(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2018 年 7 月 26 日 (26.07.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/133326 A1

(51) 国际专利分类号:
H04W 12/12 (2009.01)

(21) 国际申请号: PCT/CN2017/090077

(22) 国际申请日: 2017 年 6 月 26 日 (26.06.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710057618.5 2017年1月22日 (22.01.2017) CN

(71) 申请人: 华 为 技 术 有 限 公 司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 陈忠贤 (CHEN, Zhongxian); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 邹现军 (ZOU, Xianjun); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

WO 2018/133326 A1

(54) **Title:** METHOD AND DEVICE FOR APPLICATION DOWNLOAD MONITORING

(54) **发明名称**: 一种应用下载监控方法和设备

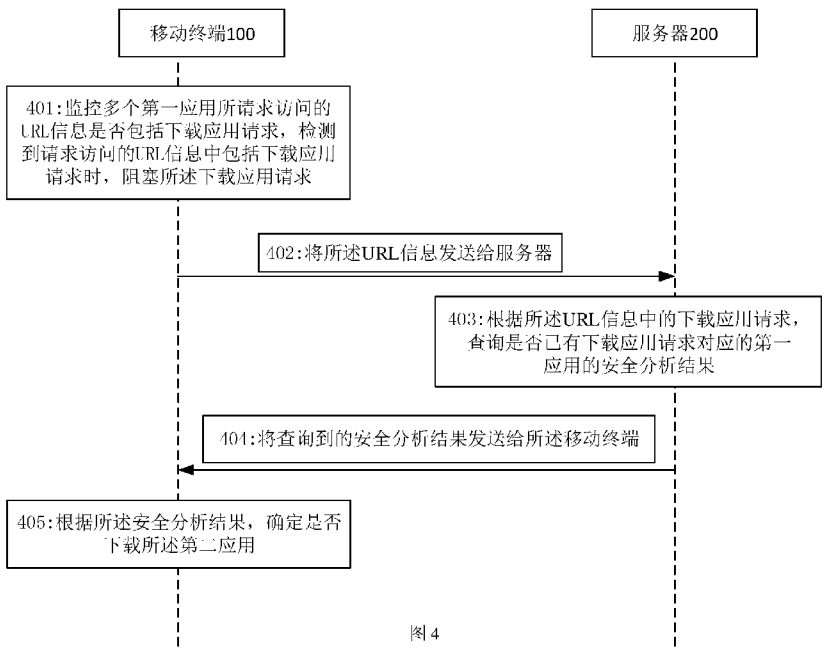

图 4

100 MOBILE TERMINAL
200 SERVER
401 MONITOR WHETHER URL INFORMATION REQUESTED TO BE ACCESSED BY A PLURALITY OF FIRST APPLICATIONS COMPRISES AN APPLICATION DOWNLOAD REQUEST, AND WHEN DETECTING THAT THE URL INFORMATION REQUESTED TO BE ACCESSED BY ANY ONE APPLICATION AMONGST THE PLURALITY OF FIRST APPLICATIONS COMPRISES AN APPLICATION DOWNLOAD REQUEST, BLOCK THE APPLICATION DOWNLOAD REQUEST
402 SEND THE URL INFORMATION TO THE SERVER
403 ON THE BASIS OF THE APPLICATION DOWNLOAD REQUEST IN THE URL INFORMATION, QUERY WHETHER THERE ARE ALREADY SECURITY ANALYSIS RESULTS OF A FIRST APPLICATION CORRESPONDING TO THE APPLICATION DOWNLOAD REQUEST
404 SEND THE QUERIED SECURITY ANALYSIS RESULTS TO THE MOBILE TERMINAL
405 ON THE BASIS OF THE SECURITY ANALYSIS RESULTS, DETERMINE WHETHER TO DOWNLOAD THE SECOND APPLICATION

(57) **Abstract:** Provided in the present application are a method and a device for implementing application download monitoring: a mobile terminal monitors whether URL information requested to be accessed by a plurality of first applications comprises an application download request; when detecting that the URL information requested to be accessed by any one application amongst the plurality of first applications comprises an application download request, the mobile terminal blocks the application download request, and sends the URL information to a server; on the basis of the application download request in the URL information, the server queries whether

[见续页]

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告(条约第21条(3))。

there are already security analysis results of a second application corresponding to the application download request and, if so, the server sends the security analysis results to the mobile terminal; and, on the basis of the security analysis results, the mobile terminal determines whether to download the second application. The mobile terminal monitors from the bottom layer the behaviour of a plurality of applications requesting download of new applications, and reports the behaviour to a server to query security analysis results; on the basis of the security analysis results issued by the server, the mobile terminal implements corresponding protective processing of the download behaviour, achieving the effective health and protection of application download behaviour.

(57) 摘要：本申请提供了一种实现应用下载监控的方法和设备，移动终端监控多个第一应用所请求访问的URL信息是否包括下载应用请求；当检测到多个第一应用中任一应用所请求访问的URL信息中包括下载应用请求时，移动终端阻塞下载应用请求，并将URL信息发送给服务器；服务器根据URL信息中的下载应用请求，查询是否已有下载应用请求对应的第二应用的安全分析结果，若查询到，则服务器将安全分析结果发送给移动终端；移动终端根据安全分析结果，确定是否下载第二应用。移动终端从底层监控多个应用中请求下载新应用的行为，将该行为上报给服务器查询安全分析结果，移动终端根据服务器下发的安全分析结果对下载行为进行相应保护处理，对应用下载行为进行有效健康和保护。

一种应用下载监控方法和设备

本申请要求于 2017 年 01 月 22 日提交中国专利局、申请号为 201710057618.5、申请名称为“一种基于防火墙的应用下载方法和设备”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

本申请涉及电子技术领域，尤其涉及一种应用下载监控方法和设备。

背景技术

移动互联网是一个开放的体系，用户在手机上浏览访问网页或资讯时，可能会被误导下载一些恶意软件，导致用户安全受损，现有技术通常在应用内部进行下载检测和管控，例如，浏览器 APP（应用，Application）会检测用户点击的链接，假如发现是下载链接，会弹框提示用户进行确认，并且会引导用户使用更安全的下载链接。

然而，在单个应用内进行下载检测，不具备通用性，当很多广告的软件开发工具包（software development kit, SDK）会嵌入到各种 APK（Android®操作系统的应用程序包，Android application package）中，在这些 APK 中弹出广告组件诱导用户进行应用下载安装时，此方案不能解决问题，用户仍然可能被诱导安装一些恶意软件，用户仍然可能被诱导安装一些恶意软件。

发明内容

根据本申请一些实施例提供的一种应用下载的方法和设备，旨在减少用户被诱导下载安装恶意应用的风险。

第一方面，本申请提供了一种应用下载监控方法，包括以下步骤：首先，移动终端监控多个第一应用所请求访问的 URL 信息是否包括下载应用请求；当检测到所述多个第一应用中任一应用所请求访问的 URL 信息中包括下载应用请求时，所述移动终端阻塞所述下载应用请求，并将所述 URL 信息发送给服务器；然后，所述服务器根据所述 URL 信息中的下载应用请求，查询是否已有所述下载应用请求对应的第二应用的安全分析结果，若查询到，则所述服务器将所述安全分析结果发送给所述移动终端；之后，所述移动终端根据所述安全分析结果，确定是否下载所述第二应用。

所述移动终端从底层监控所有应用或指定一些应用中请求下载新应用的行为，将该行为上报给服务器查询该新应用的安全分析结果，然后移动终端根据服务器下发的安全分析结果对下载行为进行相应保护处理，从而实现从底层对所有应用或指定一些应用的新应用下载行为进行有效健康和保护。

在一些可能的实现方式中，所述方法还包括以下步骤：所述移动终端将已安装应用的应用包名列表发送给所述服务器；所述服务器根据所述应用包名列表，配置监控信息并发送给所述移动终端，所述监控信息包括需要监控的所述多个第一应用的应用包名列表和识别 URL 信息中下载应用请求的规则；相应地，所述移动终端监控多个第一应用中任一应用所请求访问的 URL 信息是否包括下载应用请求的步骤包括：所述移动终端根据所述监控信息，检测所述需要监控的所述多个第一应用中任一应用所请求访问的 URL 信息是否包括下载应用请求。其中，移动终端上报已安装应用的应用包名列表及服务器下发配置并下发监控信息的步骤与第一方面所描述的方法的步骤之间的先后顺序并不被限定。

服务器定期配置并下发监控信息，可以及时更新监控范围，提高保护效果；另外，移动终端可以根据区分移动终端中需要监控的应用和不需要监控的应用，对不需要监控的应用，移动终端可以不执行上报 URL 信息，从而在安全保护下，简化监控流程，节约监控过程所占用资源。

第二方面，本申请提供了一种在移动终端侧实现的应用下载监控的方法，其中，所述方法包括：首

先，移动终端监控多个第一应用所请求访问的 URL 信息是否包括下载应用请求；当所述移动终端检测到所述多个第一应用中任一应用所请求访问的 URL 信息中包括下载应用请求时，所述移动终端阻塞所述下载应用请求，并将所述 URL 信息发送给服务器；然后，所述移动终端接收所述服务器发送的安全分析结果，其中，所述安全分析结果为所述服务器根据所述 URL 信息中的下载应用请求，查询到的对应第二应用的安全分析结果；之后，所述移动终端根据所述安全分析结果，确定是否下载所述第二应用。

在一些可能的实现方式中，所述方法还包括：所述移动终端将已安装应用的应用包名列表发送给所述服务器；然后所述移动终端接收所述服务器发送的监控信息，所述监控信息包括需要监控的所述多个第一应用的应用包名列表和识别 URL 信息中下载应用请求的规则；相应地，所述移动终端监控多个第一应用中任一应用所请求访问的 URL 信息是否包括下载应用请求的步骤包括：所述移动终端根据所述监控信息，检测所述需要监控的所述多个第一应用中任一应用所请求访问的 URL 信息是否包括下载应用请求。其中，移动终端上报已安装应用的应用包名列表及接收服务器下发配置并下发监控信息的步骤与第二方面所描述的方法的步骤之间的先后顺序并不被限定。

在一些可能的实现方式中，所述移动终端根据所述监控信息，检测所述需要监控的所述多个第一应用任一应用所请求访问的 URL 信息是否包括下载应用请求的步骤，具体包括：所述移动终端根据需要监控的所述多个第一应用的应用包名列表检测所述多个第一应用是否请求访问 URL 信息；当检测到所述多个第一应用中任一应用请求访问 URL 信息，所述移动终端根据所述识别 URL 信息中下载应用请求的规则检测该第一应用所请求访问的 URL 信息中是否包括下载应用请求。

在一些可能的实现方式中，所述移动终端根据所述安全分析结果，确定是否下载所述第二应用的步骤，具体包括：所述移动终端根据所述安全分析结果，确定直接禁止下载所述第二应用、根据用户选择输入确定是否下载所述第二应用或直接允许下载所述第二应用。

在一些可能的实现方式中，当所述移动终端确定根据用户选择输入确定是否下载所述第二应用，所述方法还包括：所述移动终端显示待选择的提示界面，并获取用户的选择操作；根据所述选择操作，确定禁止或允许下载所述第二应用。

在一些可能的实现方式中，当所述移动终端确定禁止下载所述第二应用，所述方法还包括以下至少任一步骤：所述移动终端显示已禁止下载所述第二应用的提示界面；所述移动终端提示与所述第二应用相关的第三应用的下载信息，并获取用户根据所述第三应用的下载信息所选择的下载操作，下载所述第三应用。

第三方面， 本申请提供了一种在服务器侧实现的应用下载监控的方法，其中，所述方法包括：服务器接收移动终端发送的多个第一应用中任一应用所请求访问的 URL 信息，其中，所述 URL 信息包括下载应用请求；然后，所述服务器根据所述 URL 信息中的下载应用请求，查询是否已有所述下载应用请求对应的第二应用的安全分析结果，若查询到，则所述服务器将所述安全分析结果发送给所述移动终端。

在一些可能的实现方式中，所述方法还包括：所述服务器接收所述移动终端的已安装应用的应用包名列表；随后，所述服务器根据所述应用包名列表，配置监控信息并发送给所述移动终端，其中，所述监控信息包括需要监控的所述多个第一应用的应用包名列表和识别 URL 信息中下载应用请求的规则。

在一些可能的实现方式中，所述方法还包括：若所述服务器未查询到所述下载应用请求对应的第二应用的安全分析结果，则所述服务器根据所述 URL 信息请求下载所述第二应用，下载后对所述第二应用进行安全分析并记录安全分析结果。

当服务器接收到全网移动终端首次上报的某一新应用的下载请求时，根据下载请求的 URL 信息从应用服务器下载该新应用到服务器中进行安全分析并记录安全分析结果，从而实现服务器端对网络应用的安全监控的及时更新，进一部提高移动终端对应用安装的防护效果。

在一些可能的实现方式中，所述方法还包括：若所述服务器未查询到所述下载应用请求对应的第二应用的安全分析结果，则所述服务器通知所述移动终端允许下载所述第二应用。

第四方面，本申请提供了一种实现应用下载监控的移动终端，其中，所述移动终端包括：内核防火墙组件和管控引导单元，所述内核防火墙组件用于监控多个第一应用所请求访问的 URL 信息是否包括下载应用请求，并在检测到所述多个第一应用中任一应用所请求访问的 URL 信息中包括下载应用请求时，阻塞所述下载应用请求；所述管控引导单元用于将所述 URL 信息发送给服务器、接收所述服务器发送的安全分析结果并发送所述内核防火墙组件，其中，所述安全分析结果为所述服务器根据所述 URL 信息中的下载应用请求，查询到的对应第二应用的安全分析结果；相应地，所述内核防火墙组件还用于所述安全分析结果确定是否下载所述第二应用。

在一些可能的实施例中，所述管控引导单元还用于将已安装应用的应用包名列表发送给所述服务器；相应地，所述移动终端还包括：策略下发单元，用于接收所述服务器发送的监控信息并发送给所述内核防火墙组件，所述监控信息包括需要监控的所述第一应用的应用包名列表和识别 URL 信息中下载应用请求的规则；相应地，所述内核防火墙组件用于根据所述监控信息检测到第一应用中任一应用所请求访问的 URL 信息中是否包括下载应用请求。

在一些可能的实施例中，所述移动终端还包括管控交互接口，其中，所述内核防火墙组件通过所述管控交互接口向所述管控引导单元上传检测到的包含所述多个第一应用中至少一个应用的包含下载应用请求的 URL 信息。

在一些可能的实施例中，所述内核防火墙组件用于接收移动终端的网络流量，并监控所述多个第一应用的应用进程 ID 请求访问的 URL 信息中是否有下载应用请求。

第五方面，本申请提供了一种在实现应用下载监控的服务器，其中，所述服务器包括：数据存储单元，用于存储第二应用的安全分析结果；URL 分析单元，用于接收到移动终端发送的多个第一应用中任一应用所请求访问的 URL 信息， 并根据所述 URL 信息中的下载应用请求，查询是否已有所述下载应用请求对应的所述第二应用的安全分析结果，若查询到，则将所述安全分析结果发送给所述移动终端，其中，所述 URL 信息包括下载应用请求。

在一些可能的实施例中，所述 URL 分析单元，还用于接收所述移动终端的已安装应用的应用包名列表；相应地，所述服务器还包括：策略服务单元，用于根据所述应用包名列表，配置监控信息并发送给所述移动终端，其中，所述监控信息包括需要监控的所述多个第一应用的应用包名列表和识别 URL 信息中下载应用请求的规则。

第六方面，本申请提供了一种实现应用下载监控的移动终端，其中，所述移动终端包括：至少一个处理器；至少一个存储器，所述至少一个存储器包括若干指令；所述至少一个处理器执行所述若干指令使所述移动终端至少执行如下步骤：监控多个第一应用所请求访问的 URL 信息是否包括下载应用请求；当检测到所述多个第一应用中任一应用所请求访问的 URL 信息中包括下载应用请求时，阻塞所述下载应用请求，并将所述 URL 信息发送给服务器；然后，接收所述服务器发送的安全分析结果，其中，所述安全分析结果为所述服务器根据所述 URL 信息中的下载应用请求，查询到的对应第二应用的安全分析结果；随后，根据所述安全分析结果，确定是否下载所述第二应用。

在一些可能的实现方式中，所述至少一个处理器执行所述若干指令使所述终端还执行如下步骤：将已安装应用的应用包名列表发送给所述服务器；然后，接收所述服务器发送的监控信息，所述监控信息包括需要监控的所述多个第一应用的应用包名列表和识别 URL 信息中下载应用请求的规则；相应地，在所述监控多个第一应用中任一应用所请求访问的 URL 信息是否包括下载应用请求的步骤中，所述至少一个处理器执行所述若干指令使所述终端至少执行如下步骤：根据所述监控信息，检测所述需要监控的所

述多个第一应用中任一应用所请求访问的URL信息是否包括下载应用请求。

在一些可能的实现方式中，在所述移动终端根据所述监控信息，检测所述需要监控的所述多个第一应用任一应用所请求访问的URL信息是否包括下载应用请求的步骤中，所述至少一个处理器执行所述若干指令使所述终端至少执行如下步骤：根据需要监控的所述多个第一应用的应用包名列表检测所述多个第一应用是否请求访问 URL 信息；当检测到所述多个第一应用中任一应用请求访问 URL 信息，根据所述识别 URL 信息中下载应用请求的规则检测该第一应用所请求访问的 URL 信息中是否包括下载应用请求。

在一些可能的实现方式中，在根据所述安全分析结果，确定是否下载所述第二应用的步骤中，所述至少一个处理器执行所述若干指令使所述终端至少执行如下步骤：根据所述安全分析结果，确定直接禁止下载所述第二应用、根据用户选择输入确定是否下载所述第二应用或直接允许下载所述第二应用。

在一些可能的实现方式中，所述移动终端还包括触摸屏；在根据用户选择输入确定是否下载所述第二应用的步骤中，所述至少一个处理器执行所述若干指令使所述终端至少执行如下步骤：使所述触摸屏显示待选择的提示界面，并获取用户的选择操作；根据所述选择操作，确定禁止或允许下载所述第二应用。

在一些可能的实现方式中，所述移动终端还包括触摸屏；在确定禁止下载所述第二应用的步骤之后，所述至少一个处理器执行所述若干指令使所述终端至少执行如下至少一个步骤：使所述触摸屏显示已禁止下载所述第二应用的提示界面；使所述触摸屏提示与所述第二应用相关的第三应用的下载信息并获取用户根据所述第三应用的下载信息所选择的下载操作，其后，下载所述第三应用。

第七方面，本申请提供了一种实现应用下载监控的服务器，其中，所述服务器包括：至少一个处理器；至少一个存储器，所述至少一个存储器包括若干指令；所述至少一个处理器执行所述若干指令使所述服务器至少执行如下步骤：接收移动终端发送的多个第一应用中任一应用所请求访问的URL信息，其中，所述 URL 信息包括下载应用请求；然后，根据所述 URL 信息中的下载应用请求，查询是否已有所述下载应用请求对应的第二应用的安全分析结果，若查询到，则将所述安全分析结果发送给所述移动终端。

在一些可能的实现方式中，所述至少一个处理器执行所述若干指令使所述服务器还执行如下步骤：接收所述移动终端的已安装应用的应用包名列表；根据所述应用包名列表，配置监控信息并发送给所述移动终端，所述监控信息包括需要监控的所述多个第一应用的应用包名列表和识别 URL 信息中下载应用请求的规则。

在一些可能的实现方式中，所述至少一个处理器执行所述若干指令使所述服务器还执行如下步骤：若未查询到所述下载应用请求对应的第二应用的安全分析结果，则根据所述 URL 信息请求下载所述第二应用，下载后对所述第二应用进行安全分析并记录安全分析结果。

在一些可能的实现方式中，所述至少一个处理器执行所述若干指令使所述服务器还执行如下步骤：若未查询到所述下载应用请求对应的第二应用的安全分析结果，则通知所述移动终端允许下载所述第二应用。

第八方面，本申请提供了一种显示在移动终端的触摸屏中的图形用户界面（GUI），其中，所述图形用户界面包括：在所述触摸屏中显示第一 GUI；接着，响应于检测到用户执行操作所触发的所述多个第一应用中任一应用所请求访问的 URL 信息中包括下载应用请求时，将所述 URL 信息发送给服务器；然后响应于接收到服务器根据所述 URL 信息发送的第二应用的安全分析结果确定的直接禁止下载所述第二应用、根据用户选择输入确定是否下载所述第二应用或直接允许下载所述第二应用，显示第二 GUI，所述第二 GUI 包括：提示已禁止下载所述第二应用、根据用户选择输入确定是否下载所述第二应用或已允许下载所述第二应用的界面；当响应于确定需根据用户选择输入确定是否下载所述第二应用，响应于用

户输入的选择操作，确定禁止或允许下载所述第二应用。

在一些可能的实现方式中，所述图形用户界面还包括：响应于确定禁止下载所述第二应用，所述第二 GUI 还包括： 提示与所述第二应用相关的第三应用的下载信息的界面；响应于获取用户根据所述第三应用的下载信息所选择的下载操作，下载所述第三应用，并显示第三 GUI，所述第三 GUI 包括提示已下载第三应用的界面。

本申请各实施例提供的图形用户界面，能够将对所述多个第一应用中任一应用所请求访问的 URL 信息中包括下载应用请求时进行的监控和保护过程，展示给用户，并根据安全分析结果为用户提供可选择的交互，提高用户使用体验。

第九方面，本申请提供了一种计算机程序产品，其中，当所述计算机程序产品在移动终端上运行时，使得所述移动终端执行如第二方面及第二方面中各个可能的实现方式中任一方法。

第十方面，本申请提供了一种计算机程序产品，其中，当所述计算机程序产品在服务器上运行时，使得所述服务器执行如第三方面及第三方面中各个可能的实现方式中任一方法。

第十一方面，本申请提供了一种计算机可读存储介质，包括指令，其中，当所述指令在服务器上运行时，使得所述服务器执行如第二方面及第二方面中各个可能的实现方式中任一方法。

第十二方面，本申请提供了一种计算机可读存储介质，其中，当所述指令在服务器上运行时，使得所述服务器执行如第三方面及第三方面中各个可能的实现方式中任一方法。

第十三方面，本申请提供了一种实现应用下载监控的系统，所述系统包括至少一个移动终端和服务器；所述移动终端用于监控多个第一应用所请求访问的 URL 信息是否包括下载应用请求，并在检测到所述多个第一应用中任一应用所请求访问的 URL 信息中包括下载应用请求时，所述移动终端阻塞所述下载应用请求，并将所述 URL 信息发送给服务器；所述服务器用于根据所述 URL 信息中的下载应用请求，查询是否已有所述下载应用请求对应的第二应用的安全分析结果，若查询到，则所述服务器将所述安全分析结果发送给所述移动终端；所述移动终端还用于根据所述安全分析结果，确定是否下载所述第二应用。

在一些可能的实现方式中，所述移动终端还用于将已安装应用的应用包名列表发送给所述服务器，并接收所述服务器发送的监控信息，然后，根据所述监控信息，检测所述需要监控的所述多个第一应用中任一应用所请求访问的 URL 信息是否包括下载应用请求；所述服务器还用于接收所述移动终端的已安装应用的应用包名列表，并根据所述应用包名列表，配置监控信息并发送给所述移动终端，其中，所述监控信息包括需要监控的所述多个第一应用的应用包名列表和识别 URL 信息中下载应用请求的规则。

在一些可能的实现方式中，所述服务器还用于在未查询到所述下载应用请求对应的第二应用的安全分析结果，则所述 URL 信息请求下载所述第二应用，下载后对所述第二应用进行安全分析并记录安全分析结果。

在一些可能的实现方式中，所述服务器还在未查询到所述下载应用请求对应的第二应用的安全分析结果，则所述服务器通知所述移动终端允许下载所述第二应用。

附图说明

图 1 示出根据本申请一些实施例提供的包括移动终端和服务器的一种可能的系统架构示意图；

图 2 示出根据本申请实施例提供的一种移动终端的结构示意图；

图 3 示出本申请实施例中提供的一种可能的系统架构示意图；

图 4 示出根据本申请实施例提供的一种实现应用下载监控的方法流程示意图；

图 5 示出根据本申请实施例提供的另一种实现应用下载监控的方法流程示意图；

图 6 示出根据本申请实施例提供的一种可能的场景中实现应用下载监控的方法流程示意图；

图 7-图 13 示出根据本申请实施例提供的一种可能的场景中实现应用下载监控的方法流程示意图。

具体实施方式

本申请实施例中所使用的术语只是为了描述特定实施例的目的，而并非旨在作为对本申请的限制。如在本申请的说明书和所附权利要求书中所使用的那样，单数表达形式“一个”、“一种”、“所述”、“上述”和“该”旨在也包括复数表达形式，除非其上下文中明确地有相反指示。还应当理解，本申请中可能使用的术语“和/或”是指并包含一个或多个相绑定的列出项目的任何或所有可能组合。

以下介绍了移动终端、服务器、用于这样的移动终端的图形用户界面（以下可以简称 GUI）、以及所述移动终端和服务器配合实现应用下载监控的方法的实施例。

本申请实施例用以实现，通过移动终端和服务器的配合，对移动终端中所有应用或指定一些应用中的请求下载新应用的行为进行监控和保护。下面将结合一些实施例中的附图，对实施例中的技术方案进一步描述。

图 1 示出本申请一些实施例提供的包括移动终端和服务器的简要系统架构示意图，如图 1 所示，系统包括若干移动终端、服务器和至少一个应用下载服务方，若干移动终端与服务器通信用以实现服务器对移动终端的安全管理，可以包括对新应用下载的安全管理、提供安全的应用下载等，并且，移动终端在运行过程中会根据 URL 信息向应用下载服务方请求下载应用，在本申请的实施例中，服务器也可能在全网的移动终端首次上报 URL 信息时，在服务器侧向根据该 URL 信息向应用下载服务方请求下载应用，以进行安全分析和记录更新。

在本申请一些实施例中，所述移动终端可以是还包含其它功能诸如个人数字助理和/或音乐播放器功能的便携式电子设备，诸如手机、平板电脑、具备无线通讯功能的可穿戴电子设备（如智能手表）等。便携式电子设备的示例性实施例包括但不限于搭载 iOS®、Android®、Microsoft®或者其它操作系统的便携式电子设备。上述便携式电子设备也可以是其它便携式电子设备，诸如具有触敏表面(例如触控板)的膝上型计算机（Laptop）等。还应当理解的是，在本申请其他一些实施例中，所述移动终端还可以是符合同类规范的遥控器、智能环境检测器等可作为移动安全代理的设备。

如图 2 所示，本申请实施例中的移动终端可以为手机 100。下面以手机 100 为例对实施例进行具体说明。应该理解的是，图示手机 100 仅是移动终端的一个范例，并且手机 100 可以具有比图中所示出的更多的或者更少的部件，可以组合两个或更多的部件，或者可以具有不同的部件配置。图中所示出的各种部件可以在包括一个或多个信号处理和/或专用集成电路在内的硬件、软件、或硬件和软件的组合中实现。

如图 2 所示，手机 100 具体可以包括以下硬件：处理器 101、射频（RF）电路 102、存储器 103、触摸屏 104、蓝牙装置 105、一个或多个传感器 106、Wi-Fi 装置 107、定位装置 108、音频电路 109、外设接口 110 以及电源系统 111 等部件。这些部件可通过一根或多根通信总线或信号线（图 2 中未示出）进行通信。本领域技术人员可以理解，图 2 中示出的硬件结构并不构成对手机 100 的限定，手机 100 可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

下面结合图 2 对手机 100 的各个部件进行具体的介绍：

处理器 101 是手机 100 的控制中心，利用各种接口和线路连接手机 100 的各个部分，通过运行或执行存储在存储器 103 内的应用程序（以下可以简称 App），以及调用存储在存储器 103 内的数据和指令，执行手机 100 的各种功能和处理数据。在一些实施例中，处理器 101 可包括一个或多个处理单元；处理器 101 还可以集成应用处理器和调制解调处理器；其中，应用处理器主要处理操作系统、用户界面和应

用程序等，调制解调处理器主要处理无线通信。可以理解的是，上述调制解调处理器也可以不集成到处理器 101 中。处理器 101 可以是集成芯片。在本申请一些实施例中，上述处理器 101 还可以包括指纹验证芯片，用于对采集到的指纹进行验证。

射频电路 102 可用于在收发信息或通话过程中，无线信号的接收和发送。具体地，射频电路 102 可以将基站的下行数据接收后，给处理器 101 处理；另外，将涉及上行的数据发送给基站。通常，射频电路包括但不限于天线、至少一个放大器、收发信机、耦合器、低噪声放大器、双工器等。此外，射频电路 102 还可以通过无线通信和其他设备通信。所述无线通信可以使用任一通信标准或协议，包括但不限于全球移动通讯系统、通用分组无线服务、码分多址、宽带码分多址、长期演进、电子邮件、短消息服务等。

存储器 103 用于存储应用程序以及数据，处理器 101 通过运行存储在存储器 103 的应用程序以及数据，执行手机 100 的各种功能以及数据处理。存储器 103 主要包括存储程序区以及存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需的应用程序（比如声音播放功能、图像播放功能等）；存储数据区可以存储根据使用手机 100 时所创建的数据（比如音频数据、电话本等）。此外，存储器 103 可以包括高速随机存取存储器，还可以包括非易失存储器，例如磁盘存储器件、闪存器件或其他易失性固态存储器件等。存储器 103 可以存储各种操作系统，例如苹果公司所开发的 iOS®操作系统，谷歌公司所开发的 Android®操作系统等。

触摸屏 104 可以包括触控板 104-1 和显示器 104-2。其中，触控板 104-1 可采集手机 100 的用户在其上或附近的触摸事件（比如用户使用手指、触控笔等任何适合的物体在触控板 104-1 上或在触控板 104-1 附近的操作），并将采集到的触摸信息发送给其他器件例如处理器 101。其中，用户在触控板 104-1 附近的触摸事件可以称之为悬浮触控；悬浮触控可以是指，用户无需为了选择、移动或拖动目标（例如图标等）而直接接触触控板，而只需用户位于移动终端附近以便执行所想要的功能。在悬浮触控的应用场景下，术语“触摸”、“接触”等不会暗示用于直接接触触摸屏，而是附近或接近的接触。能够进行悬浮触控的触控板 104-1 可以采用电容式、红外光感以及超声波等实现。触控板 104-1 可包括触摸检测装置和触摸控制器两个部分。其中，触摸检测装置检测用户的触摸方位，并检测触摸操作带来的信号，将信号传送给触摸控制器；触摸控制器从触摸检测装置上接收触摸信息，并将它转换成触点坐标，再发送给处理器 101，触摸控制器还可以接收处理器 101 发送的指令并加以执行。此外，可以采用电阻式、电容式、红外线以及表面声波等多种类型来实现触控板 104-1。显示器（也称为显示屏）104-2 可用于显示由用户输入的信息或提供给用户的信息以及手机 100 的各种菜单。可以采用液晶显示器、有机发光二极管等形式来配置显示器 104-2。触控板 104-1 可以覆盖在显示器 104-2 之上，当触控板 104-1 检测到在其上或附近的触摸事件后，传送给处理器 101 以确定触摸事件的类型，随后处理器 101 可以根据触摸事件的类型在显示器 104-2 上提供相应的视觉输出。虽然在图 2 中，触控板 104-1 与显示屏 104-2 是作为两个独立的部件来实现手机 100 的输入和输出功能，但是在某些实施例中，可以将触控板 104-1 与显示屏 104-2 集成而实现手机 100 的输入和输出功能。可以理解的是，触摸屏 104 是由多层的材料堆叠而成，本申请实施例中只展示出了触控板（层）和显示屏（层），其他层在本申请实施例中不予记载。另外，在本申请其他一些实施例中，触控板 104-1 可以覆盖在显示器 104-2 之上，并且触控板 104-1 的尺寸大于显示屏 104-2 的尺寸，使得显示屏 104-2 全部覆盖在触控板 104-1 下面，或者，上述触控板 104-1 可以以全面板的形式配置在手机 100 的正面，也即用户在手机 100 正面的触摸均能被手机感知，这样就可以实现手机正面的全触控体验。在其他一些实施例中，触控板 104-1 以全面板的形式配置在手机 100 的正面，显示屏 104-2 也可以以全面板的形式配置在手机 100 的正面，这样在手机的正面就能够实现无边框（Bezel）的结构。

在本申请实施例中，手机 100 还可以具有指纹识别功能。例如，可以在手机 100 的背面（例如后置摄像头的下方）配置指纹识别器，或者在手机 100 的正面（例如触摸屏 104 的下方）配置指纹识别器。不再详述。

手机 100 还可以包括蓝牙装置 105，用于实现手机 100 与其他短距离的移动终端（例如手机、智能手表等）之间的数据交换。本申请实施例中的蓝牙装置可以是集成电路或者蓝牙芯片等。

手机 100 还可以包括至少一种传感器 106，比如光传感器、运动传感器以及其他传感器。具体地，光传感器可包括环境光传感器及接近传感器，其中，环境光传感器可根据环境光线的明暗来调节触摸屏 104 的显示器的亮度，接近传感器可在手机 100 移动到耳边时，关闭显示器的电源。作为运动传感器的一种，加速计传感器可检测各个方向上（一般为三轴）加速度的大小，静止时可检测出重力的大小及方向，可用于识别手机姿态的应用（比如横竖屏切换、相关游戏、磁力计姿态校准）、振动识别相关功能（比如计步器、敲击）等; 至于手机 100 还可配置的陀螺仪、气压计、湿度计、温度计、红外线传感器等其他传感器，在此不再赘述。

Wi-Fi 装置 107，用于为手机 100 提供遵循 Wi-Fi 相关标准协议的网络接入，手机 100 可以通过 Wi-Fi 装置 107 接入到 Wi-Fi 接入点，进而帮助用户收发电子邮件、浏览网页和访问流媒体等，它为用户提供了无线的宽带互联网访问。在其他一些实施例中，该 Wi-Fi 装置 107 也可以作为 Wi-Fi 无线接入点，可以为其他移动终端提供 Wi-Fi 网络接入。

定位装置 108，用于为手机 100 提供地理位置。可以理解的是，该定位装置 108 具体可以是全球定位系统（GPS，global positioning system）或北斗卫星导航系统、俄罗斯 GLONASS 等定位系统的接收器。定位装置 108 在接收到上述定位系统发送的地理位置后，将该信息发送给处理器 101 进行处理，或者发送给存储器 103 进行保存。在另外的一些实施例中，该定位装置 108 可以是辅助全球卫星定位系统（AGPS）的接收器，AGPS 是一种在一定辅助配合下进行 GPS 定位的运行方式，它可以利用基站的信号，配合 GPS 卫星信号，可以让手机 100 定位的速度更快；在 AGPS 系统中，该定位装置 108 可通过与辅助定位服务器（例如手机定位服务器）的通信而获得定位辅助。AGPS 系统通过作为辅助服务器来协助定位装置 108 完成测距和定位服务，在这种情况下，辅助定位服务器通过无线通信网络与移动终端例如手机 100 的定位装置 108（即 GPS 接收器）通信而提供定位协助。在另外的一些实施例中，该定位装置 108 也可以是基于 Wi-Fi 接入点的定位技术。由于每一个 Wi-Fi 接入点都有一个全球唯一的 MAC 地址，移动终端在开启 Wi-Fi 的情况下即可扫描并收集周围的 Wi-Fi 接入点的广播信号，因此可以获取到 Wi-Fi 接入点广播出来的 MAC 地址；移动终端将这些能够标示 Wi-Fi 接入点的数据（例如 MAC 地址）通过无线通信网络发送给位置服务器，由位置服务器检索出每一个 Wi-Fi 接入点的地理位置，并结合 Wi-Fi 广播信号的强弱程度，计算出该移动终端的地理位置并发送到该移动终端的定位装置 108 中。

音频电路 109、扬声器 113、麦克风 114 可提供用户与手机 100 之间的音频接口。音频电路 109 可将接收到的音频数据转换后的电信号，传输到扬声器 113，由扬声器 113 转换为声音信号输出；另一方面，麦克风 114 将收集的声音信号转换为电信号，由音频电路 109 接收后转换为音频数据，再将音频数据输出至 RF 电路 102 以发送给比如另一手机，或者将音频数据输出至存储器 103 以便进一步处理。

外设接口 110，用于为外部的输入/输出设备（例如键盘、鼠标、外接显示器、外部存储器、用户识别模块卡等）提供各种接口。例如通过通用串行总线（USB）接口与鼠标连接，通过用户识别模块卡卡槽上的金属触点与电信运营商提供的用户识别模块卡（SIM）卡进行连接。外设接口 110 可以被用来将上述外部的输入/输出外围设备耦接到处理器 101 和存储器 103。

手机 100 还可以包括给各个部件供电的电源装置 111（比如电池和电源管理芯片），电池可以通过电源管理芯片与处理器 101 逻辑相连，从而通过电源装置 111 实现管理充电、放电、以及功耗管理等功

能。

尽管图 2 未示出，手机 100 还可以包括摄像头（前置摄像头和/或后置摄像头）、闪光灯、微型投影装置、近场通信（NFC）装置等，在此不再赘述。

以下实施例均可以在具有上述结构的手机 100 中实现。

在本申请实施例中，服务器 200 可以是包括处理器 204、存储器 203、系统总线 205 及通信接口 202 的计算机设备，其中，存储器 203 可以是包括 RAM 和 ROM、或任何固定的存储介质、或可移动的存储介质，用于存储可以执行本申请实施例的程序或本申请实施例的应用数据库，通过总线 205 接收其他组件的输入或被其他组件调用所存储的信息。处理器 204 用于执行存储器 203 存储的本申请实施例的程序，并通过总线与其他装置双向通信。存储器 203 和处理器 204 也可以整合成应用本申请实施例的物理模块，在该物理模块上存储和运行实现该本申请实施例的程序。服务器 200 的各个组件可以通过总线系统 205 耦合在一起，其中总线系统 205 除包括数据总线之外，还可以包括电源总线、控制总线和状态信号总线等。但是为了清楚说明起见，在图中将各种总线都标为总线系统 205。

在一些实施例中，所述电子设备 200 还可以包括显示器和输入装置，可以是阴极射线管(CRT，Cathode Ray Tube)显示器、液晶（LCD，Liquid Crystal Display）显示器或触摸式屏幕（Touch Screen）等合适的装置，通过总线 205 接收指令使得显示器的屏幕上呈现图形化的用户界面。所述输入装置可以包括键盘、鼠标、轨迹识别器、语音识别接口等任何合适的装置，用于接收用户的输入，生成控制输入通过总线 205 发送给处理器或其他组件。一些电子设备 200 的显示器具有触摸式屏幕，该显示器同时也是输入装置。

在另一些实施例中，所述服务器 200 也可以是一个云部署，即由多个服务设备组成，且每个服务设备可以具有自己的处理器、存储器、系统总线及通信接口，管理服务设备之间可以通过网络通信。

图 3 示出本申请实施例中提供的一种可能的系统架构示意图，如图 3 所示，所述系统包括移动终端 100、服务器 200 和应用下载服务方 300（App_DL_Server）。

其中，移动终端 100 可以包括管理模块 121（phone manager）、框架层 122（framework，FW）、内核防火墙组件 123（netfilter），其中，管理模块 121 可以包括策略下发单元 121a 和管控引导单元 121b，框架层 122 可以包括管控交互接口 122a，内核防火墙组件 123 可以包括上报与拦截单元 123a，服务器 200 可以是管理服务方提供的服务器，服务器 200 包括数据库存储单元 201（data base，DB，即数据库）、策略服务单元 202（policy Server）、URL 分析单元 203（URL-Analyse）。各单元之间以及用户与移动终端之间可以通过图 3 所示接口 IF0~IF10 进行通信。

具体地，Policy Server202 负责策略的配置和下发，负责配置的策略信息包括要监控的 APK 包名及要访问的 URL（Universal Resource Locator，统一资源定位符），URL 为正则表达式，如*.apk 匹配所有 apk 结尾的 URL 信息。

URL-Analyse203 为 URL 分析器，提供接口进行 URL 匹配，对于移动终端上报的 URL 信息向数据库 201 查询匹配，假如匹配成功，则返回匹配结果信息，对于新的 URL 会直接请求此 URL 并进行下载，下载成功后通过安全检测系统来检测此应用的安全属性并将结果记录到数据库 201 中。

策略下发单元 121a 负责接收服务器 200 的策略下发请求并调用 Framework 的接口进行应用下载监控策略配置。

管控引导单元 121a 根据底层匹配到的应用下载的 URL 信息进行上报，调用 URL-Analyse203 的进行 URL 匹配，并根据返回结果决定是否弹框提示用户，进行风险提示，引导用户在更安全的渠道进行下载。

管控交互接口 122a 属于 framework（框架层）122 的一部分功能单元，主要是起到接口桥接的作用，

将应用层的策略配置信息及检测决策信息传递给内核防火墙组件 123，将底层防火墙组件 123 检测匹配到的 URL 信息上报到应用层，例如通知官方应用市场客户端。

上报与拦截单元 123a 位于内核防火墙组件 123 中，用于接收系统的网络流量，并进行拦截匹配，将匹配成功的 URL 信息上报到应用层，阻塞此 URL 请求，并根据应用层决策结果进行请求放通或放弃。

此外，移动终端 100 还可以包括官方应用市场客户端，用于提供下载官方正式版本应用接口，当用户选择到官方应用市场下载应用时，调用该接口实现应用市场安装正式版本应用。

另外，应用下载服务方 300 可以是第三方应用下载服务方提供的应用下载服务器。

终端管理员用户可以通过接口 IF0 与管理模块 121 进行交互，以设置管理模块 121 是否启动未知来源应用下载监控和保护，当启动后，管理模块 121 可以通过接口 IF10 在应用下载的监控和保护过程中通知用户，在一些实施例中，管理模块 121 可以通过移动终端 100 的显示设备，例如触控显示屏显示提示，并获取用户的输入操作，实现通知和交互过程。策略服务单元 202 可以通过接口 IF1 下发监控策略，策略下发单元 121a 可以通过接口 IF2 和接口 IF3 向底层下发监控策略，上报与拦截单元 203a 可以通过接口 IF5、IF6 和 IF7 上报 URL 信息，URL 分析单元 203 通过接口 IF7 下发安全分析结果，管控引导单元 121b 可以通过接口 IF9、IF2、IF3 向底层下发该安全分析结果。此外，管控引导单元 121b 可以通过接口 IF8 与官方应用市场客户端通信，例如请求官方应用市场客户端下载可替代的安全的应用。

以下结合图 3 和图 4，对服务器 200 配合移动终端实现对应用下载的监控和保护的实现过程进行进一步描述。在一些实施例中，所述方法包括步骤 401~步骤 405。

在步骤 401 中，移动终端 100 监控多个第一应用所请求访问的 URL 信息是否包括下载应用请求，当检测到第一应用所请求访问的 URL 信息中包括下载应用请求时，所述移动终端 100 阻塞所述 URL 信息，接着，在步骤 402 中，将所述 URL 信息发送给服务器 200。

结合图 3，在一些实施例中，由移动终端 100 的内核防火墙组件 123 进行实时检测，当检测到第一应用所请求访问的 URL 信息中包括下载应用请求时，移动终端 100 的内核防火墙组件 123 可以暂时阻塞相应的下载应用请求，并将该 URL 信息经内部管控交互接口和移动终端 100 的管理模块 121 中的管控引导单元 121b 上报给服务器 200。

然后，在步骤 403 中，服务器 200 根据所述 URL 信息中的下载应用请求，查询服务器 200 本地是否已有所述下载应用请求对应的第二应用的安全分析结果，接着在步骤 404 中，若服务器 200 查询到，则将所述安全分析结果发送给移动终端 100。

在一些实施例中，服务器 200 中数据库存储单元 201 可以存储若干第二应用及其安全分析结果，服务器 200 中的 URL 分析单元 203 可以提供 URL 匹配接口，当 URL 分析单元接收到移动终端 100 发送的 URL 信息，URL 分析单元 203 可以调取数据库存储单元 201 所存储的数据进行查询，并将查询到的安全分析结果发送给移动终端 100。

在另一些实施例中，若服务器 200 未查询服务器 200 本地已有所述下载应用请求对应的第二应用的安全分析结果，则服务器 200 根据所述 URL 信息下载对应的第二应用，下载到服务器 200 后，在服务器 200 中对该第二应用进行安全分析并记录安全分析结果。

在一些实施例中，若服务器 200 未查询服务器 200 本地已有所述下载应用请求对应的第二应用的安全分析结果，服务器 200 返回通知移动终端 100 未查询到，移动终端 100 可以提示用户未查询到的第二应用的安全分析结果，提示用户选择安装，或者移动终端 100 的内核防火墙组件 123 允许下载对应的第二应用。

具体地，服务器 200 的 URL 分析单元 203 可以调取数据库存储单元所存储的数据进行查询，说明该第二应用为全网首次下载，未进行过安全分析，当未查询到对应安全分析结果，则 URL 分析单元 203

直接根据所述 URL 信息向提供所述第二应用的应用提供方（APP_DL_Server）请求下载该第二应用，下载成功后通过安全监测系统对该第二应用进行安全分析，并将下载的第二应用及其安全分析结果更新存储到服务器 200 的数据库存储单元中。当再次出现有移动终端 100 请求下载这个第二应用时，服务器 200 便可将其记录的安全分析结果下发给相应的移动终端 100，可以确保有风险的第二应用不再扩散传播。

在一些实施例中，服务器 200 还可以根据对第二应用的分析，查找与第二应用相同或基本相同的、且安全性可信度更高的替换应用，例如源于官方应用市场的第三应用的 URL 信息，服务器 200 下发第二应用的安全分析结果时，可同时将可替换的第三应用的 URL 信息下发给移动终端 100。

随后，在步骤 405 中，移动终端 100 接收所述安全分析结果，确定是否下载第二应用。

在一些实施例中，移动终端 100 的管理模块中的管控引导单元 121b 接收到所述安全分析结果，可以根据安全分析结果确定第二应用的安全等级，对于安全的第二应用，移动终端 100 的管理模块中的管控引导单元 121b 将安全分析结果经过策略下发单元 121a 和内部管控交互接口 122a 下发给内核防火墙组件 123，内核防火墙组件 123 允许利用 URL 信息请求下载安全的第二应用，同时移动终端 100 可以提示例如“第二应用为安全应用，开始下载”的提示信息；

在一些实施例中，对不安全的第二应用，移动终端 100 向用户提示例如“第二应用不安全，请选择是否继续下载”的提示信息，并获取用户的选择操作输入，移动终端 100 的管控引导单元将用户的选择信息经过策略下发单元 121a 和内部管控交互接口 122a 下发给内核防火墙组件 123a，若用户选择禁止下载，则内核防火墙组件 123a 禁止第一应用下载不安全的第二应用，若用户允许下载，则内核防火墙组件 123a 允许第一应用下载不安全的第二应用；

在一些实施例中，对高危的第二应用，管控引导单元 121b 直接经过策略下发单元 121a 和框架层 102 下发给内核防火墙组件 123，内核防火墙组件 123 直接禁止在第一应用中下载高危的第二应用，同时移动终端 100 向用户提示第二应用为高危应用，已禁止下载的消息，

在一些实施例中，若服务器 200 还下发了可替换的第三应用的 URL 信息，移动终端 100 可以将第三应用的 URL 信息提示用户选择下载安全来源的第三应用，以供用户下载更安全的第三应用。

结合前述实施例，在另一些实施例中，所述方法还可以包括步骤 406~步骤 409。以下结合图 5 进行进一步说明。

在步骤 406 中，移动终端 100 将若干第一应用的应用包名列表上报给服务器 200，其中，所述第一应用可以为系统中已安装的应用。移动终端 100 可以将所有已安装应用的应用包名列表上报给服务器 200。

在步骤 407 中，服务器 200 根据移动终端 100 上报的应用包名列表，确定移动终端 100 中需要监控的第一应用，配置包括需要监控的指定的第一应用的应用包名监控列表和 URL 信息中下载应用请求的识别规则的监控信息，接着，在步骤 408 中，服务器 200 将上述监控信息下发给移动终端 100。

在一些实施例中，服务器 200 的策略服务单元 121a 可以负责监控策略的配置和下发。

其中，步骤 406、步骤 407~步骤 408 之间以及与其他步骤 401~步骤 405 之间并无指定的先后顺序。移动终端 100 可以定期执行步骤 406（例如每周更新一次），或者当移动终端 100 有新的应用安装时，上报已安装应用的应用包名列表，其执行步骤 406 的策略可以具体确定，不做限定；服务器 200 可以定期执行步骤 407~步骤 408，（例如每三天更新一次监控策略，也就是更新管控策略），并向移动终端 100 下发监控信息，也可以在移动终端 100 上报应用包名列表时，配置并下发监控信息。

例如，服务器 200 可以根据移动终端 100 上传的应用包名列表，查询每个应用的应用服务方的安全级别，对于应用服务方的安全级别较高的应用，例如其自身应用中具有较高级别的安全监控功能，例如华为手机管家应用等，则可以不配置到监控信息中，对于应用服务方信息不详或安全级别较低的应用，

则可以选择配置到监控信息中，服务器 200 通过定期更新和下发监控信息，可以提高移动终端 100 的保护效果。其中，应用安全级别高的结果可能来源于权威安全检测机构检测结果，应用安全级别低的可能来源是用户反馈和投诉的不安全应用并经过官方核实的。

然后，在步骤 409 中，移动终端 100 根据指定的第一应用的应用包名监控列表，检测指定的第一应用是否请求访问 URL 信息并检测指定的第一应用所请求访问的 URL 信息中是否包括下载应用请求。

其中，移动终端 100 根据所述指定的第一应用的应用包名监控列表检测应用进程中是否请求访问 URL 信息，若是，则所述移动终端 100 根据 URL 信息识别规则检测该第一应用所请求访问的 URL 信息中是否包括下载应用请求。

在一些实施例中，移动终端 100 的管理模块 121 中的策略下发单元 121a 可以接收所述监控信息，并将所述监控信息通过内部管控交互接口 122a 保存到移动终端 100 的内核防火墙组件中，移动终端 100 的内核防火墙组件 123a 可以接收移动终端 100 的网络流量，并根据所述监控信息监控指定第一应用的应用进程 ID（User ID），并根据所述 URL 信息识别规则检测应用进程 ID 中是否出现下载应用请求。在一些实施例中，URL 信息识别规则可以是，例如 URL 信息为正则表达式，当识别到 URL 信息以".apk"结尾，则确认检测到应用进程 ID 中出现下载应用请求。

相比现有技术中应用中请求下载某一应用时，只会提醒用户是否下载改应用，无法判断应用否安全，也无法对应用外嵌入应用下载安装进行监控和保护，本申请的实施例中移动终端从底层监控所有应用或指定一些应用中请求下载新应用的行为，将该行为上报给服务器查询该新应用的安全分析结果，然后移动终端根据服务器下发的安全分析结果对下载行为进行相应保护处理，从而实现从底层对所有应用或指定一些应用的新应用下载行为进行有效健康和保护；进一步地，当服务器接收到全网移动终端首次上报的某一新应用的下载请求时，根据下载请求的 URL 信息从应用服务器下载该新应用到服务器中进行安全分析并记录安全分析结果，从而实现服务器端对网络应用的安全监控的及时更新，进一部提高移动终端对应用安装的防护效果。

图 6 示出本申请一具体实施例中实现应用下载监控的场景流程示意图，以下以移动终端 100，服务器 200 为官方服务器为例，以手机为例，进行具体说明。

1. 手机管家模块上报本手机上已安装的应用包名列表信息；

2. 服务器（官方服务器）结合已安装的应用包名列表及服务器配置下发拦截策略（即监控策略）；

3. 手机管家模块将拦截策略通过 framework 下发配置到手机内核防火墙组件（即防火墙）上；

4. 手机获取用户在某个应用中点击了下载链接；

5. 防火墙进行策略匹配，判断访问的 URL，匹配是否含有下载应用请求；

6. 匹配成功，则防火墙上报要访问的 URL 信息，同时阻塞本次请求；

7. framework 上报匹配到的 URL 信息；

8. 手机管家模块向 URL_Analyser 上报匹配到的 URL 信息；

9. URL_Analyser 进行后台匹配，获取匹配结果，对于需要替换的，获取并提供官方应用市场的 URL 地址，对于恶意应用给出恶意分析结果，对于新上报的 URL 信息需要对此 URL 信息进行请求并下载，并对应用进行自动化安全检测，并对检测结果进行入库；

10. URL_Analyser 匹配成功，确定需要拦截此下载请求，将此响应结果返回到手机；

11. 手机弹框提示用户进行替换下载或继续下载，用户进行选择；

12. 手机获取到用户选择继续下载的操作，则手机管家将选择结果通知到系统内核防火墙，内核防火墙放通 URL 请求；

13. 手机获取到用户选择在官方应用市场下载的操作，手机管家跳转到官方应用市场下载相应的应

用；

14. 手机管家通知内核防火墙进行拒绝本次 URL 请求；

15. 内核防火墙将拒绝响应消息通知到第一应用；

16. 手机管家跳转到官方应用市场的应用市场的应用详情页面；

17. 官方应用市场进行应用的下载流程；

18. 官方应用市场进行下载流程；

19. 官方应用市场进行应用安装流程。

在上述过程中，底层的防火墙在下载过程中，识别到 URL 为下载 APK 应用安装包，则暂停下载，并通过 framwork 上报到手机管家，手机管家模块将该 URL 上报到服务器，如果服务器没有记录该 URL 则立刻返回通知底层的防火墙继续下载。

同时服务器下载该 URL 并分析该应用包名，并搜索应用市场相同应用，如果应用市场有同样应用，则记录该 URL 对应应用市场的应用。当本移动终端或其他移动终端再次请求下载该 URL，服务器可以返回应用市场下载地址 URL2，手机管家模块可以弹出提示，让用户判断是否到应用市场下载，例如可以进行倒计时计数 10 秒获取选择输入。

如果移动终端获取到用户选择到应用市场下载的操作输入，则下发命令，通知防火墙停止下载该应用，同时手机管家模块发送一个消息，将 URL2 传递给应用市场，应用市场启动该 URL2 下载该应用并提醒用户安装。如果超时 10 秒未获得选择输入，则底层的防火墙继续下载。如果用户选择原来地址继续下载，则立刻返回防火墙继续下载。

如果移动终端获取到用户选择到应用市场下载的操作输入，但是应用市场未安装，则手机管家模块可以弹出提示，让用户安装应用市场，如果获取到用户选择安装应用市场的操作输入，则安装相应的应用市场后，将 URL2 发送给应用市场再次进行下载安装。如果获取到用户选择不安装应用市场的操作输入，则提示本次下载失败。

在一些实施例中，服务器配置的监控信息可以不包括监控应用市场，因此防火墙对于应用市场来源的 URL 下载不会上报拦截管控。

在另一些实施例中，如果对于移动终端上报的从应用市场 URL 的请求的应用下载信息，服务器可以识别并返回直接下载结果，也可以不弹出提示。

以下结合图 3、图 7~图 13 对移动终端在实现应用下载监控的交互过程，进行进一步说明。

结合图 3 中终端管理员用户通过接口 IF0 设置是否启动未知来源应用下载监控和保护，如图 7 和图 8 所示，移动终端 100 获取用户选择进入设置 501 的操作，进入设置界面，在设置界面获取用户开启监控未知来源应用下载 502 的操作。

如图 9 所示，当移动终端 100 获取到用户选择进入浏览器 503，移动终端 100 开启浏览器 503 的应用界面；如图 10 所示，当移动终端 100 检测到用户在浏览器 503 的应用界面中选择的下载播放器 504 的操作后，显示提示界面 505，提示“即将下载播放器，正在进行安全分析”，移动终端 100 在后台将请求下载该播放器的 URL 信息发送给服务器 200；如图 11 所示，移动终端 100 获取到服务器 200 返回的安全分析结果后，如果移动终端 100 确定播放器为不安全应用，即存在安全风险的应用，则显示提示界面 506，提示“检测到播放器为不安全应用，是否继续下载”，以供用户选择是否继续下载，移动终端 100 在提示界面 506 也可以同时提供官方版本应用的下载选项 507；如图 12 所示，如果移动终端 100 确定播放器为高风险应用，例如携带病毒等，则弹出提示界面 508，提示“已禁止下载”，同时移动终端 100 在底层内核防火墙组件 123 中禁止下载播放器应用，移动终端 100 还可以在弹出提示界面 508 中同时提供官方版本应用的下载选项，并根据用户对下载选项的选中操作前往下载；如图 13 所示，如果移动终端

100 确定播放器为安全应用，移动终端 100 可以允许下载播放器并弹出提示界面 509，提示例如“正在下载播放器…”。

因此，移动终端 100 能够根据用户的选择开启未知来源应用下载监控和保护的功能，在开启之后，监控过程不限于某个具体的应用方提供的应用下载安全监控，而是移动终端 100 能够从系统级别提供应用下载保护机制，当出现来源下载应用请求时，移动终端 100 能够通过云端检测与系统内核防火墙结合，选择禁止、允许下载或根据用户选择确定是否下载，提高保护效果的同时交互过程为用户可见，界面友好，易用性好。

在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时，全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如同轴电缆、光纤、数字用户线（DSL））或无线（例如红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质，(例如，软盘、硬盘、磁带)、光介质(例如，DVD)、或者半导体介质（例如固态硬盘 Solid State Disk (SSD)）等。

本申请实施例可以根据上述方法示例对设备进行功能模块的划分，例如，可以对应各个功能划分各个功能模块，也可以将两个或两个以上的功能集成在一个处理模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。本申请实施例中对模块的划分是示意性的，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将移动设备的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。上述描述的系统，移动设备和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

综上所述，以上实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照上述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对上述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的精神和范围。

权利要求

1. 一种应用下载监控方法，其中，所述方法包括：

移动终端监控多个第一应用所请求访问的 URL 信息是否包括下载应用请求；

当检测到所述多个第一应用中任一应用所请求访问的 URL 信息中包括下载应用请求时，所述移动终端阻塞所述下载应用请求，并将所述 URL 信息发送给服务器；

所述服务器根据所述 URL 信息中的下载应用请求，查询是否已有所述下载应用请求对应的第二应用的安全分析结果，若查询到，则所述服务器将所述安全分析结果发送给所述移动终端；

所述移动终端根据所述安全分析结果，确定是否下载所述第二应用。

2. 根据权利要求 1 所述的方法，其中，所述方法还包括：

所述移动终端将已安装应用的应用包名列表发送给所述服务器；

所述服务器根据所述应用包名列表，配置监控信息并发送给所述移动终端，所述监控信息包括需要监控的所述多个第一应用的应用包名列表和识别 URL 信息中下载应用请求的规则；

所述移动终端监控多个第一应用中任一应用所请求访问的 URL 信息是否包括下载应用请求的步骤包括：

所述移动终端根据所述监控信息，检测所述需要监控的所述多个第一应用中任一应用所请求访问的 URL 信息是否包括下载应用请求。

3. 一种在移动终端侧实现的应用下载监控的方法，其中，所述方法包括：

移动终端监控多个第一应用所请求访问的 URL 信息是否包括下载应用请求；

当所述移动终端检测到所述多个第一应用中任一应用所请求访问的 URL 信息中包括下载应用请求时，所述移动终端阻塞所述下载应用请求，并将所述 URL 信息发送给服务器；

所述移动终端接收所述服务器发送的安全分析结果，其中，所述安全分析结果为所述服务器根据所述 URL 信息中的下载应用请求，查询到的对应第二应用的安全分析结果；

所述移动终端根据所述安全分析结果，确定是否下载所述第二应用。

4. 根据权利要求 3 所述的方法，其中，所述方法还包括：

所述移动终端将已安装应用的应用包名列表发送给所述服务器；

所述移动终端接收所述服务器发送的监控信息，所述监控信息包括需要监控的所述多个第一应用的应用包名列表和识别 URL 信息中下载应用请求的规则；

所述移动终端监控多个第一应用中任一应用所请求访问的 URL 信息是否包括下载应用请求的步骤包括：

所述移动终端根据所述监控信息，检测所述需要监控的所述多个第一应用中任一应用所请求访问的 URL 信息是否包括下载应用请求。

5. 根据权利要求 4 所述的方法，其中，所述移动终端根据所述监控信息，检测所述需要监控的所述多个第一应用任一应用所请求访问的 URL 信息是否包括下载应用请求的步骤包括：

所述移动终端根据需要监控的所述多个第一应用的应用包名列表检测所述多个第一应用是否请求访问 URL 信息；

当检测到所述多个第一应用中任一应用请求访问 URL 信息，所述移动终端根据所述识别 URL 信息中下载应用请求的规则检测该第一应用所请求访问的 URL 信息中是否包括下载应用请求。

6. 根据权利要求 3 至 5 中任一项所述的方法，其中，所述移动终端根据所述安全分析结果，确定是否下载所述第二应用的步骤包括：

所述移动终端根据所述安全分析结果，确定直接禁止下载所述第二应用、根据用户选择输入确定

是否下载所述第二应用或直接允许下载所述第二应用。

7. 根据权利要求 6 所述的方法，其中，当所述移动终端确定根据用户选择输入确定是否下载所述第二应用，所述方法还包括：

所述移动终端显示待选择的提示界面，并获取用户的选择操作；

根据所述选择操作，确定禁止或允许下载所述第二应用。

8. 根据权利要求 6 或 7 所述的方法，其中，当所述移动终端确定禁止下载所述第二应用，所述方法还包括以下至少任一步骤：

所述移动终端显示已禁止下载所述第二应用的提示界面；

所述移动终端提示与所述第二应用相关的第三应用的下载信息，并获取用户根据所述第三应用的下载信息所选择的下载操作，下载所述第三应用。

9. 一种在服务器侧实现的应用下载监控的方法，其中，所述方法包括：

服务器接收移动终端发送的多个第一应用中任一应用所请求访问的 URL 信息，其中，所述 URL 信息包括下载应用请求；

所述服务器根据所述 URL 信息中的下载应用请求，查询是否已有所述下载应用请求对应的第二应用的安全分析结果，若查询到，则所述服务器将所述安全分析结果发送给所述移动终端。

10. 根据权利要求 9 所述的方法，其中，所述方法还包括：

所述服务器接收所述移动终端的已安装应用的应用包名列表；

所述服务器根据所述应用包名列表，配置监控信息并发送给所述移动终端，其中，所述监控信息包括需要监控的所述多个第一应用的应用包名列表和识别 URL 信息中下载应用请求的规则。

11. 根据权利要求 10 所述的方法，其中，所述方法还包括：

若所述服务器未查询到所述下载应用请求对应的第二应用的安全分析结果，则所述服务器根据所述 URL 信息请求下载所述第二应用，下载后对所述第二应用进行安全分析并记录安全分析结果。

12. 根据权利要求 10 或 11 所述的方法，其中，所述方法还包括：

若所述服务器未查询到所述下载应用请求对应的第二应用的安全分析结果，则所述服务器通知所述移动终端允许下载所述第二应用。

13. 一种实现应用下载监控的移动终端，其中，所述移动终端包括：

内核防火墙组件，用于监控多个第一应用所请求访问的 URL 信息是否包括下载应用请求，并在检测到所述多个第一应用中任一应用所请求访问的 URL 信息中包括下载应用请求时，阻塞所述下载应用请求；

管控引导单元，用于将所述 URL 信息发送给服务器、接收所述服务器发送的安全分析结果并发送所述内核防火墙组件，其中，所述安全分析结果为所述服务器根据所述 URL 信息中的下载应用请求，查询到的对应第二应用的安全分析结果；

所述内核防火墙组件还用于所述安全分析结果确定是否下载所述第二应用。

14. 根据权利要求 13 所述的移动终端，其中，

所述管控引导单元还用于将已安装应用的应用包名列表发送给所述服务器；

所述移动终端还包括：

策略下发单元，用于接收所述服务器发送的监控信息并发送给所述内核防火墙组件，所述监控信息包括需要监控的所述第一应用的应用包名列表和识别 URL 信息中下载应用请求的规则；

所述内核防火墙组件用于根据所述监控信息检测到第一应用中任一应用所请求访问的 URL 信息中是否包括下载应用请求。

15. 一种在实现应用下载监控的服务器，其中，所述服务器包括：

数据存储单元，用于存储第二应用的安全分析结果；

URL 分析单元，用于接收到移动终端发送的多个第一应用中任一应用所请求访问的 URL 信息，并根据所述 URL 信息中的下载应用请求，查询是否已有所述下载应用请求对应的所述第二应用的安全分析结果，若查询到，则将所述安全分析结果发送给所述移动终端，其中，所述 URL 信息包括下载应用请求。

16. 根据权利要求 15 所述的服务器，其中，

所述 URL 分析单元，还用于接收所述移动终端的已安装应用的应用包名列表；

所述服务器还包括：

策略服务单元，用于根据所述应用包名列表，配置监控信息并发送给所述移动终端，其中，所述监控信息包括需要监控的所述多个第一应用的应用包名列表和识别 URL 信息中下载应用请求的规则。

17. 一种实现应用下载监控的移动终端，其中，所述移动终端包括：

至少一个处理器；

至少一个存储器，所述至少一个存储器包括若干指令；

所述至少一个处理器执行所述若干指令使所述移动终端至少执行如下步骤：

监控多个第一应用所请求访问的 URL 信息是否包括下载应用请求；

当检测到所述多个第一应用中任一应用所请求访问的 URL 信息中包括下载应用请求时，阻塞所述下载应用请求，并将所述 URL 信息发送给服务器；

接收所述服务器发送的安全分析结果，其中，所述安全分析结果为所述服务器根据所述 URL 信息中的下载应用请求，查询到的对应第二应用的安全分析结果；

根据所述安全分析结果，确定是否下载所述第二应用。

18. 根据权利要求 17 所述的移动终端，其中，所述至少一个处理器执行所述若干指令使所述终端还执行如下步骤：

将已安装应用的应用包名列表发送给所述服务器；

接收所述服务器发送的监控信息，所述监控信息包括需要监控的所述多个第一应用的应用包名列表和识别 URL 信息中下载应用请求的规则；

在所述监控多个第一应用中任一应用所请求访问的 URL 信息是否包括下载应用请求的步骤中，所述至少一个处理器执行所述若干指令使所述终端至少执行如下步骤：

根据所述监控信息，检测所述需要监控的所述多个第一应用中任一应用所请求访问的 URL 信息是否包括下载应用请求。

19. 根据权利要求 18 所述的移动终端，其中，在所述移动终端根据所述监控信息，检测所述需要监控的所述多个第一应用任一应用所请求访问的 URL 信息是否包括下载应用请求的步骤中，所述至少一个处理器执行所述若干指令使所述终端至少执行如下步骤：

根据需要监控的所述多个第一应用的应用包名列表检测所述多个第一应用是否请求访问 URL 信息；

当检测到所述多个第一应用中任一应用请求访问 URL 信息，根据所述识别 URL 信息中下载应用请求的规则检测该第一应用所请求访问的 URL 信息中是否包括下载应用请求。

20. 根据权利要求 17 至 19 中任一项所述的移动终端，其中，在根据所述安全分析结果，确定是否下载所述第二应用的步骤中，所述至少一个处理器执行所述若干指令使所述终端至少执行如下步骤：

根据所述安全分析结果，确定直接禁止下载所述第二应用、根据用户选择输入确定是否下载所述第二应用或直接允许下载所述第二应用。

21. 根据权利要求 20 所述的移动终端，其中，所述移动终端还包括触摸屏；

在根据用户选择输入确定是否下载所述第二应用的步骤中，所述至少一个处理器执行所述若干指令使所述终端至少执行如下步骤：

使所述触摸屏显示待选择的提示界面，并获取用户的选择操作；

根据所述选择操作，确定禁止或允许下载所述第二应用。

22. 根据权利要求 20 或 21 所述的移动终端，其中，所述移动终端还包括触摸屏；

在确定禁止下载所述第二应用的步骤之后，所述至少一个处理器执行所述若干指令使所述终端至少执行如下至少一个步骤：

使所述触摸屏显示已禁止下载所述第二应用的提示界面；

使所述触摸屏提示与所述第二应用相关的第三应用的下载信息并获取用户根据所述第三应用的下载信息所选择的下载操作，其后，下载所述第三应用。

23. 一种实现应用下载监控的服务器，其中，所述服务器包括：

至少一个处理器；

至少一个存储器，所述至少一个存储器包括若干指令；

所述至少一个处理器执行所述若干指令使所述服务器至少执行如下步骤：

接收移动终端发送的多个第一应用中任一应用所请求访问的 URL 信息，其中，所述 URL 信息包括下载应用请求；

根据所述 URL 信息中的下载应用请求，查询是否已有所述下载应用请求对应的第二应用的安全分析结果，若查询到，则将所述安全分析结果发送给所述移动终端。

24. 根据权利要求 23 所述的服务器，其中，所述至少一个处理器执行所述若干指令使所述服务器还执行如下步骤：

接收所述移动终端的已安装应用的应用包名列表；

根据所述应用包名列表，配置监控信息并发送给所述移动终端，所述监控信息包括需要监控的所述多个第一应用的应用包名列表和识别 URL 信息中下载应用请求的规则。

25. 根据权利要求 24 所述的服务器，其中，所述至少一个处理器执行所述若干指令使所述服务器还执行如下步骤：

若未查询到所述下载应用请求对应的第二应用的安全分析结果，则根据所述 URL 信息请求下载所述第二应用，下载后对所述第二应用进行安全分析并记录安全分析结果。

26. 根据权利要求 24 或 25 所述的服务器，其中，所述至少一个处理器执行所述若干指令使所述服务器还执行如下步骤：

若未查询到所述下载应用请求对应的第二应用的安全分析结果，则通知所述移动终端允许下载所述第二应用。

27. 一种显示在移动终端的触摸屏中的图形用户界面（GUI），其中，所述图形用户界面包括：

在所述触摸屏中显示第一 GUI；

响应于检测到用户执行操作所触发的所述多个第一应用中任一应用所请求访问的 URL 信息中包括下载应用请求时，将所述 URL 信息发送给服务器；

响应于接收到服务器根据所述 URL 信息发送的第二应用的安全分析结果确定的直接禁止下载所述第二应用、根据用户选择输入确定是否下载所述第二应用或直接允许下载所述第二应用，显示第二 GUI，所述第二 GUI 包括：提示已禁止下载所述第二应用、根据用户选择输入确定是否下载所述第二应用或已允许下载所述第二应用的界面；

响应于确定需根据用户选择输入确定是否下载所述第二应用，响应于用户输入的选择操作，确定禁止或允许下载所述第二应用。

28. 根据权利要求 27 所述的图形用户界面，其中，所述图形用户界面还包括：

响应于确定禁止下载所述第二应用，所述第二 GUI 还包括：

提示与所述第二应用相关的第三应用的下载信息的界面；

响应于获取用户根据所述第三应用的下载信息所选择的下载操作，下载所述第三应用，并显示第三 GUI，所述第三 GUI 包括提示已下载第三应用的界面。

29. 一种计算机程序产品，其中，当所述计算机程序产品在移动终端上运行时，使得所述移动终端执行如权利要求 3-8 中任一项所述的方法。

30. 一种计算机程序产品，其中，当所述计算机程序产品在服务器上运行时，使得所述移动终端执行如权利要求 9-12 中任一项所述的方法。

31. 一种计算机可读存储介质，包括指令，其中，当所述指令在移动终端上运行时，使得所述移动终端执行如权利要求 3-8 中任一项所述的方法。

32. 一种计算机可读存储介质，包括指令，其中，当所述指令在服务器上运行时，使得所述服务器执行如权利要求 9-12 中任一项所述的方法。

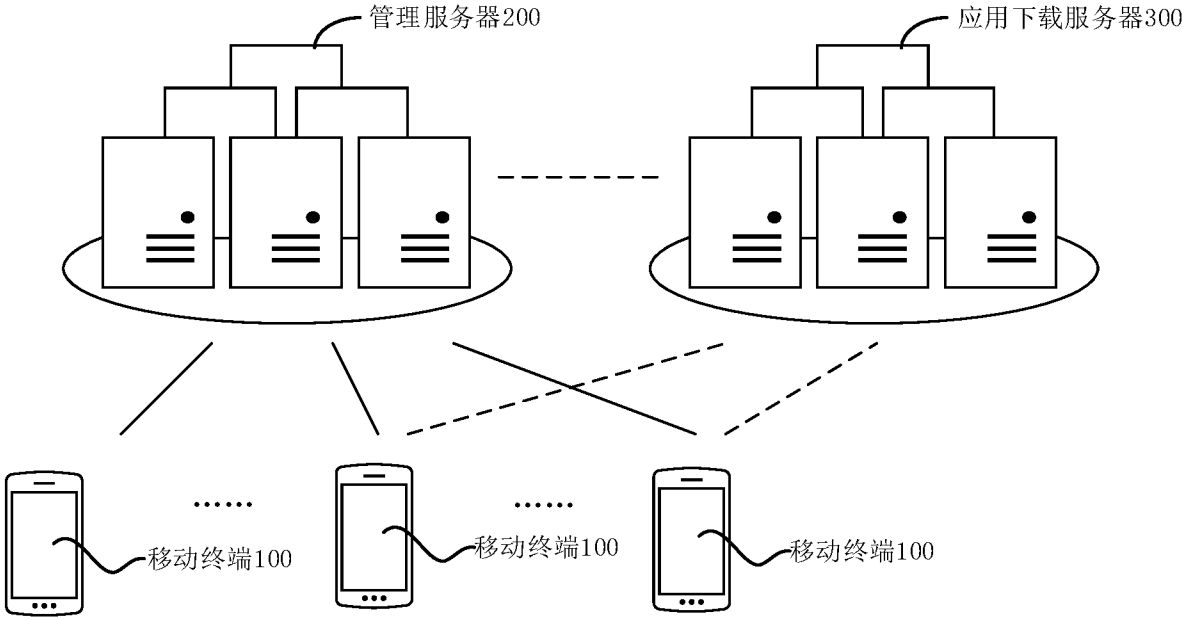

图 1

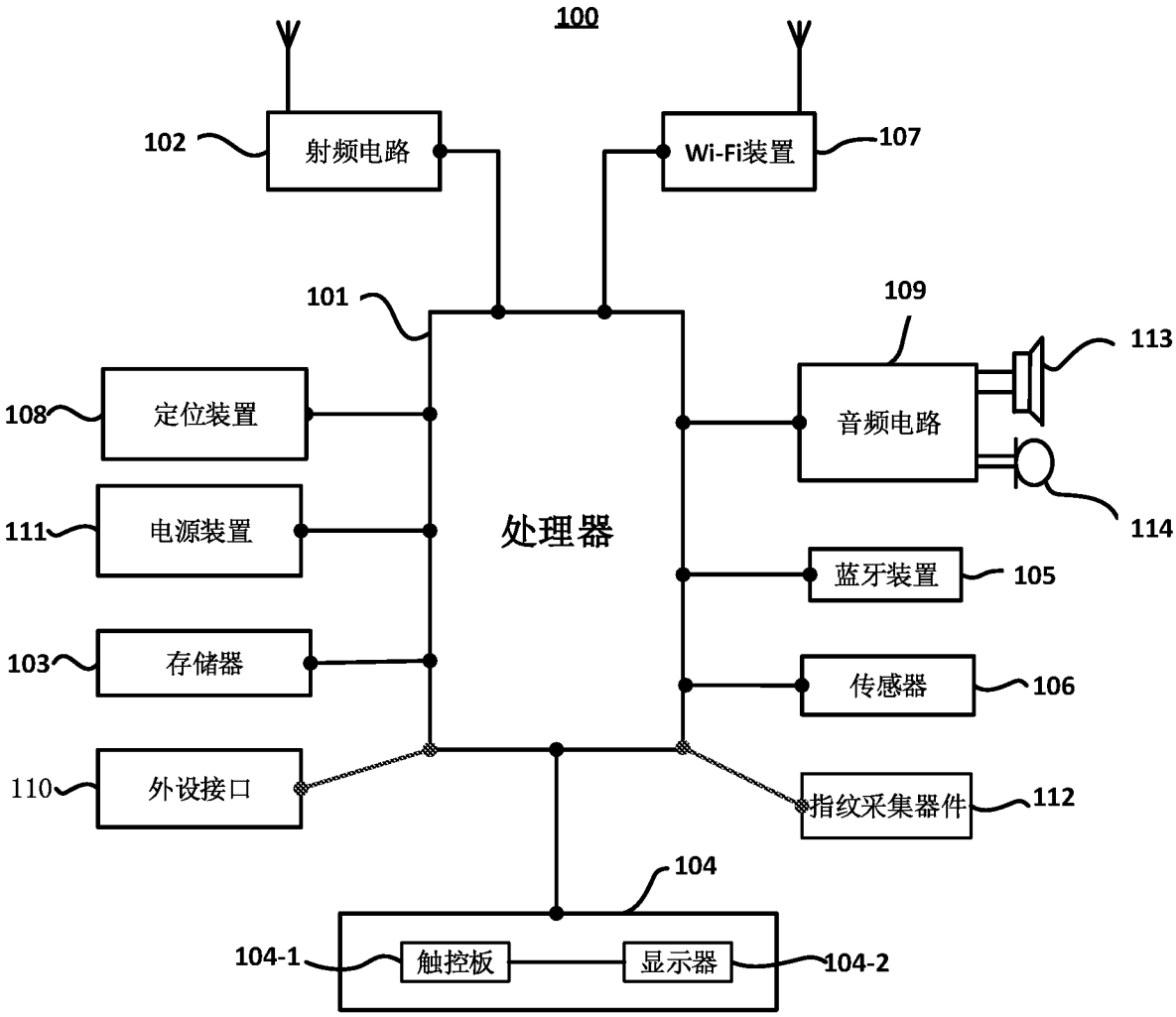
100
102
射频电路
Wi-Fi装置
107
101
109
113
108
定位装置
音频电路
处理器
111
电源装置
114
蓝牙装置
105
103
存储器
传感器
106
110
外设接口
指纹采集器件
112
104
104-1
触控板
显示器
104-2

图 2

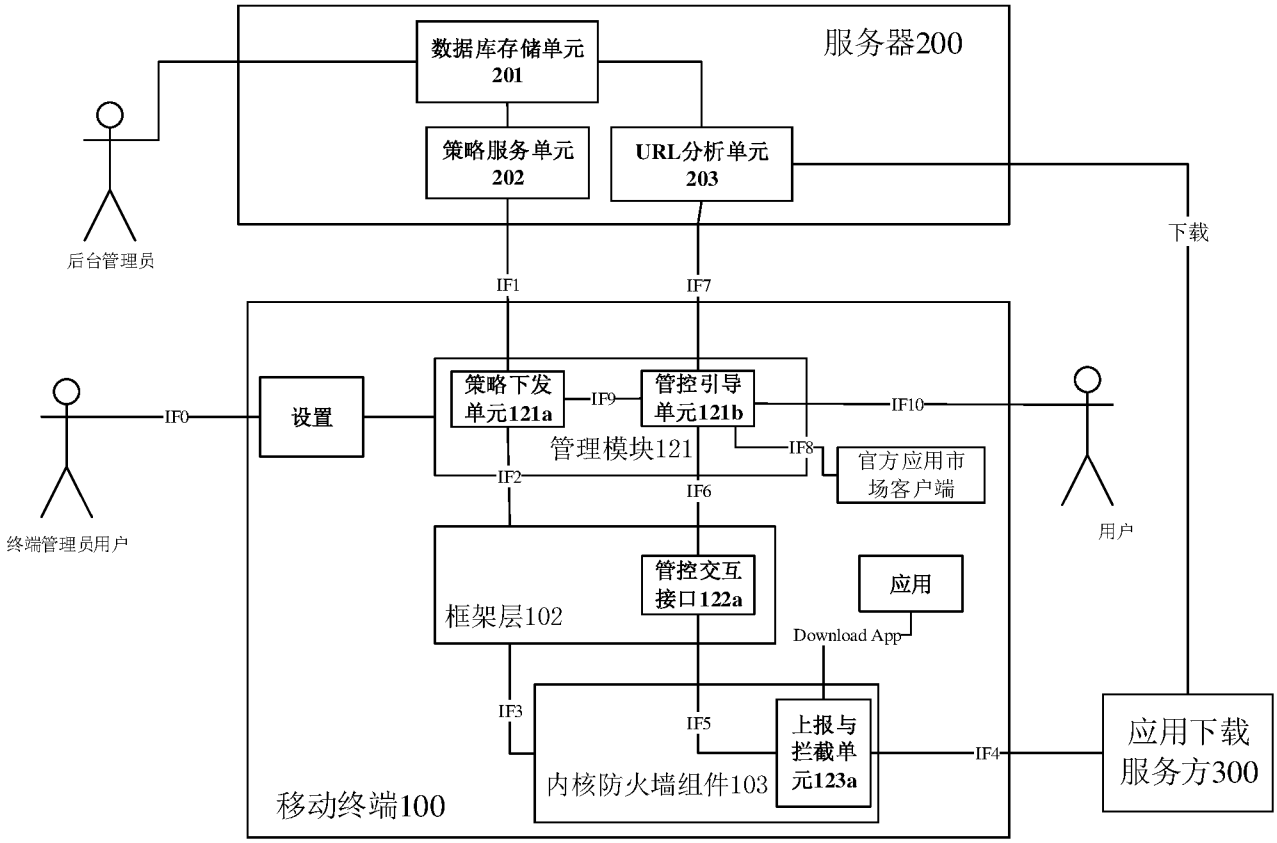
服务器200
数据库存储单元
201
策略服务单元
202
URL分析单元
203
后台管理员
下载
IF1
IF7
IF0
设置
策略下发
单元121a
IF9
管控引导
单元121b
IF10
管理模块121
IF8
官方应用市
场客户端
IF2
IF6
终端管理员用户
用户
管控交互
接口122a
应用
框架层102
Download App
IF3
IF5
上报与
拦截单
元123a
IF4
应用下载
服务方300
内核防火墙组件103
移动终端100

图 3

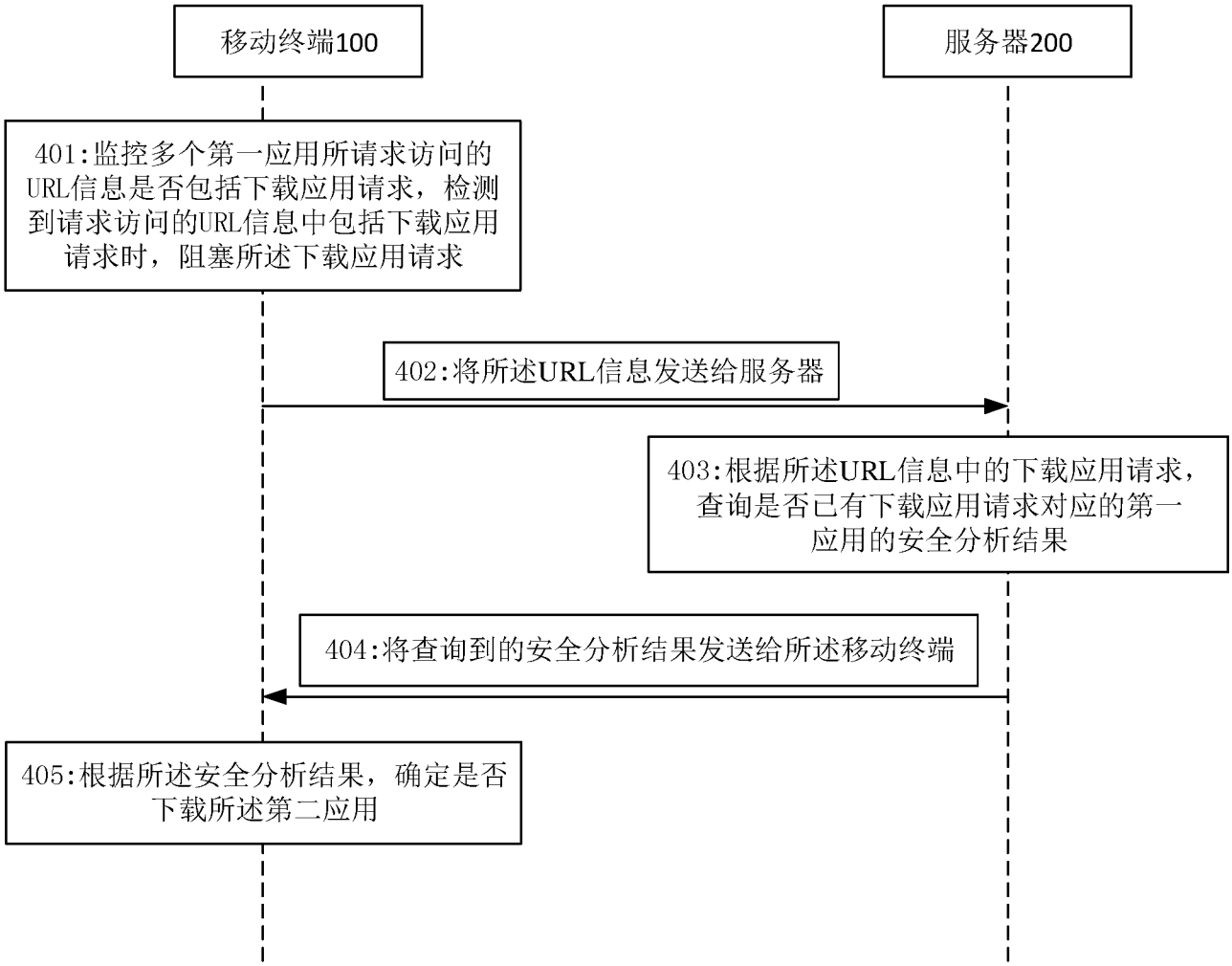
移动终端100
服务器200
401:监控多个第一应用所请求访问的URL信息是否包括下载应用请求，检测到请求访问的URL信息中包括下载应用请求时，阻塞所述下载应用请求
402:将所述URL信息发送给服务器
403:根据所述URL信息中的下载应用请求，查询是否已有下载应用请求对应的第一应用的安全分析结果
404:将查询到的安全分析结果发送给所述移动终端
405:根据所述安全分析结果，确定是否下载所述第二应用

图 4

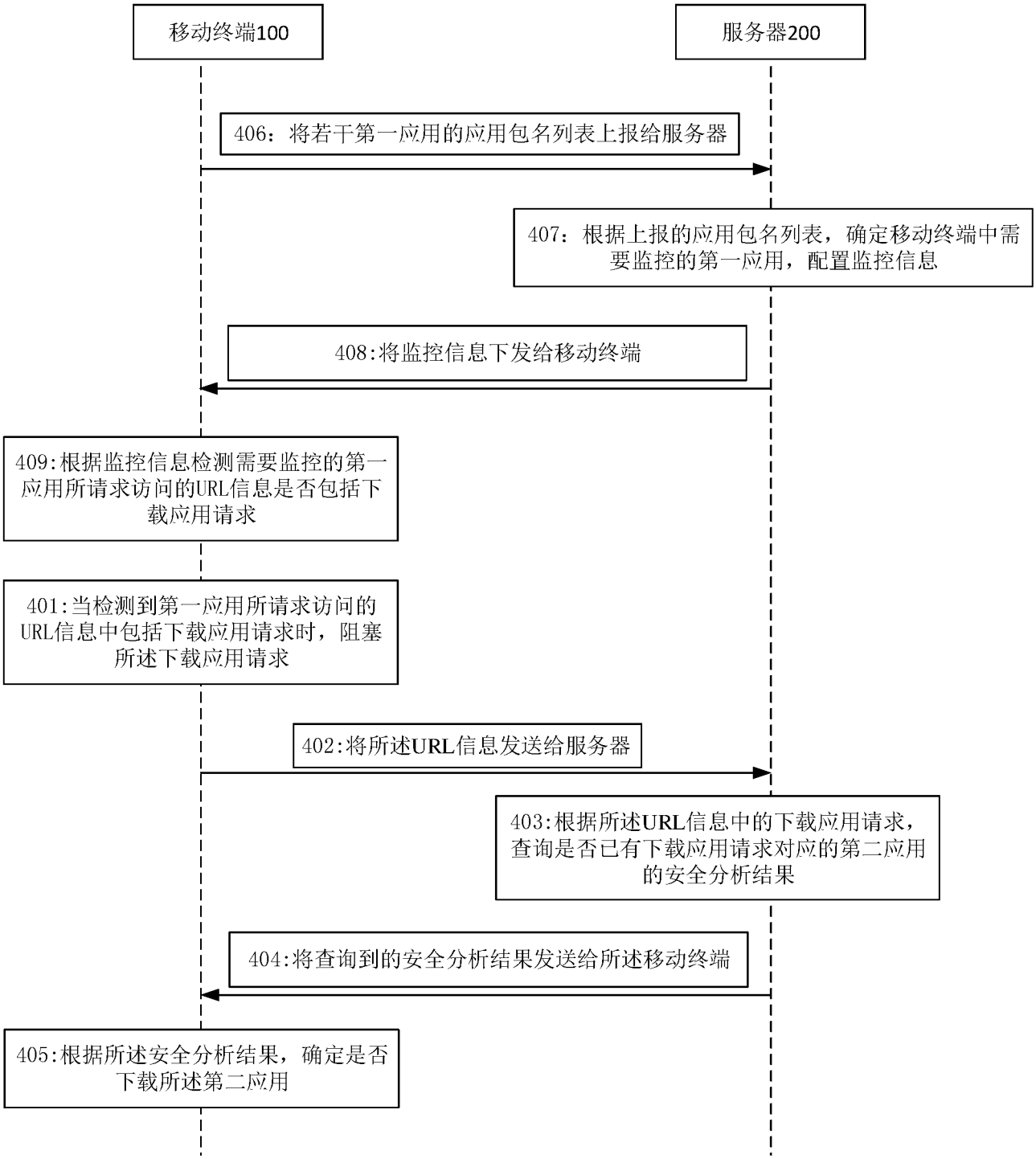
移动终端100
服务器200
406：将若干第一应用的应用包名列表上报给服务器
407：根据上报的应用包名列表，确定移动终端中需要监控的第一应用，配置监控信息
408:将监控信息下发给移动终端
409:根据监控信息检测需要监控的第一应用所请求访问的URL信息是否包括下载应用请求
401:当检测到第一应用所请求访问的URL信息中包括下载应用请求时，阻塞所述下载应用请求
402:将所述URL信息发送给服务器
403:根据所述URL信息中的下载应用请求，查询是否已有下载应用请求对应的第二应用的安全分析结果
404:将查询到的安全分析结果发送给所述移动终端
405:根据所述安全分析结果，确定是否下载所述第二应用

图 5

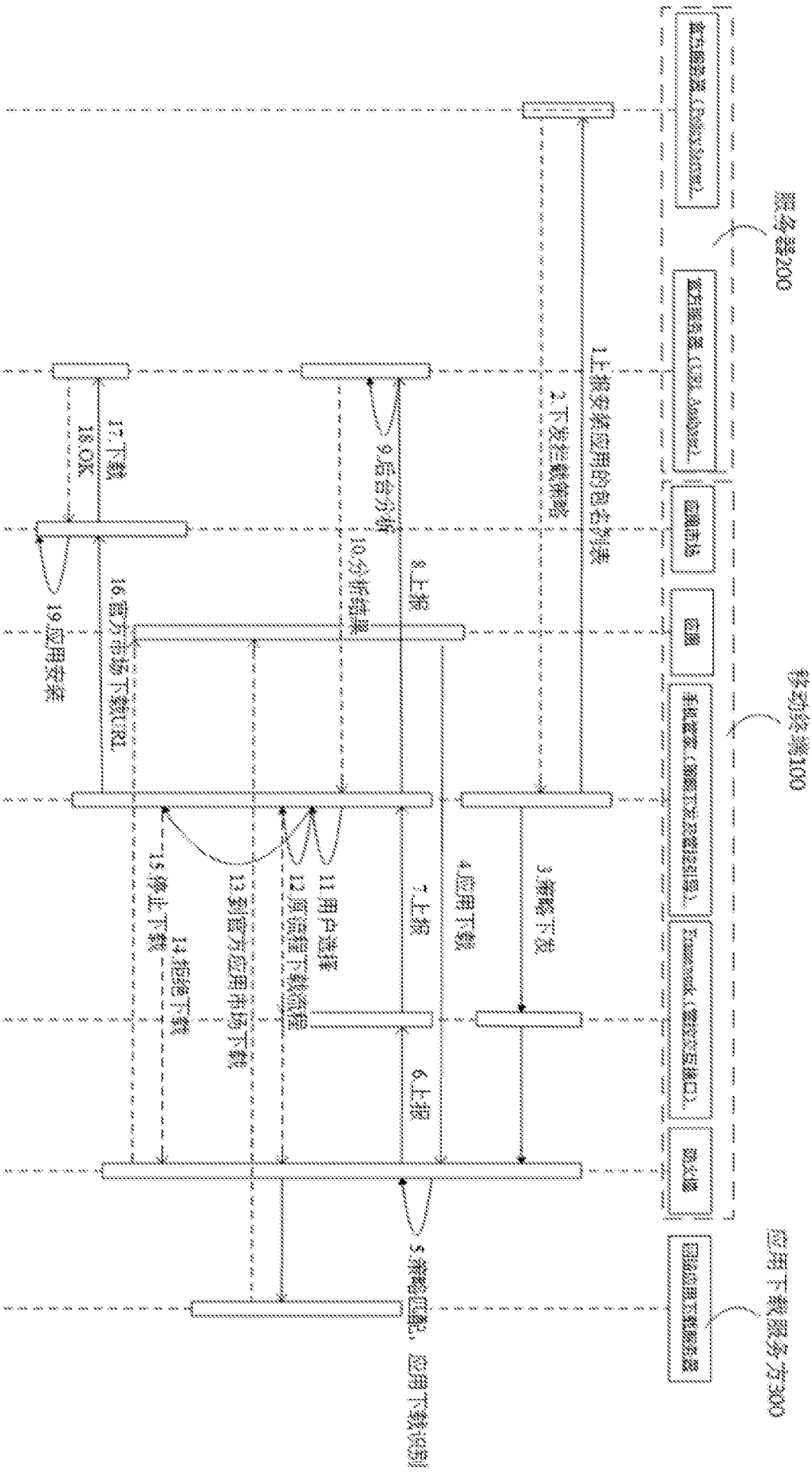
服务器200
移动终端100
应用下载服务方300
1.上报安装应用的包名列表
2.下发控制策略
3.策略下发
4.应用下载
5.策略匹配，应用下载识别
6.上报
7.上报
8.上报
9.后台分析
10.分析结果
11.用户选择
12.原流程下载流程
13.到官方应用市场下载
14.拒绝下载
15.停止下载
16.官方市场下载URL
17.下载
18.OK
19.应用安装

图 6

图 7

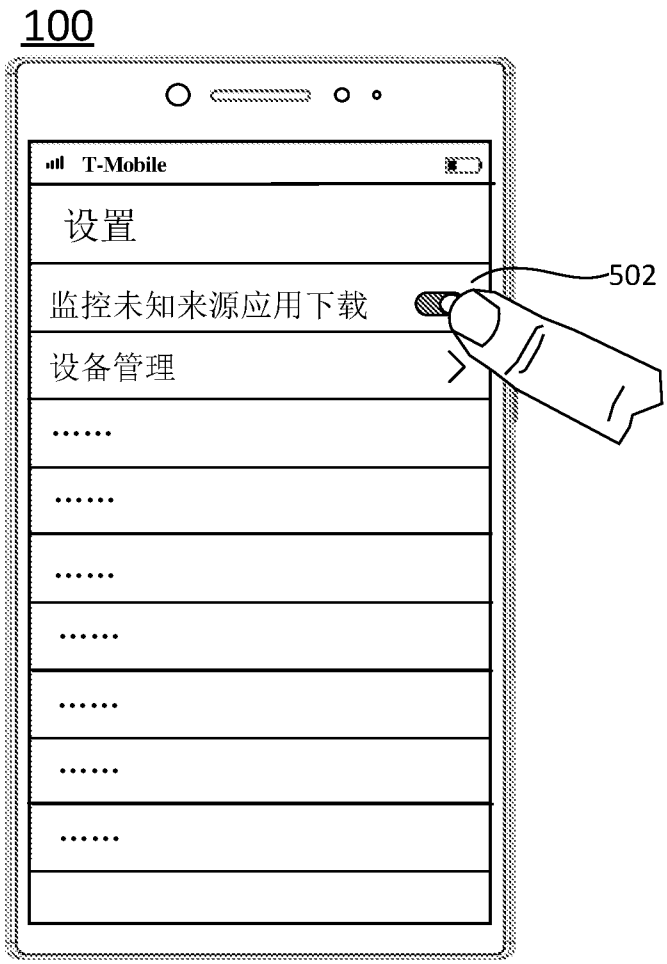

图 8

图 9

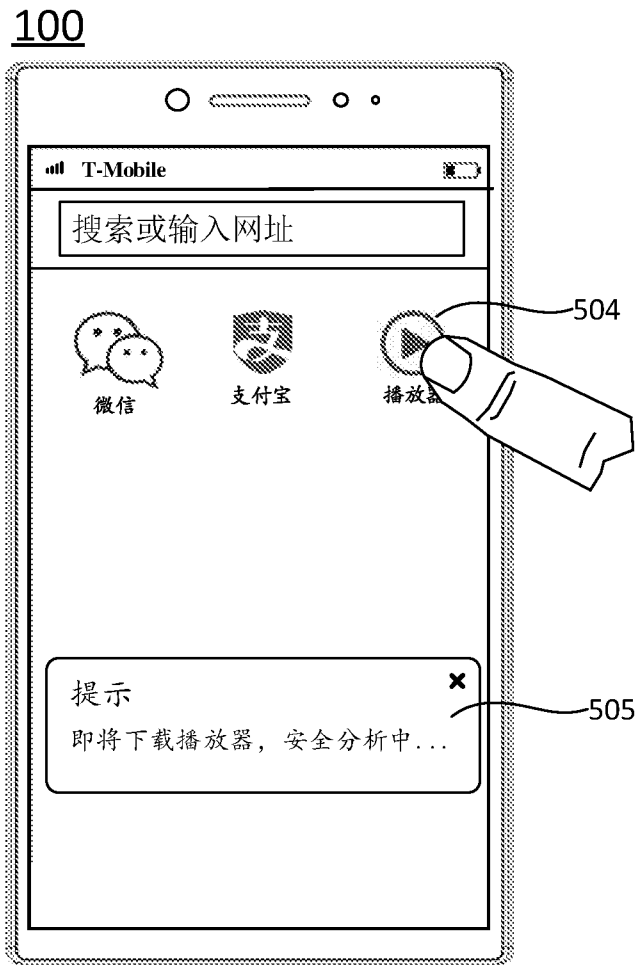

图 10

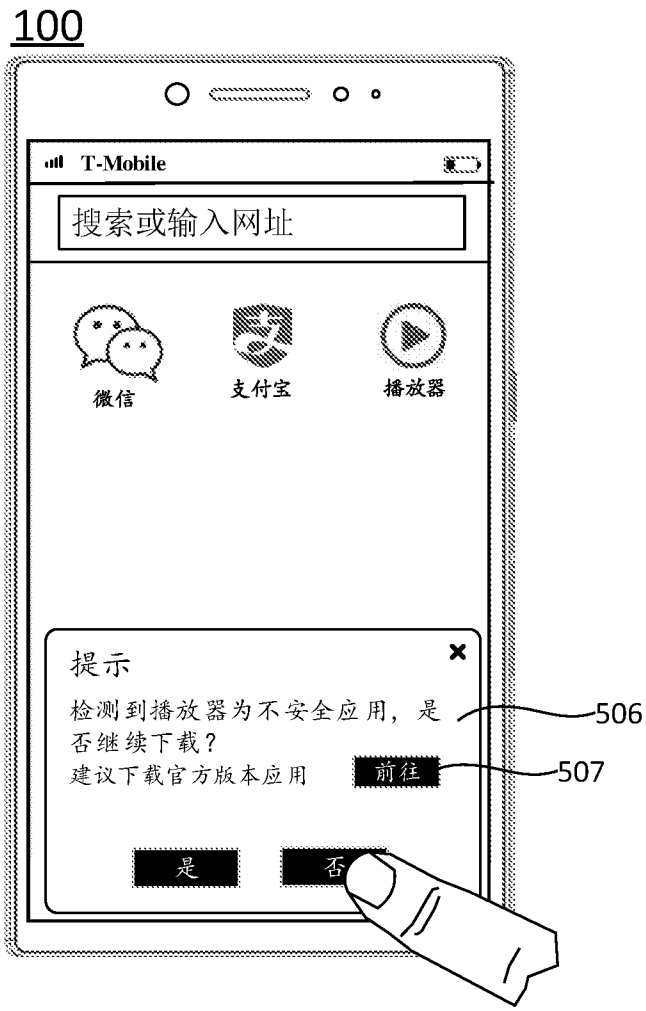
100
T-Mobile
搜索或输入网址
微信
支付宝
播放器
提示
检测到播放器为不安全应用，是否继续下载？
建议下载官方版本应用
前往
是
否
506
507

图 11


100
T-Mobile
搜索或输入网址
微信
支付宝
播放器
提示
检测到播放器携带病毒，已禁止下载。
建议下载官方版本应用
前往
508

图 12

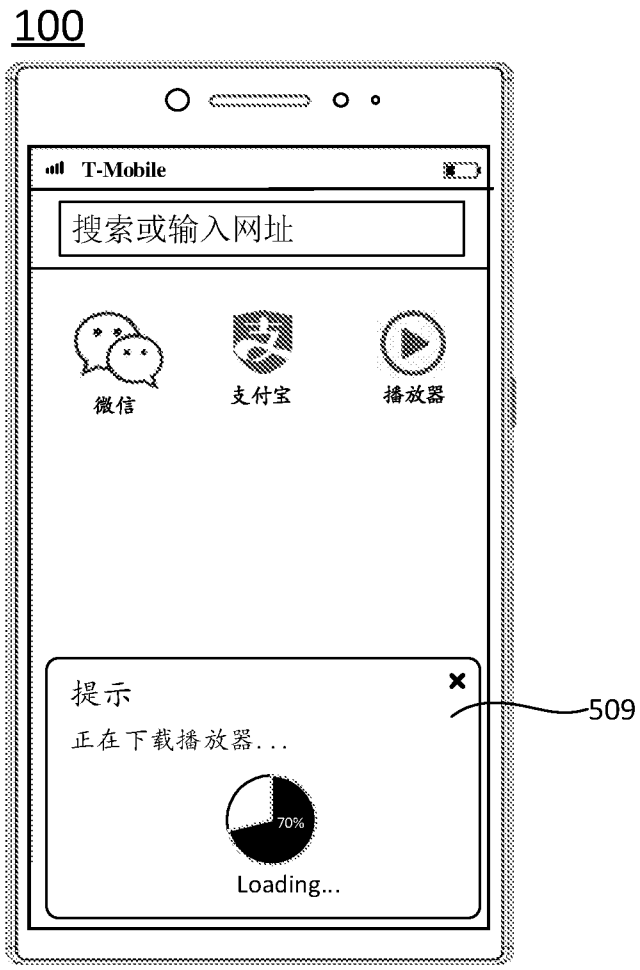

图 13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/090077

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/12 (2009.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; SIPOABS; CNTXT; DWPI; CNKI: 应用, 程序, 访问, 下载, 统一资源定位, 安全, 阻止, 拦截, 阻塞, application, program, app, access, download, URL, safety, prevent, intercept

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103442361 A (NETQIN MOBILE INC.), 11 December 2013 (11.12.2013), description, paragraphs [0033]-[0070]	1-32
A	CN 104253791 A (HUAWEI DEVICE CO., LTD.), 31 December 2014 (31.12.2014), entire document	1-32
A	CN 102946377 A (ZHUHAI JUNTIAN ELECTRONIC TECHNOLOGY CO., LTD.), 27 February 2013 (27.02.2013), entire document	1-32
A	US 2003055924 A1 (MATSUGATANI, K.), 20 March 2003 (20.03.2003), entire document	1-32

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
08 August 2017	21 August 2017
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer LIU, Fang Telephone No. (86-10) 62089108

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/090077

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103442361 A	11 December 2013	CN 103442361 B	25 January 2017
CN 104253791 A	31 December 2014	US 2016125185 A1	05 May 2016
		WO 2014206223 A1	31 December 2014
		EP 2999188 A1	23 March 2016
CN 102946377 A	27 February 2013	None	
US 2003055924 A1	20 March 2003	JP 2003092639 A	28 March 2003

国际检索报告

国际申请号 PCT/CN2017/090077

A. 主题的分类

H04W 12/12(2009.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04W, H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNABS;SIPOABS;CNTXT;DWPI;CNKI:应用，程序，访问，下载，统一资源定位，安全，阻止，拦截，阻塞，application, program, app, access, download, URL, safety, prevent, intercept

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 103442361 A (北京网秦天下科技有限公司) 2013年 12月 11日 (2013-12-11) 说明书第[0033]-[0070]段	1-32
A	CN 104253791 A (华为终端有限公司) 2014年 12月 31日 (2014-12-31) 全文	1-32
A	CN 102946377 A (珠海市君天电子科技有限公司) 2013年 2月 27日 (2013-02-27) 全文	1-32
A	US 2003055924 A1 (MATSUGATANI, K.) 2003年 3月 20日 (2003-03-20) 全文	1-32

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2017年 8月 8日	2017年 8月 21日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	刘芳
传真号 (86-10)62019451	电话号码 (86-10)62089108

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/090077

检索报告引用的专利文件			公布日（年/月/日）	同族专利			公布日（年/月/日）
CN	103442361	A	2013年 12月 11日	CN	103442361	B	2017年 1月 25日
CN	104253791	A	2014年 12月 31日	US	2016125185	A1	2016年 5月 5日
				WO	2014206223	A1	2014年 12月 31日
				EP	2999188	A1	2016年 3月 23日
CN	102946377	A	2013年 2月 27日		无		
US	2003055924	A1	2003年 3月 20日	JP	2003092639	A	2003年 3月 28日