(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 5 月 21 日 (21.05.2015)

WIPO | PCT

(10) 国际公布号
WO 2015/070633 A1

(51) 国际专利分类号:
G06F 21/55 (2013.01) *G06F 21/60* (2013.01)

(21) 国际申请号: PCT/CN2014/082432

(22) 国际申请日: 2014 年 7 月 17 日 (17.07.2014)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201310575329.6 2013 年 11 月 15 日 (15.11.2013) 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: **胡中 (HU, Zhong)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。 **王鑫 (WANG, Xin)**; 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, LT, 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, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ,

[见续页]

(54) **Title**: PRIVACY AUTHORITY MANAGEMENT METHOD AND APPARATUS

(54) **发明名称** : 隐私权限管理方法和装置

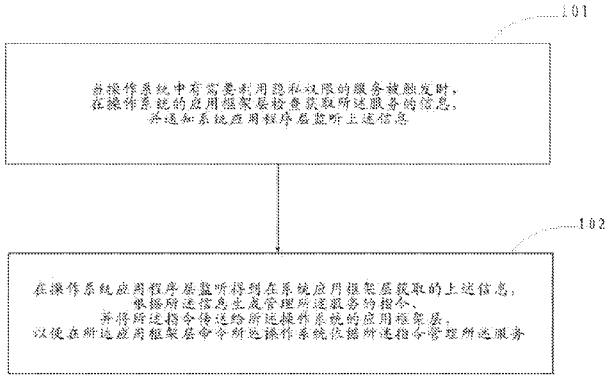

图 1 /Fig.1

101 When a service needing to use a privacy authority in an operating system is triggered, check and acquire information about the service at an application framework layer of the operating system, and instruct an application program layer of the system to listen to the information

102 Obtain, through listening at the application program layer of the operating system, the information acquired at the application framework layer of the system, generate, according to the information, an instruction used for managing the service, and transfer the instruction to the application framework layer of the operating system, so as to command, at the application framework layer, the operating system to manage the service according to the instruction

(57) **Abstract**: The present invention relates to a privacy authority management method, comprising: when a service needing to use a privacy authority in an operating system is triggered, checking and acquiring information about the service at an application framework layer of the operating system, and instructing an application program layer of the operating system to listen to the information; and after the application program layer of the operating system obtains through listening the information acquired at the application framework layer of the operating system, generating, according to the information, an instruction used for managing the service, and transferring the instruction to the application framework layer of the operating system, so as to command, at the application framework layer, the operating system to manage the service according to the instruction. This method solves a problem of a technical solution in which a user can manage a privacy authority of an operating system by using third-party security software without needing to crack an operating system of a user terminal to acquire the highest authority, thereby achieving beneficial effects of improving system security.

(57) **摘要**:

[见续页]

WO 2015/070633 A1

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))。

一种隐私权限管理方法，包括：当操作系统中有需要利用隐私权限的服务被触发时，在操作系统的应用框架层检查获取所述服务的信息，并通知操作系统应用程序层监听上述信息；在操作系统应用程序层监听得到在操作系统的应用框架层获取的上述信息后，根据所述信息生成管理所述服务的指令，并将所述指令传送给所述操作系统的应用框架层，以便在所述应用框架层命令所述操作系统依据所述指令管理所述服务。通过上述方法解决了不需要用户破解用户终端操作系统获取操作系统最高权限也能够使用第三方安全软件来管理操作系统的隐私权限的技术方案的问题，取得了提高系统安全性的有益效果。

隐私权限管理方法和装置

技术领域

本发明涉及信息处理技术领域，特别涉及一种隐私权限管理方法及装置。

背景技术

移动设备上的安全软件很多都有隐私权限管理功能，用户可以通过安全软件来控制设备上的其他应用访问系统中关键数据和实现某些行为权限，从而保护用户的隐私，比如读取通话记录、短信、发送短信、拨出电话，打开摄像头。

以android系统为例，现有的安全软件是通过进程注入的方式来实现隐私权限管理的。通过向android的servicemanager，phone等系统进程注入自己的动态库文件，在系统读取关键数据的接口中加入hook，调用安全软件的回调接口，根据用户的设置情况返回相应的结果，以决定是否要授权。只有获得授权，隐私数据访问接口才会继续原来的流程，否则直接忽略。

现有技术一个制约点就是安全软件的进程注入需要用户破解移动设备以获取root权限，但这对普通的用户是非常困难的，而且设备一旦被root，就增加了被恶意应用获取到高权限侵害系统的风险。另外目前国内的智能移动设备产商的售后服务都是不包含把已经破解获取到root的设备排除在外的，因此获取root权限之后该移动设备的售后服务也成为一个问题。

另外android设备产商众多，各家多少都会对系统本身有修改，所以现有技术方式在某些设备上存在适配的问题。

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或者减缓上述问题的隐私权限管理方法及装置。

依据本发明的一个方面，提供一种隐私权限管理方法，包括：当操作系统中有需要利用隐私权限的服务被触发时，在操作系统的应用框架层检查获取所述服务的信息，并通知操作系统应用程序层监听上述信息；在操作系统应用程序层监听得到在操作系统的应用框架层获取的上述信息后，根据所述信息生成管理所述服务的指令，并将所述指令传送给所述操作系统的应用框架层，以便在所述应用框架层命令所述操作系统依据所述指令管理所述服务。

根据本发明的另一个方面，提供一种隐私权限管理装置，包括：隐私服务检查单元，适于当操作系统中有需要利用隐私权限的服务被触发时，在操作系统的应用框架层检查获取所述服务的信息，并通知操作系统应用程序层监听上

述信息；安全软件单元，适于在操作系统应用程序层监听得到在操作系统的应用框架层获取的上述信息后，根据所述信息生成管理所述服务的指令，并将所述指令传送给所述操作系统的应用框架层，以便在所述应用框架层命令所述操作系统依据所述指令管理所述服务。

根据本发明的方法和装置，利用在操作系统的应用框架层的进程获得所述服务信息并将所述信息传送给系统应用程序层的应用，由于所述操作系统的应用框架层的应用本身就具备操作系统最高权限，因而不需要破解系统就能够在操作系统的应用框架层获取所述利用系统隐私的服务的信息。通过通知和监听的方式实现信息和安全软件指令在操作系统应用程序层和操作系统的应用框架层之间的通信，从而使得系统应用程序层的应用也可以利用正常权限来获取信息从而做出安全策略。由此解决了不需要用户破解用户终端操作系统获取操作系统最高权限也能够使用第三方安全软件来管理操作系统的隐私权限的技术方案的问题，取得了提高系统安全性的有益效果。

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。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示出了根据本发明隐私权限管理方法的步骤流程图；

图2示出了根据本发明隐私权限管理装置的结构图

图3示出了用于执行根据本发明的方法的智能电子设备的框图；

以及，

图4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。

参照图1，示出了根据本发明一个实施例的一种隐私权限管理方法实施例1的步骤流程图，在本实施例中，以安装有Android 系统的智能终端为例，对本发明的原理进行示例性描述，然而此描述仅仅是示例性的，本发明的范围并不限于此，本发明的原理也可以适用于安装有其它操作系统（例如Linux、iOS、Windows Phone、Symbian 等）的智能终端，

本实施例的方法具体可以包括以下步骤:

步骤101 ：当操作系统中有需要利用隐私权限的服务被触发时，在操作系统的应用框架层检查获取所述服务的信息，并通知系统应用程序层监听上述信息。

对于智能终端的操作系统而言，其应用程序通常分为应用框架层和应用程序层，参见图2。以android系统为例，系统框架层的某些信息在现有技术情况下不能被应用程序层得到。例如，现有技术中的android系统，其系统框架层中关于利用隐私权限的服务的信息不能被应用程序层面的软件获取，即不能被第三方软件比如第三方安全软件获取。因此当系统中有服务被触发时第三方软件不通过提权的方式不能够对该信息发送过程进行管理。提权的方式例如root、“越狱”等。

本发明中对操作系统的应用框架层中对需要利用隐私权限的服务过程进行改进，当操作系统中有需要利用隐私权限的服务被触发时，在操作系统的应用框架层对所述被触发的服务进行检查并获取该服务的信息。

以系统中有短信要发送时为例，现有的操作操作系统的应用框架层在系统有需要发短信的服务被触发时会通过IccSmsInterfacemanager类中的sendText()和sendMultipartText()方法获得所述发送短信服务的信息。

然而IccSmsInterfacemanager类中并没有方法将上述内容传输给系统应用程序层，因而并不能通过现有的android操作系统的应用框架层的程序来讲所述发短信服务的内容传送给系统应用程序层。

本发明通过在操作系统的应用框架层设置检查程序来实现读取并向操作系统的应用程序层传输所述服务的信息。由于该检查程序就位于操作系统的应用框架层的进程中，因而本身就具有该权限，即获取操作系统的应用框架层的需要利用隐私权限的服务的信息的权限。

在本发明中，当系统的应用框架层中有需要隐私权限的服务被触发时，并不直接进入到提供该服务或者不提供该服务的步骤，而是首先由在操作系统的应用框架层设置的检查程序对所述服务进行检查并获取该服务的信息。检查程序可以通过在android 系统中添加一个名为SecurityService的系统服务，来进行实际系统的隐私权限管理，所述的SecurityService服务中可以采用

checkPrivilege()的方法实现上述功能。

同时由于android系统中在有需要利用隐私权限的服务被触发时，IccSmsInterfacemanager类中的sendText()和sendMultipartText()方法已经获得了所述服务的信息，因此上述检查程序仅仅需要从IccSmsInterfacemanager类中读取上述信息即可。

根据本发明的另一个示例，当系统中有打电话的服务被触发时，同样可以通过在android 系统中的SecurityService的系统服务，来进行实际系统的隐私权限管理，所述的SecurityService服务中可以采用checkPrivilege()的方法检查所述打电话服务的相关信息。

除了本发明上述列举的发短信、打电话服务之外，系统中的其他服务例如获取手机号、读取通话记录、读取短信、写通话记录、写通信录、读取精确地里位置、读取粗略地里位置、录音、打开摄像头、打开wifi开关、打开蓝牙开关、读取已安装应用列表、获取设备ID、以及其他可能涉及到隐私数据的服务都是可以通过设置上述检查程序的方式检查读取上述服务的信息。

该信息优选地包括请求所述需要利用隐私权限的服务的应用的信息以及所述服务的具体内容。当然可以理解的是，所述检查程序也可以获取操作操作系统的应用框架层中所有与该服务相关的内容。获取不同的内容为安全软件设置具体的处理规则提供了基础。

由于该检查程序位于系统的应用框架层，参见图2，本身就具备了获取操作系统的应用框架层信息的权限，因此它不需要用户通过提权就可以获取系统中关于需要利用隐私权限的服务的信息。

优选地，该检查程序对系统中所有触发的需要利用隐私权限的服务都进行检查，这些服务包括但不仅限于：拨打电话、发送短信、获取手机号、读取通话记录、读取短信、写通话记录、写通信录、读取精确地里位置、读取粗略地里位置、录音、打开摄像头、打开wifi开关、打开蓝牙开关、读取已安装应用列表、获取设备ID、以及其他可能涉及到隐私数据的接口。这样对于系统中所有涉及隐私权限的服务都可以进行监控，这样提高了安全性。

当然，也可以设置一些检查规则，仅仅对该规则范围内的某些应用进行检查。比如，对于精确地理位置进行检查而对粗略地理位置不进行检查。即，对于隐私层级高的服务进行检查而不对隐私层级低的服务进行检查。这样可以在保证用户隐私安全的前提下对提升检查效率和用户体验。

所述检查程序检查被触发的所述服务并获取该服务的信息后，通知操作系统应用程序层接收所述信息。具体而言，通知的方式可以通过通知函数来实现。即，设置监听单元，并在监听单元中设置一个通知函数，当所述检查程序检查

并获取所述服务的信息后，所述检查程序就会调用该通知函数，通知系统的应用程序层进行监听以获得上述信息。通知函数位于系统应用程序层，参见图2，如此来实现将所述检查程序检查到的所述服务的信息传送出操作系统的应用框架层。

接着进入步骤102，在操作系统应用程序层监听得到在系统应用框架层获取的上述信息，根据所述信息生成管理所述服务的指令，并将所述指令传送给所述操作系统的应用框架层，以便在所述应用框架层命令所述操作系统依据所述指令管理所述服务。

监听过程可以通过在操作系统应用程序层设置一个QihooPrivilegeListener的接口，所述接口采用boolean CheckPrivilege(String packageName, int uid, int pid, int privilege, Bundle info)方法，来实现将在操作系统应用程序层中获取上述服务的相关信息。在检查程序检查读取需要利用隐私权限的服务的上述信息后，调用监听器中的上述函数，以将所述信息传送给系统应用程序层的安全软件。

可以通过向系统中注册隐私权限服务监听器的方式来设置上述监听器。

具体而言，可以设置一个隐私权限服务控制类，如QihooAppManager类，在所述类中采用：

setPrivilegeListener(QihooPrivilegeListener listener)方法

来实现向系统中注册隐私权限服务监听器。上述监听器包括通知函数，操作系统应用程序层的安全软件向操作系统注册了上述隐私权限服务监听器之后，操作系统的应用框架层的检查程序就能够在获取该隐私权限服务的信息后自动调用所述通知函数通知安全软件，进而通知操作系统应用程序层监听所述信息。

由此可见，通过设置上述监听程序的方式就能够实现将操作系统的应用框架层的信息传送至系统应用程序层，因而在操作系统应用程序层的安全软件就不需要提权也能够监听到操作系统的应用框架层的上述信息。

通过上述方式的设置还能够方便快捷地将数据传送给安全软件，当系统没有隐私权限服务被触发时，监听不必启动从而不会占用系统资源，而当系统中有需要利用隐私权限的服务被触发时，即能够监听获取该隐私权限服务的信息。

同时，采用这种调用和监听的方式使得操作系统的应用框架层的检查程序只能通过特定的监听器通信，这样避免了操作系统的应用框架层信息的泄露，提高了信息的安全性，其它恶意软件就不能够利用隐私权限服务的信息从而对用户造成威胁。

进一步地，安全软件和监听程序之间的通信规则也可以被设定成监听程序仅仅与预先设定的安全软件进行通信，这样就可以避免恶意软件伪装成安全软件来利用隐私权限服务信息从而造成信息泄露。

当安全软件接收到所隐私权限服务的信息后即可根据所述信息进行相关的安全处理。

例如，本发明的一个优选的实施例中，智能终端中的安全软件可以分析所述信息中关于触发该隐私权限服务的应用，当检测到恶意应用触发上述服务时，拒绝所述服务，并发送提示消息提醒用户。

另一方面，对于android系统自带的系统应用触发的系统隐私权限服务，例如android系统触发的打电话、发短信、开启wifi开关等应用，则自动允许提供所述服务，由于上述功能是用户非常用的功能，并且通常通过系统自带的应用触发上述服务不具有恶意特征，因此通过上述手段能够减少对用户的正常使用移动终端设备的打扰，提高用户体验。

根据本发明的另一个方面，当所述服务既不是安全软件识别的恶意应用发出的，也不是系统自带应用发出的情况下，安全软件可以弹出对话框栏通知用户对是否允许提供所述服务进行选择，根据用户的选择来生成管理该隐私权限服务的命令。

通过这种方式，用户可以主动选择对隐私数据进行访问的授权，避免隐私信息被而已软件窃取或者后台自动调取该服务造成隐私的泄露和/或资费的损失。

当然，安全软件可以在接收到上述服务的信息后，不判断其是否是恶意程序发出的，而是将上述信息呈现给用户，进而引导用户进行隐私权限服务的管理，这种提示的方式可以采用弹窗的方式提出，也可以选择在用户调取安全软件的隐私权限管理功能时根据用户的选择弹出。用户根据所述服务的信息做出是否允许所述隐私权限服务的指示后，安全软件根据用户的上述指示生成是否允许操作系统的应用框架层提供上述服务。

生成所述指令之后，将所述指令传送给所述操作系统的应用框架层，以便在所述应用框架层命令所述操作系统依据所述指令管理需要使用隐私权限的服务。所述指令传送至操作系统的方式包括多种，即采用任何适于在操作系统内传输信息的方式均可。

本发明优选的实施例中采用的传输方式如下，当所述指令生成后，通过监听器的通知函数将所述指令的内容返回给所述检查程序。

如前文所述，通过设置上述监听器的方式能够方便快捷地将数据回传至检查程序，同时，可以设置所述监听器仅与特定的安全软件通信。这样其它恶意

应用就不能够伪造指令以对用户造成威胁。

需要说明的是，上述指令返回给操作系统的应用框架层的步骤中，可以不设置由检查程序来接收上述指令，替代的是通过另外的判断模块来接收，判断模块接收上述指令之后控制操作系统的应用框架层来允许或禁止所述需要隐私权限的服务。

在完成上述操作后，在操作系统的应用框架层执行所述指令。当所述安全软件所发出的指令为允许该服务时，系统执行该指令提供上述服务，当所述安全软件所发出的指令为不提供上述服务时，系统执行述指令禁止该服务。参见图2。

一种优选的方式是，安全软件通过返回值的形式返回上述指令，即true表示允许上述服务的操作，false表示拒绝上述服务的操作，所述指令通过检查程序传送至服务执行单元，当时所述指令为true时所述服务执行单元即执行所述服务，当时所述指令为false时所述指令服务单元不启动，从而不执行上述服务。

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隐私权限管理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3示出了可以实现根据本发明的隐私权限管理方法的智能电子设备。该智能电子设备传统上包括处理器410和以存储器420形式的计算机程序产品或者计算机可读介质。存储器420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420具有用于执行上述方法中的任何方法步骤的程序代码431的存储空间430。例如，用于程序代码的存储空间430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431。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4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3的智能电子设备中的存储器420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431’，即可以由例如诸如410之类的处理器读取的代码，这些代码当由智能电子设备运行时，导致该智能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。

本发明公开了A1.一种隐私权限管理方法，包括:

当操作系统中有需要利用隐私权限的服务被触发时，在操作系统的应用框架层检查获取所述服务的信息，并通知操作系统应用程序层监听上述信息;

在操作系统应用程序层监听得到在操作系统的应用框架层获取的上述信息后，根据所述信息生成管理所述服务的指令，并将所述指令传送给所述操作系统的应用框架层，以便在所述应用框架层命令所述操作系统依据所述指令管理所述服务。

A2.如A1所述的方法，其特征在于，在操作系统的应用框架层对所述服务进行检查包括: 对系统中所有触发的需要利用隐私权限的服务都进行检查。

A3. 如A1所述的方法，其特征在于，所述需要利用隐私权限的服务包括:拨打电话、发送短信、获取手机号、读取通话记录、读取短信、写通话记录、写通信录、读取精确地里位置、读取粗略地里位置、录音、打开摄像头、打开wifi开关、打开蓝牙开关、读取已安装应用列表和获取设备ID中的一种或多种。

A4. 如A1-A3中任一项所述的方法，其特征在于，在操作系统应用程序层

监听得到在操作系统的应用框架层获取的上述信息包括包括：通过调用在操作系统应用程序层的通知函数使得操作系统的应用框架层与操作系统应用程序层进行通信，以在操作系统应用程序层监听所述信息；

将所述指令传送给所述操作系统的应用框架层包括，通过调用所述通知函数使操作系统应用程序层与操作系统的应用框架层进行通信，以将监听到的所述指令返回给操作系统的应用框架层。

A5. 如A1所述的方法，其特征在于，所述信息包括触发所述需要利用隐私权限的服务的应用的信息和/或该服务自身的内容。

A6. 如A1或A5所述的方法，其特征在于，根据所述信息生成管理所述服务的指令包括：通过预先设定的规则分析上述相关内容，并自动生成是否允许允许提供该服务的指令，其中所述规则可被用户设定和/或更新。

A7. 如A1或A5所述的方法，根据所述信息生成管理所述服务的指令包括：分析触发所述需要利用隐私权限的服务的应用的信息，当检测到所述服务的恶意应用触发时，禁止提供所述服务；当检测到是授信的应用触发的上述服务时，允许提供所述服务。

A8. 如A1或A5所述的方法，其特征在于，根据所述信息生成管理所述服务的指令包括：将所述信息呈现给用户，允许用户根据信息内容做出选择是否提供该服务，并依据用户的所述选择生成是否提供该服务的指令。

B9. 一种隐私权限管理装置，包括：

隐私服务检查单元，适于当操作系统中有需要利用隐私权限的服务被触发时，在操作系统的应用框架层检查获取所述服务的信息，并通知操作系统应用程序层监听上述信息；

安全软件单元，适于在操作系统应用程序层监听得到在操作系统的应用框架层获取的上述信息后，根据所述信息生成管理所述服务的指令，并将所述指令传送给所述操作系统的应用框架层，以便在所述应用框架层命令所述操作系统依据所述指令管理所述服务。

B10. 如B9所述的装置，其特征在于，在操作系统的应用框架层对所述服务进行检查包括：对系统中所有触发的需要利用隐私权限的服务都进行检查。

B11. 如B9所述的装置，其特征在于，需要利用隐私权限的服务包括：拨打电话、发送短信、获取手机号、读取通话记录、读取短信、写通话记录、写通信录、读取精确地里位置、读取粗略地里位置、录音、打开摄像头、打开wifi开关、打开蓝牙开关、读取已安装应用列表和获取设备ID中的一种或多种。

B12. 如B9-B11中任一项所述的装置，其特征在于，在操作系统应用程序层监听得到在操作系统的应用框架层获取的上述信息，包括通过调用在操作系

统应用程序层的通知函数使得操作系统的应用框架层与操作系统应用程序层进行通信，以在操作系统应用程序层监听所述相关信息，

将所述指令传送给所述操作系统的应用框架层包括，通过调用所述通知函数使操作系统应用程序层与操作系统的应用框架层进行通信，以将监听到的所述指令返回给操作系统的应用框架层。

B13. 如B9所述的装置，其特征在于，所述信息包括触发所述需要利用隐私权限的服务的应用的信息和/或该服务自身的内容。

B14. 如B9或B13所述的装置，其特征在于，根据所述信息生成管理所述服务的指令包括：通过预先设定的规则分析上述相关内容，并自动生成是否允许提供该服务的指令，其中所述规则可被用户设定和/或更新。

B15. 如B9或B13所述的装置，根据所述信息生成管理所述服务的指令包括：分析触发所述需要利用隐私权限的服务的应用的信息，当检测到所述服务恶意应用触发的时，禁止提供所述服务；当检测到是授信的应用触发的上述服务时，允许提供所述服务。

B16. 如B9或B13所述的装置，其特征在于，根据所述信息生成管理所述服务的指令包括：将所述信息呈现给用户，允许用户根据信息内容做出选择是否提供该服务，并依据用户的所述选择生成是否提供该服务的指令。

权 利 要 求

1. 一种隐私权限管理方法，包括:

当操作系统中有需要利用隐私权限的服务被触发时，在操作系统的应用框架层检查获取所述服务的信息，并通知操作系统应用程序层监听上述信息;

在操作系统应用程序层监听得到在操作系统的应用框架层获取的上述信息后，根据所述信息生成管理所述服务的指令，并将所述指令传送给所述操作系统的应用框架层，以便在所述应用框架层命令所述操作系统依据所述指令管理所述服务。

2. 根据权利要求1所述的方法，其特征在于，在操作系统的应用框架层对所述服务进行检查包括: 对系统中所有触发的需要利用隐私权限的服务都进行检查。

3. 根据权利要求1所述的方法，其特征在于，所述需要利用隐私权限的服务包括: 拨打电话、发送短信、获取手机号、读取通话记录、读取短信、写通话记录、写通信录、读取精确地里位置、读取粗略地里位置、录音、打开摄像头、打开wifi开关、打开蓝牙开关、读取已安装应用列表和获取设备ID中的一种或多种。

4. 根据权利要求1-3中任一项所述的方法，其特征在于，在操作系统应用程序层监听得到在操作系统的应用框架层获取的上述信息包括，包括: 通过调用在操作系统应用程序层的通知函数使得操作系统的应用框架层与操作系统应用程序层进行通信，以在操作系统应用程序层监听所述信息;

将所述指令传送给所述操作系统的应用框架层包括，通过调用所述通知函数使系统应用程序层与操作系统的应用框架层进行通信，以将监听到的所述指令返回给操作系统的应用框架层。

5. 根据权利要求1所述的方法，其特征在于，所述信息包括触发所述需要利用隐私权限的服务的应用的信息和/或该服务自身的内容。

6. 根据权利要求1或5所述的方法，其特征在于，根据所述信息生成管理所述服务的指令包括: 通过预先设定的规则分析上述相关内容，并自动生成是否允许允许提供该服务的指令，其中所述规则可被用户设定和/或更新。

7. 根据权利要求1或5所述的方法，根据所述信息生成管理所述服务的指令包括: 分析触发所述需要利用隐私权限的服务的应用的信息，当检测到所述服务的恶意应用触发时，禁止提供所述服务; 当检测到是授信的应用触发的上述服务时，允许提供所述服务。

8. 根据权利要求1或5所述的方法，其特征在于，根据所述信息生成管理所述服务的指令包括: 将所述信息呈现给用户，允许用户根据信息内容做出选择

是否提供该服务，并依据用户的所述选择生成是否提供该服务的指令。

9. 一种隐私权限管理装置，包括:

隐私服务检查单元，适于当操作系统中有需要利用隐私权限的服务被触发时，在操作系统的应用框架层检查获取所述服务的信息，并通知操作系统应用程序层监听上述信息;

安全软件单元，适于在操作系统应用程序层监听得到在操作系统的应用框架层获取的上述信息后，根据所述信息生成管理所述服务的指令，并将所述指令传送给所述操作系统的应用框架层，以便在所述应用框架层命令所述操作系统依据所述指令管理所述服务。

10. 根据权利要求9所述的装置，其特征在于，在操作系统的应用框架层对所述服务进行检查包括: 对系统中所有触发的需要利用隐私权限的服务都进行检查。

11. 根据权利要求9所述的装置，其特征在于，需要利用隐私权限的服务包括: 拨打电话、发送短信、获取手机号、读取通话记录、读取短信、写通话记录、写通信录、读取精确地里位置、读取粗略地里位置、录音、打开摄像头、打开wifi开关、打开蓝牙开关、读取已安装应用列表和获取设备ID中的一种或多种。

12. 根据权利要求9-11中任一项所述的装置，其特征在于，在操作系统应用程序层监听得到在操作系统的应用框架层获取的上述信息，包括通过调用在操作系统应用程序层的通知函数使得操作系统的应用框架层与操作系统应用程序层进行通信，以在操作系统应用程序层监听所述相关信息，

将所述指令传送给所述操作系统的应用框架层包括，通过调用所述通知函数使系统应用程序层与操作系统的应用框架层进行通信，以将监听到的所述指令返回给操作系统的应用框架层。

13. 根据权利要求9所述的装置，其特征在于，所述信息包括触发所述需要利用隐私权限的服务的应用的信息和/或该服务自身的内容。

14. 根据权利要求9或13所述的装置，其特征在于，根据所述信息生成管理所述服务的指令包括: 通过预先设定的规则分析上述相关内容，并自动生成是否允许提供该服务的指令，其中所述规则可被用户设定和/或更新。

15. 根据权利要求9或13所述的装置，根据所述信息生成管理所述服务的指令包括: 分析触发所述需要利用隐私权限的服务的应用的信息，当检测到所述服务恶意应用触发的时，禁止提供所述服务; 当检测到是授信的应用触发的上述服务时，允许提供所述服务。

16. 根据权利要求9或13所述的装置，其特征在于，根据所述信息生成管理

所述服务的指令包括：将所述信息呈现给用户，允许用户根据信息内容做出选择是否提供该服务，并依据用户的所述选择生成是否提供该服务的指令。

17、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服务器上运行时，导致所述服务器执行根据权利要求1-8中的任一个所述的屏幕图像的截取方法。

18、一种计算机可读介质，其中存储了如权利要求17所述的计算机程序。

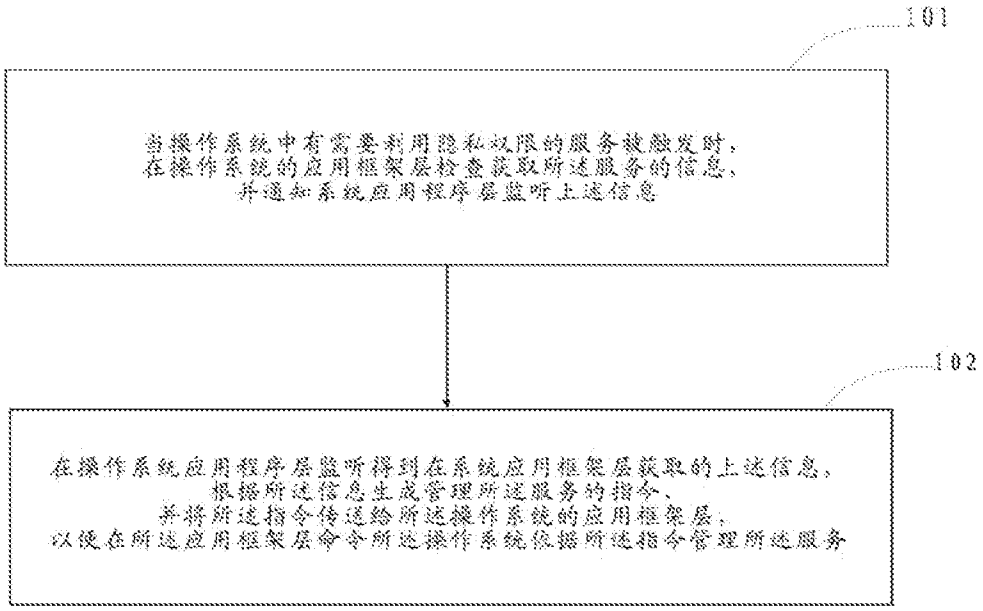
101
当操作系统中有需要利用隐私权限的服务被触发时，
在操作系统的应用框架层检查获取所述服务的信息，
并通知系统应用程序层监听上述信息
102
在操作系统应用程序层监听得到在系统应用框架层获取的上述信息，
根据所述信息生成管理所述服务的指令，
并将所述指令传送给所述操作系统的应用框架层，
以使在所述应用框架层命令所述操作系统依据所述指令管理所述服务

图 1

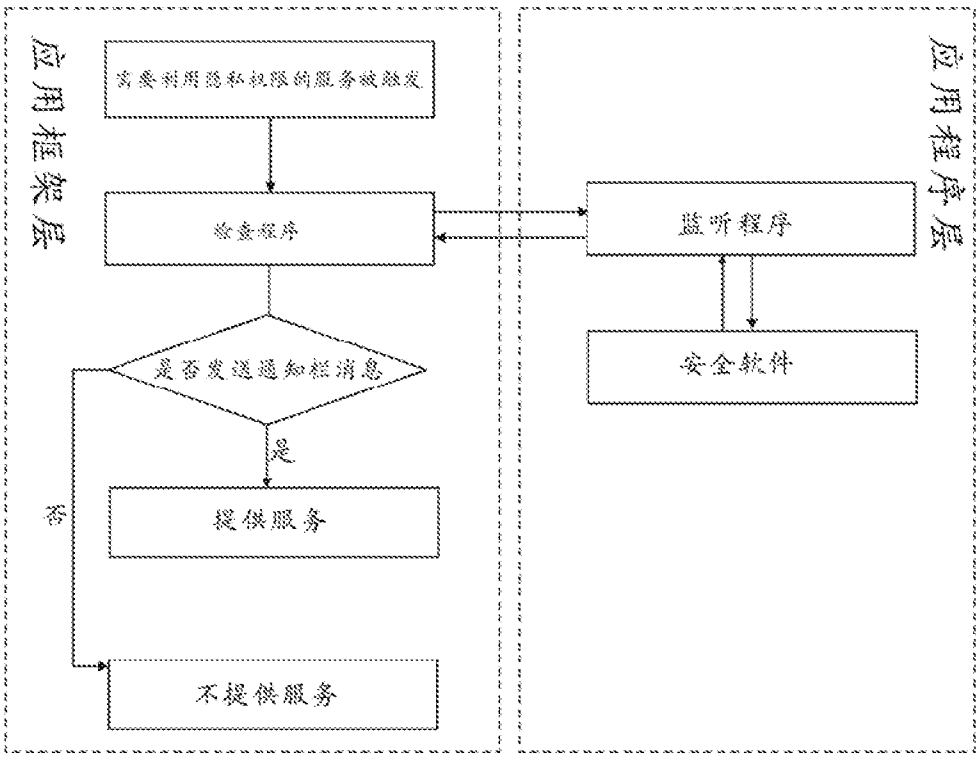
应用框架层
需要利用隐私权限的服务被触发
检查程序
是否发送通知栏消息
是
否
提供服务
不提供服务
应用程序层
监听程序
安全软件

图 2

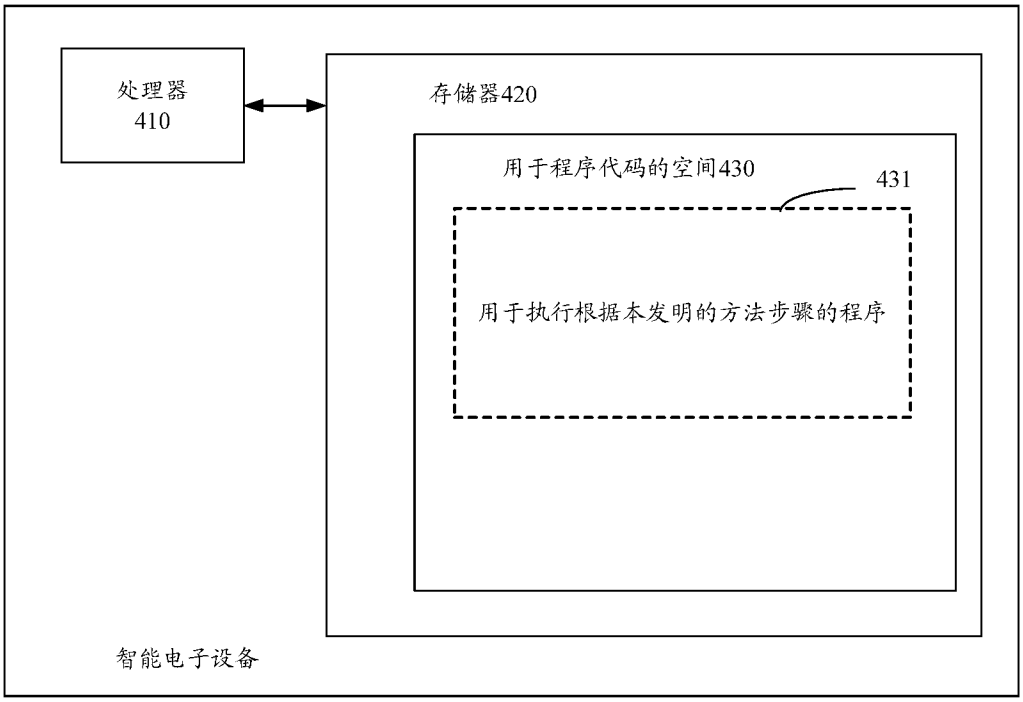
处理器
410
存储器420
用于程序代码的空间430
431
用于执行根据本发明的方法步骤的程序
智能电子设备

图 3

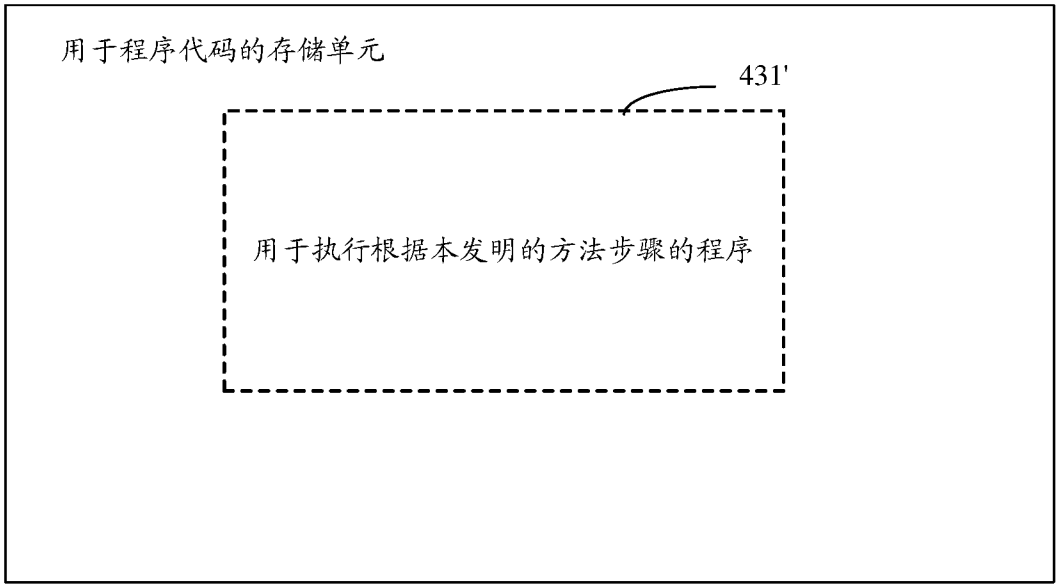
用于程序代码的存储单元
431'
用于执行根据本发明的方法步骤的程序

图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2014/082432

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/55 (2013.01) i; 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; H04L; H04M

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, WPI, EPODOC, CNKI, GOOGLE: transmission, authority, application layer, framework layer, provide, send, return, notify, notification, command, operation system, OS, private, privacy, right, android

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 103577750 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 12 February 2014 (12.02.2014), claims 1-16, and description, paragraph [0075]	1-18
PX	CN 103577749 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 12 February 2014 (12.02.2014), claims 1-10	1-18
PX	CN 103619003 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 05 March 2014 (05.03.2014), claims 1-10	1-18
PX	CN 103577757 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 12 February 2014 (12.02.2014), claims 1-10	1-18
A	CN 102355519 A (BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS), 15 February 2012 (15.02.2012), the whole document	1-18
A	US 2005286457 A1 (FOSTER, D.J. et al.), 29 December 2005 (29.12.2005), the whole document	1-18

☐ 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
25 September 2014 (25.09.2014)	**20 October 2014 (20.10.2014)**
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 **LUO, Xiao** Telephone No.: (86-10) **82245577**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2014/082432

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103577750 A	12 February 2014	None	
CN 103577749 A	12 February 2014	None	
CN 103619003 A	05 March 2014	None	
CN 103577757 A	12 February 2014	None	
CN 102355519 A	15 February 2012	None	
US 2005286457 A1	29 December 2005	US 2005289479 A1	29 December 2005
		US 2005288001 A1	29 December 2005
		US 2014033235 A1	30 January 2014

国际检索报告

国际申请号
PCT/CN2014/082432

A. 主题的分类

G06F 21/55(2013.01)i; 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; H04L; H04M

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,WPI,EPODOC,CNKI,GOOGLE:应用程序层，应用层，框架层，提供，传送，发送，返回，通知，指令，命令，操作系统，权限，隐私，私密，安卓，application layer, framework layer, provide, send, return, notify, notification, command, operation system, OS, private,privacy,right, 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
PX	CN 103577750 A (北京奇虎科技有限公司等) 2014年 2月 12日 (2014-02-12) 权利要求1-16、说明书第[0075]段	1-18
PX	CN 103577749 A (北京奇虎科技有限公司等) 2014年 2月 12日 (2014-02-12) 权利要求1-10	1-18
PX	CN 103619003 A (北京奇虎科技有限公司等) 2014年 3月 05日 (2014-03-05) 权利要求1-10	1-18
PX	CN 103577757 A (北京奇虎科技有限公司等) 2014年 2月 12日 (2014-02-12) 权利要求1-10	1-18
A	CN 102355519 A (北京邮电大学) 2012年 2月 15日 (2012-02-15) 全文	1-18
A	US 2005286457 A1 (FOSTER, DEREK JOHN等) 2005年 12月 29日 (2005-12-29) 全文	1-18

☐ 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
2014年 9月 25日	2014年 10月 20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) 北京市海淀区蓟门桥西土城路6号 100088 中国 传真号 (86-10)62019451	受权官员 罗啸 电话号码 (86-10)82245577

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2014/082432

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	103577750	A	2014年 2月 12日	无			
CN	103577749	A	2014年 2月 12日	无			
CN	103619003	A	2014年 3月 05日	无			
CN	103577757	A	2014年 2月 12日	无			
CN	102355519	A	2012年 2月 15日	无			
US	2005286457	A1	2005年 12月 29日	US	2005289479	A1	2005年 12月 29日
				US	2005288001	A1	2005年 12月 29日
				US	2014033235	A1	2014年 1月 30日