(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 8 月 4 日 (04.08.2016)

WIPO | PCT

(10) 国际公布号
WO 2016/119164 A1

(51) 国际专利分类号:
*H04W 88/02* (2009.01) *G06F 21/62* (2013.01)

(21) 国际申请号: PCT/CN2015/071818

(22) 国际申请日: 2015 年 1 月 29 日 (29.01.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 宇龙计算机通信科技(深圳)有限公司 (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。

(72) 发明人: 吕云飞 (LV, Yunfei); 中国广东省深圳市南山区坂田科技园北区梦溪道 2 号, Guangdong 518057 (CN)。 艾浩峰 (AI, Haofeng); 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。

(74) 代理人: 北京中博世达专利商标代理有限公司 (BEIJING ZBSD PATENT&TRADEMARK AGENT LTD.); 中国北京市海淀区交大东路 31 号 11 号楼 8 层, Beijing 100044 (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, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) Title: TERMINAL SECURITY MANAGEMENT METHOD AND APPARATUS

(54) 发明名称 : 一种终端安全的管理方法及装置

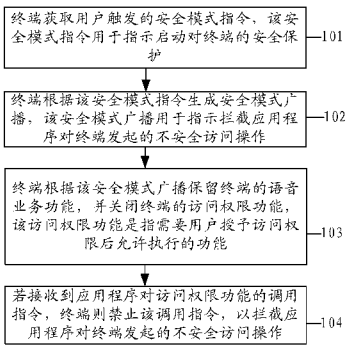


图 1

101 A TERMINAL ACQUIRING A SECURITY MODE INSTRUCTION TRIGGERED BY A USER, WHEREIN THE SECURITY MODE INSTRUCTION IS USED FOR INDICATING THE STARTING OF SECURITY PROTECTION FOR THE TERMINAL

102 THE TERMINAL GENERATING A SECURITY MODE BROADCAST ACCORDING TO THE SECURITY MODE INSTRUCTION, WHEREIN THE SECURITY MODE BROADCAST IS USED FOR INDICATING THE INTERCEPTION OF AN INSECURE ACCESS OPERATION INITIATED BY AN APPLICATION PROGRAM TO THE TERMINAL

103 THE TERMINAL RESERVING A VOICE SERVICE FUNCTION OF THE TERMINAL ACCORDING TO THE SECURITY MODE BROADCAST, AND DISABLING AN ACCESS PERMISSION FUNCTION OF THE TERMINAL, WHEREIN THE ACCESS PERMISSION FUNCTION REFERS TO A FUNCTION IN WHICH THE USER NEEDS TO BE GRANTED ACCESS PERMISSION AND IS THEN ALLOWED TO PERFORM EXECUTION

104 IF AN INVOKING INSTRUCTION OF THE APPLICATION PROGRAM FOR THE ACCESS PERMISSION FUNCTION IS RECEIVED, THE TERMINAL PROHIBITS THE INVOKING INSTRUCTION, SO AS TO INTERCEPT THE INSECURE ACCESS OPERATION INITIATED BY THE APPLICATION PROGRAM TO THE TERMINAL

(57) Abstract: Provided are a terminal security management method and apparatus, which relate to the field of communications, improve the security of a terminal during use, and avoid a security risk that may be brought about when a user uses the terminal. The solution includes: acquiring a security mode instruction triggered by a user, wherein the security mode instruction is used for indicating the starting of security protection for a terminal; generating a security mode broadcast according to the security mode instruction, wherein the security mode broadcast is used for indicating the interception of an insecure access operation initiated by an application program to the terminal; reserving a voice service function of the terminal according to the security mode broadcast, and disabling an access permission function of the terminal, wherein the access permission function refers to a function in which the user needs to be granted access permission and is then allowed to perform execution; and if an invoking instruction of the application program for the access permission function is received, prohibiting the invoking instruction, so as to intercept the insecure access operation initiated by the application program to the terminal.

(57) 摘要:

[见续页]

WO 2016/119164 A1

**本国际公布**:

— 包括国际检索报告(条约第 21 条(3))。

本发明的实施例提供一种终端安全的管理方法及装置，涉及通信领域，提高了终端在使用过程中的安全性，避免用户在使用终端时可能带来的安全隐患。该方案包括：获取用户触发的安全模式指令，该安全模式指令用于指示启动对终端的安全保护；根据安全模式指令生成安全模式广播，该安全模式广播用于指示拦截应用程序对终端发起的不安全访问操作；根据安全模式广播保留终端的语音业务功能，并关闭终端的访问权限功能，该访问权限功能是指需要用户授予访问权限后允许执行的功能；若接收到应用程序对访问权限功能的调用指令，则禁止调用指令，以拦截应用程序对终端发起的不安全访问操作。

# 一种终端安全的管理方法及装置

## 技术领域

本发明涉及通讯领域，尤其涉及一种终端安全的管理方法及装置。

## 背景技术

随着通信技术的飞速发展，尤其以手机为代表的智能终端的兴起，为人们的生活提供了极大地方便。用户可以通过在智能终端内安装各种类型的应用软件，以实现各种类型的应用功能。例如，用户在手机内成功安装地图 APP（Application，应用程序）之后，地图 APP 可以通过打开 GPS（Global Positioning System，全球定位系统）对用户当前的活动地点进行定位，以便于向用户提供线路搜索等服务。又或者，用户在手机内成功安装支付宝 APP 之后，就可以使用支付宝 APP 直接与银行进行转账支付等货币服务。

然而，这些应用软件在丰富用户的生活的同时，也容易对用户的各类信息和隐私带来巨大的安全隐患。例如，有的应用软件在应用时可能会涉及多向用户权限（例如获取用户通讯录信息，获取用户绑定的银行账户信息，获取用户的当前位置信息等），这些信息一旦被恶意非法软件获取，用户的隐私、人身以及财产安全将面临巨大危险。

因此，亟需一种终端安全的管理方法，以提高终端在使用过程中的安全性，避免用户在使用终端时可能带来的安全隐患。

## 发明内容

本发明的实施例提供一种终端安全的管理方法及装置，提高终端在使用过程中的安全性，避免用户在使用终端时可能带来的安全隐患。

为达到上述目的，本发明的实施例采用如下技术方案：

本发明实施例的第一方面，提供一种终端安全的管理方法，包

括：

获取用户触发的安全模式指令，所述安全模式指令用于指示启动对终端的安全保护；

根据所述安全模式指令生成安全模式广播，所述安全模式广播用于指示拦截应用程序对所述终端发起的不安全访问操作；

根据所述安全模式广播保留所述终端的语音业务功能，并关闭所述终端的访问权限功能，所述访问权限功能是指需要所述用户授予访问权限后允许执行的功能；

若接收到所述应用程序对所述访问权限功能的调用指令，则禁止所述调用指令，以拦截所述应用程序对所述终端发起的不安全访问操作。

结合第一方面，在第一方面的第一种可能的实现方式中，所述访问权限功能包括全球定位系统功能、数据业务功能、无线网络功能、相机功能以及录音功能中的至少一种；

其中，所述根据所述安全模式指令生成安全模式广播，包括：

获取用户选择的访问权限白名单，所述访问权限白名单中包含用户已授权访问的应用程序或者用户已授权访问的所述访问权限功能；

根据所述安全模式指令和所述访问权限白名单生成安全模式广播，所述安全模式广播用于指示拦截所述访问权限白名单之外的应用程序对所述终端发起的不安全访问操作。

结合第一方面的第一种可能的实现方式，在第一方面的第二种可能的实现方式中，所述根据所述安全模式广播保留所述终端的语音业务功能，并关闭所述终端的访问权限功能，包括：

根据所述安全模式广播保留所述终端的语音业务功能；

根据所述访问权限白名单关闭所述访问权限白名单之外的访问权限功能，其中，所述访问权限功能包括 GPS 功能、数据业务功能、无线网络功能、相机功能以及录音功能中的至少一种。

结合第一方面，在第一方面的第三种可能的实现方式中，所述

若接收到所述应用程序调用所述访问权限功能的调用指令，则禁止所述调用指令，包括：

若接收到所述应用程序调用所述访问权限功能的调用指令，则确定是否启动对所述终端的安全保护；

若已启动对所述终端的安全保护，则禁止所述调用指令，以拦截所述应用程序对所述终端发起的不安全访问操作。

结合第一方面，在第一方面的第四种可能的实现方式中，在所述根据所述安全模式指令生成安全模式广播之后，还包括：

记录所述终端当前的访问权限功能的使用状态；

其中，在所述若接收到所述应用程序调用所述访问权限功能的调用指令，则禁止所述调用指令之后，还包括：

若接收到用户触发的退出指令，则将所述访问权限功能恢复至已记录的所述访问权限功能的使用状态，以退出所述安全模式。

本发明实施例的第二方面，还提供一种终端，包括：

获取单元，用于获取用户触发的安全模式指令，所述安全模式指令用于指示启动对终端的安全保护；

广播生成单元，用于根据所述获取单元中所述安全模式指令生成安全模式广播，所述安全模式广播用于指示拦截应用程序对所述终端发起的不安全访问操作；

安全模式切换单元，用于根据所述广播生成单元中所述安全模式广播保留所述终端的语音业务功能，并关闭所述终端的访问权限功能，所述访问权限功能是指需要所述用户授予访问权限后允许执行的功能；

拦截单元，用于若接收到所述应用程序对所述访问权限功能的调用指令，则禁止所述调用指令，以拦截所述应用程序对所述终端发起的不安全访问操作。

结合第二方面，在第二方面的第一种可能的实现方式中，

所述广播生成单元，具体用于获取用户选择的访问权限白名单，所述访问权限白名单中包含用户已授权访问的应用程序或者用户已

授权访问的所述访问权限功能；根据所述安全模式指令和所述访问权限白名单生成安全模式广播，所述安全模式广播用于指示拦截所述访问权限白名单之外的应用程序对所述终端发起的不安全访问操作；

其中，所述访问权限功能包括全球定位系统功能、数据业务功能、无线网络功能、相机功能以及录音功能中的至少一种。

结合第第二方面的第一种可能的实现方式，在第二方面的第二种可能的实现方式中，

所述安全模式切换单元，具体用于根据所述安全模式广播保留所述终端的语音业务功能；根据所述访问权限白名单关闭所述访问权限白名单之外的访问权限功能，其中，所述访问权限功能包括 GPS 功能、数据业务功能、无线网络功能、相机功能以及录音功能中的至少一种。

结合第二方面，在第二方面的第三种可能的实现方式中，

所述拦截单元，具体用于若接收到所述应用程序调用所述访问权限功能的调用指令，则确定是否启动对所述终端的安全保护；若已启动对所述终端的安全保护，则禁止所述调用指令，以拦截所述应用程序对所述终端发起的不安全访问操作。

结合第二方面，在第二方面的第四种可能的实现方式中，所述终端还包括记录单元，其中，

所述记录单元，用于记录所述终端当前的访问权限功能的使用状态；

所述安全模式切换单元，还用于若接收到用户触发的退出指令，则将所述访问权限功能恢复至所述记录单元中已记录的所述访问权限功能的使用状态，以退出所述安全模式。

本发明的实施例提供一种终端安全的管理方法及装置，通过获取用户触发的安全模式指令生成安全模式广播，以使得终端内的各个功能模块根据安全模式广播保留终端的语音业务功能，并关闭终端的访问权限功能，其中，该访问权限功能是指需要用户授予访问

权限后允许执行的功能；这样一来，终端可以成功切换到安全模式，一旦接收到应用程序对该访问权限功能的调用指令，终端就可以禁止所述调用指令，以拦截所述应用程序对所述终端发起的不安全访问操作，提高了终端在使用过程中的安全性，避免用户在使用终端时可能带来的安全隐患。

**附图说明**

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍。

图 1 为本发明实施例提供的一种终端安全的管理方法的流程示意图一；

图 2 为本发明实施例提供的一种终端界面的示意图；

图 3 为本发明实施例提供的一种终端安全的管理方法的流程示意图二；

图 4 为本发明实施例提供的一种终端的硬件示意图；

图 5 为本发明实施例提供的一种终端的结构示意图一；

图 6 为本发明实施例提供的一种终端的结构示意图二。

**具体实施方式**

下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。

**实施例 1**

本发明实施例提供一种终端安全的管理方法，如图 1 所示，包括：

101、终端获取用户触发的安全模式指令，该安全模式指令用于指示启动对终端的安全保护。

102、终端根据该安全模式指令生成安全模式广播，该安全模式广播用于指示拦截应用程序对终端发起的不安全访问操作。

103、终端根据该安全模式广播保留终端的语音业务功能，并关闭终端的访问权限功能，该访问权限功能是指需要用户授予访问权

限后允许执行的功能。

104、若接收到应用程序对访问权限功能的调用指令，终端则禁止该调用指令，以拦截应用程序对终端发起的不安全访问操作。

在步骤 101 中，用户在使用终端的过程中，终端可以获取由用户触发的安全模式指令，该安全模式指令用于指示启动对终端的安全保护。

具体的，如图 2 所示，可以在终端的情景模式中加入超级安全模式选项，当用户触发该超级安全模式选项后，终端生成安全模式指令，该安全模式指令用于指示启动对终端的安全保护，这样，终端便可以根据该安全模式指令开启超级安全模式来维护终端的安全。

在步骤 102 中，在终端获取到该安全模式指令之后，终端根据该安全模式指令生成安全模式广播，其中，该安全模式广播用于指示拦截应用程序对终端发起的不安全访问操作。

由于终端获取到的安全模式指令用于指示启动对终端的安全保护，因此，终端需要通知终端内的多个硬件设备（例如摄像头、GPS 以及蓝牙等）和/或功能模块（例如数据网络模块等）开启安全模式，以便于这些硬件设备和/或功能模块关闭应用程序对其自身的访问权限，进而对终端进行安全保护。此时，终端可以根据接收到的安全模式指令生成安全模式广播，并在终端内的各个硬件设备和/或功能模块中播放该安全模式广播，以指示各个硬件设备和/或功能模块拦截应用程序对终端发起的不安全访问操作。

其中，该安全模式广播的形式可以是多种多样的，例如，该安全模式广播可以仅仅包含通知各个硬件设备和/或功能模块关闭相应功能的指示信息，这样，各个硬件设备和/或功能模块接收到该安全模式广播后关闭自身的功能，又或者，该安全模式广播还可以按优先级分为一级安全模式广播，二级安全模式广播等，其中，一级安全模式广播可用于指示所有的硬件设备和功能模块均拦截应用程序对终端发起的不安全访问操作，而二级安全模式广播可用于指示

相对重要的一些硬件设备和/或功能模块（例如 GPS 或数据网络模块等）拦截应用程序对终端发起的不安全访问操作，这样一来，用户便可根据当前所需的安全等级调整对终端安全的维护。又或者，该安全模式广播还可以包含相应应用程序的标识，以指示硬件设备和/或功能模块对安全模式广播中包含的这些应用程序发起的不安全访问操作进行屏蔽等指定操作。

在步骤 103 中，在终端根据所述安全模式指令生成安全模式广播之后，终端便可以根据该安全模式广播保留终端的语音业务功能，并关闭终端的访问权限功能，其中，该访问权限功能是指需要用户授予访问权限后允许执行的功能，示例性的，该访问权限功能可以包括全球定位系统（GPS）功能、数据业务功能、无线网络功能、相机功能以及录音功能中的至少一种。

具体的，当 GPS 模块接收到该安全模式广播之后，便可以根据该安全模式广播关闭 GPS 功能；当 WIFI 模块接收到该安全模式广播之后，便可以根据该安全模式广播关闭无线网络功能；当数据网络模块接收到该安全模式广播之后，便可以根据该安全模式广播关闭数据业务功能；终端还可以调用相机接口禁用相机功能，调用音频 HAL（Hardware Abstraction Layer,硬件抽象层）接口禁用录音功能；同时，终端将当前终端正在使用的通信模式设置为仅提供语音服务的 CS(Circuit Switch，电路交换) only 模式，以保证用户的正常通讯功能。

需要说明的是，参见图 2，在本发明的实施例中，终端进入安全模式时可以与其他任何情景模式叠加使用，即当终端开启超级安全模式时可同时开启户外模式、标准模式、会议模式、静音模式以及飞行模式中的任一种情景模式。

在步骤 104 中，当终端执行完步骤 101 至 103 之后，终端便已经开启安全模式，此时，若终端接收到应用程序对访问权限功能的调用指令，终端则禁止该调用指令，以拦截应用程序对终端发起的不安全访问操作。

示例性的，终端在开启安全模式之后，由于终端已经关闭了 GPS 功能，因此，当用户使用百度地图等应用程序向终端发起 GPS 功能的调用指令时，为保护终端的使用安全，终端此时会禁止该调用指令，以拦截应用程序对终端发起的不安全访问操作。

本发明的实施例提供一种终端安全的管理方法，通过获取用户触发的安全模式指令生成安全模式广播，以使得终端内的各个功能模块根据安全模式广播保留终端的语音业务功能，并关闭终端的访问权限功能，其中，该访问权限功能包括是指需要用户授予访问权限后允许执行的功能；这样一来，终端可以成功切换到安全模式，一旦接收到应用程序对该访问权限功能的调用指令，终端就可以禁止所述调用指令，以拦截所述应用程序对所述终端发起的不安全访问操作，提高了终端在使用过程中的安全性，避免用户在使用终端时可能带来的安全隐患。

**实施例 2**

本发明实施例提供一种终端安全的管理方法，如图 3 所示，包括：

201、终端获取用户触发的安全模式指令，该安全模式指令用于指示启动对终端的安全保护。

202、终端获取用户选择的访问权限白名单，该访问权限白名单中包含用户已授权访问的应用程序或者用户已授权访问的访问权限功能，该访问权限功能包括 GPS 功能、数据业务功能、无线网络功能、相机功能以及录音功能中的至少一种。

203、终端根据安全模式指令和访问权限白名单生成安全模式广播，该安全模式广播用于指示拦截该访问权限白名单之外的应用程序对终端发起的不安全访问操作。

204、终端记录终端当前的访问权限功能的使用状态。

205、终端根据该安全模式广播保留终端的语音业务功能，并关闭终端的访问权限功能。

206、若接收到应用程序对访问权限功能的调用指令，终端则禁

止该调用指令，以拦截应用程序对终端发起的不安全访问操作。

207、若接收到用户触发的退出指令，则将访问权限功能恢复至步骤 204 中已记录的访问权限功能的使用状态，以退出所述安全模式。

在步骤 201 中，用户在使用终端的过程中，终端可以获取由用户触发的安全模式指令，该安全模式指令用于指示启动对终端的安全保护。

示例性的，如图 2 所示，可以在终端的情景模式中加入超级安全模式选项，当用户触发该超级安全模式选项后，终端生成安全模式指令，用于指示启动对终端的安全保护，这样，终端便可以根据该安全模式指令开启超级安全模式来维护终端的安全。

在步骤 202 中，在终端获取到该安全模式指令之后，终端可以获取用户选择的访问权限白名单，该访问权限白名单中包含用户已授权访问的应用程序或者用户已授权访问的访问权限功能，其中，该访问权限功能包括 GPS 功能、数据业务功能、无线网络功能、相机功能以及录音功能中的至少一种。

示例性的，在在终端获取到该安全模式指令之后，终端可以通过设有触控面板的显示设备输出相应输出界面，以提示用户从 GPS 功能、数据业务功能、无线网络功能、相机功能以及录音功能中选择一种或多种作为用户已授权访问的访问权限白名单，又或者，终端可以输出相应输出界面，以提示用户从多个应用程序中选择一种或多种作为用户已授权访问的访问权限白名单，以便于终端根据用户已授权访问的访问权限白名单选择性的拦截相关应用程序对终端发起的不安全访问操作。

在步骤 203 中，在终端获取到用户选择的访问权限白名单之后，终端根据安全模式指令和访问权限白名单生成安全模式广播，该安全模式广播用于指示拦截该访问权限白名单之外的应用程序对终端发起的不安全访问操作。

在终端获取到的安全模式指令后，启动对该终端的安全保护，

此时，终端需要通知终端内的多个硬件设备（例如摄像头、GPS 以及蓝牙等）和/或功能模块（例如数据网络模块等）开启安全模式，以便于这些硬件设备和/或功能模块关闭应用程序对其自身的访问权限，进而对终端进行安全保护。因此，终端可以根据获取到的安全模式指令和访问权限白名单生成安全模式广播，并在终端内的各个硬件设备和/或功能模块中播放该安全模式广播，以指示各个硬件设备和/或功能模块拦截应用程序对终端发起的不安全访问操作。

示例性的，可以在搭载安卓系统的手机中的各个硬件设备和/或功能模块中设置 Broadcast Receiver(广播接收器)，等待接收终端发起的安全模式广播，其中，广播接收器是为了实现终端广播而提供的一种组件。

其中，该安全模式广播的形式可以是多种多样的，具体可参见实施例 1 中步骤 102，故此处不再赘述。

在步骤 204 中，终端在执行步骤 203 的同时或者在执行完步骤 203 之后，还可以记录终端当前的访问权限功能的使用状态，也就是说，记录当前用户正在使用的 GPS 功能、数据业务功能、无线网络功能、相机功能以及录音功能的工作状态，例如 GPS 功能为打开或关闭状态，以便于终端在退出安全模式后及时将终端的访问权限功能恢复至用户打开安全模式之前的状态。

在步骤 205 中，终端根据所述安全模式指令生成安全模式广播之后，终端便可以根据该安全模式广播保留终端的语音业务功能，并关闭终端的访问权限功能，其中，该访问权限功能包括 GPS 功能、数据业务功能、无线网络功能、相机功能以及录音功能中的至少一种。

其中，终端根据该安全模式广播保留终端的语音业务功能，并关闭终端的访问权限功能的方法可参见实施例 1 中步骤 103，可以看出，由于该安全模式广播中包含用户确定的访问权限白名单的信息，因此，在关闭终端的访问权限功能时，终端可以根据用户确定的访问权限白名单关闭 GPS 功能、数据业务功能、无线网络功能、

相机功能以及录音功能中的至少一种，实现用户自定义的安全模式，在提高终端安全性的同时可实现用户对终端安全的自主管理。

在步骤 206 中，当终端执行完步骤 201 至 205 之后，终端便已经开启安全模式，此时，若终端接收到应用程序对访问权限功能的调用指令，终端则禁止该调用指令，以拦截应用程序对终端发起的不安全访问操作。

示例性的，终端在开启安全模式之后，由于终端已经关闭了 GPS 功能，因此，当用户使用百度地图等应用程序向终端发起 GPS 功能的调用指令时，为保护终端的使用安全，终端此时会禁止该调用指令，以拦截应用程序对终端发起的不安全访问操作。

在步骤 207 中，与步骤 206 对应的，当终端执行完步骤 201 至 205 之后，终端便已经开启安全模式，此时，若接收到用户触发的退出指令，则将访问权限功能恢复至步骤 204 中已记录的访问权限功能的使用状态，以退出所述安全模式。

本发明的实施例提供一种终端安全的管理方法，通过获取用户触发的安全模式指令生成安全模式广播，以使得终端内的各个功能模块根据安全模式广播保留终端的语音业务功能，并关闭终端的访问权限功能，其中，该访问权限功能是指需要用户授予访问权限后允许执行的功能；这样一来，终端可以成功切换到安全模式，一旦接收到应用程序对该访问权限功能的调用指令，终端就可以禁止所述调用指令，以拦截所述应用程序对所述终端发起的不安全访问操作，提高了终端在使用过程中的安全性，避免用户在使用终端时可能带来的安全隐患。

**实施例 3**

附图 4 示出的是本发明的终端的硬件示意图。

所述终端可以为手机、IPAD 等，例如，使用安卓系统的智能手机。

如图 4，所述终端包括处理器 11、通信接口 12、存储器 13、显示设备 14 以及总线 15。

其中，处理器 11、通讯接口 12、存储器 13 以及显示设备 14 通过总线 15 进行通信。

处理器 11，是所述终端的控制中心，处理器 11 通过对通讯接口 12 接收到的数据进行处理，并调用存储器 13 中的软件或程序，执行所述终端的各项功能。

通信接口 12，可以由光通讯接口，电通讯接口，无线通讯接口或其任意组合实现。例如，光通讯接口可以是小封装可插拔（英文：small form-factor pluggable transceiver，缩写：SFP）通讯接口（英文：transceiver），增强小封装可插拔（英文：enhanced small form-factor pluggable，缩写：SFP+）通讯接口或 10 吉比特小封装可插拔（英文：10 Gigabit small form-factor pluggable，缩写：XFP）通讯接口。电通讯接口可以是以太网（英文：Ethernet）网络接口控制器（英文：network interface controller，缩写：NIC）。无线通讯接口可以是无线网络接口控制器（英文：wireless network interface controller，缩写：WNIC）。终端中可以有多个通信接口 12。

存储器 13，可用于存储软件程序或数据，处理器 11 通过运行存储在存储器 13 的软件程序或数据，从而执行所述终端的各种功能应用以及数据处理。

显示设备 14，可用于显示由用户输入的信息或提供给用户的信息以及终端的各种菜单。显示设备 14 可包括显示面板，可选的，可以采用 LCD(Liquid Crystal Display，液晶显示器)、OLED(Organic Light-Emitting Diode,有机发光二极管)等形式来配置显示面板。进一步的，触控面板可覆盖显示面板，当触控面板检测到在其上或附近的触摸操作后，传送给处理器 11 以确定触摸事件的类型，随后处理器 11 根据触摸事件的类型在显示面板上提供相应的视觉输出。

在本发明的实施例中，处理器 11 通过显示设备 14 获取用户触发的安全模式指令，所述安全模式指令用于指示启动对终端的安全保护；处理器 11 根据所述安全模式指令生成安全模式广播，所述安

全模式广播用于指示拦截应用程序对所述终端发起的不安全访问操作；处理器 11 根据所述安全模式广播调用通讯接口 12 保留所述终端的语音业务功能，并关闭所述终端的访问权限功能，所述访问权限功能是指需要用户授予访问权限后允许执行的功能；若处理器 11 通过通讯接口 12 接收到所述应用程序对所述访问权限功能的调用指令，处理器 11 则禁止所述调用指令并输出至显示设备 14，以拦截所述应用程序对所述终端发起的不安全访问操作。

示例性的，所述访问权限功能包括全球定位系统功能、数据业务功能、无线网络功能、相机功能以及录音功能中的至少一种。

进一步地，处理器 11 根据所述安全模式指令生成安全模式广播，可以具体包括步骤：处理器 11 通过通讯接口 12 获取用户选择的访问权限白名单，所述访问权限白名单中包含用户已授权访问的应用程序或者用户已授权访问的所述访问权限功能；处理器 11 根据所述安全模式指令和所述访问权限白名单生成安全模式广播，所述安全模式广播用于指示拦截所述访问权限白名单之外的应用程序对所述终端发起的不安全访问操作。

进一步地，在处理器 11 根据所述安全模式指令和所述访问权限白名单生成安全模式广播之后，还可以包括步骤：处理器 11 根据所述安全模式广播调用通讯接口 12 保留所述终端的语音业务功能；处理器 11 根据所述访问权限白名单调用通讯接口 12 关闭所述访问权限白名单之外的访问权限功能，其中，所述访问权限功能包括 GPS 功能、数据业务功能、无线网络功能、相机功能以及录音功能中的至少一种。

进一步地，若处理器 11 通过通讯接口 12 接收到所述应用程序对所述访问权限功能的调用指令，处理器 11 则禁止所述调用指令并输出至显示设备 14，可以具体包括步骤：若处理器 11 接收到所述应用程序调用所述访问权限功能的调用指令，处理器 11 则确定是否启动对所述终端的安全保护；若已启动对所述终端的安全保护，处理器 11 则通过禁止所述调用指令，以拦截所述应用程序对所述终端

发起的不安全访问操作。

进一步地，在处理器 11 则禁止所述调用指令并输出至显示设备 14，以拦截所述应用程序对所述终端发起的不安全访问操作之后，还可以包括步骤：处理器 11 记录所述终端当前的访问权限功能的使用状态并存储至存储器 13；这样，在处理器 11 接收到所述应用程序调用所述访问权限功能的调用指令，则禁止所述调用指令之后，可以包括步骤：若处理器 11 接收到用户触发的退出指令，处理器 11 则根据存储器 13 中已记录的所述访问权限功能的使用状态，将所述访问权限功能恢复至已记录的所述访问权限功能的使用状态，以退出所述安全模式。

本发明的实施例提供一种终端，通过获取用户触发的安全模式指令生成安全模式广播，以使得终端内的各个功能模块根据安全模式广播保留终端的语音业务功能，并关闭终端的访问权限功能，其中，该访问权限功能是指需要用户授予访问权限后允许执行的功能；这样一来，终端可以成功切换到安全模式，一旦接收到应用程序对该访问权限功能的调用指令，终端就可以禁止所述调用指令，以拦截所述应用程序对所述终端发起的不安全访问操作，提高了终端在使用过程中的安全性，避免用户在使用终端时可能带来的安全隐患。

**实施例 4**

本发明实施例提供一种终端，如图 5 所示，包括：

获取单元 21，用于获取用户触发的安全模式指令，所述安全模式指令用于指示启动对终端的安全保护；

广播生成单元 22，用于根据所述获取单元 21 中所述安全模式指令生成安全模式广播，所述安全模式广播用于指示拦截应用程序对所述终端发起的不安全访问操作；

安全模式切换单元 23，用于根据所述广播生成单元 22 中所述安全模式广播保留所述终端的语音业务功能，并关闭所述终端的访问权限功能，所述访问权限功能是指需要所述用户授予访问权限后允许执行的功能；

拦截单元 24，用于若接收到所述应用程序对所述安全模式切换单元 23 中访问权限功能的调用指令，则禁止所述调用指令，以拦截所述应用程序对所述终端发起的不安全访问操作。

进一步地，所述广播生成单元 22，具体用于获取用户选择的访问权限白名单，所述访问权限白名单中包含用户已授权访问的应用程序或者用户已授权访问的所述访问权限功能；根据所述安全模式指令和所述访问权限白名单生成安全模式广播，所述安全模式广播用于指示拦截所述访问权限白名单之外的应用程序对所述终端发起的不安全访问操作；

其中，所述访问权限功能包括全球定位系统功能、数据业务功能、无线网络功能、相机功能以及录音功能中的至少一种。

进一步地，所述安全模式切换单元 23，具体用于根据所述安全模式广播保留所述终端的语音业务功能；根据所述访问权限白名单关闭所述访问权限白名单之外的访问权限功能，其中，所述访问权限功能包括 GPS 功能、数据业务功能、无线网络功能、相机功能以及录音功能中的至少一种。

进一步地，所述拦截单元 24，具体用于若接收到所述应用程序调用所述访问权限功能的调用指令，则确定是否启动对所述终端的安全保护；若已启动对所述终端的安全保护，则禁止所述调用指令，以拦截所述应用程序对所述终端发起的不安全访问操作。

进一步地，如图 6 所示，所述终端还包括记录单元 25，其中，

所述记录单元 25，用于记录所述终端当前的访问权限功能的使用状态；

所述安全模式切换单元 23，还用于若接收到用户触发的退出指令，则将所述访问权限功能恢复至所述记录单元 25 中已记录的所述访问权限功能的使用状态，以退出所述安全模式。

需要说明的是，本发明实施例提供的终端中部分功能模块的具体描述可以参考方法实施例中的对应内容，本实施例这里不再详细赘述。

本发明的实施例提供一种终端，通过获取用户触发的安全模式指令生成安全模式广播，以使得终端内的各个功能模块根据安全模式广播保留终端的语音业务功能，并关闭终端的访问权限功能，其中，该访问权限功能是指需要用户授予访问权限后允许执行的功能；这样一来，终端可以成功切换到安全模式，一旦接收到应用程序对该访问权限功能的调用指令，终端就可以禁止所述调用指令，以拦截所述应用程序对所述终端发起的不安全访问操作，提高了终端在使用过程中的安全性，避免用户在使用终端时可能带来的安全隐患。

通过以上的实施方式的描述，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，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将装置的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。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。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统，装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述模块或单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本发明各个实施例中的各功能单元可以集成在一个处

理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）或处理器（processor）执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以所述权利要求的保护范围为准。

# 权 利 要 求 书

1、一种终端安全的管理方法，其特征在于，包括：

获取用户触发的安全模式指令，所述安全模式指令用于指示启动对终端的安全保护；

根据所述安全模式指令生成安全模式广播，所述安全模式广播用于指示拦截应用程序对所述终端发起的不安全访问操作；

根据所述安全模式广播保留所述终端的语音业务功能，并关闭所述终端的访问权限功能，所述访问权限功能是指需要所述用户授予访问权限后允许执行的功能；

若接收到所述应用程序对所述访问权限功能的调用指令，则禁止所述调用指令，以拦截所述应用程序对所述终端发起的不安全访问操作。

2、根据权利要求 1 所述的方法，其特征在于，所述访问权限功能包括全球定位系统功能、数据业务功能、无线网络功能、相机功能以及录音功能中的至少一种；

其中，所述根据所述安全模式指令生成安全模式广播，包括：

获取用户选择的访问权限白名单，所述访问权限白名单中包含用户已授权访问的应用程序或者用户已授权访问的所述访问权限功能；

根据所述安全模式指令和所述访问权限白名单生成安全模式广播，所述安全模式广播用于指示拦截所述访问权限白名单之外的应用程序对所述终端发起的不安全访问操作。

3、根据权利要求 2 所述的方法，其特征在于，所述根据所述安全模式广播保留所述终端的语音业务功能，并关闭所述终端的访问权限功能，包括：

根据所述安全模式广播保留所述终端的语音业务功能；

根据所述访问权限白名单关闭所述访问权限白名单之外的访问权限功能，其中，所述访问权限功能包括 GPS 功能、数据业务功能、无线网络功能、相机功能以及录音功能中的至少一种。

4、根据权利要求 1 所述的方法，其特征在于，所述若接收到所

述应用程序调用所述访问权限功能的调用指令，则禁止所述调用指令，包括：

若接收到所述应用程序调用所述访问权限功能的调用指令，则确定是否启动对所述终端的安全保护；

若已启动对所述终端的安全保护，则禁止所述调用指令，以拦截所述应用程序对所述终端发起的不安全访问操作。

5、根据权利要求 1 所述的方法，其特征在于，在所述根据所述安全模式指令生成安全模式广播之后，还包括：

记录所述终端当前的访问权限功能的使用状态；

其中，在所述若接收到所述应用程序调用所述访问权限功能的调用指令，则禁止所述调用指令之后，还包括：

若接收到用户触发的退出指令，则将所述访问权限功能恢复至已记录的所述访问权限功能的使用状态，以退出所述安全模式。

6、一种终端，其特征在于，包括：

获取单元，用于获取用户触发的安全模式指令，所述安全模式指令用于指示启动对终端的安全保护；

广播生成单元，用于根据所述获取单元中所述安全模式指令生成安全模式广播，所述安全模式广播用于指示拦截应用程序对所述终端发起的不安全访问操作；

安全模式切换单元，用于根据所述广播生成单元中所述安全模式广播保留所述终端的语音业务功能，并关闭所述终端的访问权限功能，所述访问权限功能是指需要所述用户授予访问权限后允许执行的功能；

拦截单元，用于若接收到所述应用程序对所述访问权限功能的调用指令，则禁止所述调用指令，以拦截所述应用程序对所述终端发起的不安全访问操作。

7、根据权利要求 6 所述的终端，其特征在于，

所述广播生成单元，具体用于获取用户选择的访问权限白名单，所述访问权限白名单中包含用户已授权访问的应用程序或者用户已

授权访问的所述访问权限功能；根据所述安全模式指令和所述访问权限白名单生成安全模式广播，所述安全模式广播用于指示拦截所述访问权限白名单之外的应用程序对所述终端发起的不安全访问操作；

其中，所述访问权限功能包括全球定位系统功能、数据业务功能、无线网络功能、相机功能以及录音功能中的至少一种。

8、根据权利要求 7 所述的终端，其特征在于，

所述安全模式切换单元，具体用于根据所述安全模式广播保留所述终端的语音业务功能；根据所述访问权限白名单关闭所述访问权限白名单之外的访问权限功能，其中，所述访问权限功能包括 GPS 功能、数据业务功能、无线网络功能、相机功能以及录音功能中的至少一种。

9、根据权利要求 6 所述的终端，其特征在于，

所述拦截单元，具体用于若接收到所述应用程序调用所述访问权限功能的调用指令，则确定是否启动对所述终端的安全保护；若已启动对所述终端的安全保护，则禁止所述调用指令，以拦截所述应用程序对所述终端发起的不安全访问操作。

10、根据权利要求 6 所述的终端，其特征在于，所述终端还包括记录单元，其中，

所述记录单元，用于记录所述终端当前的访问权限功能的使用状态；

所述安全模式切换单元，还用于若接收到用户触发的退出指令，则将所述访问权限功能恢复至所述记录单元中已记录的所述访问权限功能的使用状态，以退出所述安全模式。

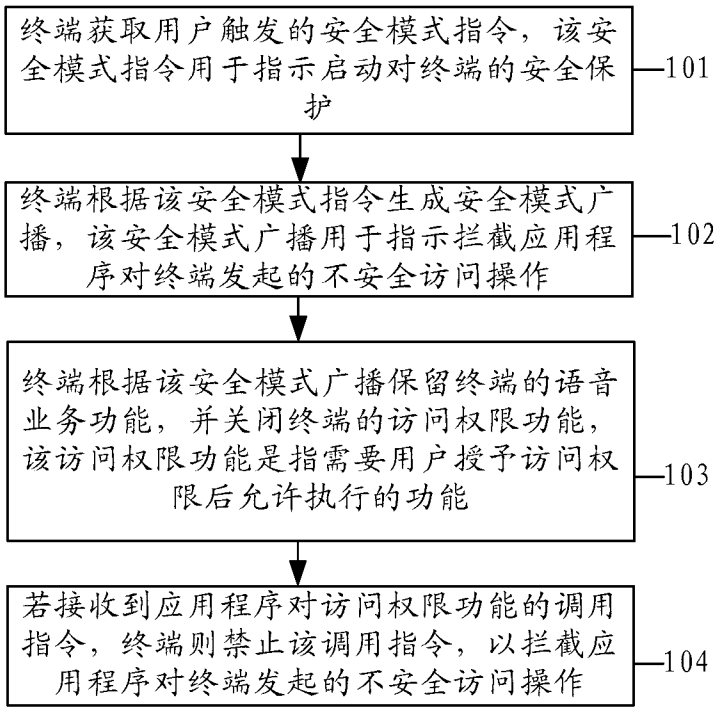
终端获取用户触发的安全模式指令，该安全模式指令用于指示启动对终端的安全保护
101
终端根据该安全模式指令生成安全模式广播，该安全模式广播用于指示拦截应用程序对终端发起的不安全访问操作
102
终端根据该安全模式广播保留终端的语音业务功能，并关闭终端的访问权限功能，该访问权限功能是指需要用户授予访问权限后允许执行的功能
103
若接收到应用程序对访问权限功能的调用指令，终端则禁止该调用指令，以拦截应用程序对终端发起的不安全访问操作
104

图 1


情景模式
户外模式
标准模式
会议模式
静音模式
飞行模式
超级安全模式

图 2

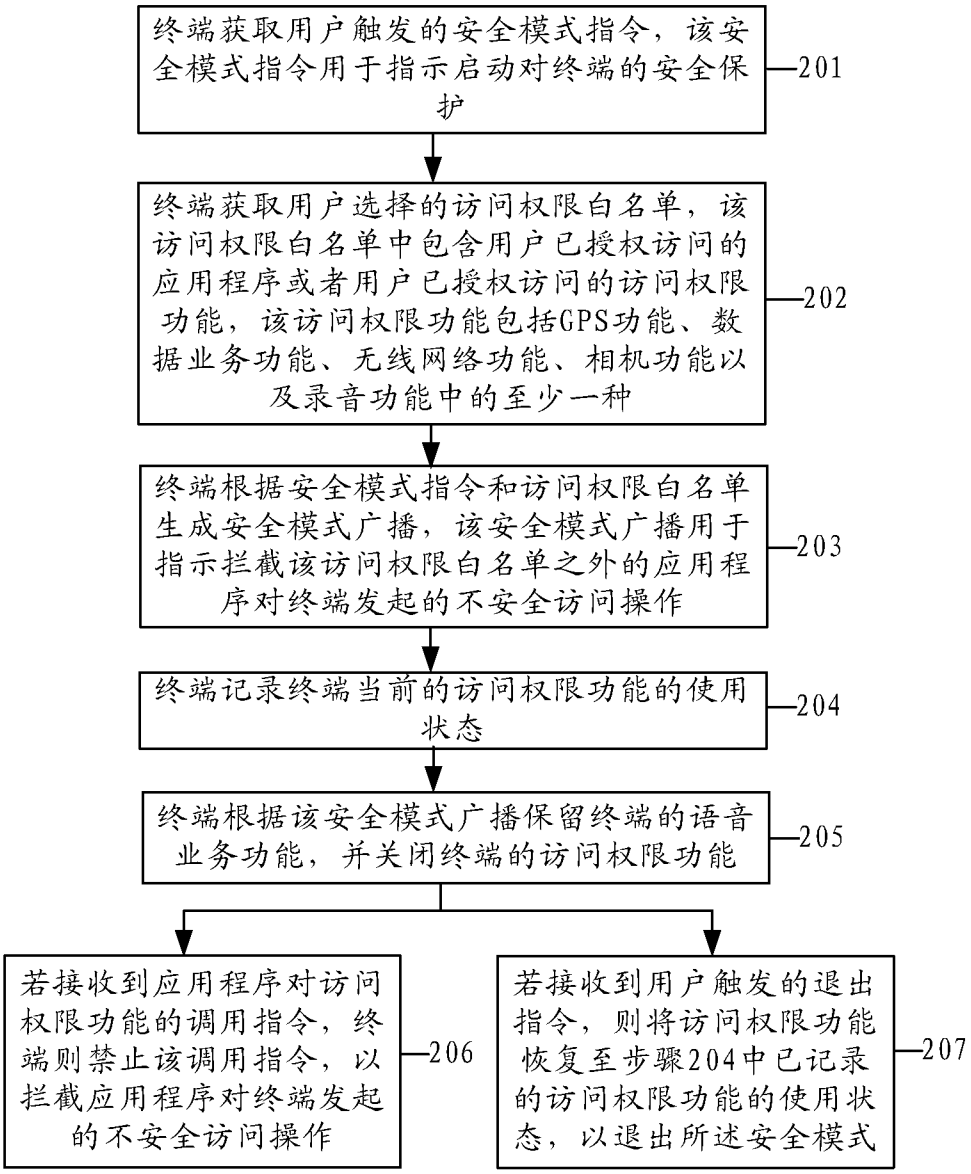
终端获取用户触发的安全模式指令，该安全模式指令用于指示启动对终端的安全保护
201
终端获取用户选择的访问权限白名单，该访问权限白名单中包含用户已授权访问的应用程序或者用户已授权访问的访问权限功能，该访问权限功能包括GPS功能、数据业务功能、无线网络功能、相机功能以及录音功能中的至少一种
202
终端根据安全模式指令和访问权限白名单生成安全模式广播，该安全模式广播用于指示拦截该访问权限白名单之外的应用程序对终端发起的不安全访问操作
203
终端记录终端当前的访问权限功能的使用状态
204
终端根据该安全模式广播保留终端的语音业务功能，并关闭终端的访问权限功能
205
若接收到应用程序对访问权限功能的调用指令，终端则禁止该调用指令，以拦截应用程序对终端发起的不安全访问操作
206
若接收到用户触发的退出指令，则将访问权限功能恢复至步骤204中已记录的访问权限功能的使用状态，以退出所述安全模式
207

图 3

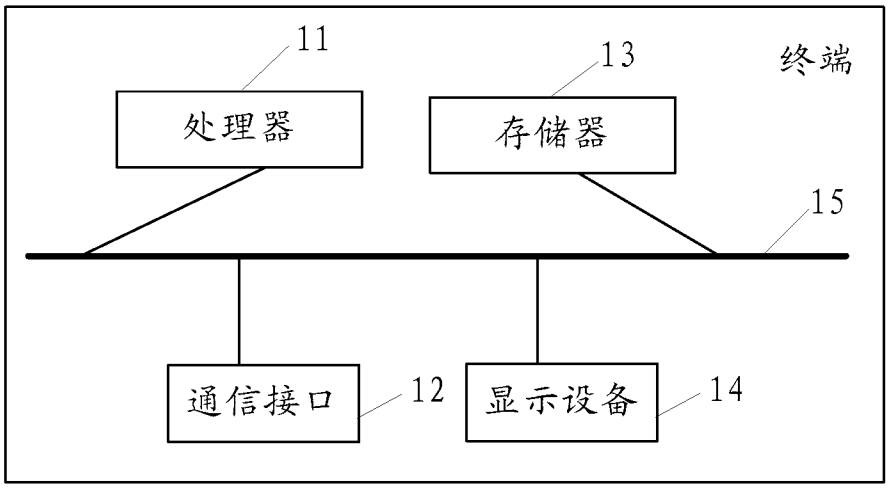
11
处理器
13
存储器
终端
15
通信接口
12
显示设备
14

图 4

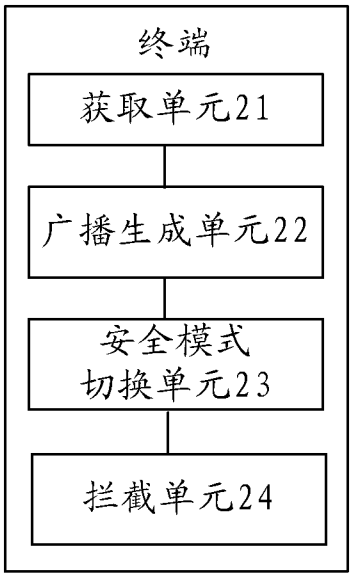
终端
获取单元21
广播生成单元22
安全模式
切换单元23
拦截单元24

图 5

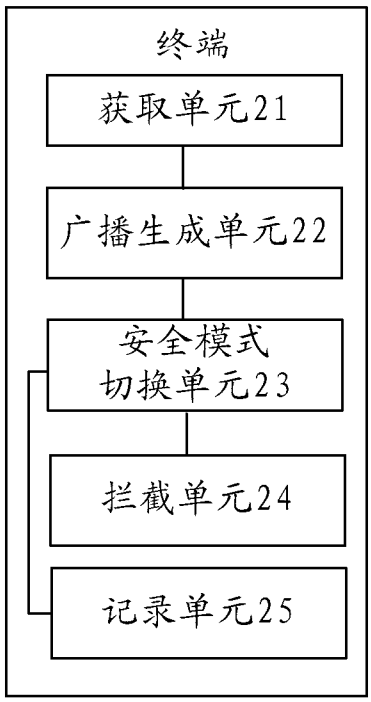


图 6

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/071818

**A. CLASSIFICATION OF SUBJECT MATTER**

H04W 88/02 (2009.01) i; G06F 21/62 (2013.01) n

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)

H04W; H04M; 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)

CNPAT, CNKI, WPI, EPODOC: prohibition, intercept, security, application program, application software, safe+, security, APP+, access, inhibit+, disable+, except, ban, limit+, restrict+, reject+, intercept+, close, command, instruct+, order, directive, authority, terminal, phone

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | CN 103324893 A (HUAWEI TECHNOLOGIES CO., LTD.) 25 September 2013 (25.09.2013) description, paragraphs [0041]-[0048] | 1-10 |
| A | CN 103686600 A (SHENZHEN COOLPAD TECHNOLOGIES CO., LTD. et al.) 26 March 2014 (26.03.2014) the whole document | 1-10 |
| A | CN 103927475 A (GUANGDONG MINGCHUANG SOFTWARE TECHNOLOGY CO., LTD.) 16 July 2014 (16.07.2014) the whole document | 1-10 |
| A | US 2007118558 A1 (RESEARCH IN MOTION LIMITED) 24 May 2007 (24.05.2007) the whole document | 1-10 |

☐ 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 |
|---|---|
| 07 August 2015 | 03 November 2015 |
| Name and mailing address of the ISA<br>State Intellectual Property Office of the P. R. China<br>No. 6, Xitucheng Road, Jimenqiao<br>Haidian District, Beijing 100088, China<br>Facsimile No. (86-10) 62019451 | Authorized officer<br>JIANG, Li<br>Telephone No. (86-10) 61648235 |

**INTERNATIONAL SEARCH REPORT**
Information on patent family members

International application No.
PCT/CN2015/071818

| Patent Documents referred in the Report | Publication Date | Patent Family | Publication Date |
|---|---|---|---|
| CN 103324893 A | 25 September 2013 | None | |
| CN 103686600 A | 26 March 2014 | None | |
| CN 103927475 A | 16 July 2014 | None | |
| US 2007118558 A1 | 24 May 2007 | US 2012297443 A1 | 22 November 2012 |
| | | US 2011289554 A1 | 24 November 2011 |
| | | US 8045958 B2 | 25 October 2011 |
| | | US 8699999 B2 | 15 April 2014 |
| | | US 8254884 B2 | 28 August 2012 |

# 国际检索报告

国际申请号 PCT/CN2015/071818

A. 主题的分类

H04W 88/02(2009.01)i; G06F 21/62(2013.01)n

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)

H04W H04M 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）)

CNPAT,CNKI,WPI,EPODOC:禁止，拦截，限制，阻止，关闭，拒绝，指令，指示，命令，安全，访问，权限，终端，手机，应用程序，应用软件，safe+，security，APP+，access，inhibit+，disable+，except，ban，limit+，restrict+，reject+，intercept+，close，command，instruct+，order，directive，authority，terminal，phone

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 |
|---|---|---|
| A | CN 103324893 A (华为技术有限公司) 2013年 9月 25日 (2013-09-25)<br>说明书第0041-0048段 | 1-10 |
| A | CN 103686600 A (深圳酷派技术有限公司等) 2014年 3月 26日 (2014-03-26)<br>全文 | 1-10 |
| A | CN 103927475 A (广东明创软件科技有限公司) 2014年 7月 16日 (2014-07-16)<br>全文 | 1-10 |
| A | US 2007118558 A1 (RESEARCH IN MOTION LIMITED) 2007年 5月 24日 (2007-05-24)<br>全文 | 1-10 |

☐ 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 8月 7日 | 2015年 11月 3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)<br>北京市海淀区蓟门桥西土城路6号<br>100088 中国<br>传真号 (86-10)62019451 | 蒋莉<br>电话号码 (86-10)61648235 |

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/CN2015/071818

| 检索报告引用的专利文件 | | | 公布日<br>(年/月/日) | 同族专利 | | | 公布日<br>(年/月/日) |
|---|---|---|---|---|---|---|---|
| CN | 103324893 | A | 2013年 9月 25日 | 无 | | | |
| CN | 103686600 | A | 2014年 3月 26日 | 无 | | | |
| CN | 103927475 | A | 2014年 7月 16日 | 无 | | | |
| US | 2007118558 | A1 | 2007年 5月 24日 | US | 2012297443 | A1 | 2012年 11月 22日 |
| | | | | US | 2011289554 | A1 | 2011年 11月 24日 |
| | | | | US | 8045958 | B2 | 2011年 10月 25日 |
| | | | | US | 8699999 | B2 | 2014年 4月 15日 |
| | | | | US | 8254884 | B2 | 2012年 8月 28日 |