(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 103632096 A
(43)申请公布日 2014.03.12

(21)申请号 201310632733.2

(22)申请日 2013.11.29

(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 张龙 孟凡磊 邱凯 田野

(74)专利代理机构 北京润泽恒知识产权代理有限公司 11319
代理人 赵娟

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

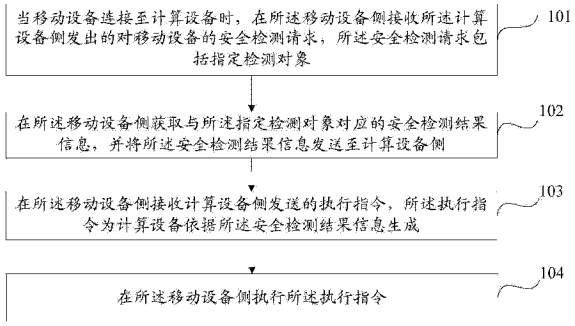
权利要求书3页 说明书30页 附图4页

(54)发明名称

一种对设备进行安全检测方法和装置

(57)摘要

本发明公开了一种对设备进行安全检测的方法和装置，其中所述方法包括：当移动设备连接至计算设备时，在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求，所述安全检测请求中包括指定检测对象；在所述移动设备侧获取与所述指定检测对象对应的安全检测结果信息，并将所述安全检测结果信息发送至计算设备侧；在所述移动设备侧接收计算设备侧发送的执行指令，所述执行指令为计算设备依据所述安全检测结果信息生成；在所述移动设备侧执行所述执行指令。本发明可以使得用户在计算设备侧即可实现对移动设备的安全检测，从而提高移动设备的安全性。



CN 103632096 A

1. 一种对设备进行安全检测的方法，包括：

当移动设备连接至计算设备时，在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求，所述安全检测请求中包括指定检测对象；

在所述移动设备侧获取与所述指定检测对象对应的安全检测结果信息，并将所述安全检测结果信息发送至计算设备侧；

在所述移动设备侧接收计算设备侧发送的执行指令，所述执行指令为计算设备依据所述安全检测结果信息生成；

在所述移动设备侧执行所述执行指令。

2. 如权利要求 1 所述的方法，其特征在于，在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求的步骤之前，还包括：

所述移动设备侧接收所述计算设备侧发送的第三方应用安装包，所述第三方应用安装包为所述计算设备侧在检测到所述移动设备侧没有安装第三方应用时，从服务器中下载得到；

所述移动设备侧依据所述第三方应用安装包安装第三方应用。

3. 如权利要求 1 或 2 所述的方法，其特征在于，在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求的步骤之前，还包括：

建立所述移动设备与所述计算设备的 SOCKET 连接通道，所述移动设备通过所述 SOCKET 连接通道接收安全检测请求、以及发送安全检测结果信息、以及接收执行指令。

4. 如权利要求 2 所述的方法，其特征在于，所述在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求的步骤为：

在所述移动设备侧采用所述第三方应用接收所述计算设备侧发出的对移动设备的安全检测请求；

所述在所述移动设备侧获取与所述指定检测对象对应的安全检测结果信息，并将所述安全检测结果信息发送至计算设备侧的步骤包括：

在所述移动设备侧采用所述第三方应用依据所述安全检测请求执行对指定检测对象的安全检测操作，获得安全检测结果信息；

由所述第三方应用将所述安全检测结果信息返回至所述计算设备侧；

所述在所述移动设备侧接收计算设备侧发送的执行指令的步骤为：

在所述移动设备侧采用所述第三方应用接收计算设备侧发送的执行指令；

所述在所述移动设备侧执行所述执行指令的步骤为：

在所述移动设备侧采用所述第三方应用执行所述执行指令。

5. 如权利要求 2 所述的方法，其特征在于，所述移动设备侧安装有第一客户端程序，所述在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求的步骤为：

在所述移动设备侧采用所述第一客户端程序接收所述计算设备侧发出的对移动设备的安全检测请求；

所述在所述移动设备侧获取与所述指定检测对象对应的安全检测结果信息，并将所述安全检测结果信息发送至计算设备侧的步骤包括：

在所述移动设备侧采用所述第一客户端程序将所述安全检测请求发送至所述第三方应用，由所述第三方医用依据所述安全检测请求执行对指定检测对象的安全检测操作，获

得安全检测结果信息并返回第一客户端程序中；

所述第一客户端程序将所述安全检测结果信息返回至所述计算设备侧；

所述在所述移动设备侧接收计算设备侧发送的执行指令的步骤为：

在所述移动设备侧采用所述第一客户端程序接收计算设备侧发送的执行指令；

所述在所述移动设备侧执行所述执行指令的步骤为：

在所述移动设备侧采用所述第一客户端程序将所述执行指令发送至第三方应用，由所述第三方应用执行所述执行指令。

6. 如权利要求 1 所述的方法，其特征在于，所述指定检测对象包括针对移动设备的如下服务的一项或多项：移动设备挂马漏洞检测、检测是否开启云查杀、检测是否存在危险软件、检测是否更新过病毒库、检测安全服务是否开启、检测移动设备是否有山寨应用、检测移动设备上是否有恶意广告应用、主动防御功能开启检测。

7. 如权利要求 1 所述的方法，其特征在于，所述指定检测对象包括针对移动设备的如下服务的一项或多项：内存优化检测、检测是否存在后台软件、自动启动的软件检测、垃圾数据清理检测、清理缓存检测、清理应用卸载后存在的残留文件检测、安装包清理检测、大文件整理、隐私痕迹清理检测。

8. 一种对设备进行安全检测的方法，包括：

当计算设备侧安全检测到有移动设备接入时，在计算设备侧向所述移动设备侧发出对移动设备的安全检测请求，所述安全检测请求包括指定检测对象；

在所述计算设备侧接收所述移动设备侧返回的针对所述安全检测请求的安全检测结果信息，所述安全检测结果信息由所述移动设备侧依据所述指定检测对象获得；

在计算设备侧依据所述安全检测结果信息生成对应的执行指令并发送至所述移动设备侧，由所述移动设备侧执行所述执行指令。

9. 一种对设备进行安全检测的装置，包括：

安全检测请求接收模块，适于在移动设备连接至计算设备时，在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求，所述安全检测请求包括指定检测对象；

安全检测结果信息发送模块，适于在所述移动设备侧获取与所述指定检测对象对应的安全检测结果信息，并将所述安全检测结果信息发送至计算设备侧；

执行指令接收模块，适于在所述移动设备侧接收计算设备侧发送的执行指令，所述执行指令为计算设备依据所述安全检测结果信息生成；

执行指令执行模块，适于在所述移动设备侧执行所述执行指令。

10. 一种对设备进行安全检测的装置，包括：

安全检测请求发送模块，适于在计算设备侧安全检测到有移动设备接入时，在计算设备侧向所述移动设备侧发出对移动设备的安全检测请求，所述安全检测请求包括指定检测对象；

安全检测结果信息接收模块，适于在所述计算设备侧接收所述移动设备侧返回的针对所述安全检测请求的安全检测结果信息，所述安全检测结果信息由所述移动设备侧依据所述指定检测对象获得；

执行指令发送模块，适于在计算设备侧依据所述安全检测结果信息生成对应的执行指

令并发送至所述移动设备侧，由所述移动设备侧执行所述执行指令。

一种对设备进行安全检测方法和装置

技术领域

[0001] 本发明涉及设备安全检测技术领域，具体涉及一种对设备进行安全检测的方法，以及一种对设备进行安全检测的装置。

背景技术

[0002] 随着信息化程度的提高以及各种适用性技术的不断推出，计算机或手机等智能终端已经广泛应用在学习、娱乐、工作等方面，在人们的日常生活中扮演着越来越重要的角色。然而，智能终端的广泛应用也对智能终端在垃圾数据清理、安全防护等方面提出了更高要求。

[0003] 针对上述需求，很多第三方安全应用厂商开发出了针对智能终端安全应用，所述安全应用可以在智能终端侧对智能终端进行体检，并依据体检结果进行一系列的修复操作，以保证智能终端的性能和安全性。针对移动设备而言，虽然有些移动设备上预先安装了一些杀毒软件，但是往往用户未在其上安装手机卫士的时候，容易感染病毒，尤其是在访问了应用市场下载一些应用的时候，很容易被捆绑或者是下载到安装有恶意应用、插件、或者是广告应用之类的软件，往往导致用户在不能感知的情况下，遭受移动设备流量被偷跑、被窃取隐私、或者是恶意扣费等损失，所以有必要从各个渠道对用户的移动设备的安全进行防护。

发明内容

[0004] 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对设备进行安全检测的方法和相应的一种对设备进行安全检测的装置。

[0005] 依据本发明的一个方面，提供了一种对设备进行安全检测的方法，包括：

[0006] 当移动设备连接至计算设备时，在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求，所述安全检测请求中包括指定检测对象；

[0007] 在所述移动设备侧获取与所述指定检测对象对应的安全检测结果信息，并将所述安全检测结果信息发送至计算设备侧；

[0008] 在所述移动设备侧接收计算设备侧发送的执行指令，所述执行指令为计算设备依据所述安全检测结果信息生成；

[0009] 在所述移动设备侧执行所述执行指令。

[0010] 可选地，在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求的步骤之前，还包括：

[0011] 所述移动设备侧接收所述计算设备侧发送的第三方应用安装包，所述第三方应用安装包为所述计算设备侧在检测到所述移动设备侧没有安装第三方应用时，从服务器中下载得到；

[0012] 所述移动设备侧依据所述第三方应用安装包安装第三方应用。

[0013] 可选地，在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请

求的步骤之前，还包括：

[0014] 建立所述移动设备与所述计算设备的 SOCKET 连接通道，所述移动设备通过所述 SOCKET 连接通道接收安全检测请求、以及发送安全检测结果信息、以及接收执行指令。

[0015] 可选地，所述在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求的步骤为：

[0016] 在所述移动设备侧采用所述第三方应用接收所述计算设备侧发出的对移动设备的安全检测请求；

[0017] 所述在所述移动设备侧获取与所述指定检测对象对应的安全检测结果信息，并将所述安全检测结果信息发送至计算设备侧的步骤包括：

[0018] 在所述移动设备侧采用所述第三方应用依据所述安全检测请求执行对指定检测对象的安全检测操作，获得安全检测结果信息；

[0019] 由所述第三方应用将所述安全检测结果信息返回至所述计算设备侧；

[0020] 所述在所述移动设备侧接收计算设备侧发送的执行指令的步骤为：

[0021] 在所述移动设备侧采用所述第三方应用接收计算设备侧发送的执行指令；

[0022] 所述在所述移动设备侧执行所述执行指令的步骤为：

[0023] 在所述移动设备侧采用所述第三方应用执行所述执行指令。

[0024] 可选地，所述移动设备侧安装有第一客户端程序，所述在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求的步骤为：

[0025] 在所述移动设备侧采用所述第一客户端程序接收所述计算设备侧发出的对移动设备的安全检测请求；

[0026] 所述在所述移动设备侧获取与所述指定检测对象对应的安全检测结果信息，并将所述安全检测结果信息发送至计算设备侧的步骤包括：

[0027] 在所述移动设备侧采用所述第一客户端程序将所述安全检测请求发送至所述第三方应用，由所述第三方医用依据所述安全检测请求执行对指定检测对象的安全检测操作，获得安全检测结果信息并返回第一客户端程序中；

[0028] 所述第一客户端程序将所述安全检测结果信息返回至所述计算设备侧；

[0029] 所述在所述移动设备侧接收计算设备侧发送的执行指令的步骤为：

[0030] 在所述移动设备侧采用所述第一客户端程序接收计算设备侧发送的执行指令；

[0031] 所述在所述移动设备侧执行所述执行指令的步骤为：

[0032] 在所述移动设备侧采用所述第一客户端程序将所述执行指令发送至第三方应用，由所述第三方应用执行所述执行指令。

[0033] 可选地，所述第一客户端程序将所述安全检测请求发送至所述第三方应用的步骤包括：

[0034] 所述第一客户端程序依据所述指定检测对象调用所述第三方应用的服务的接口，将所述安全检测请求发送至所述第三方应用。

[0035] 可选地，所述指定检测对象包括针对移动设备的如下服务的一项或多项：移动设备挂马漏洞检测、检测是否开启云查杀、检测是否存在危险软件、检测是否更新过病毒库、检测安全服务是否开启、检测移动设备是否有山寨应用、检测移动设备上是否有恶意广告应用、主动防御功能开启检测。

[0036] 可选地，所述指定检测对象包括针对移动设备的如下服务的一项或多项：内存优化检测、检测是否存在后台软件、自动启动的软件检测、垃圾数据清理检测、清理缓存检测、清理应用卸载后存在的残留文件检测、安装包清理检测、大文件整理、隐私痕迹清理检测。

[0037] 可选地，所述安全检测结果信息包括安全检测进度信息，相应地，所述执行指令包括停止指令、暂停指令、继续执行指令。

[0038] 可选地，所述安全检测结果信息包括安全检测结果，相应地，所述执行指令包括以下的一项或多项：移动设备挂马漏洞修复、开启云查杀、危险软件修复、病毒库更新、开启安全服务、山寨应用修复、恶意广告应用修复、开启主动防御功能。

[0039] 可选地，所述安全检测结果信息包括安全检测结果，相应地，所述执行指令包括以下的一项或多项：内存优化、后台软件关闭、关闭自动启动的软件、垃圾数据清理、清理缓存、清理应用卸载后存在的残留文件、安装包清理、大文件整理、隐私痕迹清理。

[0040] 依据本发明的另一个方面，提供了一种对设备进行安全检测的方法，包括：

[0041] 当计算设备侧安全检测到有移动设备接入时，在计算设备侧向所述移动设备侧发出对移动设备的安全检测请求，所述安全检测请求包括指定检测对象；

[0042] 在所述计算设备侧接收所述移动设备侧返回的针对所述安全检测请求的安全检测结果信息，所述安全检测结果信息由所述移动设备侧依据所述指定检测对象获得；

[0043] 在计算设备侧依据所述安全检测结果信息生成对应的执行指令并发送至所述移动设备侧，由所述移动设备侧执行所述执行指令。

[0044] 可选地，在所述计算设备侧向所述移动设备侧发出对移动设备的安全检测请求的步骤之前，还包括：

[0045] 在计算设备侧读取所述移动设备侧中所有已安装应用的安装包信息，所述安装包信息包括安装包标识；

[0046] 在计算设备侧判断所述安装包标识中不存在第三方应用安装包标识时，从服务器中获取所述第三方应用安装包的下载地址；

[0047] 在计算设备侧依据所述第三方应用安装包的下载地址下载所述第三方应用安装包并发送至移动设备侧。

[0048] 可选地，在所述计算设备侧向所述移动设备侧发出对移动设备的安全检测请求的步骤之前，还包括：

[0049] 建立所述移动设备与所述计算设备的 SOCKET 连接通道，所述计算设备通过所述连接通道发送安全检测请求、以及接收安全检测结果信息、以及发送执行指令。

[0050] 可选地，所述安全检测结果信息具有类型标识的信息，所述在计算设备侧依据所述安全检测结果信息生成对应的执行指令并发送至所述移动设备侧的步骤包括：

[0051] 计算设备侧在预设映射表中查找所述类型标识对应的执行建议信息，所述预设映射表中存储有计算设备与移动设备预先约定的类型标识与执行建议信息的映射关系；

[0052] 在计算设备侧展示所述安全检测结果信息以及对应的执行建议信息；

[0053] 在计算设备侧接收用户对所述一个或多个执行建议信息的选定指令；

[0054] 依据所述选定指令生成一个或多个执行建议信息对应的执行指令并发送至移动设备侧。

[0055] 可选地，所述指定检测对象包括针对移动设备的如下服务的一项或多项：移动设

备挂马漏洞检测、检测是否开启云查杀、检测是否存在危险软件、检测是否更新过病毒库、检测安全服务是否开启、检测移动设备是否有山寨应用、检测移动设备上是否有恶意广告应用、主动防御功能开启检测。

[0056] 可选地，所述指定检测对象包括针对移动设备的如下服务的一项或多项：内存优化检测、检测是否存在后台软件、自动启动的软件检测、垃圾数据清理检测、清理缓存检测、清理应用卸载后存在的残留文件检测、安装包清理检测、大文件整理、隐私痕迹清理检测。

[0057] 可选地，所述安全检测结果信息包括安全检测进度信息，相应地，所述执行指令包括停止指令、暂停指令、继续执行指令。

[0058] 可选地，所述安全检测结果信息包括安全检测结果，相应地，所述执行指令包括以下的一项或多项：移动设备挂马漏洞修复、开启云查杀、危险软件修复、病毒库更新、开启安全服务、山寨应用修复、恶意广告应用修复、开启主动防御功能。

[0059] 可选地，所述安全检测结果信息包括安全检测结果，相应地，所述执行指令包括以下的一项或多项：内存优化、后台软件关闭、关闭自动启动的软件、垃圾数据清理、清理缓存、清理应用卸载后存在的残留文件、安装包清理、大文件整理、隐私痕迹清理。

[0060] 依据本发明的另一个方面，提供了一种对设备进行安全检测的装置，包括：

[0061] 安全检测请求接收模块，适于在移动设备连接至计算设备时，在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求，所述安全检测请求包括指定检测对象；

[0062] 安全检测结果信息发送模块，适于在所述移动设备侧获取与所述指定检测对象对应的安全检测结果信息，并将所述安全检测结果信息发送至计算设备侧；

[0063] 执行指令接收模块，适于在所述移动设备侧接收计算设备侧发送的执行指令，所述执行指令为计算设备依据所述安全检测结果信息生成；

[0064] 执行指令执行模块，适于在所述移动设备侧执行所述执行指令。

[0065] 可选地，所述装置还包括：

[0066] 安装包接收模块，适于在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求的之前，所述移动设备侧接收所述计算设备侧发送的第三方应用安装包，所述第三方应用安装包为所述计算设备侧在检测到所述移动设备侧没有安装第三方应用时，从服务器中下载得到；

[0067] 安装包安装模块，适于所述移动设备侧依据所述第三方应用安装包安装第三方应用。

[0068] 可选地，所述装置还包括：

[0069] 通道建立模块，适于在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求之前，建立所述移动设备与所述计算设备的 SOCKET 连接通道，所述移动设备通过所述 SOCKET 连接通道接收安全检测请求、以及发送安全检测结果信息、以及接收执行指令。

[0070] 可选地，所述安全检测请求接收模块还适于：

[0071] 在所述移动设备侧采用所述第三方应用接收所述计算设备侧发出的对移动设备的安全检测请求；

[0072] 所述安全检测结果信息发送模块还适于：

[0073] 在所述移动设备侧采用所述第三方应用依据所述安全检测请求执行对指定检测对象的安全检测操作，获得安全检测结果信息；

[0074] 由所述第三方应用将所述安全检测结果信息返回至所述计算设备侧；

[0075] 所述执行指令接收模块还适于：

[0076] 在所述移动设备侧采用所述第三方应用接收计算设备侧发送的执行指令；

[0077] 所述执行指令执行模块还适于：

[0078] 在所述移动设备侧采用所述第三方应用执行所述执行指令。

[0079] 可选地，所述安全检测请求接收模块还适于：

[0080] 在所述移动设备侧采用所述第一客户端程序接收所述计算设备侧发出的对移动设备的安全检测请求；

[0081] 所述安全检测结果信息发送模块还适于：

[0082] 在所述移动设备侧采用所述第一客户端程序将所述安全检测请求发送至所述第三方应用，由所述第三方医用依据所述安全检测请求执行对指定检测对象的安全检测操作，获得安全检测结果信息并返回第一客户端程序中；

[0083] 所述第一客户端程序将所述安全检测结果信息返回至所述计算设备侧；

[0084] 所述执行指令接收模块还适于：

[0085] 在所述移动设备侧采用所述第一客户端程序接收计算设备侧发送的执行指令；

[0086] 所述执行指令执行模块还适于：

[0087] 在所述移动设备侧采用所述第一客户端程序将所述执行指令发送至第三方应用，由所述第三方应用执行所述执行指令。

[0088] 可选地，所述第一客户端程序将所述安全检测请求发送至所述第三方应用，具体为：

[0089] 所述第一客户端程序依据所述指定检测对象调用所述第三方应用的服务的接口，将所述安全检测请求发送至所述第三方应用。

[0090] 可选地，所述指定检测对象包括针对移动设备的如下服务的一项或多项：移动设备挂马漏洞检测、检测是否开启云查杀、检测是否存在危险软件、检测是否更新过病毒库、检测安全服务是否开启、检测移动设备是否有山寨应用、检测移动设备上是否有恶意广告应用、主动防御功能开启检测。

[0091] 可选地，所述指定检测对象包括针对移动设备的如下服务的一项或多项：内存优化检测、检测是否存在后台软件、自动启动的软件检测、垃圾数据清理检测、清理缓存检测、清理应用卸载后存在的残留文件检测、安装包清理检测、大文件整理、隐私痕迹清理检测。

[0092] 可选地，所述安全检测结果信息包括安全检测进度信息，相应地，所述执行指令包括停止指令、暂停指令、继续执行指令。

[0093] 可选地，所述安全检测结果信息包括安全检测结果，相应地，所述执行指令包括以下的一项或多项：移动设备挂马漏洞修复、开启云查杀、危险软件修复、病毒库更新、开启安全服务、山寨应用修复、恶意广告应用修复、开启主动防御功能。

[0094] 可选地，所述安全检测结果信息包括安全检测结果，相应地，所述执行指令包括以下的一项或多项：内存优化、后台软件关闭、关闭自动启动的软件、垃圾数据清理、清理缓存、清理应用卸载后存在的残留文件、安装包清理、大文件整理、隐私痕迹清理。

[0095] 依据本发明的另一个方面，提供了一种对设备进行安全检测的装置，包括：

[0096] 安全检测请求发送模块，适于在计算设备侧安全检测到有移动设备接入时，在计算设备侧向所述移动设备侧发出对移动设备的安全检测请求，所述安全检测请求包括指定检测对象；

[0097] 安全检测结果信息接收模块，适于在所述计算设备侧接收所述移动设备侧返回的针对所述安全检测请求的安全检测结果信息，所述安全检测结果信息由所述移动设备侧依据所述指定检测对象获得；

[0098] 执行指令发送模块，适于在计算设备侧依据所述安全检测结果信息生成对应的执行指令并发送至所述移动设备侧，由所述移动设备侧执行所述执行指令。

[0099] 可选地，所述装置还包括：

[0100] 安装包信息获取模块，适于在所述计算设备侧向所述移动设备侧发出对移动设备的安全检测请求之前，在计算设备侧读取所述移动设备侧中所有已安装应用的安装包信息，所述安装包信息包括安装包标识；

[0101] 查找模块，适于在计算设备侧判断所述安装包标识中不存在第三方应用安装包标识时，从服务器中获取所述第三方应用安装包的下载地址；

[0102] 安装包发送模块，适于在计算设备侧依据所述第三方应用安装包的下载地址下载所述第三方应用安装包并发送至移动设备侧。

[0103] 可选地，所述装置还包括：

[0104] 连接通道建立模块，适于在所述计算设备侧向所述移动设备侧发出对移动设备的安全检测请求之前，建立所述移动设备与所述计算设备的 SOCKET 连接通道，所述计算设备通过所述连接通道发送安全检测请求、以及接收安全检测结果信息、以及发送执行指令。

[0105] 可选地，所述安全检测结果信息具有类型标识的信息，所述执行指令发送模块还适于：

[0106] 计算设备侧在预设映射表中查找所述类型标识对应的执行建议信息，所述预设映射表中存储有计算设备与移动设备预先约定的类型标识与执行建议信息的映射关系；

[0107] 在计算设备侧展示所述安全检测结果信息以及对应的执行建议信息；

[0108] 在计算设备侧接收用户对所述一个或多个执行建议信息的选定指令；

[0109] 依据所述选定指令生成一个或多个执行建议信息对应的执行指令并发送至移动设备侧。

[0110] 可选地，所述指定检测对象包括针对移动设备的如下服务的一项或多项：移动设备挂马漏洞检测、检测是否开启云查杀、检测是否存在危险软件、检测是否更新过病毒库、检测安全服务是否开启、检测移动设备是否有山寨应用、检测移动设备上是否有恶意广告应用、主动防御功能开启检测。

[0111] 可选地，所述指定检测对象包括针对移动设备的如下服务的一项或多项：内存优化检测、检测是否存在后台软件、自动启动的软件检测、垃圾数据清理检测、清理缓存检测、清理应用卸载后存在的残留文件检测、安装包清理检测、大文件整理、隐私痕迹清理检测。

[0112] 可选地，所述安全检测结果信息包括安全检测进度信息，相应地，所述执行指令包括停止指令、暂停指令、继续执行指令。

[0113] 可选地，所述安全检测结果信息包括安全检测结果，相应地，所述执行指令包括以

下的一项或多项：移动设备挂马漏洞修复、开启云查杀、危险软件修复、病毒库更新、开启安全服务、山寨应用修复、恶意广告应用修复、开启主动防御功能。

[0114] 可选地，所述安全检测结果信息包括安全检测结果，相应地，所述执行指令包括以下的一项或多项：内存优化、后台软件关闭、关闭自动启动的软件、垃圾数据清理、清理缓存、清理应用卸载后存在的残留文件、安装包清理、大文件整理、隐私痕迹清理。

[0115] 与背景技术相比，本发明具有如下有益效果：

[0116] 在本发明中，当移动设备连接至计算设备时，在计算设备侧即可实现对移动设备的指定检测对象的安全检测，并在计算设备接收移动设备返回的安全检测结果时可以对在计算设备侧向移动设备发出执行指令促使移动设备针对安全检测结果执行相关的操作，使得用户在计算设备侧即可实现对移动设备的安全检测，从而提高移动设备的安全性。

[0117] 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

[0118] 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：

[0119] 图 1 示出了本发明的一种对设备进行安全检测的方法实施例一的步骤流程图；

[0120] 图 2 示出了本发明的一种对设备进行安全检测的方法实施例二的步骤流程图；

[0121] 图 3 示出了本发明的一种对设备进行安全检测的方法实施例三的步骤流程图；

[0122] 图 4 示出了本发明的一种对设备进行安全检测的方法实施例四的步骤流程图；

[0123] 图 5 示出了本发明的一种对设备进行安全检测的装置实施例一的结构框图；

[0124] 图 6 示出了本发明的一种对设备进行安全检测的装置实施例二的结构框图。

具体实施方式

[0125] 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。

[0126] 参照图 1，示出了本发明的一种对设备进行安全检测的方法实施例一的步骤流程图，本发明实施例从移动设备侧进行说明，可以包括如下步骤：

[0127] 步骤 101，当移动设备连接至计算设备时，在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求，所述安全检测请求包括指定检测对象；

[0128] 在本发明的一种优选实施例中，所述指定检测对象包括针对移动设备的如下服务的一项或多项：移动设备挂马漏洞检测、检测是否开启云查杀、检测是否存在危险软件、检测是否更新过病毒库、检测安全服务是否开启、检测移动设备是否有山寨应用、检测移动设备上是否有恶意广告应用、主动防御功能开启检测、内存优化检测、检测是否存在后台软件、自动启动的软件检测、垃圾数据清理检测、清理缓存检测、清理应用卸载后存在的残留

文件检测、安装包清理检测、大文件整理、隐私痕迹清理检测。

[0129] 步骤 102，在所述移动设备侧获取与所述指定检测对象对应的安全检测结果信息，并将所述安全检测结果信息发送至计算设备侧；

[0130] 步骤 103，在所述移动设备侧接收计算设备侧发送的执行指令，所述执行指令为计算设备依据所述安全检测结果信息生成；

[0131] 在本发明的一种优选实施例中，所述安全检测结果信息可以包括安全检测进度信息，相应的，所述执行指令可以包括停止指令、暂停指令、继续执行指令。

[0132] 在本发明的另一种优选实施例中，所述安全检测结果信息包括安全检测结果，相应地，所述执行指令可以包括以下的一项或多项：移动设备挂马漏洞修复、开启云查杀、危险软件修复、病毒库更新、开启安全服务、山寨应用修复、恶意广告应用修复、开启主动防御功能、内存优化、后台软件关闭、关闭自动启动的软件、垃圾数据清理、清理缓存、清理应用卸载后存在的残留文件、安装包清理、大文件整理、隐私痕迹清理。

[0133] 步骤 104，在所述移动设备侧执行所述执行指令。

[0134] 在本发明的一种优选实施例中，在所述步骤 101 之前，还可以包括：

[0135] 所述移动设备侧接收所述计算设备侧发送的第三方应用安装包，所述第三方应用安装包为所述计算设备侧在检测到所述移动设备侧没有安装第三方应用时，从服务器中下载得到；

[0136] 所述移动设备侧依据所述第三方应用安装包安装第三方应用。

[0137] 在本发明的一种优选实施例中，在所述步骤 101 之前，还可以包括：

[0138] 建立所述移动设备与所述计算设备的 SOCKET 连接通道，所述移动设备通过所述 SOCKET 连接通道接收安全检测请求、以及发送安全检测结果信息、以及接收执行指令。

[0139] 在本发明的一种优选实施例中，所述步骤 101 具体可以为：

[0140] 在所述移动设备侧采用所述第三方应用接收所述计算设备侧发出的对移动设备的安全检测请求；

[0141] 所述步骤 102 可以包括如下子步骤：

[0142] 在所述移动设备侧采用所述第三方应用依据所述安全检测请求执行对指定检测对象的安全检测操作，获得安全检测结果信息；

[0143] 由所述第三方应用将所述安全检测结果信息返回至所述计算设备侧；

[0144] 所述步骤 103 具体可以为：

[0145] 在所述移动设备侧采用所述第三方应用接收计算设备侧发送的执行指令；

[0146] 所述步骤 104 具体可以为：

[0147] 在所述移动设备侧采用所述第三方应用执行所述执行指令。

[0148] 具体而言，所述移动设备侧可以通过所述第三方应用接收计算设备侧发出的对移动设备的安全检测请求，所述第三方应用依据所述安全检测请求执行对指定检测对象的安全检测操作，获得安全检测结果信息并返回所述计算设备侧。

[0149] 在本发明的另一种优选实施例中，所述移动设备侧安装有第一客户端程序，所述步骤 101 可以为：

[0150] 在所述移动设备侧采用所述第一客户端程序接收所述计算设备侧发出的对移动设备的安全检测请求；

[0151] 所述步骤 102 可以包括如下子步骤：

[0152] 在所述移动设备侧采用所述第一客户端程序将所述安全检测请求发送至所述第三方应用，由所述第三方应用依据所述安全检测请求执行对指定检测对象的安全检测操作，获得安全检测结果信息并返回第一客户端程序中；

[0153] 所述第一客户端程序将所述安全检测结果信息返回至所述计算设备侧；

[0154] 所述步骤 103 可以为：

[0155] 在所述移动设备侧采用所述第一客户端程序接收计算设备侧发送的执行指令；

[0156] 所述步骤 104 可以为：

[0157] 在所述移动设备侧采用所述第一客户端程序将所述执行指令发送至第三方应用，由所述第三方应用执行所述执行指令。

[0158] 具体而言，所述移动设备可以通过所述第一客户端程序接收计算设备侧发出的对移动设备的安全检测请求，所述第一客户端程序将所述安全检测请求发送至所述第三方应用，接收所述第三方应用返回的安全检测结果信息并返回计算设备侧，其中，所述安全检测结果信息由所述第三方应用依据所述安全检测请求执行对指定检测对象的安全检测操作获得。

[0159] 在本发明的一种优选实施例中，所述第一客户端程序将所述安全检测请求发送至所述第三方应用的步骤可以包括：

[0160] 所述第一客户端程序依据所述指定检测对象调用所述第三方应用的服务的接口，将所述安全检测请求发送至所述第三方应用。

[0161] 在本发明实施例中，当移动设备连接至计算设备时，在计算设备侧即可实现对移动设备的指定检测对象的安全检测，并在计算设备接收在移动设备返回的安全检测结果时可以对在计算设备侧向移动设备发出执行指令促使移动设备针对安全检测结果执行相关的操作，使得用户在计算设备侧即可实现对移动设备的安全检测，从而提高移动设备的安全性。

[0162] 参照图 2，示出了本发明的一种对设备进行安全检测的方法实施例二的步骤流程图，本发明实施例从计算设备侧进行说明，本发明实施例可以包括如下步骤：

[0163] 步骤 201，当计算设备侧安全检测到有移动设备接入时，在计算设备侧向所述移动设备侧发出对移动设备的安全检测请求，所述安全检测请求包括指定检测对象；

[0164] 在本发明的一种优选实施例中，所述指定检测对象可以包括针对移动设备的如下服务的一项或多项：移动设备挂马漏洞检测、检测是否开启云查杀、检测是否存在危险软件、检测是否更新过病毒库、检测安全服务是否开启、检测移动设备是否有山寨应用、检测移动设备上是否有恶意广告应用、主动防御功能开启检测、内存优化检测、检测是否存在后台软件、自动启动的软件检测、垃圾数据清理检测、清理缓存检测、清理应用卸载后存在的残留文件检测、安装包清理检测、大文件整理、隐私痕迹清理检测。

[0165] 步骤 202，在所述计算设备侧接收所述移动设备侧返回的针对所述安全检测请求的安全检测结果信息，所述安全检测结果信息由所述移动设备侧依据所述指定检测对象获得；

[0166] 步骤 203，在计算设备侧依据所述安全检测结果信息生成对应的执行指令并发送至所述移动设备侧，由所述移动设备侧执行所述执行指令。

[0167] 在本发明的一种优选实施例中，所述安全检测结果信息可以包括安全检测进度信息，相应地，所述执行指令可以包括停止指令、暂停指令、继续执行指令。

[0168] 在本发明的一种优选实施例中，所述安全检测结果信息可以包括安全检测结果，相应地，所述可以执行指令包括以下的一项或多项：移动设备挂马漏洞修复、开启云查杀、危险软件修复、病毒库更新、开启安全服务、山寨应用修复、恶意广告应用修复、开启主动防御功能、内存优化、后台软件关闭、关闭自动启动的软件、垃圾数据清理、清理缓存、清理应用卸载后存在的残留文件、安装包清理、大文件整理、隐私痕迹清理。

[0169] 在本发明的一种优选实施例中，在所述步骤 201 之前，还可以包括：

[0170] 在计算设备侧读取所述移动设备侧中所有已安装应用的安装包信息，所述安装包信息包括安装包标识；

[0171] 在计算设备侧判断所述安装包标识中不存在第三方应用安装包标识时，从服务器中获取所述第三方应用安装包的下载地址；

[0172] 在计算设备侧依据所述第三方应用安装包的下载地址下载所述第三方应用安装包并发送至移动设备侧。

[0173] 在本发明的一种优选实施例中，在所述步骤 201 之前，还可以包括：

[0174] 建立所述移动设备与所述计算设备的 SOCKET 连接通道，所述计算设备通过所述连接通道发送安全检测请求、以及接收安全检测结果信息、以及发送执行指令。

[0175] 在本发明的一种优选实施例中，所述安全检测结果信息具有类型标识的信息，所述步骤 203 可以包括如下子步骤：

[0176] 子步骤 S11，计算设备侧在预设映射表中查找所述类型标识对应的执行建议信息，所述预设映射表中存储有计算设备与移动设备预先约定的，类型标识与执行建议信息的映射关系；

[0177] 子步骤 S12，在计算设备侧展示所述安全检测结果信息以及对应的执行建议信息；

[0178] 子步骤 S13，在计算设备侧接收用户对所述一个或多个执行建议信息的选定指令；

[0179] 子步骤 S14，依据所述选定指令生成一个或多个执行建议信息对应的执行指令并发送至移动设备侧。

[0180] 参照图 3，示出了本发明的一种对设备进行安全检测的方法实施例三的步骤流程图，其中，所述计算设备是一种能够按照程序运行，自动、高速处理海量数据的智能电子设备，如台式电脑、笔记本电脑等。所述移动设备是一种可以在移动中使用的计算设备，如手机。本实施例以安装有安卓操作系统的移动设备为例，当然，本发明并不限于安装有安卓系统的移动设备，本发明的原理同样适用于安装有其他操作系统的移动设备。

[0181] 在本发明实施例中，移动设备侧安装有第一客户端程序，计算设备侧安装有第二客户端程序，所述移动设备与所述计算设备通过所述第一客户端程序以及所述第二客户端程序进行通信，当所述第一客户端程序没有启动时，第二客户端程序可以通过向第一客户端程序发送启动指令来启动所述第一客户端程序，进而开启两者间的通信过程。

[0182] 所述方法可以包括如下步骤：

[0183] 步骤 301，当移动设备连接至计算设备时，第二客户端程序检测所述移动设备是否

安装有第三方应用，若否，则执行步骤 302，若是，则执行步骤 304 ；

[0184] 在具体实现中，计算设备侧的第二客户端程序在检测到移动设备成功连接至计算设备时，可以读取移动设备侧中所有已安装应用的安装包信息，其中所述安装包信息携带有安装包标识。第二客户端程序在所述所有安装包标识中查找是否存在第三方应用的安装包标识，若存在，则说明移动设备侧安装有第三方应用，否则，则说明移动设备侧没有安装有第三方应用。

[0185] 进一步的，所述安装包信息还可以携带有各应用的版本号，若计算设备查找发现所述移动设备安装有第三方应用，但所述第三方应用的版本号小于计算设备侧存储的第三方应用的最新版本号，则计算设备同样判定所述移动设备侧没有安装第三方应用。

[0186] 步骤 302，第二客户端程序下载所述第三方应用安装包发送至移动设备侧 ；

[0187] 在具体实现中，移动设备可以通过数据线或者无线（如无线网路通信技术 WIFI）等形式连接到计算设备，当移动设备通过数据线接入计算设备时，若第二客户端程序检测到所述移动设备没有安装有第三方应用，则在服务器中查找所述第三方应用的安装包标识，在找到所述第三方应用的安装包标识时获取所述第三方应用安装包的下载地址，从所述下载地址中下载第三方应用安装包并将所述第三方应用安装包通过数据线传送至移动设备侧。

[0188] 更进一步地，在所述移动设备为安装有安卓系统的安卓设备时，所述第二客户端程序可以通过 ADB （Android Debug Bridge，就是起到调试桥的作用）驱动将第三方应用安装包发送至移动设备侧，其中，ADB 是一个客户端 - 服务器端程序，其中客户端是计算设备，服务器端是安卓设备，而 ADB 驱动就是计算设备与安卓设备的通信的客户端驱动程序，ADB 是 androidsdk 里的一个工具，用这个工具可以直接操作管理安卓模拟器或者真实的安卓设备（如手机）。它的主要功能有 ：运行设备的 shell（命令行）；管理模拟器或设备的端口映射 ；计算设备和安卓设备之间上传 / 下载文件 ；将本地安卓安装包 apk 安装至模拟器或安卓设备等。

[0189] 当移动设备以无线的方式与计算设备建立连接时，若第二客户端程序检测到所述移动设备没有安装有第三方应用，则在服务器中查找所述第三方应用的安装包标识，在找到所述第三方应用的安装包标识时获取所述第三方应用安装包的下载地址，从所述下载地址中下载第三方应用安装包并将所述第三方应用安装包通过无线通道传送至移动设备侧。在实际中，第二客户端程序也可以直接将所述第三方应用安装包的下载地址将所述发送至移动设备侧，由移动设备侧进行下载安装。

[0190] 具体来说，移动设备以无线的方式与计算设备建立连接的过程，可以为 ：

[0191] 当计算设备与移动设备要连接时，计算设备首先会发送连接请求给服务器。其中，所述连接请求中包括设备标识和请求连接的移动设备的终端数据。

[0192] 所述设备标识用于标识一个计算设备，如，计算设备的 IP 地址，网卡地址和 MID 值等。其中，MID （Mobile Internet Device，移动互联网设备）值是通过硬件的编号计算出的唯一的特征值。

[0193] 所述终端数据是移动设备的相关数据，如移动设备的名称，移动设备的国际移动设备身份码（International Mobile Equipment Identity，IMEI），移动设备的型号等，此外，若移动设备是手机，则对应的终端数据还可以包括该手机的手机号码。其中，所述 IMEI

可以唯一标识一个移动设备。

[0194] 则服务器对应可以接收到所述连接请求，从所述连接请求中可以获取所述计算设备的设备标识，从而确定要连接的计算设备，并且获取所述计算设备请求连接的移动设备的终端数据。

[0195] 而服务器记录与其通信过的移动设备（或计算设备）的终端数据（或设备数据），因此可以依据所述终端数据查找所述移动设备，即检测所述终端数据与服务器中存储的任一移动设备的终端数据是否匹配，若匹配，则说明可以查找到所述移动设备，则构建所述设备标识与所述终端数据的映射关系，以建立所述移动设备与所述计算设备的关联关系；若不匹配，则说明未查找到所述移动设备，即所述移动设备暂时未能与服务器通信。

[0196] 步骤 303，移动设备侧依据所述第三方应用安装包安装第三方应用，继续执行步骤 304；

[0197] 具体而言，当移动设备接收到所述第三方应用安装包后即依据所述第三方应用安装包安装第三方应用；另一种情况下，当移动设备接收到的是第三方应用安装包的下载地址时，则依据所述第三方应用安装包的下载地址下载所述第三方应用安装包并进行第三方应用的安装，在第三方应用完成安装后，移动设备通过长连接返回安装完成消息至计算设备，以通知计算设备所述第三方应用已经安装完成。

[0198] 在本发明实施例中，在计算设备侧可以检测移动设备侧是否安装有第三方应用，在检测到移动设备侧没有安装第三方应用时，计算设备则自动下载第三方应用安装包发送至移动设备进行安装，在这个过程中，移动设备在不需要联网的情况下也可以顺利安装第三方应用，节省移动设备的资源，丰富了对移动设备进行安全防护的渠道，提高了移动设备的安全性；并且用户不需要进行任何操作即可以在移动设备侧安装第三方应用（或其他应用），方便快捷，提高用户体验。

[0199] 应用于本发明实施例，所述第三方应用可以为安全检测类服务应用，如 360 手机卫士，金山卫士等等，本发明实施例对第三方应用的具体类型无需加以限制。

[0200] 步骤 304，建立所述移动设备与所述计算设备的 SOCKET 连接通道；

[0201] 具体而言，所述建立所述移动设备与所述计算设备的 SOCKET（套接字）连接通道的过程，实际上是以所述移动设备作为服务器，以所述计算设备作为客户端的服务器－客户端 SOCKET 连接过程，该过程可以分为服务器监听、客户端请求、连接确认三个步骤，其中，服务器监听是指服务器端套接字并不定位具体的客户端套接字，而是处于等待连接的状态，实时监控网络状态；客户端请求是指由客户端的套接字提出连接请求，要连接的目标是服务器端的套接字。为此，客户端的套接字必须首先描述它要连接的服务器的套接字，指出服务器端套接字的地址和端口号，然后就向服务器端套接字提出连接请求；连接确认是指当服务器端套接字监听到或者说接收到客户端套接字的连接请求，它就响应客户端套接字的请求，建立一个新的线程，把服务器端套接字的描述发给客户端，一旦客户端确认了此描述，连接（或连接通道）就建立好了，此时便可以进行第一客户端程序与第二客户端程序间的一系列数据传输。

[0202] 在具体实现中，服务器通过调用 socket 函数，建立了监听连接的套接字，然后调用 bind 函数，将套接字与地址信息关联起来。调用 listen 函数实现对该端口的监听，当有连接请求时，通过调用 accept 函数建立与客户端的连接，最后，调用 read 函数来读取客户

端发送过来的消息，当然也可以使用 recv 函数实现相同的功能。

[0203] 步骤 305，所述第二客户端程序通过所述 SOCKET 连接通道向所述第一客户端程序发出对移动设备的安全检测请求，所述安全检测请求包括指定检测对象；

[0204] 所述安全检测请求为保证移动设备安全的检测请求，作为本实施例的一种优选示例，所述安全检测请求可以包括指定检测对象，所述指定检测对象为针对移动设备进行安全检测的项目，可以包括针对移动设备的如下服务的一项或多项：移动设备挂马漏洞检测、检测是否开启云查杀、检测是否存在危险软件、检测是否更新过病毒库、检测安全服务是否开启、检测移动设备是否有山寨应用、检测移动设备上是否有恶意广告应用、主动防御功能开启检测，等等。

[0205] 作为本实施例的另一种优选示例，所述安全检测请求可以包括指定检测对象，所述指定检测对象为针对移动设备进行优化和垃圾清理的项目，可以包括针对移动设备的如下服务的一项或多项：内存优化检测、检测是否存在后台软件、自动启动的软件检测、垃圾数据清理检测、清理缓存检测、清理应用卸载后存在的残留文件检测、安装包清理检测、大文件整理、隐私痕迹清理检测，等等。

[0206] 步骤 306，所述第一客户端程序将所述安全检测请求发送至第三方应用；

[0207] 在实际中，所述第三方应用在移动设备侧的安装过程中，可以建立多种服务（service），第一客户端程序在接收到安全检测请求后，根据所述指定检测对象定位第三方应用对应的服务，例如，若所述指定检测对象为垃圾数据安全检测，则其对应的第三方应用的服务为清理服务。第一客户端程序通过调用所述第三方应用对应的服务的接口来将所述安全检测请求发送至第三方应用中。

[0208] 步骤 307，所述第三方应用对所述指定检测对象执行对应的安全检测操作，获得安全检测结果信息；

[0209] 具体而言，所述安全检测请求中的指定检测对象包括类型标识的信息，所述类型标识的信息为第三方应用与服务器约定的指示指定检测对象的检测类型的信息，不同的类型标识的信息标识不同的操作，通过所述类型标识的信息第三方应用可以知道该检测对象为哪种检测，从而执行对应的操作，获得安全检测结果信息。例如，

[0210] 体检的类型标识的信息为 CMD_SYSTEM_EXAM_SCAN；

[0211] 垃圾清理的类型标识的信息为 CMD_CLEAR_GARBAGE_SCAN；

[0212] 杀毒的类型标识的信息为 CMD_SECURITY_SCAN。

[0213] 作为本发明实施例的一种优选示例，若所述检测对象为主动防御功能开启检测，其具体的检测规则可以为：第三方应用首先检测移动设备具备主动防御功能，若是，则检测所述主动防御功能是否开启；若否，则第三方设备检测所述第一客户端程序是否开启主动防御功能。

[0214] 作为本实施例的另一种示例，若所述指定检测对象为检测移动设备是否有山寨应用，其具体的检测规则可以为：第三方应用扫描移动设备的 APP（application，应用）列表，获取所述应用列表中的每个应用的开发者签名或 MD5 值，并将所述应用列表中的应用与应用白名单中的应用进行对比，如果某应用在应用白名单里，再将该应用的开发者签名或 MD5 值与白名单中对应的应用的开发者签名或 MD5 值进行比对，如果该应用的开发者签名或 MD5 值与白名单中的对应应用的开发者签名或 MD5 值不一致，则判定该应用属于山寨应用；

如果某应用不在应用白名单里，则扫描病毒库或(进行云查杀)，如果该应用在病毒库中，则报病毒或木马。

[0215] 作为本实施例的另一种示例，若所述指定检测对象为检测移动设备是否存在危险软件或是否有恶意广告应用，其具体的检测规则可以为：第三方应用扫描移动设备的APP(application，应用)列表，将应用列表中的应用与服务器中的黑白名单进行匹配。其中，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。当应用的进程为白进程(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为可信的应用(或安全应用)，允许该进程的运行；当应用进程为黑进程时(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移动设备进行任何操作(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第一客户端程序，由第一客户端程序返回计算设备侧。

[0216] 另外，本示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。

[0217] 例如，以杀毒为例，第三方应用(如手机卫士)通过以下方式获取病毒结果：

[0218] (1)扫描Android安装包，并从所述Android安装包中提取出指定的特征信息；

[0219] 本例中提取的特征信息可以包括：

[0220] 1)Android安装包包名：packageName

[0221] 2)Android安装包版本号：versionCode

[0222] 3)Android安装包的数字签名的MD5：signature[0]

[0223] 4)Android组件receiver

[0224] 5)classes.dex中的指令

[0225] 6)ELF文件中的字符串

[0226] 7)assets，res，lib等目录下各文件的MD5

[0227] 8)Android组件service，activity

[0228] (2)在预置的安全识别库中查找与指定的单个特征信息或其组合相匹配的特征记录；其中，所述安全识别库中包含特征记录及特征记录对应的安全级别，每条特征记录中包含单个特征信息或特征信息的组合；

[0229] (3)将查找到的特征记录对应的安全级别包含在所述Android安装包的安全检测结果中显示。

[0230] 本示例列举出安全、危险、谨慎和木马四个安全级别。其中，各种安全级别的定义如下：

[0231] 安全：该应用是一个正常的应用，没有任何威胁用户手机安全的行为；

[0232] 危险：该应用存在安全风险，有可能该应用本身就是恶意软件；也有可能该应用本来是正规公司发布的正常软件，但是因为存在安全漏洞，导致用户的隐私、手机安全受到威胁；

[0233] 谨慎：该应用是一个正常的应用，但是存在一些问题，例如会让用户不小心被扣费，或者有不友好的广告遭到投诉等；当发现这类应用之后，会提示用户谨慎使用并告知该应用可能的行为，但是由用户自行决定是否清除该应用；

[0234] 木马：该应用是病毒、木马或者其他恶意软件，此处为了简单统称为木马，但并不表示该应用仅仅是木马。

[0235] 所以，在设置安全识别库时，可以将安全、危险、谨慎和木马四个级别下的 Android 安装包都作为样本 Android 安装包，从而由样本中的单个特征或特征组合得到的特征记录可分别对应着一种安全级别及相关的行为和描述等信息。

[0236] 例如，安全识别库中的特征记录有四条，第一条特征记录和第四条特征记录分别对应的安全级别均为木马级别，第二条特征记录和第三条特征记录分别对应的安全级别均为安全级别。

[0237] 当然，安全识别库中还可以设置一条特征记录，列出某种木马的 Android 安装包版本号及其数字签名的 MD5 值，虽然这条特征记录使用的特征组合与第二条特征记录相同，都使用了版本号与数字签名 MD5 值的组合，但是这条特征记录对应的安全级别则为“木马”。

[0238] 所以，安全级别并不与某一种特定的特征或特征组合相对应，而是与具体的特征或特征组合的取值相对应。因此，对于相同的特征或特征组合，具体取值不同，对应的安全级别也是不同的。

[0239] 而且，上述安全、危险、谨慎和木马四个级别的定义仅作为举例说明，根据实际应用，当然也可以有其他的安全级别分类及定义，本示例的保护范围并不限定于此。

[0240] 那么，所述在预置的安全识别库中查找与指定的单个特征信息或其组合相匹配的特征记录，并将查找到的特征记录对应的安全级别包含在所述 Android 安装包的安全检测结果的步骤，可以理解为：

[0241] 在安全识别库中查找特征记录，如果提取出的指定单个特征与第一条特征记录相匹配，则可以判定当前的 Android 安装包为木马级别；如果提取出的指定特征进行组合后与第二条特征记录或者第三条特征记录相匹配，则可以判定当前的 Android 安装包为安全级别；如果提取出的指定特征进行组合后与第四条特征记录相匹配，则可以判定当前的 Android 安装包也为木马级别。

[0242] 所以，针对某个 Android 安装包的安全检测结果可以是包含安全、危险、谨慎或木马四个表示安全级别的信息，此外所述安全检测结果中还可以包括与安全级别相关的行为描述、软件描述、时间戳等至少一项提示信息，如对应“谨慎”级别的提示信息可以是“可能造成扣费，是否选择删除该应用”。

[0243] 更具体地，所述安全检测结果可以包含安全级别、行为描述信息、软件描述信息和时间戳信息。其中：

[0244] 安全级别：可以用 32 位整数表示，可表示安全、危险、谨慎或木马四个安全级别，

每个安全级别的定义如上所述。

[0245] 行为描述信息：也可以用 32 位(0 ～ 31)整数表示，可以表示出各个安全级别的软件行为描述。其中，可以选取一位表示标志位，标志位为 0 表示没有恶意行为，如果有恶意行为，则可以定义：第 1 位代表“后台偷偷下载”，第 2 位代表“私自发送短信”，第 3 位代表“包含广告”，等等。即，每一位都可以单独表示一种软件的行为描述。

[0246] 例如，对于检测为“木马级别”的 Android 应用程序，如果恶意行为 =3，翻译成二进制就是 11，第 1 位 =1，第 2 位 =1，表示的恶意行为是：同时具有后台偷偷下载和私自发送短信的行为。

[0247] 再例如，对于检测为“谨慎级别”的 Android 应用程序，如果行为描述 =4，翻译成二进制就是 100，第 1 位 =0，第 2 位 =0，第 2 位 =1，表示的行为是：包含广告。由于这个广告可能是用户允许的，也可能是用户不允许的，所以会提示用户谨慎使用，由用户自行决定是否清除。

[0248] 软件描述信息：通常表示为字符串，是对 Android 应用程序的说明，如发布者、发布时间等信息。

[0249] 时间戳信息：表明 Android 应用程序的特征信息(如正常特征、木马特征等) 是什么时候入库的。

[0250] 需要说明的是，上述主动防御功能开启检测、检测移动设备是否有山寨应用以及检测移动设备是否存在危险软件或是否有恶意广告应用的检测规则仅仅是本实施例的示例，本领域技术人员采用其他能达到检测移动设备是否存在危险软件或是否有恶意广告应用或是否存在山寨应用的目的的方法均是可以的，另外，对于其他指定检测对象的检测，本领域技术人员可以采用现有的能达到目的的任何技术进行检测，本发明对此无需加以限制。

[0251] 步骤 308，第三方应用将所述安全检测结果信息返回第一客户端程序，由所述第一客户端程序将所述安全检测结果信息通过所述 SOCKET 连接通道转发至第二客户端程序；

[0252] 具体而言，所述第三方应用执行相应的安全检测操作后，获得安全检测结果信息并返回第一客户端程序，在实际中，所述第三方应用可以通过调用所述第一客户端程序在先注册的回调函数将所述安全检测结果信息返回第一客户端程序。进一步地，第三方应用在将所述安全检测结果信息返回第一客户端程序时，可以对该安全检测结果信息标注类型标识，所述类型标识为第三方应用与第二客户端程序或与移动设备预先约定的用于标识安全检测结果信息类型的标识。

[0253] 步骤 309，所述第二客户端程序依据所述安全检测结果信息获得对应的执行建议信息；

[0254] 应用于本发明实施例，第二客户端程序接收到安全检测结果信息后，解析所述安全检测结果信息获得对应的类型标识，随后第二客户端程序在预设映射表中查找所述类型标识，获得与该类型标识对应的执行建议信息。其中，所述预设映射表中存储有每种类型标识与对应的一个或多个执行建议信息的映射关系。

[0255] 在本发明的一种优选实施例中，所述安全检测结果信息可以包括安全检测进度信息。第三方应用对应的服务在对指定检测对象进行安全检测的过程中，可以将安全检测进度信息返回第一客户端程序，由第一客户端程序通过所述 SOCKET 连接通道将安全检测进

度信息返回第二客户端程序。第二客户端程序接收到所述安全检测进度后，解析安全检测进度信息获取对应的类型标识以及安全检测进度，从预设映射表中查找所述类型标识，获得与所述安全检测进度对应的执行建议信息，其中，针对所述安全检测进度的类型标识所对应的执行建议信息可以有停止执行建议、暂停执行建议、继续执行建议等等。

[0256] 在本发明的另一种优选实施例中，所述安全检测结果信息可以包括安全检测结果，所述安全检测结果为针对指定检测对象安全检测完毕后得到的最终结果，第二客户端程序接收到所述安全检测结果后，解析安全检测结果获取对应的类型标识，从预设映射表中查找所述类型标识，获得与所述安全检测结果对应的执行建议信息，其中，针对所述安全检测结构的类型标识所对应的执行建议信息可以有移动设备挂马漏洞修复建议、开启云查杀建议、危险软件修复建议、病毒库更新建议、开启安全服务建议、山寨应用修复建议、恶意广告应用修复建议、内存优化建议、后台软件关闭建议、关闭自动启动的软件建议、垃圾数据清理建议、清理缓存建议、清理应用卸载后存在的残留文件建议、安装包清理建议、大文件整理建议、隐私痕迹清理建议。等等。

[0257] 步骤 310，所述第二客户端程序展示所述安全检测结果信息以及对应的执行建议信息；

[0258] 第二客户端程序在获得执行建议信息后，可以将所述安全检测结果信息以及其对应的执行建议信息在计算设备侧展示给用户。所述展示形式可以为以弹窗的形式进行展示，或直接在第二客户端程序的当前窗口中进行展示，展示的内容除了安全检测结果信息以及其对应的执行建议信息外，还可以包括移动设备的标识、文件路径、文件大小等等，本发明实施例对展示的形式无需加以限制。

[0259] 步骤 311，所述第二客户端程序在接收到用户针对一个或多个执行建议信息的选定指令后，依据所述选定指令生成与所述一个或多个执行建议信息对应的执行指令并发送至第一客户端程序，由第一客户端程序将所述执行指令发送至第三应用中；

[0260] 具体而言，用户可以通过选定一个或多个执行建议信息的方式来发出对安全检测结果的处理意愿，当用户选定一个或多个执行建议信息时即生成所述一个或多个执行建议信息选定指令，第二客户端程序接收到所述选定指令后，生成对应的执行指令通过所述 SOCKET 连接通道发送至第一客户端程序，由第一客户端程序发送至第三方应用中。

[0261] 例如，所述停止执行建议对应的执行指令为停止执行指令、所述暂停执行建议对应的执行指令为暂停执行指令、所述继续执行建议对应的执行指令为继续执行指令；所述移动设备挂马漏洞修复建议、开启云查杀建议、危险软件修复建议、病毒库更新建议、开启安全服务建议、山寨应用修复建议、恶意广告应用修复建议、主动防御功能开启建议、内存优化建议、后台软件关闭建议、关闭自动启动的软件建议、垃圾数据清理建议、清理缓存建议、清理应用卸载后存在的残留文件建议、安装包清理建议、大文件整理建议、隐私痕迹清理建议对应的指令分别可以为移动设备挂马漏洞修复、开启云查杀、危险软件修复、病毒库更新、开启安全服务、山寨应用修复、恶意广告应用修复、开启主动防御功能、内存优化、后台软件关闭、关闭自动启动的软件、垃圾数据清理、清理缓存、清理应用卸载后存在的残留文件、安装包清理、大文件整理、隐私痕迹清理。

[0262] 步骤 312，第三方应用执行所述执行指令。

[0263] 具体而言，所述执行指令携带有指令标识，不同的指令标识指示第三方应用执行

不同的操作，即第三方应用接收到执行指令后，依据所述指令标识执行相应的修复操作。

[0264] 例如，若第三方应用接收到的执行指令为开启主动防御功能，若移动设备上具备主动防御功能，则开启移动设备上的主动防御功能，否则，开启所述第一客户端程序的主动防御功能。具体来说，主动防御功能开启后，可以利用应用程序的名称或信息与预先定义的数据库中的信息进行比较来对所述应用程序的身份进行判断，进而采取相应的处理，其中，所述预先定义的数据库可以包含应用程序白名单、黑名单、以及特征数据。所述白名单可以包含已知的受信任的应用程序的名称（包括程序的 UID（唯一标识符）和程序的包名），所述黑名单可以包含已知的恶意应用程序的名称（包括程序的 UID（唯一标识符）和程序的包名），所述特征数据可以包含已知的恶意特征（例如广告特征）的数据。

[0265] 在利用应用程序的名称来对所述应用程序的身份进行判断时：在所述应用程序的名称包含在所述预先定义的数据库中的白名单中时，根据应用程序调用的服务的地址执行所述调用，并向所述应用程序返回实际服务结果；或者，在所述应用程序的名称包含在预先定义的数据库中的黑名单中时，向所述应用程序返回预先定义的服务结果；或者，在所述应用程序的名称未包含在预先定义的数据库中的白名单和黑名单中时，显示所述应用程序的名称和信息和所述调用的信息，并且根据在移动设备上通过操作系统对于所述调用的选择来执行处理。

[0266] 也就是说，当应用程序的名称包含在白名单中时，判定该应用程序为受信任的应用程序，允许其对于服务的调用，从而根据所述服务的地址执行调用，并向该应用程序返回实际服务结果；当应用程序的名称包含在黑名单中时，判定该应用软件为恶意应用程序，拒绝其对于服务的调用，直接向其返回虚假的服务结果，使其认为调用已经成功；而当应用程序的名称既未包含在白名单、也未包含在黑名单中时，则显示所述应用程序的名称和信息和所述调用的信息，并且根据在移动设备上通过操作系统对于所述调用的选择来执行处理。具体而言，在选择了允许所述应用程序对所述服务的调用的情况下，根据所述服务的地址执行所述调用，并向所述应用程序返回实际服务结果；或者在选择了不允许所述应用程序对所述服务的调用的情况下，向所述应用程序返回预先定义的服务结果。

[0267] 而在利用应用程序的信息来对于所述应用程序的身份进行判断时：在所述应用程序的信息包含所述预先定义的数据库中的特征数据时，向所述应用程序返回预先定义的服务结果；或者，在所述应用程序的信息不包含所述预先定义的数据库中的特征数据时，显示所述应用程序的名称和信息和所述调用的信息，并且根据在移动设备上通过操作系统对于所述调用的选择来执行处理。

[0268] 又如，当第三方应用接收到的执行指令为山寨应用修复指令，则第三方应用从服务器中匹配该山寨应用对应的官方应用安装包，并将匹配的官方应用安装包推送给用户，提示用户是否选择安装（即洗白）；当执行指令为垃圾数据清理指令时，则第三方应用清理移动设备侧安全检测得到的垃圾数据；若所述执行指令为关闭后台软件或自动启动的软件时，则第三方应用关闭所述后台软件或自动启动的软件。

[0269] 需要说明的是，本发明实施例中在计算设备上对移动设备进行安全检测，是指在计算设备上对接入的移动设备进行安全检测，具体的检测操作以及执行操作是安全在移动设备上的安全类检测应用进行的，与在计算设备侧对 u 盘的安全检测并不相同。

[0270] 本发明实施例通过在计算设备上对移动设备进行安全检测，可以拦截恶意应用偷

窥移动设备用户的隐私信息(包括联系人信息、通话记录、短信、彩信、各种账户及密码等)的行为,防止恶意应用拨打扣费电话、发送扣费短信、访问耗费网络流量的网站,防止恶意应用安装木马和病毒程序,防止恶意应用记录用户的 GPS 或网络定位,拦截恶意应用弹出骚扰广告信息等等,可以对于任何恶意应用对于服务的调用进行拦截,从而提高了移动设备的安全性。

[0271] 此外,本发明实施例通过在计算设备上对移动设备进行安全检测,还可以在检测到有后台软件或自动启动的软件时,可以关闭所述后台软件或自动启动的软件,从而节省移动设备的网络流量;通过对移动设备进行内存优化、垃圾清理等可以提高移动设备的性能。

[0272] 参照图 4,示出了本发明的一种对设备进行安全检测的方法实施例四的步骤流程图,本实施例以安装有安卓操作系统的移动设备为例,当然,本发明并不限于安装有安卓系统的移动设备,本发明的原理同样适用于安装有其他操作系统的移动设备。

[0273] 在本发明实施例中,若第三方应用中的服务中内嵌有第一客户端程序的服务时,则可以通过第三方应用直接与计算设备的第二客户端程序进行通信,所述方法可以包括如下步骤:

[0274] 步骤 401,当移动设备连接至计算设备时,第二客户端程序检测所述移动设备是否安装有第三方应用,若否,则执行步骤 402,若是,则执行步骤 404;

[0275] 步骤 402,第二客户端程序下载所述第三方应用安装包发送至移动设备侧;

[0276] 步骤 403,移动设备侧依据所述第三方应用安装包安装第三方应用,继续执行步骤 404;

[0277] 应用于本发明实施例,所述第三方应用可以为安全安全检测类服务应用,如 360 手机卫士,金山卫士等等,本发明实施例对第三方应用的具体类型无需加以限制。

[0278] 步骤 404,建立所述移动设备与所述计算设备的 SOCKET 连接通道;

[0279] 步骤 405,所述第二客户端程序 SOCKET 连接通道向所述第三方应用发出对移动设备的安全检测请求,所述安全检测请求包括指定检测对象;

[0280] 作为本实施例的一种优选示例,所述安全检测请求可以包括指定检测对象,所述指定检测对象为针对移动设备进行安全检测的项目,可以包括针对移动设备的如下服务的一项或多项:移动设备挂马漏洞检测、检测是否开启云查杀、检测是否存在危险软件、检测是否更新过病毒库、检测安全服务是否开启、检测移动设备是否有山寨应用、检测移动设备上是否有恶意广告应用、主动防御功能开启检测、内存优化检测、检测是否存在后台软件、自动启动的软件检测、垃圾数据清理检测、清理缓存检测、清理应用卸载后存在的残留文件检测、安装包清理检测、大文件整理、隐私痕迹清理检测,等等。

[0281] 步骤 406,所述第三方应用对所述指定检测对象执行对应的安全检测操作,获得安全检测结果信息;

[0282] 步骤 407,第三方应用将所述安全检测结果信息返回第二客户端程序;

[0283] 步骤 408,所述第二客户端程序依据所述安全检测结果信息获得对应的执行建议信息;

[0284] 步骤 409,所述第二客户端程序展示所述安全检测结果信息以及对应的执行建议信息;

[0285] 步骤 410，所述第二客户端程序在接收到用户针对一个或多个执行建议信息的选定指令后，依据所述选定指令生成与所述一个或多个执行建议信息对应的执行指令并发送至第三应用中；

[0286] 在本发明的一种优选实施例中，所述安全检测结果信息可以包括安全检测进度信息，相应的，所述执行指令可以包括停止指令、暂停指令、继续执行指令。

[0287] 在本发明的另一种优选实施例中，所述安全检测结果信息包括安全检测结果，相应地，所述执行指令可以包括以下的一项或多项：移动设备挂马漏洞修复、开启云查杀、危险软件修复、病毒库更新、开启安全服务、山寨应用修复、恶意广告应用修复、开启主动防御功能、内存优化、后台软件关闭、关闭自动启动的软件、垃圾数据清理、清理缓存、清理应用卸载后存在的残留文件、安装包清理、大文件整理、隐私痕迹清理。

[0288] 步骤 411，第三方应用执行所述执行指令。

[0289] 对于图 4 的方法实施例而言，由于其与上述图 3 方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0290] 对于方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本发明并不受所描述的动作顺序的限制，因为依据本发明，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模块并不一定是本发明所必须的。

[0291] 参照图 5，示出了本发明的一种对设备进行安全检测的装置实施例一的结构框图，所述的装置可以包括如下模块：

[0292] 安全检测请求接收模块 501，适于在移动设备连接至计算设备时，在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求，所述安全检测请求包括指定检测对象；

[0293] 安全检测结果信息发送模块 502，适于在所述移动设备侧获取与所述指定检测对象对应的安全检测结果信息，并将所述安全检测结果信息发送至计算设备侧；

[0294] 执行指令接收模块 503，适于在所述移动设备侧接收计算设备侧发送的执行指令，所述执行指令为计算设备依据所述安全检测结果信息生成；

[0295] 执行指令执行模块 504，适于在所述移动设备侧执行所述执行指令。

[0296] 在本发明的一种优选实施例中，所述装置还可以包括：

[0297] 安装包接收模块，适于在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求的之前，所述移动设备侧接收所述计算设备侧发送的第三方应用安装包，所述第三方应用安装包为所述计算设备侧在检测到所述移动设备侧没有安装第三方应用时，从服务器中下载得到；

[0298] 安装包安装模块，适于所述移动设备侧依据所述第三方应用安装包安装第三方应用。

[0299] 在本发明的一种优选实施例中，所述装置还可以包括：

[0300] 通道建立模块，适于在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求之前，建立所述移动设备与所述计算设备的 SOCKET 连接通道，所述移动设备通过所述 SOCKET 连接通道接收安全检测请求、以及发送安全检测结果信息、以及接收执行指令。

[0301] 在本发明的一种优选实施例中，所述安全检测请求接收模块 501 还适于：

[0302] 在所述移动设备侧采用所述第三方应用接收所述计算设备侧发出的对移动设备的安全检测请求；

[0303] 所述安全检测结果信息发送模块 502 还适于：

[0304] 在所述移动设备侧采用所述第三方应用依据所述安全检测请求执行对指定检测对象的安全检测操作，获得安全检测结果信息；

[0305] 由所述第三方应用将所述安全检测结果信息返回至所述计算设备侧；

[0306] 所述执行指令接收模块 503 还适于：

[0307] 在所述移动设备侧采用所述第三方应用接收计算设备侧发送的执行指令；

[0308] 所述执行指令执行模块 504 还适于：

[0309] 在所述移动设备侧采用所述第三方应用执行所述执行指令。

[0310] 在本发明的另一种优选实施例中，所述移动设备侧安装有第一客户端程序，所述安全检测请求接收模块 501 还适于：

[0311] 在所述移动设备侧采用所述第一客户端程序接收所述计算设备侧发出的对移动设备的安全检测请求；

[0312] 所述安全检测结果信息发送模块 502 还适于：

[0313] 在所述移动设备侧采用所述第一客户端程序将所述安全检测请求发送至所述第三方应用，由所述第三方应用依据所述安全检测请求执行对指定检测对象的安全检测操作，获得安全检测结果信息并返回第一客户端程序中；

[0314] 所述第一客户端程序将所述安全检测结果信息返回至所述计算设备侧；

[0315] 所述执行指令接收模块 503 还适于：

[0316] 在所述移动设备侧采用所述第一客户端程序接收计算设备侧发送的执行指令；

[0317] 所述执行指令执行模块 504 还适于：

[0318] 在所述移动设备侧采用所述第一客户端程序将所述执行指令发送至第三方应用，由所述第三方应用执行所述执行指令。

[0319] 在本发明的一种优选实施例中，所述第一客户端程序将所述安全检测请求发送至所述第三方应用，具体为：

[0320] 所述第一客户端程序依据所述指定检测对象调用所述第三方应用的服务的接口，将所述安全检测请求发送至所述第三方应用。

[0321] 作为本发明实施例的一种优选示例，所述指定检测对象可以包括针对移动设备的如下服务的一项或多项：移动设备挂马漏洞检测、检测是否开启云查杀、检测是否存在危险软件、检测是否更新过病毒库、检测安全服务是否开启、检测移动设备是否有山寨应用、检测移动设备上是否有恶意广告应用、主动防御功能开启检测、内存优化检测、检测是否存在后台软件、自动启动的软件检测、垃圾数据清理检测、清理缓存检测、清理应用卸载后存在的残留文件检测、安装包清理检测、大文件整理、隐私痕迹清理检测。

[0322] 作为本发明实施例的一种优选示例，所述安全检测结果信息包括安全检测进度信息，相应地，所述执行指令包括停止指令、暂停指令、继续执行指令。

[0323] 作为本发明实施例的另一种优选示例，所述安全检测结果信息包括安全检测结果，相应地，所述执行指令包括以下的一项或多项：移动设备挂马漏洞修复、开启云查杀、危

险软件修复、病毒库更新、开启安全服务、山寨应用修复、恶意广告应用修复、开启主动防御功能、内存优化、后台软件关闭、关闭自动启动的软件、垃圾数据清理、清理缓存、清理应用卸载后存在的残留文件、安装包清理、大文件整理、隐私痕迹清理。

[0324] 对于图 5 的装置实施例而言，由于其与上述方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0325] 参照图 6，示出了本发明的一种对设备进行安全检测的装置实施例二的结构框图，所述的装置可以包括如下模块：

[0326] 安全检测请求发送模块 601，适于在计算设备侧安全检测到有移动设备接入时，在计算设备侧向所述移动设备侧发出对移动设备的安全检测请求，所述安全检测请求包括指定检测对象；

[0327] 安全检测结果信息接收模块 602，适于在所述计算设备侧接收所述移动设备侧返回的针对所述安全检测请求的安全检测结果信息，所述安全检测结果信息由所述移动设备侧依据所述指定检测对象获得；

[0328] 执行指令发送模块 603，适于在计算设备侧依据所述安全检测结果信息生成对应的执行指令并发送至所述移动设备侧，由所述移动设备侧执行所述执行指令。

[0329] 在本发明的一种优选实施例中，所述装置还可以包括：

[0330] 安装包信息获取模块，适于在所述计算设备侧向所述移动设备侧发出对移动设备的安全检测请求之前，在计算设备侧读取所述移动设备侧中所有已安装应用的安装包信息，所述安装包信息包括安装包标识；

[0331] 查找模块，适于在计算设备侧判断所述安装包标识中不存在第三方应用安装包标识时，从服务器中获取所述第三方应用安装包的下载地址；

[0332] 安装包发送模块，适于在计算设备侧依据所述第三方应用安装包的下载地址下载所述第三方应用安装包并发送至移动设备侧。

[0333] 在本发明的一种优选实施例中，所述装置还可以包括：

[0334] 连接通道建立模块，适于在所述计算设备侧向所述移动设备侧发出对移动设备的安全检测请求之前，建立所述移动设备与所述计算设备的 SOCKET 连接通道，所述计算设备通过所述连接通道发送安全检测请求、以及接收安全检测结果信息、以及发送执行指令。

[0335] 在本发明的一种优选实施例中，所述安全检测结果信息具有类型标识的信息，所述执行指令发送模块 603 还适于：

[0336] 计算设备侧在预设映射表中查找所述类型标识对应的执行建议信息，所述预设映射表中存储有计算设备与移动设备预先约定的类型标识与执行建议信息的映射关系；

[0337] 在计算设备侧展示所述安全检测结果信息以及对应的执行建议信息；

[0338] 在计算设备侧接收用户对所述一个或多个执行建议信息的选定指令；

[0339] 依据所述选定指令生成一个或多个执行建议信息对应的执行指令并发送至移动设备侧。

[0340] 作为本发明实施例的一种优选示例，所述指定检测对象可以包括针对移动设备的如下服务的一项或多项：移动设备挂马漏洞检测、检测是否开启云查杀、检测是否存在危险软件、检测是否更新过病毒库、检测安全服务是否开启、检测移动设备是否有山寨应用、检测移动设备上是否有恶意广告应用、主动防御功能开启检测、内存优化检测、检测是否存在

后台软件、自动启动的软件检测、垃圾数据清理检测、清理缓存检测、清理应用卸载后存在的残留文件检测、安装包清理检测、大文件整理、隐私痕迹清理检测。

[0341] 在本发明的一种优选实施例中，所述安全检测结果信息可以包括安全检测进度信息，相应地，所述执行指令包括停止指令、暂停指令、继续执行指令。

[0342] 在本发明的另一种优选实施例中，所述安全检测结果信息包括安全检测结果，相应地，所述执行指令包括以下的一项或多项：移动设备挂马漏洞修复、开启云查杀、危险软件修复、病毒库更新、开启安全服务、山寨应用修复、恶意广告应用修复、开启主动防御功能、内存优化、后台软件关闭、关闭自动启动的软件、垃圾数据清理、清理缓存、清理应用卸载后存在的残留文件、安装包清理、大文件整理、隐私痕迹清理。对于图 6 的装置实施例而言，由于其与上述方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0343] 在此提供的算法和显示不与任何特定计算设备、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。

[0344] 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。

[0345] 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。

[0346] 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、等同或相似目的替代特征来代替。

[0347] 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。

[0348] 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对设备进行安全检测设备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，计算设备程序和计算设备程序产品）。这样的实现本发明的程序可以存储在计算设备可读介质上，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。

[0349] 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设备来实现。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。

[0350] 本发明的实施例公开了 A1、一种对设备进行安全检测的方法，包括：

[0351] 当移动设备连接至计算设备时，在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求，所述安全检测请求中包括指定检测对象；

[0352] 在所述移动设备侧获取与所述指定检测对象对应的安全检测结果信息，并将所述安全检测结果信息发送至计算设备侧；

[0353] 在所述移动设备侧接收计算设备侧发送的执行指令，所述执行指令为计算设备依据所述安全检测结果信息生成；

[0354] 在所述移动设备侧执行所述执行指令。

[0355] A2、如 A1 所述的方法，在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求的步骤之前，还包括：

[0356] 所述移动设备侧接收所述计算设备侧发送的第三方应用安装包，所述第三方应用安装包为所述计算设备侧在检测到所述移动设备侧没有安装第三方应用时，从服务器中下载得到；

[0357] 所述移动设备侧依据所述第三方应用安装包安装第三方应用。

[0358] A3、如 A1 或 A2 所述的方法，在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求的步骤之前，还包括：

[0359] 建立所述移动设备与所述计算设备的 SOCKET 连接通道，所述移动设备通过所述 SOCKET 连接通道接收安全检测请求、以及发送安全检测结果信息、以及接收执行指令。

[0360] A4、如 A2 所述的方法，所述在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求的步骤为：

[0361] 在所述移动设备侧采用所述第三方应用接收所述计算设备侧发出的对移动设备的安全检测请求；

[0362] 所述在所述移动设备侧获取与所述指定检测对象对应的安全检测结果信息，并将所述安全检测结果信息发送至计算设备侧的步骤包括：

[0363] 在所述移动设备侧采用所述第三方应用依据所述安全检测请求执行对指定检测对象的安全检测操作，获得安全检测结果信息；

[0364] 由所述第三方应用将所述安全检测结果信息返回至所述计算设备侧；

[0365] 所述在所述移动设备侧接收计算设备侧发送的执行指令的步骤为：

[0366] 在所述移动设备侧采用所述第三方应用接收计算设备侧发送的执行指令；

[0367] 所述在所述移动设备侧执行所述执行指令的步骤为：

[0368] 在所述移动设备侧采用所述第三方应用执行所述执行指令。

[0369] A5、如 A2 所述的方法，所述移动设备侧安装有第一客户端程序，所述在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求的步骤为：

[0370] 在所述移动设备侧采用所述第一客户端程序接收所述计算设备侧发出的对移动设备的安全检测请求；

[0371] 所述在所述移动设备侧获取与所述指定检测对象对应的安全检测结果信息，并将所述安全检测结果信息发送至计算设备侧的步骤包括：

[0372] 在所述移动设备侧采用所述第一客户端程序将所述安全检测请求发送至所述第三方应用，由所述第三方医用依据所述安全检测请求执行对指定检测对象的安全检测操作，获得安全检测结果信息并返回第一客户端程序中；

[0373] 所述第一客户端程序将所述安全检测结果信息返回至所述计算设备侧；

[0374] 所述在所述移动设备侧接收计算设备侧发送的执行指令的步骤为：

[0375] 在所述移动设备侧采用所述第一客户端程序接收计算设备侧发送的执行指令；

[0376] 所述在所述移动设备侧执行所述执行指令的步骤为：

[0377] 在所述移动设备侧采用所述第一客户端程序将所述执行指令发送至第三方应用，由所述第三方应用执行所述执行指令。

[0378] A6、如 A5 所述的方法，所述第一客户端程序将所述安全检测请求发送至所述第三方应用的步骤包括：

[0379] 所述第一客户端程序依据所述指定检测对象调用所述第三方应用的服务的接口，将所述安全检测请求发送至所述第三方应用。

[0380] A7、如 A1 所述的方法，所述指定检测对象包括针对移动设备的如下服务的一项或多项：移动设备挂马漏洞检测、检测是否开启云查杀、检测是否存在危险软件、检测是否更新过病毒库、检测安全服务是否开启、检测移动设备是否有山寨应用、检测移动设备上是否有恶意广告应用、主动防御功能开启检测。

[0381] A8、如 A1 所述的方法，所述指定检测对象包括针对移动设备的如下服务的一项或多项：内存优化检测、检测是否存在后台软件、自动启动的软件检测、垃圾数据清理检测、清理缓存检测、清理应用卸载后存在的残留文件检测、安装包清理检测、大文件整理、隐私痕迹清理检测。

[0382] A9、如 A7 或 A8 所述的方法，所述安全检测结果信息包括安全检测进度信息，相应地，所述执行指令包括停止指令、暂停指令、继续执行指令。

[0383] A10、如 A7 所述的方法，所述安全检测结果信息包括安全检测结果，相应地，所述执行指令包括以下的一项或多项：移动设备挂马漏洞修复、开启云查杀、危险软件修复、病毒库更新、开启安全服务、山寨应用修复、恶意广告应用修复、开启主动防御功能。

[0384] A11、如 A8 所述的方法，所述安全检测结果信息包括安全检测结果，相应地，所述执行指令包括以下的一项或多项：内存优化、后台软件关闭、关闭自动启动的软件、垃圾数据清理、清理缓存、清理应用卸载后存在的残留文件、安装包清理、大文件整理、隐私痕迹清理。

[0385] 本发明的实施例还公开了 B12、一种对设备进行安全检测的方法，包括：

[0386] 当计算设备侧安全检测到有移动设备接入时，在计算设备侧向所述移动设备侧发出对移动设备的安全检测请求，所述安全检测请求包括指定检测对象；

[0387] 在所述计算设备侧接收所述移动设备侧返回的针对所述安全检测请求的安全检测结果信息，所述安全检测结果信息由所述移动设备侧依据所述指定检测对象获得；

[0388] 在计算设备侧依据所述安全检测结果信息生成对应的执行指令并发送至所述移动设备侧，由所述移动设备侧执行所述执行指令。

[0389] B13、如 B12 所述的方法，在所述计算设备侧向所述移动设备侧发出对移动设备的安全检测请求的步骤之前，还包括：

[0390] 在计算设备侧读取所述移动设备侧中所有已安装应用的安装包信息，所述安装包信息包括安装包标识；

[0391] 在计算设备侧判断所述安装包标识中不存在第三方应用安装包标识时，从服务器中获取所述第三方应用安装包的下载地址；

[0392] 在计算设备侧依据所述第三方应用安装包的下载地址下载所述第三方应用安装包并发送至移动设备侧。

[0393] B14、如 B12 或 13 所述的方法，在所述计算设备侧向所述移动设备侧发出对移动设备的安全检测请求的步骤之前，还包括：

[0394] 建立所述移动设备与所述计算设备的 SOCKET 连接通道，所述计算设备通过所述连接通道发送安全检测请求、以及接收安全检测结果信息、以及发送执行指令。

[0395] B15、如 B12 所述的方法，所述安全检测结果信息具有类型标识的信息，所述在计算设备侧依据所述安全检测结果信息生成对应的执行指令并发送至所述移动设备侧的步骤包括：

[0396] 计算设备侧在预设映射表中查找所述类型标识对应的执行建议信息，所述预设映射表中存储有计算设备与移动设备预先约定的类型标识与执行建议信息的映射关系；

[0397] 在计算设备侧展示所述安全检测结果信息以及对应的执行建议信息；

[0398] 在计算设备侧接收用户对所述一个或多个执行建议信息的选定指令；

[0399] 依据所述选定指令生成一个或多个执行建议信息对应的执行指令并发送至移动设备侧。

[0400] B16、如 B12 所述的方法，所述指定检测对象包括针对移动设备的如下服务的一项或多项：移动设备挂马漏洞检测、检测是否开启云查杀、检测是否存在危险软件、检测是否更新过病毒库、检测安全服务是否开启、检测移动设备是否有山寨应用、检测移动设备上是否有恶意广告应用、主动防御功能开启检测。

[0401] B17、如 B12 所述的方法，所述指定检测对象包括针对移动设备的如下服务的一项或多项：内存优化检测、检测是否存在后台软件、自动启动的软件检测、垃圾数据清理检测、清理缓存检测、清理应用卸载后存在的残留文件检测、安装包清理检测、大文件整理、隐私

痕迹清理检测。

[0402] B18、如 B16 或 B17 所述的方法，所述安全检测结果信息包括安全检测进度信息，相应地，所述执行指令包括停止指令、暂停指令、继续执行指令。

[0403] B19、如 B16 所述的方法，所述安全检测结果信息包括安全检测结果，相应地，所述执行指令包括以下的一项或多项：移动设备挂马漏洞修复、开启云查杀、危险软件修复、病毒库更新、开启安全服务、山寨应用修复、恶意广告应用修复、开启主动防御功能。

[0404] B20、如 B17 所述的方法，所述安全检测结果信息包括安全检测结果，相应地，所述执行指令包括以下的一项或多项：内存优化、后台软件关闭、关闭自动启动的软件、垃圾数据清理、清理缓存、清理应用卸载后存在的残留文件、安装包清理、大文件整理、隐私痕迹清理。

[0405] 本发明的实施例还公开了 21、一种对设备进行安全检测的装置，包括：

[0406] 本发明的实施例还公开了 C21、一种对设备进行安全检测的装置，包括：

[0407] 安全检测请求接收模块，适于在移动设备连接至计算设备时，在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求，所述安全检测请求包括指定检测对象；

[0408] 安全检测结果信息发送模块，适于在所述移动设备侧获取与所述指定检测对象对应的安全检测结果信息，并将所述安全检测结果信息发送至计算设备侧；

[0409] 执行指令接收模块，适于在所述移动设备侧接收计算设备侧发送的执行指令，所述执行指令为计算设备依据所述安全检测结果信息生成；

[0410] 执行指令执行模块，适于在所述移动设备侧执行所述执行指令。

[0411] C22、如 C21 所述的装置，还包括：

[0412] 安装包接收模块，适于在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求的之前，所述移动设备侧接收所述计算设备侧发送的第三方应用安装包，所述第三方应用安装包为所述计算设备侧在检测到所述移动设备侧没有安装第三方应用时，从服务器中下载得到；

[0413] 安装包安装模块，适于所述移动设备侧依据所述第三方应用安装包安装第三方应用。

[0414] C23、如 C21 或 C22 所述的装置，还包括：

[0415] 通道建立模块，适于在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求之前，建立所述移动设备与所述计算设备的 SOCKET 连接通道，所述移动设备通过所述 SOCKET 连接通道接收安全检测请求、以及发送安全检测结果信息、以及接收执行指令。

[0416] C24、如 C22 所述的装置，所述安全检测请求接收模块还适于：

[0417] 在所述移动设备侧采用所述第三方应用接收所述计算设备侧发出的对移动设备的安全检测请求；

[0418] 所述安全检测结果信息发送模块还适于：

[0419] 在所述移动设备侧采用所述第三方应用依据所述安全检测请求执行对指定检测对象的安全检测操作，获得安全检测结果信息；

[0420] 由所述第三方应用将所述安全检测结果信息返回至所述计算设备侧；

[0421] 所述执行指令接收模块还适于：

[0422] 在所述移动设备侧采用所述第三方应用接收计算设备侧发送的执行指令；

[0423] 所述执行指令执行模块还适于：

[0424] 在所述移动设备侧采用所述第三方应用执行所述执行指令。

[0425] C25、如 C22 所述的装置，所述安全检测请求接收模块还适于：

[0426] 在所述移动设备侧采用所述第一客户端程序接收所述计算设备侧发出的对移动设备的安全检测请求；

[0427] 所述安全检测结果信息发送模块还适于：

[0428] 在所述移动设备侧采用所述第一客户端程序将所述安全检测请求发送至所述第三方应用，由所述第三方医用依据所述安全检测请求执行对指定检测对象的安全检测操作，获得安全检测结果信息并返回第一客户端程序中；

[0429] 所述第一客户端程序将所述安全检测结果信息返回至所述计算设备侧；

[0430] 所述执行指令接收模块还适于：

[0431] 在所述移动设备侧采用所述第一客户端程序接收计算设备侧发送的执行指令；

[0432] 所述执行指令执行模块还适于：

[0433] 在所述移动设备侧采用所述第一客户端程序将所述执行指令发送至第三方应用，由所述第三方应用执行所述执行指令。

[0434] C26、如 C25 所述的装置，所述第一客户端程序将所述安全检测请求发送至所述第三方应用，具体为：

[0435] 所述第一客户端程序依据所述指定检测对象调用所述第三方应用的服务的接口，将所述安全检测请求发送至所述第三方应用。

[0436] C27、如 C21 所述的装置，所述指定检测对象包括针对移动设备的如下服务的一项或多项：移动设备挂马漏洞检测、检测是否开启云查杀、检测是否存在危险软件、检测是否更新过病毒库、检测安全服务是否开启、检测移动设备是否有山寨应用、检测移动设备上是否有恶意广告应用、主动防御功能开启检测。

[0437] C28、如 C21 所述的装置，所述指定检测对象包括针对移动设备的如下服务的一项或多项：内存优化检测、检测是否存在后台软件、自动启动的软件检测、垃圾数据清理检测、清理缓存检测、清理应用卸载后存在的残留文件检测、安装包清理检测、大文件整理、隐私痕迹清理检测。

[0438] C29、如 C27 或 C28 所述的装置，所述安全检测结果信息包括安全检测进度信息，相应地，所述执行指令包括停止指令、暂停指令、继续执行指令。

[0439] C30、如 C27 所述的装置，所述安全检测结果信息包括安全检测结果，相应地，所述执行指令包括以下的一项或多项：移动设备挂马漏洞修复、开启云查杀、危险软件修复、病毒库更新、开启安全服务、山寨应用修复、恶意广告应用修复、开启主动防御功能。

[0440] C31、如 C28 所述的装置，所述安全检测结果信息包括安全检测结果，相应地，所述执行指令包括以下的一项或多项：内存优化、后台软件关闭、关闭自动启动的软件、垃圾数据清理、清理缓存、清理应用卸载后存在的残留文件、安装包清理、大文件整理、隐私痕迹清理。

[0441] 本发明的实施例还公开了 D32、一种对设备进行安全检测的装置，包括：

[0442] 安全检测请求发送模块，适于在计算设备侧安全检测到有移动设备接入时，在计算设备侧向所述移动设备侧发出对移动设备的安全检测请求，所述安全检测请求包括指定检测对象；

[0443] 安全检测结果信息接收模块，适于在所述计算设备侧接收所述移动设备侧返回的针对所述安全检测请求的安全检测结果信息，所述安全检测结果信息由所述移动设备侧依据所述指定检测对象获得；

[0444] 执行指令发送模块，适于在计算设备侧依据所述安全检测结果信息生成对应的执行指令并发送至所述移动设备侧，由所述移动设备侧执行所述执行指令。

[0445] D33、如 D32 所述的装置，还包括：

[0446] 安装包信息获取模块，适于在所述计算设备侧向所述移动设备侧发出对移动设备的安全检测请求之前，在计算设备侧读取所述移动设备侧中所有已安装应用的安装包信息，所述安装包信息包括安装包标识；

[0447] 查找模块，适于在计算设备侧判断所述安装包标识中不存在第三方应用安装包标识时，从服务器中获取所述第三方应用安装包的下载地址；

[0448] 安装包发送模块，适于在计算设备侧依据所述第三方应用安装包的下载地址下载所述第三方应用安装包并发送至移动设备侧。

[0449] D34、如 D32 或 D33 所述的装置，还包括：

[0450] 连接通道建立模块，适于在所述计算设备侧向所述移动设备侧发出对移动设备的安全检测请求之前，建立所述移动设备与所述计算设备的 SOCKET 连接通道，所述计算设备通过所述连接通道发送安全检测请求、以及接收安全检测结果信息、以及发送执行指令。

[0451] D35、如 D32 所述的装置，所述安全检测结果信息具有类型标识的信息，所述执行指令发送模块还适于：

[0452] 计算设备侧在预设映射表中查找所述类型标识对应的执行建议信息，所述预设映射表中存储有计算设备与移动设备预先约定的类型标识与执行建议信息的映射关系；

[0453] 在计算设备侧展示所述安全检测结果信息以及对应的执行建议信息；

[0454] 在计算设备侧接收用户对所述一个或多个执行建议信息的选定指令；

[0455] 依据所述选定指令生成一个或多个执行建议信息对应的执行指令并发送至移动设备侧。

[0456] D36、如 D32 所述的装置，所述指定检测对象包括针对移动设备的如下服务的一项或多项：移动设备挂马漏洞检测、检测是否开启云查杀、检测是否存在危险软件、检测是否更新过病毒库、检测安全服务是否开启、检测移动设备是否有山寨应用、检测移动设备上是否有恶意广告应用、主动防御功能开启检测。

[0457] D37、如 D32 所述的装置，所述指定检测对象包括针对移动设备的如下服务的一项或多项：内存优化检测、检测是否存在后台软件、自动启动的软件检测、垃圾数据清理检测、清理缓存检测、清理应用卸载后存在的残留文件检测、安装包清理检测、大文件整理、隐私痕迹清理检测。

[0458] D38、如 D36 或 D37 所述的装置，所述安全检测结果信息包括安全检测进度信息，相应地，所述执行指令包括停止指令、暂停指令、继续执行指令。

[0459] D39、如 D36 所述的装置，所述安全检测结果信息包括安全检测结果，相应地，所述

执行指令包括以下的一项或多项：移动设备挂马漏洞修复、开启云查杀、危险软件修复、病毒库更新、开启安全服务、山寨应用修复、恶意广告应用修复、开启主动防御功能。

[0460] D40、如 D37 所述的装置，所述安全检测结果信息包括安全检测结果，相应地，所述执行指令包括以下的一项或多项：内存优化、后台软件关闭、关闭自动启动的软件、垃圾数据清理、清理缓存、清理应用卸载后存在的残留文件、安装包清理、大文件整理、隐私痕迹清理。

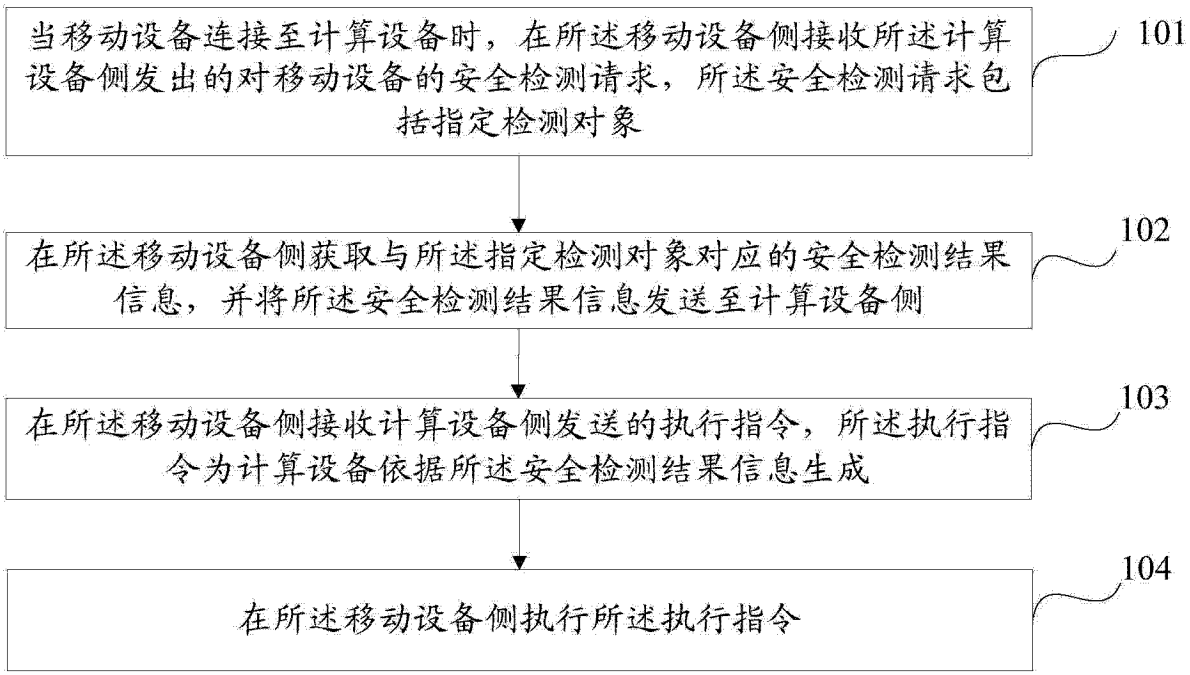

当移动设备连接至计算设备时，在所述移动设备侧接收所述计算设备侧发出的对移动设备的安全检测请求，所述安全检测请求包括指定检测对象
101
在所述移动设备侧获取与所述指定检测对象对应的安全检测结果信息，并将所述安全检测结果信息发送至计算设备侧
102
在所述移动设备侧接收计算设备侧发送的执行指令，所述执行指令为计算设备依据所述安全检测结果信息生成
103
在所述移动设备侧执行所述执行指令
104

图 1

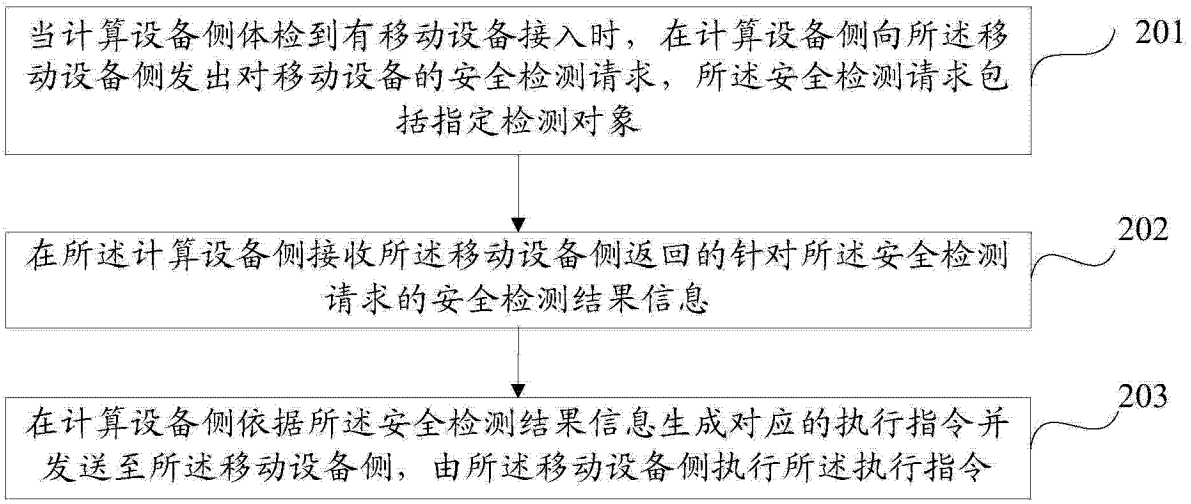

当计算设备侧体检到有移动设备接入时，在计算设备侧向所述移动设备侧发出对移动设备的安全检测请求，所述安全检测请求包括指定检测对象
201
在所述计算设备侧接收所述移动设备侧返回的针对所述安全检测请求的安全检测结果信息
202
在计算设备侧依据所述安全检测结果信息生成对应的执行指令并发送至所述移动设备侧，由所述移动设备侧执行所述执行指令
203

图 2

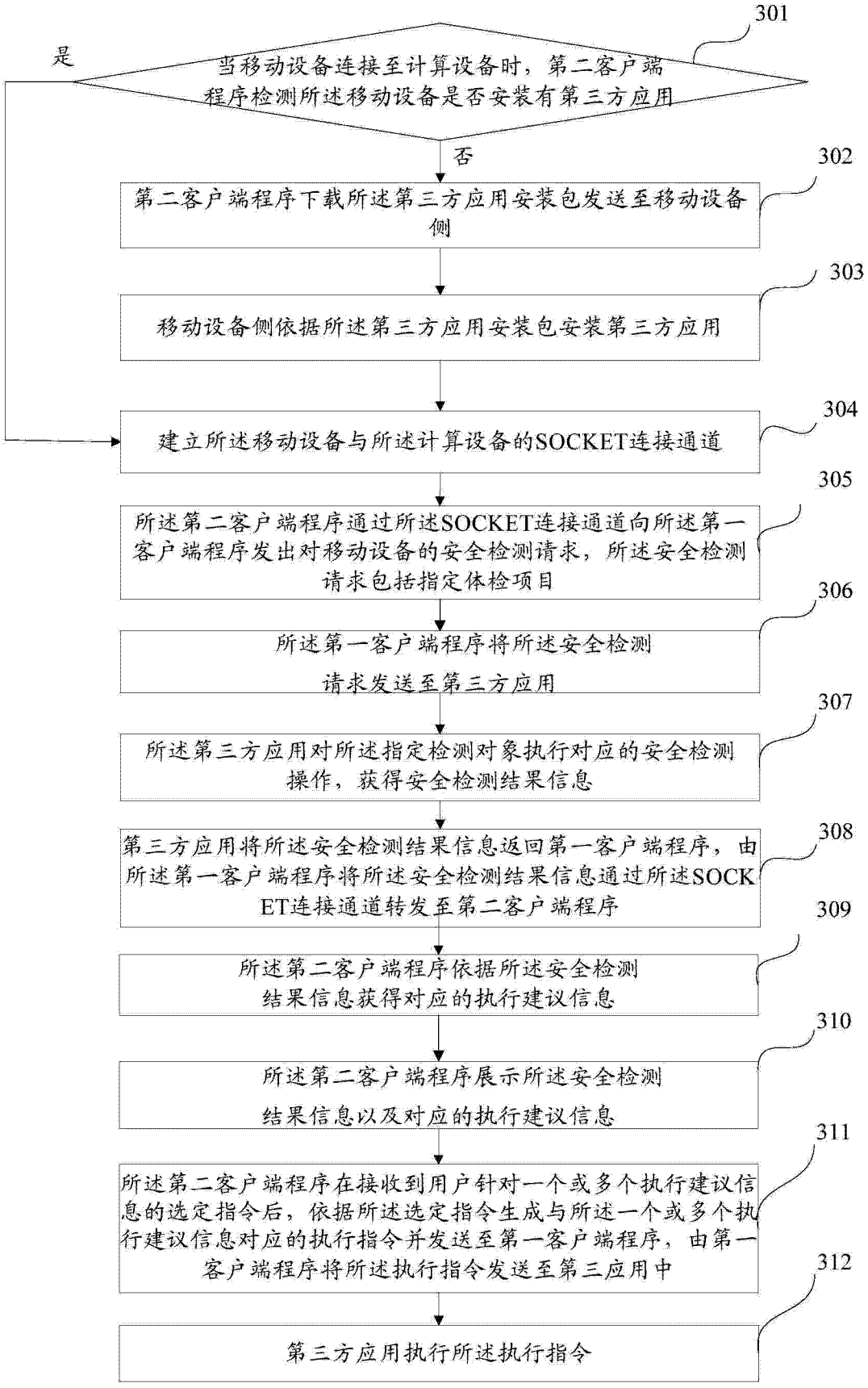

301
是
当移动设备连接至计算设备时，第二客户端程序检测所述移动设备是否安装有第三方应用
否
302
第二客户端程序下载所述第三方应用安装包发送至移动设备侧
303
移动设备侧依据所述第三方应用安装包安装第三方应用
304
建立所述移动设备与所述计算设备的SOCKET连接通道
305
所述第二客户端程序通过所述SOCKET连接通道向所述第一客户端程序发出对移动设备的安全检测请求，所述安全检测请求包括指定体检项目
306
所述第一客户端程序将所述安全检测请求发送至第三方应用
307
所述第三方应用对所述指定检测对象执行对应的安全检测操作，获得安全检测结果信息
308
第三方应用将所述安全检测结果信息返回第一客户端程序，由所述第一客户端程序将所述安全检测结果信息通过所述SOCKET连接通道转发至第二客户端程序
309
所述第二客户端程序依据所述安全检测结果信息获得对应的执行建议信息
310
所述第二客户端程序展示所述安全检测结果信息以及对应的执行建议信息
311
所述第二客户端程序在接收到用户针对一个或多个执行建议信息的选定指令后，依据所述选定指令生成与所述一个或多个执行建议信息对应的执行指令并发送至第一客户端程序，由第一客户端程序将所述执行指令发送至第三应用中
312
第三方应用执行所述执行指令

图 3

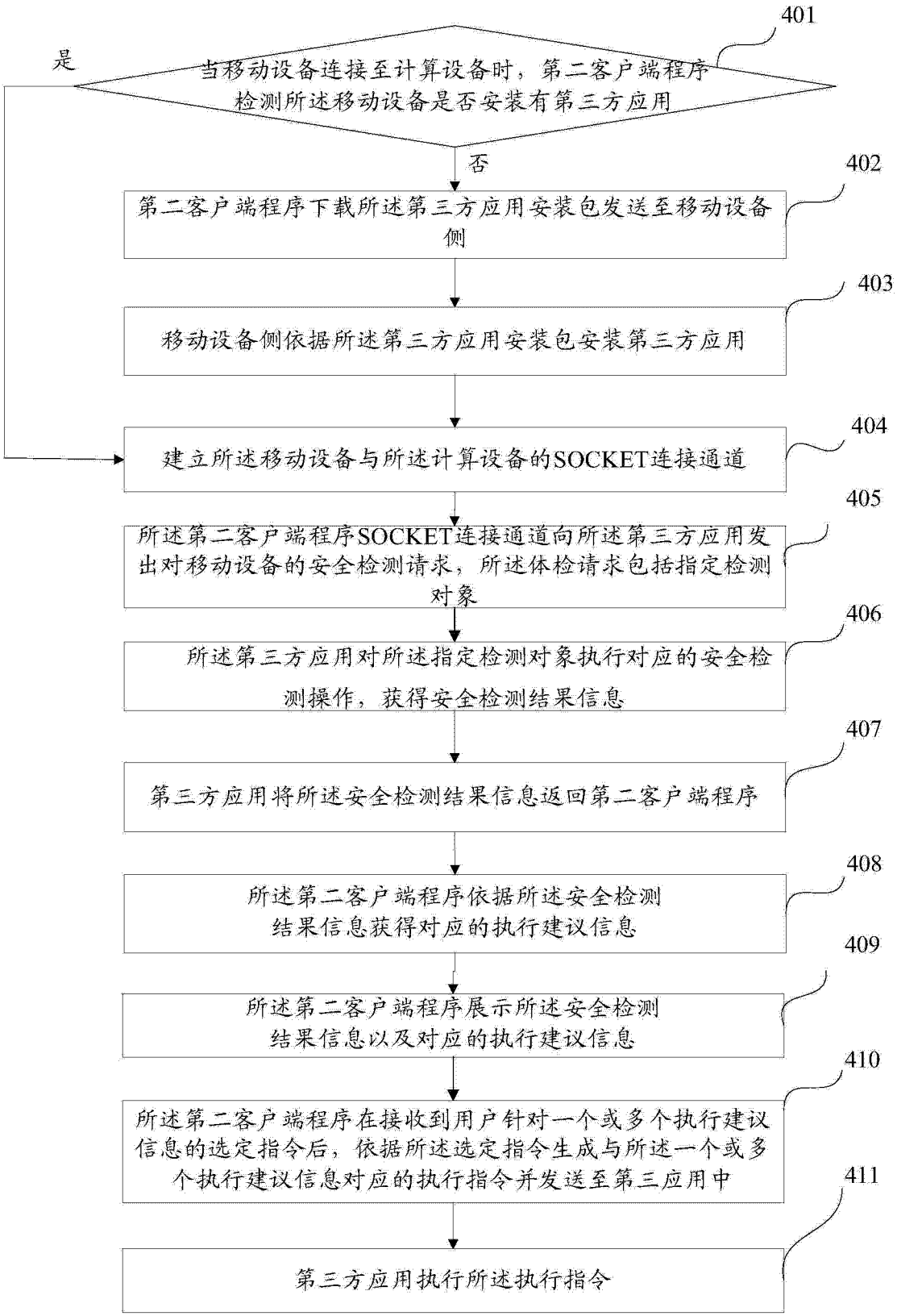

401
是
当移动设备连接至计算设备时，第二客户端程序检测所述移动设备是否安装有第三方应用
否
402
第二客户端程序下载所述第三方应用安装包发送至移动设备侧
403
移动设备侧依据所述第三方应用安装包安装第三方应用
404
建立所述移动设备与所述计算设备的SOCKET连接通道
405
所述第二客户端程序SOCKET连接通道向所述第三方应用发出对移动设备的安全检测请求，所述体检请求包括指定检测对象
406
所述第三方应用对所述指定检测对象执行对应的安全检测操作，获得安全检测结果信息
407
第三方应用将所述安全检测结果信息返回第二客户端程序
408
所述第二客户端程序依据所述安全检测结果信息获得对应的执行建议信息
409
所述第二客户端程序展示所述安全检测结果信息以及对应的执行建议信息
410
所述第二客户端程序在接收到用户针对一个或多个执行建议信息的选定指令后，依据所述选定指令生成与所述一个或多个执行建议信息对应的执行指令并发送至第三应用中
411
第三方应用执行所述执行指令

图 4

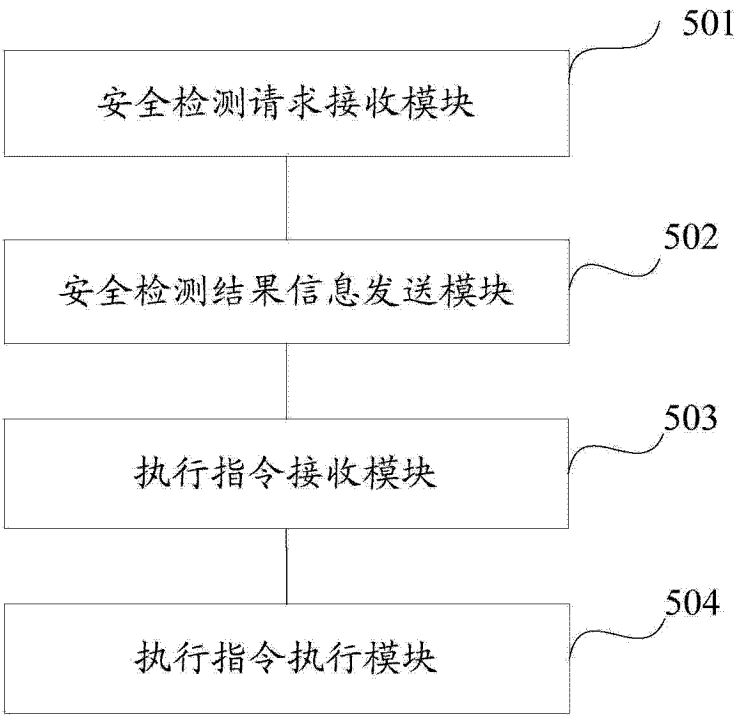

501
安全检测请求接收模块
502
安全检测结果信息发送模块
503
执行指令接收模块
504
执行指令执行模块

图 5

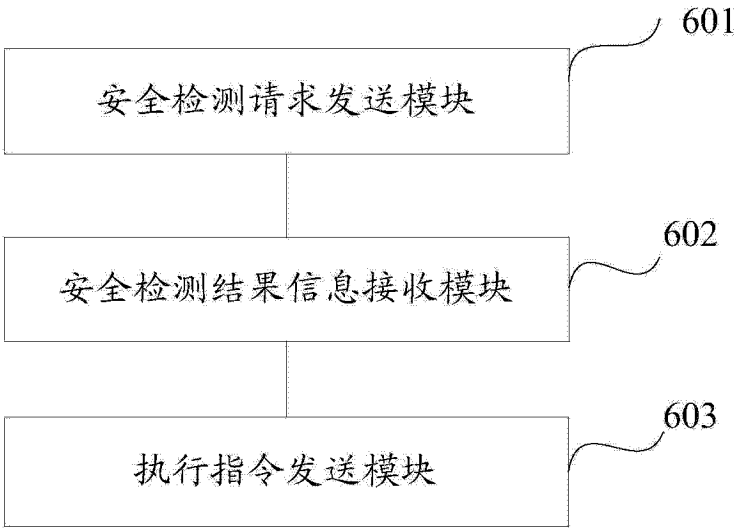

601
安全检测请求发送模块
602
安全检测结果信息接收模块
603
执行指令发送模块

图 6