(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103744686 B
(45)授权公告日 2017.03.08

(21)申请号 201310493745.1

(22)申请日 2013.10.18

(65)同一申请的已公布的文献号
申请公布号 CN 103744686 A

(43)申请公布日 2014.04.23

(73)专利权人 聚好看科技股份有限公司
地址 266100 山东省青岛市崂山区松岭路399号

(72)发明人 赵永健

(74)专利代理机构 青岛联智专利商标事务所有限公司 37101
代理人 邵新华

(51)Int.Cl.
G06F 9/445(2006.01)
G06F 21/51(2013.01)

(56)对比文件
CN 102546604 A,2012.07.04,
CN 102024107 A,2011.04.20,

审查员 谢沙沙

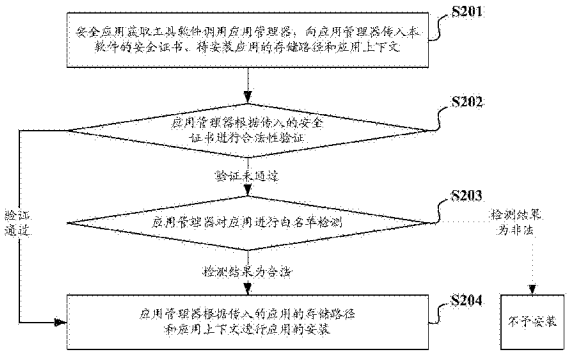
权利要求书2页 说明书6页 附图2页

(54)发明名称

智能终端中应用安装的控制方法和系统

(57)摘要

本发明公开了一种智能终端中应用安装的控制方法和系统，所述方法包括：若安全应用获取工具软件接收到应用安装指令，则调用应用管理器，并向其传入该软件的安全证书及其它；应用管理器对安全证书进行合法性验证；在验证通过后，根据传入的信息进行应用的安装；若普通应用获取工具软件接收到应用安装指令，则调用应用管理器，并向其传入应用的存储路径和应用上下文；应用管理器在确认未传入安全证书，或安全证书非法后，访问网络侧的应用合法性管理服务器对应用进行白名单检测；在确认检测结果为合法后，根据传入的信息进行应用的安装。应用本发明，可以保证智能终端中安装的应用的安全性，又能尽量节省网络访问的流量，缩短应用安装时间。



CN 103744686 B

1.一种智能终端中应用安装的控制方法，其特征在于，包括：

若安装于所述智能终端中的安全应用获取工具软件接收到应用安装指令，则调用所述智能终端中的应用管理器，并向所述应用管理器传入本安全应用获取工具软件的安全证书、该应用安装指令所涉及的应用的存储路径，以及该应用的应用上下文；所述应用管理器根据传入的安全证书进行合法性验证；在验证通过后，根据传入的应用的存储路径和应用上下文进行所述应用的安装；

若安装于所述智能终端中的普通应用获取工具软件接收到应用安装指令，则调用所述智能终端中的应用管理器，并向所述应用管理器传入该应用安装指令所涉及的应用的存储路径，以及该应用的应用上下文；所述应用管理器在确认所述普通应用获取工具软件未传入安全证书，或所述普通应用获取工具软件传入的安全证书非法后，访问网络侧的应用合法性管理服务器对所述应用进行白名单检测；在确认检测结果为合法后，根据传入的应用的存储路径和应用上下文进行所述应用的安装；其中，

所述安全应用获取工具软件包括应用商店，所述普通应用获取工具软件包括：文件管理器、下载管理器。

2.如权利要求1所述的方法，其特征在于，在所述应用管理器根据传入的安全证书进行合法性验证后，还包括：

若验证未通过，则所述应用管理器访问网络侧的应用合法性管理服务器对所述应用进行白名单检测；在确认检测结果为合法后，根据传入的应用的存储路径和应用上下文进行所述应用的安装。

3.如权利要求1或2所述的方法，其特征在于，在所述应用管理器访问网络侧的应用合法性管理服务器对所述应用进行白名单检测后，还包括：

若确认检测结果为不合法，则所述应用管理器显示非法应用，不予安装的提示信息。

4.如权利要求3所述的方法，其特征在于，所述安全应用获取工具软件接收到应用安装指令，具体包括：

所述应用商店在下载所述应用完毕后，显示应用安装提示框；在接收到所述安装提示框中的“安装”按键的点击事件信息后，确认接收到涉及所述应用的应用安装指令。

5.如权利要求4所述的方法，其特征在于，所述普通应用获取工具软件接收到应用安装指令，具体包括：

所述普通应用获取工具软件显示出至少一个应用的名称，在接收到针对所述应用的名称所显示的操作菜单中的安装选项的点击事件信息后，确认接收到涉及所述应用的应用安装指令。

6.一种智能终端中应用安装的控制系统，其特征在于，包括：安全应用获取工具模块、普通应用获取工具模块和应用管理器模块；其中，

所述安全应用获取工具模块用于在接收到应用安装指令后，调用所述智能终端中的应用管理器模块，并向所述应用管理器模块传入本安全应用获取工具软件的安全证书、该应用安装指令所涉及的应用的存储路径，以及该应用的应用上下文；

所述普通应用获取工具模块用于在接收到应用安装指令后，调用所述智能终端中的应用管理器，并向所述应用管理器传入该应用安装指令所涉及的应用的存储路径，以及该应用的应用上下文；

所述应用管理器模块根据安全应用获取工具模块传入的安全证书进行合法性验证；在验证通过后，根据传入的应用的存储路径和应用上下文进行所述应用的安装；以及所述应用管理器在确认普通应用获取工具模块未传入安全证书，或普通应用获取工具模块传入的安全证书非法后，访问网络侧的应用合法性管理服务器对所述应用进行白名单检测；在确认检测结果为合法后，根据传入的应用的存储路径和应用上下文进行所述应用的安装；其中，

所述安全应用获取工具模块包括应用商店，所述普通应用获取工具模块包括：文件管理器、下载管理器。

7.如权利要求6所述的系统，其特征在于，

所述应用管理器模块还用于在所述应用管理器根据传入的安全证书进行合法性验证后，若确认验证未通过，则访问网络侧的应用合法性管理服务器对所述应用进行白名单检测；在确认检测结果为合法后，根据传入的应用的存储路径和应用上下文进行所述应用的安装。

8.如权利要求7所述的系统，其特征在于，

所述应用管理器模块还用于在所述应用管理器访问网络侧的应用合法性管理服务器对所述应用进行白名单检测后，若确认检测结果为不合法，则所述应用管理器显示非法应用，不予安装的提示信息。

智能终端中应用安装的控制方法和系统

技术领域

[0001] 本发明涉及通信技术，尤其涉及一种智能终端中应用安装的控制方法和系统。

背景技术

[0002] 随着数字技术的不断发展，安装有Andriod安卓操作系统的智能终端越来越受到人们的青睐，例如手机、平板电脑等，用户可以使用这些智能终端随时随地方便地通过连接网络来浏览互联网、下载多媒体文件等，同时，用户将智能终端连接到网络后还可以访问应用商店或主流网站的下载资源页面根据自身喜好与需求选择、下载并安装应用来丰富智能终端的功能。

[0003] 智能终端中的应用管理器在对应用进行安装之前，为保证其安全性，需要通过网络访问网络侧的应用合法性管理服务器对应用进行白名单检测，具体地，应用管理器向应用合法性管理服务器发送针对该应用的代码序列的查询指令，应用合法性管理服务器根据接收的查询指令查询合法的代码序列数据库，如果代码序列数据库查找到该代码序列，返回确认信息；则智能终端中的应用管理器在接收到确认信息后确定通过白名单检测，检测结果为合法，智能终端中的应用管理器将该应用进行安装。

[0004] 本发明的发明人发现，现有的Android系统中的应用管理器在进行应用安装的过程中，采用白名单检测的方法虽然可以保证智能终端中安装的应用的安全性，但是，对于经过安全性认证的应用其实没必要使用白名单检测的方法：例如，对于可以通过应用商店下载的应用，均是经过应用商店服务器的安全性认证的应用，对这些应用仍采用白名单检测的方法会浪费网络访问的流量，而且安装时间也较长。因此，有必要提供一种既保证智能终端中安装的应用的安全性，又能尽量节省网络访问的流量，缩短安装时间的应用安装控制方法。

发明内容

[0005] 本发明实施例提供了一种智能终端中应用安装的控制方法和系统，既保证智能终端中安装的应用的安全性，又能尽量节省网络访问的流量，缩短应用安装时间。

[0006] 根据本发明的一个方面，提供了一种智能终端中应用安装的控制方法，包括：

[0007] 若安装于所述智能终端中的安全应用获取工具软件接收到应用安装指令，则调用所述智能终端中的应用管理器，并向所述应用管理器传入本安全应用获取工具软件的安全证书、该应用安装指令所涉及的应用的存储路径，以及该应用的应用上下文；所述应用管理器根据传入的安全证书进行合法性验证；在验证通过后，根据传入的应用的存储路径和应用上下文进行所述应用的安装；

[0008] 若安装于所述智能终端中的普通应用获取工具软件接收到应用安装指令，则调用所述智能终端中的应用管理器，并向所述应用管理器传入该应用安装指令所涉及的应用的存储路径，以及该应用的应用上下文；所述应用管理器在确认未传入安全证书，或安全证书非法后，访问网络侧的应用合法性管理服务器对所述应用进行白名单检测；在确认检测结

果为合法后，根据传入的应用的存储路径和应用上下文进行所述应用的安装。

[0009] 其中，在所述应用管理器根据传入的安全证书进行合法性验证后，还包括：

[0010] 若验证未通过，则所述应用管理器访问网络侧的应用合法性管理服务器对所述应用进行白名单检测；在确认检测结果为合法后，根据传入的应用的存储路径和应用上下文进行所述应用的安装。

[0011] 其中，在所述应用管理器访问网络侧的应用合法性管理服务器对所述应用进行白名单检测后，还包括：

[0012] 若确认检测结果为不合法，则所述应用管理器显示非法应用，不予安装的提示信息。

[0013] 其中，所述安全应用获取工具软件包括应用商店；以及

[0014] 所述普通应用获取工具软件包括：文件管理器、下载管理器。

[0015] 其中，所述安全应用获取工具软件接收到应用安装指令，具体包括：

[0016] 所述应用商店在下载所述应用完毕后，显示应用安装提示框；在接收到所述安装提示框中的“安装”按键的点击事件信息后，确认接收到涉及所述应用的应用安装指令。

[0017] 其中，所述普通应用获取工具软件接收到应用安装指令，具体包括：

[0018] 所述普通应用获取工具软件显示出至少一个应用的名称，在接收到针对所述应用的名称所显示的操作菜单中的安装选项的点击事件信息后，确认接收到涉及所述应用的应用安装指令。

[0019] 根据本发明的另一个方面，还提供了一种智能终端中应用安装的控制系统，包括：安全应用获取工具模块、普通应用获取工具模块和应用管理器模块；

[0020] 所述安全应用获取工具模块用于在接收到应用安装指令后，调用所述智能终端中的应用管理器模块，并向所述应用管理器模块传入本安全应用获取工具软件的安全证书、该应用安装指令所涉及的应用的存储路径，以及该应用的应用上下文；

[0021] 所述普通应用获取工具模块用于在接收到应用安装指令后，调用所述智能终端中的应用管理器，并向所述应用管理器传入该应用安装指令所涉及的应用的存储路径，以及该应用的应用上下文；

[0022] 所述应用管理器模块根据传入的安全证书进行合法性验证；在验证通过后，根据传入的应用的存储路径和应用上下文进行所述应用的安装；以及所述应用管理器在确认未传入安全证书，或安全证书非法后，访问网络侧的应用合法性管理服务器对所述应用进行白名单检测；在确认检测结果为合法后，根据传入的应用的存储路径和应用上下文进行所述应用的安装。

[0023] 较佳地，所述应用管理器模块还用于在所述应用管理器根据传入的安全证书进行合法性验证后，若确认验证未通过，则访问网络侧的应用合法性管理服务器对所述应用进行白名单检测；在确认检测结果为合法后，根据传入的应用的存储路径和应用上下文进行所述应用的安装。

[0024] 较佳地，所述应用管理器模块还用于在所述应用管理器访问网络侧的应用合法性管理服务器对所述应用进行白名单检测后，若确认检测结果为不合法，则所述应用管理器显示非法应用，不予安装的提示信息。

[0025] 较佳地，所述安全应用获取工具模块包括应用商店；以及

[0026] 所述普通应用获取工具模块包括：文件管理器、下载管理器。

[0027] 本发明实施例的技术方案中，对于通过安全应用获取工具软件下载的来源可靠的应用，应用管理器对其进行应用安装的过程中，根据传入的安全证书在本地进行合法性认证，而不必通过网络访问应用合法性管理服务器对该应用进行白名单检测，检测结果合法后再进行安装，从而既可以保证智能终端中安装的应用的安全性，又可以节省网络访问的流量，缩短应用安装时间；而对于通过普通应用获取工具软件下载的来源不一定可靠的应用，则应用管理器对其进行应用安装的过程中，使用白名单检测功能进行应用的合法性认证，以保证智能终端中安装的应用的安全性。

附图说明

[0028] 图1为本发明实施例的提供的智能终端的内部安装软件框图；

[0029] 图2为本发明实施例的提供的智能终端中安全应用获取工具软件调用应用管理器对应用安装的控制方法的流程示意图；

[0030] 图3为本发明实施例的提供的智能终端中普通应用获取工具软件调用应用管理器对应用安装的控制方法的流程示意图。

具体实施方式

[0031] 为使本发明的目的、技术方案及优点更加清楚明白，以下参照附图并举出优选实施例，对本发明进一步详细说明。然而，需要说明的是，说明书中列出的许多细节仅仅是为了使读者对本发明的一个或多个方面有一个透彻的理解，即便没有这些特定的细节也可以实现本发明的这些方面。

[0032] 本申请使用的“模块”、“系统”等术语旨在包括与计算机相关的实体，例如但不限于硬件、固件、软硬件组合、软件或者执行中的软件。例如，模块可以是，但并不仅限于：处理器上运行的进程、处理器、对象、可执行程序、执行的线程、程序和/或计算机。举例来说，计算设备上运行的应用程序和此计算设备都可以是模块。一个或多个模块可以位于执行中的一个进程和/或线程内。

[0033] 本发明的技术方案中，对Android系统中的应用管理器进行了改进，除了现有的白名单检测功能外，还增加了安全证书合法性验证的功能；对于下载来源可靠的应用，比如通过应用商店下载的应用，则可以在调用应用管理器进行应用安装的过程中，使用下载来源可靠的安全证书在本地进行合法性认证，而不必有网络交互的过程，从而既可以保证智能终端中安装的应用的安全性，又可以节省网络访问的流量，缩短应用安装时间；而对于下载来源不一定可靠的应用，则在调用应用管理器进行应用安装的过程中，使用白名单检测功能进行应用的合法性认证，以保证智能终端中安装的应用的安全性。

[0034] 下面结合附图详细说明本发明实施例的技术方案。本发明实施例提供的智能终端中的智能终端中应用安装的控制系统，如图1所示，包括：安全应用获取工具模块101、普通应用获取工具模块102和应用管理器模块103；

[0035] 其中，安全应用获取工具模块101具体为安装在智能终端中的安全应用获取工具软件；普通应用获取工具模块102具体为安装在智能终端中的普通应用获取工具软件102；应用管理器模块103具体为应用管理器。

[0036] 事实上，用户可以通过移动终端中不同的软件以多种方式或途径获取应用；例如，用户可以通过移动终端上安装的“应用商店”软件访问应用商店并下载应用，通常从应用商店下载的应用均是经过应用商店服务器的安全性认证的应用，因此，本文中将获取的应用安全性较高的软件称为安全应用获取工具软件。

[0037] 此外，用户也可以通过移动终端上安装的“下载管理器”软件访问主流网站的下载资源页面并下载应用；还可以通过移动终端上安装的“文档管理器”软件访问智能终端的外接存储设备并下载应用；但是，从下载管理器，或是文档管理器下载的应用一般都没有经过安全认证，因此，本文中将获取的应用安全性较低（没有经过安全认证）的软件如下载管理器、文档管理器称为普通应用获取工具软件。

[0038] 本发明的技术方案中，针对安全应用获取工具模块101和普通应用获取工具模块102获取的应用，在安装过程中采用不同的安装控制方法；具体地，本发明实施例提供的智能终端中安全应用获取工具软件调用应用管理器对应用安装的控制方法的流程如图2所示，包括如下步骤：

[0039] S201：安全应用获取工具软件在接收到应用安装指令后，调用智能终端中的应用管理器，向应用管理器传入本软件的安全证书、待安装应用的存储路径和应用上下文。

[0040] 本步骤中，若安装于智能终端中的安全应用获取工具软件接收到应用安装指令，则调用智能终端中的应用管理器，并向应用管理器传入本安全应用获取工具软件的安全证书、该应用安装指令所涉及的应用的存储路径，以及该应用的应用上下文。

[0041] 具体地，应用商店在对用户选中的应用下载完毕后，显示应用安装提示框，提示用户是否将已下载的应用安装到智能终端，应用商店在接收到提示框中的“安装”按键的点击事件信息后，确认接收到涉及该已下载的应用的应用安装指令，调用智能终端中的应用管理器，并在调用应用管理器的方法中，将安全应用获取工具软件的安全证书、该应用安装指令所涉及的应用的存储路径，以及该应用的应用上下文作为该方法的参数，向应用管理器传入。

[0042] 其中，安全应用获取工具软件的安全证书由配对的公钥、私钥生成，并由应用商店服务器提供并管理，在智能终端安装安全应用获取工具软件时与该软件绑定。

[0043] S202：应用管理器确认传入安全证书后，根据传入的安全证书进行合法性验证；若安全证书验证通过，执行S204；否则，执行S203。

[0044] 具体地，应用管理器判断是否传入安全证书；若应用管理器经判断，确认安全应用获取工具软件传入安全证书，则根据根据传入的安全证书进行合法性验证；

[0045] 应用管理器可通过公钥对安全证书进行合法性验证，具体的验证方法为本领域技术人员所熟知，此处不再赘述。

[0046] 若合法性验证通过，应用管理器确认安全证书合法，则执行S204；

[0047] 若合法性验证未通过，应用管理器确认安全证书非法，则执行S203。

[0048] S203：应用管理器访问网络侧的应用合法性管理服务器对应用进行白名单检测；若检测结果为合法，则执行S204；否则，不予安装。

[0049] 上述步骤中应用管理器确认安全证书非法后，本步骤中应用管理器通过网络访问网络侧的应用合法性管理服务器，向应用合法性管理服务器发送针对该应用的代码序列查询指令，应用合法性管理服务器根据接收的查询指令查询合法的代码序列数据库；

[0050] 应用合法性管理服务器若在代码序列数据库中未查找到该代码序列，则向应用管理器返回未找到信息，应用管理器在接收到未找到信息后确定未通过白名单检测，检测结果为不合法，显示非法应用，不予安装的提示信息；

[0051] 应用合法性管理服务器若在代码序列数据库中查找到该代码序列，则向应用管理器返回确认信息，应用管理器在接收到确认信息后确定通过白名单检测，检测结果为合法，执行步骤S204。

[0052] 事实上，虽然安全应用获取工具软件下载的应用均经过应用商店服务器的安全认证，但是与该软件绑定的安全证书也可能会存在非法的情况，因此可以在方法流程中设置此步骤。

[0053] S204：应用管理器根据传入的应用的存储路径和应用上下文进行应用的安装。

[0054] 上述步骤中应用管理器在确认安全证书合法，或检测结果为合法后，本步骤中应用管理器根据传入的应用的存储路径和应用上下文，将应用复制文件到安装目的文件夹，复制完后在注册表中注册，最后在默认的应用程序目录中生成应用程序链接，完成安装。所述安装目的文件夹可以是预设于智能终端中的。

[0055] 此外，本发明实施例提供的智能终端中普通应用获取工具软件调用应用管理器对应用安装的控制方法的流程如图3所示，包括如下步骤：

[0056] S301：普通应用获取工具软件接收到应用安装指令后，调用智能终端中的应用管理器，向应用管理器传入待安装应用的存储路径和应用上下文。

[0057] 本步骤中，若安装于智能终端中的普通应用获取工具软件接收到应用安装指令，则调用智能终端中的应用管理器，并向应用管理器传入该应用安装指令所涉及的应用的存储路径，以及该应用的应用上下文。

[0058] 具体地，普通应用获取工具软件对用户选中的应用下载完毕时，显示普通应用获取工具软件的安装界面，安装界面显示该软件下载的至少一个应用的名称，普通应用获取工具软件在接收到针对该已下载的应用的名称所显示的操作菜单中的安装选项的点击事件信息后，确认接收到该应用的应用安装指令，调用智能终端中的应用管理器，并在调用应用管理器的方法中，将该应用安装指令所涉及的应用的存储路径、以及该应用的应用上下文作为该方法的参数，向应用管理器传入。

[0059] S302：应用管理器在确认未传入安全证书后，访问网络侧的应用合法性管理服务器对待安装应用进行白名单检测；若检测结果为合法，则执行S303；否则，不予安装。

[0060] 本步骤中，应用管理器判断是否传入安全证书；若应用管理器经判断，确认普通应用获取工具软件未传入安全证书，则访问网络侧的应用合法性管理服务器对应用进行白名单检测；

[0061] 若应用管理器确定待安装应用未通过白名单检测，检测结果为不合法，即检测结果为非法，则显示非法应用，不予安装的提示信息；

[0062] 若应用管理器确定待安装应用通过白名单检测，检测结果为合法，则执行步骤S303。

[0063] 事实上，普通应用获取工具软件下载的应用一般没有经过安全认证，也就是说，普通应用获取工具软件并没有绑定安全证书，因此在方法流程中应用管理器访问网络侧的应用合法性管理服务器对应用进行白名单检测为必要步骤。

[0064] S303：应用管理器根据传入的应用的存储路径和应用上下文进行应用的安装。

[0065] 上述步骤中应用管理器确认白名单检测结果为合法后，本步骤中应用管理器根据传入的应用的存储路径和应用上下文，将应用复制文件到安装目的文件夹，复制完后在注册表中注册，最后在默认的应用程序目录中生成应用程序链接，完成安装。所述安装目的文件夹可以是预设于智能终端中的。

[0066] 本发明的技术方案中，对于通过安全应用获取工具软件下载的来源可靠的应用，应用管理器对其进行应用安装的过程中，根据传入的安全证书在本地进行合法性认证，而不必通过网络访问应用合法性管理服务器对该应用进行白名单检测，检测结果合法后再进行安装，从而既可以保证智能终端中安装的应用的安全性，又可以节省网络访问的流量，缩短应用安装时间；而对于通过普通应用获取工具软件下载的来源不一定可靠的应用，则应用管理器对其进行应用安装的过程中，使用白名单检测功能进行应用的合法性认证，以保证智能终端中安装的应用的安全性。

[0067] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，该程序可以存储于一计算机可读取存储介质中，如：ROM/RAM、磁碟、光盘等。

[0068] 以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以作出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

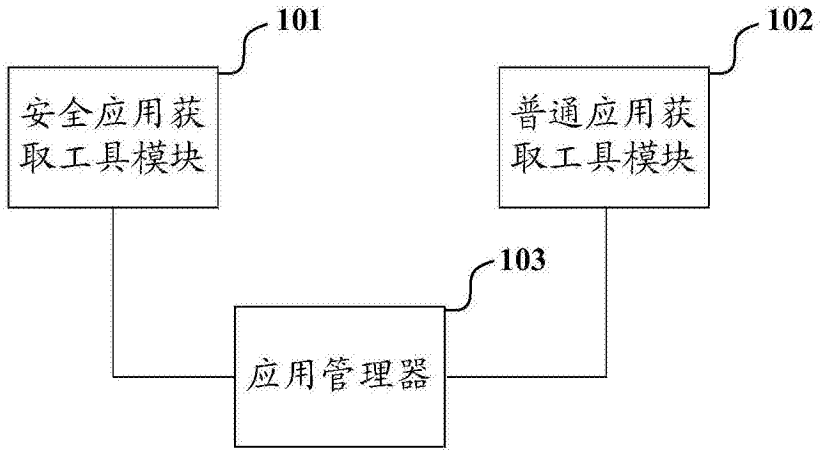

101
安全应用获取工具模块
102
普通应用获取工具模块
103
应用管理器

图1

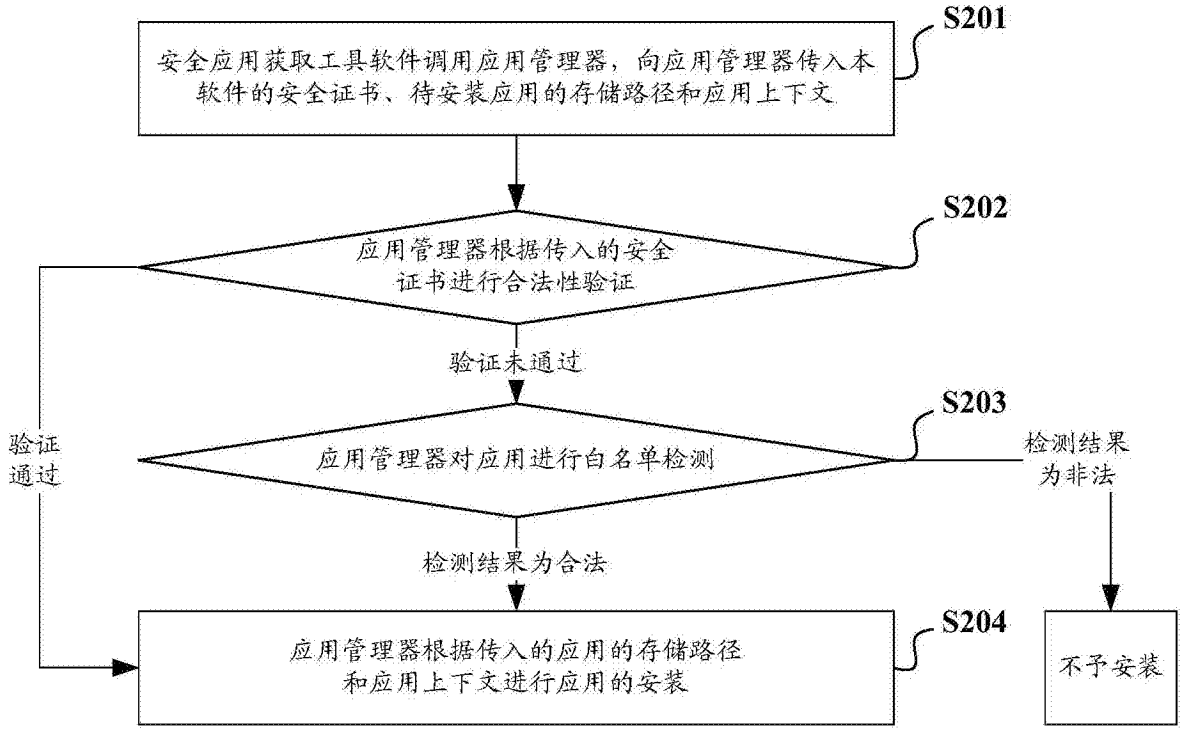

S201
安全应用获取工具软件调用应用管理器，向应用管理器传入本软件的安全证书、待安装应用的存储路径和应用上下文
S202
应用管理器根据传入的安全证书进行合法性验证
验证未通过
验证通过
S203
应用管理器对应用进行白名单检测
检测结果为非法
检测结果为合法
S204
应用管理器根据传入的应用的存储路径和应用上下文进行应用的安装
不予安装

图2

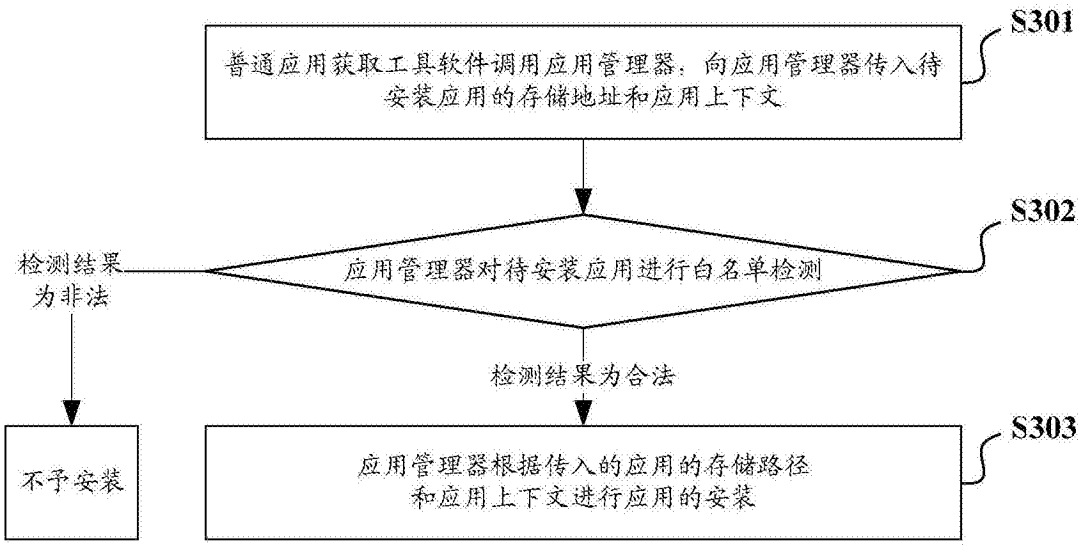

普通应用获取工具软件调用应用管理器，向应用管理器传入待安装应用的存储地址和应用上下文
S301
应用管理器对待安装应用进行白名单检测
S302
检测结果为非法
检测结果为合法
不予安装
应用管理器根据传入的应用的存储路径和应用上下文进行应用的安装
S303

图3