(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103218564 A
(43)申请公布日 2013.07.24

(21)申请号 201310111513.5

(22)申请日 2013.04.01

(71)申请人 广东欧珀移动通信有限公司
地址 523841 广东省东莞市长安镇乌沙海滨路 18 号

(72)发明人 张寅祥 林志泳

(74)专利代理机构 深圳中一专利商标事务所 44237
代理人 张全文

(51)Int.Cl.
G06F 21/55(2013.01)

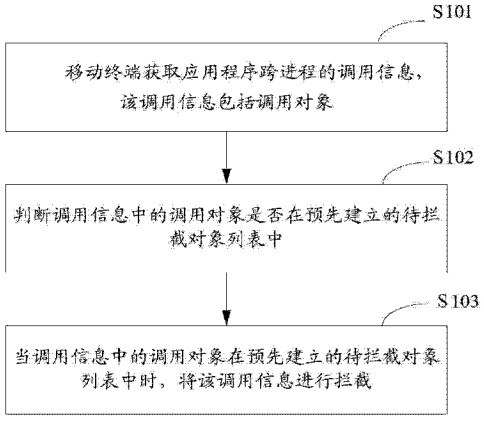
权利要求书2页 说明书6页 附图5页

(54)发明名称

一种移动终端保护方法及装置

(57)摘要

本发明适用于移动终端技术领域，提供了一种移动终端保护方法及装置，包括：获取移动终端中应用程序跨进程的调用信息，所述调用信息包括调用对象；判断调用信息中的调用对象是否在预先建立的待拦截对象列表中；当调用信息中的调用对象在所述预先建立的待拦截对象列表中时，将所述调用信息进行拦截。在本发明实施例中，判断调用信息中的调用对象是否在预先建立的待拦截对象列表中，当调用信息中的调用对象在预先建立的待拦截对象列表中时，将调用信息进行拦截，解决了现有移动终端对自身具有缺陷的应用程序导致的安全隐患缺乏防御的问题，提高了移动终端内部信息的安全性。



CN 103218564 A

1. 一种移动终端保护方法，其特征在于，包括：

获取移动终端中应用程序跨进程的调用信息，所述调用信息包括调用对象；

判断调用信息中的调用对象是否在预先建立的待拦截对象列表中；

当调用信息中的调用对象在所述预先建立的待拦截对象列表中时，将所述调用信息进行拦截。

2. 如权利要求 1 所述的方法，其特征在于，在所述移动终端获取应用程序跨进程的调用信息之前，还包括：

建立待拦截对象列表，所述待拦截对象包括需要进行拦截的应用程序。

3. 如权利要求 1 或 2 所述的方法，其特征在于，所述待拦截对象还包括需要进行拦截的预设文件，所述预设文件包括短信文件、通信录文件、定位文件、录音文件、图片文件、邮件文件中一种或多种。

4. 如权利要求 1 所述的方法，其特征在于，所述当调用信息中的调用对象在所述预先建立的待拦截对象列表中时，将所述调用信息进行拦截，具体为：

当调用信息中的调用对象在所述预先建立的待拦截对象列表中时，在预先存储与应用程序相对应的跨进程调用的权限中，查询与所述应用程序相对应的跨进程调用的权限；

当查询不到与应用程序相对应的跨进程调用的权限时，对所述调用信息进行拦截。

5. 如权利要求 1 所述的方法，其特征在于，当查询不到与应用程序相对应的跨进程调用的权限时，对所述调用信息进行拦截，具体为：

当查询不到与应用程序相对应的跨进程调用的权限时，向用户显示是否确定赋予所述应用程序跨进程调用的权限的提醒信息；

当用户确定不赋予所述应用程序跨进程调用的权限时，将所述调用信息进行拦截。

6. 一种移动终端保护装置，其特征在于，包括：

获取单元，用于获取移动终端中应用程序跨进程的调用信息，所述调用信息包括调用对象；

判断单元，用于判断调用信息中的调用对象是否在预先建立的待拦截对象列表中；

拦截单元，用于当调用信息中的调用对象在所述预先建立的待拦截对象列表中时，将所述调用信息进行拦截。

7. 如权利要求 6 所述的装置，其特征在于，还包括：

建立单元，用于建立待拦截对象列表，所述待拦截对象包括需要进行拦截的应用程序。

8. 如权利要求 6 或 7 所述的装置，其特征在于，所述待拦截对象还包括需要进行拦截的预设文件，所述预设文件包括短信文件、通信录文件、定位文件、录音文件、图片文件、邮件文件中一种或多种。

9. 如权利要求 6 所述的装置，其特征在于，所述拦截单元包括

第一查询子单元，用于当调用信息中的调用对象在所述预先建立的待拦截对象列表中时，在预先存储与应用程序相对应的跨进程调用的权限中，查询与所述应用程序对应的跨进程调用的权限；

第一拦截子单元，用于当查询不到与应用程序相对应的跨进程调用的权限时，对所述调用信息进行拦截。

10. 如权利要求 6 所述的装置，其特征在于，所述第一拦截子单元包括：

第二查询子单元，用于当查询不到与应用程序相对应的跨进程调用的权限时，向用户显示是否确定赋予所述应用程序跨进程调用的权限的提醒信息；

第二拦截子单元，用于当用户确定不赋予所述应用程序跨进程调用的权限时，将所述调用信息进行拦截。

一种移动终端保护方法及装置

技术领域

[0001] 本发明属于移动终端技术领域，尤其涉及一种移动终端保护方法及装置。

背景技术

[0002] 随着移动终端智能化时代的到来，移动终端的配置越来越强大，功能越来越齐全，适用于移动终端的应用程序也是五花八门，日益增多，用户可以通过网络下载自己喜欢的应用程序进行安装，以享受移动终端的智能化体验。

[0003] 然而，现有移动终端对自身具有缺陷的应用程序导致的安全隐患缺乏防御，由于许多不法分子会在应用程序内部植入恶意的插件，应用程序通过恶意的插件非法访问移动终端其它的应用程序的操作信息或访问在内存和扩展存储卡存储的隐私文件，然后从中窃取信息，当信息中存在商业机密时，如果泄露出去，会导致用户蒙受损失，因此对于移动终端内部信息存在的安全隐患不容忽视。

发明内容

[0004] 本发明实施例的目的在于提供一种移动终端保护方法，旨在解决现有移动终端对自身具有缺陷的应用程序导致的安全隐患缺乏防御的问题。

[0005] 本发明实施例是这样实现的，一种移动终端保护方法，包括：

[0006] 获取移动终端中应用程序跨进程的调用信息，所述调用信息包括调用对象；

[0007] 判断调用信息中的调用对象是否在预先建立的待拦截对象列表中；

[0008] 当调用信息中的调用对象在所述预先建立的待拦截对象列表中时，将所述调用信息进行拦截。

[0009] 本发明实施例的另一目的在于提供一种移动终端保护装置，包括：

[0010] 获取单元，用于获取移动终端中应用程序跨进程的调用信息，所述调用信息包括调用对象；

[0011] 判断单元，用于判断调用信息中的调用对象是否在预先建立的待拦截对象列表中；

[0012] 拦截单元，当调用信息中的调用对象在所述预先建立的待拦截对象列表中时，将所述调用信息进行拦截。

[0013] 在本发明实施例中，判断调用信息中的调用对象是否在预先建立的待拦截对象列表中，当调用信息中的调用对象在预先建立的待拦截对象列表中时，将调用信息进行拦截，解决了现有移动终端对自身具有缺陷的应用程序导致的安全隐患缺乏防御的问题，提高了移动终端内部信息的安全性。

附图说明

[0014] 图 1 是本发明实施例提供的移动终端保护方法的实现流程图；

[0015] 图 2 是本发明实施例提供的建立待拦截对象列表具体实现流程图；

[0016] 图 3 是本发明实施例提供的拦截调用信息的具体实现流程图；

[0017] 图 4 是本发明另一实施例提供的拦截调用信息的具体实现流程图；

[0018] 图 5 是本发明实施例提供的在实际应用中较佳的实现流程图；

[0019] 图 6 是本发明实施例提供的移动终端保护装置的结构框图。

具体实施方式

[0020] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0021] 在本发明实施例中，判断调用信息中的调用对象是否在预先建立的待拦截对象列表中，当调用信息中的调用对象在预先建立的待拦截对象列表中时，将调用信息进行拦截，解决了现有移动终端对自身具有缺陷的应用程序导致的安全隐患缺乏防御的问题，提高了移动终端内部信息的安全性。

[0022] 图 1 示出了本发明实施例提供的一种移动终端保护方法的实现流程，详述如下：

[0023] 在步骤 S101 中，移动终端获取应用程序跨进程的调用信息，该调用信息包括调用对象。

[0024] 在本实施例中，跨进程是指一个进程中调用另一个进程。如在第三方应用程序中调用拨号、短信、邮件等，移动终端可以通过进程间通信机制（Inter-Process Communication，IPC）完成调用。进程间通信机制包括但不限于 Binder 通信机制、命名管道通信机制、消息队列通信机制、信号通信机制、共享内存通信机制、套接字通信机制。

[0025] 在本实施例中，获取跨进程的调用信息，可在系统设置监听器，以获取跨进程的调用信息。

[0026] 为便于说明，以进程间通信机制为 Binder 通信机制为例，应用程序之间通过 Binder 通信机制调用数据，作为客户端的应用程序通过服务端代理对象的方式向作为服务端的应用程序发送调用信息，服务端代理对象会通过 Binder 驱动将请求信息发送至作为服务端的应用程序，此时，通过 Binder 自身的缓存，存储跨进程的调用信息，以完成跨进程的调用信息的获取，与此同时，通过调用预设计时器，以延迟 Binder 驱动将请求信息发送至作为服务端的应用程序的时间，避免应用程序之间通过 Binder 通信机制完成了数据的调用。

[0027] 在步骤 S102 中，判断调用信息中的调用对象是否在预先建立的待拦截对象列表中。

[0028] 在本实施例中，判断调用信息中的调用对象是否在预先建立的待拦截对象列表中，可对应用程序跨进程的调用信息进行解码，提取调用信息的调用对象，将调用对象的名称作为查询字段，在预设预先建立的待拦截对象列表中，查询是否存在调用对象。当查询到调用对象时，表示调用信息为待拦截对象；当查询不到调用对象时，表示调用信息不为待拦截对象。

[0029] 在步骤 S103 中，当调用信息中的调用对象在预先建立的待拦截对象列表中时，将该调用信息进行拦截。

[0030] 在本实施例中，当调用信息中的调用对象在预先建立的待拦截对象列表中时，将

调用信息进行拦截，具体地，可在通信机制的缓存中，将调用的信息进行丢弃，以完成调用信息进行拦截，避免应用程序之间通过 Binder 通信机制完成了数据的调用，从而不法分子无法通过恶意的插件非法访问移动终端的待拦截对象的操作信息。

[0031] 作为本发明的一个优选实施例，在移动终端获取应用程序跨进程的调用信息之前，还包括：

[0032] 建立待拦截对象列表，待该拦截对象包括需要进行拦截的应用程序；

[0033] 在本实施例中，图 2 示出了本发明实施例提供的建立待拦截对象列表具体实现流程图，详述如下：

[0034] 在步骤 S201 中，显示应用程序列表，该应用程序列表中包括终端中安装的应用程序。

[0035] 在本实施例中，在终端的界面上显示终端上安装的应用程序，由于应用程序比较多，可以通过在界面上绘制一个图表，以应用程序的功能作为满足条件的应用程序的归类标识，根据归类标识可以查看满足同一功能的所有应用程序，以便用户进行选中的操作。

[0036] 在步骤 S202 中，获取用户在应用程序列表中指定的应用程序；

[0037] 在本实施例中，获取用户在该应用程序列表中指定的应用程序，指定的方式包括但不限于触摸或者按键，通过对用户的指定的操作检测，获取到用户的指定的应用程序。

[0038] 在本实施例中，用户可以通过预设的多选方式，一次选中多个的应用程序。如预设的触摸手势或预设的多选控件。

[0039] 在步骤 S203 中，将用户指定的应用程序作为需要进行拦截的应用程序；

[0040] 在本实施例中，提取应用程序的唯一标识，唯一标识包括但不限于名称和存储路径，唯一标识作为需要进行拦截的应用程序的标识。

[0041] 在步骤 S204 中，根据需要进行拦截的应用程序，建立待拦截对象列表。

[0042] 在本实施例中，提取需要进行拦截的应用程序的唯一标识，唯一标识包括但不限于名称和存储路径，建立唯一标识和应用程序的对应关系，以预设形式记录存储，优选地，预设形式为列表，从而建立待拦截对象列表，便于后续进行根据调用对象查询。

[0043] 通过上述步骤，在终端的显示界面上显示应用程序列表，用户根据个人需要对应用程序进行选择，避免了拦截不必要的应用程序，从而提高了待拦截的应用程序的有效性。

[0044] 作为本发明的一个优选实施例，还包括：

[0045] 所述待拦截对象还包括需要进行拦截的预设文件，所述预设文件包括短信文件、通信录文件、定位文件、录音文件、图片文件、邮件文件中一种或多种。

[0046] 在本实施例中，预设文件可以为用户自设，也可以为系统默认。当用户采用自设时，用户根据个人需要对预设文件进行选择，预设文件包括短信文件、通信录文件、定位文件、录音文件、图片文件、邮件文件、视频文件中一种或多种。

[0047] 在本实施例中，在终端的界面上显示满足的文件，由于文件比较多，可以通过在界面上绘制一个图表，以功能作为的文件的归类标识，如短信、通信件、定位、录音、图片、邮件、视频等，根据归类标识可以查看满足该功能的所有文件，以便用户进行选中的操作。优选地，用户在满足该功能的所有文件中，指定其中的一个文件。

[0048] 在本实施例中，用户在该文件列表中指定的文件，指定的方式包括但不限于触摸或者按键，通过对用户的选中操作检测，接收用户的选中结果。

[0049] 在本实施例中，在本实施例中，提取文件的唯一标识，唯一标识包括但不限于名称和存储路径在待拦截对象列表中添加预设文件的标识，从而应用程序无法调用预设文件，避免了产生恶意的插件非法访问移动终端的内存和扩展存储卡存储的预设文件的情况，提高了内部信息的安全性，杜绝了移动终端内部信息存在的安全隐患。

[0050] 作为本发明的一个优选实施例，如图 3 示出了当调用信息中的调用对象在所述预先建立的待拦截对象列表中时，将所述调用信息进行拦截的实施流程，详述如下：

[0051] S301，当调用信息中的调用对象在所述预先建立的待拦截对象列表中时，在预先存储与应用程序相对应的跨进程调用的权限中，查询与该应用程序相对应的跨进程调用的权限。

[0052] 在本实施例中，预先存储与应用程序相对应的跨进程调用的权限，可以为用户自设，也可以为系统默认，在此不做限制。

[0053] 在本实施例中，当配置预先存储与应用程序相对应的跨进程调用的权限，采用系统默认时，移动终端根据应用程序的厂商以及功能类型，通过网络查询，记录下安全性系数高的应用程序，赋予该应用程序跨进程调用的权限，建立应用程序和跨进程调用的权限的对应关系，并在移动终端中建立白名单，白名单中的应用程序具有跨进程调用的权限，以便于后续进行查询。

[0054] 作为本发明的另一实施例，移动终端根据应用程序的厂商以及功能类型，通过网络查询，记录下恶意的应用程序，不赋予该应用程序跨进程调用的权限，并在移动终端中建立黑名单，黑名单中的应用程序不具有跨进程调用的权限，以便于后续进行查询和拦截调用信息。

[0055] 作为本发明的另一实施例，当配置预先存储与应用程序相对应的跨进程调用的权限采用用户自设时，可通过在移动终端中设置监听器，以监听广播信息，当存在应用程序开始安装完毕的广播信息时，向用户显示是否确定赋予该应用程序跨进程调用的权限的选择信息，优选地，将选择信息以控件的方式显示，以接收用户选择的结果，并根据选择的结果返回跨进程调用的权限的标识，在移动终端中根据权限的标识，建立应用程序和跨进程调用的权限的对应关系，并存储与应用程序相对应的跨进程调用的权限。

[0056] 作为本发明的另一个实施例，用户也可以对选择信息进行忽略，跳过确定赋予应用程序跨进程调用的权限的选择信息的操作步骤，从而避免了强制用户进行确定选择信息，影响用户操作感知的情况。

[0057] 在本实施例中，查询应用程序相对应的跨进程调用的权限，具体为，以应用程序的名称为索引，在预先存储与应用程序相对应的跨进程调用的权限的数据库中，查询发送调用信息的应用程序相对应的跨进程调用的权限，以判断存储数据库中是否存在应用程序相对应的跨进程调用的权限。

[0058] S302，当查询不到与应用程序相对应的跨进程调用的权限时，对该调用信息进行拦截。

[0059] 在本实施例中，当查询不到与应用程序相对应的跨进程调用的权限时，数据库中不存在与应用程序相对应的跨进程调用的权限，表示该应用程序不具有跨进程调用的权限，不能通过进程通信机制发送调用信息。通信机制在缓存中丢弃调用信息，以完成对调用信息的拦截。

[0060] 作为本发明的另一个实施例，当查询到所述应用程序具有跨进程调用的权限时，不对调用信息进行拦截。具体地，通信机制取消预设的计时器，在缓存中对调用信息进行发送，以完成应用程序的调用操作。

[0061] 作为本发明的一个优选实施例，如图 4 示出了当查询不到与应用程序相对应的跨进程调用的权限时，对所述调用信息进行拦截的实施流程，详述如下：

[0062] S401，当查询不到与应用程序相对应的跨进程调用的权限时，向用户显示是否确定赋予该应用程序跨进程调用的权限的提醒信息；

[0063] 在本实施例中，将选择信息以控件的方式显示，控件的方式，以接收用户选择的结果，并根据选择的结果返回跨进程调用的权限的标识，在移动终端中根据权限的标识，判断用户是否赋予应用程序跨进程调用的权限。

[0064] 在本实施例中，当查询不到所述应用程序具有跨进程调用的权限时，向用户显示是否确定赋予所述应用程序跨进程调用的权限的提醒信息，从而即使查询不到与应用程序相对应的跨进程调用的权限，用户也可以根据自身的选择，确定是否确定赋予应用程序跨进程调用的权限。

[0065] S402，当用户确定不赋予应用程序跨进程调用的权限时，将调用信息进行拦截。

[0066] 在本实施例中，当用户确定不赋予应用程序跨进程调用的权限时，表示该应用程序不具有跨进程调用的权限，不能通过进程通信机制发送调用信息。系统在缓存中丢弃调用信息，以完成对调用信息的拦截。

[0067] 作为本发明的一个实施例，当用户确定赋予应用程序跨进程调用的权限时，表示该应用程序具有跨进程调用的权限，通信机制取消预设的计时器，在缓存中对调用信息进行发送，以完成应用程序的调用操作。

[0068] 作为本发明的优选实施例，图 5 示了本发明在实际应用中较佳的实现流程图，详述如下：

[0069] 在步骤 S501 中，应用程序启动；

[0070] 在步骤 S502 中，应用程序进行了跨进程调用；

[0071] 在步骤 S503 中，获取应用程序跨进程调用的调用对象；

[0072] 在步骤 S504 中，检测调用对象是否在待拦截对象列表中，是则执行 S506，否则执行 S505。

[0073] 在步骤 S505 中，检测正在执行调用的应用程序是否不具有跨进程调用的权限，是则执行 S507，否则执行 508。

[0074] 在步骤 S506 中，根据应用程序的调用信息，完成调用操作；

[0075] 在步骤 S507 中，拦截应用程序的调用信息；

[0076] 在步骤 S508 中，检测正在执行调用的应用程序是否具有跨进程调用的权限，是则执行 506，否则执行 509；

[0077] 在步骤 S509 中，向用户显示提醒信息，是否允许应用程序进行跨进程调用，是则执行 510，否则执行 507。

[0078] 在步骤 S510 中，根据应用程序的调用信息，完成调用操作，并将应用程序对应的跨进程调用的权限保存到数据库中。

[0079] 图 6 示出了本发明实施例提供的移动终端保护装置的结构框图，该装置可以

运行于具备触摸屏的各种终端，包括但不限于移动电话、口袋计算机(Pocket Personal Computer，PPC)、掌上电脑、计算机、笔记本电脑、个人数字助理(Personal Digital Assistant，PDA)、MP4、MP3 等。为了便于说明，仅示出了与本实施例相关的部分。

[0080] 参照图 6，该待机处理装置，包括：

[0081] 获取单元 61，用于获取移动终端中应用程序跨进程的调用信息，所述调用信息包括调用对象；

[0082] 判断单元 62，用于判断调用信息中的调用对象是否在预先建立的待拦截对象列表中；

[0083] 拦截单元 63，用于当调用信息中的调用对象在所述预先建立的待拦截对象列表中时，将所述调用信息进行拦截。

[0084] 进一步地，在该装置中，还包括：

[0085] 建立单元 64，用于建立待拦截对象列表，所述待拦截对象包括需要进行拦截的应用程序。

[0086] 进一步地，在该装置中，所述待拦截对象还包括需要进行拦截的预设文件，所述预设文件包括短信文件、通信录文件、定位文件、录音文件、图片文件、邮件文件中一种或多种。

[0087] 具体地，在该装置中，所述拦截单元 63，包括

[0088] 第一查询子单元 631，用于当调用信息中的调用对象在所述预先建立的待拦截对象列表中时，在预先存储与应用程序相对应的跨进程调用的权限中，查询所述应用程序相对应的跨进程调用的权限；

[0089] 第一拦截子单元 632，用于当查询不到与应用程序相对应的跨进程调用的权限时，对所述调用信息进行拦截。

[0090] 具体地，在该装置中，所述第一拦截子单元 632，包括

[0091] 第二查询子单元，用于当查询不到与应用程序相对应的跨进程调用的权限时，向用户显示是否确定赋予所述应用程序跨进程调用的权限的提醒信息；

[0092] 第二拦截子单元，用于当用户确定不赋予所述应用程序跨进程调用的权限时，将所述调用信息进行拦截。

[0093] 在本发明实施例中，判断调用信息中的调用对象是否在预先建立的待拦截对象列表中，当调用信息中的调用对象在预先建立的待拦截对象列表中时，将调用信息进行拦截，解决了现有移动终端对自身具有缺陷的应用程序导致的安全隐患缺乏防御的问题，提高了移动终端内部信息的安全性。

[0094] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

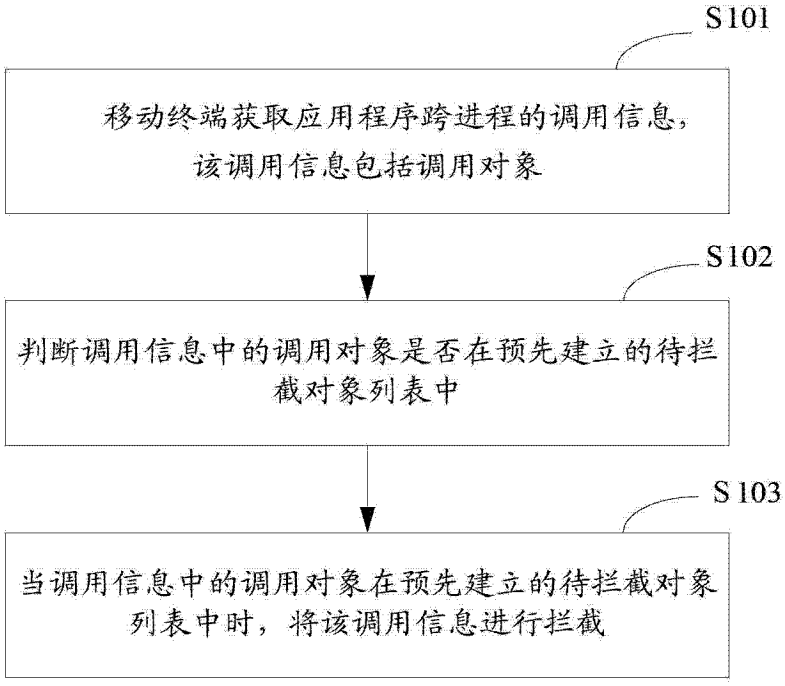

S101
移动终端获取应用程序跨进程的调用信息，该调用信息包括调用对象
S102
判断调用信息中的调用对象是否在预先建立的待拦截对象列表中
S103
当调用信息中的调用对象在预先建立的待拦截对象列表中时，将该调用信息进行拦截

图 1

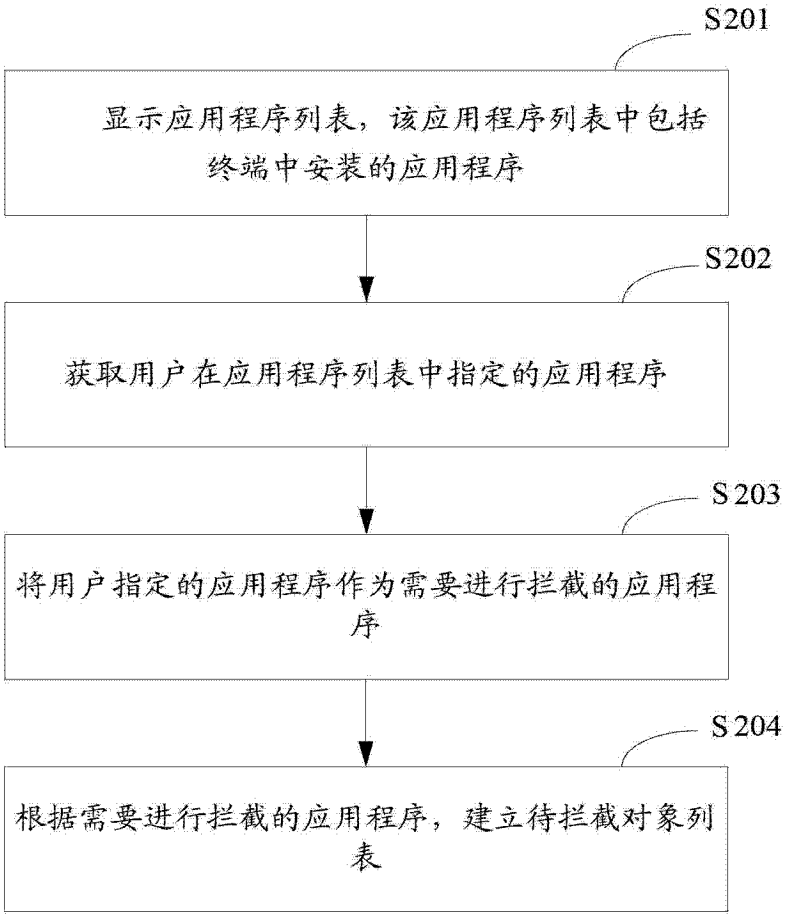

S201
显示应用程序列表，该应用程序列表中包括终端中安装的应用程序
S202
获取用户在应用程序列表中指定的应用程序
S203
将用户指定的应用程序作为需要进行拦截的应用程序
S204
根据需要进行拦截的应用程序，建立待拦截对象列表

图 2

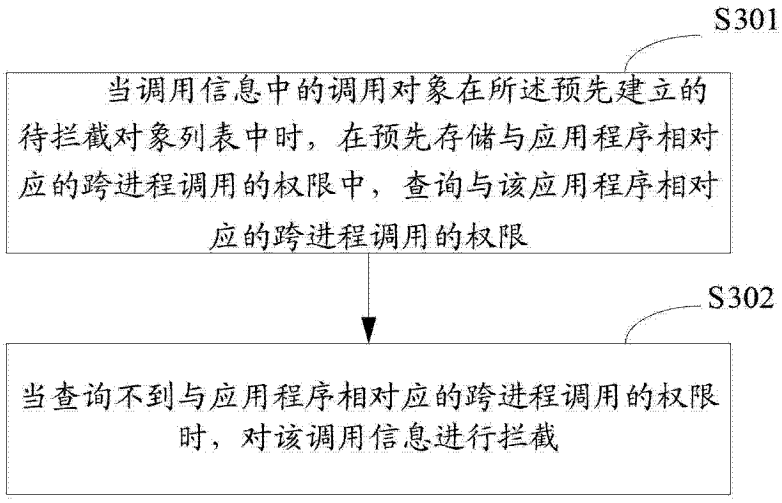

S301
当调用信息中的调用对象在所述预先建立的待拦截对象列表中时，在预先存储与应用程序相对应的跨进程调用的权限中，查询与该应用程序相对应的跨进程调用的权限
S302
当查询不到与应用程序相对应的跨进程调用的权限时，对该调用信息进行拦截

图 3

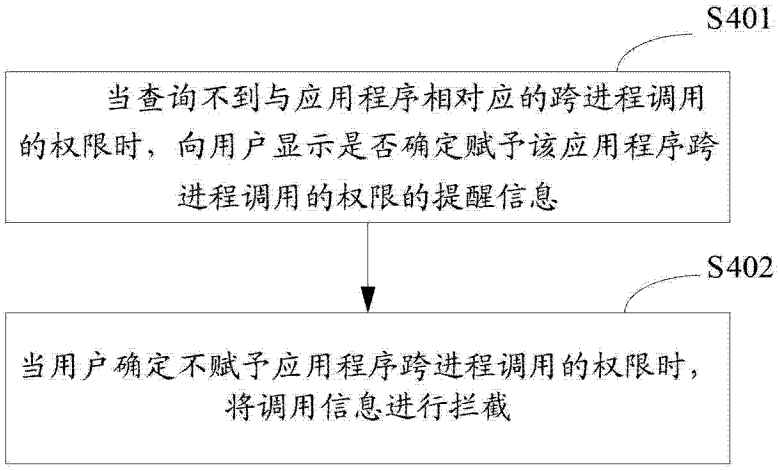

S401
当查询不到与应用程序相对应的跨进程调用的权限时，向用户显示是否确定赋予该应用程序跨进程调用的权限的提醒信息
S402
当用户确定不赋予应用程序跨进程调用的权限时，将调用信息进行拦截

图 4

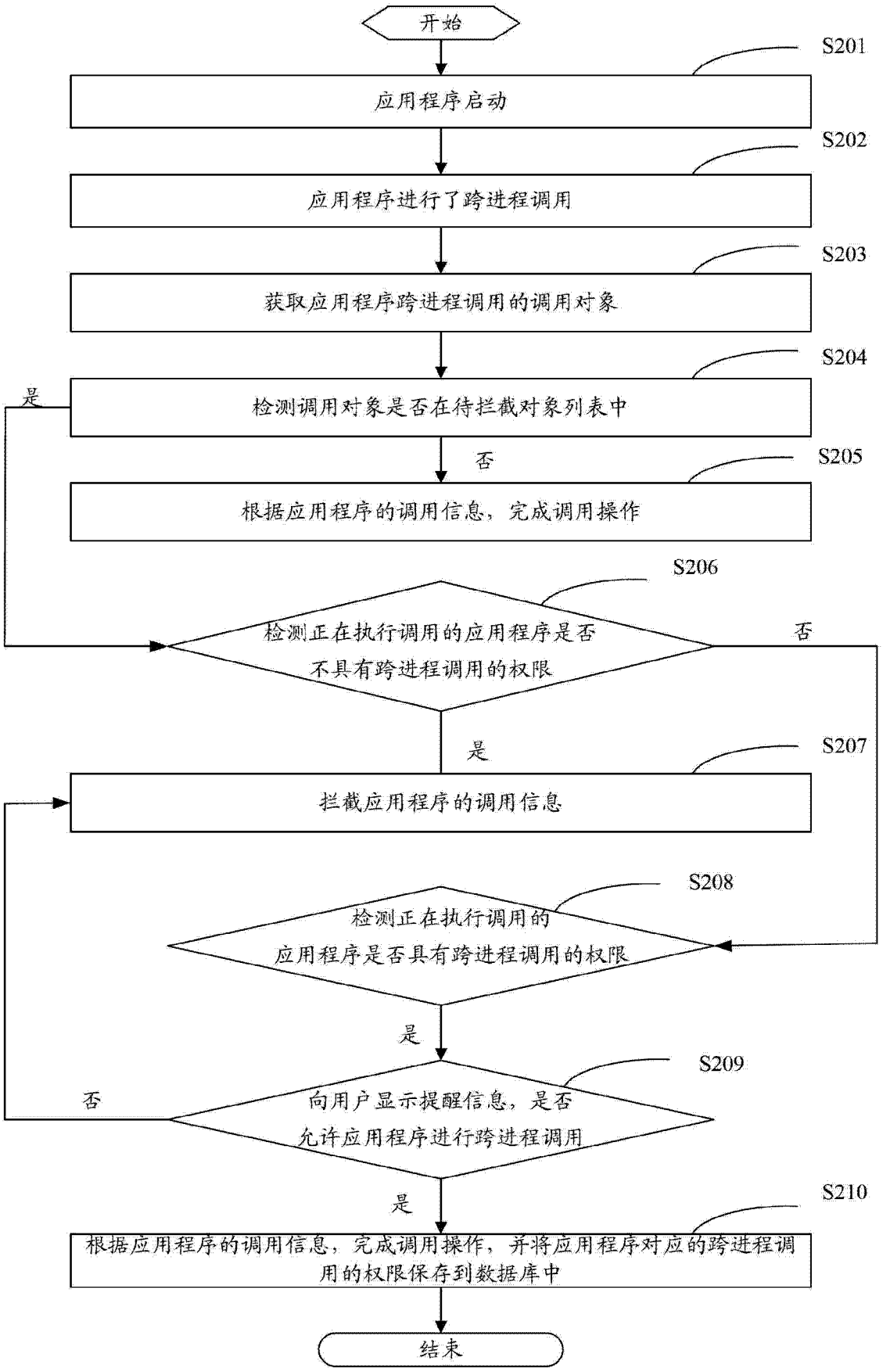

开始
S201
应用程序启动
S202
应用程序进行了跨进程调用
S203
获取应用程序跨进程调用的调用对象
S204
检测调用对象是否在待拦截对象列表中
是
否
S205
根据应用程序的调用信息，完成调用操作
S206
检测正在执行调用的应用程序是否
不具有跨进程调用的权限
否
是
S207
拦截应用程序的调用信息
S208
检测正在执行调用的
应用程序是否具有跨进程调用的权限
是
S209
否
向用户显示提醒信息，是否
允许应用程序进行跨进程调用
是
S210
根据应用程序的调用信息，完成调用操作，并将应用程序对应的跨进程调用的权限保存到数据库中
结束

图 5

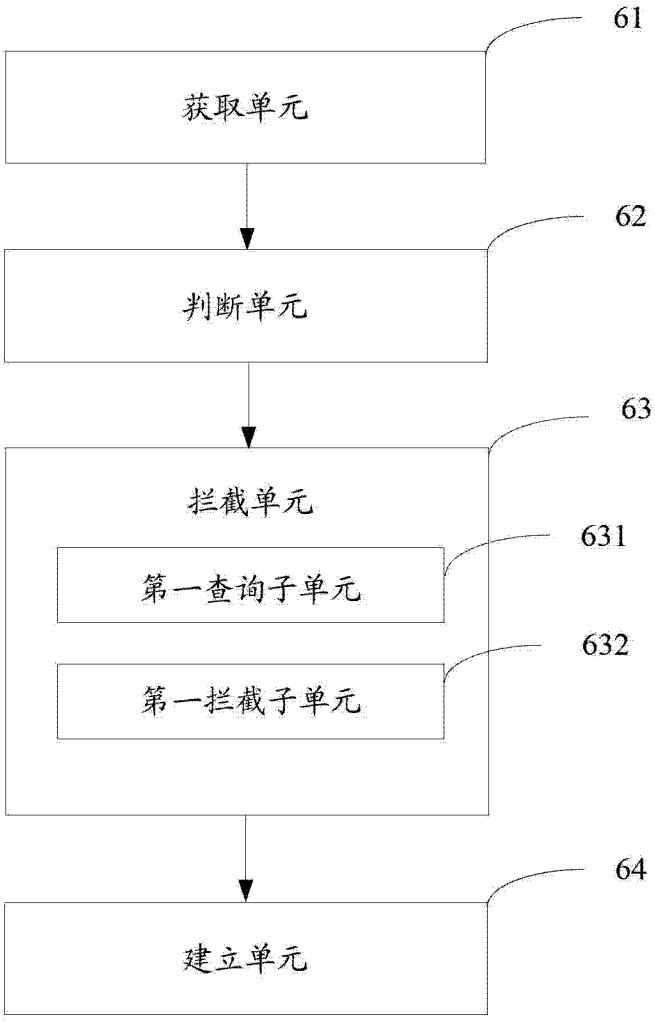


图 6