

说明书

一种应用程序的处理方法和移动终端

本申请要求于 2012 年 1 月 20 日提交中国专利局、申请号为
5 2012100187752、发明名称为“一种应用程序的处理方法和移动终端”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

10 本发明涉及移动通信技术领域，特别涉及一种应用程序的处理方法和移动
终端。

背景技术

随着移动终端的发展，移动终端的应用安全也越来越受到重视，其中，对
恶意扣费程序的防御，则是移动终端应用安全的一个重要内容。扫描防御是现
15 行的一种常用方案，其主要过程为：首先收集恶意扣费程序的样本，提取特征
添加到病毒库；当应用程序安装时或运行过程中，使用杀毒引擎扫描所述应用
程序，当发现该应用程序的特征与病毒库中的特征匹配（相同或相似），则将
该应用程序定性为病毒，提示用户进行处理（例如：禁止安装、病毒查杀、卸
载、强力卸载等操作），用户可以根据提示对该应用程序进行进一步的处理，
20 保护移动终端的应用安全。

发明人发现，上述扫描防御方案至少存在以下缺陷：对应用程序进行处理
时，每次都需要进行特征扫描，既耗费时间，又占用系统资源，影响用户对应
用程序的使用体验。

25 发明内容

为了解决现有技术中对应用程序的安全处理耗费时间、占用资源的问题，
本发明实施例提供了一种应用程序的处理和移动终端。所述技术方案如下：

一方面，提供了一种应用程序的处理方法，所述方法包括：

当应用程序执行对扣费事件的调用操作时，分析所述应用程序的操作权
30 限；

如果所述应用程序具有对所述扣费事件的操作权限，则允许所述应用程序执行所述调用操作；

如果所述应用程序不具有对所述扣费事件的操作权限，则禁止所述应用程序执行所述调用操作。

5 所述分析所述应用程序的操作权限，包括：

获取所述应用程序的操作许可状态；

如果所述操作许可状态为允许，则确认所述应用程序具有对所述扣费事件的操作权限；

10 如果所述操作许可状态为禁止，则确认所述应用程序不具有对所述扣费事件的操作权限。

在应用程序执行对扣费事件的调用操作之前，所述方法还包括：对所述应用程序进行预处理。

所述对所述应用程序进行预处理，包括：

扫描所述应用程序的安装包，获得所述应用程序的特征；

15 将所述应用程序的特征与预设的恶意特征进行比对，如果所述应用程序的特征与所述预设的恶意特征匹配，则输出禁止操作提示信息。

所述对所述应用程序进行预处理，还包括：

如果所述应用程序的特征与所述预设的恶意特征不匹配，则输出权限设置提示信息；

20 根据接收到的对所述应用程序的权限设置信息，设置所述应用程序的操作许可状态。

在对所述应用程序进行预处理之后，所述方法还包括：接收对所述应用程序的权限修改信息，根据所述权限修改信息，修改所述应用程序的操作许可状态。

25 所述应用程序的操作权限包括以下权限中的任一种或多种：短信消息服务 SMS 扣费权限、互动式语音应答 IVR 扣费权限、无线应用协议 WAP 扣费权限、WAP 代扣费权限、移动支付权限和电子银行扣费权限。

另一方面，还提供了一种移动终端，所述移动终端包括：

30 分析模块，用于当应用程序执行对扣费事件的调用操作时，分析所述应用程序的操作权限；

执行模块，用于如果所述分析模块分析出所述应用程序具有对所述扣费事

件的操作权限，则允许所述应用程序执行所述调用操作；如果所述分析模块分析出所述应用程序不具有对所述扣费事件的操作权限，则禁止所述应用程序执行所述调用操作。

分析模块包括：

5 获取单元，用于获取所述应用程序的操作许可状态；

分析单元，用于如果所述操作许可状态为允许，则确认所述应用程序具有对所述扣费事件的操作权限；如果所述操作许可状态为禁止，则确认所述应用程序不具有对所述扣费事件的操作权限。

所述移动终端还包括：

10 预处理模块，用于在应用程序执行对扣费事件的调用操作之前，对所述应用程序进行预处理。

所述预处理模块具体用于：

扫描所述应用程序的安装包，获得所述应用程序的特征；

15 将所述应用程序的特征与预设的恶意特征进行比对，如果所述应用程序的特征与所述预设的恶意特征匹配，则输出禁止操作提示信息。

所述预处理模块还用于：

如果所述应用程序的特征与所述预设的恶意特征不匹配，则输出权限设置提示信息；

20 根据接收到的对所述应用程序的权限设置信息，设置所述应用程序的操作许可状态。

所述移动终端还包括：

修改模块，用于接收对所述应用程序的权限修改信息，根据所述权限修改信息，修改所述应用程序的操作许可状态。

25 所述应用程序的操作权限包括以下权限中的任一种或多种：短信消息服务 SMS 扣费权限、互动式语音应答 IVR 扣费权限、无线应用协议 WAP 扣费权限、WAP 代扣费权限、移动支付权限和电子银行扣费权限。

30 本发明实施例提供的技术方案带来的有益效果是：当应用程序执行对扣费事件的调用操作时，分析所述应用程序的操作权限；如果所述应用程序具有对所述扣费事件的操作权限，则允许所述应用程序执行所述调用操作；如果所述应用程序不具有对所述扣费事件的操作权限，则禁止所述应用程序执行所述调用操作。本发明实施例进行应用安全处理时，不需要每次运行应用程序时都对

应用程序进行扫描，只需要对应用程序的操作权限进行判定即可，节省了处理时间，避免了资源的浪费，同时不需要用户的参与，方便用户的使用，从而提高了用户的使用体验。

5 附图说明

为了更清楚地说明本发明实施例中的技术方案，下面将对实施例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一些实施例，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，还可以根据这些附图获得其他的附图。

- 10 图 1 是本发明实施例 1 中提供的一种应用程序的处理方法的流程图；
图 2 是本发明实施例 2 中提供的一种应用程序的处理方法的流程图；
图 3 是本发明实施例 3 中提供的一种移动终端的示意图；
图 4 是本发明实施例 3 中提供的另一种移动终端的示意图。

15 具体实施方式

为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明实施方式作进一步地详细描述。

- 本发明实施例中，SMS（Short Messaging Service，短消息服务）通道扣费可以为：在计费与业务系统中设定收费标准，移动终端主动发送特定格式的短信内容到特定的业务端口号，扣取预设的话费；IVR（Interactive Voice Response，交互式语音应答）或声讯电话通道扣费可以为：在计费与业务系统中设定收费标准，移动终端主动拨打语音电话到特定的业务号码，扣取预设的话费；WAP（Wireless Application Protocol，无线应用协议）通道扣费或 WAP 代扣费可以为：在计费与业务系统中设定收费标准，移动终端通过 WAP 连接至特定的 URL
25 （Uniform / Universal Resource Locator，统一资源定位符），扣取预设的话费。

- “移动支付”是允许用户使用移动终端对所消费的商品或服务进行账务支付的一种服务方式，此方式为每个用户建立一个与其移动终端号码关联的支付账户，为用户提供一个通过移动终端进行交易支付和身份认证的途径；“电子银行支付”是指银行为用户提供的利用移动通信网络及移动终端办理相关银行
30 支付业务的服务，该服务界面可以由移动终端提供。

实施例 1

参见图 1，本发明实施例提供了一种应用程序的处理方法，包括：

101、当应用程序执行对扣费事件的调用操作时，分析所述应用程序的操作权限；

102、如果所述应用程序具有对所述扣费事件的操作权限，则允许所述应用程序执行所述调用操作；

103、如果所述应用程序不具有对所述扣费事件的操作权限，则禁止所述应用程序执行所述调用操作。

本实施例中，所述分析所述应用程序的操作权限，包括：

获取所述应用程序的操作许可状态；

10 如果所述操作许可状态为允许，则确认所述应用程序具有对所述扣费事件的操作权限；

如果所述操作许可状态为禁止，则确认所述应用程序不具有对所述扣费事件的操作权限。

15 可选地本实施例中，在应用程序执行对扣费事件的调用操作之前，所述方法还包括：对所述应用程序进行预处理。

优选地本实施例中，所述对所述应用程序进行预处理，包括：

扫描所述应用程序的安装包，获得所述应用程序的特征；

将所述应用程序的特征与预设的恶意特征进行比对，如果所述应用程序的特征与所述预设的恶意特征匹配，则输出禁止操作提示信息。

20 本实施例中，所述对所述应用程序进行预处理，还包括：

如果所述应用程序的特征与所述预设的恶意特征不匹配，则输出权限设置提示信息；

根据接收到的对所述应用程序的权限设置信息，设置所述应用程序的操作许可状态。

25 可选地本实施例中，在对所述应用程序进行预处理之后，所述方法还包括：接收对所述应用程序的权限修改信息，根据所述权限修改信息，修改所述应用程序的操作许可状态。

30 可选地，本实施例中，所述应用程序的操作权限包括以下权限中的任一种或多种：短信消息服务 SMS 扣费权限、互动式语音应答 IVR 扣费权限、无线应用协议 WAP 扣费权限、WAP 代扣费权限、移动支付权限和电子银行扣费权限。

本实施例中的移动终端包括：手机、PDA（Personal Digital Assistant，掌上电脑）等终端设备，对此本实施例不做具体限定。

本发明提供的方法实施例的有益效果是：当应用程序执行对扣费事件的调用操作时，分析所述应用程序的操作权限；如果所述应用程序具有对所述扣费事件的操作权限，则允许所述应用程序执行所述调用操作；如果所述应用程序不具有对所述扣费事件的操作权限，则禁止所述应用程序执行所述调用操作。本发明实施例进行应用安全处理时，不需要每次运行应用程序时都对应用程序进行扫描，只需要对应用程序的操作权限进行判定即可，节省了处理时间，避免了资源的浪费，同时不需要用户的参与，方便用户的使用，从而提高了用户的使用体验。

实施例 2

参见图 2，本实施例提供了一种应用程序的处理方法，本发明实施例中的移动终端可以为手机、PDA 等终端设备，本实施例以手机为例进行说明，该方法具体包括：

201、对应用程序进行预处理。

本实施例中，可选地，手机可以监控应用程序，对手机中的应用程序进行预处理，所述预处理的过程可以包括：扫描所述应用程序的安装包，获得所述应用程序的特征；将所述应用程序的特征与预设的恶意特征进行比对，如果所述应用程序的特征与所述预设的恶意特征匹配，则输出禁止操作提示信息。例如：当应用程序准备安装时，手机先对该应用程序进行预处理，具体的，可以使用手机中的安全软件（例如：杀毒引擎、防火墙等）对应用程序进行预处理，如果发现此应用程序与预设的恶意程序库中的恶意特征匹配，则确认该应用程序为恶意程序，输出禁止操作提示信息，例如：弹出提示框“该程序为恶意程序！”，提示用户拒绝安装所述应用程序；再如，当用户下载某应用程序，手机先对该应用程序的安装包进行预处理，如果发现其为恶意程序，则输出禁止下载提示信息，提示用户不要继续下载该程序。本实施例中“应用程序的特征与预设的恶意特征匹配”可以是指应用程序的特征与预设的恶意特征完全相同，也可以指应用程序的特征与预设的恶意特征相似（例如：80%或 90%以上的特征与预设的恶意特征相同，此处的比例或数据可以根据进行预设），对此本实施例不做具体限定。

本实施例中，预设的恶意特征可以存储于恶意程序库中，该恶意特征指恶意扣费程序的特征，具体的，可以预先获取恶意扣费程序的样本，例如：可以从网络中获取各种恶意扣费程序的样本，然后提取其特征添加到预设的恶意程序库中。进一步地，本步骤对应用程序进行预处理还包括：如果所述应用程序的特征与所述预设的恶意特征不匹配，则输出权限设置提示信息；根据接收到的对所述应用程序的权限设置信息，设置所述应用程序的操作许可状态。其中，操作许可状态可以为允许，表明该应用程序可以对该扣费事件进行调用操作；操作许可状态可以为禁止，表明该应用程序不能对该扣费事件执行调用操作。

所述权限设置提示信息可用于提示用户对该应用程序的操作许可状态进行设置。具体地，每个应用程序对应自己可能具备的操作权限，例如：应用程序一可能具备 SMS 扣费权限，应用程序二可能具备 WAP 扣费权限；移动终端可以首先获取该应用程序可能具备的操作权限，再输出权限设置提示信息，提示用户对该应用程序可能具备的操作权限进行设置，即设置该操作权限对应的操作许可状态，例如：针对应用程序一，移动终端输出权限设置提示信息，提示用户对该应用程序可能具备的 SMS 扣费权限进行设置，用户可根据该提示信息对 SMS 扣费权限的操作许可状态进行设置。本实施例中，应用程序的操作权限包括但不限于以下权限中的任一种或多种：短信消息服务 SMS 扣费权限、互动式语音应答 IVR 扣费权限、无线应用协议 WAP 扣费权限、WAP 代扣费权限、移动支付权限和电子银行扣费权限。

值的指出的是，本实施例中在预处理的过程中对安装包的扫描为可选步骤，预处理过程中也可以不执行安装包的扫描而直接安装该应用程序，对此本实施例不做具体限定。

202、当应用程序执行对扣费事件的调用操作时，分析应用程序的操作权限。

本实施例中，由于在应用程序安装的时，已经对该应用程序的操作权限进行了设置，所以当应用程序执行对扣费事件的调用操作时，先对该应用程序的操作权限进行分析，具体的，分析所述应用程序的操作权限包括：获取所述应用程序的操作许可状态；如果所述操作许可状态为允许，则确认所述应用程序具有对所述扣费事件的操作权限；如果所述操作许可状态为禁止，则确认所述应用程序不具有对所述扣费事件的操作权限。

203、如果该应用程序具有对所述扣费事件的操作权限，则允许应用程序

执行所述调用操作；如果该应用程序不具有对所述扣费事件的操作权限，则禁止应用程序执行所述调用操作。

本实施例中，根据步骤 202 的分析结果，如果所述应用程序不具有对所述扣费事件的操作权限，即该权限的操作许可状态为禁止，则当该应用程序运行时，禁止其执行该调用操作，即该应用程序无法进行费用的扣取。例如：用户安装某游戏程序时，设置该游戏程序的“SMS 扣费权限”的操作许可状态为禁止，则在该游戏程序调用“发送 SMS 扣费”的操作时，禁止该游戏程序发送 SMS，避免产生相关费用。

本实施例中，移动终端还可以接收对应用程序的权限修改信息，根据该权限修改信息，修改该应用程序的操作许可状态。例如：如果用户想要修改移动终端中的应用程序的操作权限，则可以向移动发送权限修改信息，该信息可以包括：修改后的操作权限的操作许可状态；移动终端基于该权限修改信息，修改该应用程序的操作许可状态，达到修改该应用程序权限的目的。

本发明提供的方法实施例的有益效果是：当应用程序执行对扣费事件的调用操作时，分析所述应用程序的操作权限；如果所述应用程序具有对所述扣费事件的操作权限，则允许所述应用程序执行所述调用操作；如果所述应用程序不具有对所述扣费事件的操作权限，则禁止所述应用程序执行所述调用操作。本发明实施例进行应用安全处理时，不需要每次运行应用程序时都对应用程序进行扫描，只需要对应用程序的操作权限进行判定即可，节省了处理时间，避免了资源的浪费，同时不需要用户的参与，方便用户的使用，从而提高了用户的使用体验。且在安装应用程序时先对该应用程序进行扫描，再对扣费事件的调用操作进行相应的设定，实现扣费的主动防御，能补充防御那些扫描式防御还没有能发现的扣费恶意程序。

25 实施例 3

参见图 3，本实施例中提供了一种移动终端，所述移动终端包括：分析模块 301 和执行模块 302；

判断模块 301，用于当应用程序执行对扣费事件的调用操作时，分析所述应用程序的操作权限；

30 执行模块 302，用于如果所述分析模块分析出所述应用程序具有对所述扣费事件的操作权限，则允许所述应用程序执行所述调用操作；如果所述分析模

块分析出所述应用程序不具有对所述扣费事件的操作权限，则禁止所述应用程序执行所述调用操作。

参见图 4，本实施例中优选地，分析模块 301 包括：

获取单元 301a，用于获取所述应用程序的操作许可状态；

- 5 分析单元 301b，用于如果所述操作许可状态为允许，则确认所述应用程序具有对所述扣费事件的操作权限；如果所述操作许可状态为禁止，则确认所述应用程序不具有对所述扣费事件的操作权限。

参见图 4，可选地本实施例中的移动终端还包括：

- 10 预处理模块 303，用于在应用程序执行对扣费事件的调用操作之前，对所述应用程序进行预处理。

优选地，本实施例中所述预处理模块 303 具体用于：

扫描所述应用程序的安装包，获得所述应用程序的特征；

将所述应用程序的特征与预设的恶意特征进行比对，如果所述应用程序的特征与所述预设的恶意特征匹配，则输出禁止操作提示信息。

- 15 进一步地，本实施例中预处理模块还用于：

如果所述应用程序的特征与所述预设的恶意特征不匹配，则输出权限设置提示信息；

根据接收到的对所述应用程序的权限设置信息，设置所述应用程序的操作许可状态。

- 20 参见图 4，可选地，本实施例中的移动终端还包括：

修改模块 304，用于接收对所述应用程序的权限修改信息，根据所述权限修改信息，修改所述应用程序的操作许可状态。

- 25 可选地，本实施例中，所述应用程序的操作权限包括以下权限中的任一种或多种：短信消息服务 SMS 扣费权限、互动式语音应答 IVR 扣费权限、无线应用协议 WAP 扣费权限、WAP 代扣费权限、移动支付权限和电子银行扣费权限。

- 30 本发明提供的装置实施例的有益效果是当应用程序执行对扣费事件的调用操作时，分析所述应用程序的操作权限；如果所述应用程序具有对所述扣费事件的操作权限，则允许所述应用程序执行所述调用操作；如果所述应用程序不具有对所述扣费事件的操作权限，则禁止所述应用程序执行所述调用操作。本发明实施例进行应用安全处理时，不需要每次运行应用程序时都对应用程序

进行扫描，只需要对应用程序的操作权限进行判定即可，节省了处理时间，避免了资源的浪费，同时不需要用户的参与，方便用户的使用，从而提高了用户的使用体验。

- 5 本实施例提供的移动终端，具体可以与方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

- 10 本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成，也可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

- 15 以上所述仅为本发明的较佳实施例，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、改进等，均应包含在本发明的保护范围之内。

权 利 要 求 书

1、一种应用程序的处理方法，其特征在于，所述方法包括：

当应用程序执行对扣费事件的调用操作时，分析所述应用程序的操作权限；

5 如果所述应用程序具有对所述扣费事件的操作权限，则允许所述应用程序执行所述调用操作；

如果所述应用程序不具有对所述扣费事件的操作权限，则禁止所述应用程序执行所述调用操作。

10 2、根据权利要求1所述的方法，其特征在于，所述分析所述应用程序的操作权限，包括：

获取所述应用程序的操作许可状态；

如果所述操作许可状态为允许，则确认所述应用程序具有对所述扣费事件的操作权限；

15 如果所述操作许可状态为禁止，则确认所述应用程序不具有对所述扣费事件的操作权限。

3、根据权利要求1所述的方法，其特征在于，在应用程序执行对扣费事件的调用操作之前，所述方法还包括：对所述应用程序进行预处理。

20

4、如权利要求3所述的方法，其特征在于，所述对所述应用程序进行预处理，包括：

扫描所述应用程序的安装包，获得所述应用程序的特征；

25 将所述应用程序的特征与预设的恶意特征进行比对，如果所述应用程序的特征与所述预设的恶意特征匹配，则输出禁止操作提示信息。

5、如权利要求4所述的方法，其特征在于，所述对所述应用程序进行预处理，还包括：

30 如果所述应用程序的特征与所述预设的恶意特征不匹配，则输出权限设置提示信息；

根据接收到的对所述应用程序的权限设置信息，设置所述应用程序的操作

许可状态。

6、根据权利要求 3 所述的方法，其特征在于，在对所述应用程序进行预处理之后，所述方法还包括：接收对所述应用程序的权限修改信息，根据所述权限修改信息，修改所述应用程序的操作许可状态。

7、根据权利要求 1-6 任一项所述的方法，其特征在于，所述应用程序的操作权限包括以下权限中的任一种或多种：短信消息服务 SMS 扣费权限、互动式语音应答 IVR 扣费权限、无线应用协议 WAP 扣费权限、WAP 代扣费权限、移动支付权限和电子银行扣费权限。

8、一种移动终端，其特征在于，所述移动终端包括：

分析模块，用于当应用程序执行对扣费事件的调用操作时，分析所述应用程序的操作权限；

15 执行模块，用于如果所述分析模块分析出所述应用程序具有对所述扣费事件的操作权限，则允许所述应用程序执行所述调用操作；如果所述分析模块分析出所述应用程序不具有对所述扣费事件的操作权限，则禁止所述应用程序执行所述调用操作。

20 9、根据权利要求 8 所述的移动终端，其特征在于，所述分析模块包括：

获取单元，用于获取所述应用程序的操作许可状态；

分析单元，用于如果所述操作许可状态为允许，则确认所述应用程序具有对所述扣费事件的操作权限；如果所述操作许可状态为禁止，则确认所述应用程序不具有对所述扣费事件的操作权限。

25

10、根据权利要求 8 所述的移动终端，其特征在于，所述移动终端还包括：

预处理模块，用于在应用程序执行对扣费事件的调用操作之前，对所述应用程序进行预处理。

30 11、根据权利要求 10 所述的移动终端，其特征在于，所述预处理模块具体用于：

扫描所述应用程序的安装包，获得所述应用程序的特征；

将所述应用程序的特征与预设的恶意特征进行比对，如果所述应用程序的特征与所述预设的恶意特征匹配，则输出禁止操作提示信息。

5 12、根据权利要求 11 所述的移动终端，其特征在于，所述预处理模块还用于：

如果所述应用程序的特征与所述预设的恶意特征不匹配，则输出权限设置提示信息；

10 根据接收到的对所述应用程序的权限设置信息，设置所述应用程序的操作许可状态。

13、根据权利要求 10 所述的移动终端，其特征在于，所述移动终端还包括：

修改模块，用于接收对所述应用程序的权限修改信息，根据所述权限修改信息，修改所述应用程序的操作许可状态。

15 14、根据权利要求 8-13 任一项所述的移动终端，其特征在于，所述应用程序的操作权限包括以下权限中的任一种或多种：短信消息服务 SMS 扣费权限、互动式语音应答 IVR 扣费权限、无线应用协议 WAP 扣费权限、WAP 代扣费权限、移动支付权限和电子银行扣费权限。

20

25