(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2015 年 8 月 27 日 (27.08.2015)

WIPO | PCT

(10) 国际公布号
WO 2015/124017 A1

(51) 国际专利分类号:
G06F 21/51 (2013.01)

(21) 国际申请号: PCT/CN2014/093595

(22) 国际申请日: 2014 年 12 月 11 日 (11.12.2014)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201410060683.X 2014 年 2 月 21 日 (21.02.2014) CN
201410060381.2 2014 年 2 月 21 日 (21.02.2014) CN
201410060681.0 2014 年 2 月 21 日 (21.02.2014) CN

(71) 申请人: **北京奇虎科技有限公司 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED)** [CN/CN]; 中国北京市西城区新街口外大街 28 号 D 座 112 室（德胜园区）, Beijing 100088 (CN)。 **奇智软件（北京）有限公司 (QIZHI SOFTWARE (BEIJING) COMPANY LIMITED)** [CN/CN]; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼 B 座 2 层、3 层 301-306 室, Beijing 100015 (CN)。

(72) 发明人: **姚彤 (YAO, Tong)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。 **丁祎 (DING, Yi)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。

(74) 代理人: **北京华沛德权律师事务所 (BEIJING BRIGHT & RIGHT LAW FIRM)**; 中国北京市朝阳区朝外大街乙 12 号昆泰国际大厦 1008 室, Beijing 100020 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA,

[见续页]

(54) Title: METHOD AND APPARATUS FOR APPLICATION INSTALLATION BASED ON INTELLIGENT TERMINAL DEVICE

(54) 发明名称 : 基于智能终端设备安装应用程序的方法与装置

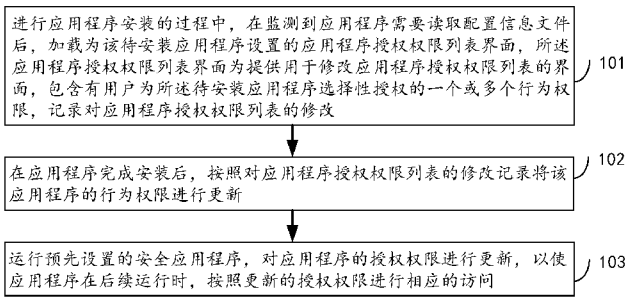

图 1 / FIG. 1

101 DURING INSTALLATION OF AN APPLICATION, UPON DETECTING THAT THE APPLICATION NEEDS TO READ A CONFIGURATION INFORMATION FILE, LOAD AN APPLICATION AUTHORIZED PERMISSION LIST INTERFACE SET FOR THE APPLICATION TO BE INSTALLED, WHEREIN THE APPLICATION AUTHORIZED PERMISSION LIST INTERFACE IS AN INTERFACE FOR MODIFYING AN APPLICATION AUTHORIZED PERMISSION LIST, COMPRISES ONE OR MORE ACTION PERMISSIONS SELECTIVELY AUTHORIZED BY A USER FOR THE APPLICATION TO BE INSTALLED, AND RECORDS MODIFICATIONS TO THE APPLICATION AUTHORIZED PERMISSION LIST

102 UPON COMPLETION OF THE INSTALLATION OF THE APPLICATION, UPDATE THE ACTION PERMISSIONS OF THE APPLICATION ACCORDING TO THE RECORDS OF THE MODIFICATIONS TO THE APPLICATION AUTHORIZED PERMISSION LIST

103 RUN A PRESET SECURITY APPLICATION AND UPDATE AUTHORIZED PERMISSIONS OF THE APPLICATION, SO THAT THE APPLICATION PERFORMS CORRESPONDING ACCESS ACCORDING TO THE UPDATED AUTHORIZED PERMISSIONS IN SUBSEQUENT RUNNING

(57) **Abstract**: Provided are a method and apparatus for application installation based on an intelligent terminal device. The method comprises: during installation of an application, upon detecting that the application needs to read a configuration information file, loading an application authorized permission list interface set for the application to be installed, wherein the application authorized permission list interface is an interface for modifying an application authorized permission list, comprises one or more action permissions selectively authorized by a user for the application to be installed, and records modifications to the application authorized permission list (101); and upon completion of the installation of the application, updating the action permissions of the application according to the records of the modifications to the application authorized permission list (102). By means of the method and apparatus, the user security can be improved.

(57) **摘要**: 提供一种基于智能终端设备安装应用程序的方法与装置，该方法包括：进行应用程序安装的过程中，在监测到应用程序需要读取配置信息文件后，加载为该待安装应用程序设置的应用程序授权权限列表界面，所述应用程序授权权限列表界面为提供用于修改应用程序授权权限列表的界面，包含有用户为所述待安装应用程序选择性授权的一个或多个行为权限，记录对应用程序授权权限列表的修改(101)；在应用程序完成安装后，按照对应用程序授权权限列表的修改记录将该应用程序的行为权限进行更新(102)。应用所述方法与装置，可以提升用户安全性。

WO 2015/124017 A1

RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

根据细则 4.17 的声明:

— 关于申请人有权申请并被授予专利(细则 4.17(ii))

— 发明人资格(细则 4.17(iv))

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

基于智能终端设备安装应用程序的方法与装置

技术领域

本发明涉及移动智能终端操作系统平台技术，具体涉及一种基于智能终端设备安装应用程序的方法与装置。

背景技术

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。

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。

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，即智能终端设备操作系统从整体上授予行为权限。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。

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。

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行为权限管理功能，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，也就是说，通过运行安全应用程序，可以提供给用户超级管理员的权限（即root权限），使得用户可以利用超级管理员权限修改和更新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行为权限前的时间段内，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

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安装应用程序的方法与装置、计算机程序以及计算机可读介质。

依据本发明的一个方面，提供了基于智能终端设备安装应用程序的方法，该方法包括：

进行应用程序安装的过程中，在监测到应用程序需要读取配置信息文件后，加载为该待安装应用程序设置的应用程序授权权限列表界面，所述应用程序授权权限列表界面为提供用于修改应用程序授权权限列表的界面，包含有用户为所述待安装应用程序选择性授权的一个或多个行为权限，记录对应用程序授权权限列表的修改；

在应用程序完成安装后，按照对应用程序授权权限列表的修改记录将该应用程序的行为权限进行更新。

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、加载模块以及权限配置模块，其中，

监测模块，用于在应用程序安装的过程中，在监测到应用程序需要读取配置信息文件后，通知加载模块；

加载模块，用于根据接收的通知，加载为该待安装应用程序设置的应用程序授权权限列表界面，所述应用程序授权权限列表界面为提供用于修改应用程序授权权限列表的界面，包含有用户为所述待安装应用程序选择性授权的一个或多个行为权限，记录对应用程序授权权限列表的修改；

权限配置模块，用于在应用程序完成安装后，按照对应用程序授权权限列表的修改记录将该应用程序的行为权限进行更新。

依据本发明的一个方面，提供了基于智能终端设备安装应用程序的方法，该方法包括：

进行应用程序安装，在监测到应用程序需要读取配置信息文件后，加载为该待安装应用程序设置的应用程序授权权限列表界面，所述应用程序授权权限列表界面为提供用于修改应用程序授权权限列表的界面，包含有用户为所述待安装应用程序选择性授权的一个或多个行为权限；

按照加载的应用程序授权权限列表界面包含的授权行为权限配置应用程序的行为权限，并完成应用程序的安装。

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、加载模块以及权限配置模块，其中，

监测模块，用于进行应用程序安装，在监测到应用程序需要读取配置信息文件后，通知加载模块；

加载模块，用于根据接收的通知，加载为该待安装应用程序设置的应用程

序授权权限列表界面，所述应用程序授权权限列表界面为提供用于修改应用程序授权权限列表的界面，包含有用户为所述待安装应用程序选择性授权的一个或多个行为权限；

权限配置模块，用于按照加载的应用程序授权权限列表界面包含的授权行为权限配置应用程序的行为权限，并完成应用程序的安装。

依据本发明的一个方面，提供了基于智能终端设备安装应用程序的方法，该方法包括：

进行应用程序安装，在监测到应用程序需要读取配置信息文件后，加载用户预先为该待安装应用程序设置的应用程序授权权限列表，所述应用程序授权权限列表中包含有用户为所述待安装应用程序选择性授权的一个或多个行为权限；

按照加载的应用程序授权权限列表包含的授权行为权限配置应用程序的行为权限，并完成应用程序的安装。

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、加载模块以及权限配置模块，其中，

监测模块，用于进行应用程序安装，在监测到应用程序需要读取配置信息文件后，通知加载模块；

加载模块，用于根据接收的通知，加载用户预先为该待安装应用程序设置的应用程序授权权限列表，所述应用程序授权权限列表中包含有用户为所述待安装应用程序选择性授权的一个或多个行为权限；

权限配置模块，用于按照加载的应用程序授权权限列表包含的授权行为权限配置应用程序的行为权限，并完成应用程序的安装。

根据本发明的另一个方面，提供了一种计算机程序，其包括计算机可读代码，当电子设备运行所述计算机可读代码时，导致所述的基于智能终端设备安装应用程序的方法被执行。

根据本发明的再一个方面，提供了一种计算机可读介质，其中存储了如上所述的计算机程序。

根据本发明的基于智能终端设备安装应用程序的方法与装置，可以通过安装应用程序安装完成，重新选择并确定可以授予该应用程序的权限以及禁止授予的权限，从而更新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，或根据本发明的基于智能终端设备安装应用程序的方法与装置，可以通过安装应用程序之前，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，在应用程序安装时，配置用户预先为该应用程序的授权权限，由此解决了在安装应用程序前，即可禁止应用程序获取用户对敏感行为权

限的授权，使得应用程序安装后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。

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

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。本实施例的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：

图1示出了本发明实施例基于智能终端设备安装应用程序的方法流程；以及，

图2示出了本发明实施例基于智能终端设备安装应用程序的另一方法流程；

图3示出了本发明实施例基于智能终端设备安装应用程序的又一方法流程；

图4示出了本发明实施例基于智能终端设备安装应用程序的装置结构；

图5示出了用于执行本发明的方法的电子设备的框图；以及

图6示出了用于保持或者携带实现根据本发明的方法的程序代码的存储单元示意图。

具体实施方式

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。

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行为权限前，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。

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安装应用程序的方法，通过预先获取各应用程序申请的行为权限，并在应用程序安装前，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，并在应用程序安装过程中，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安装后具有的行为权限，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，或通过应用程序授权权限列表更新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，从而使得应用程序将生成的应用程序授权权限列表作为应用程序安装后具有的行为权限，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。

图1示出了本发明实施例基于智能终端设备安装应用程序的方法流程，所述智能终端设备的运行平台包括但不限于安卓平台。参见图1，该流程包括：

步骤101，进行应用程序安装的过程中，在监测到应用程序需要读取配置信息文件后，加载为该待安装应用程序设置的应用程序授权权限列表界面，所述应用程序授权权限列表界面为提供用于修改应用程序授权权限列表的界面，包含有用户为所述待安装应用程序选择性授权的一个或多个行为权限，记录对应用程序授权权限列表的修改；

本步骤中，加载为该待安装应用程序设置的应用程序授权权限列表界面包括：

A11，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；

本步骤中，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。

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；

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，但用户仍可对所有权限授权或禁止。

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：

对每一应用程序，执行如下步骤B11和B12：

B11，在应用程序安装过程中，在监测到应用程序读取配置信息文件后，采集并获取应用程序在所述配置信息文件中针对智能终端设备操作系统申请的行为权限；

本步骤中，在安装某一应用程序之前，需要预先为该应用程序进行权限授权。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。

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针对智能终端设备操作系统需要申请的行为权限。

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。

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

文件名：AndroidManifest.xml

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

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。

B12，根据用户从获取的应用程序申请的行为权限中选取的授权的行为权限，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。

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，作为可选实施例，可以在应用程序安装过程中，在应用程序读取的配置信息文件对应的安装界面，分别为每一应用程序进行权限授权，智能终端设备操作系统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，即记录用户在安装界面选取并授权的行为权限，以作后续加载应用，其中，配置信息文件中包含有由智能终端设备操作系统授予应用程序的行为权限。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，后续用于更新应用程序的行为权限符合所述用程序授权权限列表界面的显示。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，且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，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。

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：

将获取的应用程序申请的行为权限进行展示。

本步骤中，还可以为用户提供授权设置界面（应用程序授权权限列表界面），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。

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：

对获取的应用程序申请的行为权限进行分类。

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。

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.permission.CALL_PHONE）、写系统设置（android.permission.WRITE_SYNC_SETTINGS）、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，对于发送短消息权限，对应的函数为SmsManager.sendTextMessage、SmsManager.sendDataMessage、SmsManager.sendMultipartTextMessage 等。

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。

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。

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行为权限，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。

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。

A13，在安装界面加载得到的应用程序授权权限列表，生成所述应用程序授权权限列表界面。

本步骤中，采用加载的应用程序授权权限列表界面替换所述应用程序在安装过程中由智能终端设备操作系统提供的安装界面。加载为该待安装应用程序设置的应用程序授权权限列表界面包括：通过 钩子将由智能终端设备操作系统提供的安装界面跳转指向至所述应用程序授权权限列表界面，并在确认或完成应用程序授权权限列表修改后，结束对所述智能终端设备操作系统提供的安装界面的跳转。具体地，可以在Android平台框架层的源代码中找到应用程序

安装执行中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，使得需要读取配置信息文件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，而非指向应用程序文件包中的配置信息文件，运行预先设置的程序代码段，将应用程序授权权限列表加载到当前安装界面，生成所述应用程序授权权限列表界面，并在完成该应用程序授权权限列表界面后，指向读取该应用程序的配置信息文件后的操作，使得在完成该应用程序授权权限列表界面后的操作与现有读取应用程序的配置信息文件后的操作相同。即在按照加载的应用程序授权权限列表界面包含的授权行为权限配置应用程序的行为权限后的界面中，设置下一步控件需对应插入钩子的类和接口指向，所述指向与所述应用程序读取配置信息文件进行应用程序的行为权限配置后显示的下一步控件需对应插入钩子的类和接口的指向相同。关于依据本发明实施例描述的功能实现源代码的修改，为公知技术，在此略去详述。实际应用中，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加载，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。

步骤102，在应用程序完成安装后，按照对应用程序授权权限列表的修改记录将该应用程序的行为权限进行更新。

本步骤中，在应用程序安装器按照加载的应用程序授权权限列表配置好应用程序的行为权限后，后续安装流程为公知技术，在此略去详述。

本发明实施例在应用程序安装过程中，举例来说，向用户展示的应用程序授权权限列表界面可以分行显示，每行依序具体如下：该应用程序申请11项权限，是否安装此应用程序？（第一行）；3项隐私权限（非必要权限，建议取消）（第二行）；读取位置信息（第三行，读取位置信息前设置有可选框控件）；发送短信（第四行，发送短信前设置有可选框控件）；拨打电话（第五行，拨打电话前设置有可选框控件）；8项其它权限（第六行）等；在界面的最底端，设置有取消控件、安装控件。这样，在加载应用程序授权权限列表后，可以按照安卓平台的整体授权策略进行应用程序的安装，不同的是，该应用程序授权权限列表为用户预先为该应用程序设置的授权权限以及禁止权限，而非应用程序文件包携带的配置信息文件中的申请的权限，使得配置的所述应用程序的行为权限符合所述用程序授权权限列表界面的显示。

作为可选实施例，在后续流程中，用户如果需要对应用程序的授权权限进

行调整，该方法还可以进一步包括：

步骤103，运行预先设置的安全应用程序，对应用程序的授权权限进行更新，以使应用程序在后续运行时，按照更新的授权权限进行相应的访问。

本步骤中，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，可以通过运行安全应用程序，在安全应用程序对应的更新界面，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。

当然，实际应用中，也可以在应用程序试图访问需要权限的应用程序接口（API，Application Program Interface）时，Android 平台根据用户为该应用程序设置的应用程序授权权限列表中的记录，判断访问API的权限是否被禁用，如果访问API的权限被禁用，该应用程序可以通过人机接口提示用户是否选择修改；若用户选择修改权限，则Android 平台允许该应用程序访问所述API，否则，Android 平台通知该应用程序退出访问。

作为另一可选实施例，还可以在安装应用程序对应的应用程序文件包之前，对该待安装的应用程序文件包进行安全扫描，以确保待安装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：

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，执行所述安装应用程序文件包的流程，否则，结束流程。

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。

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，使得在现有应用程序的安装界面不显示包含应用程序安装完成的提示信息，并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界面，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界面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，进而，在监测到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完成后，触发在安装界面显示包含应用程序安装完成的提示信息。

由上述可见，本发明实施例的基于Android平台安装应用程序的方法，用户在安装应用程序后，触发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。这样，对于一些敏感行为权限，例如，发送短信、读取联系人等权限，用户在安装该应用程序后，通过利用预先为应用程序设置的应用程序授权权限列表界面包含的授权行为权限，更新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，即可禁止该应用程序获取用户对敏感行为权限的授权。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后至应用程序运行前已被用户禁止，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，用户可以为待安装的应用程序授予选择的行为权限；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权限进行相应的访问。

图4示出了本发明实施例基于智能终端设备安装应用程序的装置结构。参见图4，该装置包括：监测模块、加载模块以及权限配置模块，其中，

监测模块，用于在应用程序安装的过程中，在监测到应用程序需要读取配置信息文件后，通知加载模块；

本发明实施例中，监测模块在应用程序安装完成后，控制在现有应用程序的安装界面不显示包含应用程序安装完成的提示信息，并通知加载模块，并在监测到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完成后，触发在安装界面显示包含应用程序安装完成的提示信息。

作为可选实施例，监测模块还可以进一步用于在监测到应用程序访问需要行为权限的应用程序接口后，安卓平台根据用户为该应用程序设置的应用程序授权权限列表中的记录，判断访问应用程序接口的权限是否被禁用，如果访问应用程序接口的权限被禁用，通过人机接口提示用户是否选择修改；若用户选择修改权限，则安卓平台允许该应用程序访问所述应用程序接口，否则，安卓平台通知该应用程序退出访问。

加载模块，用于根据接收的通知，加载为该待安装应用程序设置的应用程序授权权限列表界面，所述应用程序授权权限列表界面为提供用于修改应用程序授权权限列表的界面，包含有用户为所述待安装应用程序选择性授权的一个

或多个行为权限，记录对应用程序授权权限列表的修改；

权限配置模块，用于在应用程序完成安装后，按照对应用程序授权权限列表的修改记录将该应用程序的行为权限进行更新。

本发明实施例中，加载模块包括：解析单元、查询单元以及加载单元（图中未示出），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；

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。

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；

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。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。

加载单元，用于在安装界面加载得到的应用程序授权权限列表，生成所述应用程序授权权限列表界面。

较佳地，加载模块还可以进一步包括：

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。

实际应用中，加载模块还可以进一步包括：

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。

作为可选实施例，加载模块还可以进一步包括：

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。

作为可选实施例，加载单元包括：查询子单元、重配置子单元以及界面生成子单元，其中，

查询子单元，用于在智能终端设备运行平台框架层的源代码中，找到应用程序的配置信息文件中需要插入钩子的类和接口，所述类和接口为涉及到用户隐私权限的类和接口；

重配置子单元，用于分析并修改所述类和接口的源代码，使得需要读取配置信息文件时插入的钩子的所述类和接口指向预先为该待安装应用程序设置的应用程序授权权限列表；

界面生成子单元，运行预先设置的程序代码段，将应用程序授权权限列表加载到当前安装界面，生成所述应用程序授权权限列表界面。

作为可选实施例，该装置还可以进一步包括：

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。

作为另一可选实施例，该装置还可以进一步包括：

权限更新模块，用于运行预先设置的安全应用程序，对应用程序的授权行为权限进行更新，以使应用程序在后续运行时，按照更新的授权行为权限进行相应的访问。

作为再一可选实施例，该装置还可以进一步包括：

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，执行所述安装应用程序文件包的流程，否则，结束流程。

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。

图2示出了本发明实施例基于智能终端设备安装应用程序的方法流程。参见图2，该流程包括：

步骤201，进行应用程序安装，在监测到应用程序需要读取配置信息文件后，加载为该待安装应用程序设置的应用程序授权权限列表界面，所述应用程序授权权限列表界面为提供用于修改应用程序授权权限列表的界面，包含有用户为所述待安装应用程序选择性授权的一个或多个行为权限；

本步骤中，加载为该待安装应用程序设置的应用程序授权权限列表界面包括：

A211，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；

本步骤中，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。

A212，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；

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，但用户仍可对所有权限授权或禁止。

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：

对每一应用程序，执行如下步骤B211和B212：

B211，采集并获取应用程序申请的行为权限；

本步骤中，在安装某一应用程序之前，需要预先为该应用程序进行权限授权。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。

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。

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。

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

文件名：AndroidManifest.xml

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

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。

B212,根据用户从获取的应用程序申请的行为权限中选取的授权的行为权限，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。

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。

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：

将获取的应用程序申请的行为权限进行展示。

本步骤中，为用户提供授权设置界面（应用程序授权权限列表界面），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。

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：

对获取的应用程序申请的行为权限进行分类。

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。

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.permission.CALL_PHONE）、写系统设置（android.permission.WRITE_SYNC_SETTINGS）、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，对于发送短消息权限，对应的函数为SmsManager.sendTextMessage、SmsManager.sendDataMessage、SmsManager.sendMultipartTextMessage 等。

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。

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。

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行为权限，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。

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。

A213，在安装界面加载得到的应用程序授权权限列表，生成所述应用程序授权权限列表界面。

本步骤中，采用加载的应用程序授权权限列表界面替换所述应用程序安装过程中由智能终端设备操作系统提供的安装界面。加载为该待安装应用程序设置的应用程序授权权限列表界面包括：通过 钩子将由智能终端设备操作系统提供的安装界面跳转指向至所述应用程序授权权限列表界面，并在确认或完成应用程序授权权限列表修改后，结束对所述智能终端设备操作系统提供的安装界面的跳转。具体地，可以在Android平台框架层的源代码中找到应用程序安装执行中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，使得需要读取配置信息文件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，而

非指向应用程序文件包中的配置信息文件，运行预先设置的程序代码段，将应用程序授权权限列表加载到当前安装界面，生成所述应用程序授权权限列表界面，并在完成该应用程序授权权限列表界面后，指向读取该应用程序的配置信息文件后的操作，使得在完成该应用程序授权权限列表界面后的操作与现有读取应用程序的配置信息文件后的操作相同。即在按照加载的应用程序授权权限列表界面包含的授权行为权限配置应用程序的行为权限后的界面中，设置下一步控件需对应插入钩子的类和接口指向，所述指向与所述应用程序读取配置信息文件进行应用程序的行为权限配置后显示的下一步控件需对应插入钩子的类和接口的指向相同。关于依据本发明实施例描述的功能实现源代码的修改，为公知技术，在此略去详述。实际应用中，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加载，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。

步骤202，按照加载的应用程序授权权限列表界面包含的授权行为权限配置应用程序的行为权限，并完成应用程序的安装。

本步骤中，在应用程序安装器按照加载的应用程序授权权限列表配置好应用程序的行为权限后，后续安装流程为公知技术，在此略去详述。

本发明实施例在应用程序安装过程中，举例来说，向用户展示的应用程序授权权限列表界面可以分行显示，每行依序具体如下：该应用程序申请11项权限，是否安装此应用程序？（第一行）；3项隐私权限（非必要权限，建议取消）（第二行）；读取位置信息（第三行，读取位置信息前设置有可选框控件）；发送短信（第四行，发送短信前设置有可选框控件）；拨打电话（第五行，拨打电话前设置有可选框控件）；8项其它权限（第六行）等；在界面的最底端，设置有取消控件、安装控件。这样，在加载应用程序授权权限列表后，可以按照安卓平台的整体授权策略进行应用程序的安装，不同的是，该应用程序授权权限列表为用户预先为该应用程序设置的授权权限以及禁止权限，而非应用程序文件包携带的配置信息文件中的申请的权限，使得配置的所述应用程序的行为权限符合所述用程序授权权限列表界面的显示。

作为可选实施例，在后续流程中，用户如果需要对应用程序的授权权限进行调整，该方法还可以进一步包括：

步骤203，运行预先设置的安全应用程序，对应用程序的授权权限进行更新，以使应用程序在后续运行时，按照更新的授权权限进行相应的访问。

本步骤中，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，可以通过运行安全应用程序，在安全应用程序对应的更新界面，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。

当然，实际应用中，也可以在应用程序试图访问需要权限的应用程序接口（API，Application Program Interface） 时，Android 平台根据用户为该应用程序设置的应用程序授权权限列表中的记录，判断访问API的权限是否被禁用，如果访问API的权限被禁用，该应用程序可以通过人机接口提示用户是否选择修改；若用户选择修改权限，则Android 平台允许该应用程序访问所述API，否则，Android 平台通知该应用程序退出访问。

作为另一可选实施例，还可以在安装应用程序文件包之前，对该待安装的应用程序文件包进行安全扫描，以确保待安装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：

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，执行所述安装应用程序文件包的流程，否则，结束流程。

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。

由上述可见，本发明实施例的基于Android平台安装应用程序的方法，用户在安装应用程序之前，即可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。这样，对于一些敏感行为权限，例如，发送短信、读取联系人等权限，用户在安装该应用程序前，即可禁止该应用程序获取用户对敏感行为权限的授权，在应用程序安装过程中，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权限进行配置。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，用户可以为待安装的应用程序授予选择的行为权限；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权限进行相应的访问。

图4示出了本发明实施例基于智能终端设备安装应用程序的装置结构。参见图4，该装置包括：监测模块、加载模块以及权限配置模块，其中，

监测模块，用于进行应用程序安装，在监测到应用程序需要读取配置信息文件后，通知加载模块；

本发明实施例中，监测模块还可以进一步用于在监测到应用程序访问需要行为权限的应用程序接口后，安卓平台根据用户为该应用程序设置的应用程序授权权限列表中的记录，判断访问应用程序接口的权限是否被禁用，如果访问应用程序接口的权限被禁用，通过人机接口提示用户是否选择修改；若用户选择修改权限，则安卓平台允许该应用程序访问所述应用程序接口，否则，安卓平台通知该应用程序退出访问。

加载模块，用于根据接收的通知，加载为该待安装应用程序设置的应用程序授权权限列表界面，所述应用程序授权权限列表界面为提供用于修改应用程序授权权限列表的界面，包含有用户为所述待安装应用程序选择性授权的一个或多个行为权限；

权限配置模块，用于按照加载的应用程序授权权限列表界面包含的授权行为权限配置应用程序的行为权限，并完成应用程序的安装。

本发明实施例中，加载模块包括：解析单元、查询单元以及加载单元（图中未示出），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；

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。

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；

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。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。

加载单元，用于在安装界面加载得到的应用程序授权权限列表，生成所述应用程序授权权限列表界面。

较佳地，加载模块还可以进一步包括：

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。

实际应用中，加载模块还可以进一步包括：

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。

作为可选实施例，加载模块还可以进一步包括：

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。

作为可选实施例，加载单元包括：查询子单元、重配置子单元以及界面生成子单元，其中，

查询子单元，用于在智能终端设备运行平台框架层的源代码中，找到应用程序的配置信息文件中需要插入钩子的类和接口，所述类和接口为涉及到用户隐私权限的类和接口；

重配置子单元，用于分析并修改所述类和接口的源代码，使得需要读取配置信息文件时插入的钩子的所述类和接口指向预先为该待安装应用程序设置的应用程序授权权限列表；

界面生成子单元，运行预先设置的程序代码段，将应用程序授权权限列表加载到当前安装界面，生成所述应用程序授权权限列表界面。

作为可选实施例，该装置还可以进一步包括：

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。

作为另一可选实施例，该装置还可以进一步包括：

权限更新模块，用于运行预先设置的安全应用程序，对应用程序的授权行为权限进行更新，以使应用程序在后续运行时，按照更新的授权行为权限进行相应的访问。

作为再一可选实施例，该装置还可以进一步包括：

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，执行所述安装应用程序文件包的流程，否则，结束流程。

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。

图3示出了本发明实施例基于智能终端设备安装应用程序的方法流程。参见图3，该流程包括：

步骤301，进行应用程序安装，在监测到应用程序需要读取配置信息文件后，加载用户预先为该待安装应用程序设置的应用程序授权权限列表，所述应用程序授权权限列表中包含有用户为所述待安装应用程序选择性授权的一个或多个行为权限；

本步骤中，加载用户预先为该待安装应用程序设置的应用程序授权权限列表包括：

A311，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；

本步骤中，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。

A312，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；

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，但用户仍可对所有权限授权或禁止。

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：

对每一应用程序，执行如下步骤B311和B312：

B311，在应用程序安装过程中，在监测到应用程序读取配置信息文件后，采集并获取应用程序在所述配置信息文件中针对智能终端设备操作系统申请的行为权限；

本步骤中，在安装某一应用程序之前，需要预先为该应用程序进行权限授权。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。

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。

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。

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

文件名：AndroidManifest.xml

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

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。

B312，根据用户从获取的应用程序申请的行为权限中选取的授权的行为权限，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。

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。

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：

将获取的应用程序申请的行为权限进行展示。

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。

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：

对获取的应用程序申请的行为权限进行分类。

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。

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.permission.CALL_PHONE）、写系统设置（android.permission.WRITE_SYNC_SETTINGS）、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，对于发送短消息权限，对应的函数为SmsManager.sendTextMessage、SmsManager.sendDataMessage、SmsManager.sendMultipartTextMessage 等。

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。

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。

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行为权限，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。

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。

A313，在安装界面加载得到的应用程序授权权限列表。

本步骤中，智能终端设备操作系统为安卓系统。加载用户预先为该待安装应用程序设置的应用程序授权权限列表包括：通过 钩子将由智能终端设备操作系统提供的安装界面跳转指向至应用程序授权权限列表对应的界面，并在确认或完成应用程序授权权限列表修改后，结束对所述智能终端设备操作系统提供的安装界面的跳转。具体地，可以在Android平台框架层的源代码中找到应用程序安装执行中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，使得需要读取配置信息文件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，而非指向应用程序文件包中的配置信息文件，运行预先设置的程序代码段，将应用程序授权权限列表加载到当前安装界面，并在完成加载到当前安装界面后，指向读取该应用程序的配置信息文件后的操作，使得在完成该应用程序授权权限列表后的操作与现有读取应用程序的配置信息文件后的操作相同。即在按照加载的应用程序授权权限列表包含的授权行为权限配置应用程序的行为权限后的界面中，设置下一步控件需对应插入钩子的类和接口指向，所述指向与所述应用程序读取配置信息文件进行应用程序的行为权限配置后显示的下一步控件需对应插入钩子的类和接口的指向相同。关于依据本发明实施例描述的功能实现源代码的修改，为公知技术，在此略去详述。实际应用中，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加载，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。

步骤302，按照加载的应用程序授权权限列表包含的授权行为权限配置应用程序的行为权限，并完成应用程序的安装。

本步骤中，在应用程序安装器按照加载的应用程序授权权限列表配置好应用程序的行为权限后，后续安装流程为公知技术，在此略去详述。

本发明实施例在应用程序安装过程中，举例来说，向用户展示的应用程序

授权权限列表对应的界面可以分行显示，每行依序具体如下：该应用程序申请11项权限，是否安装此应用程序？（第一行）；3项隐私权限（非必要权限，建议取消）（第二行）；读取位置信息（第三行，读取位置信息前设置有可选框控件）；发送短信（第四行，发送短信前设置有可选框控件）；拨打电话（第五行，拨打电话前设置有可选框控件）；8项其它权限（第六行）等；在界面的最底端，设置有取消控件、安装控件。这样，在加载应用程序授权权限列表后，可以按照安卓平台的整体授权策略进行应用程序的安装，不同的是，该应用程序授权权限列表为用户预先为该应用程序设置的授权权限以及禁止权限，而非应用程序文件包携带的配置信息文件中的申请的权限，使得配置的所述应用程序的行为权限符合所述用程序授权权限列表。

作为可选实施例，在后续流程中，用户如果需要对应用程序的授权权限进行调整，该方法还可以进一步包括：

步骤303，运行预先设置的安全应用程序，对应用程序的授权权限进行更新，以使应用程序在后续运行时，按照更新的授权权限进行相应的访问。

本步骤中，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，可以通过运行安全应用程序，在安全应用程序对应的更新界面，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。

当然，实际应用中，也可以在应用程序试图访问需要权限的应用程序接口（API，Application Program Interface）时，Android 平台根据用户为该应用程序设置的应用程序授权权限列表中的记录，判断访问API的权限是否被禁用，如果访问API的权限被禁用，该应用程序可以通过人机接口提示用户是否选择修改；若用户选择修改权限，则Android 平台允许该应用程序访问所述API，否则，Android 平台通知该应用程序退出访问。

作为另一可选实施例，还可以在安装应用程序文件包之前，对该待安装的应用程序文件包进行安全扫描，以确保待安装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：

对待安装的应用程序对应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，执行所述安装应用程序文件包的流程，否则，结束流程。

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。

由上述可见，本发明实施例的基于Android平台安装应用程序的方法，用户在安装应用程序之前，即可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。这样，对于一些敏感行为权限，例如，发送短信、读取联系人等权限，用户在安装该应用程序前，即可禁止该应用程序获取用户对敏感行为权限的授权，在应用程序安装过程中，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权限进行配置。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，用户可以为待安装的应用程序授予选择的行为权限；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权限进行相应的访问。

图4示出了本发明实施例基于智能终端设备安装应用程序的装置结构。参见图4，该装置包括：监测模块、加载模块以及权限配置模块，其中，

监测模块，用于进行应用程序安装，在监测到应用程序需要读取配置信息文件后，通知加载模块；

本发明实施例中，监测模块还可以进一步用于在监测到应用程序访问需要行为权限的应用程序接口后，安卓平台根据用户为该应用程序设置的应用程序授权权限列表中的记录，判断访问应用程序接口的权限是否被禁用，如果访问应用程序接口的权限被禁用，通过人机接口提示用户是否选择修改；若用户选择修改权限，则安卓平台允许该应用程序访问所述应用程序接口，否则，安卓平台通知该应用程序退出访问。

加载模块，用于根据接收的通知，加载用户预先为该待安装应用程序设置的应用程序授权权限列表，所述应用程序授权权限列表中包含有用户为所述待安装应用程序选择性授权的一个或多个行为权限；

权限配置模块，用于按照加载的应用程序授权权限列表包含的授权行为权限配置应用程序的行为权限，并完成应用程序的安装。

本发明实施例中，加载模块包括：解析单元、查询单元以及加载单元（图

中未示出），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；

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。

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；

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。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。

加载单元，用于在安装界面加载得到的应用程序授权权限列表。

较佳地，加载模块还可以进一步包括：

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。

实际应用中，加载模块还可以进一步包括：

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。

作为可选实施例，加载模块还可以进一步包括：

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。

作为可选实施例，加载单元包括：查询子单元、重配置子单元以及界面生成子单元，其中，

查询子单元，用于在智能终端设备运行平台框架层的源代码中，找到应用

程序的配置信息文件中需要插入钩子的类和接口，所述类和接口为涉及到用户隐私权限的类和接口；

重配置子单元，用于分析并修改所述类和接口的源代码，使得需要读取配置信息文件时插入的钩子的所述类和接口指向预先为该待安装应用程序设置的应用程序授权权限列表；

界面生成子单元，运行预先设置的程序代码段，将应用程序授权权限列表加载到当前安装界面。

作为可选实施例，该装置还可以进一步包括：

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。

作为另一可选实施例，该装置还可以进一步包括：

权限更新模块，用于运行预先设置的安全应用程序，对应用程序的授权行为权限进行更新，以使应用程序在后续运行时，按照更新的授权行为权限进行相应的访问。

作为再一可选实施例，该装置还可以进一步包括：

安全扫描模块，用于对待安装的应用程序对应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，执行所述安装应用程序文件包的流程，否则，结束流程。

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。

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。

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。

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。

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。

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。

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安装应用程序的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。

例如，图5示出了可以实现本发明的基于智能终端设备安装应用程序的方法的电子设备。该电子设备传统上包括处理器1210和以存储器1220形式的计算机程序产品或者计算机可读介质。存储器1220可以是诸如闪存、EEPROM（电可擦除可编程只读存储器）、EPROM、硬盘或者ROM之类的电子存储器。存储器1220具有用于执行上述方法中的任何方法步骤的程序代码1231的存储空间1230。例如，用于程序代码的存储空间1230可以包括分别用于实现上面的方法中的各种步骤的各个程序代码1231。这些程序代码可以从一个或者多个计算机程序产品中读出或者写入到这一个或者多个计算机程序产品中。这些计算机程序产品包括诸如硬盘，紧致盘（CD）、存储卡或者软盘之类的程序代码载体。这样的计算机程序产品通常为如参考图6所述的便携式或者固定存储单元。该存储单元可以具有与图5的电子设备中的存储器1220类似布置的存储段或者存储空间

等。程序代码可以例如以适当形式进行压缩。通常，存储单元包括用于执行根据本发明的方法步骤的程序1231’，即可以由例如诸如1210之类的处理器读取的代码，这些代码当由电子设备运行时，导致该电子设备执行上面所描述的方法中的各个步骤。

本文中所称的“一个实施例”、“实施例”或者“一个或者多个实施例”意味着，结合实施例描述的特定特征、结构或者特性包括在本发明的至少一个实施例中。此外，请注意，这里“在一个实施例中”的词语例子不一定全指同一个实施例。

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被实践。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。

应该注意的是，上述实施例对本发明进行的详细说明并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”或“包括”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。

此外，还应当注意，本说明书中使用的语言主要是为了可读性和教导的目的而选择的，而不是为了解释或者限定本发明的主题而选择的。因此，在不偏离所附权利要求书的范围和精神的情况下，对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。对于本发明的范围，对本发明所做的公开是说明性的，而非限制性的，本发明的范围由所附权利要求书限定。

权 利 要 求

1、一种基于智能终端设备安装应用程序的方法，包括：

进行应用程序安装的过程中，在监测到应用程序需要读取配置信息文件后，加载为该待安装应用程序设置的应用程序授权权限列表界面，所述应用程序授权权限列表界面为提供用于修改应用程序授权权限列表的界面，包含有用户为所述待安装应用程序选择性授权的一个或多个行为权限，记录对应用程序授权权限列表的修改；

在应用程序完成安装后，按照对应用程序授权权限列表的修改记录将该应用程序的行为权限进行更新。

2、如权利要求1所述的方法，所述加载为该待安装应用程序设置的应用程序授权权限列表界面包括：

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；

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；

在安装界面加载得到的应用程序授权权限列表，生成所述应用程序授权权限列表界面。

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，在应用程序安装过程中，在监测到应用程序读取配置信息文件后，采集并获取应用程序在所述配置信息文件中针对智能终端设备操作系统申请的行为权限；

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，所述获取应用程序在所述配置信息文件中针对智能终端设备操作系统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，得到该应用程序针对智能终端设备操作系统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、如权利要求5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。

7、如权利要求1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智能终端设备操作系统授予的行为权限的一部分。

8、如权利要求3所述的方法，在所述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之前，所述方法进一步包括：

将获取的应用程序申请的行为权限进行展示。

9、如权利要求3所述的方法，在所述获取应用程序在所述配置信息文件中针对智能终端设备操作系统申请的行为权限之后，所述方法进一步包括：

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。

10、如权利要求9所述的方法，所述方法进一步包括：

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。

11、如权利要求10所述的方法，所述方法进一步包括：

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。

12、如权利要求1所述的方法，所述方法进一步包括：

运行预先设置的安全应用程序，对应用程序的授权行为权限进行更新，以使应用程序在后续运行时，按照更新的授权行为权限进行相应的访问。

13、如权利要求1所述的方法，所述方法进一步包括：

在监测到应用程序访问需要行为权限的应用程序接口后，安卓平台根据用户为该应用程序设置的应用程序授权权限列表中的记录，判断访问应用程序接口的行为权限是否被禁用，如果访问应用程序接口的行为权限被禁用，通过人机接口提示用户是否选择修改；若用户选择修改行为权限，则安卓平台允许该应用程序访问所述应用程序接口，否则，安卓平台通知该应用程序退出访问。

14、如权利要求1所述的方法，在所述应用程序安装完成之前，所述方法进一步包括：

对待安装的应用程序对应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，执行所述应用程序安装的流程，否则，结束流

程。

15、如权利要求14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。

16、如权利要求1所述的方法，进一步包括：

采用加载的应用程序授权权限列表界面替换所述应用程序在安装过程中由智能终端设备操作系统提供的安装界面。

17、如权利要求1所述的方法，所述加载为该待安装应用程序设置的应用程序授权权限列表界面包括：

通过 钩子将由智能终端设备操作系统提供的安装界面跳转指向至所述应用程序授权权限列表界面，并在确认或完成应用程序授权权限列表修改后，结束对所述智能终端设备操作系统提供的安装界面的跳转。

18、如权利要求1所述的方法，所述智能终端设备操作系统为安卓系统。

19、如权利要求1所述的方法，所述加载为该待安装应用程序设置的应用程序授权权限列表界面包括：

在智能终端设备运行平台框架层的源代码中，找到应用程序的配置信息文件中需要插入钩子的类和接口，所述类和接口为涉及到用户隐私权限的类和接口；

分析并修改所述类和接口的源代码，使得需要读取配置信息文件时插入的钩子的所述类和接口指向预先为该待安装应用程序设置的应用程序授权权限列表；

运行预先设置的程序代码段，将应用程序授权权限列表加载到当前安装界面，生成所述应用程序授权权限列表界面。

20、如权利要求1所述的方法，在所述应用程序安装完成之前，所述方法进一步包括：

在按照加载的应用程序授权权限列表界面包含的授权行为权限配置应用程序的行为权限后的界面中，设置下一步控件需对应插入钩子的类和接口指向，所述指向与所述应用程序读取配置信息文件进行应用程序的行为权限配置后显示的下一步控件需对应插入钩子的类和接口的指向相同。

21、如权利要求1所述的方法，配置的所述应用程序的行为权限符合所述用程序授权权限列表界面的显示。

22、如权利要求1所述的方法，所述配置信息文件中包含有针对智能终端设备操作系统授予所述应用程序的行为权限。

23、如权利要求1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。

24、如权利要求1所述的方法，所述方法进一步包括：

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，并在该应用程序安装完成后，在安装界面不显示包含应用程序安装完成的提示信息；：

在监测到更新所述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完成后，在安装界面显示包含应用程序安装完成的提示信息。

25、一种基于智能终端设备安装应用程序的装置，其特征在于，该装置包括：监测模块、加载模块以及权限配置模块，其中，

监测模块，用于在应用程序安装的过程中，在监测到应用程序需要读取配置信息文件后，通知加载模块；

加载模块，用于根据接收的通知，加载为该待安装应用程序设置的应用程序授权权限列表界面，所述应用程序授权权限列表界面为提供用于修改应用程序授权权限列表的界面，包含有用户为所述待安装应用程序选择性授权的一个或多个行为权限，记录对应用程序授权权限列表的修改；

权限配置模块，用于在应用程序完成安装后，按照对应用程序授权权限列表的修改记录将该应用程序的行为权限进行更新。

26、如权利要求25所述的装置，其特征在于，所述加载模块包括：解析单元、查询单元以及加载单元，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；

加载单元，用于在安装界面加载得到的应用程序授权权限列表，生成所述应用程序授权权限列表界面。

27、如权利要求26所述的装置，所述加载模块进一步包括：

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。

28、如权利要求27所述的装置，所述加载模块进一步包括：

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。

29、如权利要求27所述的装置，所述加载模块进一步包括：

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。

30、如权利要求25所述的装置，进一步包括：

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。

31、如权利要求25所述的装置，进一步包括：

权限更新模块，用于运行预先设置的安全应用程序，对应用程序的授权行为权限进行更新，以使应用程序在后续运行时，按照更新的授权行为权限进行相应的访问。

32、如权利要求25所述的装置，进一步包括：

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，执行所述安装应用程序文件包的流程，否则，结束流程。

33、如权利要求26所述的装置，所述加载单元包括：查询子单元、重配置子单元以及界面生成子单元，其中，

查询子单元，用于在智能终端设备运行平台框架层的源代码中，找到应用程序的配置信息文件中需要插入钩子的类和接口，所述类和接口为涉及到用户隐私权限的类和接口；

重配置子单元，用于分析并修改所述类和接口的源代码，使得需要读取配置信息文件时插入的钩子的所述类和接口指向预先为该待安装应用程序设置的应用程序授权权限列表；

界面生成子单元，运行预先设置的程序代码段，将应用程序授权权限列表加载到当前安装界面，生成所述应用程序授权权限列表界面。

34、一种基于智能终端设备安装应用程序的方法，包括：

进行应用程序安装，在监测到应用程序需要读取配置信息文件后，加载为该待安装应用程序设置的应用程序授权权限列表界面，所述应用程序授权权限列表界面为提供用于修改应用程序授权权限列表的界面，包含有用户为所述待安装应用程序选择性授权的一个或多个行为权限；

按照加载的应用程序授权权限列表界面包含的授权行为权限配置应用程序的行为权限，并完成应用程序的安装。

35、如权利要求34所述的方法，所述加载为该待安装应用程序设置的应用程序授权权限列表界面包括：

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；

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；

在安装界面加载得到的应用程序授权权限列表，生成所述应用程序授权权限列表界面。

36、一种基于智能终端设备安装应用程序的装置，其特征在于，该装置包括：监测模块、加载模块以及权限配置模块，其中，

监测模块，用于进行应用程序安装，在监测到应用程序需要读取配置信息文件后，通知加载模块；

加载模块，用于根据接收的通知，加载为该待安装应用程序设置的应用程序授权权限列表界面，所述应用程序授权权限列表界面为提供用于修改应用程序授权权限列表的界面，包含有用户为所述待安装应用程序选择性授权的一个或多个行为权限；

权限配置模块，用于按照加载的应用程序授权权限列表界面包含的授权行为权限配置应用程序的行为权限，并完成应用程序的安装。

37、如权利要求36所述的装置，其特征在于，所述加载模块包括：解析单元、查询单元以及加载单元，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；

加载单元，用于在安装界面加载得到的应用程序授权权限列表，生成所述应用程序授权权限列表界面。

38、一种基于智能终端设备安装应用程序的方法，包括：

进行应用程序安装，在监测到应用程序需要读取配置信息文件后，加载用户预先为该待安装应用程序设置的应用程序授权权限列表，所述应用程序授权权限列表中包含有用户为所述待安装应用程序选择性授权的一个或多个行为权限；

按照加载的应用程序授权权限列表包含的授权行为权限配置应用程序的行为权限，并完成应用程序的安装。

39、如权利要求38所述的方法，所述加载用户预先为该待安装应用程序设置的应用程序授权权限列表包括：

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；

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；

在安装界面加载得到的应用程序授权权限列表。

40、一种基于智能终端设备安装应用程序的装置，其特征在于，该装置包括：监测模块、加载模块以及权限配置模块，其中，

监测模块，用于进行应用程序安装，在监测到应用程序需要读取配置信息文件后，通知加载模块；

加载模块，用于根据接收的通知，加载用户预先为该待安装应用程序设置的应用程序授权权限列表，所述应用程序授权权限列表中包含有用户为所述待安装应用程序选择性授权的一个或多个行为权限；

权限配置模块，用于按照加载的应用程序授权权限列表包含的授权行为权限配置应用程序的行为权限，并完成应用程序的安装。

41、如权利要求40所述的装置，其特征在于，所述加载模块包括：解析单元、查询单元以及加载单元，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；

加载单元，用于在安装界面加载得到的应用程序授权权限列表。

42、一种计算机程序，包括计算机可读代码，当电子设备运行所述计算机可读代码运行时，导致权利要求1-24或34-35或38-39中的任一项权利要求所述的方法被执行。

43、一种计算机可读介质，其中存储了如权利要求42所述的计算机程序。

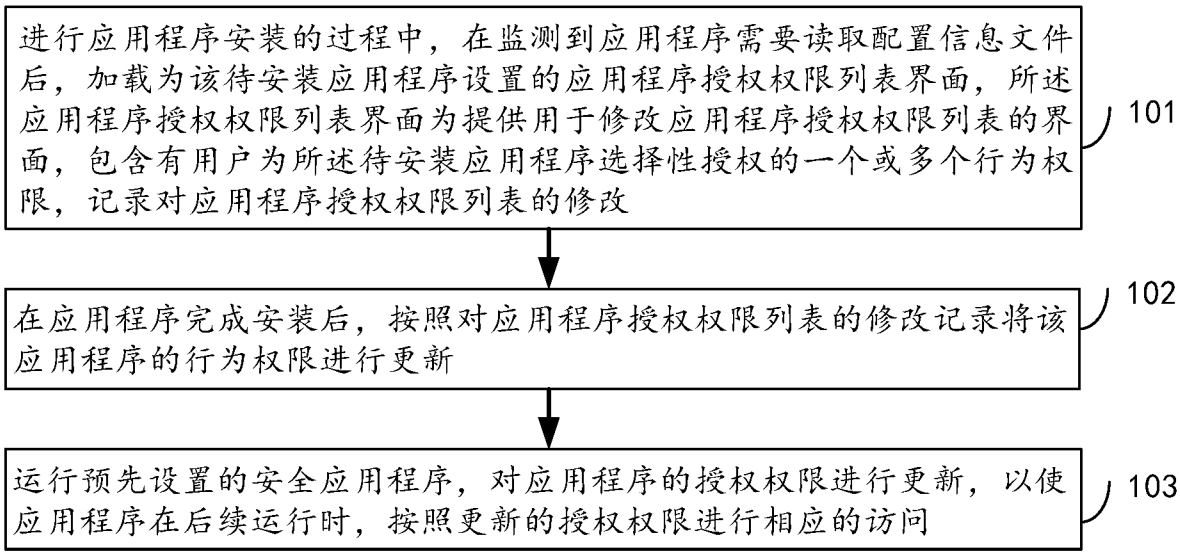
进行应用程序安装的过程中，在监测到应用程序需要读取配置信息文件后，加载为该待安装应用程序设置的应用程序授权权限列表界面，所述应用程序授权权限列表界面为提供用于修改应用程序授权权限列表的界面，包含有用户为所述待安装应用程序选择性授权的一个或多个行为权限，记录对应用程序授权权限列表的修改
101
在应用程序完成安装后，按照对应用程序授权权限列表的修改记录将该应用程序的行为权限进行更新
102
运行预先设置的安全应用程序，对应用程序的授权权限进行更新，以使应用程序在后续运行时，按照更新的授权权限进行相应的访问
103

图 1

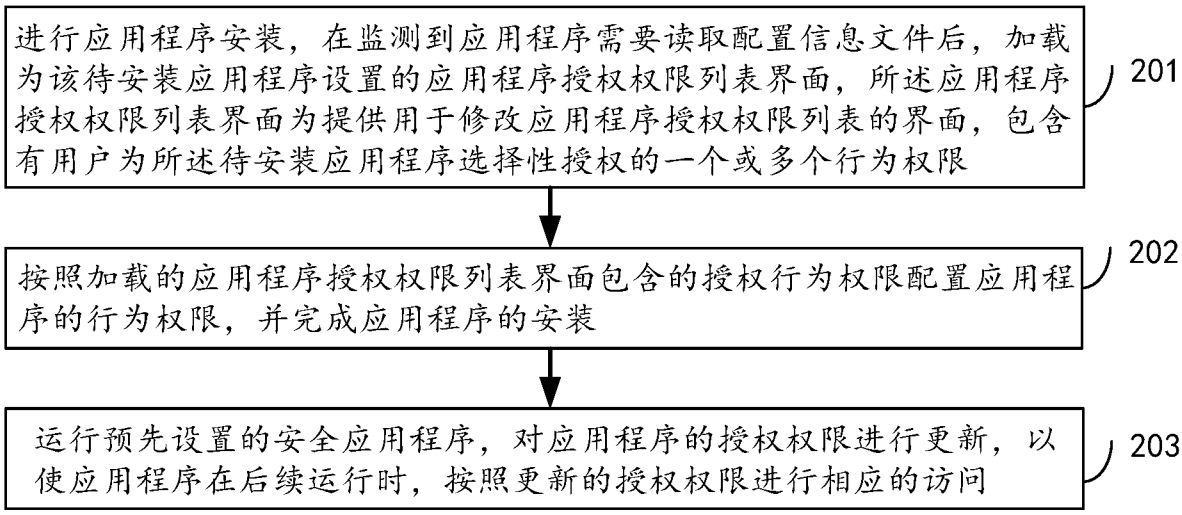
进行应用程序安装，在监测到应用程序需要读取配置信息文件后，加载为该待安装应用程序设置的应用程序授权权限列表界面，所述应用程序授权权限列表界面为提供用于修改应用程序授权权限列表的界面，包含有用户为所述待安装应用程序选择性授权的一个或多个行为权限
201
按照加载的应用程序授权权限列表界面包含的授权行为权限配置应用程序的行为权限，并完成应用程序的安装
202
运行预先设置的安全应用程序，对应用程序的授权权限进行更新，以使应用程序在后续运行时，按照更新的授权权限进行相应的访问
203

图 2

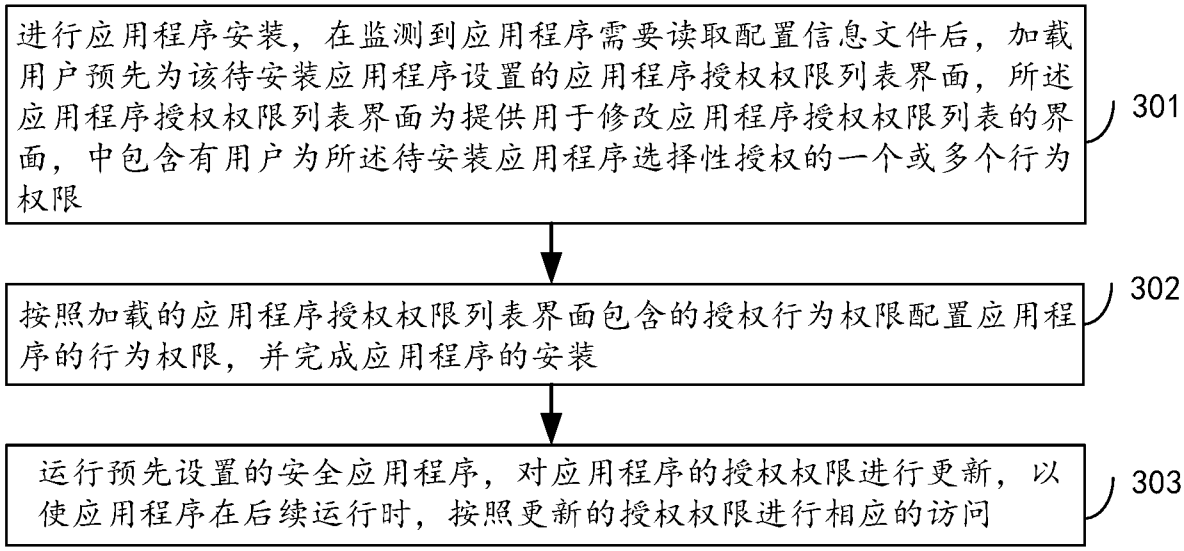
进行应用程序安装，在监测到应用程序需要读取配置信息文件后，加载用户预先为该待安装应用程序设置的应用程序授权权限列表界面，所述应用程序授权权限列表界面为提供用于修改应用程序授权权限列表的界面，中包含有用户为所述待安装应用程序选择性授权的一个或多个行为权限
301
按照加载的应用程序授权权限列表界面包含的授权行为权限配置应用程序的行为权限，并完成应用程序的安装
302
运行预先设置的安全应用程序，对应用程序的授权权限进行更新，以使应用程序在后续运行时，按照更新的授权权限进行相应的访问
303

图 3

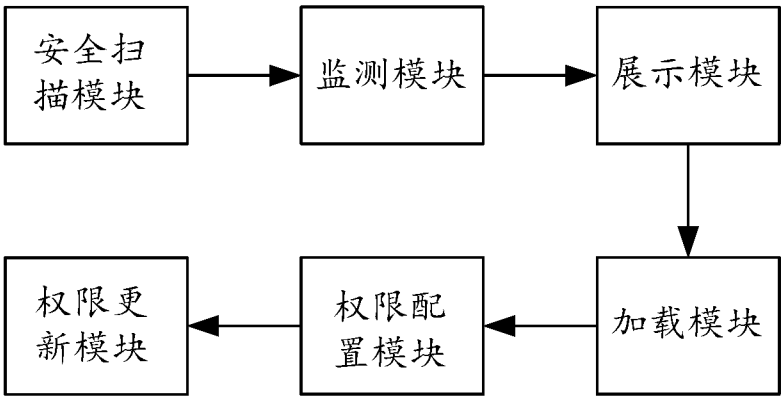
安全扫描模块
监测模块
展示模块
加载模块
权限配置模块
权限更新模块

图 4

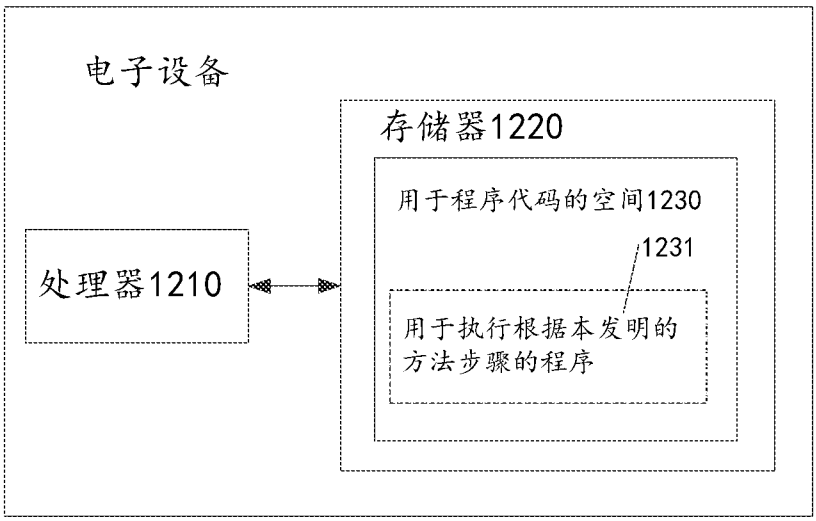
电子设备
存储器1220
用于程序代码的空间1230
1231
处理器1210
用于执行根据本发明的方法步骤的程序

图 5

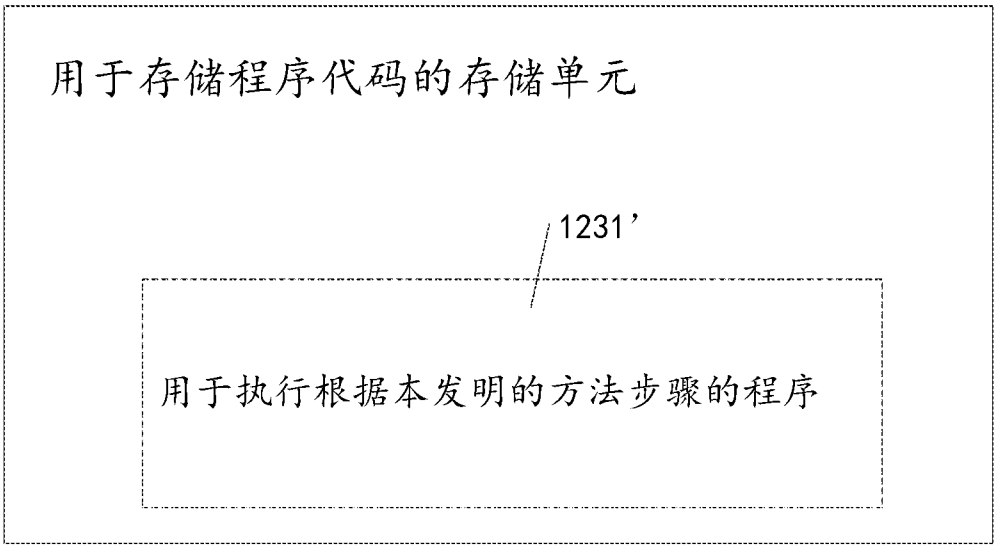
用于存储程序代码的存储单元
1231'
用于执行根据本发明的方法步骤的程序

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2014/093595

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/51 (2013.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/-

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT; CNKI; EPODOC; WPI: table, intelligence terminal, app, application, program, software, install, authorization, authority, rights, list, select, modif+, alter, chang+, update+, android

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102200922 A (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.), 28 September 2011 (28.09.2011), see claims 1-3, 5-8 and 10, and figures 2-3, 5-6, 8 and 10	1, 7, 12, 14-18, 21-23, 25, 30-32, 34, 36, 38, 40, 42-43
PX	CN 103761471 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 30 April 2014 (30.04.2014), see claims 1-4, description, paragraphs [0008]-[0079], and figures 1-2	1-33, 42-43
PX	CN 103870306 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 18 June 2014 (18.06.2014), see claims 1-2 and 8-9, and figures 1-2	34-37, 42-43
PX	CN 103839000 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 04 June 2014 (04.06.2014), see claims 1-2 and 9-10, and figures 1-2	38-43
A	CN 102289633 A (GUANG DONG OPPO MOBILE TELECOMMUNICATIONS CO., LTD.), 21 December 2011 (21.12.2011), see the whole document	1-43
A	CN 103514386 A (WISTRON CORPORATION), 15 January 2014 (15.01.2014), see the whole document	1-43

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 February 2015 (11.02.2015)	**27 February 2015 (27.02.2015)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **LI, Xinyu** Telephone No.: (86-10) **62089924**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2014/093595

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102200922 A	28 September 2011	CN 102200922 B	11 December 2013
CN 103761471 A	30 April 2014	None	
CN 103870306 A	18 June 2014	None	
CN 103839000 A	04 June 2014	None	
CN 102289633 A	21 December 2011	None	
CN 103514386 A	15 January 2014	US 2013347096 A1	26 December 2013
		TW 201401100 A	01 January 2014

国际检索报告

国际申请号 PCT/CN2014/093595

A. 主题的分类

G06F 21/51 (2013.01) i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F 21/-

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNPAT; CNKI ;EPODOC;WPI; 应用,程序,软件,安装,授权,权限,列表,表,选择,修改,更改,更新,安卓,智能终端, app, application, program, software, install, authorization, authority, rights, list, select, modif+, alter, chang+, update+, android

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 102200922 A (宇龙计算机通信科技深圳有限公司) 2011年 9月 28日 (2011-09-28) 参见权利要求1-3，5-8，10、图2-3，5-6，8，10	1，7，12，14-18，21-23，25，30-32，34，36，38，40，42-43
PX	CN 103761471 A (北京奇虎科技有限公司 等) 2014年 4月 30日 (2014-04-30) 参见权利要求1-4，说明书第【0008】至【0079】段，图1-2	1-33，42-43
PX	CN 103870306 A (北京奇虎科技有限公司 等) 2014年 6月 18日 (2014-06-18) 参见权利要求1-2，8-9，图1-2	34-37，42-43
PX	CN 103839000 A (北京奇虎科技有限公司 等) 2014年 6月 4日 (2014-06-04) 参见权利要求1-2，9-10，图1-2	38-43
A	CN 102289633 A (广东欧珀移动通信有限公司) 2011年 12月 21日 (2011-12-21) 参见全文	1-43
A	CN 103514386 A (纬创资通股份有限公司) 2014年 1月 15日 (2014-01-15) 参见全文	1-43

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2015年 2月 11日	2015年 2月 27日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 北京市海淀区蓟门桥西土城路6号 100088 中国 传真号 (86-10)62019451	李昕宇 电话号码 (86-10)62089924

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2014/093595

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	102200922	A	2011年 9月 28日	CN	102200922	B	2013年 12月 11日
CN	103761471	A	2014年 4月 30日		无		
CN	103870306	A	2014年 6月 18日		无		
CN	103839000	A	2014年 6月 4日		无		
CN	102289633	A	2011年 12月 21日		无		
CN	103514386	A	2014年 1月 15日	US	2013347096	A1	2013年 12月 26日
				TW	201401100	A	2014年 1月 1日