施例或现有技术中的技术方案,下面将对实施例或现有技术描述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例,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。

[0040] 图1是本发明实施例的一种第三方应用禁止安装方法的流程示意图;

[0041] 图2是本发明实施例的另一种第三方应用禁止安装方法的流程示意图;

[0042] 图3是本发明实施例的一种第三方应用禁止安装装置的结构示意图;

[0043] 图4是本发明实施例的另一种第三方应用禁止安装装置的结构示意图;

[0044] 图5是本发明实施例的一种终端的结构示意图。

### 具体实施方式

[0045] 为了使本技术领域的人员更好地理解本发明方案,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的实施例,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做出创造性劳动前提下所获得的所有其他实施例,都应当属于本发明保护的范围。

[0046] 本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”和“第三”(如果存在)等是用于区别不同对象,而非用于描述特定顺序。此外,术语“包括”以及它们任何变形,意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、系统、产品或设备没有限定于已列出的步骤或单元,而是可选地还包括没有列出的步骤或单元,或可选地还包括对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0047] 请参见图1,是本发明实施例的一种第三方应用禁止安装方法的流程示意图,本发明实施例的所述方法可以应用在诸如智能手机、平板电脑、智能可穿戴设备等带通信网络功能的终端中,具体可由这些终端的处理器来实现。本发明实施例的所述方法还包括如下步骤。

[0048] S101、接收包管理冻结请求,其中,所述包管理冻结请求包括需要冻结的包管理的标识。

[0049] 本发明实施例中,用户可以对终端进行操作(如点击系统冻结按钮,开启系统冻结模式等)来冻结所述终端的操作系统。当所述终端的操作系统处于冻结状态后,能够禁止第三方应用通过包括显示安装、静默安装或者其他的安装方式在该操作系统中进行安装。

[0050] 需要说明的是,冻结所述终端的操作系统,以下简称系统冻结,并不是指冻结所述终端的整个操作系统,导致所述终端不能使用;这里的系统冻结可以是指对所述终端的操作系统中的一部分功能模块进行冻结,这样使得被冻结掉的相应功能被丧失,即所述终端的相应功能将不能再使用,诸如用户可以根据自己的需求保留手机系统中的一些基本功能

能够正常运行(包括打电话和发短信相关的进程),使得所述手机可以变成一个功能机,不能上网等。

[0051] 所述显示安装可以是指在所述终端的显示界面上弹出/显示应用安装界面,让用户清楚地知道某个应用安装包Apk(AndroidPackage,Apk)将会安装到所述终端中;所述静默安装可以是指在安装某个应用安装包Apk时,不会在所述终端的显示界面上弹出安装界面,而是在所述终端的后台自动进行安装,用户不能察觉/知道该Apk在所述终端中的安装,其中,所述静默安装主要有以下几种实现方式:ADB(Android Debug Bridge,ADB)工具安装(命令行的方式)、系统应用安装(开机时完成)、网络下载应用安装(部分商店下载后自动安装,不弹出安装界面),或者其他用户/系统自定义的不被用户察觉的安装方式,本发明实施例不作限定。

[0052] 在所述终端的操作系统中,所有安装方式的应用APK安装都将调用系统中的包管理,因此我们可以对操作系统中的包管理进行冻结,来达到禁止在所述操作系统中安装第三方应用的目的。

[0053] 用户可以对所述终端进行操作(如点击系统冻结按钮等)向所述终端发送包管理冻结请求;或者,其他终端可以通过无线通讯的方式(如蓝牙、wifi等)与所述终端建立通信连接,并向所述终端发送用于指示冻结该终端的操作系统中的包管理冻结请求。所述终端可以检测并接收用户或者所述其他终端发送的所述包管理冻结请求,其中,所述包管理冻结请求可以包括所述包管理的标识(如名称、ID号等)。

[0054] 所述操作系统可以包括Android操作系统、Linux操作系统、Unix操作系统、Windows操作系统,或者包括其他形式的操作系统,本发明实施例不作限定。

[0055] 所述终端可以包括智能手机(如Android手机、IOS手机等)、个人电脑、平板电脑、掌上电脑、移动互联网设备(MID,Mobile Internet Devices)或穿戴式智能设备等互联网设备,本发明实施例不作限定。

[0056] S102、根据所述包管理的标识查找所述包管理。

[0057] 本发明实施例中,终端可以根据S101中接收到的所述包管理冻结请求中的所述包管理的标识来查找对应的所述包管理。

[0058] S103、对所述包管理进行分析,确定与所述包管理所关联的系统层,其中,所述系统层包括框架framework、系统内核kernel、应用包安装驱动中的至少一个。

[0059] 本发明实施例中,终端可以对S102中确定到的所述包管理进行分析,确定与所述包管理相关联的系统层,其中所述系统层包括框架framework、系统内核kernel、应用包安装驱动中的至少一个。

[0060] 可以理解的是,在所述终端的操作系统中进行应用APK运行安装时,需要依赖于系统层;因此所述终端需要对所述包管理进行冻结时,可以对系统层(framework、kernel、驱动等)进行冻结,彻底让所述包管理不能运行,这样第三方应用自然就不能在所述终端的操作系统中进行安装了。

[0061] 所述系统层可以包括框架framework、系统内核kernel、应用包安装驱动,等,所述框架framework下还可以包括PackageManager进程(为了方便描述以下简称PM进程)和PackageManagerService服务(为了方便描述以下简称PMS服务),或者包括其他的与安装应用APK相关联的应用包安装进程和/或应用包安装服务,本发明实施例不作限定。

[0062] S104、对所述系统层进行冻结处理,以禁止第三方应用在操作系统中进行安装;其中,所述对所述系统层进行冻结处理包括:对所述系统层中的框架framework、系统内核kernel、应用包安装驱动中的至少一个进行冻结处理。

[0063] 本发明实施例中,终端可以进一步地对S103中确定到的与所述包管理关联的系统层进行冻结,从源头上阻止第三方应用在所述终端的操作系统中进行安装;具体实现中,所述终端可以对所述系统层中的框架framework、系统内核kernel、应用包安装驱动中的至少一个进行冻结处理。

[0064] 需要说明的是,由于所述包管理在安装包括所述第三方应用的所有应用过程中起到控制调度的作用,因此,所述终端还可以直接对所述包管理进行冻结,也可以达到禁止第三方应用在操作系统中进行安装的目的。

[0065] 其中可选地,所述对所述系统层中的框架framework进行冻结处理,包括:

[0066] 对所述系统层中的框架framework进行分析,确定与所述框架framework对应的应用包安装进程和/或应用包安装服务;

[0067] 对所确定的所述应用包安装进程和/或所述应用包安装服务进行冻结处理。

[0068] 所述终端还可以对所述框架framework进行分析,确定与所述framework相关联或者所述framework中的应用包安装进程和/或应用包安装服务(如PM进程、PMS服务等);所述终端进一步地可以对确定到的所述应用包安装进程和/或所述应用包安装服务进行冻结处理,以到达禁止在所述终端中安装第三方应用的目的。

[0069] 进一步地,所述终端还可以查找并确定所述应用包安装进程和/或所述应用包安装服务(如PM进程、PMS服务)可以相应调用系统(系统层)中的哪些接口,分析这些接口都有哪些模块调用,查找与这些模块相对应的进程和/或服务;进一步地,所述终端可以对查找到的所述与这些模块相对应的进程和/或服务进行冻结,也能达到在所述终端中安装第三方应用的目的。可选地,所述终端可以将查找到的所述与这些模块相对应的进程和/或服务添加到本终端中的系统冻结模块列表list中;所述终端在接收到所述包管理冻结请求后,还可以查找所述系统冻结模块列表list,并对所述系统冻结模块列表list中的进程和/或服务进行冻结,同样也能到达禁止在所述终端中安装第三方应用的目的。

[0070] 其中可选地,所述方法还包括:

[0071] 当检测到所述第三方应用要被安装时,发送用于提示所述操作系统禁止安装所述第三方应用的提示信息,停止所述第三方应用的安装。

[0072] 所述终端在检测到存在一个或者多个第三方应用在该终端中进行安装时,所述终端可以发送一个或者多个提示信息,并停止所述第三方应用的安装,其中,所述提示信息用于提示用户当前使用的所述终端的操作系统已被冻结,不能支持所述第三方应用的安装。具体实现中,所述终端可以通过语音、文字、字幕、震动、图片或者其他提醒方式中的一种或者多种来发送相应的提示信息。

[0073] 其中可选地,所述方法还包括:

[0074] 检测并获取当前处于后台运行的应用程序;

[0075] 对与所述后台运行的应用程序关联的程序运行服务、程序运行进程、程序运行广播接收器中的至少一个进行冻结处理,以便停止运行所述后台运行的应用程序。

[0076] 所述终端还可以检测并获取当前在该终端中进行后台运行的应用程序,所述终端



还可以对与所述后台运行的应用程序相关联的服务、进程、广播接收器或者额外的线程等进行冻结处理,以便停止所述后台运行的应用程序。

[0077] 其中可选地,所述方法还包括:

[0078] 接收用于对冻结处理后的所述系统层进行解冻处理的包管理解冻请求;

[0079] 根据所述包管理解冻请求的指示对所述冻结处理后的系统层进行解冻处理,以允许所述第三方应用在所述操作系统中进行安装。

[0080] 当用户想要在冻结后的操作系统中安装第三方应用时,用户可以对所述终端进行操作(如点击系统解冻按钮等)向所述终端发送包管理解冻请求;或者,所述终端可以接收其他终端发送的用于指示解冻所述终端的操作系统的包管理解冻请求。所述终端可以检测并接收所述包管理解冻请求,其中,所述包管理解冻模块用于指示对所述冻结处理后的系统层进行解冻处理。所述终端可以响应所述包管理解冻请求,并根据所述包管理解冻请求的指示对所述冻结处理后的系统层进行解冻处理,以便允许在所述终端的操作系统中安装所述第三方应用。

[0081] 其中可选地,所述终端还可以对所述终端中的一些不安全的进程和/或服务(如恶意软件运行时所涉及到的一些进程或者服务)进行冻结处理,以保证所述终端的通信安全。

[0082] 实施例一:下面给出在所述终端的操作系统中分别进行应用APK冻结和系统冻结的详细阐述,以帮助理解应用冻结和系统冻结的区别。在应用APK冻结中,APK冻结可以从该APK应用出发,APK的正常运行与进程和服务有关,比如“唯品会”应用处于运行状态时存在有两个进程和一个服务(即是,LogService服务、com.achievo.vipshop进程和com.achievo.vipshop.remote进程),这个服务和两个进程是使得该唯品会应用能够正常运行的前提,进程和服务正常运行的前提是操作系统(如android系统)没有异常;冻结“唯品会”应用就是通过将系统的相关接口置为disable(不可使用标识),使得该唯品会应用处于假卸载状态,该APK相应的这两个进程和服务也不会启动,使得唯品会应用处于停止运行的状态。

[0083] 在系统冻结中,系统冻结并不是从APK应用出发将其相关接口置为disable,所述系统冻结可以从某一个功能项出发,冻结系统层的相应功能项,所有依赖于该功能项的APK都将不能正常运行。例如:位于系统层的包管理(有PackageManager和PackageManagerService)可以对应用层的包安装APK和权限管理模块进行管理,系统冻结就是要将比如“包管理”一样的功能项进行冻结,使得与所述包管理对应的包安装和权限管理就不能运行了,这样APK所依赖的相应进程和服务也将不会运行。

[0084] 进一步可以理解的是,在所述包管理被冻结后,某些第三方应用的一些功能如果用到了包管理中的一些功能,这些第三方应用的这一部分功能将丧失;也即是,如果在运行所述第三方应用中的某些功能程序时需要通过调用所述包管理才能运行,由于所述包管理已被冻结,因此所述第三方应用中的这些相应功能将被丧失、不能被用户使用。例如:android桌面会用到包管理中的获取应用信息的功能,包管理被冻结后,android桌面的这一部分功能将丧失掉。

[0085] 实施例二:下面以Android系统启动为例,具体给出了PMS服务启动以及应用安装详细阐述过程。由于在android系统启动过程中,ServerThread线程会运行,且该线程会拉起包括PMS服务在内的很多系统服务,下面从android系统启动过程中如何拉起PMS服务

启动以及应用如何安装的过程进行描述:1) Zygote进程启动了SystemServer组件, SystemServer会调用init1和init2方法进行一些系统初始化的工作;2) 在init2方法中, 会创建一个ServerThread线程, 该线程将调用run方法进行启动;3) 在该run方法中, 会调用PMS中的main方法, main方法中将创建一个PMS的实例m, 并将该实例m加入到ServiceManager (Android系统Binder进程间通信机制的守护进程, 负责管理系统中的Binder对象) 中;4) 在创建该实例m时, 将会扫描上述的五个文件目录: 首先扫描安装“system\framework”目录下的jar包, 接着扫描安装系统system\app的应用程序, 其次制造商的目录下\vendor\app应用包, 再接着扫描“data\app”目录, 即用户安装的第三方应用, 最后扫描“data\app-private”目录, 即安装DRM保护的APK文件(受保护的歌曲或受保护的视频是使用DRM保护的文件);5) 如果扫描到APK文件, PackageParser类将对APK文件进行解析, 将解析得到的应用信息结果保存到PMS中;6) PMS再调用Installer类中的install方法执行安装应用。

[0086] 根据上述的描述可以理解的是, 针对所述静默安装中的网络下载应用安装而言, 由于此时android系统已经启动, PMS服务也处于运行状态, APK下载完成后将调用PMS中的installPackage()函数进行应用的安装;针对adb工具安装而言, 由于此时android系统也已经启动, PMS服务也处于运行状态, 将通过\system\framework\目录下面的pm脚本和pm.jar(包管理库)进行APK的解析以及安装;针对从SD卡点击APK文件进行安装而言, 由于此时android系统也已经启动, PMS服务也处于运行状态, 最终也会调用到PMS中的installPackage方法进行应用的安装。

[0087] 综上所述, 从PMS服务启动过程以及PMS管理应用安装的过程可知, 想在所述终端中的操作系统中禁止第三方应用的安装, 所述终端可以从以下几个方面分析, 进而进行对应的冻结处理:

[0088] (1) android系统已经启动完成, PMS服务也处于运行状态, 所述终端可以直接将PMS服务进行冻结;这样若该服务停止运行, 就不能进行应用的安装。

[0089] (2) android系统启动过程中, 在创建好PMS的实例m后, 不进行启动, 不加入到ServiceManager中, 直接将ServiceManager进行冻结, 让PMS处于停止运行的状态, 这样也不会去扫描上述的五个目录进行系统应用和第三方应用的安装(这种情况进入launcher桌面后, 不会显示任何应用)。

[0090] (3) android系统启动过程中, 在扫描五个目录时, 可以选择只扫描系统目录, 不扫描安装第三方应用的目录(data\app), 这样可以不安装第三方应用。可以让android系统正常启动, 并且进入launcher桌面后, 初始化安装的各种系统应用能够正常运行, 未安装第三方应用。此时进入桌面后再对PMS进行冻结。

[0091] 由于用户在使用终端的过程中, 使用最多的还是android系统已经启动完成后进行应用安装, 此时可以通过将PMS服务直接冻结掉来阻止第三方应用的安装;示例性地, 给出一种应用安装的具体操作流程:

[0092] (1) 点击SD卡中的APK文件, 弹出安装界面;

[0093] (2) 点击安装按钮, 所述终端判定PMS服务是否被冻结, 如果被冻结, 则弹出PMS服务被冻结的通知信息, 停止应用的安装;如果未被冻结, 则PMS服务将调用PMS中的installPackage方法进行应用的安装。

[0094] 本发明实施例可通过接收包括有需要冻结的包管理的标识的包管理冻结请求,并根据所述包管理的标识查找所述包管理,接着对所述包管理进行分析,确定与所述包管理所关联的系统层,最后对所述系统层进行冻结处理,以禁止第三方应用在操作系统中进行安装,其中,所述对所述系统层进行冻结处理包括:对所述系统层中的框架framework、系统内核kernel、应用包安装驱动中的至少一个进行冻结处理。这样可通过对系统层中的框架framework、系统内核kernel、应用包安装驱动中的至少一个进行冻结处理,来阻止第三方应用的安装,达到保护终端操作系统的目的,从而提升了终端使用的安全性。

[0095] 请一并参阅图2,是本发明实施例的另一种第三方应用禁止安装方法的流程示意图,本发明实施例的所述方法可以包括如上所述的步骤S101至步骤S104,还包括如下步骤。

[0096] S201、对所述系统层中的框架framework进行分析,确定与所述框架framework对应的应用包安装进程和/或应用包安装服务。

[0097] S202、对所确定的所述应用包安装进程和/或所述应用包安装服务进行冻结处理。

[0098] 本发明实施例中,步骤S201和步骤S202是上述步骤S104中所述对所述系统层中的框架framework进行冻结处理的具体实现方式。

[0099] S203、当检测到所述第三方应用需要被安装时,发送用于提示所述操作系统禁止安装所述第三方应用的提示信息,停止所述第三方应用的安装。

[0100] S204、检测并获取当前处于后台运行的应用程序。

[0101] S205、对与所述后台运行的应用程序关联的程序运行服务、程序运行进程、程序运行广播接收器中的至少一个进行冻结处理,以便停止运行所述后台运行的应用程序。

[0102] S206、接收用于对所述冻结处理后的系统层进行解冻处理的包管理解冻请求。

[0103] S207、根据所述包管理解冻请求的指示对所述冻结处理后的系统层进行解冻处理,以允许所述第三方应用在操作系统中进行安装。

[0104] 本发明实施例可通过接收包括有需要冻结的包管理的标识的包管理冻结请求,并根据所述包管理的标识查找所述包管理,接着对所述包管理进行分析,确定与所述包管理所关联的系统层,最后对所述系统层进行冻结处理,以禁止第三方应用在操作系统中进行安装,其中,所述对所述系统层进行冻结处理包括:对所述系统层中的框架framework、系统内核kernel、应用包安装驱动中的至少一个进行冻结处理。这样可通过对系统层中的框架framework、系统内核kernel、应用包安装驱动中的至少一个进行冻结处理,来阻止第三方应用的安装,达到保护终端操作系统的目的,从而提升了终端使用的安全性。

[0105] 请参见图3,是本发明实施例的一种第三方应用禁止安装装置的结构示意图,本发明实施例的所述装置可以可设置在诸如智能手机、平板电脑、智能可穿戴设备等带通信网络功能的终端中,所述装置3包括:

[0106] 第一接收模块30,用于接收包管理冻结请求,其中,所述包管理冻结请求包括需要冻结的包管理的标识;

[0107] 查找模块31,用于根据所述包管理的标识查找所述包管理;

[0108] 确定模块32,用于对所述包管理进行分析,确定与所述包管理所关联的系统层;

[0109] 冻结模块33,用于对所述系统层进行冻结处理,以禁止第三方应用在操作系统中进行安装;其中,所述对所述系统层进行冻结处理包括:对所述系统层中的框架framework、系统内核kernel、应用包安装驱动中的至少一个进行冻结处理。

[0110] 本发明实施例中涉及各个模块的具体实现可参考图1至图2对应实施例中相关功能模块或者实施步骤的描述,在此不赘述。

[0111] 本发明实施例可通过接收包括有需要冻结的包管理的标识的包管理冻结请求,并根据所述包管理的标识查找所述包管理,接着对所述包管理进行分析,确定与所述包管理所关联的系统层,最后对所述系统层进行冻结处理,以禁止第三方应用在操作系统中进行安装,其中,所述对所述系统层进行冻结处理包括:对所述系统层中的框架framework、系统内核kernel、应用包安装驱动中的至少一个进行冻结处理。这样可通过对系统层中的框架framework、系统内核kernel、应用包安装驱动中的至少一个进行冻结处理,来阻止第三方应用的安装,达到保护终端操作系统的目的,从而提升了终端使用的安全性。

[0112] 请一并参阅图4,是本发明实施例的另一种第三方应用禁止安装装置的结构示意图,本发明实施例的所述装置4可以包括:上述的第一接收模块30、查找模块31、确定模块32、冻结模块33,其中,

[0113] 所述冻结模块33,具体用于对所述系统层中的框架framework进行分析,确定与所述框架framework对应的应用包安装进程和/或应用包安装服务;对所确定的所述应用包安装进程和/或所述应用包安装服务进行冻结处理。

[0114] 其中可选地,所述装置还包括:

[0115] 发送模块34,用于当检测到所述第三方应用要被安装时,发送用于提示所述操作系统禁止安装所述第三方应用的提示信息,停止所述第三方应用的安装。

[0116] 其中可选地,所述装置还包括:

[0117] 检测模块35,用于检测并获取当前处于后台运行的应用程序;

[0118] 所述冻结模块33,还用于对与所述后台运行的应用程序关联的程序运行服务、程序运行进程、程序运行广播接收器中的至少一个进行冻结处理,以便停止运行所述后台运行的应用程序。

[0119] 其中可选地,所述装置还包括:

[0120] 第二接收模块36,用于接收用于对冻结处理后的所述系统层进行解冻处理的包管理解冻请求;

[0121] 解冻模块37,用于根据所述包管理解冻请求的指示对所述冻结处理后的系统层进行解冻处理,以允许所述第三方应用在该所述操作系统中进行安装。

[0122] 本发明实施例中涉及各个模块的具体实现可参考图1至图2对应实施例中相关功能模块或者实施步骤的描述,在此不赘述。

[0123] 本发明实施例可通过接收包括有需要冻结的包管理的标识的包管理冻结请求,并根据所述包管理的标识查找所述包管理,接着对所述包管理进行分析,确定与所述包管理所关联的系统层,最后对所述系统层进行冻结处理,以禁止第三方应用在操作系统中进行安装,其中,所述对所述系统层进行冻结处理包括:对所述系统层中的框架framework、系统内核kernel、应用包安装驱动中的至少一个进行冻结处理。这样可通过对系统层中的框架framework、系统内核kernel、应用包安装驱动中的至少一个进行冻结处理,来阻止第三方应用的安装,达到保护终端操作系统的目的,从而提升了终端使用的安全性。

[0124] 再请参见图5,是本发明实施例的一种终端的结构示意图。所述终端可以为智能手机、平板电脑、智能可穿戴设备等带通信网络功能的设备,如图5所示,本发明实施例的所述

终端可以包括显示屏、按键、扬声器、拾音器等模块,并且还包括:至少一个总线501、与总线501相连的至少一个处理器502以及与总线501相连的至少一个存储器503,实现通信功能的通信装置505,为终端各耗电模块供电的电源装置504。

[0125] 所述处理器502可通过总线501,调用存储器503中存储的代码以执行相关的功能,其中,所述存储器503包括操作系统、数据传输应用程序。

[0126] 所述处理器502,用于接收包管理冻结请求,其中,所述包管理冻结请求包括需要冻结的包管理的标识;根据所述包管理的标识查找所述包管理;对所述包管理进行分析,确定与所述包管理所关联的系统层;对所述系统层进行冻结处理,以禁止第三方应用在操作系统中进行安装;其中,所述对所述系统层进行冻结处理包括:对所述系统层中的框架framework、系统内核kernel、应用包安装驱动中的至少一个进行冻结处理。

[0127] 进一步可选地,所述处理器502还用于对所述系统层中的框架framework进行分析,确定与所述框架framework对应的应用包安装进程和/或应用包安装服务;对所确定的所述应用包安装进程和/或所述应用包安装服务进行冻结处理。

[0128] 进一步可选地,所述处理器502还用于当检测到所述第三方应用要被安装时,发送用于提示所述操作系统禁止安装所述第三方应用的提示信息,停止所述第三方应用的安装。

[0129] 进一步可选地,所述处理器502还用于检测并获取当前处于后台运行的应用程序;对与所述后台运行的应用程序关联的程序运行服务、程序运行进程、程序运行广播接收器中的至少一个进行冻结处理,以便停止运行所述后台运行的应用程序。

[0130] 进一步可选地,所述处理器502还用于接收用于对冻结处理后的所述系统层进行解冻处理的包管理解冻请求;根据所述包管理解冻请求的指示对所述冻结处理后的系统层进行解冻处理,以允许所述第三方应用在所述操作系统中进行安装。

[0131] 本发明实施例可通过接收包括有需要冻结的包管理的标识的包管理冻结请求,并根据所述包管理的标识查找所述包管理,接着对所述包管理进行分析,确定与所述包管理所关联的系统层,最后对所述系统层进行冻结处理,以禁止第三方应用在操作系统中进行安装,其中,所述对所述系统层进行冻结处理包括:对所述系统层中的框架framework、系统内核kernel、应用包安装驱动中的至少一个进行冻结处理。这样可通过对系统层中的框架framework、系统内核kernel、应用包安装驱动中的至少一个进行冻结处理,来阻止第三方应用的安装,达到保护终端操作系统的目的,从而提升了终端使用的安全性。

[0132] 本发明实施例还提供一种计算机存储介质,其中,该计算机存储介质可存储有程序,该程序执行时包括上述方法实施例中记载的任何音频播放应用的操作方法的部分或全部步骤。

[0133] 需要说明的是,对于前述的各方法实施例,为了简单描述,故将其都表述为一系列的动作组合,但是本领域技术人员应该知悉,本发明并不受所描述的动作顺序的限制,因为依据本发明,某些步骤可以采用其他顺序或者同时进行。其次,本领域技术人员也应该知悉,说明书中所描述的实施例均属于优选实施例,所涉及的动作和模块并不一定是本发明所必须的。

[0134] 在上述实施例中,对各个实施例的描述都各有侧重,某个实施例中未详述的部分,可以参见其他实施例的相关描述。

[0135] 在本申请所提供的几个实施例中,应该理解到,所揭露的装置,可通过其它的方式实现。例如,以上所描述的装置实施例仅仅是示意性的,例如所述单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,例如多个单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另一点,所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口,装置或单元的间接耦合或通信连接,可以是电性或其它的形式。

[0136] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0137] 另外,在本发明的各个实施例中的各功能单元可以集成在一个处理单元中,也可以是各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现,也可以采用软件功能单元的形式实现。

[0138] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用,可以存储在一个计算机可读取存储介质中。基于这样的理解,本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以使得一台计算机设备(可为个人计算机、服务器或者网络设备)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括:U盘、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

[0139] 以上所述,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应当理解: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,并不使相应技术方案的本质脱离本发明各实施例技术方案的范围。

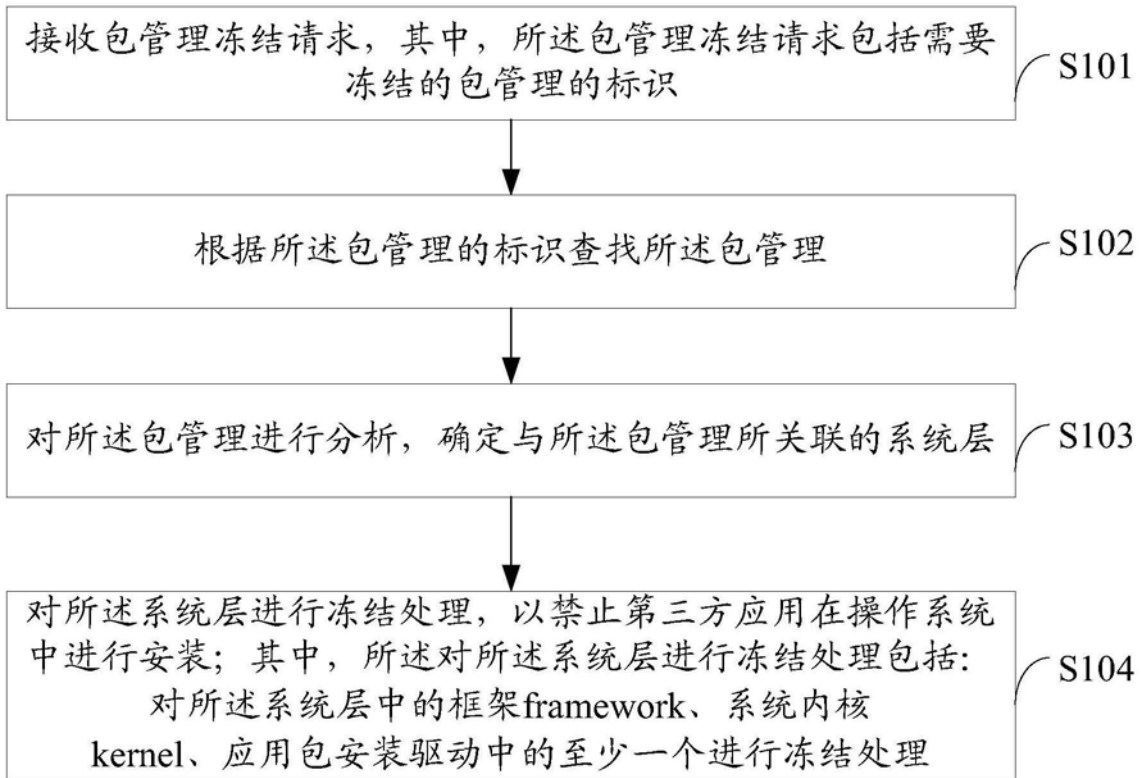


图1

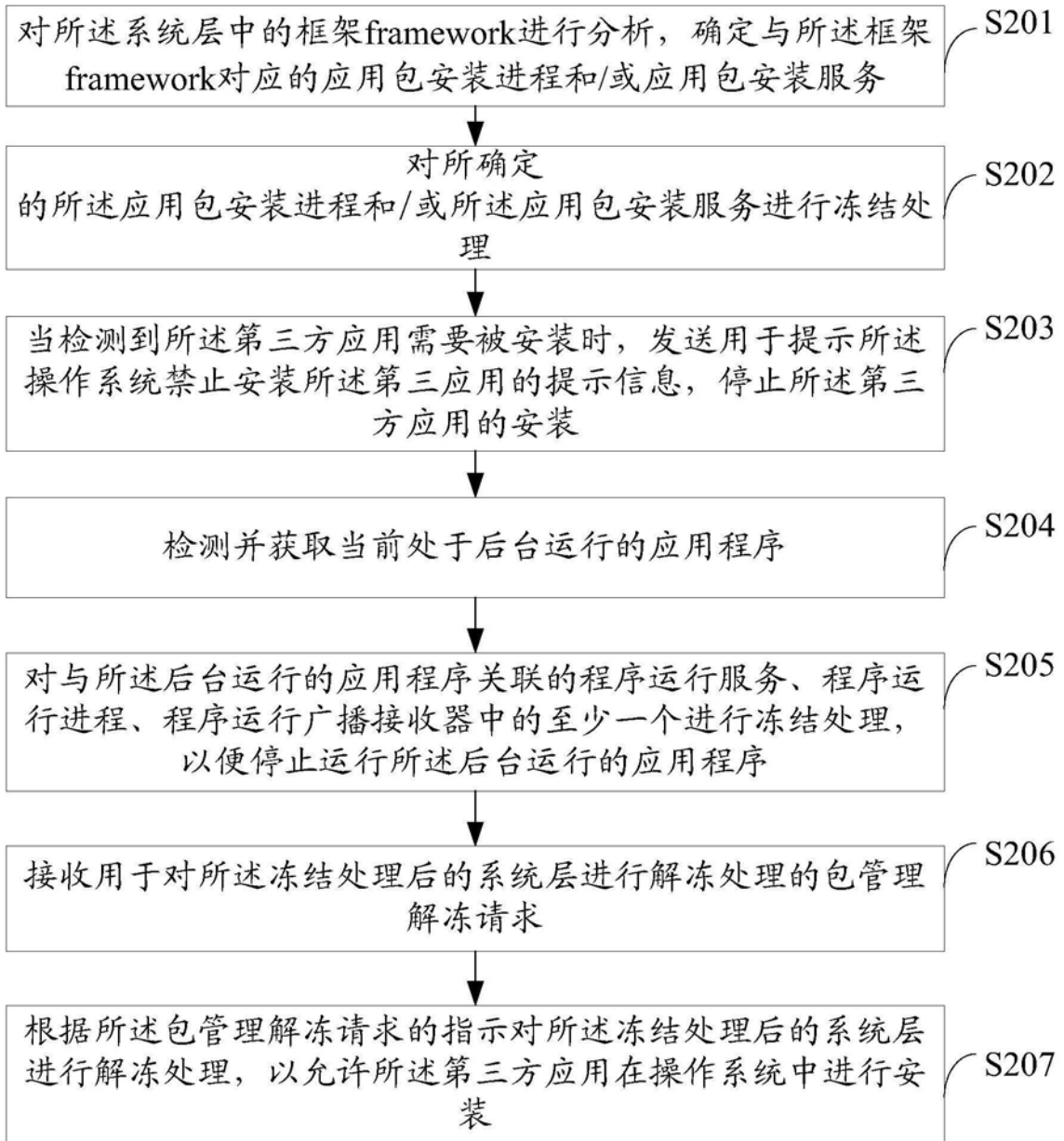


图2



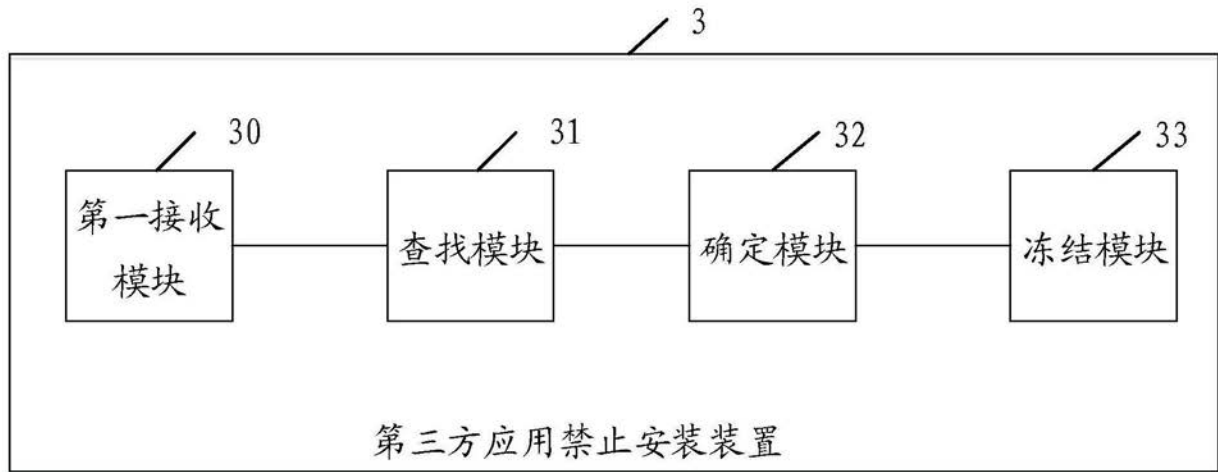


图3

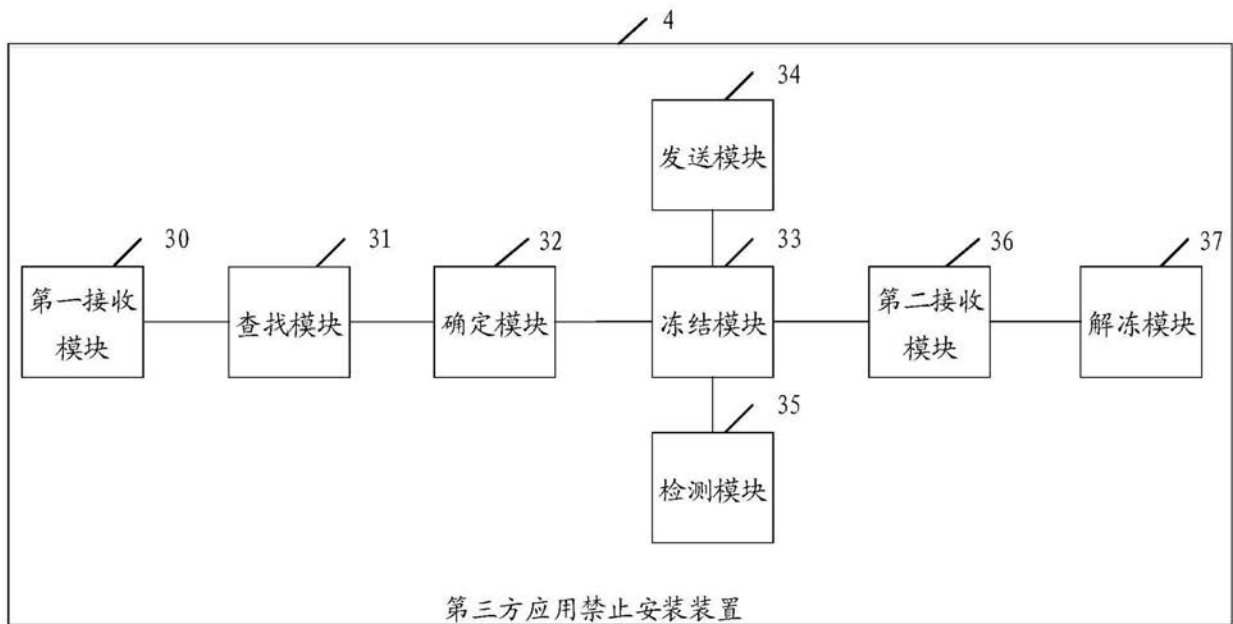


图4

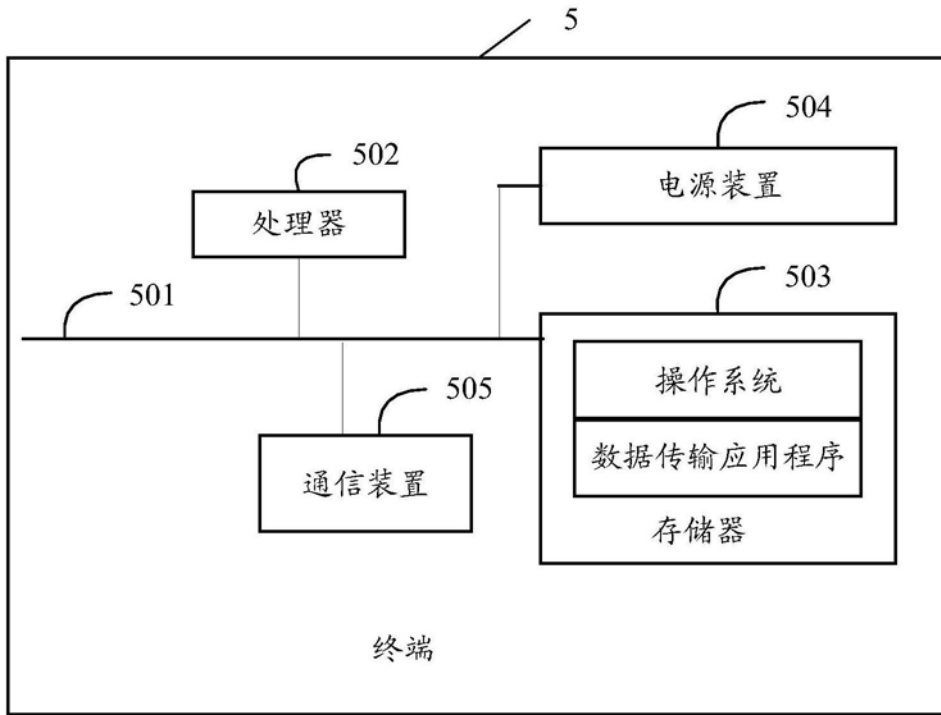


图5