(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 103646215 A
(43)申请公布日 2014.03.19

(21)申请号 201310717660.7

(22)申请日 2013.12.23

(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 王鹏程 苏云琳 窦文科 王力

(74)专利代理机构 北京中强智尚知识产权代理有限公司 11448
代理人 姜精斌

(51)Int.Cl.
G06F 21/57(2013.01)
G06F 21/56(2013.01)

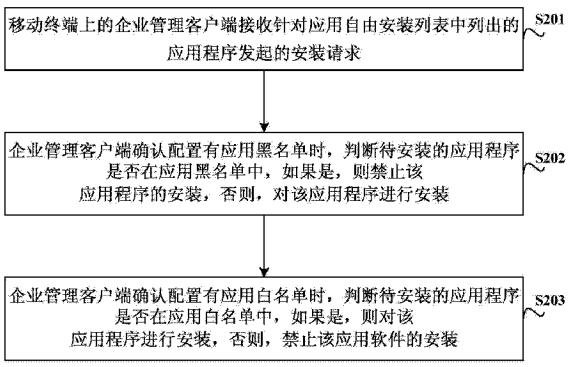
权利要求书2页 说明书10页 附图4页

(54)发明名称

一种应用程序的安装控制方法、相关系统及装置

(57)摘要

本发明公开了一种应用程序的安装控制方法、相关系统及装置，用以对移动终端上的应用程序实现安全管理。应用程序的安装控制方法，包括：移动终端上的企业管理客户端接收针对应用自由安装列表中列出的应用程序发起的安装请求；确认配置有应用黑名单时，判断待安装的应用程序是否在应用黑名单中，如果是，则禁止应用程序的安装，否则，对应用程序进行安装；确认配置有应用白名单时，判断待安装的应用程序是否在应用白名单中，如果是，则对应用程序进行安装，否则，禁止应用软件的安装。本方案能够有效保护企业信息安全。



CN 103646215 A

1. 一种应用程序的安装控制方法，其特征在于，包括：

移动终端上的企业管理客户端接收针对应用自由安装列表中列出的应用程序发起的安装请求，所述应用自由安装列表是企业管理服务器推送给所述企业管理客户端的；

所述企业管理客户端确认配置有应用黑名单时，判断待安装的应用程序是否在所述应用黑名单中，如果是，则禁止所述应用程序的安装，否则，对所述应用程序进行安装；

所述企业管理客户端确认配置有应用白名单时，判断待安装的应用程序是否在所述应用白名单中，如果是，则对所述应用程序进行安装，否则，禁止所述应用软件的安装。

2. 如权利要求 1 所述的方法，其特征在于，所述应用自由安装列表中列出的各应用程序的安装包保存在所述企业管理服务器中；以及，所述企业管理服务器保存应用程序的安装包之前，还包括：

对应用程序的安装包进行病毒检测和加固处理。

3. 如权利要求 2 所述的方法，其特征在于，所述企业管理服务器推送应用自由安装列表的方法，包括：

所述企业管理服务器根据自身维护的应用管理列表、以及各用户组的应用管理策略，为每个用户组生成对应的应用自由安装列表；并

将每个用户组对应的应用自由安装列表推送到该用户组中各用户的企业管理客户端上，所述应用管理列表中包括所有安装包已上传到所述企业管理服务器的应用程序的名称及版本号，所述应用自由安装列表中包括供用户组自由安装的应用程序的名称及版本号。

4. 如权利要求 2 或 3 所述的方法，其特征在于，所述对所述应用程序进行安装，具体包括：

所述企业管理客户端使用提取的超级用户 Root 权限，根据所述安装请求从所述企业管理服务器处下载所述应用程序的安装包并在个人区内存空间中进行自动安装，所述个人区内存空间是指所述移动终端的内存空间中工作区内存空间之外的内存空间，所述工作区内存空间是指分配给所述企业管理客户端的内存空间；和 / 或，

所述禁止所述应用程序的安装，具体包括：

所述企业管理客户端使用提取的超级用户 Root 权限，禁止从所述企业管理服务器处下载所述应用程序的安装包，并发出所述应用程序禁止安装的告警信息。

5. 如权利要求 4 所述的方法，其特征在于，所述应用黑名单或应用白名单是由企业管理服务器配置给所述企业管理客户端的；以及，

所述方法还包括：

企业管理客户端接收到所述企业管理服务器配置的应用黑名单时，根据应用黑名单中列出的应用程序的名称及版本号检测个人区内存空间中是否安装有所述应用黑名单中列出的应用程序，并针对检测到的应用程序发出所述应用程序禁止安装的告警信息；

企业管理客户端接收到所述企业管理服务器配置的应用白名单时，根据应用白名单中列出的应用程序的名称及版本号检测个人区内存空间中是否安装有所述应用白名单中未列出的应用程序；并针对检测到的应用程序发出所述应用程序禁止安装的告警信息。

6. 一种移动终端的企业管理系统，其特征在于，包括企业管理服务器和安装在移动终端上的企业管理客户端，其中：

所述企业管理服务器，用于向企业管理客户端推送应用自由安装列表；

所述企业管理客户端，用于接收针对所述应用自由安装列表中列出的应用程序发起的安装请求；确认配置有应用黑名单时，判断待安装的应用程序是否在所述应用黑名单中，如果是，则禁止所述应用程序的安装，否则，对所述应用程序进行安装；确认配置有应用白名单时，判断待安装的应用程序是否在所述应用白名单中，如果是，则对所述应用程序进行安装，否则，禁止所述应用软件的安装。

7. 如权利要求 6 所述的系统，其特征在于，

所述企业管理服务器，还用于对上传到本企业管理服务器的应用程序的安装包进行病毒检测和加固处理后保存；和 / 或，

所述企业管理服务器，还用于根据自身维护的应用管理列表、以及各用户组的应用管理策略，为每个用户组生成对应的应用自由安装列表，并将每个用户组对应的应用自由安装列表推送到该用户组中各用户的企业管理客户端上，所述应用管理列表中包括所有安装包已上传到所述企业管理服务器的应用程序的名称及版本号，所述应用自由安装列表中包括供用户组自由安装的应用程序的名称及版本号。

8. 如权利要求 7 所述的系统，其特征在于，

所述企业管理客户端，具体用于使用提取的超级用户 Root 权限，根据所述安装请求从所述企业管理服务器处下载所述应用程序的安装包并在个人区内存空间中进行自动安装，所述个人区内存空间是指所述移动终端的内存空间中工作区内存空间之外的内存空间，所述工作区内存空间是指分配给所述企业管理客户端的内存空间；和 / 或，

所述企业管理客户端，具体用于使用提取的超级用户 Root 权限，禁止从所述企业管理服务器处下载所述应用程序的安装包，并发出所述应用程序禁止安装的告警信息。

9. 如权利要求 8 所述的系统，其特征在于，

所述企业管理服务器，还用于将所述应用黑名单或应用白名单配置给所述企业管理客户端；

所述企业管理客户端，还用于接收到所述企业管理服务器配置的应用黑名单时，根据应用黑名单中列出的应用程序的名称及版本号检测个人区内存空间中是否安装有所述应用黑名单中列出的应用程序，并针对检测到的应用程序发出所述应用程序禁止安装的告警信息；接收到所述企业管理服务器配置的应用白名单时，根据应用白名单中列出的应用程序的名称及版本号检测个人区内存空间中是否安装有所述应用白名单中未列出的应用程序；并针对检测到的应用程序发出所述应用程序禁止安装的告警信息。

10. 一种企业管理客户端装置，其特征在于，所述企业管理客户端装置安装在移动终端上，包括：

接收模块，用于接收针对应用自由安装列表中列出的应用程序发起的安装请求；

确认模块，用于确认是否配置有应用黑名单或者应用白名单；

第一控制模块，用于当所述确认模块确认配置有应用黑名单时，判断待安装的应用程序是否在所述应用黑名单中，如果是，则禁止所述应用程序的安装，否则，对所述应用程序进行安装；

第二控制模块，用于当所述确认模块确认配置有应用白名单时，判断待安装的应用程序是否在所述应用白名单中，如果是，则对所述应用程序进行安装，否则，禁止所述应用软件的安装。

一种应用程序的安装控制方法、相关系统及装置

技术领域

[0001] 本发明涉及信息安全领域，尤其涉及一种应用程序的安装控制方法、相关系统及装置。

背景技术

[0002] 随着移动终端的成熟与普及，以智能手机、平板电脑为代表的个人移动终端设备逐渐进入企业领域。据国际权威咨询公司 Gartner 预测，到 2014 年 90% 的企业将会支持员工在个人移动终端设备上运行企业办公应用程序，员工使用个人移动终端设备办公已经成为一种无法逆转的潮流。这类被称为 BYOD(Bring Your Own Device, 自带设备办公）的现象为企业信息安全带来了新的挑战：

[0003] 1、企业网络边界变得模糊，原有的边界防御系统无法有效保护企业信息安全

[0004] 企业员工的移动终端可以在任何时间、任何地点接入移动互联网或公共 / 家庭 Wi-Fi 网络，移动终端中的企业数据也会暴露在来自互联网的攻击之下，BYOD 打破了原有的企业网络边界，正是这种边界的模糊性使 BYOD 成为企业信息安全体系的薄弱环节，需要新的方法保护企业信息安全。

[0005] 2、个人应用与企业应用混用，为企业带来信息安全风险

[0006] 同一移动终端上既有个人应用，又有企业应用和数据，个人应用可以随意访问、存取企业数据，从而存在企业数据被个人应用非法上传、共享和外泄的风险。如存储在手机中的办公邮件、文件、图片、通信记录以及与业务内容有关的短信等，这些敏感企业信息的泄漏给企业带来极大的信息安全风险。

[0007] 3、遗失或被窃移动终端，会给企业带来泄密隐患

[0008] 移动终端容易丢失，移动终端中所保存的企业数据也因此面临泄密风险，设备丢失不但意味着敏感企业信息的泄漏和丢失，所丢失的设备也可能会变成攻击企业网络的跳板。

[0009] 4、手机病毒呈指数式增长，移动终端成为渗透企业内网的跳板

[0010] 在移动互联网越来越深入人心的今天，攻击者们已经开始将视线由 PC（Personal Computer，个人计算机）转向了移动终端。根据国家互联网应急中心统计，2012 年新发现的恶意程序超过 16 万，较 2011 年增长 25 倍。根据 2013 年 7 月 6 日央视《新闻联播》报道，2013 上半年安卓手机病毒暴涨 7.96 倍。同时，由于 Root（超级用户）权限滥用和新的黑客攻击技术，移动终端成为滋生信息安全风险的新温床，容易成为黑客入侵渗透企业内网的跳板。

[0011] 由此可见，BYOD 给企业带来的信息安全问题成为现有技术中亟待解决的技术问题。

发明内容

[0012] 本发明实施例提供一种应用程序的安装控制方法、相关系统及装置，用以对移动

终端上的应用程序实现安全管理，从而有效保护企业信息安全。

[0013] 本发明实施例提供的应用程序的安装控制方法，包括：

[0014] 移动终端上的企业管理客户端接收针对应用自由安装列表中列出的应用程序发起的安装请求，所述应用自由安装列表是企业管理服务器推送给所述企业管理客户端的；

[0015] 所述企业管理客户端确认配置有应用黑名单时，判断待安装的应用程序是否在所述应用黑名单中，如果是，则禁止所述应用程序的安装，否则，对所述应用程序进行安装；

[0016] 所述企业管理客户端确认配置有应用白名单时，判断待安装的应用程序是否在所述应用白名单中，如果是，则对所述应用程序进行安装，否则，禁止所述应用软件的安装。

[0017] 其中，所述应用自由安装列表中列出的各应用程序的安装包保存在所述企业管理服务器中；以及，所述企业管理服务器保存应用程序的安装包之前，还包括：

[0018] 对应用程序的安装包进行病毒检测和加固处理。

[0019] 进一步的，所述企业管理服务器推送应用自由安装列表的方法，包括：

[0020] 所述企业管理服务器根据自身维护的应用管理列表、以及各用户组的应用管理策略，为每个用户组生成对应的应用自由安装列表，并将每个用户组对应的应用自由安装列表推送到该用户组中各用户的企业管理客户端上，所述应用管理列表中包括所有安装包已上传到所述企业管理服务器的应用程序的名称及版本号，所述应用自由安装列表中包括供用户组自由安装的应用程序的名称及版本号。

[0021] 其中，所述对所述应用程序进行安装，具体包括：

[0022] 所述企业管理客户端使用提取的超级用户 Root 权限，根据所述安装请求从所述企业管理服务器处下载所述应用程序的安装包并在个人区内存空间中进行自动安装，所述个人区内存空间是指所述移动终端的内存空间中工作区内存空间之外的内存空间，所述工作区内存空间是指分配给所述企业管理客户端的内存空间。

[0023] 其中，所述禁止所述应用程序的安装，具体包括：

[0024] 所述企业管理客户端使用提取的超级用户 Root 权限，禁止从所述企业管理服务器处下载所述应用程序的安装包，并发出所述应用程序禁止安装的告警信息。

[0025] 其中，所述应用黑名单或应用白名单是由企业管理服务器配置给所述企业管理客户端的；以及，所述方法还包括：

[0026] 企业管理客户端接收到所述企业管理服务器配置的应用黑名单时，根据应用黑名单中列出的应用程序的名称及版本号检测个人区内存空间中是否安装有所述应用黑名单中列出的应用程序，并针对检测到的应用程序发出所述应用程序禁止安装的告警信息；

[0027] 企业管理客户端接收到所述企业管理服务器配置的应用白名单时，根据应用白名单中列出的应用程序的名称及版本号检测个人区内存空间中是否安装有所述应用白名单中未列出的应用程序；并针对检测到的应用程序发出所述应用程序禁止安装的告警信息。

[0028] 本发明实施例还提供一种移动终端的企业管理系统，包括企业管理服务器和安装在移动终端上的企业管理客户端，其中：

[0029] 所述企业管理服务器，用于向企业管理客户端推送应用自由安装列表；

[0030] 所述企业管理客户端，用于接收针对所述应用自由安装列表中列出的应用程序发起的安装请求；确认配置有应用黑名单时，判断待安装的应用程序是否在所述应用黑名单中，如果是，则禁止所述应用程序的安装，否则，对所述应用程序进行安装；确认配置有应用

白名单时，判断待安装的应用程序是否在所述应用白名单中，如果是，则对所述应用程序进行安装，否则，禁止所述应用软件的安装。

[0031] 进一步的，所述企业管理服务器，还用于对上传到本企业管理服务器的应用程序的安装包进行病毒检测和加固处理后保存。

[0032] 进一步的，所述企业管理服务器，还用于根据自身维护的应用管理列表、以及各用户组的应用管理策略，为每个用户组生成对应的应用自由安装列表，并将每个用户组对应的应用自由安装列表推送到该用户组中各用户的企业管理客户端上，所述应用管理列表中包括所有安装包已上传到所述企业管理服务器的应用程序的名称及版本号，所述应用自由安装列表中包括供用户组自由安装的应用程序的名称及版本号。

[0033] 进一步的，所述企业管理客户端，具体用于使用提取的超级用户 Root 权限，根据所述安装请求从所述企业管理服务器处下载所述应用程序的安装包并在个人区内存空间中进行自动安装，所述个人区内存空间是指所述移动终端的内存空间中工作区内存空间之外的内存空间，所述工作区内存空间是指分配给所述企业管理客户端的内存空间。

[0034] 进一步的，所述企业管理客户端，具体用于使用提取的超级用户 Root 权限，禁止从所述企业管理服务器处下载所述应用程序的安装包，并发出所述应用程序禁止安装的告警信息。

[0035] 进一步的，所述企业管理服务器，还用于将所述应用黑名单或应用白名单配置给所述企业管理客户端；

[0036] 所述企业管理客户端，还用于接收到所述企业管理服务器配置的应用黑名单时，根据应用黑名单中列出的应用程序的名称及版本号检测个人区内存空间中是否安装有所述应用黑名单中列出的应用程序，并针对检测到的应用程序发出所述应用程序禁止安装的告警信息；接收到所述企业管理服务器配置的应用白名单时，根据应用白名单中列出的应用程序的名称及版本号检测个人区内存空间中是否安装有所述应用白名单中未列出的应用程序；并针对检测到的应用程序发出所述应用程序禁止安装的告警信息。

[0037] 本发明实施例还提供一种企业管理客户端装置，所述企业管理客户端装置安装在移动终端上，包括：

[0038] 接收模块，用于接收针对应用自由安装列表中列出的应用程序发起的安装请求；

[0039] 确认模块，用于确认是否配置有应用黑名单或者应用白名单；

[0040] 第一控制模块，用于当所述确认模块确认配置有应用黑名单时，判断待安装的应用程序是否在所述应用黑名单中，如果是，则禁止所述应用程序的安装，否则，对所述应用程序进行安装；

[0041] 第二控制模块，用于当所述确认模块确认配置有应用白名单时，判断待安装的应用程序是否在所述应用白名单中，如果是，则对所述应用程序进行安装，否则，禁止所述应用软件的安装。

[0042] 本发明实施例提供的应用程序的安装控制方法、相关系统及装置，由企业管理服务器和安装在移动终端上的企业管理客户端组成了移动终端的企业管理系统，对移动终端上的应用程序进行安全管理。企业管理服务器向企业管理客户端推送应用自由安装列表，用户仅能针对应用自由安装列表中列出的应用程序发起安装，保证了应用程序来源的安全可靠性；针对待安装的应用程序发起安装请求后，采用应用黑白名单机制进行控制，仅允许

对未在应用黑名单中的应用程序或者在应用白名单中的应用程序进行安装，而禁止其他应用程序的安装，避免了移动终端上的企业数据被恶意应用非法上传、共享和外泄的风险，从而有效保护企业信息安全。

[0043] 本申请的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本申请而了解。本申请的目的和其他优点可通过在所写的说明书、权利要求书、以及附图中所特别指出的结构来实现和获得。

附图说明

[0044] 附图用来提供对本发明的进一步理解，并且构成说明书的一部分，与本发明实施例一起用于解释本发明，并不构成对本发明的限制。在附图中：

[0045] 图 1 为本发明实施例中移动终端的企业管理系统的系统架构示意图；

[0046] 图 2 为本发明实施例中应用程序的安装控制方法流程图；

[0047] 图 3 为本发明实施例中企业管理客户端上配置有应用黑名单时应用程序的安装控制方法流程图；

[0048] 图 4 为本发明实施例中企业管理客户端上配置有应用白名单时应用程序的安装控制方法流程图；

[0049] 图 5 为本发明实施例中移动终端的企业管理系统框图；

[0050] 图 6 为本发明实施例中企业管理客户端装置的结构框图。

具体实施方式

[0051] 为了解决 BYOD 给企业带来的信息安全问题，本发明实施例提供了一种移动终端的企业管理系统，基于该移动终端的企业管理系统，本发明实施例还提供了一种应用程序的安装控制方法、相关系统及装置，用以对移动终端上的应用程序实现安全管理，从而有效保护企业信息安全。以下结合说明书附图对本发明的优选实施例进行说明，应当理解，此处所描述的优选实施例仅用于说明和解释本发明，并不用于限定本发明。并且在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。

[0052] 首先，对本发明实施例提供的移动终端的企业管理系统的系统架构进行说明。如图 1 所示，本发明实施例提供的移动终端的企业管理系统是面向企业的移动终端管理平台，包括部署在企业内网的服务端和安装在需要被管理的移动终端上的客户端，本发明实施例中，将部署在企业内网的服务端称为企业管理服务器，安装在需要被管理的移动终端上的客户端称为企业管理客户端。其中：

[0053] 企业管理服务器的主要功能包括：管理、下发企业内网的应用，以及管理、下发安全策略等；企业管理服务器还提供丰富的移动终端统计与管理工具，企业管理员可以通过企业管理服务器查看每个需要被管理的移动终端的详细信息，包括：终端型号、系统版本、IMEI(International Mobile Equipment Identification Number，国际移动设备识别码)、序列号、MSISDN（移动台识别号码，俗称手机号码）、是否离线、是否 Root（超级用户）、更换密码时间、是否安装安全软件、电源信息、无线网络信息等。企业管理客户端的主要功能包括：数据防泄密，执行安全策略等，数据防泄密包括数据加密、数据隔离等，加密的数据可以是涉及系统文件内的数据；或者是用户选定的财务文件、生产文件、销售文件、市场文件、人

力资源文件等内的数据；还可以是用户个人文件的数据，例如：照片、视频、日志等。以在Android（安卓）系统上实现为例对数据加密进行简要说明。数据加密是通过.so（动态链接库）文件实现，主要是在应用程序中注入代码，使得apk（Android Package，安卓安装包）初始化时去调用该.so文件，要保证.so文件运行的时机比应用程序的读写文件的时间早，如果晚了文件就会变成“一半加密的状态”，导致文件损坏。通过数据加密，.so文件会拦截该应用程序的所有文件操作，实现加密。

[0054] 本发明实施例提供的移动终端的企业管理系统，基于企业管理客户端的数据防泄密机制，在不影响企业员工对个人应用使用感受的基础上，在移动终端上建立了一个安全、独立的工作区内存空间，工作区内存空间（简称工作区）是指分配给企业管理客户端的内存空间，所有的企业应用和数据存储在受保护的工作区内。相应的，移动终端的内存空间中工作区内存空间之外的内存空间称为个人区内存空间（简称个人区），所有的个人应用和数据存储在个人区内，个人应用无法访问企业数据，从而避免企业数据被个人应用非法访问、存取。本发明实施例提供的移动终端的企业管理系统，不仅将企业数据和个人数据完全隔离，更好地保护企业应用和数据，也为企业员工提供了无差别的个人应用体验，达到了“一机两用”的效果。

[0055] 企业管理服务器提供两种应用程序下发方式：自由安装和强制安装。通过自由安装方式下发的应用程序，供企业用户自由选择下载安装；通过强制安装方式下发的应用程序，企业用户需安装该应用程序后才能正常使用工作区。具体实施中，针对工作区内的企业应用，一般采用强制安装方式；针对个人区内的个人应用，一般采用自由安装方式。，当然也可以对工作区内的企业应用采用自由安装方式。

[0056] 为了对移动终端上的应用程序实现安全管理，从而有效保护企业信息安全，基于上述移动终端的企业管理系统，本发明实施例针对通过自由安装方式下发的应用程序，提供了一种应用程序的安装控制方法，由于工作区内的企业应用通常情况下具备企业强制安装的特点，因此该方案主要是针对个人区内的个人应用提供的安全管理机制，当然也不排除对非强制安装的企业应用提供安全管理的应用场景。如图2所示，本发明实施例提供的应用程序的安装控制方法，包括如下步骤：

[0057] S201、移动终端上的企业管理客户端接收针对应用自由安装列表中列出的应用程序发起的安装请求，其中，应用自由安装列表是企业管理服务器推送给企业管理客户端的。

[0058] 具体实施中，该安装请求是企业用户根据企业管理客户端展示的应用自由安装列表选择待安装的应用程序后发起的。

[0059] 具体实施中，企业管理服务器中建立了一个专用空间，用于存储上传到企业管理服务器中的应用程序的安装包，本发明实施例中将该专用空间称为企业应用库。企业管理服务器上维护有应用管理列表，应用管理列表中包括所有安装包已上传到企业管理服务器的应用程序的名称及版本号，当然也可以包括该应用程序的其他信息，例如上传时间、安装包大小、安装量等。企业管理员可以查看、编辑应用管理列表，查看各应用程序的安装量等统计信息。一般情况下，应用程序的安装包是由企业上传给企业管理服务器的，为了保证移动终端上所使用应用程序的安全可靠性，企业管理服务器在保存应用程序的安装包之前，对应用程序的安装包进行病毒检测和加固处理。对应用程序的安装包进行加固处理，可以防止应用程序被轻易逆向从而获取密钥体系等关键信息，同时给应用程序增加了数据加密

的功能，增加安全系数。以在 Android（安卓）系统上实现为例对应用程序的安装包进行加固处理进行简要说明。对应用程序的安装包进行加固处理主要就是改变应用程序的 class.dex 文件的内容，对其内容进行一些算法加密，在 apk（Android Package，安卓安装包）运行时再动态的去解密，还原内容；在修改 class.dex 文件的时候要保证其符合 dex 文件的固有格式。所有上传的应用程序的安装包均经过病毒检测和加固处理，从而杜绝恶意篡改、代码注入、内存修改、窃取数据、反编译等威胁。

[0060] 企业管理服务器还可以将企业员工按照部门、或者职能等划分为不同的用户组，并且为各用户组制定不同的应用管理策略，例如将企业应用库中的应用程序划分类型，为不同部门或者不同职能的用户组下发特定类型的应用程序。通过企业管理服务器的分组功能，可以对不同的用户组分发不同的应用程序。企业管理服务器可以根据自身维护的应用管理列表、以及各用户组的应用管理策略，为每个用户组生成对应的应用自由安装列表，并将每个用户组对应的应用自由安装列表推送到该用户组中各用户的企业管理客户端上，应用自由安装列表中包括供用户组自由安装的应用程序的名称及版本号。企业管理客户端将应用自由安装列表展示在工作区的企业应用市场中，供企业用户自由选择下载安装。

[0061] S202、企业管理客户端确认配置有应用黑名单时，判断待安装的应用程序是否在应用黑名单中，如果是，则禁止该应用程序的安装，否则，对该应用程序进行安装。

[0062] S203、企业管理客户端确认配置有应用白名单时，判断待安装的应用程序是否在应用白名单中，如果是，则对应用程序进行安装，否则，禁止应用软件的安装。

[0063] 具体实施中，应用黑名单或应用白名单一般是由企业管理服务器配置给企业管理客户端的，当然也可以预先由人工配置给企业管理客户端。应用黑名单中会列出禁止安装的应用程序的名称及版本号，应用白名单中会列出仅允许安装的应用程序的名称及版本号。判断待安装的应用程序是否在应用黑名单中，是指判断待安装的应用程序的名称及版本号是否在应用黑名单中列出的应用程序的名称及版本号中；判断待安装的应用程序是否在应用白名单中，是指判断待安装的应用程序的名称及版本号是否在应用白名单中列出的应用程序的名称及版本号中。

[0064] 应用黑名单或应用白名单的设置都是企业管理员可以配置的。企业管理员对应用黑名单或者应用白名单的设置包括如下场景：

[0065] 场景一、企业所有移动终端设备，仅允许企业员工办公使用，因此会限制仅允许安装办公使用的应用程序，即可以采用应用白名单的方式限定仅允许安装工作相关的应用程序。

[0066] 场景二、禁止被曝出有安全漏洞或恶意行为的应用程序的安装。例如一些特定的应用程序，或者是安全软件查出有恶意行为的应用程序，或者是漏洞扫描功能扫描出的有安全漏洞的应用程序等，即可以采用应用黑名单的方式禁止有安全漏洞或恶意行为的应用程序的安装。

[0067] 场景三、禁止某些文件分享类应用程序的安装，例如网盘等应用程序的安装，因为文件分享类应用程序会导致企业内部的资源被上传到云端，从而破坏了企业信息的私密性，即可以采用应用黑名单的方式禁止文件分享类应用程序的安装。

[0068] 其他具体场景不再一一列举，总之，企业可以按照本企业的实际需求，采用应用黑名单或者应用白名单的方式，灵活的控制每一个用户组中应用程序的安装。

[0069] 较佳的，本发明实施例中，企业管理客户端使用应用黑名单或应用白名单对个人应用即个人区中需要安装的应用程序进行管理，通过对个人区中应用程序的管理，使得个人区中仅能安装受信任的应用程序，进一步保证工作区中企业数据的安全性。相应的，如果判断出待安装的应用程序不在应用黑名单中，或者判断出待安装的应用程序在应用白名单中，对该应用程序进行安装，具体包括如下步骤：

[0070] 企业管理客户端使用提取的 Root 权限，根据安装请求从企业管理服务器处下载应用程序的安装包并在个人区内存空间中进行自动安装。

[0071] 相应的，如果判断出待安装的应用程序在应用黑名单中，或者判断出待安装的应用程序不在应用白名单中，禁止该应用程序的安装，具体包括如下步骤：

[0072] 企业管理客户端使用提取的 Root 权限，禁止从企业管理服务器处下载该应用程序的安装包，并发出该应用程序禁止安装的告警信息。

[0073] 下面对实现应用黑白名单的技术原理进行简要说明，以在 Android（安卓）系统上实现为例进行说明。企业管理客户端首先通过一段 Root 代码提取 Root 权限，使用 Root 权限启动一个具有 Root 权限的 Service（服务）。具有 Root 权限的 Service 启动之后，预留本地的 Socket（套接字）接口供调用。企业管理客户端调用该 Socket 接口，使得具有 Root 权限的 Service Hook 在 Android 系统的一个核心进程 System Service（系统服务）上，从而具有 Root 权限的 Service 可以监控与 Binder（Android 系统中进程间通信的机制）相关的 IOCTL（输入输出控制）函数，如果监控到与 Package Manager（Android 系统中对安装包进行管理的服务）相关的内容，即需要启动 Package Manager，则将安装请求转发给企业管理客户端中负责应用黑白名单判断逻辑的 Service（服务），由负责应用黑白名单判断逻辑的 Service 判断是否允许安装，如果允许，则将该安装请求转发给 Package Manager，如果不允许，则向具有 Root 权限的 Service 返回一个错误信息。

[0074] 本发明实施例中，根据应用黑名单或应用白名单，企业管理客户端不仅可以对待安装的应用程序进行管理，还可以对个人区内存空间中已安装的应用程序进行管理，包括如下两种情况：

[0075] 第一种情况、企业管理客户端接收到企业管理服务器配置的应用黑名单时，根据应用黑名单中列出的应用程序的名称及版本号检测个人区内存空间中是否安装有应用黑名单中列出的应用程序，并针对检测到的应用程序发出应用程序禁止安装的告警信息；

[0076] 第二种情况、企业管理客户端接收到企业管理服务器配置的应用白名单时，根据应用白名单中列出的应用程序的名称及版本号检测个人区内存空间中是否安装有应用白名单中未列出的应用程序；并针对检测到的应用程序发出应用程序禁止安装的告警信息。

[0077] 本发明实施例提供的应用程序的安装控制方法，由企业管理服务器和安装在移动终端上的企业管理客户端组成了移动终端的企业管理系统，对移动终端上的应用程序进行安全管理。企业管理服务器向企业管理客户端推送应用自由安装列表，用户仅能针对应用自由安装列表中列出的应用程序发起安装，保证了应用程序来源的安全可靠性；针对待安装的应用程序发起安装请求后，采用应用黑白名单机制进行控制，仅允许对未在应用黑名单中的应用程序或者在应用白名单中的应用程序进行安装，而禁止其他应用程序的安装，避免了移动终端上的企业数据被恶意应用非法上传、共享和外泄的风险，从而有效保护企业信息安全。需要说明的是，由于应用黑名单中规定了不能安装的应用程序，应用白名单中

规定了只能安装的应用程序，两者在逻辑上是无法共存的，所以企业管理客户端上仅能配置应用黑名单或应用白名单中的任意一种，而不能同时配置应用黑名单和应用白名单。下面针对企业管理客户端上配置有应用黑名单或应用白名单的方案分别进行说明。

[0078] 首先对企业管理客户端上配置有应用黑名单的方案进行说明，如图 3 所示，企业管理客户端上配置有应用黑名单时应用程序的安装控制方法，包括如下步骤：

[0079] S300、企业管理服务器向企业管理客户端推送应用自由安装列表，下发应用黑名单；

[0080] S301、企业管理客户端在桌面上展示应用自由安装列表；

[0081] S302、企业用户根据展示的应用自由安装列表选择待安装的应用程序后发起安装请求；

[0082] S303、企业管理客户端确认配置有应用黑名单；

[0083] S304、企业管理客户端判断待安装的应用程序是否在应用黑名单中，如果是，则执行 S305，如果否，则执行 S306；

[0084] S305、企业管理客户端禁止该应用程序的安装；

[0085] S306、企业管理客户端对该应用程序进行安装。

[0086] 接着对企业管理客户端上配置有应用白名单的方案进行说明，如图 4 所示，企业管理客户端上配置有应用白名单时应用程序的安装控制方法，包括如下步骤：

[0087] S400、企业管理服务器向企业管理客户端推送应用自由安装列表，下发应用白名单；

[0088] S401、企业管理客户端在桌面上展示应用自由安装列表；

[0089] S402、企业用户根据展示的应用自由安装列表选择待安装的应用程序后发起安装请求；

[0090] S403、企业管理客户端确认配置有应用白名单；

[0091] S404、企业管理客户端判断待安装的应用程序是否在应用白名单中，如果否，则执行 S405，如果是，则执行 S406；

[0092] S405、企业管理客户端禁止该应用程序的安装；

[0093] S406、企业管理客户端对该应用程序进行安装。

[0094] 基于同一技术构思，本发明实施例提供了一种移动终端的企业管理系统，用以对移动终端上的应用程序实现安全管理，从而有效保护企业信息安全，如图 5 所示，包括企业管理服务器 501 和安装在移动终端上的企业管理客户端 502，一般情况下，企业管理客户端 502 有多个，分别安装在各需要被管理的移动终端上。其中：

[0095] 企业管理服务器 501，用于向企业管理客户端 502 推送应用自由安装列表；

[0096] 企业管理客户端 502，用于接收针对应用自由安装列表中列出的应用程序发起的安装请求；确认配置有应用黑名单时，判断待安装的应用程序是否在所述应用黑名单中，如果是，则禁止该应用程序的安装，否则，对该应用程序进行安装；确认配置有应用白名单时，判断待安装的应用程序是否在应用白名单中，如果是，则对该应用程序进行安装，否则，禁止该应用软件的安装。

[0097] 具体实施中，企业管理服务器 501，还用于对上传到本企业管理服务器的应用程序的安装包进行病毒检测和加固处理后保存。

[0098] 具体实施中，企业管理服务器501，还用于根据自身维护的应用管理列表、以及各用户组的应用管理策略，为每个用户组生成对应的应用自由安装列表，并将每个用户组对应的应用自由安装列表推送到该用户组中各用户的企业管理客户端502上，其中，应用管理列表中包括所有安装包已上传到企业管理服务器501的应用程序的名称及版本号，所述应用自由安装列表中包括供用户组自由安装的应用程序的名称及版本号。

[0099] 具体实施中，如果判断出对待安装的应用程序进行安装，则企业管理客户端502，具体用于使用提取的超级用户Root权限，根据安装请求从企业管理服务器501处下载该应用程序的安装包并在个人区内存空间中进行自动安装，其中，个人区内存空间是指移动终端的内存空间中工作区内存空间之外的内存空间，工作区内存空间是指分配给所述企业管理客户端的内存空间。

[0100] 具体实施中，如果判断出禁止对待安装的应用程序的安装，则企业管理客户端502，具体用于使用提取的Root权限，禁止从企业管理服务器501处下载该应用程序的安装包，并发出应用程序禁止安装的告警信息。

[0101] 具体实施中，企业管理服务器501，还用于将应用黑名单或应用白名单配置给企业管理客户端502；

[0102] 为了实现对已安装的应用程序的管理，企业管理客户端502，还用于接收到企业管理服务器501配置的应用黑名单时，根据应用黑名单中列出的应用程序的名称及版本号检测个人区内存空间中是否安装有应用黑名单中列出的应用程序，并针对检测到的应用程序发出应用程序禁止安装的告警信息；接收到企业管理服务器501配置的应用白名单时，根据应用白名单中列出的应用程序的名称及版本号检测个人区内存空间中是否安装有应用白名单中未列出的应用程序；并针对检测到的应用程序发出应用程序禁止安装的告警信息。

[0103] 基于同一技术构思，本发明实施例还提供一种企业管理客户端装置，该企业管理客户端装置安装在移动终端上，如图6所示，该企业管理客户端装置的一种可能结构，包括：

[0104] 接收模块601，用于接收针对应用自由安装列表中列出的应用程序发起的安装请求；

[0105] 确认模块602，用于确认是否配置有应用黑名单或者应用白名单；

[0106] 第一控制模块603，用于当确认模块602确认配置有应用黑名单时，判断待安装的应用程序是否在应用黑名单中，如果是，则禁止该应用程序的安装，否则，对该应用程序进行安装；

[0107] 第二控制模块604，用于当确认模块602确认配置有应用白名单时，判断待安装的应用程序是否在应用白名单中，如果是，则对该应用程序进行安装，否则，禁止该应用软件的安装。

[0108] 本申请的实施例所提供的企业管理客户端装置可通过计算机程序实现。本领域技术人员应该能够理解，上述的模块划分方式仅是众多模块划分方式中的一种，如果划分为其他模块或不划分模块，只要搜索直达服务器具有上述功能，都应该在本申请的保护范围之内。

[0109] 本领域的技术人员应明白，本发明的实施例可提供为方法、系统、设备或计算机程

序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[0110] 本发明是参照根据本发明实施例的方法、设备（系统）和计算机程序产品的流程图和／或方框图来描述的。应理解可由计算机程序指令实现流程图和／或方框图中的每一流程和／或方框、以及流程图和／或方框图中的流程和／或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的装置。

[0111] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能。

[0112] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的步骤。

[0113] 尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

[0114] 显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

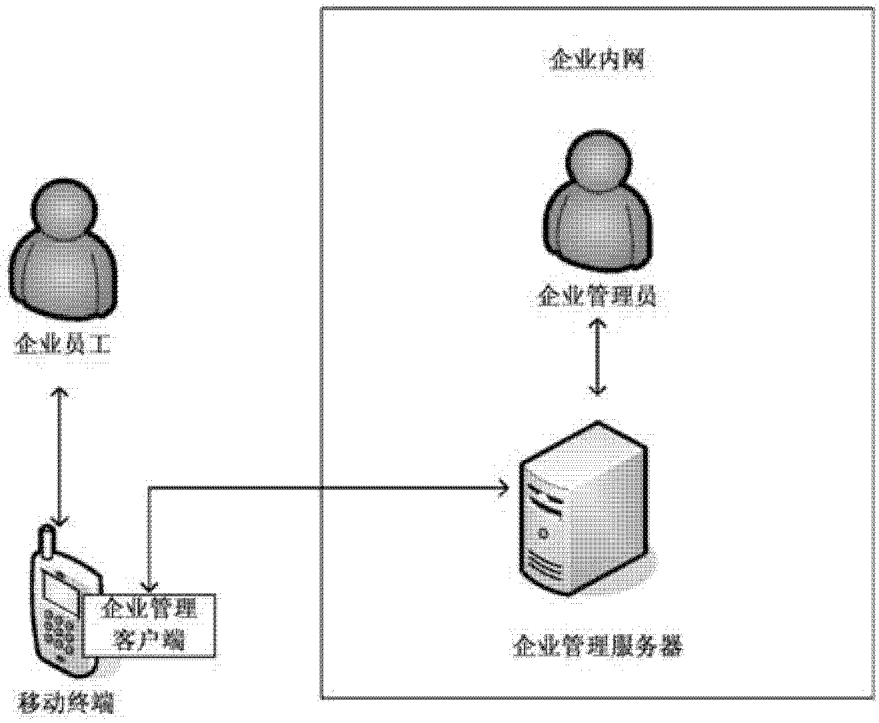

企业内网
企业管理员
企业员工
企业管理
客户端
移动终端
企业管理服务器

图 1

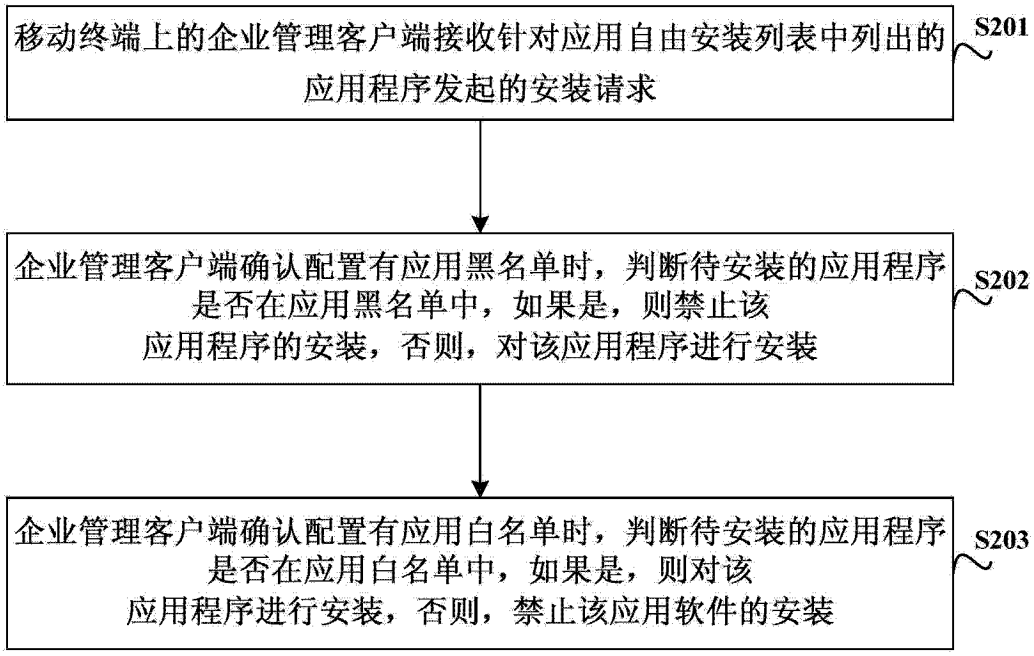

移动终端上的企业管理客户端接收针对应用自由安装列表中列出的应用程序发起的安装请求
S201
企业管理客户端确认配置有应用黑名单时，判断待安装的应用程序是否在应用黑名单中，如果是，则禁止该应用程序的安装，否则，对该应用程序进行安装
S202
企业管理客户端确认配置有应用白名单时，判断待安装的应用程序是否在应用白名单中，如果是，则对该应用程序进行安装，否则，禁止该应用软件的安装
S203

图 2

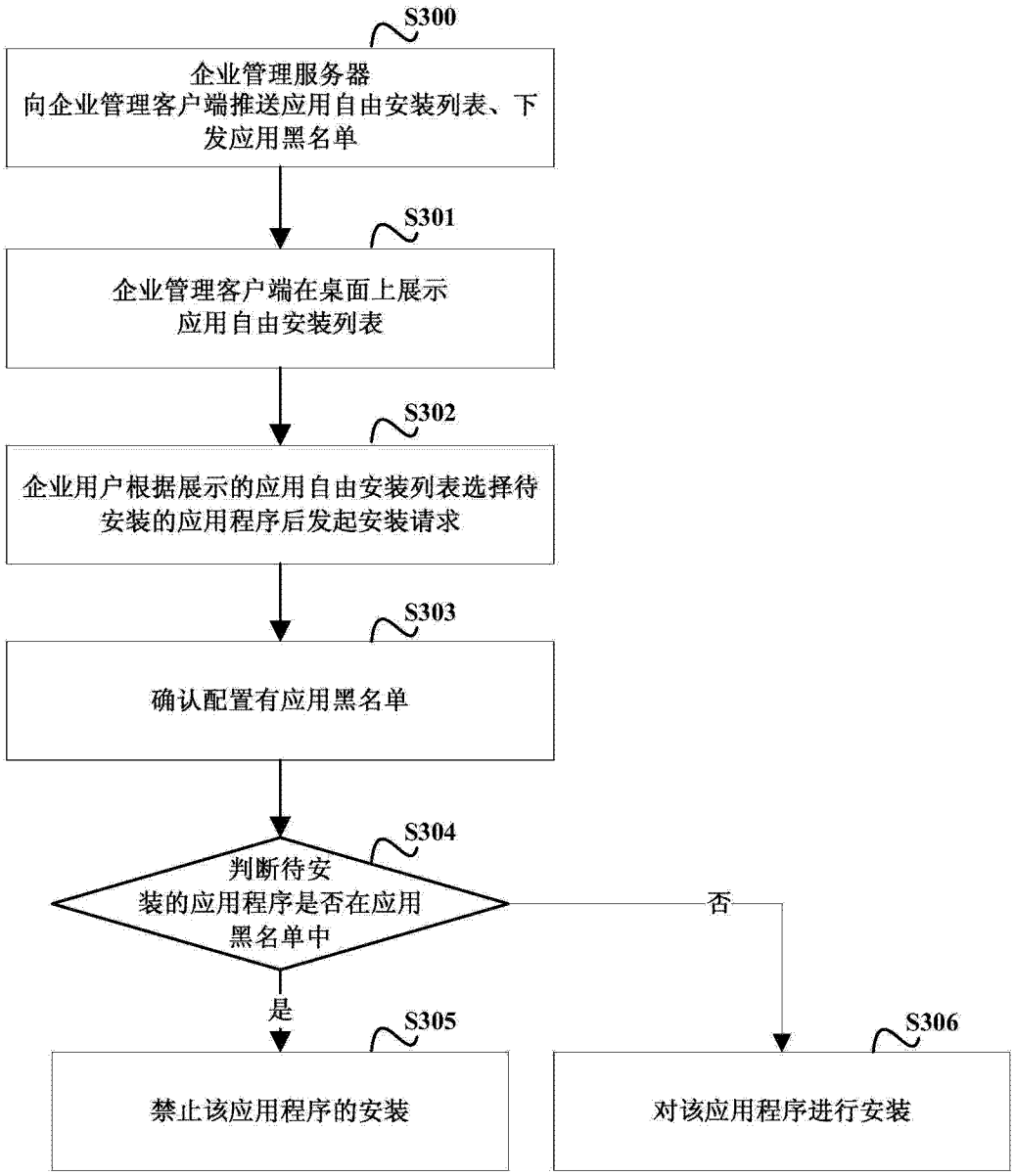

S300
企业管理服务器
向企业管理客户端推送应用自由安装列表、下发应用黑名单
S301
企业管理客户端在桌面上展示
应用自由安装列表
S302
企业用户根据展示的应用自由安装列表选择待安装的应用程序后发起安装请求
S303
确认配置有应用黑名单
S304
判断待安装的应用程序是否在应用黑名单中
否
是
S305
禁止该应用程序的安装
S306
对该应用程序进行安装

图 3

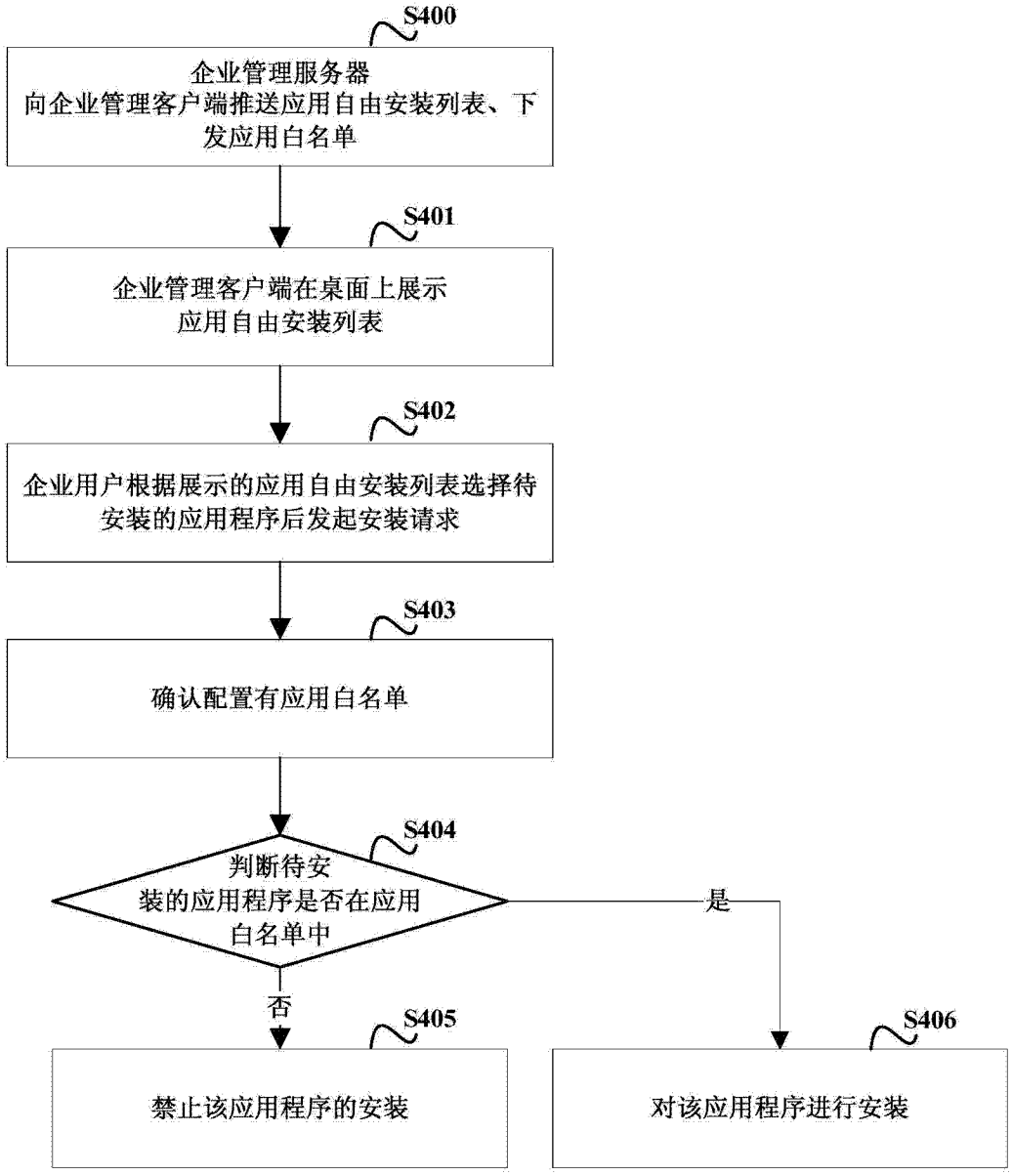

S400
企业管理服务器
向企业管理客户端推送应用自由安装列表、下发应用白名单
S401
企业管理客户端在桌面上展示
应用自由安装列表
S402
企业用户根据展示的应用自由安装列表选择待安装的应用程序后发起安装请求
S403
确认配置有应用白名单
S404
判断待安装的应用程序是否在应用白名单中
是
否
S405
禁止该应用程序的安装
S406
对该应用程序进行安装

图 4

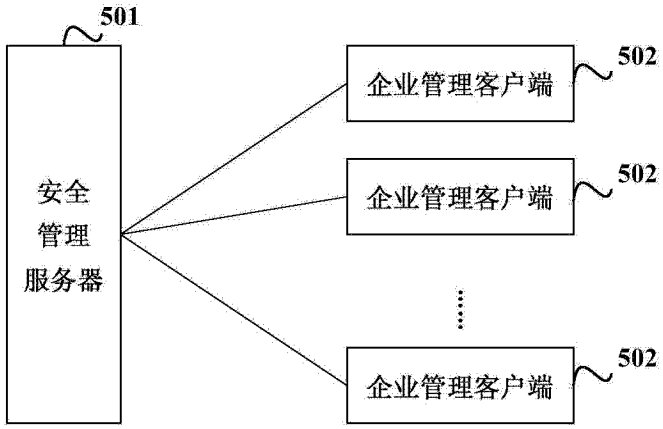

501
安全
管理
服务器
企业管理客户端
502
企业管理客户端
502
企业管理客户端
502

图 5

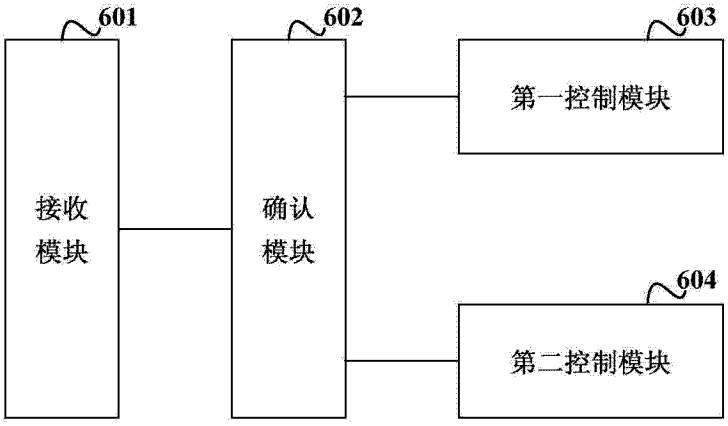

601
接收
模块
602
确认
模块
603
第一控制模块
604
第二控制模块

图 6