(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
2017 年 7 月 6 日 (06.07.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/113584 A1

(51) 国际专利分类号:
H04W 12/06 (2009.01) *G06F 21/53* (2013.01)

(21) 国际申请号: PCT/CN2016/084103

(22) 国际申请日: 2016 年 5 月 31 日 (31.05.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201511031383.X 2015 年 12 月 31 日 (31.12.2015) CN

(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: **邵寿平 (SHAO, Shouping)**; 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: **广州三环专利代理有限公司 (GUANGZHOU SCIHEAD PATENT AGENT CO. , LTD.)**; 中国广东省广州市越秀区先烈中路 80 号汇华商贸大厦 1508 室, Guangdong 510070 (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)。

本国际公布:
— 包括国际检索报告(条约第 21 条(3))。

(54) **Title**: SECURITY CONTROL METHOD AND SYSTEM FOR CONTAINER OF TERMINAL

(54) **发明名称** : 一种终端容器安全的控制方法与系统

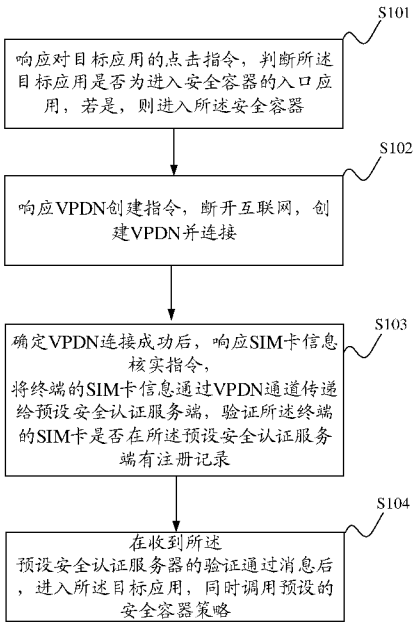

图 1

(57) **Abstract**: A security control method and system for a container of a terminal. The method comprises: determining, in response to a tap instruction on a target application, whether the target application is a portal application for entering a secure container, and if yes, entering the secure container (S101); disconnecting the Internet, and creating and connecting to a VPDN, in response to a VPDN creation instruction (S102); transferring, after determining that the VPDN is successfully connected, information about a SIM card of a terminal to a preset security authentication server by means of a VPDN channel in response to a SIM card information verification instruction, to verify whether the SIM card of the terminal has a registration record in the preset security authentication server (S103); entering the target application after receiving a verification success message from the preset security authentication server and invoking a preset secure container policy (S104). Whereby, a secure container can be provided for applications requiring client privacy protection, and all application programs can be run in a same system, without the need to allocate additional memory and space, such that data security of the terminal user can be protected conveniently and efficiently.

(57) **摘要**:

[见续页]

WO 2017/113584 A1

一种终端容器安全的控制方法与系统，所述方法包括：响应对目标应用的点击指令，判断目标应用是否为进入安全容器的入口应用，若是，则进入安全容器（S101）；响应 VPDN 创建指令，断开互联网，创建 VPDN 并连接（S102）；确定 VPDN 连接成功后，响应 SIM 卡信息核实指令，将终端的 SIM 卡信息通过 VPDN 通道传递给预设安全认证服务端，验证所述终端的 SIM 卡是否在所述预设安全认证服务端有注册记录（S103）；在收到所述预设安全认证服务器的验证通过消息后，进入所述目标应用，同时调用预设的安全容器策略（S104），可以为需要保护客户隐私的应用提供安全容器，所有的应用程序可在同一系统中运行，不必分配额外的内存和空间，可以简单高效的保护终端用户的数据安全。

一种终端容器安全的控制方法与系统

本申请要求于2015年12月31日提交中国专利局，申请号为201511031383.X、发明名称为“一种终端容器安全的控制方法与系统”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及终端信息安全领域，特别是涉及一种终端容器安全的控制方法与系统。

背景技术

自从手机智能化和网络化介入之后，所带来功能和使用效率的提升，既为手机用户提供了非常大的帮助，同时也将一些安全隐患带到人们面前。

现有的手机安全方案较少，一些公司推出双系统方案，在独立的安全系统中实现手机的安全策略，保障用户的信息的安全，为安全系统预留单独的数据分区，同标准系统独立开来。该方法能够有效保障用户数据的独立性，保障用户数据的隐私，但是双系统同时运行不仅制造成本高，且需要为安全系统预分配内存，加大电量消耗，运行成本也较高，不能简单高效地保障手机用户数据安全。

发明内容

有鉴于此，本发明的主要目的在于提供一种终端容器安全的控制方法与系统，可以为手机应用提供安全容器，保障容器内应用的运行安全。

为实现上述目的，本发明提供了一种终端容器安全的控制方法，包括:

响应对目标应用的点击指令，判断所述目标应用是否为进入安全容器的入口应用，若是，则进入所述安全容器;

响应VPDN创建指令，断开互联网，创建VPDN并连接;

确定VPDN连接成功后，响应SIM卡信息核实指令将终端的SIM卡信息

通过 VPDN 通道传递给预设安全认证服务端，验证所述终端的 SIM 卡是否在所述预设安全认证服务端有注册记录;

在收到所述预设安全认证服务器的验证通过消息后，进入所述目标应用，同时调用预设的安全容器策略。

优选地，所述安全容器策略包括:

隐藏 APN 的配置信息，禁用数据连接途径，屏蔽 USB 功能以及禁用终端的预设禁用设备功能。

优选地，所述判断所述目标应用是否为进入安全容器的入口应用包括:

判断对所述目标应用的点击所发送的广播中的包名参数是否为所述安全容器预设的应用包名。

优选地，所述响应 SIM 卡信息核实指令，将终端的 SIM 卡信息通过 VPDN 通道传递给预设安全认证服务端前还包括:

响应所述终端的 SIM 卡信息对应的二维码的扫描指令，获取所述终端的 SIM 卡信息。

优选地，所述预设禁用设备功能包括照相机功能、粘贴板功能、SD 卡功能、截屏功能、录屏功能和 GPS 功能。

优选地，所述安全容器策略还包括:

推送目标应用内预置应用的下载。

优选地，所述隐藏 APN 的配置信息包括:

对所述 APN 的配置信息进行预设的隐藏字段赋值。

本发明还提供了一种终端容器安全的控制系统，包括:

容器内外判别模块，用于响应对目标应用的点击指令，判断所述目标应用是否为进入安全容器的入口应用，若是，则进入所述安全容器;

安全认证模块，用于响应 VPDN 创建指令，断开互联网，创建 VPDN 并连接；确定 VPDN 连接成功后，响应 SIM 卡信息核实指令，将终端的 SIM 卡信息通过 VPDN 通道传递给预设安全认证服务端，验证所述终端的 SIM 卡是否在所述预设安全认证服务端有注册记录;

容器内策略调用模块，用于在收到所述预设安全认证服务器的验证通过消息后，进入所述目标应用，同时调用预设的安全容器策略。

优选地，所述安全容器策略包括:

隐藏 APN 的配置信息，禁用数据连接途径，屏蔽 USB 功能以及禁用终端的预设禁用设备功能。

优选地，所述预设禁用设备功能包括照相机功能、粘贴板功能、SD 卡功能、截屏功能、录屏功能和 GPS 功能。

应用本发明提供的一种终端容器安全的控制方法与系统，判断目标应用是否为进入安全容器的入口应用，若是，则进入安全容器；断开互联网，创建 VPDN 并连接；确定 VPDN 连接成功后，将终端的 SIM 卡信息通过 VPDN 通道传递给预设安全认证服务端，验证所述终端的 SIM 卡是否在所述预设安全认证服务端有注册记录；在验证通过后，进入所述目标应用，同时调用预设的安全策略，可以为需要保护客户隐私的应用提供安全容器，所有的应用程序可在同一系统中运行，不必分配额外的内存和空间，可以简单高效的保护终端用户的数据安全。

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，显而易见地，下面描述中的附图仅仅是本发明的实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据提供的附图获得其他的附图。

图1为本发明一种终端容器安全的控制方法实施例一的流程图；

图2为本发明一种终端容器安全的控制方法实施例一的详细原理示意图；

图3为本发明一种终端容器安全的控制方法实施例一的又一详细原理示意图；

图4为本发明一种终端容器安全的控制方法实施例一的又一详细原理示意图；

图 5 为本发明一种终端容器安全的控制系统实施例二的结构示意图。

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。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

本发明所述终端包括但不限于智能手机、平板电脑等。

实施例一:

本发明提供了一种终端容器安全的控制方法，图 1 示出了本发明终端容器安全的控制方法实施例的流程图，包括:

步骤 S101: 响应对目标应用的点击指令，判断所述目标应用是否为进入安全容器的入口应用，若是，则进入所述安全容器;

容器专指一组应用的运行环境，这组应用可以从 MDM 移动管理平台分发给设备，默认情况下，MDM 客户端属于容器内应用。MDM 移动管理平台可以下发容器策略，即当这组应用运行时（顶层活动为该应用），MDM 客户端应用该策略（比如切换 APN 等行为）。当顶层活动发生变化时，会发送一个广播，广播的 ACTION 为“com.pekall.action.TOP_PACKAGE”，并且带参数 Intent.putExtra(“toppackage”, 当前包名)，即容器变化触发者是顶层活动发生改变并且参数中“包名”为手机设定的“应用包名”的广播，判断所述目标应用是否为进入安全容器的入口应用即通过: 判断对目标应用的点击所发送的广播中的包名参数是否为安全容器预设的应用包名来实现，原理图如图 2 所示。

步骤 S102: 响应 VPDN 创建指令，断开互联网，创建 VPDN 并连接;

终端会预置一个创建并连接 vpdn 的应用，vpdn 配置信息由客户提供，创建前自动断开互联网，如果 vpdn 创建成功，给出用户提示，否则提示失败，退出应用，连接互联网。

步骤 S103: 确定 VPDN 连接成功后，响应 SIM 卡信息核实指令，将终端的 SIM 卡信息通过 VPDN 通道传递给预设安全认证服务端，验证所述终端的 SIM 卡是否在所述预设安全认证服务端有注册记录;

SIM 卡信息可通过对终端 SIM 卡信息对应的二维码的扫描获取，在 vpdn 连接成功后，提示用户扫描 SIM 商提供的二维码，并且把扫描信息通过 VPDN 通道传递给预设安全认证服务端进行 SIM 卡信息核实比对，验证所述终端的 SIM 卡是否在所述预设安全认证服务端有注册记录，验证通过则返回成功消息，并且推送预置的应用和策略; 否则提示 SIM 卡身份信息不匹配，退出应用，连接互联网，流程如图 3 所示。

步骤 S104：在收到所述预设安全认证服务器的验证通过消息后，进入所述目标应用，同时调用预设的安全容器策略；

所述安全容器策略可包括：

隐藏 APN 的配置信息，禁用数据连接途径，屏蔽 USB 功能以及禁用终端的预设禁用设备功能。

当收到预设的安全认证服务器的验证通过消息后，代表完全进入安全容器，进入最初点击的目标应用，并同时调用安全容器预设的策略：

（1）APN 安全控制

为了保护用户的 vpdn 信息，需要对 APN 的配置信息进行隐藏处理。点击应用进入容器内部时，VPDN 已经配置好并且连接上，为了方便控制 APN 的显示或者隐藏，在 TelephonyProvider 类中为所有 APN 添加一个”Hidden”字段，并且赋值为 0，代表默认显示。在配置 VPDN 时，为该 APN 的”Hidden”字段赋值为 1，表示隐藏。当用户点击设置页面去查看 APN 列表时，Setting 类会去加载 apn 数据库，此时，进行”Hidden”字段判定，如果值为 1 就不予显示，达到对 VPDN 配置信息进行保护的目的。

（2）数据连接安全控制

为了防止用户隐私信息被木马获取，就需要截断所有木马流入的数据连接途径，包括 wifi,Bluetooth,mms,sms。

控制的步骤分为系统属性设定和功能控制，当进入容器内部时，容器内部的 MDM 应用会立即调用设置数据连接的系统属性值的接口函数。它们的接口函数分别为：boolean allowOutgoingWifi(boolean allow)，boolean allowOutgoingBluetooth(boolean allow)，boolean allowOutgoingMms(boolean allow)，boolean allowOutgoingSms(boolean allow)；当数据功能被启动时，通过读取系统属性值来判断是否进行数据连接流程，比如 wifi 的属性“persist.yulong.mdm.wifi” =1，说明在容器内，不允许进行数据连接，立即返回，从而实现对数据连接的安全控制。

（3）应用安装安全控制

容器内部采用服务器推送安装应用的方式进行应用安装，通过屏蔽 USB 功能和应用来源判断阻止用户或者黑客在容器内部进行应用安装，USB 屏蔽方法和数据连接控制一样，通过系统属性值的设定和读取实现。

（4）手机设备安全控制

手机设备的安全控制主要包括照相机、粘贴版、SD卡、截屏、录屏、GPS等设备的屏蔽，从硬件上阻断木马黑客的流入，从而到达保障用户信息安全性目的。为了便于方案的普及和扩展，把以上四个模块封装成相应的策略，分别是应用策略：ApplicationPolicy getApplicationPolicy()；数据连接策略：PhoneRestrictionPolicy getPhoneRestrictionPolicy()；设备控制策略：RestrictionPolicy getRestrictionPolicy()；APN控制策略 getAnpPolicy()。策略内部的方案实现可以根据用户具体实现，具有简单易扩展的特点，适用于大部分政企用户，安全容器策略设计如图4所示。

应用本实施例提供的一种终端容器安全的控制方法，判断目标应用是否为进入安全容器的入口应用，若是，则进入安全容器；断开互联网，创建VPDN并连接；确定VPDN连接成功后，将终端的SIM卡信息通过VPDN通道传递给预设安全认证服务端，验证所述终端的SIM卡是否在所述预设安全认证服务端有注册记录；在验证通过后，进入所述目标应用，同时调用预设的安全策略，隐藏APN的配置信息，禁用数据连接途径，屏蔽USB功能以及禁用终端的预设禁用设备功能。可以为需要保护客户隐私的应用提供安全容器，所有的应用程序可在同一系统中运行，不必分配额外的内存和空间，可以简单高效的保护终端用户的数据安全。

实施例二：

本发明还提供了一种终端容器安全的控制系统，图5示出了本发明终端容器安全的控制系统实施例结构示意图，包括：

容器内外判别模块101，用于响应对目标应用的点击指令，判断所述目标应用是否为进入安全容器的入口应用，若是，则进入所述安全容器；

安全认证模块102，用于响应VPDN创建指令，断开互联网，创建VPDN并连接；确定VPDN连接成功后，响应SIM卡信息核实指令，将终端的SIM卡信息通过VPDN通道传递给预设安全认证服务端，验证所述终端的SIM卡是否在所述预设安全认证服务端有注册记录；

容器内策略调用模块103，用于在收到所述预设安全认证服务器的验证通过消息后，进入所述目标应用，同时调用预设的安全容器策略；

所述安全容器策略可包括：

隐藏 APN 的配置信息，禁用数据连接途径，屏蔽 USB 功能以及禁用终端的预设禁用设备功能。

应用本实施例提供的一种终端容器安全的控制系统，容器内外判别模块 101 判断目标应用是否为进入安全容器的入口应用，若是，则进入安全容器；安全认证模块 102 断开互联网，创建 VPDN 并连接；确定 VPDN 连接成功后，将终端的 SIM 卡信息通过 VPDN 通道传递给预设安全认证服务端，验证所述终端的 SIM 卡是否在所述预设安全认证服务端有注册记录；在验证通过后，进入所述目标应用，同时容器内策略调用模块 103 调用预设的安全策略，隐藏 APN 的配置信息，禁用数据连接途径，屏蔽 USB 功能以及禁用终端的预设禁用设备功能。可以为需要保护客户隐私的应用提供安全容器，所有的应用程序可在同一系统中运行，不必分配额外的内存和空间，可以简单高效的保护终端用户的数据安全。

需要说明的是，本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。对于系统类实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

最后，还需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

以上对本发明所提供的方法和系统进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

权 利 要 求

1、一种终端容器安全的控制方法，其特征在于，包括:

响应对目标应用的点击指令，判断所述目标应用是否为进入安全容器的入口应用，若是，则进入所述安全容器;

响应 VPDN 创建指令，断开互联网，创建 VPDN 并连接;

确定 VPDN 连接成功后，响应 SIM 卡信息核实指令，将终端的 SIM 卡信息通过 VPDN 通道传递给预设安全认证服务端，验证所述终端的 SIM 卡是否在所述预设安全认证服务端有注册记录;

在收到所述预设安全认证服务器的验证通过消息后，进入所述目标应用，同时调用预设的安全容器策略。

2、根据权利要求 1 所述的终端容器安全的控制方法，其特征在于，所述安全容器策略包括:

隐藏 APN 的配置信息，禁用数据连接途径，屏蔽 USB 功能以及禁用终端的预设禁用设备功能。

3、根据权利要求 1 所述的终端容器安全的控制方法，其特征在于，所述判断所述目标应用是否为进入安全容器的入口应用包括:

判断对所述目标应用的点击所发送的广播中的包名参数是否为所述安全容器预设的应用包名。

4、根据权利要求 1 所述的终端容器安全的控制方法，其特征在于，所述响应 SIM 卡信息核实指令，将终端的 SIM 卡信息通过 VPDN 通道传递给预设安全认证服务端前还包括:

响应所述终端的 SIM 卡信息对应的二维码的扫描指令，获取所述终端的 SIM 卡信息。

5、根据权利要求 2 所述的终端容器安全的控制方法 ，其特征在于，所述预设禁用设备功能包括照相机功能、粘贴板功能、SD 卡功能、截屏功能、录屏功能和 GPS 功能。

6、根据权利要求 2 所述的终端容器安全的控制方法，其特征在于，所述安全容器策略还包括:

推送目标应用内预置应用的下载。

7、根据权利要求 2 所述的终端容器安全的控制方法，其特征在于，所述隐藏 APN 的配置信息包括:

对所述 APN 的配置信息进行预设的隐藏字段赋值。

8、一种终端容器安全的控制系统，其特征在于，包括:

容器内外判别模块，用于响应对目标应用的点击指令，判断所述目标应用是否为进入安全容器的入口应用，若是，则进入所述安全容器;

安全认证模块，用于响应 VPDN 创建指令，断开互联网，创建 VPDN 并连接；确定 VPDN 连接成功后，响应 SIM 卡信息核实指令，将终端的 SIM 卡信息通过 VPDN 通道传递给预设安全认证服务端，验证所述终端的 SIM 卡是否在所述预设安全认证服务端有注册记录;

容器内策略调用模块，用于在收到所述预设安全认证服务器的验证通过消息后，进入所述目标应用，同时调用预设的安全容器策略。

9、根据权利要求 8 所述的终端容器安全的控制系统，所述安全容器策略包括:

隐藏 APN 的配置信息，禁用数据连接途径，屏蔽 USB 功能以及禁用终端的预设禁用设备功能。

10、根据权利要求 9 所述的终端容器安全的控制系统 ，其特征在于，所述预设禁用设备功能包括照相机功能、粘贴板功能、SD 卡功能、截屏功能、录屏功能和 GPS 功能。

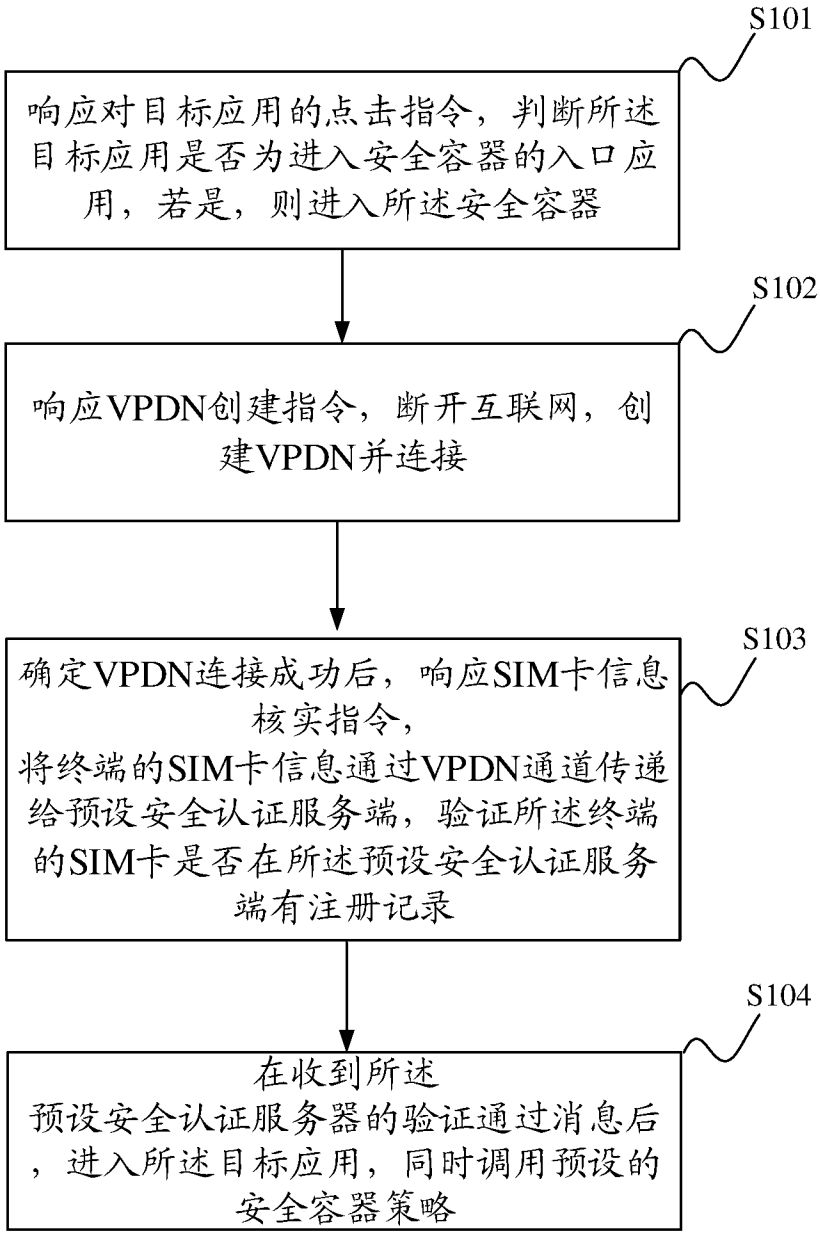
S101
响应对目标应用的点击指令，判断所述目标应用是否为进入安全容器的入口应用，若是，则进入所述安全容器
S102
响应VPDN创建指令，断开互联网，创建VPDN并连接
S103
确定VPDN连接成功后，响应SIM卡信息核实指令，
将终端的SIM卡信息通过VPDN通道传递给预设安全认证服务端，验证所述终端的SIM卡是否在所述预设安全认证服务端有注册记录
S104
在收到所述
预设安全认证服务器的验证通过消息后，进入所述目标应用，同时调用预设的安全容器策略

图 1

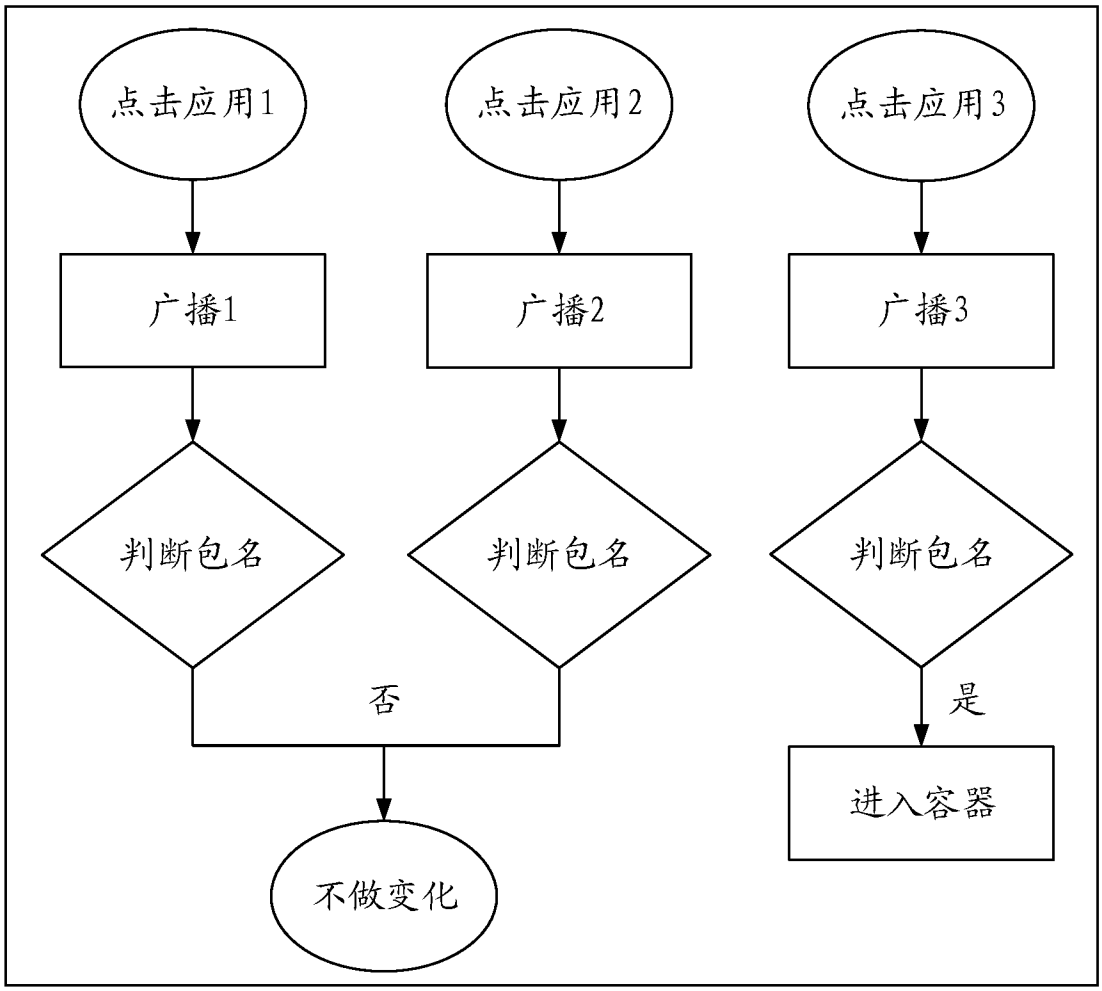

图 2

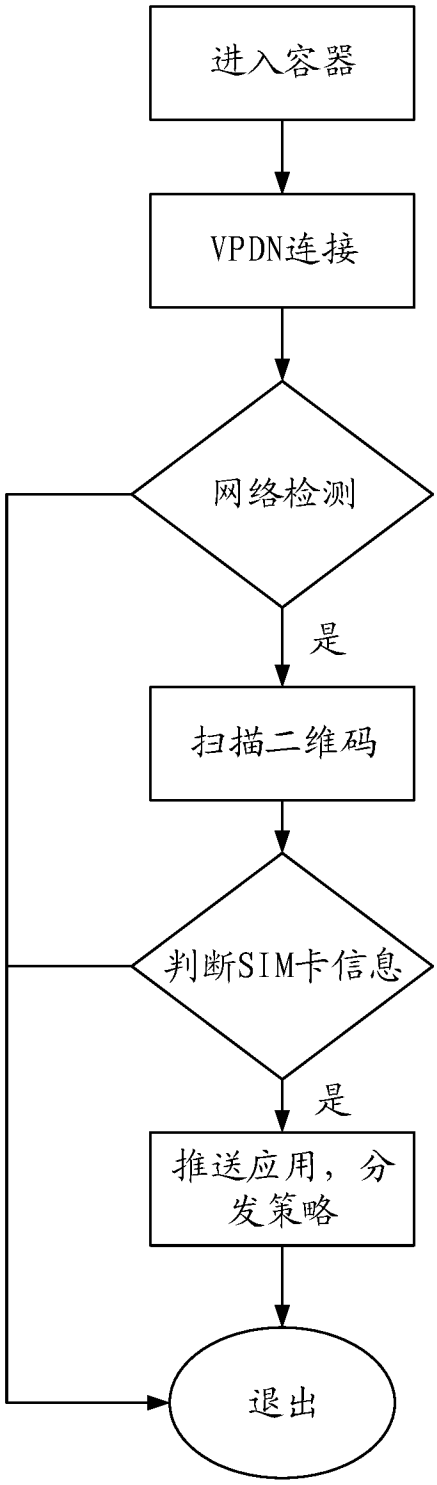

图 3

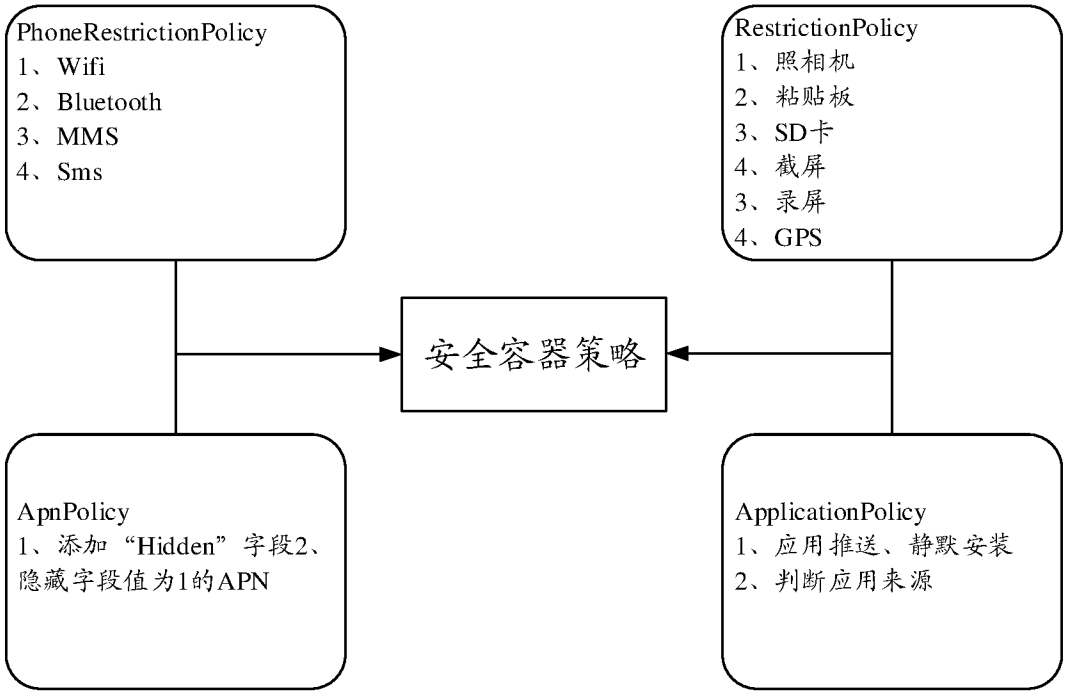
PhoneRestrictionPolicy
1、Wifi
2、Bluetooth
3、MMS
4、Sms
RestrictionPolicy
1、照相机
2、粘贴板
3、SD卡
4、截屏
3、录屏
4、GPS
安全容器策略
ApnPolicy
1、添加“Hidden”字段2、隐藏字段值为1的APN
ApplicationPolicy
1、应用推送、静默安装
2、判断应用来源

图 4

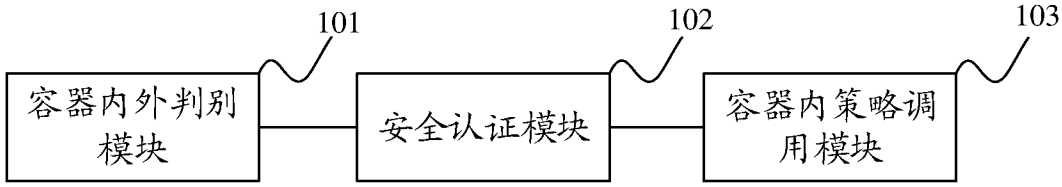
101
102
103
容器内外判别模块
安全认证模块
容器内策略调用模块

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/084103

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/06 (2009.01) i; G06F 21/53 (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)

H04W; 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, EPODOC, WPI, GOOGLE, CNKI: VPDN, SIM, MDM, safety, terminal, authentication, security, disconnect+, specific, internal, network, policy, card, virtual, channel, environment, VPN, creation, connect, dedication, application, container

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 105550577 A (YULONG COMPUTER TELECOMMUNICATION TECHNOLOGIES (SHENZHEN) CO., LTD.) 04 May 2016 (04.05.2016) claims 1-10	1-10
X	CN 103619020 A (CHENGDU DAXINTONG COMMUNICATIONS EQUIPMENT CO., LTD.) 05 March 2014 (05.03.2014) description, paragraphs [0022], [0030], [0031], [0036], [0038], [0039] and [0046]	1-10
A	CN 103581184 A (NO.15 INSTITUTE OF CHINA ELECTRONICS TECHNOLOGY GROUP CORPORATION) 12 February 2014 (12.02.2014) the whole document	1-10
A	CN 103618736 A (CHENGDU DAXINTONG COMMUNICATIONS EQUIPMENT CO., LTD.) 05 March 2014 (05.03.2014) the whole document	1-10
A	US 2005125661 A1 (NOKIA CORPORATION) 09 June 2005 (09.06.2005) 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
22 September 2016	08 October 2016
Name and mailing address of the ISA 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 HU, Mingjun Telephone No. (86-10) 62414105

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/084103

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 105550577 A	04 May 2016	None	
CN 103619020 A	05 March 2014	WO 2015085809 A1	18 June 2015
CN 103581184 A	12 February 2014	None	
CN 103618736 A	05 March 2014	WO 2015085808 A1	18 June 2015
US 2005125661 A1	09 June 2005	EP 1680719 A1	19 July 2006
		WO 2005045735 A1	19 May 2005
		CN 1886747 A	27 December 2006
		AU 2003278449 A1	26 May 2005
		KR 20060073976 A	29 June 2006

国际检索报告

国际申请号
PCT/CN2016/084103

A. 主题的分类

H04W 12/06(2009.01)i; G06F 21/53(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)

H04W, 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, EPODOC, WPI, GOOGLE, CNKI：容器，安全，应用，断开，创建，连接，内网，专用，虚拟专用网,认证，环境，VPDN, SIM, MDM, safety, terminal, authentication, security, disconnect+, specific, internal, network, policy, card, virtual,channel

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 105550577 A (宇龙计算机通信科技深圳有限公司) 2016年 5月 4日 (2016-05-04) 权利要求1－10	1－10
X	CN 103619020 A (成都达信通通讯设备有限公司) 2014年 3月 5日 (2014-03-05) 说明书第22，30－31，36，38－39，46段	1－10
A	CN 103581184 A (中国电子科技集团公司第十五研究所) 2014年 2月 12日 (2014-02-12) 全文	1－10
A	CN 103618736 A (成都达信通通讯设备有限公司) 2014年 3月 5日 (2014-03-05) 全文	1－10
A	US 2005125661 A1 (NOKIA CORPORATION) 2005年 6月 9日 (2005-06-09) 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
2016年 9月 22日	2016年 10月 8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 胡明军 电话号码 (86-10)62414105

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/084103

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	105550577	A	2016年 5月 4日		无		
CN	103619020	A	2014年 3月 5日	WO	2015085809	A1	2015年 6月 18日
CN	103581184	A	2014年 2月 12日		无		
CN	103618736	A	2014年 3月 5日	WO	2015085808	A1	2015年 6月 18日
US	2005125661	A1	2005年 6月 9日	EP	1680719	A1	2006年 7月 19日
				WO	2005045735	A1	2005年 5月 19日
				CN	1886747	A	2006年 12月 27日
				AU	2003278449	A1	2005年 5月 26日
				KR	20060073976	A	2006年 6月 29日