(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 103761472 A
(43)申请公布日 2014.04.30

(21)申请号 201410060982.3
(22)申请日 2014.02.21
(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 姚彤 丁祎
(74)专利代理机构 北京华沛德权律师事务所 11302
代理人 刘杰
(51)Int.Cl.
G06F 21/51(2013.01)
G06F 21/53(2013.01)
G06F 21/55(2013.01)

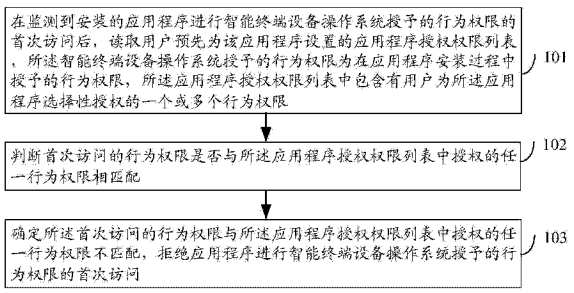
权利要求书2页 说明书15页 附图1页

(54)发明名称

基于智能终端设备的应用程序访问方法与装置

(57)摘要

本发明公开了一种基于智能终端设备的应用程序访问方法与装置。该方法包括:在监测到安装的应用程序进行智能终端设备操作系统授予的行为权限的首次访问后,读取用户预先为该应用程序设置的应用程序授权权限列表,所述智能终端设备操作系统授予的行为权限为在应用程序安装过程中授予的行为权限,所述应用程序授权权限列表中包含有用户为所述应用程序选择性授权的行为权限;判断首次访问的行为权限是否与所述应用程序授权权限列表中授权的任一行为权限相匹配;确定所述首次访问的行为权限与所述应用程序授权权限列表中授权的任一行为权限不匹配,拒绝应用程序进行智能终端设备操作系统授予的行为权限的首次访问。应用本发明,可以提升用户安全性。



CN 103761472 A

1. 一种基于智能终端设备的应用程序访问方法，包括：

在监测到安装的应用程序进行智能终端设备操作系统授予的行为权限的首次访问或曾经被拒绝访问后，读取用户预先为该应用程序设置的应用程序授权权限列表，所述智能终端设备操作系统授予的行为权限为在应用程序安装过程中授予的行为权限，所述应用程序授权权限列表中包含有用户为所述应用程序选择性授权的一个或多个行为权限；

判断首次访问或曾经被拒绝访问的行为权限是否与所述应用程序授权权限列表中授权的任一行为权限相匹配；

确定所述首次访问或曾经被拒绝访问的行为权限与所述应用程序授权权限列表中授权的任一行为权限不匹配，拒绝应用程序进行智能终端设备操作系统授予的行为权限的首次访问。

2. 如权利要求 1 所述的方法，所述读取用户预先为该应用程序设置的应用程序授权权限列表包括：

解析应用程序对应的应用程序文件包，获取应用程序文件包中的应用程序标识；

根据获取的应用程序标识，查询预先设置的应用程序授权权限列表库，得到该应用程序标识对应的应用程序授权权限列表。

3. 如权利要求 2 所述的方法，设置所述应用程序授权权限列表库包括：

对每一应用程序，采集并获取应用程序申请的行为权限；

根据用户从获取的应用程序申请的行为权限中授权的行为权限，生成存储在应用程序授权权限列表库中的应用程序授权权限列表。

4. 如权利要求 3 所述的方法，所述获取应用程序申请的权限包括：

通过应用程序官方下载网站获取应用程序文件包；

解析应用程序文件包中的配置信息文件，得到该应用程序需要申请的行为权限。

5. 如权利要求 4 所述的方法，所述解析应用程序文件包中的配置信息文件包括：

解压基于智能终端设备的应用程序文件，从解压的应用程序文件中获取加密的全局变量描述的配置信息文件，并对加密的配置信息文件进行解密，获取解密的原始配置信息文件，扫描解密的原始配置信息文件中的行为权限描述部分。

6. 一种基于智能终端设备的应用程序访问装置，其特征在于，该装置包括：监测模块、判断模块以及权限处理模块，其中，

监测模块，用于在监测到安装的应用程序进行智能终端设备操作系统授予的行为权限的首次访问后，通知判断模块，所述智能终端设备操作系统授予的行为权限为在应用程序安装过程中授予的行为权限；

判断模块，用于根据接收的通知，读取用户预先为该应用程序设置的应用程序授权权限列表，判断首次访问的行为权限是否与所述应用程序授权权限列表中授权的任一行为权限相匹配，所述应用程序授权权限列表中包含有用户为所述应用程序选择性授权的一个或多个行为权限；

权限处理模块，用于确定所述首次访问的行为权限与所述应用程序授权权限列表中授权的任一行为权限不匹配，拒绝应用程序进行智能终端设备操作系统授予的行为权限的首次访问。

7. 如权利要求 6 所述的装置，其特征在于，所述判断模块包括：解析单元、查询单元以

及判断单元，其中，

解析单元，解析用于安装应用程序的应用程序文件包，获取应用程序文件包中的应用程序标识；

查询单元，用于根据获取的应用程序标识，查询预先设置的应用程序授权权限列表库，得到该应用程序标识对应的应用程序授权权限列表；

判断单元，用于判断首次访问的行为权限是否与得到的所述应用程序授权权限列表中授权的任一行为权限相匹配。

8. 如权利要求 7 所述的装置，其特征在于，所述判断模块进一步包括：

第一分类单元，用于将获取的应用程序申请的权限分类为用于提醒用户重点关注的隐私权限以及按照应用程序申请直接授权的其它权限。

9. 如权利要求 8 所述的装置，其特征在于，所述判断模块进一步包括：

第二分类单元，用于将隐私权限分为运行应用程序所必需的必需权限以及运行应用程序可选的非必需权限，并在授权设置界面向用户展示所述非必要权限的提示信息。

10. 如权利要求 9 所述的装置，其特征在于，所述判断模块进一步包括：

验证单元，用于利用隔离沙箱、和 / 或，静态代码分析、和 / 或，自动代码特征扫描方法，对应用程序申请的所述必需权限进行合法性以及合理性的验证，以确定必需权限中的每一权限是否都为应用程序运行时所需的必不可少的权限，如果不是，则将该权限从必需权限中删除，并作为非必要权限向用户展示。

基于智能终端设备的应用程序访问方法与装置

技术领域

[0001] 本发明涉及安卓(Android)平台技术，具体涉及一种基于智能终端设备的应用程序访问方法与装置。

背景技术

[0002] Android 平台是基于 Linux 的开源手机操作系统平台，由操作系统、用户界面和应用程序组成，对第三方应用程序完全开放。由于 Android 平台的开放性，使得应用程序开发者在开发应用程序时拥有更大的自由度，因而，吸引了很多应用程序开发者，应用程序开发者也开发并提供了大量基于 Android 平台的安卓的应用程序，这种应用程序的安装包是以一种被称为 APK（Android Package）的形式进行发布，通过安装安卓安装包实现应用程序的运行，使得越来越多的应用程序可以承载在 Android 平台上。Android 平台作为世界上最流行的移动操作系统平台，已经覆盖了数以十亿计的移动终端以及众多的应用程序。

[0003] Android 平台在设计之初设计了基于授予行为权限的安全访问策略，在用户进行应用程序安装时，如果应用程序涉及到对用户安全性的操作，例如，读取用户隐私信息的操作，或是可能导致用户费用损失的操作，都需要用户对应用程序进行行为授权方可进行。举例来说，如果应用程序在安装后需要执行发送短信、访问联系人数据、读取存储卡数据等读取用户隐私信息的操作，以及使用网络连接等增加用户费用的操作时，需要在安装时向用户申请对应的行为权限，也就是在应用程序安装过程中，通过移动终端将需要用户授权的行为权限声明向用户展示，从而由用户决定是否授予该应用程序执行用户安全性操作的访问权限。

[0004] 在应用程序安装过程中，由于 Android 平台的安全访问策略，用户在安装应用程序时，只能从整体上授予应用程序申请的行为权限，因而，在应用程序安装时，向用户展示出应用程序申请的行为权限服务后，用户或者接受应用程序申请的所有行为权限服务以继续安装该应用程序，或者，只能取消安装该应用程序并退出该应用程序安装。举例来说，当用户安装 KC 网络电话应用程序时，由于需要获取用户安全信息的相关行为权限，Android 平台根据基于行为权限的安全访问策略，在移动终端的显示界面展示需要用户授权的安全相关行为权限，例如，读取移动终端状态和 ID、拦截呼出、直接呼叫电话号码、编辑 SMS 或 MMS、发送文本信息、录音以及精确 GPS 位置信息等，如果用户授权 KC 网络电话应用程序执行上述所有安全操作，则可以通过点击显示界面的下一步控件继续进行安装，这样，在安装 KC 网络电话应用程序后，KC 网络电话应用程序将有权限获取用户的录音信息以及精确 GPS 位置信息等用户安全信息；如果用户不授权 KC 网络电话应用程序执行上述所有安全操作，则可以通过点击显示界面的取消控件，退出当前 KC 网络电话应用程序安装。

[0005] 近年来，利用 Android 平台对应用程序只能从整体上授予行为权限的特点，针对 Android 平台的恶意应用程序大量增加，恶意应用程序在申请用户授权的行为权限上，增加多个影响用户安全性的行为权限，例如，发送短信、读取联系人、联网、录音、读取用户精确 GPS 位置信息等行为权限，与该恶意应用程序正常运行所需的行为权限进行绑定，并以各

种诱人的名字、功能和应用吸引用户安装，同时，在移动终端的显示界面展示需要用户授权的安全相关行为权限时，将增加的影响用户安全性的行为权限置于用户不太关注的地方，从而通过用户点击显示界面的下一步控件继续进行安装，而一旦安装并运行该恶意应用程序，意味着用户授予了该恶意应用程序申请的所有行为权限，使得用户的安全面临重大风险，而该恶意应用程序通过用户的安装，实现了窃取用户隐私、恶意吸费等目的。进一步地，即使用户对恶意应用程序申请的其中一些行为权限存有疑虑，但除了放弃安装外没有其他选择。

[0006] 为了降低恶意应用程序给用户带来的安全隐患，现有 Android 平台提供了安全应用程序，用以提供主动防御以及权限管理功能，即通过运行安全应用程序，可以由用户选择需要禁用的各应用程序的行为权限，从而使应用程序在运行时，不再享有用户在安装该应用程序过程中授予的行为权限，从而在后续应用中，可以避免该应用程序对用户安全性形成威胁。但该方法，不能有效避免用户在安装应用程序后，通过安全应用程序设置禁止权限前的时间段内，由于应用程序运行时给用户带来的安全性隐患，用户的安全信息在该时间段内，还是可能被窃取或泄露，从而给用户带来损失，使得用户安全性降低。进一步地，一些应用程序中确实存在较好的体验点，但由于用户担心该应用程序申请的行为权限可能会导致个人隐私信息的泄露，最终选择不安装该应用程序，这样，不仅降低了用户的业务体验，也给应用程序开发商带来了极大的经济损失。

发明内容

[0007] 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基于智能终端设备的应用程序访问方法与装置。

[0008] 依据本发明的一个方面，提供了基于智能终端设备的应用程序访问方法，该方法包括：

[0009] 在监测到安装的应用程序进行智能终端设备操作系统授予的行为权限的首次访问或曾经被拒绝访问后，读取用户预先为该应用程序设置的应用程序授权权限列表，所述智能终端设备操作系统授予的行为权限为在应用程序安装过程中授予的行为权限，所述应用程序授权权限列表中包含有用户为所述应用程序选择性授权的一个或多个行为权限；

[0010] 判断首次访问或曾经被拒绝访问的行为权限是否与所述应用程序授权权限列表中授权的任一行为权限相匹配；

[0011] 确定所述首次访问或曾经被拒绝访问的行为权限与所述应用程序授权权限列表中授权的任一行为权限不匹配，拒绝应用程序进行智能终端设备操作系统授予的行为权限的首次访问。

[0012] 优选地，所述读取用户预先为该应用程序设置的应用程序授权权限列表包括：

[0013] 解析应用程序对应的应用程序文件包，获取应用程序文件包中的应用程序标识；

[0014] 根据获取的应用程序标识，查询预先设置的应用程序授权权限列表库，得到该应用程序标识对应的应用程序授权权限列表。

[0015] 优选地，设置所述应用程序授权权限列表库包括：

[0016] 对每一应用程序，采集并获取应用程序申请的行为权限；

[0017] 根据用户从获取的应用程序申请的行为权限中授权的行为权限，生成存储在应用

程序授权权限列表库中的应用程序授权权限列表。

[0018] 优选地，所述获取应用程序申请的权限包括：

[0019] 通过应用程序官方下载网站获取应用程序文件包；

[0020] 解析应用程序文件包中的配置信息文件，得到该应用程序需要申请的行为权限。

[0021] 优选地，所述解析应用程序文件包中的配置信息文件包括：

[0022] 解压基于智能终端设备的应用程序文件，从解压的应用程序文件中获取加密的全局变量描述的配置信息文件，并对加密的配置信息文件进行解密，获取解密的原始配置信息文件，扫描解密的原始配置信息文件中的行为权限描述部分。

[0023] 优选地，利用 Java 中的可扩展标记语言文件解析器，解析所述解密的原始配置信息文件中的行为权限描述部分。

[0024] 优选地，每一所述应用程序对应一所述应用程序授权权限列表，多个应用程序授权权限列表组成应用程序授权权限列表库，所述应用程序授权权限列表中包含的授权行为权限为所述智能终端设备操作系统授予的行为权限的一部分。

[0025] 优选地，在所述根据用户从获取的应用程序申请的权限中授权的行为权限之前，所述方法进一步包括：

[0026] 将获取的应用程序申请的行为权限进行展示。

[0027] 优选地，在所述获取应用程序申请的行为权限之后，所述方法进一步包括：

[0028] 将获取的应用程序申请的行为权限分类为用于提醒用户重点关注的隐私权限以及按照应用程序申请直接授权的其它权限。

[0029] 优选地，所述方法进一步包括：

[0030] 将隐私权限分为运行应用程序所必需的必需权限以及运行应用程序可选的非必需权限，并由用户选取和更新必需权限以及非必需权限，以及，在授权设置界面向用户展示所述非必要权限的提示信息。

[0031] 优选地，所述方法进一步包括：

[0032] 利用隔离沙箱、和 / 或，静态代码分析、和 / 或，自动代码特征扫描方法，对应用程序申请的所述必需权限进行合法性以及合理性的验证，以确定必需权限中的每一权限是否都为应用程序运行时所需的必不可少的权限，如果不是，则将该权限从必需权限中删除，并作为非必要权限向用户展示。

[0033] 优选地，在所述监测到安装的应用程序首次进行申请的权限访问之前，所述方法进一步包括：

[0034] 对待安装的应用程序文件包进行安全扫描，如果待安装的应用程序文件包通过安全扫描，安装所述应用程序文件包，否则，结束流程。

[0035] 优选地，所述安全扫描包括但不限于木马病毒扫描、广告插件扫描、漏洞扫描。

[0036] 优选地，所述智能终端设备的运行平台包括但不限于安卓平台。

[0037] 根据本发明的另一个方面提供了一种基于智能终端设备安装应用程序的装置，该装置包括：监测模块、判断模块以及权限处理模块，其中，

[0038] 监测模块，用于在监测到安装的应用程序进行智能终端设备操作系统授予的行为权限的首次访问后，通知判断模块，所述智能终端设备操作系统授予的行为权限为在应用程序安装过程中授予的行为权限；

[0039] 判断模块，用于根据接收的通知，读取用户预先为该应用程序设置的应用程序授权权限列表，判断首次访问的行为权限是否与所述应用程序授权权限列表中授权的任一行为权限相匹配，所述应用程序授权权限列表中包含有用户为所述应用程序选择性授权的一个或多个行为权限；

[0040] 权限处理模块，用于确定所述首次访问的行为权限与所述应用程序授权权限列表中授权的任一行为权限不匹配，拒绝应用程序进行智能终端设备操作系统授予的行为权限的首次访问。

[0041] 优选地，所述判断模块包括：解析单元、查询单元以及判断单元，其中，

[0042] 解析单元，解析用于安装应用程序的应用程序文件包，获取应用程序文件包中的应用程序标识；

[0043] 查询单元，用于根据获取的应用程序标识，查询预先设置的应用程序授权权限列表库，得到该应用程序标识对应的应用程序授权权限列表；

[0044] 判断单元，用于判断首次访问的行为权限是否与得到的所述应用程序授权权限列表中授权的任一行为权限相匹配。

[0045] 优选地，所述判断模块进一步包括：

[0046] 第一分类单元，用于将获取的应用程序申请的权限分类为用于提醒用户重点关注的隐私权限以及按照应用程序申请直接授权的其它权限。

[0047] 优选地，所述判断模块进一步包括：

[0048] 第二分类单元，用于将隐私权限分为运行应用程序所必需的必需权限以及运行应用程序可选的非必需权限，并在授权设置界面向用户展示所述非必要权限的提示信息。

[0049] 优选地，所述判断模块进一步包括：

[0050] 验证单元，用于利用隔离沙箱、和／或，静态代码分析、和／或，自动代码特征扫描方法，对应用程序申请的所述必需权限进行合法性以及合理性的验证，以确定必需权限中的每一权限是否都为应用程序运行时所需的必不可少的权限，如果不是，则将该权限从必需权限中删除，并作为非必要权限向用户展示。

[0051] 优选地，进一步包括：

[0052] 展示模块，用于将获取的应用程序申请的行为权限进行展示。

[0053] 优选地，进一步包括：

[0054] 安全扫描模块，用于对待安装的应用程序文件包进行安全扫描，如果待安装的应用程序文件包通过安全扫描，安装所述应用程序文件包，否则，结束流程。

[0055] 根据本发明的基于智能终端设备的应用程序访问方法与装置，可以通过安装应用程序之前，预先选择并确定可以授予该应用程序的行为权限以及禁止授予的行为权限，按照现有整体授权的方式进行应用程序安装后，在应用程序首次进行申请的行为权限访问时，将申请的行为权限与预先选择并确定的行为权限进行匹配，如果申请的行为权限与预先选择并确定的行为权限不匹配，则拒绝应用程序进行申请的行为权限访问或者返回虚假数据，比如对于查询用户 GPS 位置的请求可以直接拒绝也可以采用返回假位置的方法。由此解决了在按整体授权的方式安装应用程序后，亦可禁止应用程序获取用户对敏感权限的授权，使得安装后的应用程序采用用户预先设置的授权权限进行相应访问的技术问题，取得了既可以保证用户正常使用该应用程序提供的业务功能，又可有效保障用户安全的有益

效果。

[0056] 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

[0057] 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：

[0058] 图 1 示出了本发明实施例基于智能终端设备的应用程序访问方法流程；以及，

[0059] 图 2 示出了本发明实施例基于智能终端设备的应用程序访问装置结构。

具体实施方式

[0060] 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。

[0061] 现有基于智能终端设备安装应用程序时，由于具有只能从整体上授予应用程序申请的行为权限的特点，用户不能按照自己安全性的需求选择行为权限服务，如需安装应用程序，在移动终端的显示界面展示的需要用户授权的行为权限服务中，只能被迫接受应用程序申请的所有行为权限以继续进行应用程序安装，即默认用户对应用程序申请的行为权限进行全部授权，从而通过用户点击显示界面的下一步控件继续进行安装，而一旦安装并运行应用程序，意味着用户授予了该应用程序申请的所有行为权限，使得用户的安全将面临重大风险。而安全应用程序提供的主动防御以及权限管理功能，还是不能有效避免用户在安装应用程序后，通过安全应用程序设置禁止权限前，由于应用程序运行时给用户带来的安全性隐患，使得用户安全性降低。

[0062] 现有的应用程序，向用户申请的行为权限以及对应用程序的配置信息携带在应用程序的配置信息文件中，由于配置信息文件由应用程序开发者通过签名生成，因而，不能通过解析配置信息文件，并对解析的配置信息文件进行修改而更改应用程序申请的行为权限。本发明实施例中，提出一种基于智能终端设备的应用程序访问方法，通过预先获取各应用程序申请的行为权限，并由用户对应用程序申请的行为权限进行选择性授权，使用户可以根据自己对应用程序的功能需要以及安全性考虑，在应用程序所申请的行为权限中进行相应选择并授权，生成应用程序授权权限列表，并在应用程序安装后，当应用程序首次进行申请的行为权限访问时，触发应用程序将生成的应用程序授权权限列表作为应用程序进行访问具有的行为权限，从而既可以保证用户正常使用该应用程序提供的业务功能，又可有效保障用户安全。

[0063] 图 1 示出了本发明实施例基于智能终端设备的应用程序访问方法流程。参见图 1，该流程包括：

[0064] 步骤 101，在监测到安装的应用程序进行智能终端设备操作系统授予的行为权限

的首次访问后，读取用户预先为该应用程序设置的应用程序授权权限列表，所述智能终端设备操作系统授予的行为权限为在应用程序安装过程中授予的行为权限，所述应用程序授权权限列表中包含有用户为所述应用程序选择性授权的一个或多个行为权限；

[0065] 本步骤中，基于 Android 平台的安全访问策略，采用从整体上授予应用程序申请的权限的方式安装应用程序，关于应用程序的安装为公知技术，在此略去详述。本发明实施例中，对于安装的应用程序进行智能终端设备操作系统授予的行为权限的曾经被拒绝访问的流程，与首次访问的流程相同。

[0066] 读取用户预先为该应用程序设置的应用程序授权权限列表包括：

[0067] A11，解析应用程序对应的应用程序文件包，获取应用程序文件包中的应用程序标识；

[0068] 本步骤中，每一应用程序，在安装前，对应有一应用程序安装包，即利用应用程序安装包进行安装后，得到可以进行访问操作的应用程序。通过解析应用程序文件包，可以获取用于对应用程序进行唯一标记的应用程序标识。

[0069] A12，根据获取的应用程序标识，查询预先设置的应用程序授权权限列表库，得到该应用程序标识对应的应用程序授权权限列表。

[0070] 本步骤中，在预先设置的应用程序授权权限列表库中，某些应用程序对应有一应用程序授权权限列表，应用程序授权权限列表以应用程序标识为标记。在每一应用程序授权权限列表中，存储有用户预先为该应用程序授权的行为权限。如果该列表中没有对应于该应用程序的行为权限，则没有具体权限建议，但用户仍可对所有行为权限授权或禁止。

[0071] 本发明实施例中，预先设置的应用程序授权权限列表库可以通过下述方法得到：

[0072] 对每一应用程序，执行如下步骤 B11 和 B12：

[0073] B11，采集并获取应用程序申请的行为权限；

[0074] 本步骤中，可以在安装某一应用程序之前，预先为该应用程序进行行为权限授权。作为可选实施例，可以通过应用程序官方下载网站获取应用程序文件包，也可以从其他途径获取正规的应用程序提供商提供的应用程序文件包。例如，从应用程序运营商网站获取应用程序文件包。也就是说，应用程序文件包可以是应用程序开发者上传的，也可以是应用程序运营商上传的，还可以是通过其他渠道上传的正版的应用程序文件包，只要能够获取正版的应用程序文件包即可。这样，通过正规途径获取应用程序文件包，可以保证该应用程序申请行为权限的合法性和合理性，避免通过其他方法对应用程序文件包进行非法修改后，使得非法修改后的应用程序恶意申请更多涉及用户安全的行为权限。

[0075] 在下载得到应用程序文件包后，通过解析应用程序文件包中的配置信息文件，可以得到该应用程序需要申请的行为权限。

[0076] 本发明实施例中，在 Android 平台下，应用程序文件包即为 APK 文件，每一 APK 文件中包含了应用程序的二进制代码信息、资源信息、配置信息文件等。配置信息文件即为 APK 文件中的 AndroidManifest.xml 文件，是每一应用程序都必须定义和包含的，它描述了应用程序的名字、版本、权限、引用的库文件等信息。实际应用中，解析应用程序文件包中的配置信息文件包括：解压基于 Android 平台的应用程序文件，从解压的应用程序文件中获取加密的全局变量描述的配置信息文件，即 AndroidManifest.xml 文件，并对加密的配置信息文件进行解密，获取解密的原始配置信息文件：AndroiManifest.xml 文件；扫描

AndroidManifest.xml 文件中的权限描述部分，即可获取应用程序所申请的行为权限列表，行为权限列表中包含的行为权限即为应用程序申请的行为权限。

[0077] 应用程序的行为权限在 AndroidManifest.xml 文件中的声明形式如下：

[0078] 文件名：AndroidManifest.xml

[0079] <uses-permission android:name =“使用权限”/>

[0080] 作为可选实施例，在上述解析流程中，可以使用 Java 中的可扩展标记语言（XML，Extensible Markup Language）文件解析器，解析 AndroidManifest.xml 文件中的权限描述部分，以获取应用程序申请的行为权限列表。当然，也可以使用其他 XML 解析器，或者，使用其他编程语言，例如 C/C++、python 等编程语言开发 XML 解析器，对 AndroidManifest.xml 文件进行解析，以获得相应的应用程序所申请的行为权限列表。

[0081] B12，根据用户从获取的应用程序申请的行为权限中选取并授权的行为权限，生成存储在应用程序授权权限列表库中的应用程序授权权限列表。

[0082] 本步骤中，用户从每一应用程序申请的行为权限中，根据自身的业务需求以及安全性考虑，分别为每一应用程序进行行为权限授权，根据为每一应用程序选取的授权行为权限，生成对应该应用程序的应用程序授权权限列表。每一应用程序对应一应用程序授权权限列表，应用程序授权权限列表以应用程序标识进行标记。本发明实施例中，多个应用程序授权权限列表组成应用程序授权权限列表库，应用程序授权权限列表中，不仅包含有用户为应用程序授权的一个或多个行为权限，也包含有用户为应用程序禁止授权的一个或多个行为权限，也就是说，应用程序授权权限列表中的行为权限，其属性为授权或禁止授权，如果申请的行为权限在应用程序授权权限列表中，其属性为授权，则允许应用程序进行申请的行为权限访问；如果申请的行为权限在应用程序授权权限列表中，其属性为禁止授权，则拒绝应用程序进行申请的行为权限访问。

[0083] 作为可选实施例，为了便于用户对行为权限的授权选取操作，在根据用户从获取的应用程序申请的行为权限中选取授权权限之前，该方法还可以进一步包括：

[0084] 将获取的应用程序申请的行为权限进行展示。

[0085] 本步骤中，为用户提供授权设置界面，在授权设置界面上展示应用程序申请的行为权限，用户在授权设置界面上对展示的行为权限进行授权选取。这样，用户可以借助可视的授权设置界面，方便地选取所需的行为权限进行授权。

[0086] 作为另一可选实施例，为了提高用户对应用程序申请的行为权限的了解，该方法还可以进一步包括：

[0087] 对获取的应用程序申请的行为权限进行分类。

[0088] 本步骤中，可针对每一应用程序，将获取的行为权限分类为隐私权限以及其它权限，其中，对于隐私权限，由于涉及到用户的隐私，需要提醒用户重点关注，而对于其它权限，用户可以根据应用程序的申请，无需过多关注，授予其权限即可。

[0089] 本发明实施例中，隐私权限包括但不限于以下信息：发送短消息（android.permission.SEND_SMS）、接入互联网（android.permission.INTERNET）、读短消息（android.permission.READ_SMS）、写短消息（android.permission.WRITE_SMS）、读通讯录（android.permission.READ_CONTACTS）、写通讯录（android.permission.WRITE_CONTACTS）、拨打电话（android.permissi on.CALL_PHONE）、写系统设置（android.

permission.WRITE_SYNC_SETTI NGS)、读取位置信息、进行录音以及读取录音信息。每一隐私权限对应有一函数，例如，对于发送短消息行为权限，对应的函数为 SmsManager.sendTextMessage、SmsManager.sendDataMessage、SmsManager.sendMultipartTextMe ssage 等。

[0090] 对于隐私权限，又可进一步分为必需权限以及非必需权限。其中，必需权限为运行应用程序所必需的、由用户授权的行为权限，缺少该授权的行为权限，则应用程序无法正常运行，用户如果需要安装该应用程序，则必须对应用程序申请的必需权限进行全部授权，否则无法安装。非必需权限为应用程序需要的用户授权的行为权限，但为可选项，不会影响应用程序的运行，如果该行为权限未获用户授权，不影响应用程序的安装和运行。例如，必需权限可以包括：写通讯录、拨打电话等，非必需权限可以包括：读取位置信息、接入互联网、读取录音信息等。

[0091] 作为可选实施例，对于非必要权限，进一步在授权设置界面向用户展示该非必要权限的提示信息。提示信息可以是：非必须权限建议取消，或行为权限为可选授权项，请根据自身安全策略进行授权等。即建议用户在授权非必要权限时，基于自己隐私安全的考虑，慎重选择授予应用程序的行为权限。

[0092] 作为另一可选实施例，对于必需权限，还可以进行验证，以确定所有的必需权限是否都为应用程序运行时所必需的，即对应用程序申请的必需权限进行合法性以及合理性的验证。验证的方法可以利用包括隔离沙箱、和 / 或，静态代码分析、和 / 或，自动代码特征扫描等方法，以确定必需权限中的每一行为权限是否都为应用程序运行时所需的必不可少的行为权限，如果不是，则将该行为权限从必需权限中删除，并作为非必要权限向用户展示。其中，应用静态代码分析，能够快速、准确地查找、定位每一应用程序申请的必需权限存在的安全风险及漏洞。而隔离沙箱利用虚拟机技术，通过虚拟机克隆 Android 平台内硬盘的某一分区或所有分区，并形成一个影子，称之为影子模式。影子模式与 Android 平台系统具有相同架构和功能，用户可以在影子模式下运行应用程序，对应用程序的任何操作，例如，删改文件、安装测试各种应用程序(包括流氓应用程序、病毒应用程序)，都被隔离沙箱所包裹，恶意应用程序对用户隐私信息的截取，都被限制在隔离沙箱内，只要将隔离沙箱关闭，就可以使得危害 Android 平台的操作消失。因而，通过隔离沙箱方法，监测应用程序对用户数据的访问行为，可以确定应用程序申请的必需权限是否涉及权限滥用，即应用程序出于各种目的，是否向用户申请了本不该申请的行为权限。如果应用程序通过必需权限的方式申请了额外的行为权限，可能导致用户隐私信息泄露，因而，需要将该额外申请的行为权限从必需权限中剔除。例如，如果一个单机游戏应用程序申请了读取用户电话本的权限，该读取用户电话本就可能属于单机游戏应用程序本不该申请的行为权限，从而提升用户隐私的安全性。关于利用隔离沙箱、静态代码分析、自动代码特征扫描等方法对应用程序申请的必需权限进行合法性以及合理性的验证，为公知技术，在此略去详述。

[0093] 这样，通过将应用程序申请的行为权限分类为隐私权限以及其它权限，使得用户对其中涉及的隐私权限进行关注，从而考虑是否需要对应用程序授予该权限，保障了用户隐私安全；进一步地，通过将隐私权限分为必需权限以及非必需权限，使得用户对于非必需权限，基于自身的安全策略，尽量避免对其授权，从而提升用户隐私安全性；而且，对于必需权限，进行合法性以及合理性的验证，可以将恶意应用程序额外申请的行为权限进行剔除，最大限度地保障用户安全性。

[0094] 作为可选实施例，在应用程序安装过程中，安卓平台授予了该应用程序所有申请的行为权限，而当安装后的该应用程序在首次实际使用申请的行为权限涉及的访问操作时，动态根据用户预先为该应用程序的选择，选择拒绝或者返回假数据的方法，对应用程序进行权限管理。也就是说，可以在 Android 平台框架层的源代码中找到应用程序执行行为权限访问时需要插入钩子的类和接口，这些类和接口为涉及到用户隐私信息的类和接口，通过分析并修改类和接口的源代码，使得需要执行行为权限访问时插入的钩子的类和接口指向本发明实施例预先设置的应用程序授权权限列表，其中，应用程序授权权限列表中包含的授权行为权限为所述智能终端设备操作系统授予的行为权限的一部分。具体来说，通过修改源代码的方式替换 Android 平台原默认的应用程序安装器，从而实现本发明实施例的应用程序授权权限列表读取，其中，替换 Android 平台原安装器的方法包括但不限于如下几种：由用户选择新的安装器为 Android 平台默认的安装器、如果在 Root 过的移动终端上，可以直接替换 Android 平台原应用程序安装方案，以及在移动终端的 ROM 中，替换 Android 平台原应用程序安装方案。

[0095] 步骤 102，判断首次访问的行为权限是否与所述应用程序授权权限列表中授权的任一行为权限相匹配；

[0096] 步骤 103，确定所述首次访问的行为权限与所述应用程序授权权限列表中授权的任一行为权限不匹配，拒绝应用程序进行智能终端设备操作系统授予的行为权限的首次访问。

[0097] 本步骤中，如果申请的行为权限与应用程序授权权限列表中的任一行为权限相同，例如，对于进行录音以及读取精确 GPS 位置信息，如果申请的行为权限中，进行录音以及读取精确 GPS 位置信息的权限均为允许，而在应用程序授权权限列表中，对于进行录音，权限为允许，对于读取精确 GPS 位置信息，权限为禁止。则：申请的进行录音行为权限与应用程序授权权限列表中的进行录音的行为权限相匹配，申请的读取精确 GPS 位置信息与应用程序授权权限列表中的读取精确 GPS 位置信息的行为权限不相匹配，对于不相匹配的情形，可以直接拒绝应用程序的权限访问，或者向应用程序返回虚假数据。举例来说，对于查询用户精确 GPS 位置信息的请求，安卓平台可以直接拒绝应用程序的行为权限访问，也可以向应用程序返回预先设置的假 GPS 位置信息。

[0098] 当用户安装好相应的应用程序后，如果需要对应用程序的一些功能或授予应用程序的授权权限进行更新，可以通过运行应用程序授权权限列表，在应用程序授权权限列表对应的更新界面，由用户选择需要禁用或授权的各应用程序的行为权限，以对应用程序的相应功能以及授权权限进行修改，从而在应用程序再重新运行时，支持用户修改后的相应功能和授权权限的访问。例如，如果禁用了某一授权权限，则在应用程序再次运行时，不再享有用户禁用了的授权权限。因而，实际应用中，可以为每一应用程序设置对应的一计数器，在监测到安装的应用程序需要进行申请的行为权限访问时，读取该应用程序对应的计数器，如果计数器的计数值为零，表明该应用程序为首次行为权限访问。在应用程序进行相应的行为权限访问后，将对应计数器的计数值加 1。后续应用中，如果用户对应用程序授权权限列表进行了更新，则将对应的计数器的计数值清零，这样，在应用程序再次进行申请的行为权限访问时，需要执行与更新的应用程序授权权限列表进行匹配的流程。

[0099] 作为另一可选实施例，还可以在安装应用程序文件包之前，对该应用程序文件包

进行安全扫描，以确保该应用程序文件包的安全性，降低安装恶意应用程序的概率。这样，该方法进一步包括：

[0100] 对待安装的应用程序文件包进行安全扫描，如果待安装的应用程序文件包通过安全扫描，安装应用程序文件包以形成应用程序，否则，结束流程。

[0101] 本步骤中，在安装应用程序文件包前，通过对该应用程序文件包进行深度安全扫描，深度安全扫描包括但不限于木马病毒扫描、广告插件扫描、漏洞扫描。例如，对于木马病毒扫描，可以通过将应用程序文件包与预存储的恶意程序库内的特征进行匹配，当应用程序文件包与恶意程序库内的特征相匹配时，提示该应用程序文件包为恶意程序，并建议用户禁止对该应用程序的安装。这样，在安装应用程序前，通过对待安装应用程序文件包进行深度安全扫描，可以识别出恶意应用程序，极大降低用户误安装恶意应用程序的概率。

[0102] 本发明实施例中，作为可选实施例，应用程序按照智能终端设备操作系统提供的钩子的类和接口进行安装，即应用程序按照现有安装流程进行安装，本发明实施例提供的基于智能终端设备安装应用程序的第三方软件在该应用程序安装完成后，在监测到安装的应用程序进行智能终端设备操作系统授予的行为权限的首次访问后，触发加载用户预先为该应用程序设置的应用程序授权权限列表，使得智能终端设备操作系统按照加载的应用程序授权权限列表包含的授权行为权限，更新该应用程序在安装过程中针对智能终端设备操作系统授予的行为权限，即判断首次访问的行为权限(应用程序安装过程中智能终端设备操作系统授予的行为权限)是否与所述应用程序授权权限列表中授权的任一行为权限相匹配。

[0103] 由上述可见，本发明实施例的基于 Android 平台的应用程序访问方法，用户预先选择并确定可以授予应用程序的行为权限以及禁止授予的行为权限，并在应用程序安装后，当安装的应用程序需要进行在安装过程中申请的行为权限访问时，将申请的行为权限与用户预先选择并确定的行为权限进行匹配，依据匹配结果执行相应的操作。这样，对于一些敏感行为权限，例如，发送短信、读取联系人等行为权限，用户在该应用程序安装前，即可禁止该应用程序获取用户对敏感行为权限的授权，在应用程序安装后，采用用户安装该应用程序前选择并确定的授权权限对应用程序行为权限进行权限管理。因而，即使用户不小心安装并运行了恶意应用程序，由于相应的行为权限已经在安装前被用户禁止，可以将安全隐患损失降到最低，有效提高 Android 平台的安全性。具体来说，本发明实施例具有安装前的权限管理机制，即在应用程序安装前，用户可以为应用程序授予选择的行为权限；行为权限访问控制机制，在应用程序首次进行申请的行为权限访问时，需要与用户预先设置的行为权限进行匹配；以及，安装后的权限管理机制，即在应用程序安装完成后，允许用户对已安装的应用程序授予的行为权限进行权限修改，并将修改的授权权限进行存储，以供应用程序在运行时根据修改的行为权限进行相应的访问。

[0104] 图 2 示出了本发明实施例基于智能终端设备的应用程序访问装置结构。参见图 2，该装置包括：监测模块、判断模块以及权限处理模块，其中，

[0105] 监测模块，用于在监测到安装的应用程序进行智能终端设备操作系统授予的行为权限的首次访问后，通知判断模块，所述智能终端设备操作系统授予的行为权限为在应用程序安装过程中授予的行为权限；

[0106] 判断模块，用于根据接收的通知，读取用户预先为该应用程序设置的应用程序授

权权限列表，判断首次访问的行为权限是否与所述应用程序授权权限列表中授权的任一行为权限相匹配，所述应用程序授权权限列表中包含有用户为所述应用程序选择性授权的一个或多个行为权限；

[0107] 权限处理模块，用于确定所述首次访问的行为权限与所述应用程序授权权限列表中授权的任一行为权限不匹配，拒绝应用程序进行智能终端设备操作系统授予的行为权限的首次访问。

[0108] 本发明实施例中，判断模块包括：解析单元、查询单元以及判断单元(图中未示出)，其中，

[0109] 解析单元，解析用于安装应用程序的应用程序文件包，获取应用程序文件包中的应用程序标识；

[0110] 本发明实施例中，获取应用程序申请的行为权限包括：通过应用程序官方下载网站获取应用程序文件包；解析应用程序文件包中的配置信息文件，得到该应用程序需要申请的行为权限。其中，解析应用程序文件包中的配置信息文件包括：解压基于智能终端设备的应用程序文件，从解压的应用程序文件中获取加密的全局变量描述的配置信息文件，并对加密的配置信息文件进行解密，获取解密的原始配置信息文件，利用 Java 中的可扩展标记语言文件解析器扫描解密的原始配置信息文件中的权限描述部分。

[0111] 查询单元，用于根据获取的应用程序标识，查询预先设置的应用程序授权权限列表库，得到该应用程序标识对应的应用程序授权权限列表；

[0112] 本发明实施例中，设置应用程序授权权限列表库包括：对每一应用程序，采集并获取应用程序申请的行为权限；根据用户从获取的应用程序申请的行为权限中选取的行为权限，生成存储在应用程序授权权限列表库中的应用程序授权权限列表。每一所述应用程序对应一所述应用程序授权权限列表，多个应用程序授权权限列表组成应用程序授权权限列表库。

[0113] 判断单元，用于判断首次访问的行为权限是否与得到的所述应用程序授权权限列表中的任一行为权限相匹配。

[0114] 较佳地，判断模块还可以进一步包括：

[0115] 第一分类单元，用于将获取的应用程序申请的行为权限分类为用于提醒用户重点关注的隐私权限以及按照应用程序申请直接授权的其它权限。

[0116] 实际应用中，判断模块还可以进一步包括：

[0117] 第二分类单元，用于将隐私权限分为运行应用程序所必需的必需权限以及运行应用程序可选的非必需权限，并在授权设置界面向用户展示所述非必要权限的提示信息。

[0118] 作为可选实施例，判断模块还可以进一步包括：

[0119] 验证单元，用于利用隔离沙箱、和 / 或，静态代码分析、和 / 或，自动代码特征扫描方法，对应用程序申请的所述必需权限进行合法性以及合理性的验证，以确定必需权限中的每一行为权限是否都为应用程序运行时所需的必不可少的行为权限，如果不是，则将该行为权限从必需权限中删除，并作为非必要权限向用户展示。

[0120] 作为可选实施例，该装置还可以进一步包括：

[0121] 展示模块，用于将获取的应用程序申请的行为权限进行展示。

[0122] 作为另一可选实施例，该装置还可以进一步包括：

[0123] 安全扫描模块，用于对待安装的应用程序文件包进行安全扫描，如果待安装的应用程序文件包通过安全扫描，安装该应用程序文件包以生成应用程序，否则，结束流程。

[0124] 本发明实施例中，安全扫描包括但不限于木马病毒扫描、广告插件扫描、漏洞扫描。

[0125] 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。

[0126] 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。

[0127] 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。

[0128] 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。

[0129] 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。

[0130] 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基于智能终端设备的应用程序访问装置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。

[0131] 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。

[0132] 本发明公开了，A1. 一种基于智能终端设备的应用程序访问方法，包括：

[0133] 在监测到安装的应用程序进行智能终端设备操作系统授予的行为权限的首次访问或曾经被拒绝访问后，读取用户预先为该应用程序设置的应用程序授权权限列表，所述智能终端设备操作系统授予的行为权限为在应用程序安装过程中授予的行为权限，所述应用程序授权权限列表中包含有用户为所述应用程序选择性授权的一个或多个行为权限；

[0134] 判断首次访问或曾经被拒绝访问的行为权限是否与所述应用程序授权权限列表中授权的任一行为权限相匹配；

[0135] 确定所述首次访问或曾经被拒绝访问的行为权限与所述应用程序授权权限列表中授权的任一行为权限不匹配，拒绝应用程序进行智能终端设备操作系统授予的行为权限的首次访问。

[0136] A2. 根据 A1 所述的方法，所述读取用户预先为该应用程序设置的应用程序授权权限列表包括：

[0137] 解析应用程序对应的应用程序文件包，获取应用程序文件包中的应用程序标识；

[0138] 根据获取的应用程序标识，查询预先设置的应用程序授权权限列表库，得到该应用程序标识对应的应用程序授权权限列表。

[0139] A3. 根据 A2 所述的方法，设置所述应用程序授权权限列表库包括：

[0140] 对每一应用程序，采集并获取应用程序申请的行为权限；

[0141] 根据用户从获取的应用程序申请的行为权限中授权的行为权限，生成存储在应用程序授权权限列表库中的应用程序授权权限列表。

[0142] A4. 根据 A3 所述的方法，所述获取应用程序申请的权限包括：

[0143] 通过应用程序官方下载网站获取应用程序文件包；

[0144] 解析应用程序文件包中的配置信息文件，得到该应用程序需要申请的行为权限。

[0145] A5. 根据 A4 所述的方法，所述解析应用程序文件包中的配置信息文件包括：

[0146] 解压基于智能终端设备的应用程序文件，从解压的应用程序文件中获取加密的全局变量描述的配置信息文件，并对加密的配置信息文件进行解密，获取解密的原始配置信息文件，扫描解密的原始配置信息文件中的行为权限描述部分。

[0147] A6. 根据 A5 所述的方法，利用 Java 中的可扩展标记语言文件解析器，解析所述解密的原始配置信息文件中的行为权限描述部分。

[0148] A7. 根据 A1 所述的方法，每一所述应用程序对应一所述应用程序授权权限列表，多个应用程序授权权限列表组成应用程序授权权限列表库，所述应用程序授权权限列表中包含的授权行为权限为所述智能终端设备操作系统授予的行为权限的一部分。

[0149] A8. 根据 A3 所述的方法，在所述根据用户从获取的应用程序申请的权限中授权的行为权限之前，所述方法进一步包括：

[0150] 将获取的应用程序申请的行为权限进行展示。

[0151] A9. 根据 A3 所述的方法，在所述获取应用程序申请的行为权限之后，所述方法进一步包括：

[0152] 将获取的应用程序申请的行为权限分类为用于提醒用户重点关注的隐私权限以及按照应用程序申请直接授权的其它权限。

[0153] A10. 根据 A9 所述的方法，所述方法进一步包括：

[0154] 将隐私权限分为运行应用程序所必需的必需权限以及运行应用程序可选的非必需权限，并由用户选取和更新必需权限以及非必需权限，以及，在授权设置界面向用户展示所述非必要权限的提示信息。

[0155] A11. 根据 A10 所述的方法，所述方法进一步包括：

[0156] 利用隔离沙箱、和 / 或，静态代码分析、和 / 或，自动代码特征扫描方法，对应用程序申请的所述必需权限进行合法性以及合理性的验证，以确定必需权限中的每一权限是否都为应用程序运行时所需的必不可少的权限，如果不是，则将该权限从必需权限中删除，并作为非必要权限向用户展示。

[0157] A12. 根据 A1 所述的方法，在所述监测到安装的应用程序首次进行申请的权限访问之前，所述方法进一步包括：

[0158] 对待安装的应用程序文件包进行安全扫描，如果待安装的应用程序文件包通过安全扫描，安装所述应用程序文件包，否则，结束流程。

[0159] A13. 根据 A12 所述的方法，所述安全扫描包括但不限于木马病毒扫描、广告插件扫描、漏洞扫描。

[0160] A14. 根据 A1 所述的方法，所述智能终端设备的运行平台包括但不限于安卓平台。

[0161] A15. 一种基于智能终端设备的应用程序访问装置，该装置包括：监测模块、判断模块以及权限处理模块，其中，

[0162] 监测模块，用于在监测到安装的应用程序进行智能终端设备操作系统授予的行为权限的首次访问后，通知判断模块，所述智能终端设备操作系统授予的行为权限为在应用程序安装过程中授予的行为权限；

[0163] 判断模块，用于根据接收的通知，读取用户预先为该应用程序设置的应用程序授权权限列表，判断首次访问的行为权限是否与所述应用程序授权权限列表中授权的任一行为权限相匹配，所述应用程序授权权限列表中包含有用户为所述应用程序选择性授权的一个或多个行为权限；

[0164] 权限处理模块，用于确定所述首次访问的行为权限与所述应用程序授权权限列表中授权的任一行为权限不匹配，拒绝应用程序进行智能终端设备操作系统授予的行为权限的首次访问。

[0165] A16. 根据 A15 所述的装置，所述判断模块包括：解析单元、查询单元以及判断单元，其中，

[0166] 解析单元，解析用于安装应用程序的应用程序文件包，获取应用程序文件包中的应用程序标识；

[0167] 查询单元，用于根据获取的应用程序标识，查询预先设置的应用程序授权权限列表库，得到该应用程序标识对应的应用程序授权权限列表；

[0168] 判断单元，用于判断首次访问的行为权限是否与得到的所述应用程序授权权限列表中授权的任一行为权限相匹配。

[0169] A17. 根据 A16 所述的装置，所述判断模块进一步包括：

[0170] 第一分类单元，用于将获取的应用程序申请的权限分类为用于提醒用户重点关注的隐私权限以及按照应用程序申请直接授权的其它权限。

[0171] A18. 根据 A17 所述的装置，所述判断模块进一步包括：

[0172] 第二分类单元，用于将隐私权限分为运行应用程序所必需的必需权限以及运行应用程序可选的非必需权限，并在授权设置界面向用户展示所述非必要权限的提示信息。

[0173] A19. 根据 A18 所述的装置，所述判断模块进一步包括：

[0174] 验证单元，用于利用隔离沙箱、和 / 或，静态代码分析、和 / 或，自动代码特征扫描方法，对应用程序申请的所述必需权限进行合法性以及合理性的验证，以确定必需权限中的每一权限是否都为应用程序运行时所需的必不可少的权限，如果不是，则将该权限从必需权限中删除，并作为非必要权限向用户展示。

[0175] A20. 根据 A15 所述的装置，进一步包括：

[0176] 展示模块，用于将获取的应用程序申请的行为权限进行展示。

[0177] A21. 根据 A17 所述的装置，进一步包括：

[0178] 安全扫描模块，用于对待安装的应用程序文件包进行安全扫描，如果待安装的应用程序文件包通过安全扫描，安装所述应用程序文件包，否则，结束流程。

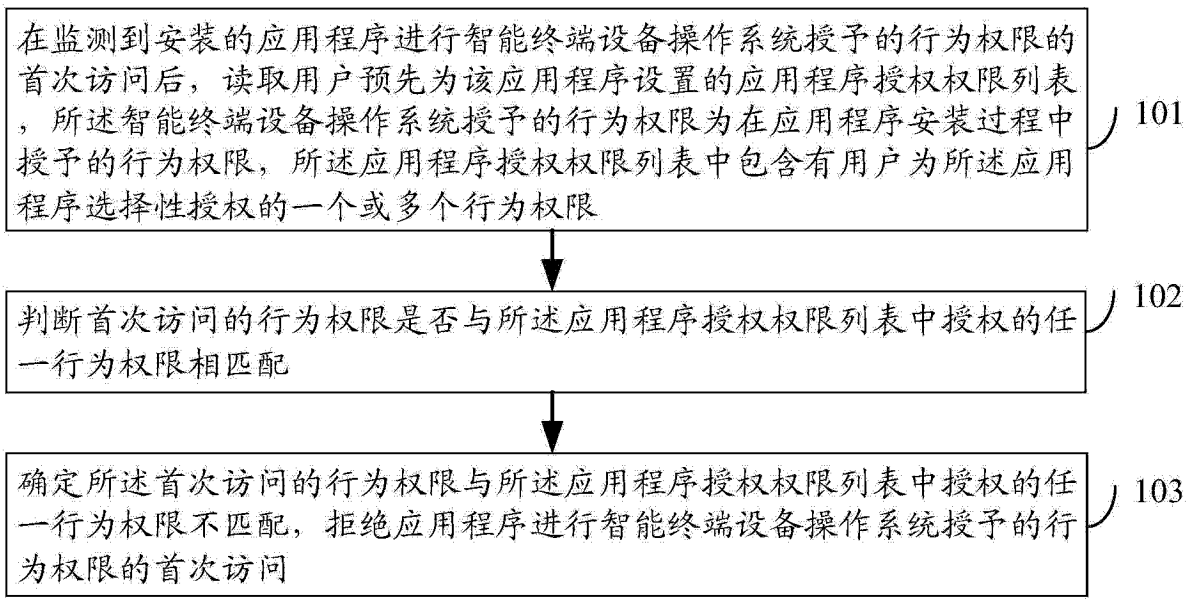

在监测到安装的应用程序进行智能终端设备操作系统授予的行为权限的首次访问后，读取用户预先为该应用程序设置的应用程序授权权限列表，所述智能终端设备操作系统授予的行为权限为在应用程序安装过程中授予的行为权限，所述应用程序授权权限列表中包含有用户为所述应用程序选择性授权的一个或多个行为权限
101
判断首次访问的行为权限是否与所述应用程序授权权限列表中授权的任一行为权限相匹配
102
确定所述首次访问的行为权限与所述应用程序授权权限列表中授权的任一行为权限不匹配，拒绝应用程序进行智能终端设备操作系统授予的行为权限的首次访问
103

图 1

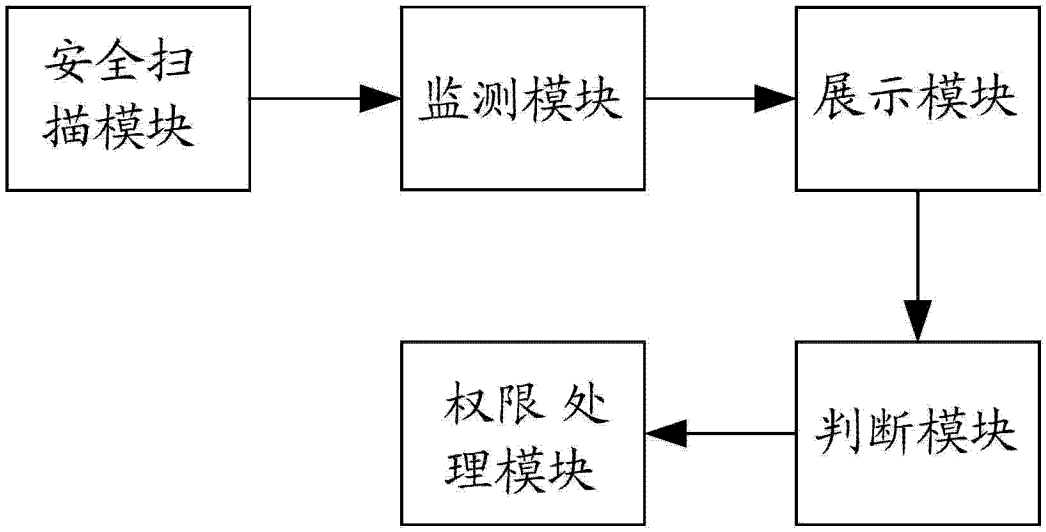

安全扫描模块
监测模块
展示模块
判断模块
权限 处理模块

图 2