(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
2013 年 12 月 19 日 (19.12.2013)

WIPO | PCT

(10) 国际公布号
WO 2013/185413 A1

(51) 国际专利分类号:
H04W 12/00 (2009.01)

(21) 国际申请号: PCT/CN2012/079659

(22) 国际申请日: 2012 年 8 月 3 日 (03.08.2012)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201210192660.5 2012 年 6 月 12 日 (12.06.2012) CN

(71) 申请人 (对除美国外的所有指定国): **中兴通讯股份有限公司 (ZTE CORPORATION)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): **鲁司运 (LU, Siyun)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。 **张贞志 (ZHANG, Zhenzhi)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。 **钟声 (ZHONG, Sheng)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(74) 代理人: **北京康信知识产权代理有限责任公司 (KANGXIN PARTNERS,P.C.)**; 中国北京市海淀区知春路甲 48 号盈都大厦 A 座 16 层, Beijing 100098 (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, IS, JP, KE, KG, KM, 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, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, 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**: METHOD AND APPARATUS FOR CONTROLLING APPLICATION RIGHT

(54) **发明名称** : 应用权限的控制方法及装置

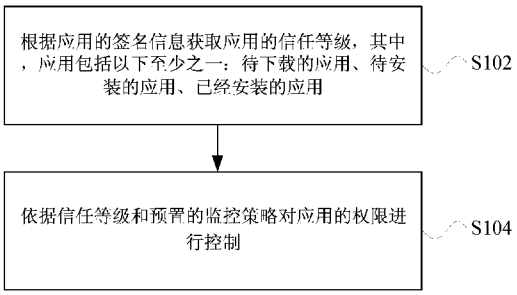

图 1 / FIG. 1

S102 OBTAIN A TRUST LEVEL OF AN APPLICATION ACCORDING TO SIGNATURE INFORMATION OF THE APPLICATION, THE APPLICATION COMPRISING AT LEAST ONE OF THE FOLLOWING: A TO-BE-DOWNLOADED APPLICATION, A TO-BE-INSTALLED APPLICATION, AND AN INSTALLED APPLICATION

S104 CONTROL A RIGHT OF THE APPLICATION ACCORDING TO THE TRUST LEVEL AND A PRESET MONITORING POLICY

(57) **Abstract**: Disclosed are a method and an apparatus for controlling an application right. The method comprises: obtaining a trust level of an application according to signature information of the application, the application comprising at least one of the following: a to-be-downloaded application, a to-be-installed application, and an installed application; and controlling a right of the application according to the trust level and a preset monitoring policy. By means of the present invention, the problem that there is no security system for controlling an application right in the prior art, and in a procedure that a mobile terminal downloads an application or running an application, since the application has no explicit right, a huge security hidden trouble exists in the mobile terminal is solved, and further provided is a secure and comprehensive method for monitoring an application right, so as to improve performances of the mobile terminal.

(57) **摘要**:

[见续页]

WO 2013/185413 A1

RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, 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))。

本发明公开了一种应用权限的控制方法及装置，其中，该方法包括：根据应用的签名信息获取应用的信任等级，其中，应用包括以下至少之一：待下载的应用、待安装的应用、已经安装的应用；依据信任等级和预置的监控策略对应用的权限进行控制。通过运用本发明，解决了相关技术中没有一种对应用权限进行控制的安全体系，移动终端在下载、运行应用等过程中，由于应用具有的权限不明确，致使移动终端存在很大的安全隐患的问题，进而提供了一种较为安全且全面的应用权限的监控方法，提升了移动终端的性能。

应用权限的控制方法及装置

技术领域

本发明涉及通信领域，具体而言，涉及一种应用权限的控制方法及装置。

背景技术

随着移动终端进入智能时代，在自由、开放的智能移动终端平台上，由于应用软件的开发者较多，质量也参差不齐，使其安全性难以得到保证。应用软件容易被植入含有恶意扣费、窃取用户隐私信息等行为的恶意代码，从而对安全造成严重威胁。

当前智能移动终端系统的安全监控能力相对薄弱，其只能保证对下载程序的稳定性、数据完整性进行检测，而无法有效的验证手机应用软件的来源，缺乏全面的测试及有效的验证机制，也无法对安装后的应用程序可能存在安全威胁行为进行有效的监控，因而无法对移动终端的安全性进行有效的保证。

相关技术中没有一种对应用权限进行控制的安全体系，移动终端在下载、运行应用等过程中，由于应用具有的权限不明确，致使移动终端存在很大的安全隐患。

发明内容

本发明提供了一种应用权限的控制方法及装置，以至少解决相关技术中没有一种对应用权限进行控制的安全体系，移动终端在下载、运行应用等过程中，由于应用具有的权限不明确，致使移动终端存在很大的安全隐患的问题。

根据本发明的一个方面，提供了一种应用权限的控制方法，包括：根据应用的签名信息获取应用的信任等级，其中，所述应用包括以下至少之一：待下载的应用、待安装的应用、已经安装的应用；依据所述信任等级和预置的监控策略对所述应用的权限进行控制。

优选地，根据应用的签名信息获取应用的信任等级包括：获取所述应用的签名信息；将所述签名信息与移动终端内的一个或多个预置证书的证书公钥进行匹配，并根据不同匹配结果设置所述应用不同的信任等级。

优选地，根据不同匹配结果设置所述应用不同的信任等级包括：记录所述签名信息与所述证书公钥匹配的个数或所述证书的名称；依据匹配的个数或所述证书的名称设置所述应用的信任等级。

优选地，依据所述信任等级和预置的监控策略对所述应用的权限进行控制包括：判断所述应用当前使用的权限是否为系统默认监控策略中的权限；如果是，则在所述系统默认监控策略中查找所述信任等级对应的策略，并根据所述对应的策略控制所述应用的权限。

优选地，在所述系统默认监控策略中查找所述信任等级对应的策略包括：判断是否存在与所述应用当前使用的权限对应的应用监控策略，其中，所述应用监控策略用于指示对权限使用情况进行监控的时间段；如果是，则在所述应用监控策略中查找所述信任等级对应的策略。

优选地，依据所述信任等级和预置的监控策略对所述应用的权限进行控制之后，还包括：将所述应用当前使用的权限的控制过程进行保存和分析以获得处理策略；或将所述应用当前使用的权限的控制过程同步到云端服务器以获得处理策略。

根据本发明的另一方面，提供了一种应用权限的控制装置，应用于移动终端，包括：获取模块，设置为根据应用的签名信息获取应用的信任等级，其中，所述应用包括以下至少之一：待下载的应用、待安装的应用、已经安装的应用；控制模块，设置为依据所述信任等级和预置的监控策略对所述应用的权限进行控制。

优选地，所述获取模块包括：获取单元，设置为获取所述应用的签名信息；匹配单元，设置为将所述签名信息与移动终端内的一个或多个预置证书的证书公钥进行匹配；设置单元，设置为根据不同匹配结果设置所述应用不同的信任等级。

优选地，所述控制模块包括：判断单元，设置为判断所述应用当前使用的权限是否为系统默认监控策略中的权限；查找单元，设置为在所述当前权限为系统默认监控策略中的权限的情况下，在所述系统默认监控策略中查找所述信任等级对应的策略；控制单元，设置为根据所述对应的策略控制所述应用的权限。

优选地，所述装置还包括：保存模块，设置为将所述应用当前使用的权限的控制过程进行保存和分析以获得处理策略；或设置为将所述应用当前使用的权限的控制过程同步到云端服务器以获得处理策略。

本发明采用了如下方法：将获取的信任等级加入到对应用权限的控制过程中，并为信任等级预置了相应的监控策略。通过运用本发明，解决了相关技术中没有一种对应用权限进行控制的安全体系，移动终端在下载、运行应用等过程中，由于应用具有的权限不明确，致使移动终端存在很大的安全隐患的问题，进而提供了一种较为安全且全面的应用权限的监控方法，提升了移动终端的性能。

附图说明

此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

图 1 是根据本发明实施例的应用权限的控制方法的流程图；

图 2 是根据本发明优选实施例一的应用信任等级获取的流程图；

图 3 是根据本发明优选实施例一的系统默认监控策略生成方法的流程图；

图 4 是根据本发明优选实施例一的应用控制策略生成过程的流程图；

图 5 是根据本发明优选实施例一的应用权限进行监控的流程图；

图 6 是根据本发明优选实施例二的系统默认监控策略生成过程的流程图；

图 7 是根据本发明优选实施例二的监控应用使用权限的处理流程；

图 8 是根据本发明实施例的应用权限的控制装置的结构框图一；

图 9 是根据本发明实施例的应用权限的控制装置的结构框图二；

图 10 是根据本发明实施例的应用权限的控制装置的结构框图三；

图 11 是根据本发明实施例的应用权限的控制装置的结构框图四；以及

图 12 是根据本发明优选实施例三的应用权限的控制装置的结构示意图。

具体实施方式

下文中将参考附图并结合实施例来详细说明本发明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。

相关技术中移动终端对应用监控能力较为薄弱，其主要表现在以下几个方面：（1）对应用软件的可信任等级缺乏有效的支持及验证手段，而应用的信任等级是有效监控权限使用的基础，这也就导致无法很好的对应用权限使用进行有效分类监控；（2）默认需监控权限相对比较多和监控过于繁琐，用户的实际需求可能只是对某些权限进行监控；（3）由于开发平台较为开放，因此对移动终端应用的权限使用控制比较宽松，绝大部分的权限应用开发者只需要声明即可获取，例如，手机设备上的敏感权限，其中，涉及用户付费类的权限（包括发送消息、拨打电话、上网等）、用户隐私信息类权限（包括消息记录、联系人记录、通话记录等）、手机设备本地连接类权限（包括 WIFI 连接、蓝牙连接等）等使用未进行有效的监控。

鉴于上述问题，本发明实施例提供了一种应用权限的控制方法，该方法的流程如图 1 所示，包括步骤 S102 至步骤 S104：

步骤 S102，根据应用的签名信息获取应用的信任等级，其中，应用包括以下至少之一：待下载的应用、待安装的应用、已经安装的应用；

步骤 S104，依据信任等级和预置的监控策略对应用的权限进行控制。

本实施例将获取的信任等级加入到对应用权限的控制过程中，并为信任等级预置了相应的监控策略，解决了相关技术中没有一种对应用权限进行控制的安全体系，移动终端在下载、运行应用等过程中，由于应用具有的权限不明确，致使移动终端存在很大的安全隐患的问题，进而提供了一种较为安全且全面的应用权限的监控方法，提升了移动终端的性能。

在实施过程中，根据应用的签名信息获取应用的信任等级可以包括：获取应用的签名信息；将签名信息与移动终端内的一个或多个预置证书的证书公钥进行匹配，并根据不同匹配结果设置应用不同的信任等级。

其中，根据不同匹配结果设置应用不同的信任等级还可以包括：记录签名信息与证书公钥匹配的个数或证书的名称；依据匹配的个数设置或证书的名称应用的信任等级。在实施的过程中，信任等级可以以信任和非信任的形式体现，也可以以不同信任等级的形式体现，例如一级信任，二级信任等。

在上述步骤实施的过程中，当以不同信任等级的形式体现时，还可以分为两种情况。第一种，信任等级可以通过记录证书的名称来进行设置，例如，“厂商信任级别”、“运营商信任级别”、“第 3 方合作厂商信任级别”等，则通过其中某个证书就可以获得某个证书对应的信任级别；第二种，信任等级也可以根据通过不同认证证书的个数

对级别进行设置，例如，通过两个认证证书，则级别设置为一级，即“一级信任级别”，或者设置通过两个认证证书的情况下该应用被设置为二级等。

当信任等级以信任和非信任的形式体现时，则可以设定一个匹配阈值，即当该应用的签名信息与证书公钥匹配的个数达到一个预设的个数时，则确定该应用的信任等级为信任，当该信任应用触及敏感权限时，可以选择不对其操作权限进行控制；上述匹配阈值还可以设置为通过某一固定证书，例如，只要与运营商证书匹配后，则确定该应用的信任等级是信任，只要无法通过运营商证书的，都认为是非信任。上述信任等级可根据不同用户的不同需求进行相应的设定。

在步骤 S102 执行后，判断应用当前使用的权限是否为系统默认监控策略中的权限。如果是，说明该权限是用户重视的权限，则在系统默认监控策略中查找信任等级对应的策略，并根据对应的策略控制应用的权限。如果不是系统默认监控策略中的权限，则可以不对该权限进行控制。

在系统默认监控策略中存在该权限时，需要在系统默认监控策略中查找该应用信任等级对应的策略。执行过程中，需要判断是否存在当前使用的权限对应的应用监控策略。如果存在应用监控策略，则可以在应用监控策略中查找信任等级对应的策略，例如，播放器的信任等级为 3 级，当检测到该播放器访问联系人数据库时，则判断联系人数据库是否为系统默认监控策略中的监控权限。如果是，则在系统默认监控策略中查找信任等级为 3 级的播放器的控制策略。如果 3 级信任等级及 3 级以上的信任等级触及该敏感权限时不进行控制，则不对该播放器访问联系人数据库进行控制；如果 1 至 3 级信任等级的应用触及该权限时需要进行控制，则记录该控制过程或对该播放器访问联系人数据库时进行报警，或同时记录并报警。

在一个实施例中，上网权限为敏感权限，当移动终端检测一个游戏应用在凌晨 3 点钟使用了上网权限，则将上网权限的使用过程进行记录，以进行后续处理。

在不存在当前权限的应用监控策略时，由于当前权限还没有对应的应用监控策略记录，因此，系统可以弹出提示框提醒用户，等待接收用户设置该权限监控策略。然后将用户对于该权限的监控设置（全时段监控/全时段不监控/时段内监控）转化为权限使用的应用监控策略，保存和更新系统记录的监控策略记录值。此时，系统具备了应用监控策略，则可以根据该策略对该权限使用进行监控。

在上述步骤结束后，可以将应用当前使用的权限的控制过程进行分析以获得处理策略，或将应用当前使用的权限的控制过程同步到云端服务器以获得处理策略。如果选择本地对应用使用权限的过程进行分析，则可以将该过程的记录呈现给用户，用户

根据实际情况进行处理；如果选择同步到云端服务器以获得处理策略的方式，则云端服务器根据同步的过程进行分析，并将分析结果发送给移动终端，以便用户根据云端服务器的分析获得的处理策略进行处理。

优选实施例一

本优选实施例提供了一种应用权限的控制方法，在本优选实施例中，以移动终端为手机为例，进行说明。

图 2 示出应用信任等级获取的流程，包括步骤 S202 至步骤 S212：

步骤 S202，开机扫描或应用安装时进行应用包信息解析处理。在开机进行应用扫描或者是进行新应用的安装时，首先进行对应用包进行解压操作，并完成对应用包信息的解析处理。

步骤 S204，根据对应用包解析处理的结果，提取出应用的签名信息数据，并记录下来。

步骤 S206，将应用签名信息与手机预制数字证书的公钥文件进行认证处理，判断认证是否通过。如果认证通过执行步骤 S208，否则执行步骤 S210。

步骤 S208，赋予认证通过的数字证书所对应的信任级别，例如：“厂商信任级别”、“运营商信任级别”、“第 3 方合作厂商信任级别”等；或者也可以根据通过不同认证证书的个数对级别进行设置，例如，通过一个认证证书，则级别设置为一级，即“一级信任级别”，或者设置通过两个认证证书的情况下该应用被设置为一级。执行完该步骤则进入步骤 S212。

步骤 S210，赋予该应用“不可信任级别”。

步骤 S212，将认证得到的应用信任级别记录到应用对应的属性配置文件中，作为应用的一个常态属性对待。

如图 3 所示，该图为系统默认监控策略生成方法的流程图，该流程包括步骤 S302 至步骤 S306：

步骤 S302，加载系统默认监控策略的配置文件。实施中，系统开机时初始化时，首先会在指定的系统目录加载预置好的系统默认监控策略配置文件。

步骤 S304，进行系统默认监控策略配置文件的解析处理，得到各应用模块所需监控的权限列表。

步骤 S306，将解析得到的各应用模块所需监控的权限列表记录到内存数据结构中，生成系统默认监控策略。

图 4 是应用控制策略生成过程的流程图，该流程包括步骤 S402 至步骤 S414：

步骤 S402，当监测到当前应用使用到系统中的敏感权限时，进入步骤 404。其中，在该步骤中，敏感权限可以根据用户的需求进行自定义，例如，涉及用户付费类的权限，或用户隐私信息类权限等。

步骤 S404，判断该权限是否属于系统默认控制策略所需控制的权限。若不属于系统默认控制策略所需控制的权限，执行步骤 S406，若属于，则执行步骤 S408。

步骤 S406，忽略非系统默认监控策略所需监控的权限使用。

步骤 S408，判断是否已经存在该权限使用的应用监控策略。若不存在该权限使用的应用监控策略，则执行步骤 S410，若存在，执行步骤 S412。

步骤 S410，没有该权限的应用监控策略，不做监控处理。

步骤 S412，按应用监控策略进行监控。

步骤 S414，记录应用的权限使用情况。

图 5 示出了对应用权限进行监控的总体流程，下面结合图 5 对整个监控过程进行说明。该过程包括步骤 S502 至步骤 S518：

步骤 S502，当监测到应用系统敏感权限被访问时，进入步骤 S504。

步骤 S504，判断该权限是否属于系统默认控制策略中定义所需控制的权限。在该步骤实施的过程中，需在系统默认控制策略中进行查找，若不属于系统默认控制策略中的权限，则执行步骤 S506，若属于，则执行步骤 S508。

步骤 S506，由于该权限为非系统默认控制策略所需控制的权限，因此对该权限的使用不进行监控。例如，当用户访问的敏感权限涉及手机设备本地连接类权限时，其不在系统默认控制策略中，则不对该权限进行控制。

步骤 S508，判断是否已经存在该权限的应用监控策略。若存在，则执行步骤 S510，若不存在则执行步骤 512。

步骤 S510，获取该权限的应用监控策略记录，并根据该应用监控策略对权限的使用进行监控。

步骤 S512，由于当前权限还没有对应的权限监控策略的记录，因此，弹出提示框提醒用户当前系统敏感权限正在被使用，并且没有对该权限进行监控，等待接收用户对于该权限监控的进一步设置。

步骤 S514，接收到用户对于该权限的监控策略的设置。

步骤 S516，将用户对于该权限的监控设置转化为权限使用的应用监控策略，保存和更新系统记录的监控策略记录值，其中，监控设置可以为全时段监控、全时段不监控、时段内监控等设置。

步骤 S518，根据用户的设置的应用监控策略进行监控。

该优选实施的实施，能够有效的对手机终端应用进行基于信任等级的分类，并根据应用信任等级分类来进行关键权限使用的分类管理，该实施例可以针对厂商或用户的不同控制需求来对手机关键权限控制的可定制化及可动态调整化。用户通过运用本实施例，可以很容易的实现对手机终端关键敏感权限组的管理和控制的目的，能够有效的对手机应用可能存在的安全威胁行为进行管理控制，有效的保证了手机的安全性。

优选实施例二

本发明实施例可以通过软件实现对智能手机上最易被恶意入侵和最需要重点保护的敏感权限组的监控，实现被监控的权限组可以包括：发送消息、呼叫、网络流量访问控制权限、访问联系人记录，消息记录、手机设备信息、地理位置信息、wifi 连接、蓝牙连接。在实施过程中，均以“非可信应用”的权限使用的监控为例进行说明，其它信任等级下应用权限使用的监控原理及处理流程均相似。

在本优选实施例中，设置系统默认监控策略，将发送消息、呼叫、网络流量访问等加入到“ 非可信应用信任等级”需要控制权限中，配置文件以 xml 文件格式定义，定义的配置文件内容如下：

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>

<sysControlPermission>
```

```
<trustLevel name="unApproved">
<permission name=" SEND_SMS" />
<permission name=" CALL_PHONE" />
<permission name="ACCESS_ INTERNET" />
<permission name="ACCESS_MESSAGE" />
<permission name=" ACCESS_CONTACTS" />
<permission name=" ACCESS_CALLLOG" />
<permission name=" ACCESS_LOCATION" />
<permission name=" ACCESS_DEVICE_INFO" />
<permission name="WIFI" />
<permission name=" BLUETOOTH" />
</trustLevel >
</sysControlPermission>
```

其中，sysControlPermission 标签代表这是系统默认控制权限；trustLevel 标签代表权限信任等级，“unApproved”代表权限不可信需要监控； permission 标签代表了信任等级下所需监控的权限 SEND_SMS 代表发送消息权限； CALL_PHONE 代表拨打电话权限；ACCESS_ INTERNET 代表网路流量访问权限；ACCESS_MESSAGE 代表访问消息记录权限； ACCESS_CONTACTS 代表访问联系人记录权限；ACCESS_MESSAGE 代表访问消息记录权限；ACCESS_CALLLOG 代表访问通话记录权限；ACCESS_LOCATION 代表访问个人地理位置信息（包括 GPS 定位以及基站定位）权限；ACCESS_DEVICE_INFO 代表访问手机设备信息权限（包括 IMEI、IMSI 以及本机号码等）；WIFI 代表使用 wifi 进行本地网络连接权限； BLUETOOTH 代表通过蓝牙建立本地连接权限。优选地，可以根据需要对列出的监控权限进行增减修改，控制的原理和流程都是相似的。

如图 6 所示，该图是权限的系统默认监控策略生成过程的流程图，该流程包括步骤 S602 至步骤 S606：

步骤 S602，系统开机时初始化时，首先会在指定的系统目录加载预置好的系统默认监控策略配置文件。

步骤 S604，进行系统默认监控策略配置文件的解析处理，解析得到“不可信需监控权限”所需监控的权限列表。

步骤 S606，将解析得到所需监控的权限列表记录到内存数据中，形成系统默认监控策略。

下面结合图 7 对本优选实施例进行说明。图 7 中监控应用使用权限的处理流程包括步骤 S702 至步骤 S724：

步骤 S702，当监测到应用使用到权限时，执行步骤 S704。例如，一个播放应用在使用的过程中，被记录到其访问联系人数据库，则此时执行步骤 S704。

步骤 S704，获取应用的权限，将该权限与系统默认权限列表进行比较。

步骤 S706，判断该权限是否属于系统默认控制的权限。若不属于系统默认控制的权限，则执行步骤 S708，若属于，执行步骤 S710。

步骤 S708，由于权限为非系统默认控制权限，因此对该权限的使用情况不做监控。

步骤 S710，判断是否已经存在对该权限使用的应用监控策略。若存在，则执行步骤 S712，否则执行步骤 S714。

步骤 S712，获取该权限的应用监控策略记录，并根据监控策略进行权限的监控。

步骤 S714，由于当前权限还没有对应的应用监控策略记录，因此，系统会弹出提示框提醒用户，等待接收用户设置该权限监控策略。

步骤 S716，接收到用户对于该权限的监控策略。

步骤 S718，将用户对于该权限的监控设置（全时段监控/全时段不监控/时段内监控）转化为权限使用的应用监控策略，保存和更新系统记录的监控策略记录值。

步骤 S720，根据用户的选择对该权限使用进行监控。

步骤 S722，把监控信息保存或同步到云服务端。

步骤 S724，根据分析策略对保存的数据分析或将云端处理策略反馈至用户。

本优选实施例可以很好的根据应用的不同进行权限控制，可以分别监控和管理手机应用的权限（发送消息、拨打电话、网络流量访问等），可以根据用户的实际监控需求和场景来灵活调整应用权限的应用监控策略。本优选实施例可以实现对手机终端权限监控管理的目的，能够有效发现、即时提醒和阻止对手机终端权限被恶意侵害的安全威胁行为，从而有效的保证了手机终端权限的安全性。

本发明实施例还提供了一种应用权限的控制装置，该装置可以应用于移动终端中对应用权限安全性的检测，该装置的结构框图可以如图 8 所示，包括：获取模块 **10**，设置为根据应用的签名信息获取应用的信任等级，其中，应用包括以下至少之一：待下载的应用、待安装的应用、已经安装的应用；控制模块 **20**，与获取模块 **10** 耦合，设置为依据信任等级和预置的监控策略对应用的权限进行控制。

其中，图 9 所示装置的获取模块 **10** 可以包括：获取单元 **102**，设置为获取应用的签名信息；匹配单元 **104**，与获取单元 **102** 耦合，设置为将签名信息与移动终端内的一个或多个预置证书的证书公钥进行匹配；设置单元 **106**，与匹配单元 **104** 耦合，设置为根据不同匹配结果设置应用不同的信任等级。

在实施过程中，获取模块 **10** 还可以设置为记录签名信息与证书公钥匹配的个数；依据匹配的个数设置应用的信任等级。

在一个优选实施例中，应用权限的控制装置还可以如图 10 所示，其控制模块 **20** 可以包括：判断单元 **202**，设置为判断应用当前使用的权限是否为系统默认监控策略中的权限；查找单元 **204**，与判断单元 **202** 耦合，设置为在当前权限为系统默认监控策略中的权限的情况下，在系统默认监控策略中查找信任等级对应的策略；控制单元 **206**，与查找单元 **204** 耦合，设置为根据对应的策略控制应用的权限。

在实施过程中，控制模块 **20** 还可以设置为判断是否存在当前权限的应用监控策略；如果是，则在应用监控策略中查找信任等级对应的策略。

图 11 示出的应用权限的控制装置还包括保存模块 **30**，与控制模块 **20** 耦合，设置为将应用当前使用的权限的控制过程进行保存和分析以获得处理策略；或将应用当前使用的权限的控制过程同步到云端服务器以获得处理策略。

下面结合附图及优选实施例对上述实施例中的应用权限的控制装置进行说明。

优选实施例三

本优选实施例提供了一种应用权限的控制装置，该装置的实现基于签名认证的应用信任等级分级机制，能够将手机中预制/安装的应用进行基于信任等级的有效分类；建立对需监控应用的权限的监控管理策略，并且可以实现根据用户需求对监控策略的可配制化，即可灵活调整各应用所需监控的权限；同时，具有基于应用为监控单元的权限使用监控策略设置能力，即用户可以根据实际需要分别定义应用对权限使用的监控策略；在应用信任等级及权限监控策略和日志分析策略机制的支持下，实现对手机系统关键敏感权限的动态监控功能。

在本优选实施例中，各模块的命名与上述实施例中装置的模块命名略有不同，但本实施例中各模块的组合能实现与上述实施例装置相同的功能。本实施例包括如下模块：

（1）认证模块：实现应用信任等级认证功能，在开机扫描手机预制应用/下载安装应用时，认证模块会解析应用的签名信息，同时与手机预制的证书（包括预制的“厂商签名证书”、“ 运营商签名证书”、“第 3 方合作厂商签名证书”等）进行认证，根据应用的签名信息与证书公钥的认证结果，赋予应用不同的信任等级属性。

（2）监控策略模块：采用基于配置文件方式的策略定义机制，应用权限访问监控策略分为“系统默认监控策略”以及“应用监控策略”2 级管理策略体系。其中，“系统默认监控策略”定义了各级任级别下应用所需要监控的敏感权限，系统初始化时，通过解析预制的策略配置文件得到。“应用监控策略”记录了各具体应用本身对各敏感权限使用的监控策略（全时段监控/全时间不监控/时段监控），具体策略通过动态记录用户的权限监控设置操作生成。

（3）权限使用日志模块：实现对监控流程的保存，在（1）（2）扩展的应用信任等级以及监控策略机制的支持下，实现对手机上最易被滥用和需要重点保护的敏感权限组的动态监控。应用在使用到系统敏感权限时，首先，权限监控模块会获取应用所属的信任等级属性；其次，依据应用信任等级通过监控策略模块来确定该权限的具体监控策略；并根据确认的监控策略对应用对该权限使用进行监控，监控的形式包括：全时段监控、全时段不监控、时段监控，在没有查到监控形式的情况，弹出提示后根据用户的设置动态保存/更新对应的“应用控制策略”，把监控的应用使用权限情况记录到日志中，保存在本地或更新到云端服务器；最后根据本地的日志分析策略或云端服务器返回的处理意见反馈给用户。

（4）权限使用监控模块：用于实现后台监控运行。

在具体实施过程中，本优选实施例的结构示意图可以如图 12 所示，系统初始化时，首先调用监控策略模块，加载和解析预制的监控策略配置文件，然后根据解析的结果生成系统默认监控权限策略。

系统启动时，调用认证模块，随后加载权限使用监控模块在后台监控。当监控到应用使用手机关键敏感权限时，会把权限使用情况数据传入权限使用日志模块进行记录，在记录后会进入分析权限使用策略模块的分析流程。监控权限使用模块通过与日志模块及监控策略模块协同工作，最终完成对应用权限使用的监控及用户建议功能。

从以上的描述中，可以看出，上述实施例实现了如下技术效果的至少之一：

本发明采用了如下方法：将获取的信任等级加入到对应用权限的控制过程中，并为信任等级预置了相应的监控策略。通过运用本发明，解决了相关技术中没有一种对应用权限进行控制的安全体系，移动终端在下载、运行应用等过程中，由于应用具有的权限不明确，致使移动终端存在很大的安全隐患的问题，进而提供了一种较为安全且全面的应用权限的监控方法，提升了移动终端的性能。

显然，本领域的技术人员应该明白，上述的本发明的各模块或各步骤可以用通用的计算装置来实现，它们可以集中在单个的计算装置上，或者分布在多个计算装置所组成的网络上，可选地，它们可以用计算装置可执行的程序代码来实现，从而，可以将它们存储在存储装置中由计算装置来执行，并且在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤，或者将它们分别制作成各个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样，本发明不限制于任何特定的硬件和软件结合。

以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权 利 要 求 书

1. 一种应用权限的控制方法，包括：

根据应用的签名信息获取应用的信任等级，其中，所述应用包括以下至少之一：待下载的应用、待安装的应用、已经安装的应用；

依据所述信任等级和预置的监控策略对所述应用的权限进行控制。

2. 根据权利要求 1 所述的方法，其中，根据应用的签名信息获取应用的信任等级包括：

获取所述应用的签名信息；

将所述签名信息与移动终端内的一个或多个预置证书的证书公钥进行匹配，并根据不同匹配结果设置所述应用不同的信任等级。

3. 根据权利要求 2 所述的方法，其中，根据不同匹配结果设置所述应用不同的信任等级包括：

记录所述签名信息与所述证书公钥匹配的个数或所述证书的名称；

依据匹配的个数或所述证书的名称设置所述应用的信任等级。

4. 根据权利要求 1 至 3 中任一项所述的方法，其中，依据所述信任等级和预置的监控策略对所述应用的权限进行控制包括：

判断所述应用当前使用的权限是否为系统默认监控策略中的权限；

如果是，则在所述系统默认监控策略中查找所述信任等级对应的策略，并根据所述对应的策略控制所述应用的权限。

5. 根据权利要求 4 所述的方法，其中，在所述系统默认监控策略中查找所述信任等级对应的策略包括：

判断是否存在与所述应用当前使用的权限对应的应用监控策略，其中，所述应用监控策略用于指示对权限使用情况进行监控的时间段；

如果是，则在所述应用监控策略中查找所述信任等级对应的策略。

6. 根据权利要求 1 所述的方法，其中，依据所述信任等级和预置的监控策略对所述应用的权限进行控制之后，还包括：

将所述应用当前使用的权限的控制过程进行保存和分析以获得处理策略；或将所述应用当前使用的权限的控制过程同步到云端服务器以获得处理策略。

7. 一种应用权限的控制装置，应设置为移动终端，包括：

获取模块，设置为根据应用的签名信息获取应用的信任等级，其中，所述应用包括以下至少之一：待下载的应用、待安装的应用、已经安装的应用；

控制模块，设置为依据所述信任等级和预置的监控策略对所述应用的权限进行控制。

8. 根据权利要求 7 所述的装置，其中，所述获取模块包括：

获取单元，设置为获取所述应用的签名信息；

匹配单元，设置为将所述签名信息与移动终端内的一个或多个预置证书的证书公钥进行匹配；

设置单元，设置为根据不同匹配结果设置所述应用不同的信任等级。

9. 根据权利要求 7 或 8 所述的装置，其中，所述控制模块包括：

判断单元，设置为判断所述应用当前使用的权限是否为系统默认监控策略中的权限；

查找单元，设置为在所述当前权限为系统默认监控策略中的权限的情况下，在所述系统默认监控策略中查找所述信任等级对应的策略；

控制单元，设置为根据所述对应的策略控制所述应用的权限。

10. 根据权利要求 7 所述的装置，其中，所述装置还包括：

保存模块，设置为将所述应用当前使用的权限的控制过程进行保存和分析以获得处理策略；或将所述应用当前使用的权限的控制过程同步到云端服务器以获得处理策略。

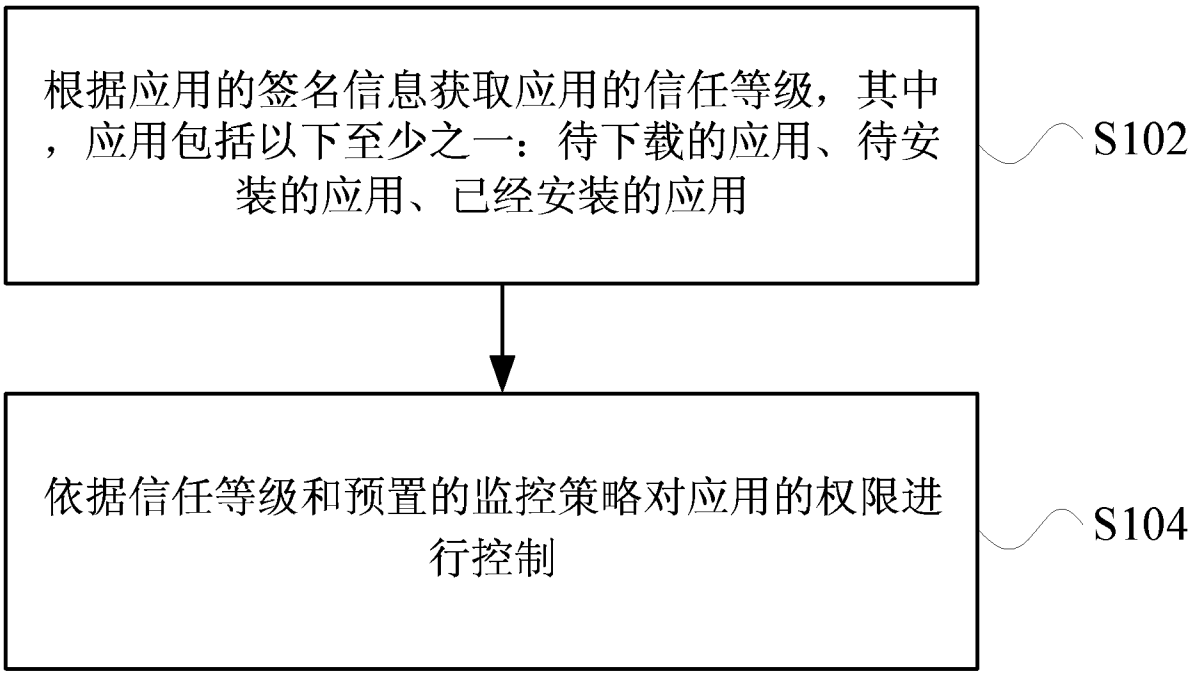
根据应用的签名信息获取应用的信任等级，其中，应用包括以下至少之一：待下载的应用、待安装的应用、已经安装的应用
S102
依据信任等级和预置的监控策略对应用的权限进行控制
S104

图 1

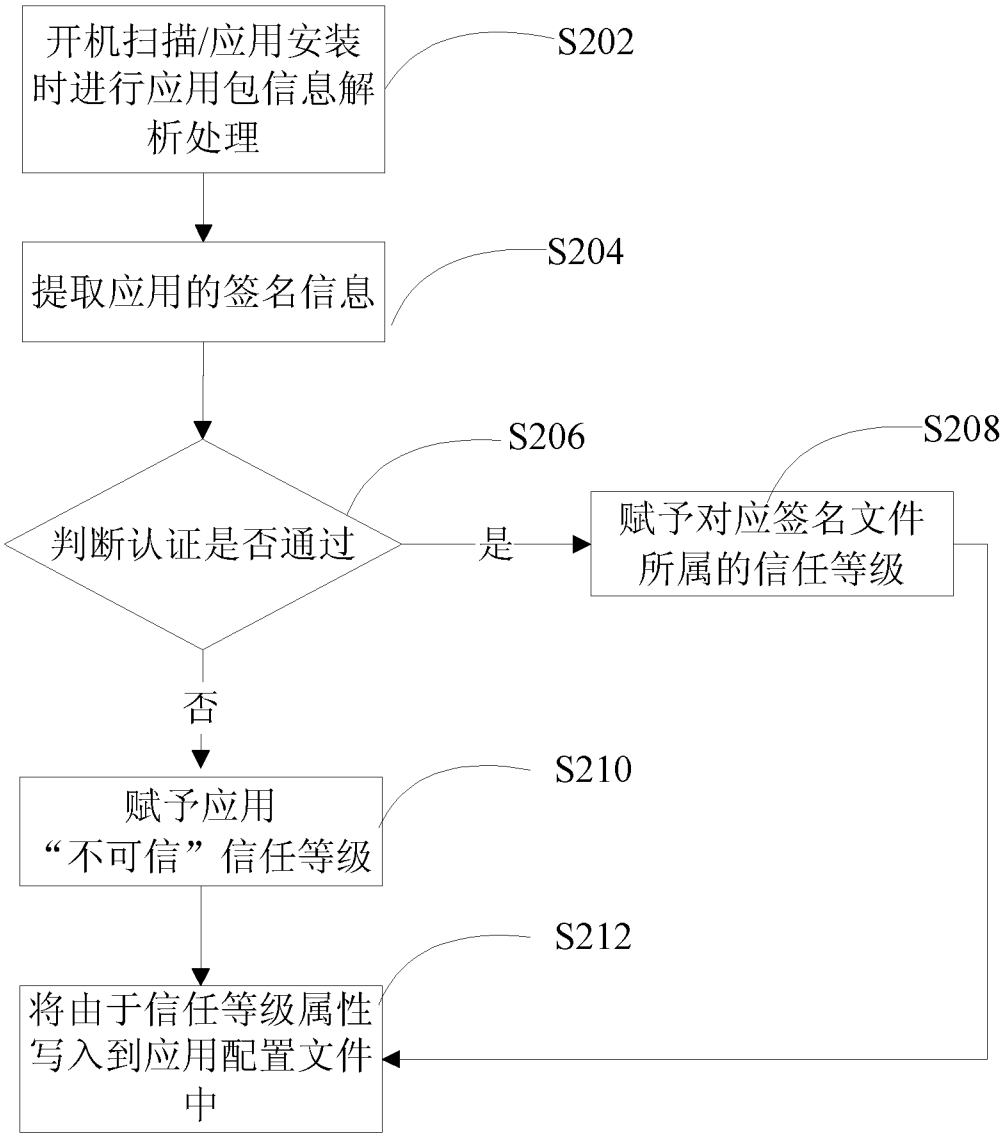
开机扫描/应用安装时进行应用包信息解析处理
S202
提取应用的签名信息
S204
判断认证是否通过
S206
是
赋予对应签名文件所属的信任等级
S208
否
赋予应用“不可信”信任等级
S210
将由于信任等级属性写入到应用配置文件中
S212

图 2

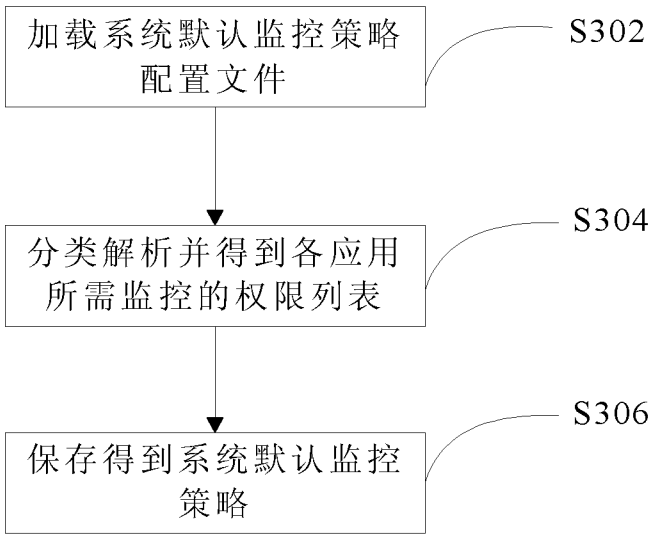
加载系统默认监控策略配置文件
S302
分类解析并得到各应用所需监控的权限列表
S304
保存得到系统默认监控策略
S306

图 3

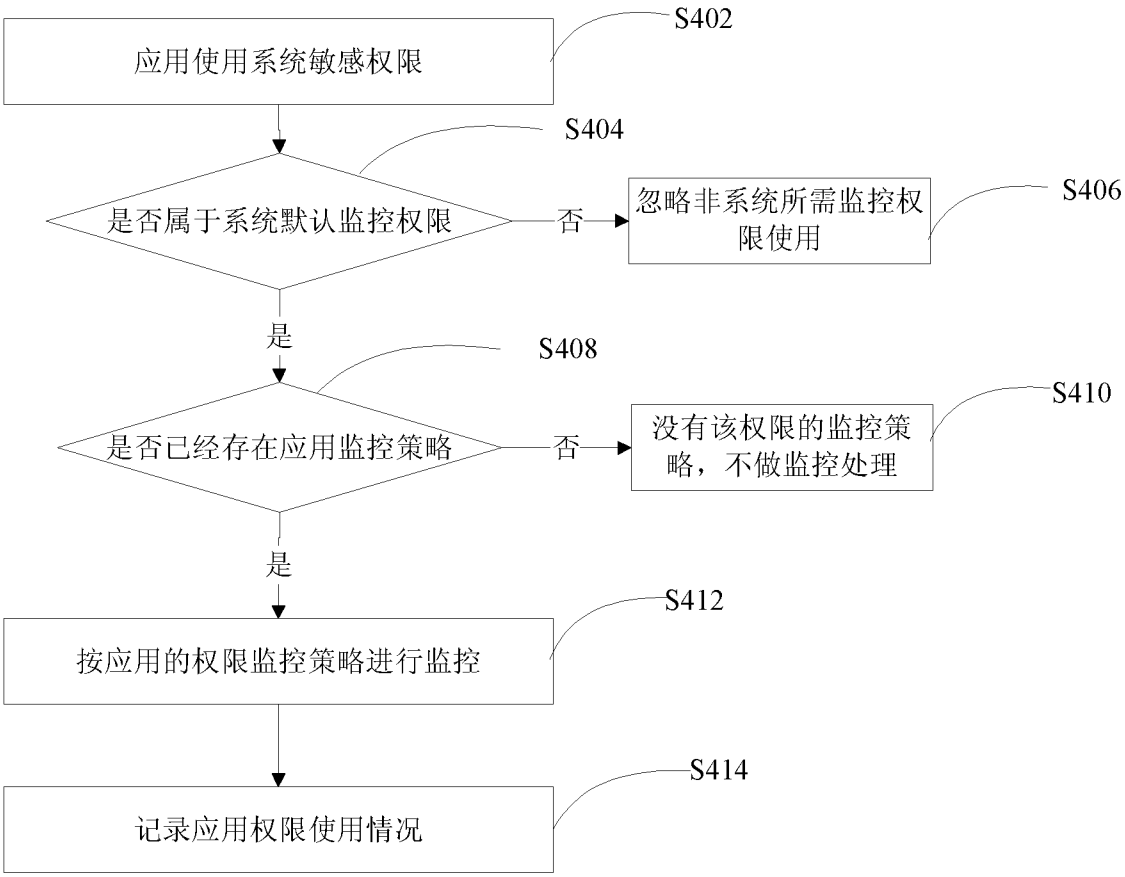
应用使用系统敏感权限
S402
是否属于系统默认监控权限
S404
否
忽略非系统所需监控权限使用
S406
是
是否已经存在应用监控策略
S408
否
没有该权限的监控策略，不做监控处理
S410
是
按应用的权限监控策略进行监控
S412
记录应用权限使用情况
S414

图 4

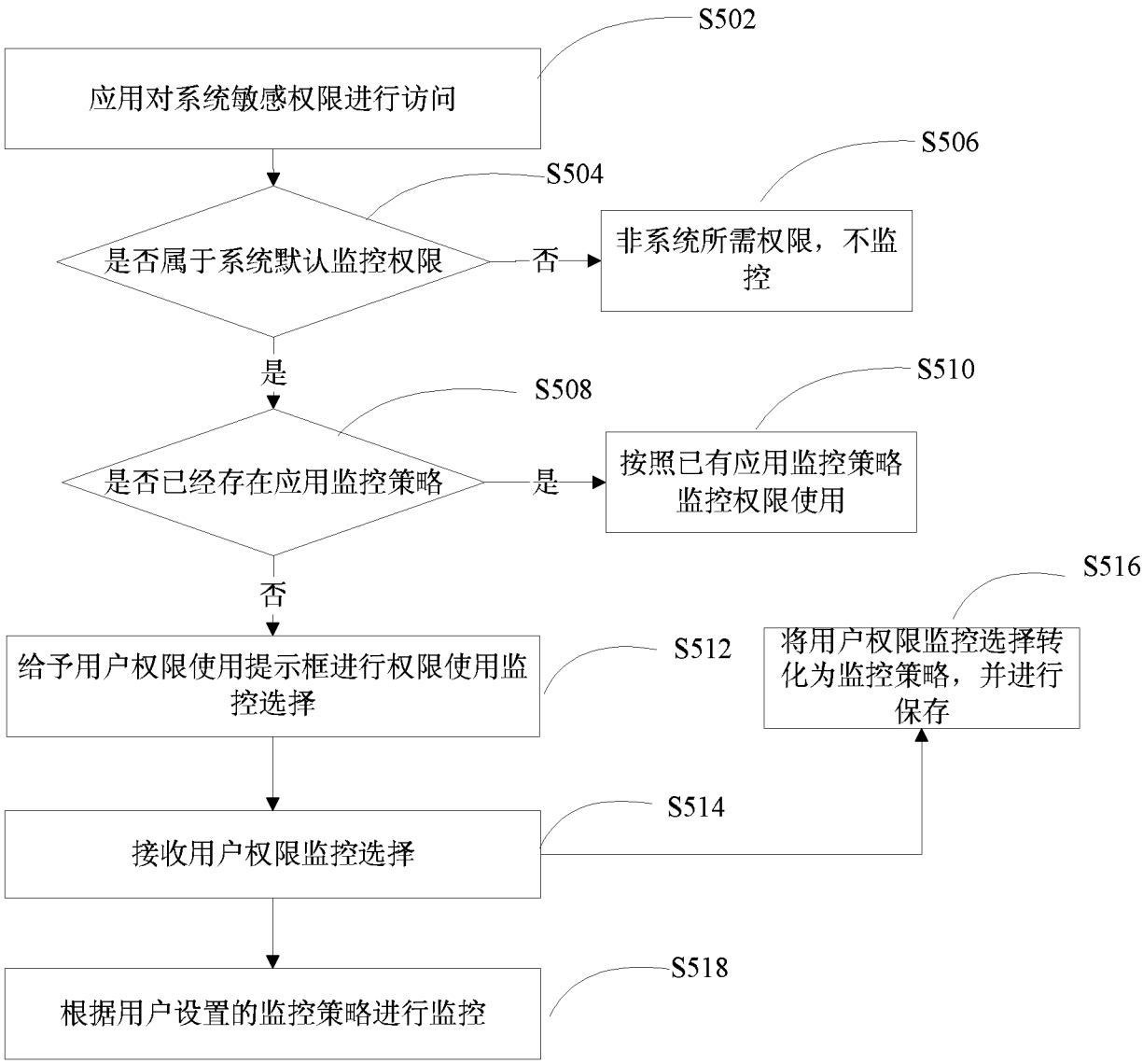
S502
应用对系统敏感权限进行访问
S504
是否属于系统默认监控权限
否
S506
非系统所需权限，不监控
是
S508
是否已经存在应用监控策略
是
S510
按照已有应用监控策略监控权限使用
否
S512
给予用户权限使用提示框进行权限使用监控选择
S514
接收用户权限监控选择
S516
将用户权限监控选择转化为监控策略，并进行保存
S518
根据用户设置的监控策略进行监控

图 5

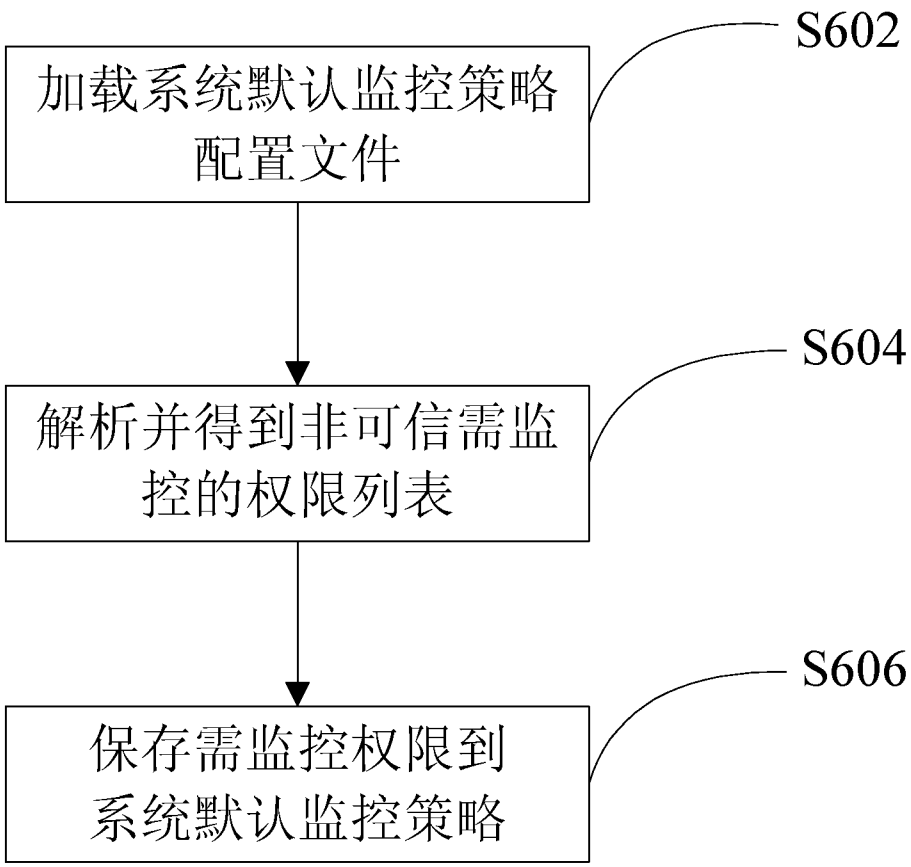
S602
加载系统默认监控策略配置文件
S604
解析并得到非可信需监控的权限列表
S606
保存需监控权限到系统默认监控策略

图 6

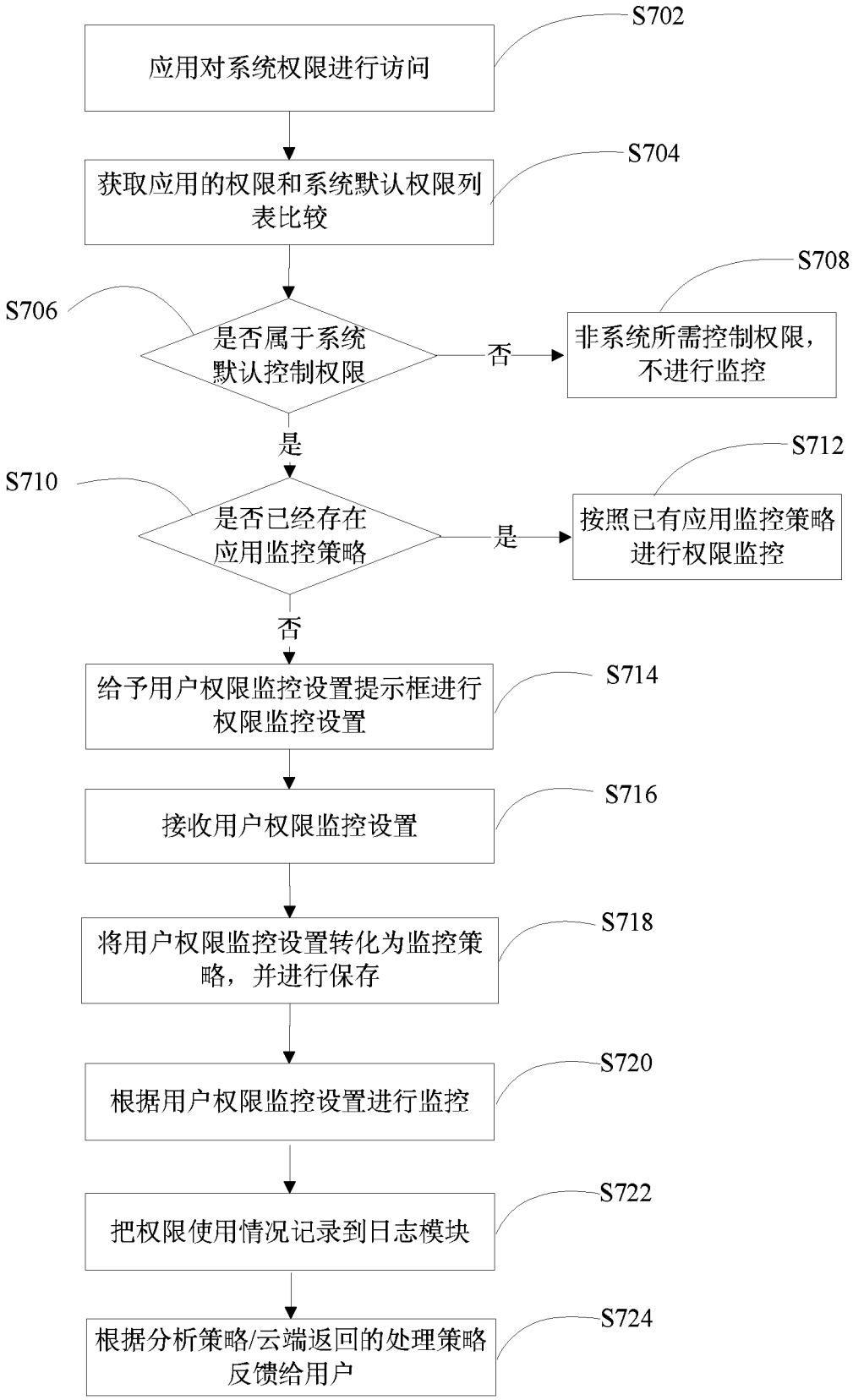
S702
应用对系统权限进行访问
S704
获取应用的权限和系统默认权限列表比较
S706
是否属于系统默认控制权限
否
S708
非系统所需控制权限，不进行监控
是
S710
是否已经存在应用监控策略
是
S712
按照已有应用监控策略进行权限监控
否
S714
给予用户权限监控设置提示框进行权限监控设置
S716
接收用户权限监控设置
S718
将用户权限监控设置转化为监控策略，并进行保存
S720
根据用户权限监控设置进行监控
S722
把权限使用情况记录到日志模块
S724
根据分析策略/云端返回的处理策略反馈给用户

图 7

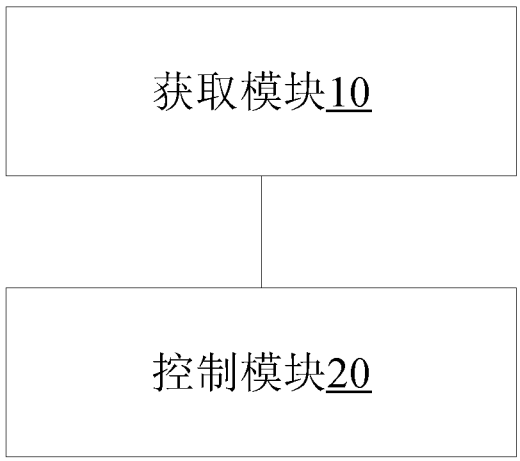

图 8

图 9


获取模块10
控制模块20
判断单元202
查找单元204
控制单元206

图 10


获取模块10
控制模块20
保存模块30

图 11

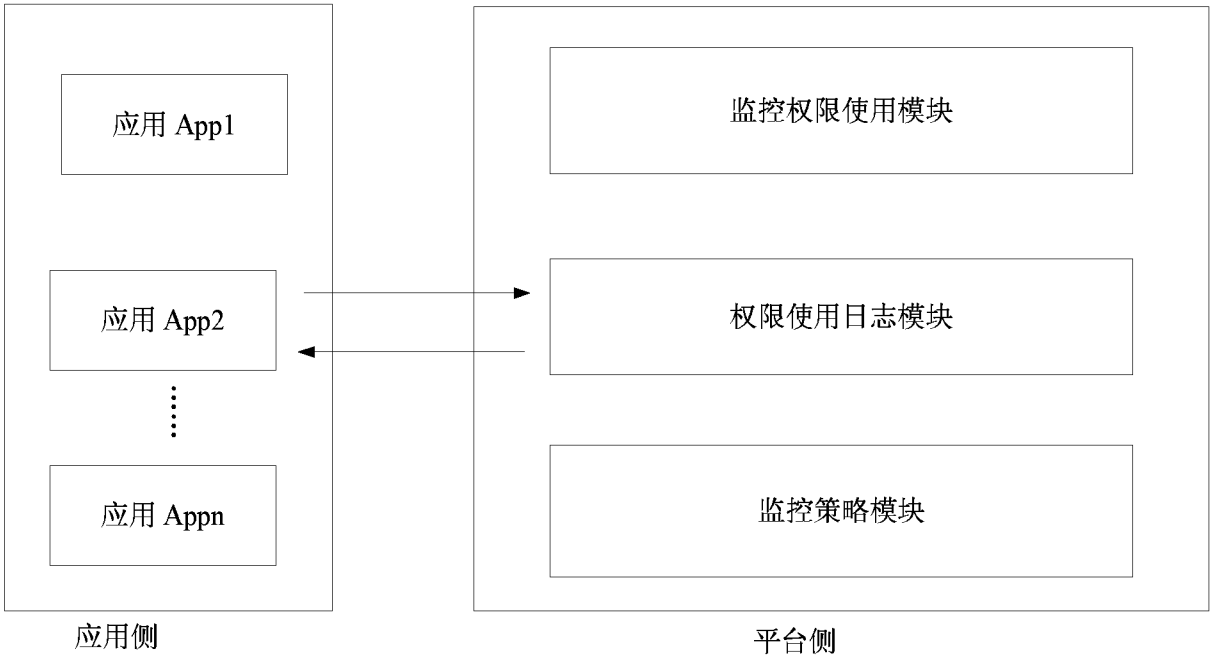

图 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2012/079659

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/00 (2009.01) 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)

IPC: H04W, G06F, H04L

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)

WPI, EPODOC, CNPAT, CNKI: cloud, terminal, portable, mobile phone, control, Mobile, application, authority, Trust, signature, policy, monitor

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102404727 A (ZTE CORP.), 04 April 2012 (04.04.2012), description, pages 3-11, and figures 1-14	1-10
A	CN 102420902 A (ZTE CORP.), 18 April 2012 (18.04.2012), the whole document	1-10
A	CN 101707652 A (LI, Dongsheng), 12 May 2010 (12.05.2010), the whole document	1-10
A	US 2010/0332848 A1 (RESEARCH IN MOTION LIMITED), 30 December 2010 (30.12.2010), 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
29 January 2013 (29.01.2013)	**28 February 2013 (28.02.2013)**
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 **TANG, Yan** Telephone No.: (86-10) **62414047**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2012/079659

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102404727 A	04.04.2012	None	
CN 102420902 A	18.04.2012	None	
CN 101707652 A	12.05.2010	None	
US 2010/0332848 A1	30.12.2010	None	

国际检索报告

国际申请号
PCT/CN2012/079659

A. 主题的分类

H04W 12/00 (2009.01) 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)

IPC: H04W, G06F, H04L

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）)

WPI,EPODOC,CNPAT,CNKI: 应用，权限，信任，签名，云，移动，终端，便携，手机，监控，控制, Mobile, application, authority, Trust, signature, policy, monitor

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	CN102404727A (中兴通讯股份有限公司) 04.4 月 2012(04.04.2012) 说明书第 3-11 页，图 1-14	1-10
A	CN102420902A (中兴通讯股份有限公司) 18.4 月 2012(18.04.2012) 全文	1-10
A	CN101707652A (李东声) 12.5 月 2010(12.05.2010) 全文	1-10
A	US2010/0332848A1 (RESEARCH IN MOTION LIMITED) 30.12 月 2010(30.12.2010) 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
29.1 月 2013(29.01.2013)	**28.2 月 2013 (28.02.2013)**
ISA/CN 的名称和邮寄地址： 中华人民共和国国家知识产权局 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 唐嫣 电话号码：(86-10) **62414047**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2012/079659

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN102404727A	04.04.2012	无	
CN102420902A	18.04.2012	无	
CN101707652A	12.05.2010	无	
US2010/0332848A1	30.12.2010	无	