(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 103617387 A
(43)申请公布日 2014.03.05

(21)申请号 201310608020.2

(22)申请日 2013.11.25

(71)申请人 北京奇虎科技有限公司
地址 100088 北京市西城区新街口外大街28号D座112室(德胜园区)

(72)发明人 宁敢

(74)专利代理机构 北京国昊天诚知识产权代理有限公司 11315
代理人 许志勇

(51)Int.Cl.
G06F 21/51(2013.01)
G06F 21/56(2013.01)

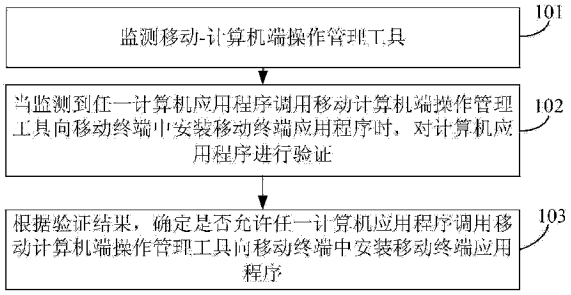
权利要求书2页 说明书12页 附图4页

(54)发明名称

一种防止自动安装应用程序的方法及装置

(57)摘要

本申请公开了一种防止自动安装应用程序的方法及装置,属于通信安全处理领域。所述方法包括:监测移动-计算机端操作管理工具;当监测到任一计算机应用程序调用所述移动-计算机端操作管理工具向移动终端中安装移动终端应用程序时,对任一计算机应用程序进行验证;根据验证结果,确定是否允许任一计算机应用程序调用所述移动-计算机端操作管理工具。所述装置包括:监测模块、验证模块和处理模块。本发明通过对计算机应用程序进行验证,根据验证结果,确定是否允许计算机应用程序调用移动-计算机端操作管理工具,可以阻止计算机应用程序自动向移动终端中安装移动终端应用程序,可以节约移动终端的内存和资源。



CN 103617387 A

1. 一种防止自动安装应用程序的方法，其特征在于，所述方法包括：

监测移动－计算机端操作管理工具；

当监测到任一计算机应用程序调用所述移动－计算机端操作管理工具向移动终端中安装移动终端应用程序时，对任一计算机应用程序进行验证；

根据验证结果，确定是否允许任一计算机应用程序调用所述移动－计算机端操作管理工具向移动终端中安装移动终端应用程序。

2. 如权利要求 1 所述的方法，其特征在于，根据验证结果，确定是否允许任一计算机应用程序调用所述移动－计算机端操作管理工具向移动终端中安装移动终端应用程序，包括：

当判断任一计算机应用程序的进程的类型为位于白名单中的白进程时，则验证成功，允许任一计算机应用程序调用所述移动－计算机端操作管理工具向移动终端中安装移动终端应用程序，以及其他任何操作；

当判断任一计算机应用程序的进程的类型为位于黑名单中的黑进程时，则验证失败，对任一计算机应用程序进行拦截，禁止任一计算机应用程序对移动终端执行任何操作并在用户界面弹出框中展示对任一计算机应用程序拦截成功的信息；

当判断任一计算机应用程序的进程的类型既不是为位于白名单中的白进程也不是位于黑名单中的黑进程时，对任一计算机应用程序的进程进行进一步监控，根据进一步监控的结果，确定是否允许任一计算机应用程序调用所述移动－计算机端操作管理工具向移动终端中安装移动终端应用程序。

3. 如权利要求 1 所述的方法，其特征在于，所述方法还包括：

当获取到任一计算机应用程序向所述移动终端中安装移动终端应用程序安装包的信息时，判断任一计算机应用程序是否是预先锁定的用于安装所述移动终端应用程序安装包的计算机应用程序；

如果是，则允许任一计算机应用程序向所述移动终端中安装所述移动终端应用程序安装包。

4. 如权利要求 3 所述的方法，其特征在于，当获取到任一计算机应用程序向所述移动终端中安装移动终端应用程序安装包的信息时，判断任一计算机应用程序是否是预先锁定的用于安装所述移动终端应用程序安装包的计算机应用程序，包括：

通过注册表防御体系 RD 监控所述移动终端应用程序安装包在注册表中的安装设置项；

当获取到任一计算机应用程序对所述移动终端应用程序安装包在注册表中的安装设置项进行修改的信息时，判断任一计算机应用程序是否具有对所述移动终端应用程序安装包在注册表中的安装设置项进行修改的权限；

如果具有，则确定任一计算机应用程序是预先锁定的用于安装所述移动终端应用程序安装包的计算机应用程序。

5. 如权利要求 1 所述的方法，其特征在于，所述监测移动－计算机端操作管理工具之前，还包括：

检测移动终端连接接口；

当检测到有计算机与移动终端进行连接时，执行监测移动－计算机端操作管理工具的

步骤。

6. 一种防止自动安装应用程序的装置，其特征在于，所述装置包括：

监测模块，用于监测移动－计算机端操作管理工具；

验证模块，用于当监测到任一计算机应用程序调用所述移动－计算机端操作管理工具向移动终端中安装移动终端应用程序时，对任一计算机应用程序进行验证；

第一处理模块，用于根据验证结果，确定是否允许任一计算机应用程序调用所述移动－计算机端操作管理工具向移动终端中安装移动终端应用程序。

7. 如权利要求 6 所述的装置，其特征在于，所述第一处理模块包括：

第一处理单元，用于当判断任一计算机应用程序的进程的类型为位于白名单中的白进程时，则验证成功，允许任一计算机应用程序调用所述移动－计算机端操作管理工具向移动终端中安装移动终端应用程序，以及其他任何操作；

第二处理单元，用于当判断任一计算机应用程序的进程的类型为位于黑名单中的黑进程时，则验证失败，对任一计算机应用程序进行拦截，禁止任一计算机应用程序对移动终端执行任何操作并在用户界面弹出框中展示对任一计算机应用程序拦截成功的信息；

第三处理单元，用于当判断任一计算机应用程序的进程的类型既不是为位于白名单中的白进程也不是位于黑名单中的黑进程时，对任一计算机应用程序的进程进行进一步监控，根据进一步监控的结果，确定是否允许任一计算机应用程序调用所述移动－计算机端操作管理工具向移动终端中安装移动终端应用程序。

8. 如权利要求 6 所述的装置，其特征在于，所述装置还包括：

判断模块，用于当获取到任一计算机应用程序向所述移动终端中安装移动终端应用程序安装包的信息时，判断任一计算机应用程序是否是预先锁定的用于安装所述移动终端应用程序安装包的计算机应用程序；

第二处理模块，用于如果所述判断模块的判断结果是是，则允许任一计算机应用程序向所述移动终端中安装所述移动终端应用程序安装包。

9. 如权利要求 8 所述的装置，其特征在于，所述判断模块包括：

监控单元，用于通过注册表防御体系 RD 监控所述移动终端应用程序安装包在注册表中的安装设置项；

判断单元，用于当获取到任一计算机应用程序对所述移动终端应用程序安装包在注册表中的安装设置项进行修改的信息时，判断任一计算机应用程序是否具有对所述移动终端应用程序安装包在注册表中的安装设置项进行修改的权限；

第一确定单元，用于如果具有，则确定任一计算机应用程序是预先锁定的用于安装所述移动终端应用程序安装包的计算机应用程序。

10. 如权利要求 6 所述的装置，其特征在于，所述装置还包括：

检测模块，用于检测移动终端连接接口；

通知模块，用于当检测到有计算机与移动终端进行连接时，通知所述监测模块执行监测移动－计算机端操作管理工具的步骤。

一种防止自动安装应用程序的方法及装置

技术领域

[0001] 本申请涉及通信安全处理领域，具体涉及一种防止自动安装应用程序的方法及装置。

背景技术

[0002] 随着通信技术的发展，手机等移动终端的功能越来越多，不但可以通过移动终端打电话发短信息，而且还可以在移动终端中安装即使通信等各种移动终端应用程序，实现聊天等各种应用。

[0003] 然而，当将移动终端与计算机连接时，计算机中的计算机应用程序会自动安装相应的移动终端应用程序至移动终端中，而安装的这些移动终端应用程序不一定是用户需要的，浪费移动终端的内存和资源。

发明内容

[0004] 本申请所要解决的技术问题在于提供一种防止自动安装应用程序的方法及装置，当监测到计算机应用程序调用移动－计算机端操作管理工具向移动终端中安装移动终端应用程序时，通过对计算机应用程序进行验证，验证通过后，才允许计算机应用程序调用移动－计算机端操作管理工具，可以阻止计算机应用程序自动向移动终端中安装移动终端应用程序，可以节约移动终端的内存和资源。

[0005] 为了解决上述问题，本申请公开了一种防止自动安装应用程序的方法，所述方法包括：

[0006] 监测移动－计算机端操作管理工具；

[0007] 当监测到任一计算机应用程序调用所述移动－计算机端操作管理工具向移动终端中安装移动终端应用程序时，对任一计算机应用程序进行验证；

[0008] 根据验证结果，确定是否允许任一计算机应用程序调用所述移动－计算机端操作管理工具向移动终端中安装移动终端应用程序。

[0009] 进一步地，根据验证结果，确定是否允许任一计算机应用程序调用所述移动－计算机端操作管理工具向移动终端中安装移动终端应用程序，包括：

[0010] 当判断任一计算机应用程序的进程的类型为位于白名单中的白进程时，则验证成功，允许任一计算机应用程序调用所述移动－计算机端操作管理工具向移动终端中安装移动终端应用程序，以及其他任何操作；

[0011] 当判断任一计算机应用程序的进程的类型为位于黑名单中的黑进程时，则验证失败，对任一计算机应用程序进行拦截，禁止任一计算机应用程序对移动终端执行任何操作并在用户界面弹出框中展示对任一计算机应用程序拦截成功的信息；

[0012] 当判断任一计算机应用程序的进程的类型既不是为位于白名单中的白进程也不是位于黑名单中的黑进程时，对任一计算机应用程序的进程进行进一步监控，根据进一步监控的结果，确定是否允许任一计算机应用程序调用所述移动－计算机端操作管理工具向

移动终端中安装移动终端应用程序。

[0013] 进一步地，所述方法还包括：

[0014] 当获取到任一计算机应用程序向所述移动终端中安装移动终端应用程序安装包的信息时，判断任一计算机应用程序是否是预先锁定的用于安装所述移动终端应用程序安装包的计算机应用程序；

[0015] 如果是，则允许任一计算机应用程序向所述移动终端中安装所述移动终端应用程序安装包。

[0016] 进一步地，当获取到任一计算机应用程序向所述移动终端中安装移动终端应用程序安装包的信息时，判断任一计算机应用程序是否是预先锁定的用于安装所述移动终端应用程序安装包的计算机应用程序，包括：

[0017] 通过注册表防御体系 RD 监控所述移动终端应用程序安装包在注册表中的安装设置项；

[0018] 当获取到任一计算机应用程序对所述移动终端应用程序安装包在注册表中的安装设置项进行修改的信息时，判断任一计算机应用程序是否具有对所述移动终端应用程序安装包在注册表中的安装设置项进行修改的权限；

[0019] 如果具有，则确定任一计算机应用程序是预先锁定的用于安装所述移动终端应用程序安装包的计算机应用程序。

[0020] 进一步地，所述移动 - 计算机端操作管理工具为：安卓调试桥 ADB；

[0021] 相应地，所述移动终端应用程序安装包为：安卓安装包 APK。

[0022] 进一步地，所述方法还包括：

[0023] 提取所述移动终端中包含的 APK 的信息；所述 APK 的信息包括：安装包名称、版本号、数字签名、安卓组件接收器的特征、安卓组件服务的特征、安卓组件活动的特征、可执行文件中的指令和 / 或 APK 目录下各文件的消息摘要算法第五版 MD5 值；

[0024] 将提取出的信息发送至设置有安全识别库的服务器侧，以使所述服务器侧利用安全识别库中的特征信息对所述移动终端中包含的 APK 的信息进行扫描；

[0025] 接收所述服务器侧下发的扫描结果。

[0026] 进一步地，所述监测移动 - 计算机端操作管理工具之前，还包括：

[0027] 检测移动终端连接接口；

[0028] 当检测到有计算机与移动终端进行连接时，执行监测移动 - 计算机端操作管理工具的步骤。

[0029] 进一步地，所述方法还包括：

[0030] 对所述移动终端进行安全扫描；

[0031] 鉴别所述移动终端中是否存在木马、恶意扣费软件和 / 或山寨软件。

[0032] 进一步地，所述鉴别所述移动终端中是否存在或山寨软件包括：

[0033] 从所述移动终端中某移动终端应用软件对应的安装包的元信息 META-INF 目录下提取开发者签名；

[0034] 从某移动终端应用软件对应的安装包的项目自描述文件 manifast.xml 中的许可 permission 组件解析得到应用权限信息；

[0035] 根据某移动终端应用软件对应的安装包的开发者签名偏离其他安装包的开发者

签名的状况，以及应用权限信息，确定某移动终端应用软件是否为山寨软件。

[0036] 为了解决上述问题，本申请公开了一种防止自动安装应用程序的装置，所述装置包括：

[0037] 监测模块，用于监测移动－计算机端操作管理工具；

[0038] 验证模块，用于当监测到任一计算机应用程序调用所述移动－计算机端操作管理工具向移动终端中安装移动终端应用程序时，对任一计算机应用程序进行验证；

[0039] 第一处理模块，用于根据验证结果，确定是否允许任一计算机应用程序调用所述移动－计算机端操作管理工具向移动终端中安装移动终端应用程序。

[0040] 进一步地，所述第一处理模块包括：

[0041] 第一处理单元，用于当判断任一计算机应用程序的进程的类型为位于白名单中的白进程时，则验证成功，允许任一计算机应用程序调用所述移动－计算机端操作管理工具向移动终端中安装移动终端应用程序，以及其他任何操作；

[0042] 第二处理单元，用于当判断任一计算机应用程序的进程的类型为位于黑名单中的黑进程时，则验证失败，对任一计算机应用程序进行拦截，禁止任一计算机应用程序对移动终端执行任何操作并在用户界面弹出框中展示对任一计算机应用程序拦截成功的信息；

[0043] 第三处理单元，用于当判断任一计算机应用程序的进程的类型既不是为位于白名单中的白进程也不是位于黑名单中的黑进程时，对任一计算机应用程序的进程进行进一步监控，根据进一步监控的结果，确定是否允许任一计算机应用程序调用所述移动－计算机端操作管理工具向移动终端中安装移动终端应用程序。

[0044] 进一步地，所述装置还包括：

[0045] 判断模块，用于当获取到任一计算机应用程序向所述移动终端中安装移动终端应用程序安装包的信息时，判断任一计算机应用程序是否是预先锁定的用于安装所述移动终端应用程序安装包的计算机应用程序；

[0046] 第二处理模块，用于如果所述判断模块的判断结果是是，则允许任一计算机应用程序向所述移动终端中安装所述移动终端应用程序安装包。

[0047] 进一步地，所述判断模块包括：

[0048] 监控单元，用于通过注册表防御体系 RD 监控所述移动终端应用程序安装包在注册表中的安装设置项；

[0049] 判断单元，用于当获取到任一计算机应用程序对所述移动终端应用程序安装包在注册表中的安装设置项进行修改的信息时，判断任一计算机应用程序是否具有对所述移动终端应用程序安装包在注册表中的安装设置项进行修改的权限；

[0050] 第一确定单元，用于如果具有，则确定任一计算机应用程序是预先锁定的用于安装所述移动终端应用程序安装包的计算机应用程序。

[0051] 进一步地，所述移动－计算机端操作管理工具为：安卓调试桥 ADB；

[0052] 相应地，所述移动终端应用程序安装包为：安卓安装包 APK。

[0053] 进一步地，所述装置还包括：

[0054] 提取模块，用于提取所述移动终端中包含的 APK 的信息；所述 APK 的信息包括：安装包名称、版本号、数字签名、安卓组件接收器的特征、安卓组件服务的特征、安卓组件活动的特征、可执行文件中的指令和／或 APK 目录下各文件的消息摘要算法第五版 MD5 值；

[0055] 发送模块，用于将提取出的信息发送至设置有安全识别库的服务器侧，以使所述服务器侧利用安全识别库中的特征信息对所述移动终端中包含的 APK 的信息进行扫描；

[0056] 接收模块，用于接收所述服务器侧下发的扫描结果。

[0057] 进一步地，所述装置还包括：

[0058] 检测模块，用于检测计算机的移动终端连接接口；

[0059] 通知模块，用于当检测到有移动终端与计算机进行连接时，通知所述监测模块执行监测移动 - 计算机端操作管理工具的步骤。

[0060] 进一步地，所述装置还包括：

[0061] 扫描模块，用于对所述移动终端进行安全扫描；

[0062] 鉴别模块，用于鉴别所述移动终端中是否存在木马、恶意扣费软件和 / 或山寨软件。

[0063] 进一步地，所述鉴别模块包括：

[0064] 提取单元，用于从所述移动终端中某移动终端应用软件对应的安装包的元信息 META-INF 目录下提取开发者签名；

[0065] 解析单元，用于从某移动终端应用软件对应的安装包的项目自描述文件 manifast.xml 中的许可 permission 组件解析得到应用权限信息；

[0066] 第二确定单元，用于根据某移动终端应用软件对应的安装包的开发者签名偏离其他安装包的开发者签名的状况，以及应用权限信息，确定某移动终端应用软件是否为山寨软件。

[0067] 与现有技术相比，本申请可以获得包括以下技术效果：

[0068] 当监测到计算机应用程序调用移动 - 计算机端操作管理工具向移动终端中安装移动终端应用程序时，通过对计算机应用程序进行验证，根据验证结果，确定是否允许计算机应用程序调用移动 - 计算机端操作管理工具，可以阻止计算机应用程序自动向移动终端中安装移动终端应用程序，可以节约移动终端的内存和资源。当获取到计算机应用程序向移动终端中安装移动终端应用程序安装包的信息时，判定计算机应用程序是预先锁定的用于安装该应用程序安装包的计算机应用程序时，才允许计算机应用程序向移动终端中安装移动终端应用程序安装包，使得只有预先锁定的计算机应用程序才有权安装该应用程序安装包到移动终端，实现了对安装应用程序安装包的计算机应用程序的锁定。

[0069] 当然，实施本申请的任一产品必不一定需要同时达到以上所述的所有技术效果。

附图说明

[0070] 此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

[0071] 图 1 是本申请实施例的第一种防止自动安装应用程序的方法流程图；

[0072] 图 2 是本申请实施例的第二种防止自动安装应用程序的方法流程图；

[0073] 图 3 是本申请实施例的第一种防止自动安装应用程序的装置结构示意图；

[0074] 图 4 是本申请实施例的第二种防止自动安装应用程序的装置结构示意图；

[0075] 图 5 是本申请实施例的第三种防止自动安装应用程序的装置结构示意图。

具体实施方式

[0076] 以下将配合附图及实施例来详细说明本申请的实施方式，藉此对本申请如何应用技术手段来解决技术问题并达成技术功效的实现过程能充分理解并据以实施。

[0077] 实施例描述

[0078] 下面以一实施例对本申请方法的实现作进一步说明。如图 1 所示，为本申请实施例的一种防止自动安装应用程序的方法流程图，该方法包括：

[0079] S101：监测移动 - 计算机端操作管理工具。

[0080] S102：当监测到任一计算机应用程序调用移动 - 计算机端操作管理工具向移动终端中安装移动终端应用程序时，对计算机应用程序进行验证。

[0081] S103：根据验证结果，确定是否允许任一计算机应用程序调用移动 - 计算机端操作管理工具向移动终端中安装移动终端应用程序。

[0082] 优选地，根据验证结果，确定是否允许任一计算机应用程序调用移动 - 计算机端操作管理工具向移动终端中安装移动终端应用程序，包括：

[0083] 当判断任一计算机应用程序的进程的类型为位于白名单中的白进程时，则验证成功，允许任一计算机应用程序调用移动 - 计算机端操作管理工具向移动终端中安装移动终端应用程序，以及其他任何操作；

[0084] 当判断任一计算机应用程序的进程的类型为位于黑名单中的黑进程时，则验证失败，对任一计算机应用程序进行拦截，禁止任一计算机应用程序对移动终端执行任何操作并在用户界面弹出框中展示对任一计算机应用程序拦截成功的信息；

[0085] 当判断任一计算机应用程序的进程的类型既不是为位于白名单中的白进程也不是位于黑名单中的黑进程时，对任一计算机应用程序的进程进行进一步监控，根据进一步监控的结果，确定是否允许任一计算机应用程序调用移动 - 计算机端操作管理工具向移动终端中安装移动终端应用程序。

[0086] 优选地，该方法还包括：

[0087] 当获取到任一计算机应用程序向移动终端中安装移动终端应用程序安装包的信息时，判断任一计算机应用程序是否是预先锁定的用于安装该移动终端应用程序安装包的计算机应用程序；

[0088] 如果是，则允许任一计算机应用程序向移动终端中安装移动终端应用程序安装包。

[0089] 优选地，当获取到任一计算机应用程序向移动终端中安装移动终端应用程序安装包的信息时，判断任一计算机应用程序是否是预先锁定的用于安装移动终端应用程序安装包的计算机应用程序，包括：

[0090] 通过注册表防御体系 RD 监控移动终端应用程序安装包在注册表中的安装设置项；

[0091] 当获取到任一计算机应用程序对移动终端应用程序安装包在注册表中的安装设置项进行修改的信息时，判断任一计算机应用程序是否具有对移动终端应用程序安装包在注册表中的安装设置项进行修改的权限；

[0092] 如果具有，则确定任一计算机应用程序是预先锁定的用于安装移动终端应用程序安装包的计算机应用程序。

[0093] 优选地，移动－计算机端操作管理工具为：安卓调试桥 ADB；相应地，移动终端应用程序安装包为：安卓安装包 APK。

[0094] 优选地，该方法还包括：

[0095] 提取移动终端中包含的 APK 的信息；APK 的信息包括：安装包名称、版本号、数字签名、安卓组件接收器的特征、安卓组件服务的特征、安卓组件活动的特征、可执行文件中的指令和／或 APK 目录下各文件的消息摘要算法第五版 MD5 值；

[0096] 将提取出的信息发送至设置有安全识别库的服务器侧，以使服务器侧利用安全识别库中的特征信息对移动终端中包含的 APK 的信息进行扫描；

[0097] 接收服务器侧下发的扫描结果。

[0098] 优选地，监测移动－计算机端操作管理工具之前，还包括：

[0099] 检测移动终端连接接口；

[0100] 当检测到有计算机与移动终端进行连接时，执行监测移动－计算机端操作管理工具的步骤。

[0101] 优选地，该方法还包括：

[0102] 对移动终端进行安全扫描；

[0103] 鉴别移动终端中是否存在木马、恶意扣费软件和／或山寨软件。

[0104] 优选地，鉴别移动终端中是否存在或山寨软件包括：

[0105] 从移动终端中某移动终端应用软件对应的安装包的元信息 META-INF 目录下提取开发者签名；

[0106] 从某移动终端应用软件对应的安装包的项目自描述文件 manifast.xml 中的许可 permission 组件解析得到应用权限信息；

[0107] 根据某移动终端应用软件对应的安装包的开发者签名偏离其他安装包的开发者签名的状况，以及应用权限信息，确定某移动终端应用软件是否为山寨软件。

[0108] 本实施例所述的防止自动安装应用程序的方法，当监测到计算机应用程序调用移动－计算机端操作管理工具向移动终端中安装移动终端应用程序时，通过对计算机应用程序进行验证，根据验证结果，确定是否允许计算机应用程序调用移动－计算机端操作管理工具，可以阻止计算机应用程序自动向移动终端中安装移动终端应用程序，可以节约移动终端的内存和资源。当获取到计算机应用程序向移动终端中安装移动终端应用程序安装包的信息时，判定计算机应用程序是预先锁定的用于安装该应用程序安装包的计算机应用程序时，才允许计算机应用程序向移动终端中安装移动终端应用程序安装包，使得只有预先锁定的计算机应用程序才有权安装该应用程序安装包到移动终端，实现了对安装应用程序安装包的计算机应用程序的锁定。

[0109] 下面以另一实施例对本申请方法的实现作进一步说明。如图 2 所示，为本申请实施例的一种防止自动安装应用程序的方法流程图，该方法包括：

[0110] S201：检测移动终端连接接口，判断是否有计算机与移动终端进行连接，如果有，则执行 S202；否则，结束。

[0111] 具体地，移动终端连接接口可以是 USB 接口等可以与计算机等进行连接的接口。

[0112] S202：监测移动－计算机端操作管理工具，判断是否有计算机应用程序调用移动－计算机端操作管理工具向移动终端中安装移动终端应用程序，如果有，则执行 S203；否

则，执行 S206。

[0113] 具体地，当手机等移动终端的系统为 Android 系统时，移动 - 计算机端操作管理工具为：安卓调试桥 ADB；相应地，移动终端应用程序安装包为：安卓安装包 APK。

[0114] 具体地，手机等移动终端的系统还可以为 symbian、Linux、Palm、BlackBerry、BADA、WindowsMobile、iOS unbutu、wp8 等系统。移动 - 计算机端操作管理工具和移动终端应用程序安装包可以为与上述系统相应的工具和包，对此不做具体限定。

[0115] S203：对计算机应用程序进行验证，判断验证是否成功，如果成功，则执行 S204；否则，执行 S205。

[0116] 具体地，当判断计算机应用程序的进程的类型为位于白名单中的白进程时，则验证成功，允许计算机应用程序调用移动 - 计算机端操作管理工具向移动终端中安装移动终端应用程序，以及其他任何操作；

[0117] 当判断计算机应用程序的进程的类型为位于黑名单中的黑进程时，则验证失败，对计算机应用程序进行拦截，禁止任一计算机应用程序对移动终端执行任何操作并在用户界面弹出框中展示对任一计算机应用程序拦截成功的信息。

[0118] 具体地，还包括：

[0119] 当判断计算机应用程序的进程的类型既不是为位于白名单中的白进程也不是位于黑名单中的黑进程时，对任一计算机应用程序的进程进行进一步监控，根据进一步监控的结果，确定是否允许计算机应用程序调用移动 - 计算机端操作管理工具向移动终端中安装移动终端应用程序。

[0120] 具体地，当计算机应用程序的进程的类型既不是为位于白名单中的白进程也不是位于黑名单中的黑进程时，可以称该进程的类型为灰进程(即不在白名单和黑名单中的未知进程)，当监测到的进程的类型属于灰进程时，需要对该进程进行进一步的监控，确定是否允许该灰进程相关的计算机应用程序调用移动 - 计算机端操作管理工具向移动终端中安装移动终端应用程序。

[0121] 其中，本实施例中在服务器的数据库中会维护一个白名单和黑名单，白名单为记录安全进程的名单，黑名单为记录危险进程的名单，当进程位于白名单中时，允许该白进程后续的所有操作，不再对该白进程进行监控，当进程位于黑名单中时，立即执行拦截。

[0122] S204：允许计算机应用程序调用移动 - 计算机端操作管理工具，然后执行 S206。

[0123] S205：禁止计算机应用程序调用移动 - 计算机端操作管理工具，然后执行 S206。

[0124] S206：判断是否获取到计算机应用程序向移动终端中安装移动终端应用程序安装包的信息，如果有，则执行 S207；否则，结束。

[0125] S207：判断计算机应用程序是否是预先锁定的用于安装移动终端应用程序安装包的计算机应用程序，如果是，则执行 S208；否则，执行 S209。

[0126] 具体地，当获取到任一计算机应用程序向移动终端中安装移动终端应用程序安装包的信息时，判断任一计算机应用程序是否是预先锁定的用于安装移动终端应用程序安装包的计算机应用程序，包括：

[0127] 通过注册表防御体系 RD 监控移动终端应用程序安装包在注册表中的安装设置项；

[0128] 当获取到任一计算机应用程序对移动终端应用程序安装包在注册表中的安装设

置项进行修改的信息时，判断任一计算机应用程序是否具有对移动终端应用程序安装包在注册表中的安装设置项进行修改的权限；

[0129] 如果具有，则确定任一计算机应用程序是预先锁定的用于安装移动终端应用程序安装包的计算机应用程序；否则，计算机应用程序不是预先锁定的用于安装移动终端应用程序安装包的计算机应用程序。

[0130] 其中，移动－计算机端操作管理工具为：安卓调试桥 ADB；相应地，移动终端应用程序安装包为：安卓安装包 APK。

[0131] 相应地，该方法还包括：

[0132] 提取移动终端中包含的 APK 的信息；移动终端中包含的 APK 的信息包括：安装包名称、版本号、数字签名、安卓组件接收器的特征、安卓组件服务的特征、安卓组件活动的特征、可执行文件中的指令和／或 APK 目录下各文件的消息摘要算法第五版 MD5 值；

[0133] 将提取出的信息发送至设置有安全识别库的服务器侧，以使服务器侧利用安全识别库中的特征信息对移动终端中包含的 APK 的信息进行扫描；

[0134] 接收服务器侧下发的扫描结果。

[0135] S208：允许计算机应用程序向移动终端中安装移动终端应用程序安装包，然后结束。

[0136] S209：禁止计算机应用程序向移动终端中安装移动终端应用程序安装包，然后结束。

[0137] 需要说明的是，该方法还可以包括：

[0138] 对移动终端进行安全扫描；

[0139] 鉴别移动终端中是否存在木马、恶意扣费软件和／或山寨软件。

[0140] 具体地，鉴别移动终端中是否存在或山寨软件包括：

[0141] 从移动终端中某移动终端应用软件对应的安装包的元信息 META-INF 目录下提取开发者签名；

[0142] 从某移动终端应用软件对应的安装包的项目自描述文件 manifast.xml 中的许可 permission 组件解析得到应用权限信息；

[0143] 根据某移动终端应用软件对应的安装包的开发者签名偏离其他安装包的开发者签名的状况，以及应用权限信息，确定某移动终端应用软件是否为山寨软件。

[0144] 本实施例所述的防止自动安装应用程序的方法，当监测到计算机应用程序调用移动－计算机端操作管理工具向移动终端中安装移动终端应用程序时，通过对计算机应用程序进行验证，根据验证结果，确定是否允许计算机应用程序调用移动－计算机端操作管理工具，可以阻止计算机应用程序自动向移动终端中安装移动终端应用程序，可以节约移动终端的内存和资源。当获取到计算机应用程序向移动终端中安装移动终端应用程序安装包的信息时，判定计算机应用程序是预先锁定的用于安装该应用程序安装包的计算机应用程序时，才允许计算机应用程序向移动终端中安装移动终端应用程序安装包，使得只有预先锁定的计算机应用程序才有权安装该应用程序安装包到移动终端，实现了对安装应用程序安装包的计算机应用程序的锁定。

[0145] 如图 3 所示，是本申请实施例的装置结构图。防止自动安装应用程序的装置，包括：

[0146] 监测模块 301，用于监测移动 - 计算机端操作管理工具；

[0147] 验证模块 302，用于当监测到任一计算机应用程序调用移动 - 计算机端操作管理工具向移动终端中安装移动终端应用程序时，对任一计算机应用程序进行验证；

[0148] 第一处理模块 303，用于根据验证结果，确定是否允许任一计算机应用程序调用移动 - 计算机端操作管理工具向移动终端中安装移动终端应用程序。

[0149] 优选地，第一处理模块 303 包括：

[0150] 第一处理单元，用于当判断任一计算机应用程序的进程的类型为位于白名单中的白进程时，则验证成功，允许任一计算机应用程序调用移动 - 计算机端操作管理工具向移动终端中安装移动终端应用程序，以及其他任何操作；

[0151] 第二处理单元，用于当判断任一计算机应用程序的进程的类型为位于黑名单中的黑进程时，则验证失败，对任一计算机应用程序进行拦截，禁止任一计算机应用程序对移动终端执行任何操作并在用户界面弹出框中展示对任一计算机应用程序拦截成功的信息；

[0152] 第三处理单元，用于当判断任一计算机应用程序的进程的类型既不是为位于白名单中的白进程也不是位于黑名单中的黑进程时，对任一计算机应用程序的进程进行进一步监控，根据进一步监控的结果，确定是否允许任一计算机应用程序调用移动 - 计算机端操作管理工具向移动终端中安装移动终端应用程序。

[0153] 优选地，参见图 4，该装置还包括：

[0154] 判断模块 304，用于当获取到任一计算机应用程序向移动终端中安装移动终端应用程序安装包的信息时，判断任一计算机应用程序是否是预先锁定的用于安装该移动终端应用程序安装包的计算机应用程序；

[0155] 第二处理模块 305，用于如果判断模块 304 的判断结果是是，则允许任一计算机应用程序向移动终端中安装移动终端应用程序安装包。

[0156] 优选地，判断模块 304 包括：

[0157] 监控单元，用于通过注册表防御体系 RD 监控移动终端应用程序安装包在注册表中的安装设置项；

[0158] 判断单元，用于当获取到任一计算机应用程序对移动终端应用程序安装包在注册表中的安装设置项进行修改的信息时，判断任一计算机应用程序是否具有对移动终端应用程序安装包在注册表中的安装设置项进行修改的权限；

[0159] 第一确定单元，用于如果具有，则确定任一计算机应用程序是预先锁定的用于安装移动终端应用程序安装包的计算机应用程序。

[0160] 优选地，移动 - 计算机端操作管理工具为：安卓调试桥 ADB；

[0161] 相应地，移动终端应用程序安装包为：安卓安装包 APK。

[0162] 优选地，该装置还包括：

[0163] 提取模块，用于提取移动终端中包含的 APK 的信息；APK 的信息包括：安装包名称、版本号、数字签名、安卓组件接收器的特征、安卓组件服务的特征、安卓组件活动的特征、可执行文件中的指令和 / 或 APK 目录下各文件的消息摘要算法第五版 MD5 值；

[0164] 发送模块，用于将提取出的信息发送至设置有安全识别库的服务器侧，以使服务器侧利用安全识别库中的特征信息对移动终端中包含的 APK 的信息进行扫描；

[0165] 接收模块，用于接收服务器侧下发的扫描结果。

[0166] 优选地，参见图 5，该装置还包括：

[0167] 检测模块 306，用于检测移动终端连接接口；

[0168] 通知模块 307，用于当检测到有计算机与移动终端进行连接时，通知监测模块 301 执行监测移动 - 计算机端操作管理工具的步骤。

[0169] 优选地，该装置还包括：

[0170] 扫描模块，用于对移动终端进行安全扫描；

[0171] 鉴别模块，用于鉴别移动终端中是否存在木马、恶意扣费软件和 / 或山寨软件。

[0172] 优选地，鉴别模块包括：

[0173] 提取单元，用于从移动终端中某移动终端应用软件对应的安装包的元信息 META-INF 目录下提取开发者签名；

[0174] 解析单元，用于从某移动终端应用软件对应的安装包的项目自描述文件 manifast.xml 中的许可 permission 组件解析得到应用权限信息；

[0175] 第二确定单元，用于根据某移动终端应用软件对应的安装包的开发者签名偏离其他安装包的开发者签名的状况，以及应用权限信息，确定某移动终端应用软件是否为山寨软件。

[0176] 所述装置与前述的方法流程描述对应，不足之处参考上述方法流程的叙述，不再一一赘述。

[0177] 本实施例所述的防止自动安装应用程序的装置，当监测到计算机应用程序调用移动 - 计算机端操作管理工具向移动终端中安装移动终端应用程序时，通过对计算机应用程序进行验证，根据验证结果，确定是否允许计算机应用程序调用移动 - 计算机端操作管理工具，可以阻止计算机应用程序自动向移动终端中安装移动终端应用程序，可以节约移动终端的内存和资源。当获取到计算机应用程序向移动终端中安装移动终端应用程序安装包的信息时，判定计算机应用程序是预先锁定的用于安装该应用程序安装包的计算机应用程序时，才允许计算机应用程序向移动终端中安装移动终端应用程序安装包，使得只有预先锁定的计算机应用程序才有权安装该应用程序安装包到移动终端，实现了对安装应用程序安装包的计算机应用程序的锁定。

[0178] 上述说明示出并描述了本申请的若干优选实施例，但如前所述，应当理解本申请并非局限于本文所披露的形式，不应看作是对其他实施例的排除，而可用于各种其他组合、修改和环境，并能够在本文所述发明构想范围内，通过上述教导或相关领域的技术或知识进行改动。而本领域人员所进行的改动和变化不脱离本申请的精神和范围，则都应在本申请所附权利要求的保护范围内。

[0179] 本申请的实施例揭示了 A1、一种防止自动安装应用程序的方法，其特征在于，所述方法包括：监测移动 - 计算机端操作管理工具；当监测到任一计算机应用程序调用所述移动 - 计算机端操作管理工具向移动终端中安装移动终端应用程序时，对任一计算机应用程序进行验证；根据验证结果，确定是否允许任一计算机应用程序调用所述移动 - 计算机端操作管理工具向移动终端中安装移动终端应用程序。A2、如 A1 所述的方法，其特征在于，根据验证结果，确定是否允许任一计算机应用程序调用所述移动 - 计算机端操作管理工具向移动终端中安装移动终端应用程序，包括：当判断任一计算机应用程序的进程的类型为位于白名单中的白进程时，则验证成功，允许任一计算机应用程序调用所述移动 - 计算机端操作管理工具向移动终端中安装移动终端应用程序，以及其他任何操作；当判断任一计算

机应用程序的进程的类型为位于黑名单中的黑进程时，则验证失败，对任一计算机应用程序进行拦截，禁止任一计算机应用程序对移动终端执行任何操作并在用户界面弹出框中展示对任一计算机应用程序拦截成功的信息；当判断任一计算机应用程序的进程的类型既不是为位于白名单中的白进程也不是位于黑名单中的黑进程时，对任一计算机应用程序的进程进行进一步监控，根据进一步监控的结果，确定是否允许任一计算机应用程序调用所述移动－计算机端操作管理工具向移动终端中安装移动终端应用程序。A3、如 A1 所述的方法，其特征在于，所述方法还包括：当获取到任一计算机应用程序向所述移动终端中安装移动终端应用程序安装包的信息时，判断任一计算机应用程序是否是预先锁定的用于安装所述移动终端应用程序安装包的计算机应用程序；如果是，则允许任一计算机应用程序向所述移动终端中安装所述移动终端应用程序安装包。A4、如 A3 所述的方法，其特征在于，当获取到任一计算机应用程序向所述移动终端中安装移动终端应用程序安装包的信息时，判断任一计算机应用程序是否是预先锁定的用于安装所述移动终端应用程序安装包的计算机应用程序，包括：通过注册表防御体系 RD 监控所述移动终端应用程序安装包在注册表中的安装设置项；当获取到任一计算机应用程序对所述移动终端应用程序安装包在注册表中的安装设置项进行修改的信息时，判断任一计算机应用程序是否具有对所述移动终端应用程序安装包在注册表中的安装设置项进行修改的权限；如果具有，则确定任一计算机应用程序是预先锁定的用于安装所述移动终端应用程序安装包的计算机应用程序。A5、如 A3 所述的方法，其特征在于，所述移动－计算机端操作管理工具为：安卓调试桥 ADB；相应地，所述移动终端应用程序安装包为：安卓安装包 APK。A6、如 A5 所述的方法，其特征在于，所述方法还包括：提取所述移动终端中包含的 APK 的信息；所述 APK 的信息包括：安装包名称、版本号、数字签名、安卓组件接收器的特征、安卓组件服务的特征、安卓组件活动的特征、可执行文件中的指令和／或 APK 目录下各文件的消息摘要算法第五版 MD5 值；将提取出的信息发送至设置有安全识别库的服务器侧，以使所述服务器侧利用安全识别库中的特征信息对所述移动终端中包含的 APK 的信息进行扫描；接收所述服务器侧下发的扫描结果。A7、如 A1 所述的方法，其特征在于，所述监测移动－计算机端操作管理工具之前，还包括：检测移动终端连接接口；当检测到有计算机与移动终端进行连接时，执行监测移动－计算机端操作管理工具的步骤。A8、如 A1-7 任一权利所述的方法，其特征在于，所述方法还包括：对所述移动终端进行安全扫描；鉴别所述移动终端中是否存在木马、恶意扣费软件和／或山寨软件。A9、如 A8 所述的方法，其特征在于，所述鉴别所述移动终端中是否存在或山寨软件包括：从所述移动终端中某移动终端应用软件对应的安装包的元信息 META-INF 目录下提取开发者签名；从某移动终端应用软件对应的安装包的项目自描述文件 manifast.xml 中的许可 permission 组件解析得到应用权限信息；根据某移动终端应用软件对应的安装包的开发者签名偏离其他安装包的开发者签名的状况，以及应用权限信息，确定某移动终端应用软件是否为山寨软件。

[0180] 本申请的实施例还揭示了 B10、一种防止自动安装应用程序的装置，其特征在于，所述装置包括：监测模块，用于监测移动－计算机端操作管理工具；验证模块，用于当监测到任一计算机应用程序调用所述移动－计算机端操作管理工具向移动终端中安装移动终端应用程序时，对任一计算机应用程序进行验证；第一处理模块，用于根据验证结果，确定是否允许任一计算机应用程序调用所述移动－计算机端操作管理工具向移动终端中安装

移动终端应用程序。B11、如 B10 所述的装置，其特征在于，所述第一处理模块包括：第一处理单元，用于当判断任一计算机应用程序的进程的类型为位于白名单中的白进程时，则验证成功，允许任一计算机应用程序调用所述移动 - 计算机端操作管理工具向移动终端中安装移动终端应用程序，以及其他任何操作；第二处理单元，用于当判断任一计算机应用程序的进程的类型为位于黑名单中的黑进程时，则验证失败，对任一计算机应用程序进行拦截，禁止任一计算机应用程序对移动终端执行任何操作并在用户界面弹出框中展示对任一计算机应用程序拦截成功的信息；第三处理单元，用于当判断任一计算机应用程序的进程的类型既不是为位于白名单中的白进程也不是位于黑名单中的黑进程时，对任一计算机应用程序的进程进行进一步监控，根据进一步监控的结果，确定是否允许任一计算机应用程序调用所述移动 - 计算机端操作管理工具向移动终端中安装移动终端应用程序。B12、如 B10 所述的装置，其特征在于，所述装置还包括：判断模块，用于当获取到任一计算机应用程序向所述移动终端中安装移动终端应用程序安装包的信息时，判断任一计算机应用程序是否是预先锁定的用于安装所述移动终端应用程序安装包的计算机应用程序；第二处理模块，用于如果所述判断模块的判断结果是是，则允许任一计算机应用程序向所述移动终端中安装所述移动终端应用程序安装包。B13、如 B12 所述的装置，其特征在于，所述判断模块包括：监控单元，用于通过注册表防御体系 RD 监控所述移动终端应用程序安装包在注册表中的安装设置项；判断单元，用于当获取到任一计算机应用程序对所述移动终端应用程序安装包在注册表中的安装设置项进行修改的信息时，判断任一计算机应用程序是否具有对所述移动终端应用程序安装包在注册表中的安装设置项进行修改的权限；第一确定单元，用于如果具有，则确定任一计算机应用程序是预先锁定的用于安装所述移动终端应用程序安装包的计算机应用程序。B14、如 B12 所述的装置，其特征在于，所述移动 - 计算机端操作管理工具为：安卓调试桥 ADB；相应地，所述移动终端应用程序安装包为：安卓安装包 APK。B15、如 B10 所述的装置，其特征在于，所述装置还包括：提取模块，用于提取所述移动终端中包含的 APK 的信息；所述 APK 的信息包括：安装包名称、版本号、数字签名、安卓组件接收器的特征、安卓组件服务的特征、安卓组件活动的特征、可执行文件中的指令和 / 或 APK 目录下各文件的消息摘要算法第五版 MD5 值；发送模块，用于将提取出的信息发送至设置有安全识别库的服务器侧，以使所述服务器侧利用安全识别库中的特征信息对所述移动终端中包含的 APK 的信息进行扫描；接收模块，用于接收所述服务器侧下发的扫描结果。B16、如 B10 所述的装置，其特征在于，所述装置还包括：检测模块，用于检测移动终端连接接口；通知模块，用于当检测到有计算机与移动终端进行连接时，通知所述监测模块执行监测移动 - 计算机端操作管理工具的步骤。B17、如 B10-16 任一权利要求所述的装置，其特征在于，所述装置还包括：扫描模块，用于对所述移动终端进行安全扫描；鉴别模块，用于鉴别所述移动终端中是否存在木马、恶意扣费软件和 / 或山寨软件。B18、如 B17 所述的装置，其特征在于，所述鉴别模块包括：提取单元，用于从所述移动终端中某移动终端应用软件对应的安装包的元信息 META-INF 目录下提取开发者签名；解析单元，用于从某移动终端应用软件对应的安装包的项目自描述文件 manifast.xml 中的许可 permission 组件解析得到应用权限信息；第二确定单元，用于根据某移动终端应用软件对应的安装包的开发者签名偏离其他安装包的开发者签名的状况，以及应用权限信息，确定某移动终端应用软件是否为山寨软件。

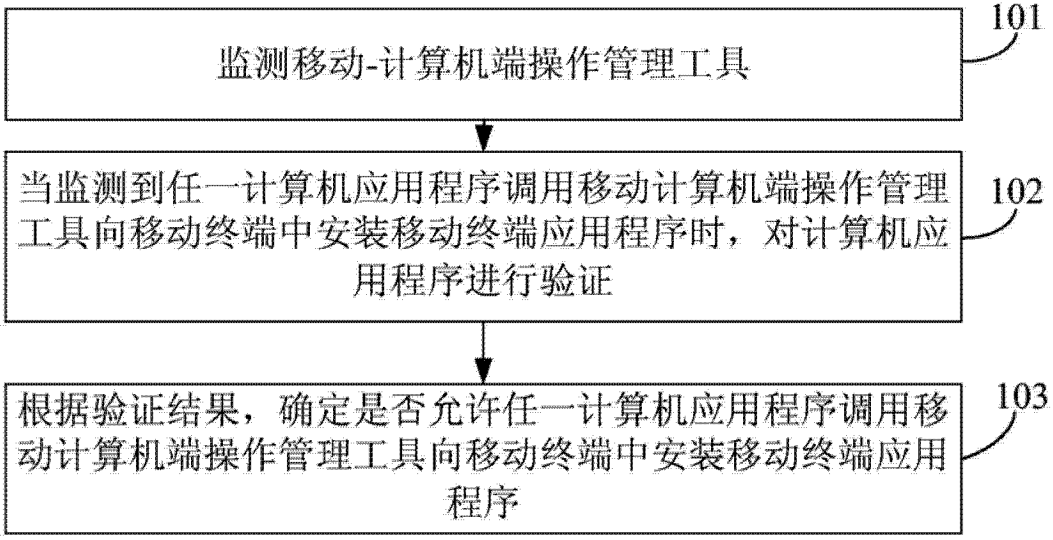

监测移动-计算机端操作管理工具
101
当监测到任一计算机应用程序调用移动计算机端操作管理工具向移动终端中安装移动终端应用程序时，对计算机应用程序进行验证
102
根据验证结果，确定是否允许任一计算机应用程序调用移动计算机端操作管理工具向移动终端中安装移动终端应用程序
103

图 1

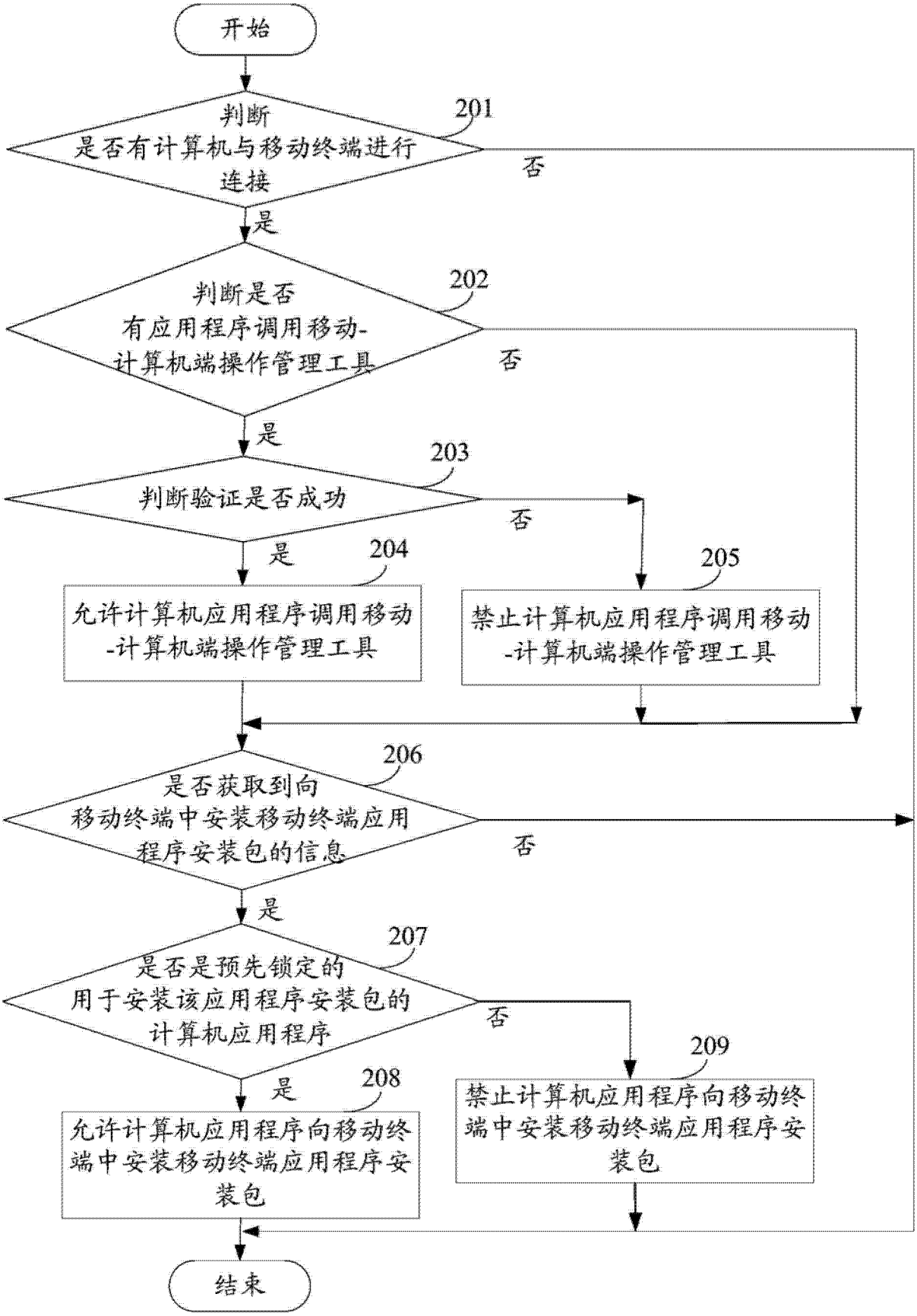

开始
判断是否有计算机与移动终端进行连接
201
否
是
判断是否有应用程序调用移动-计算机端操作管理工具
202
否
是
判断验证是否成功
203
否
是
204
允许计算机应用程序调用移动-计算机端操作管理工具
205
禁止计算机应用程序调用移动-计算机端操作管理工具
是否获取到向移动终端中安装移动终端应用程序安装包的信息
206
否
是
是否是预先锁定的用于安装该应用程序安装包的计算机应用程序
207
否
是
208
允许计算机应用程序向移动终端中安装移动终端应用程序安装包
209
禁止计算机应用程序向移动终端中安装移动终端应用程序安装包
结束

图 2

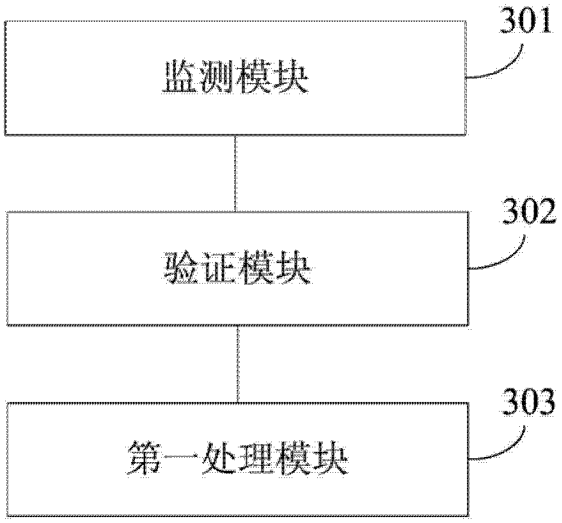

301
监测模块
302
验证模块
303
第一处理模块

图 3

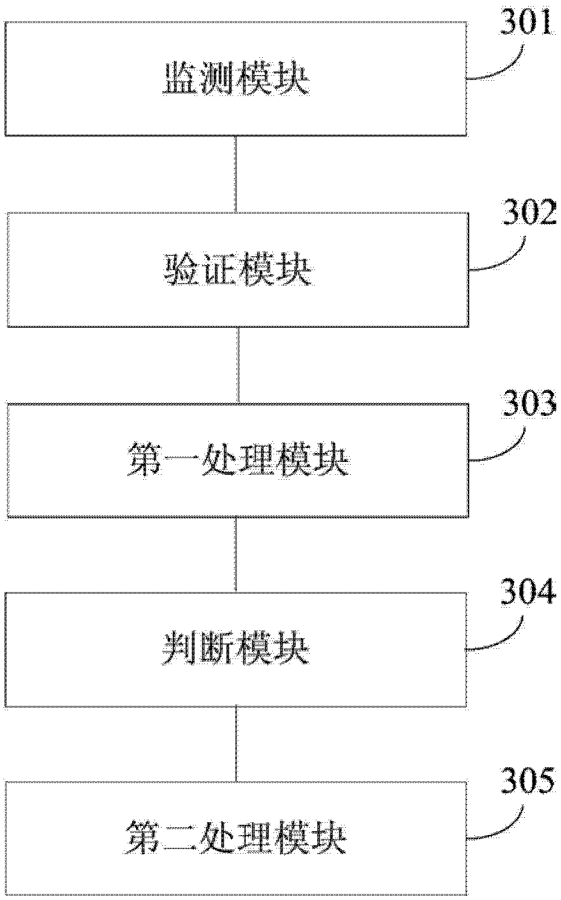

301
监测模块
302
验证模块
303
第一处理模块
304
判断模块
305
第二处理模块

图 4

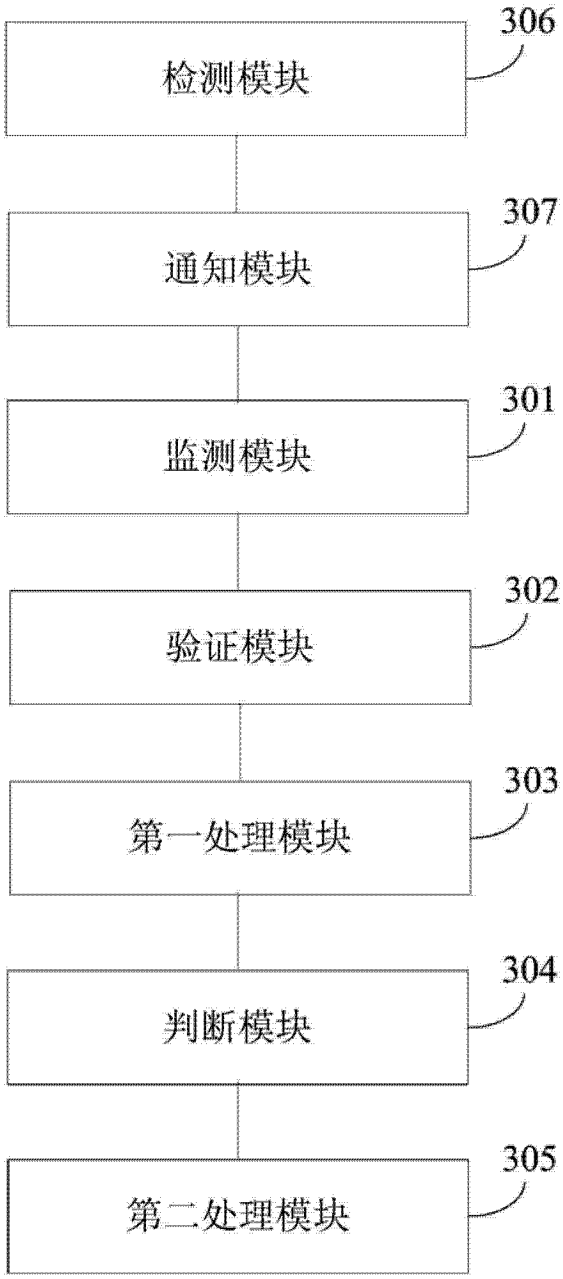

306
检测模块
307
通知模块
301
监测模块
302
验证模块
303
第一处理模块
304
判断模块
305
第二处理模块

图 5