(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 106557669 A
(43)申请公布日 2017.04.05

(21)申请号 201510640948.8

(22)申请日 2015.09.30

(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 王务志 王军

(74)专利代理机构 北京国昊天诚知识产权代理有限公司 11315
代理人 许志勇 刘戈

(51)Int.Cl.
G06F 21/12(2013.01)

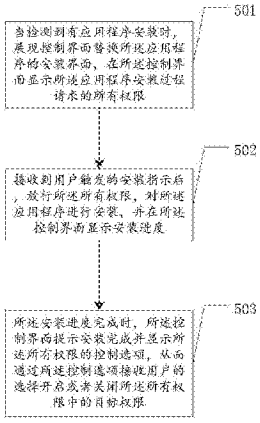
权利要求书2页 说明书13页 附图7页

(54)发明名称

一种应用程序安装过程的权限控制方法及装置

(57)摘要

本申请公开了一种程序安装过程的权限控制方法及装置。当检测到有应用程序安装时，展现控制界面替换所述应用程序的安装界面，在所述控制界面显示所述应用程序安装过程请求的所有权限；接收到用户触发的安装指示后，放行所述所有权限，对所述应用程序进行安装，并在所述控制界面显示安装进度；所述安装进度完成时，所述控制界面提示安装完成并显示所述所有权限的控制选项，从而通过所述控制选项接收用户的选择开启或者关闭所述所有权限中的目标权限。申请通过对待安装的应用程序进行权限监测，在安装之前拦截安装获取应用程序所请求的权限信息，并对应用程序的访问权限进行了控制，一方面保证了用户的信息数据安全，另一方面保证程序正常运转。



CN 106557669 A

1.一种程序安装过程的权限控制方法,其特征在于,

当检测到有应用程序安装时,展现控制界面替换所述应用程序的安装界面,在所述控制界面显示所述应用程序安装过程请求的所有权限;

接收到用户触发的安装指示后,放行所述所有权限,对所述应用程序进行安装,并在所述控制界面显示安装进度;

所述安装进度完成时,所述控制界面提示安装完成并显示所述所有权限的控制选项,从而通过所述控制选项接收用户的选择开启或者关闭所述所有权限中的目标权限。

2.如权利要求1所述的方法,其特征在于,当检测到有应用程序安装时,在展现控制界面替换所述应用程序的安装界面之前,进一步包括,

采用中断机制对所述应用程序的应用程序编程接口进行监听,从而中断所述应用程序的安装进程;

通过调用框架层中的所述应用程序编程接口,得到包含权限信息的APK文件;

对所述APK进行解析获得所述应用程序请求获取的所有权限的信息。

3.如权利要求2所述的方法,其特征在于,对所述APK进行解析获得所述应用程序请求获取的所有权限的信息,进一步包括,

解压所述APK文件并进行反编译,获取AndroidManifest.xml配置文件;

对所述配置文件进行逐行扫描,提取所述应用程序请求的所有权限。

4.如权利要求1所述的方法,其特征在于,通过所述控制选项接收用户的选择开启或者关闭所述所有权限中的目标权限,进一步包括,

监听用户对所权限信息的控制选项的操作结果,根据所述操作结果对所述应用程序的权限进行配置。

5.如权利要求1所述的方法,其特征在于,通过控制选项接收用户的选择开启或者关闭所述所有权限中目标权限之后,进一步包括,

当通过控制选项接收用户的选择开启所述所有权限中的目标权限时,若运行所述应用程序,则拦截所述应用程序请求目标权限以外的其他权限;当通过控制选项接收用户的选择关闭所述所有权限中的目标权限时,运行所述应用程序时,拦截所述应用程序请求的所述所有权限中的目标权限。

6.一种程序安装过程的权限控制装置,其特征在于,包括如下模块:

权限监测模块,用于当检测到有应用程序安装时,展现控制界面替换所述应用程序的安装界面,在所述控制界面显示所述应用程序安装过程请求的所有权限;

安装管理模块,用于接收到用户触发的安装指示后,放行所述所有权限,对所述应用程序进行安装,并在所述控制界面显示安装进度;

权限配置模块,用于当所述安装进度完成时,所述控制界面提示安装完成并显示所述所有权限的控制选项,从而通过所述控制选项接收用户的选择开启或者关闭所述所有权限中的目标权限;

显示模块,用于与其它模块结合,进行显示。

7.如权利要求6所述的装置,其特征在于,所述权限监测模块,进一步包括监听模块,

所述监听模块,用于采用中断机制对所述应用程序的应用程序编程接口进行监听,从而中断所述应用程序的安装进程;

通过调用框架层中的所述应用程序编程接口，得到包含权限信息的 APK 文件；

对所述 APK 进行解析获得所述应用程序请求获取的所有权限的信息。

8. 如权利要求 7 所述的装置，其特征在于，所述权限监测模块，进一步包括权限解析模块：

所述权限解析模块，解压所述 APK 文件并进行反编译，获取 AndroidManifest.xml 配置文件；

对所述配置文件进行逐行扫描，提取所述应用程序请求的所有权限。

9. 如权利要求 6 所述的装置，其特征在于，所述权限配置模块进一步用于，

监听用户对所权限信息的控制选项的操作结果，根据所述操作结果对所述应用程序的权限进行配置。

10. 如权利要求 6 所述的装置，其特征在于，所述权限配置模块，进一步用于，

当通过控制选项接收用户的选择开启所述所有权限中的目标权限时，若运行所述应用程序，则拦截所述应用程序请求目标权限以外的其他权限；当通过控制选项接收用户的选择关闭所述所有权限中的目标权限时，运行所述应用程序时，拦截所述应用程序请求的所述所有权限中的目标权限。

一种应用程序安装过程的权限控制方法及装置

技术领域

[0001] 本申请属于移动终端安全领域，具体地说，涉及一种应用程序安装过程的权限控制方法。

背景技术

[0002] Android是一种基于Linux的自由及开放源代码的操作系统，主要使用于移动设备，如智能手机和平板电脑，由Google公司和开放手机联盟领导及开发。由于Android的开放性，它允许任何移动终端厂商加入到Android联盟中来。显著的开放性可以使其拥有更多的开发者，随着用户和应用的日益丰富，大量的应用程序鱼龙混杂，难免会有一些应用程序被嵌入某些非法行为，从而导致用户的安全受到一定程度的威胁。

[0003] 应用程序安装时往往需要在后台获取系统的一些权限，有些权限确实涉及到个人的隐私，也严重危急信息安全，比如用户的个人信息。通常系统优化、地图、输入法、浏览器、数据同步管理等应用需要用到，它可以在未经允许的情况下，直接调用手机中联系人的资料以及你的日历活动，就连浏览器的历史记录和收藏书签也不会放过，还能自动发送电子邮件。对于有些需要用户付费的服务，应用程序在用户毫无察觉的情况下在后台拨打电话、发送短消息。

[0004] 有些应用程序需获取用户的位置，通过GPS定位芯片或者基站定位获得手机所在的位置。但也不乏有些间谍程序，配合网络通信权限，能实时将地理位置发送出去，实现手机跟踪。上述的网络通信权限允许应用在运行过程中从网络下载数据，偷偷消耗流量。

[0005] 现实中，许多应用程序会同时触碰很多权限，这对于手机系统和用 户数据来说是不安全的，那么对于应用程序的权限就要进行控制。在选择控制时机时，一方面要保证安全，另一方面要保证应用程序正常运转。

[0006] 如果在程序安装之前就对一些涉及到的权限进行限制，可能会导致这个程序完全无法完成安装，这样用户体验就会很差；而如果在安装完成之后，才对访问权限进行限制，那从安装完成时的一段时间程序已经在后台使用权限做了很多数据的窃取，造成用户数据的不安全。

[0007] 因此，为了解决上述缺陷，本申请提供了一种应用程序安装过程的权限控制方法和装置。

发明内容

[0008] 有鉴有鉴于此，本申请所要解决的技术问题是提供了一种应用程序安装过程的权限控制方法及装置。

[0009] 本申请一种应用程序安装过程的权限控制方法，包括如下步骤：

[0010] 当检测到有应用程序安装时，展现控制界面替换所述应用程序的安装界面，在所述控制界面显示所述应用程序安装过程请求的所有权限；

[0011] 接收到用户触发的安装指示后，放行所述所有权限，对所述应用程序进行安装，并

在所述控制界面显示安装进度；

[0012] 所述安装进度完成时，所述控制界面提示安装完成并显示所述所有权限的控制选项，从而通过所述控制选项接收用户的选择开启或者关闭所述所有权限中的目标权限。

[0013] 当检测到有应用程序安装时，在展现控制界面替换所述应用程序的安装界面之前，进一步包括，

[0014] 采用中断机制对所述应用程序的应用程序编程接口进行监听，从而中断所述应用程序的安装进程。

[0015] 采用中断机制对所述应用程序接口进行监听，进一步包括：

[0016] 对所述应用程序的行为进行监听，通过调用框架层中的所述应用程序编程接口，得到包含权限信息的APK文件；对所述APK进行解析获 得所述应用程序请求获取的所有权限的信息。

[0017] 对所述APK进行解析获得所述应用程序请求获取的所有权限的信息，进一步包括：

[0018] 解压所述APK文件并进行反编译，获取AndroidManifest.xml配置文件；

[0019] 对所述配置文件进行逐行扫描，提取所述应用程序请求的所有权限。

[0020] 通过所述控制选项接收用户的选择开启或者关闭所述所有权限中的目标权限，进一步包括：

[0021] 监听用户对所权限信息的控制选项的操作结果，根据所述操作结果对所述应用程序的权限进行配置。

[0022] 通过控制选项接收用户的选择开启或者关闭所述所有权限中目标权限之后，进一步包括：

[0023] 当通过控制选项接收用户的选择开启所述所有权限中的目标权限时，若运行所述应用程序，则拦截所述应用程序请求目标权限以外的其他权限；当通过控制选项接收用户的选择关闭所述所有权限中的目标权限时，运行所述应用程序时，拦截所述应用程序请求的所述所有权限中的目标权限。

[0024] 本申请一种应用程序安装过程的权限控制装置，包括如下模块：

[0025] 权限监测模块，用于当检测到有应用程序安装时，展现控制界面替换所述应用程序的安装界面，在所述控制界面显示所述应用程序安装过程请求的所有权限；

[0026] 安装管理模块，用于接收到用户触发的安装指示后，放行所述所有权限，对所述应用程序进行安装，并在所述控制界面显示安装进度；

[0027] 权限配置模块，用于当所述安装进度完成时，所述控制界面提示安装完成并显示所述所有权限的控制选项，从而通过所述控制选项接收用 户的选择开启或者关闭所述所有权限中的目标权限；

[0028] 显示模块，用于与其它模块结合，进行显示。

[0029] 进一步地，所述权限监测模块，进一步包括监听模块，所述监听模块，用于采用中断机制对所述应用程序编程接口进行监听，从而中断所述应用程序的安装进程。

[0030] 进一步地，所述所述监听模块，进一步还用于对所述应用程序的行为进行监听，通过调用框架层中的所述应用程序编程接口，得到包含权限信息的APK文件；通过解析APK文件得到所述所有权限的信息。

[0031] 进一步地，所述权限监测模块还包括权限解析模块，所述权限解析模块，用于解压所述 APK 文件并进行反编译，获取 AndroidManifest.xml 配置文件；

[0032] 对所述配置文件进行逐行扫描，提取所述应用程序请求的所有权限。

[0033] 进一步地，所述显示模块还用于，对提取到的所述应用程序请求的所有权限信息进行列表并通过所述权限信息的控制选项显示给用户。

[0034] 进一步地，所述权限配置模块，还用于，当通过所述控制选项接收用户的选择开启所述所有权限中的目标权限时，若运行所述应用程序，则拦截所述应用程序请求目标权限以外的其他权限；当通过控制选项接收用户的选择关闭所述所有权限中的目标权限时，运行所述应用程序时，拦截所述应用程序请求的所述所有权限中的目标权限。

[0035] 与现有技术相比，本申请通过对待安装的应用程序进行权限监测，在安装之前拦截安装获取应用程序所请求的权限信息，并对应用程序的访问权限进行了控制，一方面保证了用户的信息数据安全，另一方面保证程序正常运转。

附图说明

[0036] 此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

[0037] 此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

[0038] 图 1 是本申请实施例一的技术流程图；

[0039] 图 2 是本申请一种应用程序安装过程的权限控制方法的用户操作流程图；

[0040] 图 3 是本申请实施例三提取应用程序请求访问的所有权限的技术流程图；

[0041] 图 4 是本申请一种应用程序安装过程的权限控制方法的又一技术流程图；

[0042] 图 5 是本申请一种应用程序安装过程的权限控制方法的可视化界面跳转流程图；

[0043] 图 6 是本申请实施例五的装置结构示意图；

[0044] 图 7 是本申请实施例六的装置结构及功能示意图。

具体实施方式

[0045] 以下将配合附图及实施例来详细说明本申请的实施方式，藉此对本申请如何应用技术手段来解决技术问题并达成技术功效的实现过程能充分理解并据以实施。

[0046] 本发明实施例中，所述应用程序的安装主要针对于基于 Android 系统的各类终端，包括但不限于 Android 手机、平板电脑、笔记本电脑、车载终端等等。

[0047] 实施例一

[0048] 图 1 是本发明实施例一的技术流程图，结合图 1，本发明实施例一种应用程序安装过程的权限控制方法在移动终端的实现主要包括如下 的步骤：

[0049] 步骤 101：当检测到有应用程序安装时，拦截所述应用程序的安装进程，监测所述应用程序请求获取的所有权限，并将所监测到的所述所有权限展示给用户；

[0050] 权限是对 Android 设备上代码或数据的访问所施加的一种限制，以防止关键数据和代码被滥用而给用户带来不同程度的损害。一个 Android 应用程序可能需要权限才能调用 Android 系统的功能；一个 Android 应用也可能被其它应用调用，因此它也需要声明调用

自身所需要的权限。

[0051] 当应用程序作为权限的需求方时，如果一个应用程序需要使用到系统提供的API（应用程序编程接口）及其他服务，而这些API和服务受权限保护，需要在AndroidManifest.xml文件中定义所需访问API以及服务的权限；从另一角度来说，当应用程序是授权方时，如果一个应用里提供了其他应用需要访问的功能，为安全起见，防止不具备访问条件的应用程序非法访问，需要在代码中指定访问这些功能所需要的访问权限。无论是需求方还是授权方都需要对应用程序的权限进行设置。

[0052] Android提供了大约有130多种内置的权限，都是android.Manifest.permission类的静态成员。Android权限有时也称之为Manifest权限，它们控制着各种系统操作，如电话呼叫(CALL_PHONE)、照相(CAMERA)、网络(INTERNET)、键盘输入(READ_INPUT_STATE)、写短信(WRITE_SMS)等。除了内置的权限以外，任何一个应用程序可以自定义适当的权限，以供其他应用程序访问。Android权限主要有4种级别：Normal、Dangerous、Signature和SignatureOrSystem。

[0053] Normal级别的权限产生的危险严重性较小，适合给用户一个警告予以考虑；Dangerous级别的权限意味着用户可能会遇到某些意外的危险，Android会在安装时提示用户是否需要这些权限；Signature界别的权限特殊性在于一旦一个应用程序声明权限为Signature级别，仅限于其他与该应用程序具有相同签名的应用程序可以访问它；SignatureOrSystem权限的级别最高，属于一种特殊的Signature权限，第三方的应用程序是无法访问持有这种权限的应用程序。这种权限的保护级别需要系统像应用程 序或与系统镜像具有相同签名的应用程序才可以访问。此权限有助于整合系统编译，通常用于第三方应用程序整合，一般不适用于开发者。

[0054] Android权限机制的实现贯穿应用层、框架层、系统层。应用层通过设置Android-Manifest.xml中<uses-permission>指定对应权限，再映射到底层的用户和组权限；框架层通过设置platform.xml中<permission>指定其对应权限，platform.xml文件位于frameworks/base/data/etc/；系统层的权限定义在system/core/include/private/android_filesystem_config.h文件中。

[0055] 本申请实施例中，应用程序作为权限的需求方时，向被安装的Android平台请求一些权限。以Android系统手机安装应用程序为例，假设在Android手机上安装一款社交软件，这款社交软件可以与用户的通信录进行匹配或者绑定，查看用户通信录中已绑定该社交软件的用户，在网络状态下与之互通信或互加好友；该所述社交软件还可以向通信录中的好友通过短信发送邀请链接；所述社交软件还可以与好友互相定位对方的地理位置，还可以通过相机与好友分享照片等。这样的社交软件对于Android用户并不陌生，从以上的功能描述，这样一款常用的社交软件安装在Android平台上需要获取网络状态信息权限、WI-FI网络状态信息权限、读取用户联系人的权限、发送短信的权限、使用照相机的权限、使用GPS定位权限等等。

[0056] 通常，一款应用程序需安装的权限不止上述举例的种类，而用户通常在安装的时候不知道应用程序需要对哪些权限进行访问，当然也并非所有的权限都在用户的默许下，甚至有些恶意软件试图获取一些涉及到用户隐私的信息用于非法途径。因此，在应用程序安装的时候，监测所述应用程序请求获取的所有权限，同时拦截所述应用程序的安装进程，

并将所监测到的所述所有权限展示给用户，这样做避免了在应用程序安装之前对应用程序访问的权限进行控制从而导致应用程序无法安装，另一方面也避免了应用程序安装完成之后在后台利用权限进行数据的窃取。

[0057] 步骤 102：监听用户的操作过程，当检测到用户触发安装功能，则响应所述触发放行所述安装进程以及所述所有权限；

[0058] 本发明实施例中，后台监测到应用程序请求获取的权限之后，会生成权限列表通过显示界面对用户作出提示。本发明实施例中所述提示可以是一个下拉菜单，用户点击所述下拉菜单可以查看所述应用程序安装过程中需要获取的所有权限。当然本发明实施例中所述提示也可以是一个弹窗，或者是一个通知栏的推送等，本发明并不限于此。

[0059] 将所述权限列表显示给用户之后，用户会获知所述应用程序请求访问的所有权限信息，用户根据意愿选择选择安装或者放弃安装。后台监测用户的操作，当检测到用户触发安装功能之后，后台响应所述触发，放行所述被拦截的安装进程以及所述所有的权限。此时放行所述所有权限可以保证所述应用程序的正确安装。

[0060] 步骤 104：在检测所述安装进程完成时，显示所述所有权限的控制选项；

[0061] 本发明实施例中，实时监测应用程序的所述安装进度并通过控制界面进行显示，显示方式可以为传统的直线进度条显示方式，可以是圆形或齿轮型旋转进度显示方式，也可以是配有动画的 loading 图案，或者也可以是上述任意方式的组合形式。在安装过程中提供趣味的进度显示方式，能够缓解用户等待安装时的无聊和焦虑，同时有效地让用户明确知道目前的安装状态，并对安装完成的时间有一个直观的预期。当然，本发明的进度提示方法包括但不限于此。

[0062] 当后台监测到安装进度达到 100％时，控制界面提示用户安装完成并显示权限控制选项。其中，所述权限控制选项可以是一个列表，列表中展示应用程序安装请求访问的所有权限，每一权限都对应一个关闭和一个开启的选项供用户进行选择，用户可以根据意愿选择关闭或者开启部分目标权限。本发明实施例中，所有权限都是默认开启的，当然本发明包括但不限于此。

[0063] 步骤 105：获取用户对所述系统权限的控制选项的操作结果，并根据所述操作结果，对所述应用程序中用户所允许开放的目标权限进行配置。

[0064] 本发明实施例中，实时监测用户对所述权限控制选项的操作，记录用户支持开启或者禁用的目标权限，与此同时，通过控制界面对用户进行提示保存权限设置，并根据用户允许开放的所述目标权限进行权限配置。待权限配置完成后，用户可通过控制界面的退出界面选项结束此次安装或者通过开启应用程序的选项直接开启安装完成的所述应用程序，值得注意的是，当通过所述控制选项接收用户的选择开启所述所有权限中的目标权限时，若运行所述应用程序，则拦截所述应用程序请求目标权限以外的其他权限；当通过控制选项接收用户的选择关闭所述所有权限中的目标权限时，运行所述应用程序时，拦截所述应用程序请求的所述所有权限中的目标权限。

[0065] 实施例二

[0066] 图 2 是本发明实施例二应用程序安装过程的权限控制方法的用户操作流程图，结合图 2，本发明实施例 Android 平台下的应用程序安装步骤如下：

[0067] 步骤 201：启动安装，进入安装界面；

[0068] 应用程序安装包 APK 是 AndroidPackage 的缩写，即 Android 安装包。通过将 APK 文件直接传到 Android 设备中执行即可安装。

[0069] 通常用户在 Android 设备中安装应用程序通过以下几种方式：

[0070] 其一，可以从资源下载区下载应用程序安装包，存放在设备的 SD 卡上，当然也不限于是设备的内部存储空间中；然后通过文件管理器找到此安装包，对其进行触发即可激活安装，这样就可以在 Android 设备里直接进行应用程序的安装。

[0071] 其二，可以用 USB 数据线连接电脑，在电脑上通过移动设备助手 PC 端等安装软件对 Android 设备进行安装。

[0072] 其三，是用户最常用的安装方式，即通过设备中各样的助手以及应用市场直接进行安装，此安装方式最为简单快捷。

[0073] 本发明实施例适用于上述所有的安装方式，当然也并不仅限于上述的几种。无论是哪一种安装方式，后台一旦检测到有应用程序的安装，就会对权限进行监测以及后续步骤操作。

[0074] 步骤 202：当安装界面被控制界面替换时，根据控制界面提示查看所述应用程序请求访问的所有权限并选择是否继续安装；

[0075] 本发明实施例中，控制界面对安装界面的替换可以是弹窗覆盖形式，可以是转页替换形式，也可以托盘形式展现，本发明并不限于此。

[0076] 本发明实施例中控制界面的提示可以是一个下拉菜单，用户点击所述下拉菜单可以查看所述应用程序安装过程中需要获取的所有权限。当然本发明实施例中所述提示也可以是一个弹窗，或者是一个通知栏的推送等，本发明并不限于此。

[0077] 将所述权限列表显示给用户之后，用户会获知所述应用程序请求访问的所有权限信息，用户可以在明确安装风险之后根据意愿选择选择安装或者放弃安装。

[0078] 步骤 203：安装完成后，查看应用程序需要访问的权限菜单，对所述权限菜单进行操作，选择开启或者禁用部分目标控制选项。

[0079] 安装过程中，用户可以通过控制界面查看安装进度，待安装进度达到 100％时，查看控制界面显示的权限菜单，根据意愿选择开启支持的权限或者关闭希望能够禁用的权限。

[0080] 步骤 204：保存权限设置并可以选择打开所述应用程序或者退出界面。

[0081] 本发明实施例中，若是用户确定了对权限的开启或关闭并进行了保存，则后台会自动记录用户对权限的选择并为所述应用程序进行权限配置。此时用户可以选择退出当前界面结束安装，也可以通过当前界面的开启应用程序选项直接激活启动所述应用程序。此时应用程序运行时，已经根据用户的设置对用户选择关闭的权限进行禁用，用户便可放心使用。

[0082] 本申请实施例的安装流程中，一方面保证了安装过程的正常进行， 另一方面将应用程序所请求的权限展示给用户一目了然由用户自主选择支持或者禁用某些权限，在保障用户信息安全的同时，极大地提升了用户的使用体验。

[0083] 实施例三

[0084] 图 3 是本发明实施例三的技术流程图，结合图 3，本发明实施例监测所述应用程序请求获取的所有权限，同时拦截所述应用程序的安装进程进一步包括如下步骤：

[0085] 步骤 301 :对所述应用程序的行为进行监听,通过调用框架层中的应用程序编程接口,得到包含权限信息的 APK 文件 ;

[0086] Android 分为四个层,从高层到低层分别是应用程序层、应用程序框架层、系统运行库层和 linux 核心层,本发明实施例中,通过调用框架层中的应用程序编程接口即 API,对框架层中的应用程序安装行为进行监听。

[0087] API(Application Programming Interface,应用程序编程接口)是操作系统留给应用程序的一个调用接口,应用程序通过调用操作系统的 API 而使操作系统去执行应用程序的命令(动作)。

[0088] 步骤 302 :解压所述 APK 文件并进行反编译,获取 AndroidManifest.xml 配置文件 ;

[0089] 基于 Android 的应用程序的安装文件通常是以 APK 为后缀,APK 文件其实是 zip 格式,但后缀名被修改为 apk,通过 UnZip 解压后,可以看到字节码 Dex 文件 (classes.dex)、资源文件 (res)、配置文件 (AndroidManifest.xml) 和签名信息文件 (META-INF)。其中,Dex 是 DalvikVM executes 的简称,即 Android Dalvik 执行程序。利用解析工具(包括但不限于 :apktool、apkmanager、dex 2java、XJad 以及 Google 发布的 Android SDK 提供的反编译工具 dexdump.exe 等)对 Dex 文件进行反编译,将其转化为可读的 Java 文件即可以获得所述应用程序的源码信息。

[0090] AndroidManifest.xml 是每个 APK 应用程序都必须包含的文件,它 描述了应用程序的名字、版本、权限、引用文库等信息。因此,若要读取所述应用程序请求访问的权限信息,就必须获取获取 AndroidManifest.xml 配置文件。

[0091] 步骤 303 :对所述配置文件进行逐行扫描,提取所述应用程序请求的所有权限。

[0092] AndroidManifest.xml 配置文件的清单中,包含许多元素,其中包括权限元素。

[0093] 如果应用程序需要访问一个被权限保护的功能,那么它必须在清单文件中用 <uses-permission> 元素来声明其要求的权限。每种权限都会有一个唯一的标签来标识。通常,标签指明了要约束的操作。例如 :

[0094] android.permission.WRITE_SMS< 允许程序写短信 >

[0095] android.permission.READ_SMS< 允许程序读取短信息 >

[0096] android.permission.READ_OWNER_DATA< 允许程序读取所有者数据 >

[0097] android.permission.SEND_SMS< 允许程序发送 SMS 短信 >

[0098] android.permission.WRITE_CALENDAR< 允许一个程序写入用户日历数据 >

[0099] android.permission.WRITE_CONTACTS< 允许程序写入联系人数据 >

[0100] 因此,通过对所述配置文件 AndroidManifest.xml 进行逐行扫描即可以得到所述应用程序所请求获取的所有权限信息。

[0101] 实施例四

[0102] 图 4 是本发明实施例四的技术流程图,结合图 4,本发明实施例一种应用程序安装过程的权限控制方法主要包括如下步骤 :

[0103] 步骤 401 :当检测到有应用程序安装时,用于采用中断机制对所述应用程序编程接口进行监听,从而中断所述应用程序的安装进程。

[0104] 本发明实施例中,可以采用 hook(挂钩或钩子)机制实现对 framework 层中的用

于实现安装应用程序的接口(API)进行监听。hook机制是一种截获windows系统中某应用程序或者所有进程的消息的一种技术,hook机制允许应用程序截获处理操作系统的消息或特定事件。钩子实际上是一个处理消息的程序段,通过系统调用,把它挂入系统。每当特定的消息发出,在没有到达目的窗口前,钩子程序就先捕获该消息,亦即钩子函数先得到控制权。这时钩子函数既可以加工处理(改变)该消息,也可以不作处理而继续传递该消息,还可以强制结束消息的传递。在本发明实施例中,采用hook机制中断安装应用程序的过程,实现在应用程序安装之前获取相关信息,当然本发明包括但不限于这一种中断拦截方法。

[0105] 实现一个钩子一般有三个步骤,首先创建钩子,有专门的API;创建成功后,消息将会传给指定的处理函数。然后在消息处理函数中分析收到的消息,做相应的处理。最后,钩子用完后,用相应的API消毁钩子。钩子过程有许多类型,每种钩子可以拦截并处理相应种类的消息,本发明实施例中需将idHook(钩子过程类型)设置为相应的值。

[0106] 步骤402:对所述应用程序的行为进行监听,通过调用框架层中的应用程序编程接口(API),得到包含权限信息的APK文件;

[0107] API(Application Programming Interface,应用程序编程接口)是操作系统留给应用程序的一个调用接口,应用程序通过调用操作系统的API而使操作系统去执行应用程序的命令(动作)。

[0108] 步骤403:解压所述APK文件并进行反编译,获取AndroidManifest.xml配置文件;

[0109] AndroidManifest.xml是每个APK应用程序都必须包含的文件,它描述了应用程序的名字、版本、权限、引用文库等信息。因此,若要读取所述应用程序请求访问的权限信息,就必须获取获取AndroidManifest.xml配置文件。

[0110] 步骤404:对所述配置文件进行逐行扫描,提取所述应用程序请求的所有权限;

[0111] AndroidManifest.xml配置文件的清单中,包含许多元素,其中包括权限元素。

[0112] 如果应用程序需要访问一个被权限保护的功能,那么它必须在清单文件中用<uses-permission>元素来声明其要求的权限。每种权限都会有一个唯一的标签来标识。通常,标签指明了要约束的操作。例如:

[0113] android.permission.WRITE_SMS< 允许程序写短信 >

[0114] android.permission.READ_SMS< 允许程序读取短信息 >

[0115] android.permission.READ_OWNER_DATA< 允许程序读取所有者数据 >

[0116] android.permission.SEND_SMS< 允许程序发送SMS短信 >

[0117] android.permission.WRITE_CALENDAR< 允许一个程序写入用户日历数据 >

[0118] android.permission.WRITE_CONTACTS< 允许程序写入联系人数据 >

[0119] 因此,通过对所述配置文件AndroidManifest.xml进行逐行扫描即可以得到所述应用程序所请求获取的所有权限信息。

[0120] 步骤405:将所提取到的所述所有权限展示给用户。

[0121] 本发明实施例中,控制界面对安装界面的替换可以是弹窗覆盖形式,可以是转页替换形式,也可以托盘形式展现,本发明并不限于此。

[0122] 本发明实施例中控制界面的提示可以是一个下拉菜单,用户点击所述下拉菜单可以查看所述应用程序安装过程中需要获取的所有权限。当然本发明实施例中所述提示也可

以是一个弹窗，或者是一个通知栏的推送等，本发明并不限于此。

[0123] 将所述权限列表显示给用户之后，用户会获知所述应用程序请求访问的所有权限信息，用户可以在明确安装风险之后根据意愿选择选择安装或者放弃安装。

[0124] 步骤 406：监听用户的操作过程，当检测到用户触发安装功能，则响应所述触发放行所述安装进程以及所述所有权限；

[0125] 在步骤 401 中，采用中断机制对所述应用程序编程接口进行监听，实现了对应用程序安装过程的拦截，从而在拦截之后进一步操作获取应用程序安装请求访问的所有权限。将所述所有权限告知用户之后，用户获得安装的风险信息后选择是否安装，若用户选择安装，则响应用户的选择，结束中断，继续安装并放行所有权限以保证安装过程的顺利。

[0126] 步骤 407：检测所述安装进程是否完成；

[0127] 本发明实施例中，当应用程序安装完成之后，操作系统对当前安装的包是否成功返回相关代码 (code)，得到 code 后通过反射机制，得到所述 code 代表的相关信息。如安装成功、安装失败、签名不同、空间不足等等。当然，本发明检测所述安装进程是否完成的方法并不仅限于上述方法。

[0128] 步骤 408：显示所述所有权限的控制选项；

[0129] 本发明实施例中，实时监测应用程序的所述安装进度并通过控制界面进行显示，显示方式可以为传统的直线进度条显示方式，可以是圆形或齿轮型旋转进度显示方式，也可以是配有动画的 loading 图案，或者也可以是上述任意方式的组合形式。在安装过程中提供趣味的进度显示方式，能够缓解用户等待安装时的无聊和焦虑，同时有效地让用户明确知道目前的安装状态，并对安装完成的时间有一个直观的预期。当然，本发明的进度提示方法包括但不限于此。

[0130] 当后台监测到安装进度达到 100％时，控制界面提示用户安装完成并显示权限控制选项。其中，所述权限控制选项可以是一个列表，列表中展示应用程序安装请求访问的所有权限，每一权限都对应一个关闭和一个开启的选项供用户进行选择，用户可以根据意愿选择关闭或者开启部分目标权限。本发明实施例中，所有权限都是默认开启的，当然本发明包括但不限于此。

[0131] 步骤 409：获取用户对所述系统权限的控制选项的操作结果，并根据所述操作结果，对所述应用程序中用户所允许开放的目标权限进行配置。

[0132] 本发明实施例中，实时监测用户对所述权限控制选项的操作，记录用户支持开启或者禁用的目标权限，与此同时，通过控制界面对用户进行提示保存权限设置，并根据用户允许开放的所述目标权限进行权限配置。待权限配置完成后，用户可通过控制界面的退出界面选项结束此次安装或者通过开启应用程序的选项直接开启安装完成的所述应用程序，值得注意的是，当通过所述控制选项接收用户的选择开启所述所有权限中的目标权限时，若运行所述应用程序，则拦截所述应用程序请求目标权限以外的其他权限；当通过控制选项接收用户的选择关闭所述所有权限中的目标权限时，运行所述应用程序时，拦截所述应用程序请求的所述所有权限中的目标权限。

[0133] 实施例五

[0134] 图 5 是本发明实施例一的技术流程图，结合图 5，本发明实施例一种应用程序安装过程的权限控制方法在移动终端的实现从可视化角度主要包括如下的步骤：

[0135] 步骤 501：当检测到有应用程序安装时，展现控制界面替换所述应用程序的安装界面，在所述控制界面显示所述应用程序安装过程请求的所有权限；

[0136] 本发明实施例中，可假设用户在 Android 系统的手机上安装一款地图软件。假设安装方式为用户直接从应用市场下载而后安装。当用户启动安装时，首先手机将展现一个控制界面替换所述应用程序的安装界面。于此同时，控制界面上可以是一个列表，该列表上显示所述地图软件所请求访问的所有权限，比如：（基于网络的）粗略位置或精准的 (GPS) 位置以获取用户的地理位置；网络通讯、完全的互联网访问权限、更改 Wi-Fi 状态等，用以通过网络进行定位或查询；检索当前运行的应用程序、读取联系人数据、读取短信等，用以分享或注册所述地图软件；手机通话、直接拨打电话号码等，用以实现打车服务等。

[0137] 步骤 502：接收到用户触发的安装指示后，放行所述所有权限，对 所述应用程序进行安装，并在所述控制界面显示安装进度；

[0138] 承接上一步骤的例子，当用户获知所述地图软件请求访问的所有权限之后，判断安装后的风险，自行选择安装与否。此时可根据界面提示，选择是否继续安装并可在控制界面上查看安装进度。

[0139] 步骤 503：所述安装进度完成时，所述控制界面提示安装完成并显示所述所有权限的控制选项，从而通过所述控制选项接收用户的选择开启或者关闭所述所有权限中的目标权限。

[0140] 承接上一步骤的例子，当所述地图软件显示安装完成之后，控制界面会再次所述地图软件请求访问的所有权限，此时用户可以对所述权限控制选项进行设置，选择开启或禁用某些目标权限，比如，用户不希望自己的手机联系人信息泄露，则可以在读取联系人信息一项中，将该权限进行关闭。

[0141] 实施例六

[0142] 图 6 是本发明实施例五的装置结构示意图，如图 6 所示，本发明实施例五的一种应用程序安装过程的权限控制装置主要包括以下模块：权限监测模块 601、安装管理模块 602、显示模块 603、权限配置模块 604。

[0143] 所述权限监测模块 601，用于当检测到有应用程序安装时，拦截所述应用程序的安装进程，监测所述应用程序请求获取的所有权限；前台表现为：展现控制界面替换所述应用程序的安装界面，在所述控制界面显示所述应用程序安装过程请求的所有权限；

[0144] 所述安装管理模块 602，用于监听用户的操作过程，当检测到用户触发安装功能，则响应所述触发放行所述安装进程以及所述所有权限；前台表现为：调用所述显示模块 603，在所述控制界面显示安装进度；

[0145] 所述显示模块 603，用于将所述权限监测模块 601 监测到的所述所有权限展示给用户；用于在检测所述安装进程完成时，显示所述所有权限的控制选项；

[0146] 所述权限配置模块 604，用于获取用户对所述系统权限的控制选项 的操作结果，并根据所述操作结果，对所述应用程序中用户所允许开放的目标权限进行配置。前台表现为：用于当所述安装进度完成时，所述控制界面提示安装完成并显示所述所有权限的控制选项。

[0147] 进一步地，所述权限监测模块 601，进一步包括监听模块 601a，所述监听模块 601a，用于采用中断机制对所述应用程序编程接口进行监听，从而中断所述应用程序的安

装进程。

[0148] 进一步地，所述所述监听模块601a，进一步还用于对所述应用程序的行为进行监听，通过调用框架层中的应用程序编程接口，得到包含权限信息的APK文件；通过解析APK文件得到所述所有权限的信息。

[0149] 进一步地，所述权限监测模块601还包括权限解析模块601b，所述权限解析模块601b，用于解压所述APK文件并进行反编译，获取AndroidManifest.xml配置文件；

[0150] 对所述配置文件进行逐行扫描，提取所述应用程序请求的所有权限。

[0151] 进一步地，所述显示模块603还用于，对提取到的所述应用程序请求的所有权限信息进行列表并通过所述权限信息的控制选项显示给用户。

[0152] 进一步地，所述权限配置模块604，还用于，当通过所述控制选项接收用户的选择开启所述所有权限中的目标权限时，若运行所述应用程序，则拦截所述应用程序请求目标权限以外的其他权限；当通过控制选项接收用户的选择关闭所述所有权限中的目标权限时，运行所述应用程序时，拦截所述应用程序请求的所述所有权限中的目标权限。

[0153] 实施例六

[0154] 图7是本发明一种应用程序安装过程的权限控制装置的又一实施例的装置结构示意图，结合图7，本发明一种应用程序安装过程的权限控制装置的操作进程如下：

[0155] 首先，所述权限监测模块601检测到有应用程序安装时，拦截所述 应用程序的安装进程，监测所述应用程序请求获取的所有权限；

[0156] 监测所述应用程序请求获取的所有权限主要由权限监测模块中的所述监听模块601a完成。所述监听模块601a用于采用中断机制对所述应用程序编程接口进行监听，从而中断所述应用程序的安装进程。

[0157] 其中，所述监听模块601a还对应用程序的行为进行监听，通过调用框架层中的应用程序编程接口，得到包含权限信息的APK文件；通过解析APK文件得到所述所有权限的信息。

[0158] 所述权限监测模块还包括权限解析模块601b，所述权限解析模块的功能在于：

[0159] 解压所述APK文件并进行反编译，获取AndroidManifest.xml配置文件；

[0160] 对所述配置文件进行逐行扫描，提取所述应用程序请求的所有权限。

[0161] 当获得所述应用程序请求的所有权限之后，需要调用所述显示模块504，所述显示模块603此时将对提取到的所述应用程序请求的所有权限信息进行列表并显示给用户。

[0162] 将所述所有权限信息展示给用户之后，所述安装管理模块602监听用户的操作过程，当检测到用户触发安装功能，则响应所述触发放行所述安装进程以及所述所有权限；

[0163] 显示模块603显示安装进度，当检测所述安装进程完成时，再次调用显示模块603对提取到的所述应用程序请求的所有权限信息进行列表并通过所述权限信息的控制选项显示给用户。

[0164] 待用户对所述权限控制选项进行操作之后，所述权限配置模块604获取用户对所述系统权限的控制选项的操作结果，并根据所述操作结果，对所述应用程序中用户所允许开放的目标权限进行配置。

[0165] 当通过所述控制选项接收用户的选择开启所述所有权限中的目标权限时，若运行所述应用程序，则拦截所述应用程序请求目标权限以外的其他权限；

[0166] 当通过控制选项接收用户的选择关闭所述所有权限中的目标权限时，运行所述应用程序时，拦截所述应用程序请求的所述所有权限中的目标权限。

[0167] 本实施例所述的一种应用程序安装过程的权限控制装置通过对待安装的应用程序进行权限监测，在安装之前拦截安装获取应用程序所请求的权限信息，并对应用程序的访问权限进行了控制，一方面保证了用户的信息数据安全，另一方面保证程序正常运转。

[0168] a1、一种程序安装过程的权限控制方法，其特征在于，

[0169] 当检测到有应用程序安装时，展现控制界面替换所述应用程序的安装界面，在所述控制界面显示所述应用程序安装过程请求的所有权限；

[0170] 接收到用户触发的安装指示后，放行所述所有权限，对所述应用程序进行安装，并在所述控制界面显示安装进度；

[0171] 所述安装进度完成时，所述控制界面提示安装完成并显示所述所有权限的控制选项，从而通过所述控制选项接收用户的选择开启或者关闭所述所有权限中的目标权限。

[0172] a2、如 a1 所述的方法，其特征在于，当检测到有应用程序安装时，在展现控制界面替换所述应用程序的安装界面之前，进一步包括，

[0173] 采用中断机制对所述应用程序的应用程序编程接口进行监听，从而中断所述应用程序的安装进程。

[0174] a3、如 a2 所述的方法，其特征在于，采用中断机制对所述应用程序的应用程序编程接口进行监听，进一步包括，

[0175] 对所述应用程序的行为进行监听，通过调用框架层中的所述应用程序编程接口，得到包含权限信息的 APK 文件；

[0176] 对所述 APK 进行解析获得所述应用程序请求获取的所有权限的信息。

[0177] a4、如 a3 所述的方法，其特征在于，对所述 APK 进行解析获得所述应用程序请求获取的所有权限的信息，进一步包括，

[0178] 解压所述 APK 文件并进行反编译，获取 AndroidManifest.xml 配置文件；

[0179] 对所述配置文件进行逐行扫描，提取所述应用程序请求的所有权限。

[0180] a5、如 a1 所述的方法，其特征在于，通过所述控制选项接收用户的选择开启或者关闭所述所有权限中的目标权限，进一步包括，

[0181] 监听用户对所权限信息的控制选项的操作结果，根据所述操作结果对所述应用程序的权限进行配置。

[0182] a6、如 a1 所述的方法，其特征在于，通过控制选项接收用户的选择开启或者关闭所述所有权限中目标权限之后，进一步包括，

[0183] 当通过控制选项接收用户的选择开启所述所有权限中的目标权限时，若运行所述应用程序，则拦截所述应用程序请求目标权限以外的其他权限；当通过控制选项接收用户的选择关闭所述所有权限中的目标权限时，运行所述应用程序时，拦截所述应用程序请求的所述所有权限中的目标权限。

[0184] b7、一种程序安装过程的权限控制装置，其特征在于，包括如下模块：

[0185] 权限监测模块，用于当检测到有应用程序安装时，展现控制界面替换所述应用程序的安装界面，在所述控制界面显示所述应用程序安装过程请求的所有权限；

[0186] 安装管理模块，用于接收到用户触发的安装指示后，放行所述所有权限，对所述应

用程序进行安装，并在所述控制界面显示安装进度；

[0187] 权限配置模块，用于当所述安装进度完成时，所述控制界面提示安装完成并显示所述所有权限的控制选项，从而通过所述控制选项接收用户的选择开启或者关闭所述所有权限中的目标权限；

[0188] 显示模块，用于与其它模块结合，进行显示。

[0189] b8、如b7所述的装置，其特征在于，所述权限监测模块，进一步包 括监听模块，

[0190] 所述监听模块，用于采用中断机制对所述应用程序的应用程序编程接口进行监听，从而中断所述应用程序的安装进程。

[0191] b9、如b8所述的装置，其特征在于，所述监听模块，进一步用于，

[0192] 对所述应用程序的行为进行监听，通过调用框架层中的所述应用程序编程接口，得到包含权限信息的APK文件；

[0193] 对所述APK进行解析获得所述应用程序请求获取的所有权限的信息。

[0194] b10、如b9所述的装置，其特征在于，所述权限监测模块，进一步包括权限解析模块：

[0195] 所述权限解析模块，解压所述APK文件并进行反编译，获取AndroidManifest.xml配置文件；

[0196] 对所述配置文件进行逐行扫描，提取所述应用程序请求的所有权限。

[0197] b11、如b7所述的装置，其特征在于，所述权限配置模块进一步用于，

[0198] 监听用户对所权限信息的控制选项的操作结果，根据所述操作结果对所述应用程序的权限进行配置。

[0199] b12、如b7所述的装置，其特征在于，所述权限配置模块，进一步用于，

[0200] 当通过控制选项接收用户的选择开启所述所有权限中的目标权限时，若运行所述应用程序，则拦截所述应用程序请求目标权限以外的其他权限；当通过控制选项接收用户的选择关闭所述所有权限中的目标权限时，运行所述应用程序时，拦截所述应用程序请求的所述所有权限中的目标权限。

[0201] 上述说明示出并描述了本发明的若干优选实施例，但如前所述，应当理解本发明并非局限于本文所披露的形式，不应看作是对 其他实施例的排除，而可用于各种其他组合、修改和环境，并能够在本文所述发明构想范围内，通过上述教导或相关领域的技术或知识进行改动。而本领域人员所进行的改动和变化不脱离本发明的精神和范围，则都应在本发明所附权利要求的保护范围内。

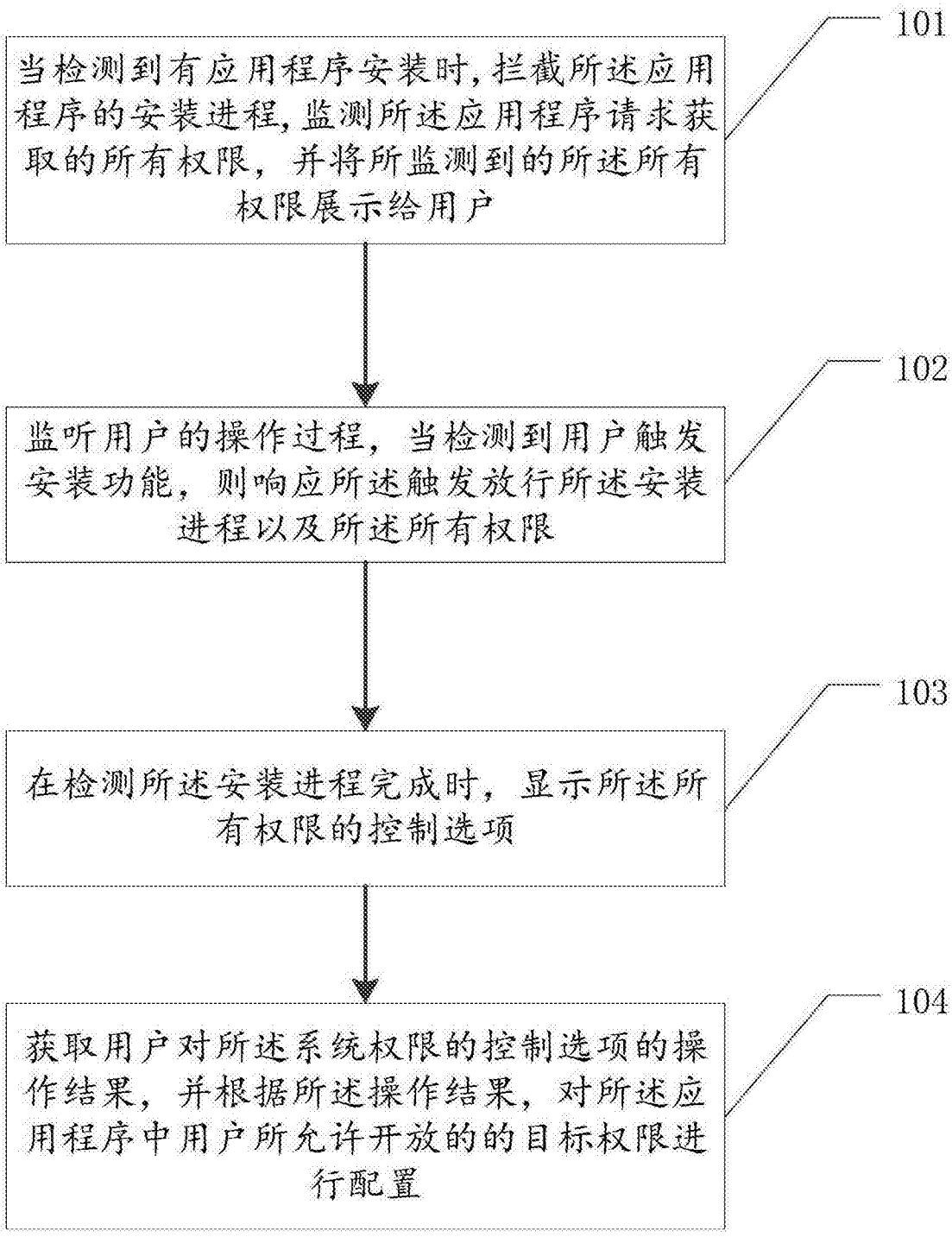

101
当检测到有应用程序安装时，拦截所述应用程序的安装进程，监测所述应用程序请求获取的所有权限，并将所监测到的所述所有权限展示给用户
102
监听用户的操作过程，当检测到用户触发安装功能，则响应所述触发放行所述安装进程以及所述所有权限
103
在检测所述安装进程完成时，显示所述所有权限的控制选项
104
获取用户对所述系统权限的控制选项的操作结果，并根据所述操作结果，对所述应用程序中用户所允许开放的的目标权限进行配置

图 1

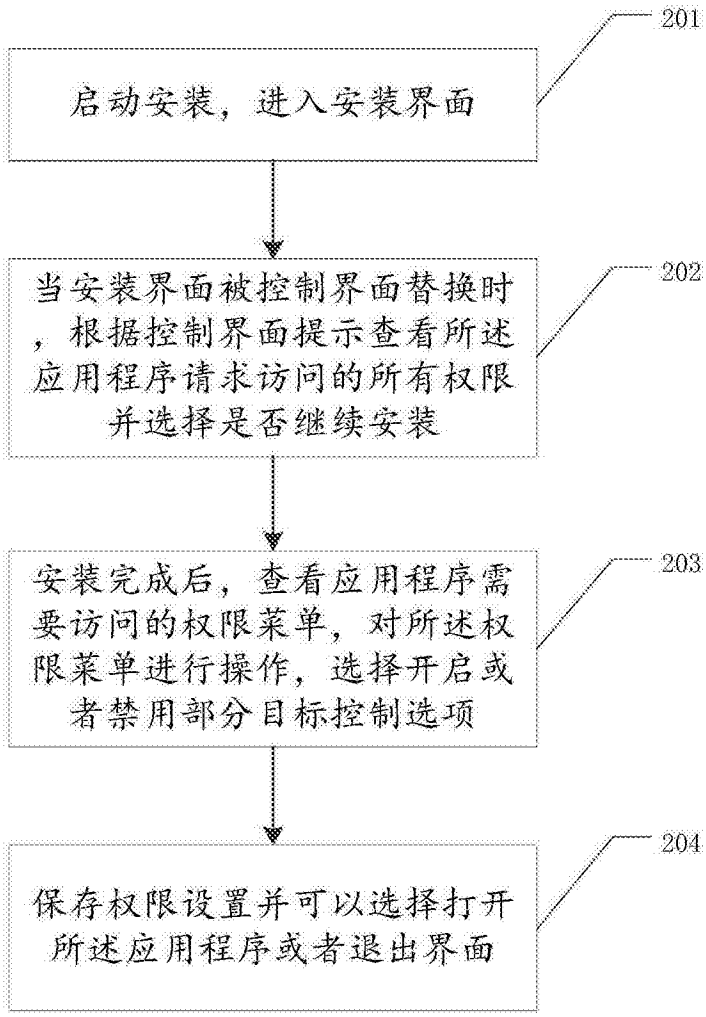

201
启动安装，进入安装界面
202
当安装界面被控制界面替换时，根据控制界面提示查看所述应用程序请求访问的所有权限并选择是否继续安装
203
安装完成后，查看应用程序需要访问的权限菜单，对所述权限菜单进行操作，选择开启或者禁用部分目标控制选项
204
保存权限设置并可以选择打开所述应用程序或者退出界面

图 2

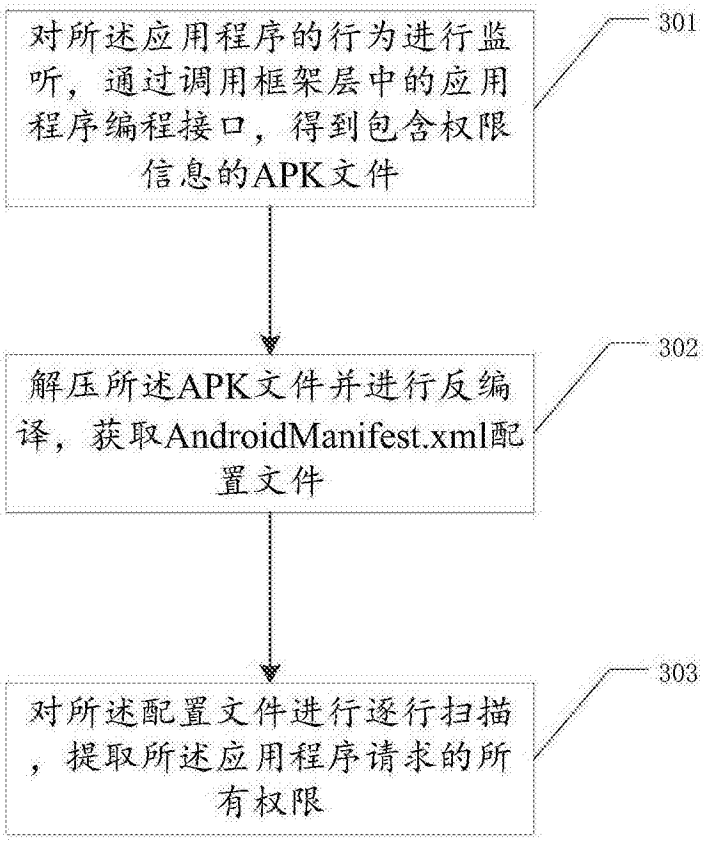

对所述应用程序的行为进行监听，通过调用框架层中的应用程序编程接口，得到包含权限信息的APK文件
301
解压所述APK文件并进行反编译，获取AndroidManifest.xml配置文件
302
对所述配置文件进行逐行扫描，提取所述应用程序请求的所有权限
303

图 3

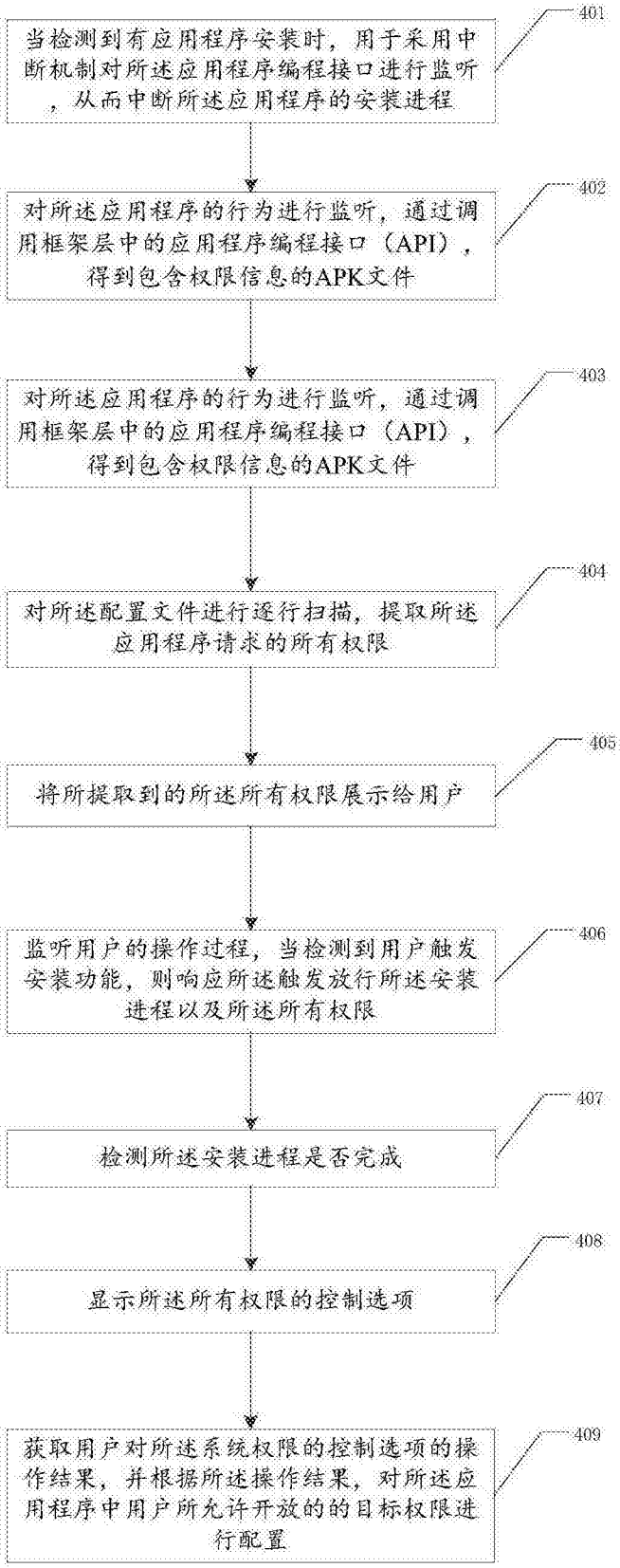

401
当检测到有应用程序安装时，用于采用中断机制对所述应用程序编程接口进行监听，从而中断所述应用程序的安装进程
402
对所述应用程序的行为进行监听，通过调用框架层中的应用程序编程接口（API），得到包含权限信息的APK文件
403
对所述应用程序的行为进行监听，通过调用框架层中的应用程序编程接口（API），得到包含权限信息的APK文件
404
对所述配置文件进行逐行扫描，提取所述应用程序请求的所有权限
405
将所提取到的所述所有权限展示给用户
406
监听用户的操作过程，当检测到用户触发安装功能，则响应所述触发放行所述安装进程以及所述所有权限
407
检测所述安装进程是否完成
408
显示所述所有权限的控制选项
409
获取用户对所述系统权限的控制选项的操作结果，并根据所述操作结果，对所述应用程序中用户所允许开放的的目标权限进行配置

图 4

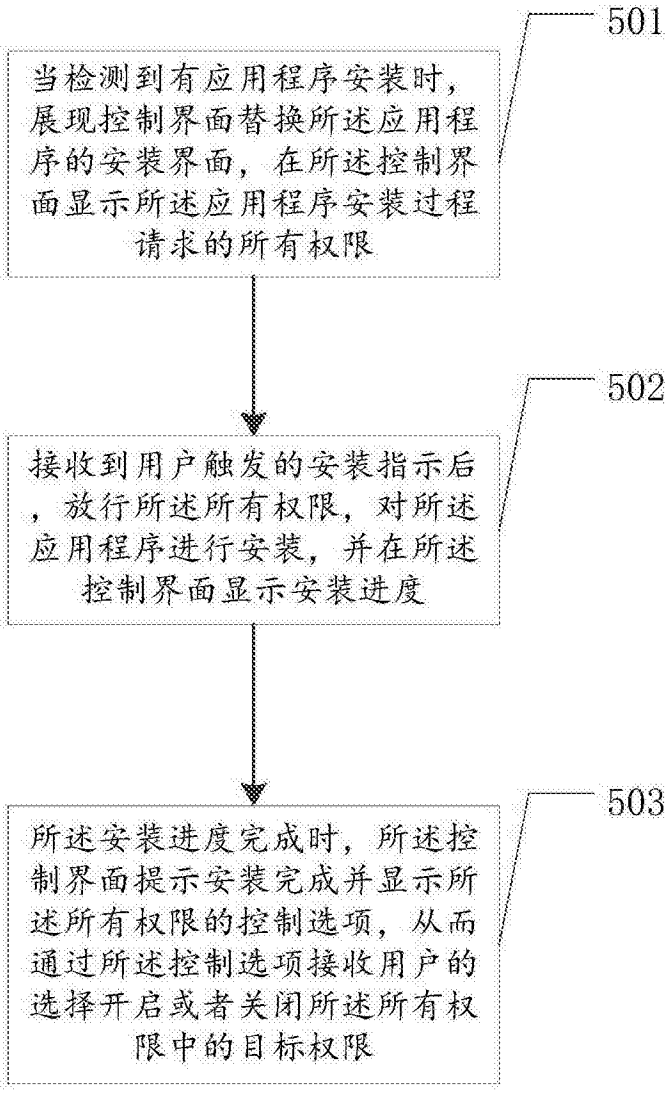

501
当检测到有应用程序安装时，展现控制界面替换所述应用程序的安装界面，在所述控制界面显示所述应用程序安装过程请求的所有权限
502
接收到用户触发的安装指示后，放行所述所有权限，对所述应用程序进行安装，并在所述控制界面显示安装进度
503
所述安装进度完成时，所述控制界面提示安装完成并显示所述所有权限的控制选项，从而通过所述控制选项接收用户的选择开启或者关闭所述所有权限中的目标权限

图 5

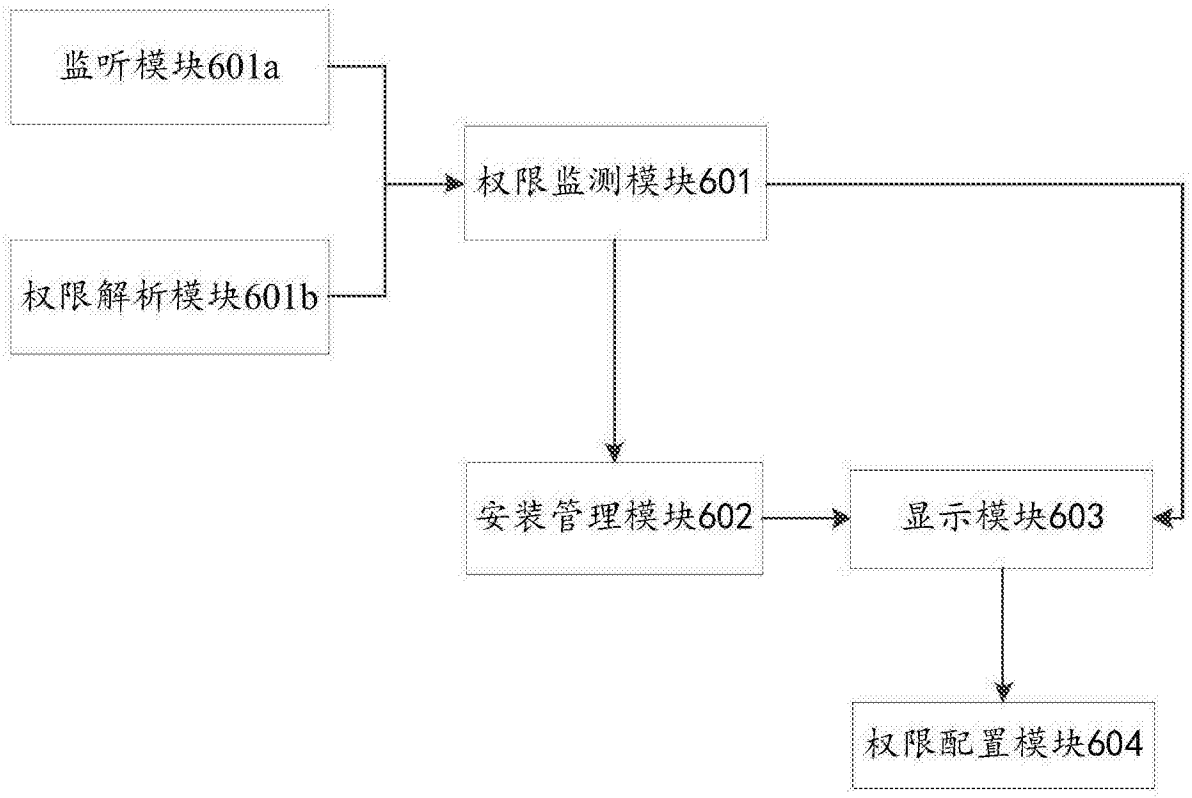

监听模块601a
权限解析模块601b
权限监测模块601
安装管理模块602
显示模块603
权限配置模块604

图 6

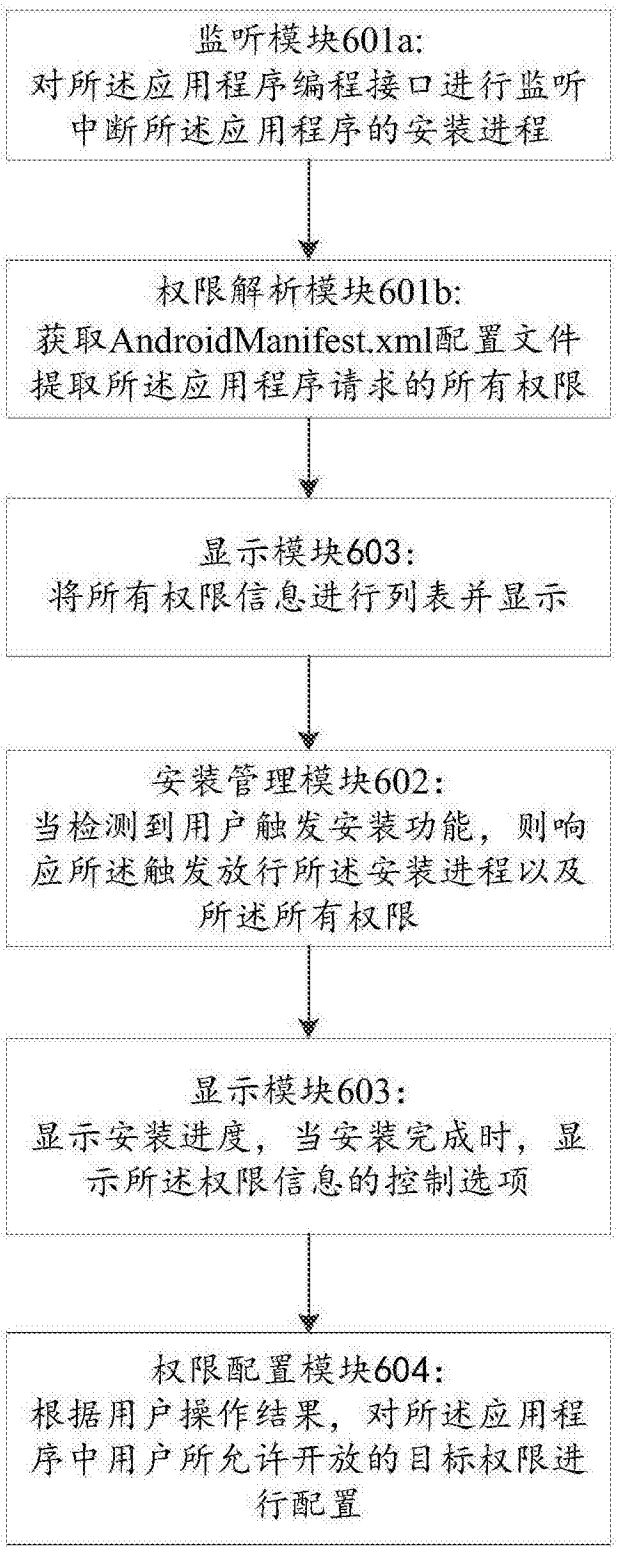

监听模块601a:
对所述应用程序编程接口进行监听中断所述应用程序的安装进程
权限解析模块601b:
获取AndroidManifest.xml配置文件提取所述应用程序请求的所有权限
显示模块603:
将所有权限信息进行列表并显示
安装管理模块602:
当检测到用户触发安装功能，则响应所述触发放行所述安装进程以及所述所有权限
显示模块603:
显示安装进度，当安装完成时，显示所述权限信息的控制选项
权限配置模块604:
根据用户操作结果，对所述应用程序中用户所允许开放的目标权限进行配置

图 7