(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 103279706 A
(43)申请公布日 2013.09.04

(21)申请号 201310226610.9

(22)申请日 2013.06.07

(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)
申请人 奇智软件(北京)有限公司

(72)发明人 熊昱之 潘剑锋 张聪

(74)专利代理机构 北京市隆安律师事务所 11323
代理人 权鲜枝 齐辉

(51)Int.Cl.
G06F 21/52(2013.01)

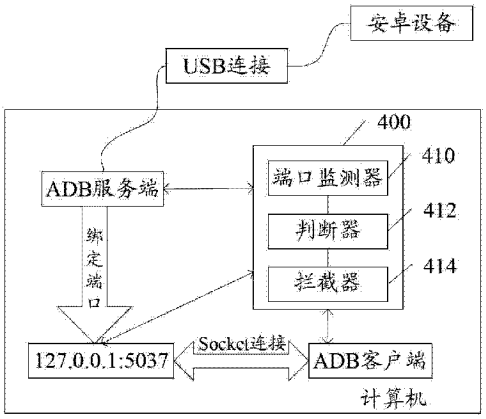
权利要求书2页 说明书14页 附图3页

(54)发明名称

拦截在移动终端中安装安卓应用程序的方法和装置

(57)摘要

本发明公开了一种拦截在移动终端中安装安卓应用程序的方法和装置。本发明实施例提供的一种拦截在移动终端中安装安卓应用程序的方法,包括:在网络驱动层对计算机中与ADB工具相绑定的预定端口进行监测;当监测到计算机中的进程通过ADB工具与移动终端建立连接时,判断进程是否是灰进程;若判断出该进程是灰进程,当获知该灰进程相关的应用程序要通过ADB工具向移动终端安装安卓应用程序时,判断是否允许该灰进程相关的应用程序向移动终端中安装安卓应用程序;当不允许灰进程相关的应用程序向移动终端中安装安卓应用程序时,拦截灰进程相关的应用程序向移动终端中安装安卓应用程序的操作。



CN 103279706 A

1. 一种拦截在移动终端中安装安卓应用程序的方法，包括：

在网络驱动层对计算机中与安卓调试桥 ADB 工具相绑定的预定端口进行监测；

当监测到计算机中的进程通过 ADB 工具与移动终端建立连接时，判断所述进程是否是灰进程；

若判断出所述进程是灰进程，当获知所述灰进程相关的应用程序要通过 ADB 工具向移动终端安装安卓应用程序时，判断是否允许该灰进程相关的应用程序向移动终端中安装安卓应用程序；

当不允许所述灰进程相关的应用程序向移动终端中安装安卓应用程序时，拦截所述灰进程相关的应用程序向移动终端中安装安卓应用程序的操作。

2. 根据权利要求 1 所述的方法，其中，所述方法还包括：

当监测到计算机中的进程通过 ADB 工具与移动终端建立连接时，若判断所述进程的类型为位于白名单中的白进程，则允许该白进程相关的应用程序对移动终端执行的所有操作；

若判断所述进程的类型为位于黑名单中的黑进程，则立即对该黑进程相关的应用程序进行拦截，禁止所述黑进程相关的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该黑进程相关的应用程序拦截成功的信息。

3. 根据权利要求 1 或 2 所述的方法，其中，在判断所述进程是否是灰进程之前，所述方法还包括：

判断所述进程是否为支持 ADB 协议的进程，是则，继续执行判断所述进程是否是灰进程的操作，否则，允许所述进程的运行。

4. 根据权利要求 3 所述的方法，其中，所述判断所述进程是否为支持 ADB 协议的进程包括：

判断所述进程向所述预定端口发送的数据包的格式和数据内容是否满足 ADB 协议，若满足，则所述进程为支持 ADB 协议的进程，若不满足，则所述进程不是支持 ADB 协议的进程。

5. 根据权利要求 3 所述的方法，其中，所述当获知所述灰进程相关的应用程序要通过 ADB 工具向移动终端安装安卓应用程序时，判断是否允许该灰进程相关的应用程序向移动终端中安装安卓应用程序包括：

当监测到所述灰进程向所述预定端口发送安卓应用程序的安装指令时，获知所述灰进程相关的应用程序要通过 ADB 工具向移动终端安装安卓应用程序；

当监测到所述灰进程向所述预定端口发送安卓安装包 APK 文件，获取该 APK 文件并对该 APK 文件进行扫描，当扫描结果指示 APK 文件安全时，判断允许该灰进程相关的应用程序向移动终端中安装安卓应用程序，否则，判断不允许该灰进程相关的应用程序向移动终端中安装安卓应用程序。

6. 根据权利要求 5 所述的方法，其中，所述对该 APK 文件进行扫描包括：

提取所述 APK 文件的安装包名称、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，以使服务器侧利用安全识别库中的特征信息对所述 APK 文件的信息进行扫描；

接收服务器侧下发的所述 APK 文件对应的扫描结果。

7. 根据权利要求 1 所述的方法，其中，所述当获知所述灰进程相关的应用程序要通过 ADB 工具向移动终端安装安卓应用程序时，判断是否允许该灰进程相关的应用程序向移动终端中安装安卓应用程序包括：

在用户界面弹出框中展示提示信息，所述提示信息包括所述灰进程相关的应用程序的图标、名称、应用描述、是否广告程序或者恶意程序的指示信息和 / 或处理方式信息；

接收用户通过所述用户界面弹出框发送的选择指令；

当所述选择指令指示允许所述灰进程相关的应用程序时，判断允许该灰进程相关的应用程序向移动终端中安装安卓应用程序，当所述选择指令指示禁止所述灰进程相关的应用程序时，判断禁止该灰进程相关的应用程序向移动终端中安装安卓应用程序。

8. 根据权利要求 1 所述的方法，其中，所述拦截所述灰进程相关的应用程序向移动终端中安装安卓应用程序的操作包括：

中断所述灰进程与所述预定端口的连接，禁止通过所述预定端口将来自所述灰进程的 APK 文件发送至移动终端。

9. 一种拦截在移动终端中安装安卓应用程序的装置，包括：

端口监测器，适于在网络驱动层对计算机中与安卓调试桥 ADB 工具相绑定的预定端口进行监测；

判断器，适于当监测到计算机中的进程通过 ADB 工具与移动终端建立连接时，判断所述进程是否是灰进程；以及，若判断出所述进程是灰进程，当获知所述灰进程相关的应用程序要通过 ADB 工具向移动终端安装安卓应用程序时，判断是否允许该灰进程相关的应用程序向移动终端中安装安卓应用程序；

拦截器，适于当不允许所述灰进程相关的应用程序向移动终端中安装安卓应用程序时，拦截所述灰进程相关的应用程序向移动终端中安装安卓应用程序的操作。

10. 根据权利要求 9 所述的装置，其中，

所述判断器，还适于当监测到计算机中的进程通过 ADB 工具与移动终端建立连接时，判断所述进程的类型为白名单中的白进程，则所述拦截器，还适于允许该白进程相关的应用程序对移动终端执行的所有操作；以及

所述判断器，还适于当监测到计算机中的进程通过 ADB 工具与移动终端建立连接时，判断所述进程的类型为黑名单中的黑进程，则所述拦截器，还适于对该黑进程相关的应用程序进行拦截，禁止所述黑进程相关的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该黑进程相关的应用程序拦截成功的信息。

拦截在移动终端中安装安卓应用程序的方法和装置

技术领域

[0001] 本发明涉及安卓技术应用程序领域，特别涉及一种拦截在移动终端中安装安卓应用程序的方法和装置。

背景技术

[0002] Android（安卓）是一种以 Linux 为基础的开放源码操作系统，主要使用于手机等移动终端。Android 平台由操作系统、中间件、用户界面和应用程序软件组成。

[0003] 随着智能手机的普及和发展，手机恶意程序成为了病毒发展的新的渠道，各种各样的APK(Android Application Package File，安卓安装包文件）应运而生，这其中就包括了病毒 APK，例如，一些病毒 APK 通过诸如短信定制付费服务、弹出骚扰广告、付费电话、备份用户手机中的敏感数据至特定服务器等恶意行为来损害用户的权益，还有一些手机恶意程序可能会导致用户手机死机、关机、资料被删、向外发送垃圾邮件、拨打电话。。其中广告行为是安卓应用程序在移动设备中通过图片或文字将预设的广告信息在用户使用该应用程序时显示，或者联网从网上下载显示在用户的显示界面，还包括将图片或文字嵌入链接，引导用户点击进入等，还有一些隐私行为包括安卓应用程序未经用户授权读取或修改移动设备的信息的操作，例如获取手机号、或者获取手机内安装软件的内容并发送至其服务器统计用户的信息。

[0004] Android 设备连接计算机时需要驱动程序 ADB(Android Debug Bridge，安卓调试桥），通过 ADB 可以调试 Android 程序。利用 ADB 可以直接操作管理 Android 模拟器或者真实的 Android 设备（如手机终端）。

[0005] Android 系统本身不具备拦截的机制，只是在恶意程序安装之前告知系统用户此程序可能会访问某些服务，但是对于应用程序是否是恶意程序不做判断。当用户将 Android 设备通过 ADB 连接至计算机时，第三方程序可能会在未经用户允许的情况下，监控 USB 接口，一旦发现 Android 设备，通过 ADB 向 Android 设备安装广告以推广应用程序，或者向 Android 设备安装一些恶意应用程序，从而导致 Android 设备往往由于与计算机的连接，会安装进来广告推广应用程序或者其它恶意应用程序。由于安装的程序可以不显示在 Android 系统的应用程序列表中，用户对这些应用程序的安装并不知情，但打开手机访问网页或者应用程序的时候会收到很多的广告推广等骚扰信息，给用户的使用带来了困扰和不便，并给用户的信息安全造成了隐患。

发明内容

[0006] 鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决上述问题的一种拦截在移动终端中安装安卓应用程序的方法和装置。

[0007] 依据本发明的一个方面，本发明实施例提供了一种拦截在移动终端中安装安卓应用程序的方法，包括：

[0008] 在网络驱动层对计算机中与安卓调试桥 ADB 工具相绑定的预定端口进行监测；

[0009] 当监测到计算机中的进程通过 ADB 工具与移动终端建立连接时，判断进程是否是灰进程；

[0010] 若判断出上述进程是灰进程，当获知灰进程相关的应用程序要通过 ADB 工具向移动终端安装安卓应用程序时，判断是否允许该灰进程相关的应用程序向移动终端中安装安卓应用程序；

[0011] 当不允许灰进程相关的应用程序向移动终端中安装安卓应用程序时，拦截灰进程相关的应用程序向移动终端中安装安卓应用程序的操作。

[0012] 其中，上述方法还包括：当监测到计算机中的进程通过 ADB 工具与移动终端建立连接时，若判断进程的类型为位于白名单中的白进程，则允许该白进程相关的应用程序对移动终端执行的所有操作；

[0013] 若判断进程的类型为位于黑名单中的黑进程，则立即对该黑进程相关的应用程序进行拦截，禁止黑进程相关的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该黑进程相关的应用程序拦截成功的信息。

[0014] 其中，在判断进程是否为灰进程之前，上述方法还包括：判断进程是否为支持 ADB 协议的进程，是则，继续执行判断进程是否为灰进程的操作，否则，允许进程的运行。

[0015] 其中，上述判断进程是否为支持 ADB 协议的进程包括判断进程向预定端口发送的数据包的格式和数据内容是否满足 ADB 协议，若满足，则进程为支持 ADB 协议的进程，若不满足，则进程不是支持 ADB 协议的进程。

[0016] 其中，上述当获知灰进程相关的应用程序要通过 ADB 工具向移动终端安装安卓应用程序时，判断是否允许该灰进程相关的应用程序向移动终端中安装安卓应用程序包括：当监测到灰进程向预定端口发送安卓应用程序的安装指令时，获知灰进程相关的应用程序要通过 ADB 工具向移动终端安装安卓应用程序；当监测到灰进程向预定端口发送安卓安装包 APK 文件，获取该 APK 文件并对该 APK 文件进行扫描，当扫描结果指示 APK 文件安全时，判断允许该灰进程相关的应用程序向移动终端中安装安卓应用程序，否则，判断不允许该灰进程相关的应用程序向移动终端中安装安卓应用程序。

[0017] 其中，上述对该 APK 文件进行扫描包括：提取述 APK 文件的安装包名称、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，以使服务器侧利用安全识别库中的特征信息对 APK 文件的信息进行扫描；接收服务器侧下发的 APK 文件对应的扫描结果。

[0018] 其中，上述当获知灰进程相关的应用程序要通过 ADB 工具向移动终端安装安卓应用程序时，判断是否允许该灰进程相关的应用程序向移动终端中安装安卓应用程序包括：在用户界面弹出框中展示提示信息，该提示信息包括灰进程相关的应用程序的图标、名称、应用描述、是否广告程序或者恶意程序的指示信息和 / 或处理方式信息；接收用户通过用户界面弹出框发送的选择指令；当选择指令指示允许灰进程相关的应用程序时，判断允许该灰进程相关的应用程序向移动终端中安装安卓应用程序，当选择指令指示禁止灰进程相关的应用程序时，判断禁止该灰进程相关的应用程序向移动终端中安装安卓应用程序。

[0019] 其中，上述拦截灰进程相关的应用程序向移动终端中安装安卓应用程序的操作包括：中断灰进程与预定端口的连接，禁止通过预定端口将来自灰进程的 APK 文件发送至移

动终端。

[0020] 根据本发明的另一方面，本发明实施例提供了一种拦截在移动终端中安装安卓应用程序的装置，包括：

[0021] 端口监测器，适于在网络驱动层对计算机中与安卓调试桥 ADB 工具相绑定的预定端口进行监测；

[0022] 判断器，适于当监测到计算机中的进程通过 ADB 工具与移动终端建立连接时，判断进程是否是灰进程；以及，若判断出进程是灰进程，当获知灰进程相关的应用程序要通过 ADB 工具向移动终端安装安卓应用程序时，判断是否允许该灰进程相关的应用程序向移动终端中安装安卓应用程序；

[0023] 拦截器，适于当不允许灰进程相关的应用程序向移动终端中安装安卓应用程序时，拦截灰进程相关的应用程序向移动终端中安装安卓应用程序的操作。

[0024] 其中，判断器，还适于当监测到计算机中的进程通过 ADB 工具与移动终端建立连接时，判断进程的类型为位于白名单中的白进程，则拦截器，还适于允许该白进程相关的应用程序对移动终端执行的所有操作；以及

[0025] 判断器，还适于当监测到计算机中的进程通过 ADB 工具与移动终端建立连接时，判断进程的类型为黑名单中的黑进程，则拦截器，还适于对该黑进程相关的应用程序进行拦截，禁止黑进程相关的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该黑进程相关的应用程序拦截成功的信息。

[0026] 其中，判断器，还适于在判断进程是否是灰进程之前，判断进程是否为支持 ADB 协议的进程，是则，继续执行判断进程是否是灰进程的操作，否则，允许进程的运行。

[0027] 其中，判断器，适于判断进程向预定端口发送的数据包的格式和数据内容是否满足 ADB 协议，若满足，则进程为支持 ADB 协议的进程，若不满足，则进程不是支持 ADB 协议的进程。

[0028] 其中，判断器，适于当监测到灰进程向预定端口发送安卓应用程序的安装指令时，获知灰进程相关的应用程序要通过 ADB 工具向移动终端安装安卓应用程序；当监测到灰进程向预定端口发送安卓安装包 APK 文件，获取该 APK 文件并对该 APK 文件进行扫描，当扫描结果指示 APK 文件安全时，判断允许该灰进程相关的应用程序向移动终端中安装安卓应用程序，否则，判断不允许该灰进程相关的应用程序向移动终端中安装安卓应用程序。

[0029] 其中，判断器适于通过如下方式获取扫描结果：提取 APK 文件的安装包名称、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 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，以使服务器侧利用安全识别库中的特征信息对 APK 文件的信息进行扫描；接收服务器侧下发的 APK 文件对应的扫描结果。

[0030] 其中，判断器适于在用户界面弹出框中展示提示信息，该提示信息包括灰进程相关的应用程序的图标、名称、应用描述、是否广告程序或者恶意程序的指示信息和 / 或处理方式信息；接收用户通过用户界面弹出框发送的选择指令；当选择指令指示允许灰进程相关的应用程序时，判断允许该灰进程相关的应用程序向移动终端中安装安卓应用程序，当选择指令指示禁止灰进程相关的应用程序时，判断禁止该灰进程相关的应用程序向移动终端中安装安卓应用程序。

[0031] 其中，拦截器，适于中断灰进程与预定端口的连接，禁止通过预定端口将来自灰进程的 APK 文件发送至移动终端。

[0032] 由上所述，本发明实施例通过对与 ADB 工具相绑定的预定端口的监测，获知到与 ADB 工具建立连接的所有进程，筛选出其中的灰进程并对灰进程相关的应用程序向移动终端中安装安卓应用程序的权限进行判断的技术手段，解决了现有技术中第三方程序随意向移动终端中安装应用程序造成的问题，能够对利用 ADB 工具与安卓交互的第三方程序进行有效监控，并通过进程类型和判断逻辑控制第三方程序的权限，从而保障了移动终端中信息的安全性，方便了用户使用。

[0033] 上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

[0034] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0035] 图 1 示出了根据本发明一个实施例的一种拦截在移动终端中安装安卓应用程序的方法流程图；

[0036] 图 2 示出了根据本发明另一个实施例的一种拦截在移动终端中安装安卓应用程序的方法流程图；以及

[0037] 图 3 示出了根据本发明另一个实施例的进程利用 ADB 工具向移动终端中安装安卓应用程序时的交互流程示意图；

[0038] 图 4 示出了根据本发明又一个实施例一种拦截在移动终端中安装安卓应用程序的装置的结构示意图。

具体实施方式

[0039] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0040] 本发明一个实施例提供了一种拦截在移动终端中安装安卓应用程序的方法，参见图 1，该方法包括：

[0041] S100：在网络驱动层对计算机中与 ADB(Android Debug Bridge，安卓调试桥）工具相绑定的预定端口进行监测。

[0042] 本实施例在网络驱动层中执行对在移动终端中安装安卓应用程序的操作的拦截，该网络驱动层处于上层驱动，是作为 winsock(WindowsSockets) 调用转发到内核协议驱动的一个辅助中间层。处于这层的驱动可以无差别的监控到所有本地及远程的 winsock 调用以及监控到网络底层协议驱动。

[0043] 上述计算机中的预定端口可以为 127.0.0.1：5037 端口 (5037 端口)，其中，ADB 工

具与该 5037 端口相绑定。

[0044] S102 :当监测到计算机中的进程通过 ADB 工具与移动终端建立连接时,判断进程是否是灰进程。

[0045] 本实施例中以移动终端为安卓设备(如安卓手机或其它支持安卓系统的终端)为例进行说明。

[0046] 灰进程为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,确认是否允许该灰进程相关的应用程序向安卓设备中安装安卓应用程序。

[0047] 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,一旦监测出黑进程,立即执行拦截。

[0048] 需要说明的是,本实施例在进程的层次上,对拦截在移动终端(安卓设备)中安装安卓应用程序的方案进行描述。应用程序是静态的,进程是动态的,进程是一个正在执行的程序,即计算机中正在运行的程序实例 ;其可以分配给处理器并作为一个实体由处理器执行。进程能够得到应用程序的处理结果。一个应用程序在一个数据集上的一次运行为一个进程,进程和应用程序并非一一对应的,一个应用程序运行在多个不同的数据集上形成多个不同的进程。进程在创建时产生,因应用程序的调度而运行,在完成任务后进程会被撤消。进程能够反映一个应用程序在一定的数据集上运行的全部动态过程。上述进程相关的应用程序是指进程上正在运行的应用程序。

[0049] S104 :当获知灰进程相关的应用程序要通过 ADB 工具向移动终端安装安卓应用程序时,判断是否允许该灰进程相关的应用程序向移动终端中安装安卓应用程序。

[0050] 进程相关的应用程序利用 ADB 工具可以执行多种类型的操作,例如,枚举当前系统连接的安卓设备、与安卓设备建立连接、读写安卓设备中的文件及目录、给安卓设备安装 APK 文件、执行安卓设备上的 shell 指令等等。在此,本方案主要关注基于 ADB 协议安装 APK 文件的功能,则在本步骤中,当获知灰进程相关的应用程序要通过 ADB 工具向安卓设备安装安卓应用程序时启动拦截操作的逻辑判断。

[0051] S106 :当不允许灰进程相关的应用程序向移动终端中安装安卓应用程序时,拦截灰进程相关的应用程序向移动终端中安装安卓应用程序的操作。

[0052] 由上所述,本发明实施例在 PC 端设备例如电脑与安卓设备连接传输时,保护安卓设备不被强制安装广告软件或恶意软件。本方案不仅能够拦截到恶意骚扰程序,也可以拦截到任何通过 ADB 工具获得在手机上安装应用程序的权限的恶意程序。

[0053] 现有的安卓系统中无法对利用 ADB 工具在手机上安装安卓应用程序的第三方应用进行检查,而 ADB 工具又可以获得安卓应用程序的所有权限,包括执行 shell 指令等等,从而导致手机与计算机连接后,病毒易于传播至手机,为解决这一问题,本实施例通过对与 ADB 工具相绑定的预定端口的监测,获知到与 ADB 工具建立连接的所有进程,筛选出其中的灰进程并对灰进程相关的应用程序向安卓设备中安装安卓应用程序的权限进行判断的技术手段,解决了现有技术中第三方程序随意向安卓设备中安装应用程序造成的问题,能够对利用 ADB 工具与安卓交互的第三方程序进行有效监控,并通过进程类型和判断逻辑控制

第三方程序的权限，从而保障了移动终端中信息的安全性，方便了用户使用。

[0054] 在图 1 所示实施例的基础上，本发明另一个实施例提供的一种拦截在移动终端中安装安卓应用程序的方法，参见图 2，包括如下步骤：

[0055] S200：对与 ADB 工具绑定的 5037 端口进行监测。

[0056] 本步骤中，在后台程序中监测 5037 端口中通过的数据包，这些数据包可以为发送指令的数据包，也可以为发送实体数据的数据包。

[0057] 上述监测可以由 ADB 工具或者设置在 ADB 工具中的器件实现。

[0058] ADB 工具的功能主要包括：运行安卓设备的命令，管理安卓模拟器或安卓设备的端口映射，控制计算机或者安卓设备之间的上传或者下载文件，以及将本地的 APK 文件安装至安卓模拟器或者安卓设备。ADB 工具在计算机和安卓设备之间起到了一个中转的作用。

[0059] ADB 工具是基于客户端 - 服务端模型实现的，包括三个部分：ADB 客户端、ADB 服务端和守护进程。

[0060] ADB 客户端，运行在开发用的电脑上，可以在命令行中运行 ADB 命令来调用该客户端，像 ADB 插件和 DDMS 这样的安卓工具也可以调用 ADB 客户端。

[0061] ADB 服务端，是运行在开发用电脑上的后台进程，管理设备并负责计算机与设备之间的数据交换；

[0062] ADB 客户端和 ADB 服务端在可以存在于同一个可执行文件之中，例如 Windows 系统中名为 adb.exe 的可执行文件中。ADB 客户端负责与用户交互，执行完命令后就退出；而 ADB 服务端在启动后一直运行于计算机中。

[0063] 守护进程，运行在安卓系统中的进程，接收 ADB 服务端发来的数据并执行指令。

[0064] 当启动 ADB 客户端时，客户端首先检测 ADB 服务端进程是否运行，如果没有运行，则启动 ADB 服务端。当 ADB 服务端启动时，它会绑定到本地的 TCP5037 端口，并且监听从 ADB 客户端发来的命令。所有的 ADB 客户端都使用 5037 端口与 ADB 服务端通信。

[0065] S202：当监测到计算机中的进程通过 ADB 工具与安卓设备建立连接。

[0066] ADB 工具可以通过预定端口操作安卓手机、向安卓手机中安装应用程序、执行手机同步和上传文件等功能，第三方程序可以通过捆绑一个 ADB 工具和向安卓设备发送命令进行通信。

[0067] ADB 工具包括 ADB 客户端和 ADB 服务端。ADB 服务端一直在后台运行，负责和安卓设备通讯，可以通过网络将 APK 文件传递到 ADB 服务端，从而通过中转安装到移动终端上去；ADB 客户端负责第三方程序与预定端口的连接，而本地网络层中设置有 ADB 通讯协议，以支持 ADB 工具的通信。例如，手机助手就相当于一个 ADB 服务端，当其他的应用程序与手机助手连接上后，其他的应用程序也可会利用手机助手的服务向安卓设备安装应用程序等。

[0068] 第三方程序会通过 ADB 客户端与 5037 端口建立 Socket（套接字）连接，然后通过该 Socket 连接和 ADB 服务端连接至安卓设备。如在将应用程序安装到手机上时，ADB 客户端将应用程序的安装包传递给 ADB 服务端，ADB 服务端就安装该应用程序到手机上。

[0069] S204：判断进程是否为支持 ADB 协议的进程，是则执行步骤 S206。

[0070] 通过 5037 端口传输的数据包除了与安卓设备通讯的数据包之外，还会包括其他类型的数据包，为了避免拦截到其他正常的程序，保证其他程序的正常运行，本实施例中，

判断监测到的进程的是否使用ADB协议，当使用ADB协议时，说明该进程为会与安卓设备通信的进程，继续对该进程进行监控，当不使用ADB协议时，说明该进程为不与安卓设备通信的其他进程，不再对该进程进行监控，允许该进程的运行。

[0071] ADB协议支持的操作包括使用ADB枚举当前系统连接的安卓设备、与安卓设备建立连接、读写安卓设备中的文件及目录、给安卓设备安装APK文件、执行安卓设备上的shell指令等等。

[0072] 在判断进程是否为支持ADB协议的进程时，可以判断该进程向预定端口（5037端口）发送的数据包的格式和数据内容是否满足ADB协议，若满足，则该进程为支持ADB协议的进程，若不满足，则该进程不是支持ADB协议的进程。例如，当判断数据包的格式满足ADB协议的格式要求，且数据内容中指示了本数据包为基于ADB协议的数据包时，确认进程为支持ADB协议的进程。

[0073] S206：判断进程的类型。

[0074] 本实施例会预先对进程的信息进行收集和统计，维护和保存进程的白名单和黑名单。

[0075] 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。位于白名单中进程的类型为白进程，位于黑名单中进程的类型为黑进程，在白名单和黑名单之外的所有未知进程属于灰进程。另外，本实施例还可以通过客户端收集程序行为并关联到程序特征，从而在数据库中记录程序特征及其对应的程序行为，根据收集到的程序行为和程序特征的关联关系，可以在数据库中对样本进行分析归纳，从而有助于对软件或程序属于黑名单或者白名单的判断。由于在数据库中记录了程序特征及该特征对应的行为记录，因此可以结合已知白名单对未知程序进行分析。例如，如果未知程序特征与现有白名单中的已知程序特征相同，则将该未知程序特征及其程序行为都列入白名单。如果未知程序行为与现有白名单中的已知程序行为相同或近似，则将该未知程序行为及其程序特征都列入白名单。

[0076] 当进程为白进程（如360手机助手、91手机助手或豌豆荚调用的进程等）时，确认该进程相关的应用程序为可信的应用程序，允许该进程的运行。

[0077] 当进程为黑进程时（如恶意推广APK的应用程序调用的进程等），确认该进程相关的应用程序为不可信的应用程序，在判断出该进程的类型后，立即拦截该进程的运行（如通过断开该进程与5037端口的连接来拦截该进程），禁止该进程相关的应用程序对安卓设备进行任何操作（如枚举系统中连接的安卓设备），并将拦截成功的信息发送至用户，如在用户界面弹出框中展示对该黑进程相关的应用程序拦截成功的信息。

[0078] 当进程为灰进程时，进入步骤S208，继续对该灰进程进行监控。

[0079] S208：判断是否允许该灰进程相关的应用程序向安卓设备中安装安卓应用程序。

[0080] 本方案主要关注第三方程序利用ADB协议在安卓设备上安装应用程序的场景，当灰进程执行其他操作时，如枚举操作、读写安卓设备目录的操作，可以允许这些操作的执行。

[0081] 为了更清楚地说明本方案，下面首先结合图3对进程相关的应用程序利用ADB工具向安卓设备中安装安卓应用程序的场景的进行说明，图3示出了进程利用ADB工具向安卓设备中安装安卓应用程序时的交互流程示意图。其中，进程通过ADB客户端与5037端口建立Socket连接，通过该Socket连接将各种指令和数据发送至5037端口，然后再由ADB

服务端将指令和数据发送至安卓设备，在执行 APK 文件安装时，主要包括如下操作：

[0082] 1)、进程通过 ADB 客户端和 ADB 服务端向安卓设备发送 install（安装）指令。

[0083] 上述 install 指令指示进程即将要执行向安卓设备安装安卓应用程序的操作。

[0084] 2)、进程通过 ADB 客户端和 ADB 服务端向安卓设备发送 Sync(synchronous，同步）指令，指示进入同步状态。

[0085] 3)、进程通过 ADB 客户端和 ADB 服务端向安卓设备发送 SEND（发送）指令，指定 APK 文件的存放路径。

[0086] 4)、进程通过 ADB 客户端和 ADB 服务端向安卓设备发送 DATA（数据）指令，从而将需要安装的 APK 文件发送给安卓设备。

[0087] 5)、进程通过 ADB 客户端和 ADB 服务端向安卓设备发送 pm shell 指令，启动 APK 文件在安卓设备上的安装。

[0088] 在 APK 文件安装后，还可以包括下述步骤 6)。

[0089] 6)、进程通过 ADB 客户端和 ADB 服务端向安卓设备发送 rm shell 指令，删除在安装过程中上传的 APK 文件等数据。

[0090] 本步骤在获知灰进程相关的应用程序要通过 ADB 工具向安卓设备安装安卓应用程序时触发开始执行。当监测到灰进程调用 ADB 工具的 install 功能向预定端口发送安卓应用程序的 install 指令时，获知灰进程相关的应用程序要通过 ADB 工具向安卓设备安装安卓应用程序；在发送完 install 指令后，灰进程还会通过 ADB 工具向预定端口发送 Sync(synchronous，同步）指令、SEND（发送）指令等，然后灰进程向预定端口发送携带有 APK 文件的 DATA（数据）指令，则当监测到灰进程向预定端口发送安卓安装包 APK 文件，获取该 APK 文件并对该 APK 文件进行扫描，扫描该要安装的 APK 文件中是否含有恶意扣费、恶意骚扰、窃取隐私的代码等恶意内容，当没有恶意内容时扫描结果为 APK 文件安全，否则扫描结果为 APK 文件危险。

[0091] 当扫描结果指示 APK 文件安全时，判断允许该灰进程相关的应用程序向安卓设备中安装安卓应用程序，否则，判断不允许该灰进程相关的应用程序向安卓设备中安装安卓应用程序。

[0092] 在执行对 APK 文件的扫描时，具体执行如下操作：

[0093] 提取 APK 文件的各种信息，这些信息包括但不局限于安装包名称、版本号、数字签名、安卓组件接收器 (receiver) 的特征、安卓组件服务 (service) 的特征、安卓组件活动 (activity) 的特征、可执行文件中的指令（或字符串）和 / 或 APK 目录下各文件的 MD5 值；然后，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 APK 文件的信息进行扫描；接收服务器侧下发的 APK 文件对应的扫描结果，从而获知扫描结果，程序包名称、证书等信息。

[0094] 优选的，上述安全识别库可以为云查杀引擎。

[0095] 其中，上述可执行文件包括 Dex 文件和 / 或 ELF 文件，该 Dex 文件包括 classes.dex 文件、扩展名为 .jar 的文件以及 Dex 格式的文件等。

[0096] 需要说明的是，本实施例在采用上述方式进行扫描之前，需要预先对 APK 文件的信息进行收集，例如，选取样本安卓安装包，该样本安卓安装包包括各种安全级别下的安卓安装包。对各种样本安卓安装包的包名、版本号、数字签名、安卓组件 receiver 的特征、安

卓组件 service 的特征、安卓组件 activity 的特征、可执行文件中的指令或字符串，安卓安装包目录下各文件的 MD5 值进行收集，将收集到的信息预置在服务器侧的安全识别库中。

[0097] 服务器侧预置的安全识别库中既收集了识别病毒、木马等各种恶意软件的 APK 文件的特征信息，也收集了识别正常应用的 APK 文件的特征信息。当 APK 文件的信息中有一项信息命中恶意软件的特征信息，则得到的该 APK 文件对应的扫描结果指示该 APK 文件不是安全的。

[0098] 进一步的，本实施例中还允许用户对安卓应用程序的安装进行选择，即在通过上述判断逻辑对是否允许进程相关的应用程序向安卓设备中安装安卓应用程序进行判断之后，结合用户的选择做出最终的判决结果。当根据上述判断逻辑确认允许灰进程相关的应用程序向安卓设备中安装安卓应用程序时（或者其他允许在安卓设备中安装应用程序的场景，如白进程），本方法还包括：

[0099] 在用户界面弹出框中展示提示信息，该提示信息包括灰进程相关的应用程序的图标、名称、应用描述、是否广告程序或者恶意程序的指示信息和 / 或处理方式信息，该处理方式信息可以包括所推荐的对应用程序的处理建议等。然后，接收用户通过用户界面弹出框发送的选择指令；当选择指令指示允许灰进程相关的应用程序时，最终判断允许该灰进程相关的应用程序向安卓设备中安装安卓应用程序，并执行该安卓应用程序的安装操作，当选择指令指示禁止灰进程相关的应用程序时，判断禁止该灰进程相关的应用程序向安卓设备中安装安卓应用程序，不再执行该安卓应用程序的安装过程。

[0100] S210：拦截灰进程相关的应用程序向安卓设备中安装安卓应用程序的操作。

[0101] 本方案的拦截机制中，中断灰进程与 5037 端口的连接，如控制 ADB 客户端终端与灰进程断开连接，以及，禁止通过 5037 端口将来自灰进程的 APK 文件发送至安卓设备，例如，控制 ADB 服务端，禁止将该灰进程的 APK 文件发送至安卓设备。

[0102] 本发明又一个实施例提供了一种拦截在移动终端中安装安卓应用程序的装置 400，参见图 4，包括端口监测器 410、判断器 412 和拦截器 414。

[0103] 端口监测器 410，适于在网络驱动层对计算机中与安卓调试桥 ADB 工具相绑定的预定端口进行监测。该预定端口为 127.0.0.1 :5037 端口 (5037 端口）。参见图 4，ADB 工具包括 ADB 客户端和 ADB 服务端。第三方应用程序的进程通过 ADB 客户端与 5037 端口建立 Socket 连接，5037 端口与 ADB 服务端相绑定，ADB 服务端通过 USB 与安卓设备相连接。装置 400 能够对计算机中的 ADB 工具和 5037 端口进行控制。

[0104] 本实施例中以移动终端为安卓设备（如安卓手机或其它支持安卓系统的终端）为例进行说明。

[0105] 判断器 412 适于当监测到计算机中的进程通过 ADB 工具与移动终端（安卓设备）建立连接时，判断进程是否是灰进程；以及，若判断出进程是灰进程，当获知灰进程相关的应用程序要通过 ADB 工具向安卓设备安装安卓应用程序时，判断是否允许该灰进程相关的应用程序向安卓设备中安装安卓应用程序。具体的，判断器 412 当监测到灰进程向预定端口发送安卓应用程序的安装指令时，获知灰进程相关的应用程序要通过 ADB 工具向安卓设备安装安卓应用程序；当监测到灰进程向预定端口发送安卓安装包 APK 文件，获取该 APK 文件并对该 APK 文件进行扫描，当扫描结果指示 APK 文件安全时，判断允许该灰进程相关的应用程序向安卓设备中安装安卓应用程序，否则，判断不允许该灰进程相关的应用程序向安

卓设备中安装安卓应用程序。

[0106] 判断器 412 在执行对 APK 文件的扫描时，具体执行如下操作：提取 APK 文件的各种信息，这些信息包括但不局限于安装包名称、版本号、数字签名、安卓组件接收器(receiver)的特征、安卓组件服务(service)的特征、安卓组件活动(activity)的特征、可执行文件中的指令（或字符串）和 / 或 APK 目录下各文件的 MD5 值（也可以是 SHA1 值）；然后，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 APK 文件的信息进行扫描；接收服务器侧下发的 APK 文件对应的扫描结果，从而获知扫描结果。其中，在服务器侧，将判断器上报的 APK 文件的信息与安全识别库中的恶意软件的特征信息进行比对，只要有一项信息命中，则该 APK 文件就不是安全的文件。优选的，上述安全识别库可以为云查杀引擎。

[0107] 灰进程为预设的白名单和黑名单之外的所有进程，本实施例还利用预设的白名单和黑名单对白进程和黑进程进行识别，具体的，判断器 412 还适于当监测到计算机中的进程通过 ADB 工具与安卓设备建立连接时，判断进程的类型为位于白名单中的白进程，则拦截器 414 还适于允许该白进程相关的应用程序对安卓设备执行的所有操作。

[0108] 以及，判断器 412 还适于当监测到计算机中的进程通过 ADB 工具与安卓设备建立连接时，判断进程的类型为位于黑名单中的黑进程，则拦截器 414 还适于立即对该黑进程相关的应用程序进行拦截，禁止黑进程相关的应用程序对安卓设备执行任何操作。

[0109] 进一步的，由于通过 5037 端口传输的数据包除了与安卓设备通讯的数据包之外，还会包括其他类型的数据包，为了避免拦截到其他正常的程序，保证其他程序的正常运行，本实施例中，判断器 412 还适于在判断进程是否是灰进程之前，判断进程是否为支持 ADB 协议的进程，是则，继续执行判断进程是否是灰进程的操作，否则，允许进程的运行。具体的，判断器 412 判断进程向预定端口发送的数据包的格式和数据内容是否满足 ADB 协议，若满足，则进程为支持 ADB 协议的进程，若不满足，则进程不是支持 ADB 协议的进程。

[0110] 进一步的，本实施例在通过判断器 412 按照上述判断逻辑对是否允许进程向安卓设备中安装安卓应用程序进行判断之后，还结合用户的选择做出最终的判决结果。例如，判断器 412 在用户界面弹出框中展示提示信息，该提示信息包括灰进程相关的应用程序的图标、名称、应用描述、是否广告程序或者恶意程序的指示信息和 / 或处理方式信息；接收用户通过用户界面弹出框发送的选择指令；当选择指令指示允许灰进程相关的应用程序时，判断允许该灰进程相关的应用程序向安卓设备中安装安卓应用程序，当选择指令指示禁止灰进程相关的应用程序时，判断禁止该灰进程相关的应用程序向安卓设备中安装安卓应用程序。

[0111] 对于灰进程的拦截，拦截器 414 当不允许灰进程相关的应用程序向安卓设备中安装安卓应用程序时，拦截灰进程相关的应用程序向安卓设备中安装安卓应用程序的操作。例如，拦截器 414 中断灰进程与预定端口的连接，禁止通过预定端口将来自灰进程的 APK 文件发送至安卓设备。对于白进程和黑进程的拦截，参见上文的相关内容的描述。

[0112] 本发明装置实施例中各器件的具体工作方式可以参见本发明的方法实施例，在此不再赘述。

[0113] 由上所述，本发明实施例通过对与 ADB 工具相绑定的预定端口的监测，获知到与 ADB 工具建立连接的所有进程，筛选出其中的灰进程并对灰进程相关的应用程序向移动终

端中安装安卓应用程序的权限进行判断的技术手段，解决了现有技术中第三方程序随意向移动终端中安装应用程序造成的问题，能够对利用 ADB 工具与安卓交互的第三方程序进行有效监控，并通过进程类型和判断逻辑控制第三方程序的权限，从而保障了移动终端中信息的安全性，方便了用户使用。

[0114] 在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

[0115] 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

[0116] 类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

[0117] 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和 / 或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0118] 此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0119] 本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器 (DSP) 来实现根据本发明实施例的拦截在移动终端中安装安卓应用程序的装置中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

[0120] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

[0121] 本发明的实施例揭示了 A1、一种拦截在移动终端中安装安卓应用程序的方法，包括：在网络驱动层对计算机中与安卓调试桥 ADB 工具相绑定的预定端口进行监测；当监测到计算机中的进程通过 ADB 工具与移动终端建立连接时，判断所述进程是否是灰进程；若判断出所述进程是灰进程，当获知所述灰进程相关的应用程序要通过 ADB 工具向移动终端安装安卓应用程序时，判断是否允许该灰进程相关的应用程序向移动终端中安装安卓应用程序；当不允许所述灰进程相关的应用程序向移动终端中安装安卓应用程序时，拦截所述灰进程相关的应用程序向移动终端中安装安卓应用程序的操作。A2、根据权利要求 A1 所述的方法，其中，所述方法还包括：当监测到计算机中的进程通过 ADB 工具与移动终端建立连接时，若判断所述进程的类型为位于白名单中的白进程，则允许该白进程相关的应用程序对移动终端执行的所有操作；若判断所述进程的类型为位于黑名单中的黑进程，则立即对该黑进程相关的应用程序进行拦截，禁止所述黑进程相关的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该黑进程相关的应用程序拦截成功的信息。A3、根据权利要求 A1 或 A2 所述的方法，其中，在判断所述进程是否是灰进程之前，所述方法还包括：判断所述进程是否为支持 ADB 协议的进程，是则，继续执行判断所述进程是否是灰进程的操作，否则，允许所述进程的运行。A4、根据权利要求 A3 所述的方法，其中，所述判断所述进程是否为支持 ADB 协议的进程包括：判断所述进程向所述预定端口发送的数据包的格式和数据内容是否满足 ADB 协议，若满足，则所述进程为支持 ADB 协议的进程，若不满足，则所述进程不是支持 ADB 协议的进程。A5、根据权利要求 A3 所述的方法，其中，所述当获知所述灰进程相关的应用程序要通过 ADB 工具向移动终端安装安卓应用程序时，判断是否允许该灰进程相关的应用程序向移动终端中安装安卓应用程序包括：当监测到所述灰进程向所述预定端口发送安卓应用程序的安装指令时，获知所述灰进程相关的应用程序要通过 ADB 工具向移动终端安装安卓应用程序；当监测到所述灰进程向所述预定端口发送安卓安装包 APK 文件，获取该 APK 文件并对该 APK 文件进行扫描，当扫描结果指示 APK 文件安全时，判断允许该灰进程相关的应用程序向移动终端中安装安卓应用程序，否则，判断不允许该灰进程相关的应用程序向移动终端中安装安卓应用程序。A6、根据权利要求 A5 所述的方法，其中，所述对该 APK 文件进行扫描包括：提取所述 APK 文件的安装包名称、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，以使服务器侧利用安全识别库中的特征信息对所述 APK 文件的信息进行扫描；接收服务器侧下发的所述 APK 文件对应的扫描结果。A7、根据权利要求 A1 所述的方法，其中，所述当获知所述灰进程相关的应用程序要通过 ADB 工具向移动终端安装安卓应用程

序时，判断是否允许该灰进程相关的应用程序向移动终端中安装安卓应用程序包括：在用户界面弹出框中展示提示信息，所述提示信息包括所述灰进程相关的应用程序的图标、名称、应用描述、是否广告程序或者恶意程序的指示信息和/或处理方式信息；接收用户通过所述用户界面弹出框发送的选择指令；当所述选择指令指示允许所述灰进程相关的应用程序时，判断允许该灰进程相关的应用程序向移动终端中安装安卓应用程序，当所述选择指令指示禁止所述灰进程相关的应用程序时，判断禁止该灰进程相关的应用程序向移动终端中安装安卓应用程序。A8、根据权利要求A1所述的方法，其中，所述拦截所述灰进程相关的应用程序向移动终端中安装安卓应用程序的操作包括：中断所述灰进程与所述预定端口的连接，禁止通过所述预定端口将来自所述灰进程的APK文件发送至移动终端。A9、一种拦截在移动终端中安装安卓应用程序的装置，包括：端口监测器，适于在网络驱动层对计算机中与安卓调试桥ADB工具相绑定的预定端口进行监测；判断器，适于当监测到计算机中的进程通过ADB工具与移动终端建立连接时，判断所述进程是否是灰进程；以及，若判断出所述进程是灰进程，当获知所述灰进程相关的应用程序要通过ADB工具向移动终端安装安卓应用程序时，判断是否允许该灰进程相关的应用程序向移动终端中安装安卓应用程序；拦截器，适于当不允许所述灰进程相关的应用程序向移动终端中安装安卓应用程序时，拦截所述灰进程相关的应用程序向移动终端中安装安卓应用程序的操作。A10、根据权利要求A9所述的装置，其中，所述判断器，还适于当监测到计算机中的进程通过ADB工具与移动终端建立连接时，判断所述进程的类型为白名单中的白进程，则所述拦截器，还适于允许该白进程相关的应用程序对移动终端执行的所有操作；以及所述判断器，还适于当监测到计算机中的进程通过ADB工具与移动终端建立连接时，判断所述进程的类型为黑名单中的黑进程，则所述拦截器，还适于对该黑进程相关的应用程序进行拦截，禁止所述黑进程相关的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该黑进程相关的应用程序拦截成功的信息。A11、根据权利要求A9或A10所述的装置，其中，所述判断器，还适于在判断所述进程是否是灰进程之前，判断所述进程是否为支持ADB协议的进程，是则，继续执行判断所述进程是否是灰进程的操作，否则，允许所述进程的运行。A12、根据权利要求A11所述的装置，其中，所述判断器，适于判断所述进程向所述预定端口发送的数据包的格式和数据内容是否满足ADB协议，若满足，则所述进程为支持ADB协议的进程，若不满足，则所述进程不是支持ADB协议的进程。A13、根据权利要求A11所述的装置，其中，所述判断器，适于当监测到所述灰进程向所述预定端口发送安卓应用程序的安装指令时，获知所述灰进程相关的应用程序要通过ADB工具向移动终端安装安卓应用程序；当监测到所述灰进程向所述预定端口发送安卓安装包APK文件，获取该APK文件并对该APK文件进行扫描，当扫描结果指示APK文件安全时，判断允许该灰进程相关的应用程序向移动终端中安装安卓应用程序，否则，判断不允许该灰进程相关的应用程序向移动终端中安装安卓应用程序。A14、根据权利要求A9所述的装置，其中，所述判断器，适于通过如下方式获取所述扫描结果：提取所述APK文件的安装包名称、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，以使服务器侧利用安全识别库中的特征信息对所述APK文件的信息进行扫描；接收服务器侧下发的所述APK文件对应的扫描结果。A15、根据权利要求A9所述的装置，其中，所述判断器适于在用户界面弹出框中展示提示信息，

所述提示信息包括所述灰进程相关的应用程序的图标、名称、应用描述、是否广告程序或者恶意程序的指示信息和 / 或处理方式信息；接收用户通过所述用户界面弹出框发送的选择指令；当所述选择指令指示允许所述灰进程相关的应用程序时，判断允许该灰进程相关的应用程序向移动终端中安装安卓应用程序，当所述选择指令指示禁止所述灰进程相关的应用程序时，判断禁止该灰进程相关的应用程序向移动终端中安装安卓应用程序。A16、根据权利要求 A9 所述的装置，其中，所述拦截器，适于中断所述灰进程与所述预定端口的连接，禁止通过所述预定端口将来自所述灰进程的 APK 文件发送至移动终端。

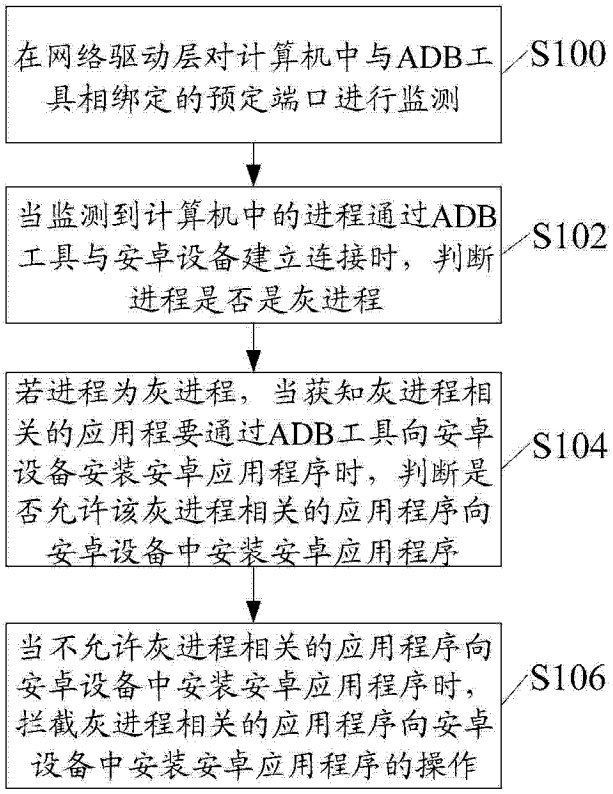

在网络驱动层对计算机中与ADB工具相绑定的预定端口进行监测
S100
当监测到计算机中的进程通过ADB工具与安卓设备建立连接时，判断进程是否是灰进程
S102
若进程为灰进程，当获知灰进程相关的应用程要通过ADB工具向安卓设备安装安卓应用程序时，判断是否允许该灰进程相关的应用程序向安卓设备中安装安卓应用程序
S104
当不允许灰进程相关的应用程序向安卓设备中安装安卓应用程序时，拦截灰进程相关的应用程序向安卓设备中安装安卓应用程序的操作
S106

图 1

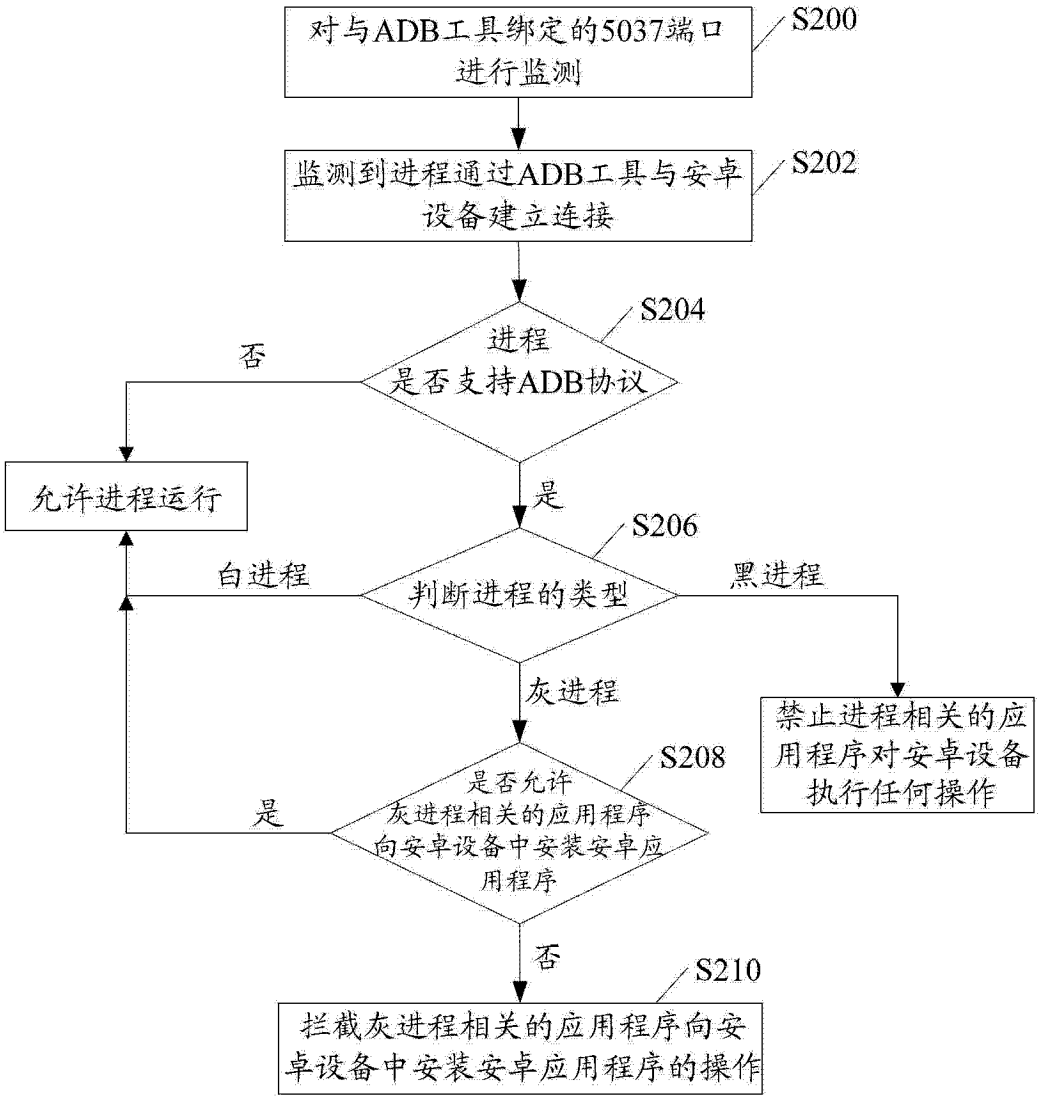

对与ADB工具绑定的5037端口进行监测
S200
监测到进程通过ADB工具与安卓设备建立连接
S202
进程是否支持ADB协议
S204
否
是
允许进程运行
判断进程的类型
S206
白进程
黑进程
灰进程
禁止进程相关的应用程序对安卓设备执行任何操作
是否允许灰进程相关的应用程序向安卓设备中安装安卓应用程序
S208
是
否
拦截灰进程相关的应用程序向安卓设备中安装安卓应用程序的操作
S210

图 2

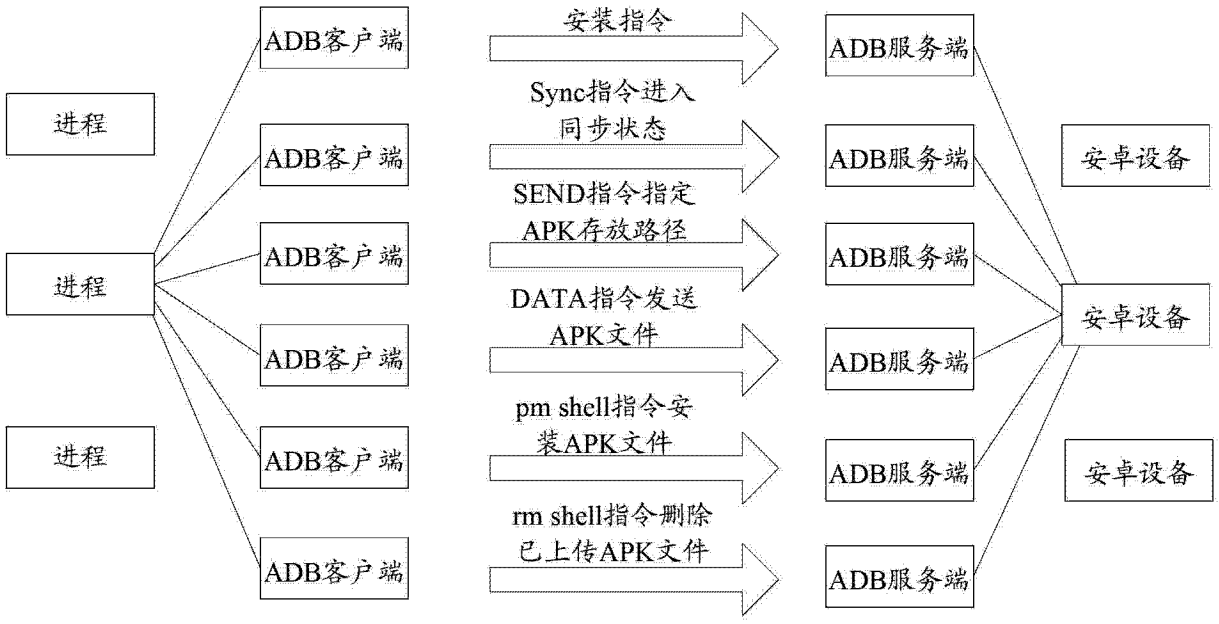

进程
进程
进程
ADB客户端
ADB客户端
ADB客户端
ADB客户端
ADB客户端
ADB客户端
安装指令
Sync指令进入同步状态
SEND指令指定APK存放路径
DATA指令发送APK文件
pm shell指令安装APK文件
rm shell指令删除已上传APK文件
ADB服务端
ADB服务端
ADB服务端
ADB服务端
ADB服务端
ADB服务端
安卓设备
安卓设备
安卓设备

图 3

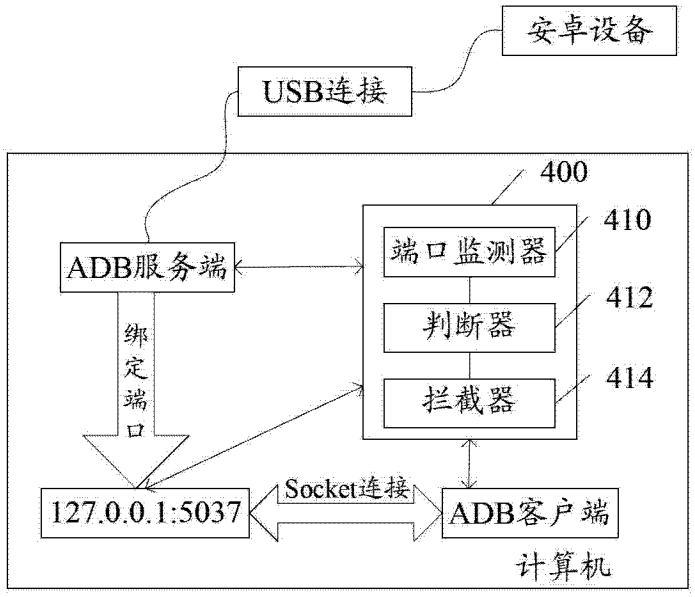

安卓设备
USB连接
400
410
412
414
ADB服务端
端口监测器
判断器
拦截器
绑定端口
127.0.0.1:5037
Socket连接
ADB客户端
计算机

图 4