(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
2016 年 7 月 7 日 (07.07.2016)

WIPO | PCT

(10) 国际公布号
WO 2016/107343 A1

(51) 国际专利分类号:
G06F 21/60 (2013.01)

(21) 国际申请号: PCT/CN2015/095596

(22) 国际申请日: 2015 年 11 月 26 日 (26.11.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201410838081.2 2014 年 12 月 29 日 (29.12.2014) 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: **张爽 (ZHANG, Shuang)**; 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: **北京润泽恒知识产权代理有限公司 (BEIJING RISEHIGH INTELLECTUAL PROPERTY LAW FIRM)**; 中国北京市海淀区中关村南大街 31 号神舟大厦 702, Beijing 100081 (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, 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,

[见续页]

(54) **Title**: DETECTION METHOD AND DEVICE FOR APPLICATION PRIVACY SECURITY INFORMATION

(54) **发明名称** : 应用隐私安全信息的检测方法及装置

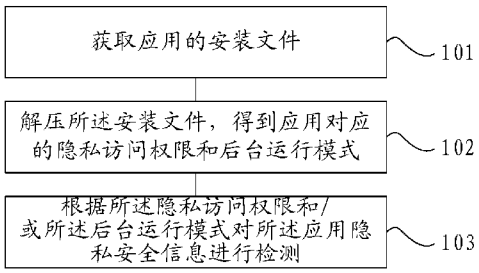

图 1 / FIG. 1

101 ACQUIRING AN INSTALLATION DOCUMENT OF AN APPLICATION
102 DECOMPRESSING THE INSTALLATION DOCUMENT TO OBTAIN A PRIVACY ACCESS PERMISSION AND A BACKGROUND OPERATION MODE CORRESPONDING TO THE APPLICATION
103 DETECTING THE APPLICATION PRIVACY SECURITY INFORMATION ACCORDING TO THE PRIVACY ACCESS PERMISSION AND/OR THE BACKGROUND OPERATION MODE

(57) **Abstract**: Disclosed are a detection method and device for application privacy security information, which relate to the technical field of information security, can more fully analyse and detect the application privacy security information, and can improve the detection efficiency of the application privacy security information at the same time. The method comprises: firstly acquiring an installation document of an application, then decompressing the installation document to obtain a privacy access permission and a background operation mode corresponding to the application, and finally detecting the application privacy security information according to the privacy access permission and/or the background operation mode. The present invention is applicable to the protection of a user's privacy security.

(57) **摘要**: 本发明公开了一种应用隐私安全信息的检测方法及装置，涉及信息安全技术领域，可以对所述应用隐私安全信息进行更加全面的分析与检测，同可以提高应用隐私安全信息的检测效率。所述方法包括：先获取应用的安装文件，然后解压所述安装文件，得到所述应用对应的隐私访问权限和后台运行模式，最后根据所述隐私访问权限和/或所述后台运行模式对所述应用隐私安全信息进行检测。本发明适用于对于用户隐私安全的保护。

WO 2016/107343 A1

RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

应用隐私安全信息的检测方法及装置

技术领域

本发明涉及一种信息安全技术，特别是涉及一种应用隐私安全信息的检测方法及装置。

背景技术

近些年来，随着智能终端设备的飞速发展，智能移动操作系统给越来越多的人们带来了简单、愉快、实用的体验。目前市场上比较流行的操作系统有：苹果公司的 ios 系统、谷歌公司的安卓系统、微软公司的 Windows Phone 系统等，这些操作系统可以配置很多的应用，使得智能终端设备具有丰富的功能。但是对于一些具有特定权限的应用，可能会对用户隐私信息安全造成危害。

目前为了防止侵犯用户隐私安全，需要首先将应用安装在操作系统上，然后采用人工方式在操作系统的隐私设置中查看并人工记录该应用的隐私访问权限，然后根据隐私访问权限分析人工分析应用隐私安全信息。

然而上述人工方式检测的方法，虽然能达到检测应用隐私安全信息的目的，但是进行检测的前提条件是应用已安装在操作系统上，而且检测过程和检测结果记录过程都是人工方式完成的，费时费力，造成检测效率较低；同时，由于只根据隐私访问权限分析应用隐私安全信息，造成对应用隐私安全信息的检测不够全面。

发明内容

有鉴于此，本发明提供一种应用隐私安全信息的检测方法及装置，主要目的在于提高应用隐私安全信息的检测效率和检测精度。

依据本发明一个方面，提供了一种应用隐私安全信息的检测方法，包

括：

获取应用的安装文件；

解压所述安装文件，得到所述应用对应的隐私访问权限和后台运行模式；

根据所述隐私访问权限和/或所述后台运行模式，对所述应用隐私安全信息进行检测。

另一方面，本发明实施例提供了一种应用隐私安全信息的检测装置，包括：

获取单元，用于获取应用的安装文件；

解压单元，用于解压所述获取单元获取的所述安装文件，得到所述应用对应的隐私访问权限和后台运行模式；

检测单元，用于根据所述隐私访问权限和/或所述后台运行模式，对所述应用隐私安全信息进行检测。

根据本发明的又一个方面，提供了一种计算机程序，其包括计算机可读代码，当所述计算机可读代码在终端设备上运行时，导致所述终端设备执行上述的任一个应用隐私安全信息的检测方法。

根据本发明的再一个方面，提供了一种计算机可读介质，其中存储了执行上述的任一个应用隐私安全信息的检测方法的计算机程序。

借由上述技术方案，本发明实施例提供的技术方案至少具有下列优点：

本发明实施例提供的技术方案，先获取应用的安装文件，然后解压所述安装文件，得到所述应用对应的隐私访问权限和后台运行模式，最后根据所述隐私访问权限和/或所述后台运行模式对所述应用隐私安全信息进行检测。与目前根据应用的隐私访问权限，通过人工方式检测应用隐私安全信息相比，本发明实施例根据隐私访问权限和后台运行模式可以对所述应用隐私安全信息进行更加全面的分析与检测，而且检测过程和检测结果记录过程可以通过智能终端自动执行完成，进而提升了检测效率。

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。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提供的一种应用隐私安全信息的检测方法流程图；

图 2 示出了本发明实施例提供的另一种应用隐私安全信息的检测方法流程图；

图 3 示出了本发明实施例提供的一种应用隐私安全信息的检测装置结构示意图。

图 4 示出了本发明实施例提供的另一种应用隐私安全信息的检测装置结构示意图；

图 5 示出了用于执行根据本发明的方法的终端设备的框图；

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。

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。

本发明实施例提供一种应用隐私安全信息的检测方法，如图 1 所示，所述方法可以应用于智能终端上，所述方法包括：

101、获取应用的安装文件。

对于本发明实施例，当操作系统为苹果公司的 ios 系统时，可以从苹果官方应用商店里下载相应应用的安装文件，此时，安装文件可以为 IPA（iPhone Application）格式文件,当操作系统为安卓系统时，也可以从第三方的应用分发平台下载相应应用的安装文件,此时，安装文件可以为 APK(Android Package)格式文件。

102、解压所述安装文件，得到所述应用对应的隐私访问权限和后台运行模式。

其中，隐私访问权限为应用具有的一些特定权限，例如，对终端中保存的联系人信息、照片信息、短信息等私密数据的访问权限，后台运行模式具体可以为应用具有在后台运行的功能，在苹果的 ios 系统中，对应用的后台运行模式的授权有着严格要求，目前只对具有音乐播放功能、或者导航功能、或者网络电话功能的应用授权后台运行模式。

103、根据所述隐私访问权限和/或所述后台运行模式，对所述应用隐私安全信息进行检测。

对于本发明实施例，通过隐私访问权限和/或所述后台运行模式相结合的方式对应用隐私安全信息进行检测，与目前只通过隐私访问权限对应用隐私安全信息进行检测相比，可以更加全面的对应用隐私安全信息进行分析，提高了应用隐私安全信息的检测效率。

本发明实施例提供的一种应用隐私安全信息的检测方法，先获取应用的安装文件，然后解压所述安装文件，得到所述应用对应的隐私访问权限和后台运行模式，最后根据所述隐私访问权限和/或所述后台运行模式对所述应用隐私安全信息进行检测。与目前根据应用的隐私访问权限，通过人工方式检测应用隐私安全信息相比，本发明实施例根据隐私访问权限和后台运行模式可以对所述应用隐私安全信息进行更加全面的分析与检测，而且检测过程和检测结果记录过程可以通过智能终端自动执行完成，进而提升了检测效率。

进一步地，本发明实施例提供另一种应用隐私安全信息的检测方法，如图 2 所示，所述方法可以应用于智能终端上，所述方法包括：

201、获取应用的安装文件。

对于本发明实施例，当操作系统为苹果公司的 ios 系统时，可以从苹果官方应用商店里下载相应应用的安装文件，此时，安装文件可以为 IPA（iPhone Application）格式文件,当操作系统为安卓系统时，也可以从第三方的应用分发平台下载相应应用的安装文件，此时，安装文件可以为 APK(Android Package)格式文件。

202、解压所述安装文件，得到所述应用对应的隐私访问权限和后台运行模式。

对于本发明实施例，解压所述安装文件，得到所述应用对应的隐私访问权限可以包括：解压所述安装文件，得到所述应用对应的可执行文件，然后通过预置命令行工具解析所述可执行文件，得到所述应用对应的隐私访问权限。其中，可执行文件为可移植可执行（PE）文件格式的文件，它可以加载到内存中，并由操作系统加载程序执行，可以为.exe 文件、.sys 文件、.com 文件等。

例如，当操作系统为苹果公司的 ios 系统时，命令行工具可以为 XCode 编程软件中的 otool 命令行工具。通过命令行工具所述可执行文件进行解析，得到所述应用对应的隐私访问权限，与目前通过人工方式检测相比，可以通过命令行工具进行解析得到所述应用对应的隐私访问权限，增加了检测的准确性，并且检测过程和检测结果记录过程可以由智能终端自动执行完成，进而提高了检测效率。

进一步地，所述解压所述安装文件，得到所述应用对应的可执行文件可以包括：解压所述安装文件，得到配置信息文件，然后从所述配置信息文件中获取所述应用对应的可执行文件名称，最后根据所述可执行文件名称，从所述安装文件中获取所述应用对应的可执行文件。

其中，配置信息文件可以为一种结构化的文本文件，其中包含了一些重要的配置信息，当被系统进行读取时，可向系统提供应用的配置信息。例如，当操作系统为苹果公司的 ios 系统时，配置信息文件可以为 Info.plist 文件，Info.plist 文件是一种结构化的文本文件，包含了一些重要的 ios 应用

配置信息，例如，包含本地化语言、应用图标名称、帮助文件的名称、可执行文件名称、后台运行模式等等。Info.plist 文件包含的可执行文件名称为 CFBundleExecutable。对于本发明实施例，解压所述安装文件，得到所述应用对应的后台运行模式可以包括：解压所述安装文件，得到所述应用的配置信息文件，然后通过所述预置命令行工具从所述配置信息文件中，获取所述应用对应的后台运行模式。

例如，当操作系统为苹果公司的 ios 系统时，配置信息文件可以为 Info.plist 文件，其中 Info.plist 文件包含的后台运行模式为 UIBackgroundModes，与目前进行应用隐私安全信息的检测时，只能通过人工方式获取到应用隐私访问权限相比，本发明实施例增加了对应用后台运行模式的获取与分析，可以更加全面地检测应用隐私安全信息。

203、根据所述隐私访问权限和/或所述后台运行模式对所述应用隐私安全信息进行检测。

具体地，检测所述应用的隐私访问权限是否符合预置条件，并且检测所述应用对应的应用类别信息是否与预置应用类别信息相匹配，所述预置应用类别信息为 ios 系统中授权可执行后台运行模式的应用对应的应用类别信息。

其中，预置条件可以根据用户实际需求进行配置，例如，预置条件可以配置为不具有对终端中保存的联系人信息、照片信息、短信息等私密数据的访问权限。在苹果的 ios 系统中，对应用的后台运行模式的授权有着严格要求，目前只对具有音乐播放功能、或者导航功能、或者网络电话功能的应用授权后台运行模式，因此，预置应用类别信息可以配置为音乐播放类应用、导航类应用、网络电话类应用

204、若所述应用的隐私访问权限不符合预置条件或者所述应用对应的应用类别信息与所述预置应用类别信息不匹配，则进行告警。

具体地，若所述应用的隐私访问权限不符合预置条件或者所述应用对应的应用类别信息与所述预置应用类别信息不匹配，可以对应用进行威胁标识，或者实时显示提示信息以提示用户该应用存在风险。

对于本发明实施例，在在苹果的 ios 系统中，解压所述安装文件，得到所述应用对应的隐私访问权限和后台运行模式的过程可以包括：

首先先将ios应用的安装文件下载到智能终端，所述安装文件可以从苹果官方AppStore商店或者从第三方的应用分发平台下载得到；然后通过解压缩工具将ios应用的IPA安装文件进行解压，得到配置信息文件，即Info.plist文件；再通过检查Info.plist文件信息，从中获取所述ios应用的后台运行模式,即UIBackgroundModes，以及获取所述ios应用的可执行文件名称，即CFBundleExecutable，然后根据CFBundleExecutable，通过解压缩工具解压所述ios应用的IPA安装文件，得到所述ios应用的可执行文件；最后通过XCode编程软件中的otool命令行工具，对所述ios应用的可执行文件进行分析应用的可执行文件进行解析，得到所述ios应用中配置的ios Framework，通过ios Framework，得到所述ios应用的隐私访问权限，其中，所述 ios Framework的具体表现形式可以如下表所示：

ios Framework名称	功能
AddressBook	通讯录
AssetsLibrary	相册（照片和视频）
EventKit	日历
CoreLocation	位置服务，即定位

以上表格只列举了与应用隐私安全信息相关的ios Framework的部分信息，但不限于此，对于多个ios应用依次执行以上步骤，可以得到每一个ios应用的隐私访问权限和后台运行模式等信息。

本发明实施例提供的另一种应用隐私安全信息的检测方法，先获取应用的安装文件，然后解压所述安装文件，得到所述应用对应的隐私访问权

限和后台运行模式，最后根据所述隐私访问权限和/或所述后台运行模式对所述应用隐私安全信息进行检测。与目前根据应用的隐私访问权限，通过人工方式检测应用隐私安全信息相比，本发明实施例根据隐私访问权限和后台运行模式可以对所述应用隐私安全信息进行更加全面的分析与检测，而且检测过程和检测结果记录过程可以通过智能终端自动执行完成，进而提升了检测效率。

进一步地，作为图 1 所述方法的具体实现，本发明实施例提供一种应用隐私安全信息的检测装置，如图 3 所示，所述装置可以为智能终端，所述装置可以包括：获取单元 31、解压单元 32、检测单元 33。

所述获取单元 31，可以用于获取应用的安装文件。

所述解压单元 32，可以用于解压获取单元 31 获取的安装文件，得到所述应用对应的隐私访问权限和后台运行模式。

所述检测单元 33，可以用于根据所述隐私访问权限和/或所述后台运行模式对所述应用隐私安全信息进行检测。

需要说明的是，本发明实施例提供的数据的处理装置所涉及各功能单元的其他相应描述，可以参考图1所示方法中的对应描述，在此不再赘述。

本发明实施例提供的一种应用隐私安全信息的检测装置，先获取应用的安装文件，然后解压所述安装文件，得到所述应用对应的隐私访问权限和后台运行模式，最后根据所述隐私访问权限和/或所述后台运行模式对所述应用隐私安全信息进行检测。与目前根据应用的隐私访问权限，通过人工方式检测应用隐私安全信息相比，本发明实施例根据隐私访问权限和后台运行模式可以对所述应用隐私安全信息进行更加全面的分析与检测，而且检测过程和检测结果记录过程可以通过智能终端自动执行完成，进而提升了检测效率。

再进一步地，作为图 2 所述方法的具体实现，本发明实施例提供另一种应用隐私安全信息的检测装置，如图 4 所示，所述装置可以为智能终端，所述装置包括：获取单元 41、解压单元 42、检测单元 43。

所述获取单元 41，可以用于获取应用的安装文件。

所述解压单元 42，可以用于解压获取单元 41 获取的安装文件，得到所述应用对应的隐私访问权限和后台运行模式。

所述检测单元 43，可以用于根据所述隐私访问权限和/或所述后台运行模式对所述应用隐私安全信息进行检测。

进一步地，所述解压单元 42，具体用于解压所述安装文件，得到所述应用对应的可执行文件；通过预置命令行工具解析所述可执行文件，得到所述应用对应的隐私访问权限。

进一步地，所述解压单元 42 包括：

第一解压模块 421、用于解压所述安装文件，得到配置信息文件配置信息文件。

第一获取模块 422、用于通过所述预置命令行工具从所述配置信息文件中，获取所述应用对应的后台运行模式。

进一步地，所述解压单元 42 还包括：

第二解压模块 423、用于解压所述安装文件，得到配置信息文件。

第二获取模块 424、用于从所述第二解压模块 423 得到的配置信息文件中，获取所述应用对应的可执行文件名称。

所述第二获取模块 424、还用于根据所述获取的可执行文件名称，从所述安装文件中获取所述应用对应的可执行文件。

进一步地，所述应用为 ios 应用，所述检测单元 43，具体用于检测所述应用的隐私访问权限是否符合预置条件，并且检测所述应用对应的应用类别信息是否与预置应用类别信息相匹配，所述预置应用类别信息为 ios 系统中授权可执行后台运行模式的应用对应的应用类别信息。

进一步地，所述装置还包括：

告警单元 44，用于若所述应用的隐私访问权限不符合预置条件或者所述应用对应的应用类别信息与所述预置应用类别信息不匹配，则进行告警。

需要说明的是，本发明实施例提供的数据的处理装置所涉及各功能单元的其他相应描述，可以参考图2所示方法中的对应描述，在此不再赘述。

本发明实施例提供的另一种应用隐私安全信息的检测装置，先获取应

用的安装文件，然后解压所述安装文件，得到所述应用对应的隐私访问权限和后台运行模式，最后根据所述隐私访问权限和/或所述后台运行模式对所述应用隐私安全信息进行检测。与目前根据应用的隐私访问权限，通过人工方式检测应用隐私安全信息相比，本发明实施例根据隐私访问权限和后台运行模式可以对所述应用隐私安全信息进行更加全面的分析与检测，而且检测过程和检测结果记录过程可以通过智能终端自动执行完成，进而提升了检测效率。

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

可以理解的是，上述方法及装置中的相关特征可以相互参考。另外，上述实施例中的“ 第一”、“ 第二”等是用于区分各实施例，而并不代表各实施例的优劣。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统，装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

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应用隐私安全信息的检测方法及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 示出了可以实现根据本发明的一种应用隐私安全信息的检测的终端设备。该终端设备传统上包括处理器 510 和以存储器 520 形式的计算机程序产品或者计算机可读介质。存储器 520 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 520 具有用于执行上述方法中的任何方法步骤的程序代码 531 的存储空间 530。例如，用于程序代码的存储空间 530 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 531。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 的终端设备中的存储器 520 类似布置的存储段、存储空间等。程序代码可以例如以适当形式进行压缩。通常，存储单元包括计算机可读代码 531’，即可以由例如诸如 510 之类的处理器读取的代码，这些代码当由终端设备运行时，导致该终端设备执行上面所描述的方法中的各个步骤。

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。

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 书

1、一种应用隐私安全信息的检测方法，包括：

获取应用的安装文件；

解压所述安装文件，得到所述应用对应的隐私访问权限和后台运行模式；

根据所述隐私访问权限和/或所述后台运行模式，对所述应用隐私安全信息进行检测。

2、根据权利要求 1 所述的应用隐私安全信息的检测方法，其特征在于，所述解压所述安装文件，得到所述应用对应的隐私访问权限包括：

解压所述安装文件，得到所述应用对应的可执行文件；

通过预置命令行工具解析所述可执行文件，得到所述应用对应的隐私访问权限。

3、根据权利要求 2 所述的应用隐私安全信息的检测方法，其特征在于，所述解压所述安装文件，得到所述应用对应的后台运行模式包括：

解压所述安装文件，得到所述应用的配置信息文件；

通过所述预置命令行工具从所述配置信息文件中，获取所述应用对应的后台运行模式。

4、根据权利要求 2 所述的应用隐私安全信息的检测方法，所述解压所述安装文件，得到所述应用对应的可执行文件包括：

解压所述安装文件，得到配置信息文件；

从所述配置信息文件中获取所述应用对应的可执行文件名称；

根据所述可执行文件名称，从所述安装文件中获取所述应用对应的可执行文件。

5、根据权利要求 1 所述的应用隐私安全信息的检测方法，其特征在于，所述应用为 ios 应用，所述根据所述隐私访问权限和所述后台运行模式对所述应用隐私安全信息进行检测包括：

检测所述应用的隐私访问权限是否符合预置条件，并且检测所述应用对应的应用类别信息是否与预置应用类别信息相匹配，所述预置应用类别信息为 ios 系统中授权可执行后台运行模式的应用对应的应用类别信息。

6、根据权利要求 5 所述的应用隐私安全信息的检测方法 ,其特征在于，还包括：

若所述应用的隐私访问权限不符合预置条件或者所述应用对应的应用类别信息与所述预置应用类别信息不匹配，则进行告警。

7、一种应用隐私安全信息的检测装置，包括：

获取单元，用于获取应用的安装文件；

解压单元，用于解压所述获取单元获取的所述安装文件，得到所述应用对应的隐私访问权限和后台运行模式；

检测单元，用于根据所述隐私访问权限和/或所述后台运行模式，对所述应用隐私安全信息进行检测。

8、根据权利要求 7 所述的应用隐私安全信息的检测装置 ,其特征在于，

所述解压单元，具体用于解压所述安装文件，得到所述应用对应的可执行文件；通过预置命令行工具解析所述可执行文件，得到所述应用对应的隐私访问权限。

9、根据权利要求 8 所述的应用隐私安全信息的检测装置 ,其特征在于，所述解压单元包括：

第一解压模块，用于解压所述安装文件，得到配置信息文件配置信息文件；

第一获取模块，用于通过所述预置命令行工具从所述配置信息文件中，获取所述应用对应的后台运行模式。

10、根据权利要求 8 所述的应用隐私安全信息的检测装置，所述解压单元还包括：

第二解压模块，用于解压所述安装文件，得到配置信息文件；

第二获取模块，用于从所述第二解压模块得到的配置信息文件中，获取所述应用对应的可执行文件名称；

所述第二获取模块，还用于根据所述获取的可执行文件名称，从所述安装文件中获取所述应用对应的可执行文件。

11、根据权利要求 7 所述的应用隐私安全信息的检测装置，其特征在于，所述应用为 ios 应用，

所述检测单元，具体用于检测所述应用的隐私访问权限是否符合预置条件，并且检测所述应用对应的应用类别信息是否与预置应用类别信息相匹配，所述预置应用类别信息为 ios 系统中授权可执行后台运行模式的应用对应的应用类别信息。

12、根据权利要求 11 所述的应用隐私安全信息的检测装置，其特征在于，所述装置还包括：

告警单元，用于若所述应用的隐私访问权限不符合预置条件或者所述应用对应的应用类别信息与所述预置应用类别信息不匹配，则进行告警。

13、一种计算机程序，包括计算机可读代码，当所述计算机可读代码在终端设备上运行时，导致所述终端设备执行根据权利要求 1-6 中的任一个所述的应用隐私安全信息的检测方法。

14、一种计算机可读介质，其中存储了如权利要求 13 所述的计算机程序。

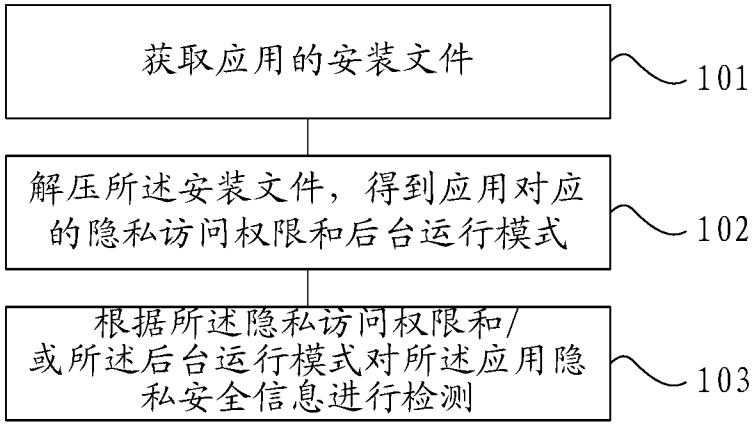
获取应用的安装文件
101
解压所述安装文件，得到应用对应的隐私访问权限和后台运行模式
102
根据所述隐私访问权限和/或所述后台运行模式对所述应用隐私安全信息进行检测
103

图 1

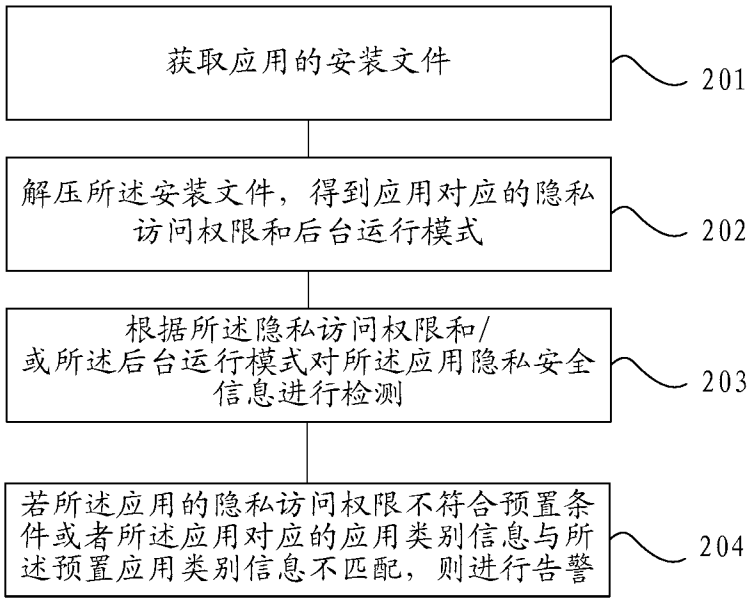
获取应用的安装文件
201
解压所述安装文件，得到应用对应的隐私访问权限和后台运行模式
202
根据所述隐私访问权限和/或所述后台运行模式对所述应用隐私安全信息进行检测
203
若所述应用的隐私访问权限不符合预置条件或者所述应用对应的应用类别信息与所述预置应用类别信息不匹配，则进行告警
204

图 2

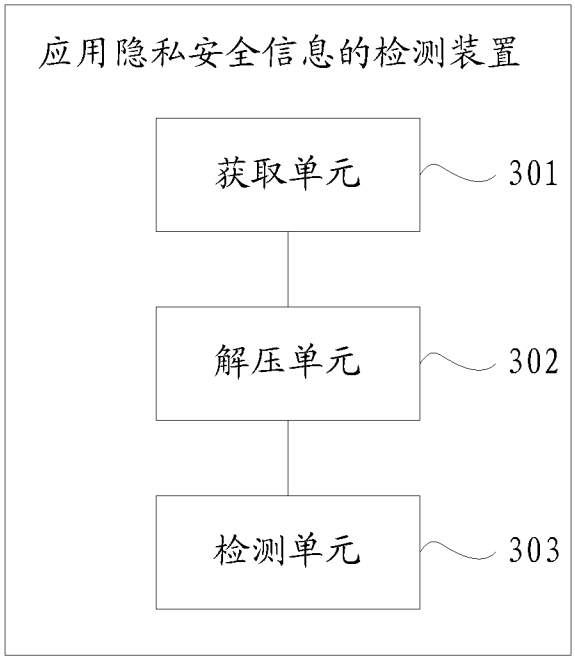
应用隐私安全信息的检测装置
获取单元
301
解压单元
302
检测单元
303

图 3

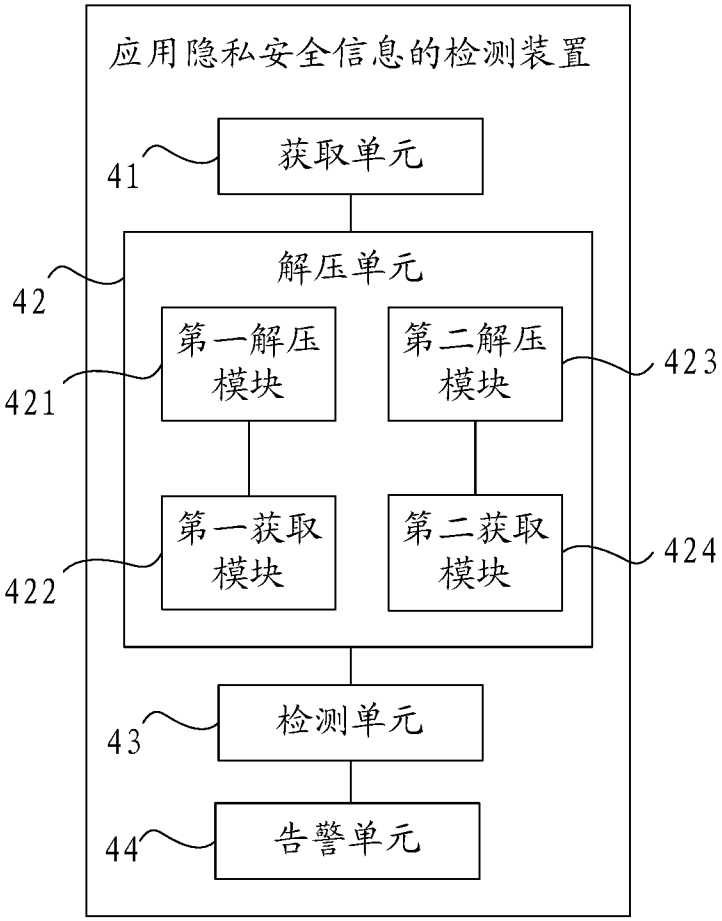
应用隐私安全信息的检测装置
41
获取单元
解压单元
42
第一解压模块
421
第二解压模块
423
第一获取模块
422
第二获取模块
424
43
检测单元
44
告警单元

图 4

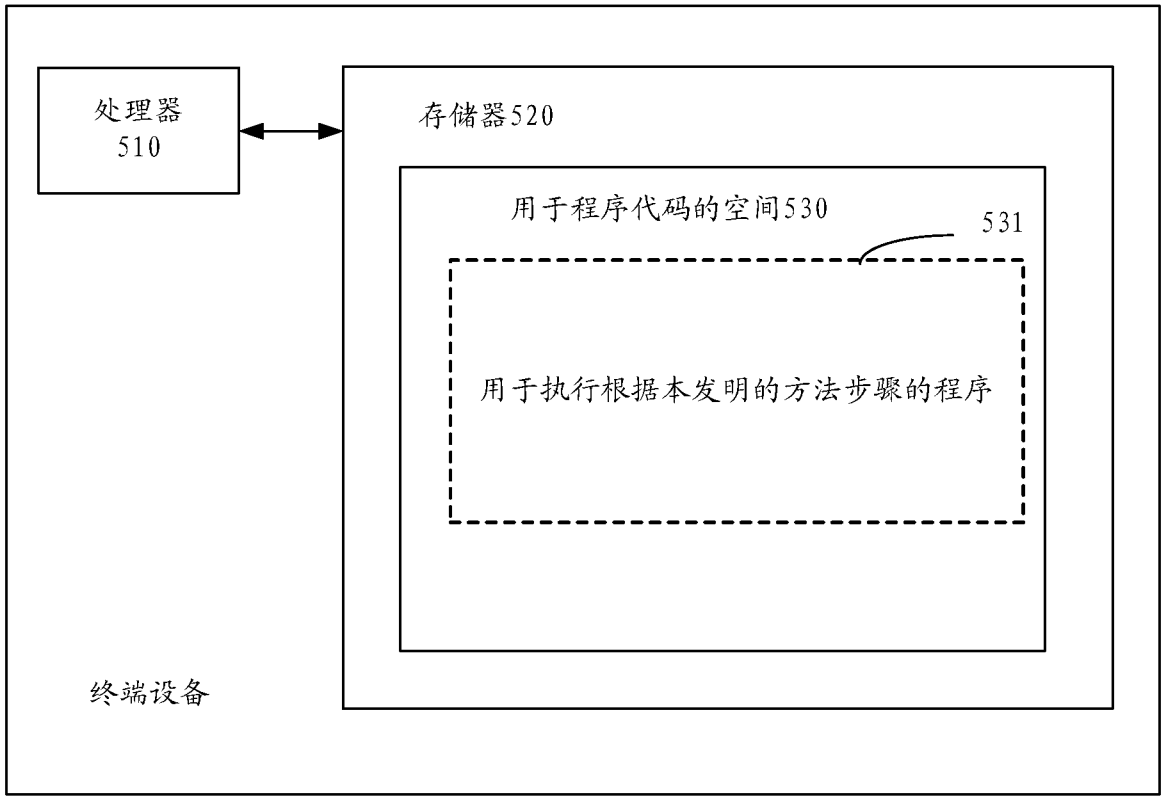
处理器
510
存储器520
用于程序代码的空间530
531
用于执行根据本发明的方法步骤的程序
终端设备

图 5

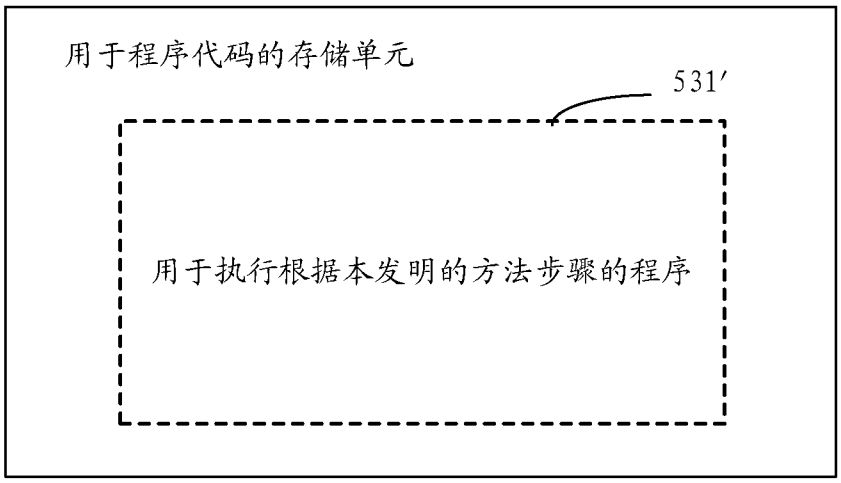
用于程序代码的存储单元
531′
用于执行根据本发明的方法步骤的程序

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/095596

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/60 (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

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)

CPRS, VEN: install, application, decompression, privacy, permission

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102426639 A (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.), 25 April 2012 (25.04.2012), description, pages 2-3	1-14
A	CN 103136472 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.), 05 June 2013 (05.06.2013), the whole document	1-14

☐ 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
22 February 2016 (22.02.2016)	**26 February 2016 (26.02.2016)**
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 **WANG, Dan** Telephone No.: (86-10) **62412062**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/095596

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102426639 A	25 April 2012	CN 102426639 B	08 April 2015
CN 103136472 A	05 June 2013	US 2014013429 A1	09 January 2014
		WO 2013079010 A1	06 June 2013
		KR 20130135952 A	11 December 2013

国际检索报告

国际申请号
PCT/CN2015/095596

A. 主题的分类

G06F 21/60(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

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））

CPRS，VEN:安装，应用，解压，隐私，权限，

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 102426639 A (宇龙计算机通信科技深圳有限公司) 2012年 4月 25日 (2012 - 04 - 25) 说明书第2-3页	1-14
A	CN 103136472 A (腾讯科技深圳有限公司) 2013年 6月 5日 (2013 - 06 - 05) 全文	1-14

☐ 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
2016年 2月 22日	2016年 2月 26日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 王丹 电话号码 (86-10)62412062

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/CN2015/095596

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	102426639	A	2012年 4月 25日	CN	102426639	B	2015年 4月 8日
CN	103136472	A	2013年 6月 5日	US	2014013429	A1	2014年 1月 9日
				WO	2013079010	A1	2013年 6月 6日
				KR	20130135952	A	2013年 12月 11日