(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 106339629 A
(43)申请公布日 2017.01.18

(21)申请号 201610701670.5

(22)申请日 2016.08.22

(71)申请人 浪潮(苏州)金融技术服务有限公司
地址 215104 江苏省苏州市吴中经济开发区越溪街道塔韵路178号1幢2层

(72)发明人 张家重 董毅 李光瑞 王玉奎

(74)专利代理机构 济南信达专利事务所有限公司 37100
代理人 李世喆

(51)Int.Cl.
G06F 21/55(2013.01)

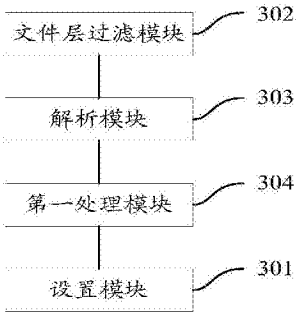
权利要求书3页 说明书10页 附图4页

(54)发明名称

一种应用程序管理方法及装置

(57)摘要

本发明提供了一种应用程序管理方法及装置，其中，方法包括：预先设置至少一个第一应用程序的文件访问规则；在操作系统运行所述至少一个第一应用程序之后，截获所述至少一个第一应用程序发起的文件访问请求；解析所述文件访问请求以确定所述文件访问请求对应的目标应用程序和目标文件对象；根据所述文件访问规则判断所述目标应用程序是否可以访问所述目标文件对象，如果是，则释放所述文件访问请求，以使所述操作系统响应所述文件访问请求；否则，拦截所述文件访问请求。通过本发明的技术方案，可提高操作系统的安全性。



CN 106339629 A

1.一种应用程序管理方法,其特征在于,包括:

预先设置至少一个第一应用程序的文件访问规则;

在操作系统运行所述至少一个第一应用程序之后,截获所述至少一个第一应用程序发起的文件访问请求;

解析所述文件访问请求以确定所述文件访问请求对应的目标应用程序和目标文件对象;

根据所述文件访问规则判断所述目标应用程序是否可以访问所述目标文件对象,如果是,则释放所述文件访问请求,以使所述操作系统响应所述文件访问请求;否则,拦截所述文件访问请求。

2.根据权利要求1所述的应用程序管理方法,其特征在于,

在所述拦截所述文件访问请求之后,还包括:

记录在设定时间长度的一个检测周期内拦截的对应所述目标应用程序的文件访问请求的拦截数量,当所述拦截数量大于预先设定的标准参数时,产生告警信息,并将所述告警信息发送至外部告警系统,以使外部告警系统进行告警。

3.根据权利要求1所述的应用程序管理方法,其特征在于,

所述预先设置至少一个第一应用程序的文件访问规则,包括:预先设置文件访问规则链表,其中,所述文件访问规则链表用于存储所述至少一个第一应用程序与至少一个文件对象之间的对应关系;

所述根据所述文件访问规则判断所述目标应用程序是否可以访问所述目标文件对象,包括:查询所述文件访问规则链表,判断所述文件访问规则链表中是否存在所述目标应用程序与所述目标文件对象之间的对应关系。

4.根据权利要求1所述的应用程序管理方法,其特征在于,

所述预先设置至少一个第一应用程序的文件访问规则,包括:预先设置至少一个第一应用程序分别对应的至少两个权限维度;其中,每一个所述权限维度分别与所述操作系统的至少一种工作状态相对应;

所述根据所述文件访问规则判断所述目标应用程序是否可以访问所述目标文件对象,包括:

获取所述操作系统的运行参数;

根据所述运行参数确定所述操作系统的至少一种目标工作状态;

确定所述目标应用程序在所述操作系统处于所述至少一种目标工作状态时对应的目标权限维度;

根据所述目标权限维度判断所述目标应用程序是否可以访问所述目标访问对象。

5.根据权利要求4所述的应用程序管理方法,其特征在于,

所述操作系统的至少一种工作状态包括如下工作状态中的一种或多种:

安装所述操作系统的终端设备与外部网络相连通、安装所述操作系统的终端设备与外部网络未连通、所述目标应用程序在设定时间长度的一个检测周期内访问所述操作系统的系统文件的次数大于预先设定的阈值。

6.根据权利要求1至5中任一所述的应用程序管理方法,其特征在于,

还包括:预先设置至少一个第二应用程序的用户启动规则;

截获对应所述至少一个第二应用程序的运行指令；

获取在当前时刻已经登录所述操作系统的登录用户的用户信息；

根据所述用户信息及所述用户启动规则，确定所述至少一个第二应用程序是否包括所述登录用户可以启动的至少一个第一应用程序，如果是，则释放所述运行指令，以使所述操作系统运行所述至少一个第一应用程序；否则，拦截所述运行指令。

7.一种应用程序管理装置，其特征在于，包括：

设置模块，用于预先设置至少一个第一应用程序的文件访问规则；

文件层过滤模块，用于在操作系统运行所述至少一个第一应用程序之后，截获所述至少一个第一应用程序发起的文件访问请求；

解析模块，用于解析所述文件访问请求以确定所述文件访问请求对应的目标应用程序和目标文件对象；

第一处理模块，用于根据所述文件访问规则判断所述目标应用程序是否可以访问所述目标文件对象，如果是，则释放所述文件访问请求，以使所述操作系统响应所述文件访问请求；否则，拦截所述文件访问请求。

8.根据权利要求7所述的应用程序管理装置，其特征在于，

还包括：告警处理模块，用于记录在设定时间长度的一个检测周期内拦截的对应所述目标应用程序的文件访问请求的拦截数量，当所述拦截数量大于预先设定的标准参数时，产生告警信息，并将所述告警信息发送至外部告警系统，以使外部告警系统进行告警；

和/或，

所述设置模块，用于预先设置文件访问规则链表，其中，所述文件访问规则链表用于存储所述至少一个第一应用程序与至少一个文件对象之间的对应关系；

所述第一处理模块，用于查询所述文件访问规则链表，判断所述文件访问规则链表中是否存在所述目标应用程序与所述目标文件对象之间的对应关系。

9.根据权利要求7所述的应用程序管理装置，其特征在于，

所述设置模块，用于预先设置至少一个第一应用程序分别对应的至少两个权限维度；其中，每一个所述权限维度分别与所述操作系统的至少一种工作状态相对应；

所述第一处理模块，包括：

获取子单元，用于获取所述操作系统的运行参数；

第一确定子单元，用于根据所述运行参数确定所述操作系统的至少一种目标工作状态；

第二确定子单元，用于确定所述目标应用程序在所述操作系统处于所述至少一种目标工作状态时对应的目标权限维度；

处理子单元，用于根据所述目标权限维度判断所述目标应用程序是否可以访问所述目标访问对象。

10.根据权利要求6至9中任一所述的应用程序管理装置，其特征在于，

所述设置模块，进一步用于预先设置至少一个第二应用程序的用户启动规则；

还包括：应用层过滤模块、获取模块和第二处理模块；其中，

所述应用层过滤模块，用于截获对应所述至少一个第二应用程序的运行指令；

所述获取模块，用于获取在当前时刻已经登录所述操作系统的登录用户的用户信息；

所述第二处理模块，用于根据所述用户信息及所述用户启动规则，确定所述至少一个第二应用程序是否包括所述登录用户可以启动的至少一个第一应用程序，如果是，则释放所述运行指令，以使所述操作系统运行所述至少一个第一应用程序；否则，拦截所述运行指令。

一种应用程序管理方法及装置

技术领域

[0001] 本发明涉及计算机技术领域，特别涉及一种应用程序管理方法、装置及系统。

背景技术

[0002] 随着计算机技术的不断发展，计算机操作系统中安装的各类应用程序也日益增多，当应用程序本身存在漏洞时，入侵者则可利用该漏洞在应用程序中植入木马病毒，进而在操作系统中运行该应用程序执行相应的任务(比如读写操作系统的系统文件)以威胁操作性系统安全。

[0003] 目前，主要通过特征码识别技术来提高操作系统的安全性，具体地，通过提取现有木马病毒的特征码并加载至特征码识别库，判断应用程序中是否存在与特征码识别库中相同的特征码，如果是，则阻止该应用程序在操作系统中运行。

[0004] 但是，在上述技术方案中，由于木马病毒更新速度极快，特征码的提取总是滞后于木马病毒的更新速度，使得应用程序在被植入新的目标病毒后，即可通过该应用程序在操作系统的相应文件对象下读写业务数据，操作系统的安全性较低。

发明内容

[0005] 本发明实施例提供了一种应用程序管理方法及装置，可提高操作系统的安全性。

[0006] 第一方面，本发明实施例提供了一种应用程序管理方法，包括：

[0007] 预先设置至少一个第一应用程序的文件访问规则；

[0008] 在操作系统运行所述至少一个第一应用程序之后，截获所述至少一个第一应用程序发起的文件访问请求；

[0009] 解析所述文件访问请求以确定所述文件访问请求对应的目标应用程序和目标文件对象；

[0010] 根据所述文件访问规则判断所述目标应用程序是否可以访问所述目标文件对象，如果是，则释放所述文件访问请求，以使所述操作系统响应所述文件访问请求；否则，拦截所述文件访问请求。

[0011] 优选地，

[0012] 在所述拦截所述文件访问请求之后，还包括：

[0013] 记录在设定时间长度的一个检测周期内拦截的对应所述目标应用程序的文件访问请求的拦截数量，当所述拦截数量大于预先设定的标准参数时，产生告警信息，并将所述告警信息发送至外部告警系统，以使外部告警系统进行告警。

[0014] 优选地，

[0015] 所述预先设置至少一个第一应用程序的文件访问规则，包括：预先设置文件访问规则链表，其中，所述文件访问规则链表用于存储所述至少一个第一应用程序与至少一个文件对象之间的对应关系；

[0016] 所述根据所述文件访问规则判断所述目标应用程序是否可以访问所述目标文件

对象，包括：查询所述文件访问规则链表，判断所述文件访问规则链表中是否存在所述目标应用程序与所述目标文件对象之间的对应关系。

[0017] 优选地，

[0018] 所述预先设置至少一个第一应用程序的文件访问规则，包括：预先设置至少一个第一应用程序分别对应的至少两个权限维度；其中，每一个所述权限维度分别与所述操作系统的至少一种工作状态相对应；

[0019] 所述根据所述文件访问规则判断所述目标应用程序是否可以访问所述目标文件对象，包括：

[0020] 获取所述操作系统的运行参数；

[0021] 根据所述运行参数确定所述操作系统的至少一种目标工作状态；

[0022] 确定所述目标应用程序在所述操作系统处于所述至少一种目标工作状态时对应的目标权限维度；

[0023] 根据所述目标权限维度判断所述目标应用程序是否可以访问所述目标访问对象。

[0024] 优选地，

[0025] 所述操作系统的至少一种工作状态包括如下工作状态中的一种或多种：

[0026] 安装所述操作系统的终端设备与外部网络相连通、安装所述操作系统的终端设备与外部网络未连通、所述目标应用程序在设定时间长度的一个检测周期内访问所述操作系统的系统文件的次数大于预先设定的阈值。

[0027] 优选地，

[0028] 还包括：预先设置至少一个第二应用程序的用户启动规则；

[0029] 截获对应所述至少一个第二应用程序的运行指令；

[0030] 获取在当前时刻已经登录所述操作系统的登录用户的用户信息；

[0031] 根据所述用户信息及所述用户启动规则，确定所述至少一个第二应用程序是否包括所述登录用户可以启动的至少一个第一应用程序，如果是，则释放所述运行指令，以使所述操作系统运行所述至少一个第一应用程序；否则，拦截所述运行指令。

[0032] 第二方面，本发明实施例提供了一种应用程序管理装置，包括：

[0033] 设置模块，用于预先设置至少一个第一应用程序的文件访问规则；

[0034] 文件层过滤模块，用于在操作系统运行所述至少一个第一应用程序之后，截获所述至少一个第一应用程序发起的文件访问请求；

[0035] 解析模块，用于解析所述文件访问请求以确定所述文件访问请求对应的目标应用程序和目标文件对象；

[0036] 第一处理模块，用于根据所述文件访问规则判断所述目标应用程序是否可以访问所述目标文件对象，如果是，则释放所述文件访问请求，以使所述操作系统响应所述文件访问请求；否则，拦截所述文件访问请求。

[0037] 优选地，

[0038] 还包括：告警处理模块，用于记录在设定时间长度的一个检测周期内拦截的对应所述目标应用程序的文件访问请求的拦截数量，当所述拦截数量大于预先设定的标准参数时，产生告警信息，并将所述告警信息发送至外部告警系统，以使外部告警系统进行告警；

[0039] 和/或，

[0040] 所述设置模块，用于预先设置文件访问规则链表，其中，所述文件访问规则链表用于存储所述至少一个第一应用程序与至少一个文件对象之间的对应关系；

[0041] 所述第一处理模块，用于查询所述文件访问规则链表，判断所述文件访问规则链表中是否存在所述目标应用程序与所述目标文件对象之间的对应关系。

[0042] 优选地，

[0043] 所述设置模块，用于预先设置至少一个第一应用程序分别对应的至少两个权限维度；其中，每一个所述权限维度分别与所述操作系统的至少一种工作状态相对应；

[0044] 所述第一处理模块，包括：

[0045] 获取子单元，用于获取所述操作系统的运行参数；

[0046] 第一确定子单元，用于根据所述运行参数确定所述操作系统的至少一种目标工作状态；

[0047] 第二确定子单元，用于确定所述目标应用程序在所述操作系统处于所述至少一种目标工作状态时对应的目标权限维度；

[0048] 处理子单元，用于根据所述目标权限维度判断所述目标应用程序是否可以访问所述目标访问对象。

[0049] 优选地，

[0050] 所述设置模块，进一步用于预先设置至少一个第二应用程序的用户启动规则；

[0051] 还包括：应用层过滤模块、获取模块和第二处理模块；其中，

[0052] 所述应用层过滤模块，用于截获对应所述至少一个第二应用程序的运行指令；

[0053] 所述获取模块，用于获取在当前时刻已经登录所述操作系统的登录用户的用户信息；

[0054] 所述第二处理模块，用于根据所述用户信息及所述用户启动规则，确定所述至少一个第二应用程序是否包括所述登录用户可以启动的至少一个第一应用程序，如果是，则释放所述运行指令，以使所述操作系统运行所述至少一个第一应用程序；否则，拦截所述运行指令。

[0055] 本发明实施例提供了一种应用程序管理方法及装置，通过预先设置至少一个第一应用程序的文件访问规则，在操作系统运行第一应用程序后，截获每一个第一应用程序发起的文件访问请求，解析截获的文件访问请求以确定当前文件访问请求对应的目标应用程序和目标文件对象(比如操作系统的系统文件、日志文件等)，即确定发起该文件访问请求的目标应用程序以及该目标应用程序执行本次数据访问任务时需要访问的目标文件对象，进而根据预先设定的文件访问规则判断目标应用程序是否可以访问目标文件对象，只有预先设定的文件访问规则中允许目标应用程序访问目标文件对象时，才释放截获的文件访问请求，使得操作系统响应该文件访问请求(比如在目标文件对象内读写业务数据)，否则，拦截该文件访问请求，使得操作系统不会响应该文件访问请求；综上可见，本发明实施例提供的技术方案中，通过限定应用程序可访问的文件对象的范围，使得入侵者不能访问不在当前应用程序可访问的文件对象范围内的其他文件对象，避免应用程序在被入侵者控制后，通过该应用程序继续入侵操作系统，可提高操作系统的安全性。

附图说明

[0056] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0057] 图1是本发明一实施例提供的一种应用程序管理方法的流程图；

[0058] 图2是本发明一实施例提供的另一种应用程序管理方法的流程图；

[0059] 图3是本发明一实施例提供的一种应用程序管理装置的结构图；

[0060] 图4是本发明一实施例提供的另一种应用程序管理装置的结构图；

[0061] 图5是本发明一实施例提供的又一种应用程序管理装置的结构图；

[0062] 图6是本发明一实施例提供的再一种应用程序管理装置的结构图。

具体实施方式

[0063] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例，基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0064] 如图1所示，本发明实施例提供了一种应用程序管理方法，包括：

[0065] 步骤101，预先设置至少一个第一应用程序的文件访问规则；

[0066] 步骤102，在操作系统运行所述至少一个第一应用程序之后，截获所述至少一个第一应用程序发起的文件访问请求；

[0067] 步骤103，解析所述文件访问请求以确定所述文件访问请求对应的目标应用程序和目标文件对象；

[0068] 步骤104根据所述文件访问规则判断所述目标应用程序是否可以访问所述目标文件对象，如果是，则释放所述文件访问请求，以使所述操作系统响应所述文件访问请求；否则，拦截所述文件访问请求。

[0069] 本发明上述实施例中，通过预先设置至少一个第一应用程序的文件访问规则，在操作系统运行第一应用程序后，截获每一个第一应用程序发起的文件访问请求，解析截获的文件访问请求以确定当前文件访问请求对应的目标应用程序和目标文件对象(比如操作系统的系统文件、日志文件等)，即确定发起该文件访问请求的目标应用程序以及该目标应用程序执行本次数据访问任务时需要访问的目标文件对象，进而根据预先设定的文件访问规则判断目标应用程序是否可以访问目标文件对象，只有预先设定的文件访问规则中允许目标应用程序访问目标文件对象时，才释放截获的文件访问请求，使得操作系统响应该文件访问请求(比如在目标文件对象内读写业务数据)，否则，拦截该文件访问请求，使得操作系统不会响应该文件访问请求；综上可见，本发明实施例提供的技术方案中，通过限定应用程序可访问的文件对象的范围，使得入侵者不能访问不在当前应用程序可访问的文件对象范围内的其他文件对象，避免应用程序在被入侵者控制后，通过该应用程序继续入侵操作系统，可提高操作系统的安全性。

[0070] 具体地，本发明一个优选实施例中，所述预先设置至少一个第一应用程序的文件访问规则，包括：预先设置文件访问规则链表，其中，所述文件访问规则链表用于存储所述

至少一个第一应用程序与至少一个文件对象之间的对应关系；

[0071] 所述根据所述文件访问规则判断所述目标应用程序是否可以访问所述目标文件对象，包括：查询所述文件访问规则链表，判断所述文件访问规则链表中是否存在所述目标应用程序与所述目标文件对象之间的对应关系。

[0072] 本发明上述实施例中，工作人员仅需要向文件访问规则链表填充至少一个第一应用程序与至少一个文件对象之间的对应关系，在截获到至少一个第一应用程序发起的文件访问请求后，在不改变操作系统原本的权限配置信息的前提下，即可根据该文件访问规则链表来实现控制释放或拦截已经截获的文件访问请求；同时，文件访问规则链表中仅存储至少一个应用程序与至少一个文件对象之间的对应关系，无需向文件访问规则链表中写入每一个文件对象的详细路径，用户体验较好。

[0073] 本发明一实施例中，预先设置的文件访问规则种，还可以根据文件对象的类型限定每一个第一应用程序可访问文件对象的范围，比如，限定一个目标应用程序只能访问指定文件类型的文件(比如txt文本文件)，相应的，在确定出文件对象访问请求对应的目标文件对象后，进一步识别目标文件对象的文件类型，进而根据预先设定的文件访问规则判断确定的目标应用程序是否可以访问该类型的目标文件对象；具体地，这里可以通过目标文件的文件名后缀名或文件二进制数据类型确定目标文件的文件类型。

[0074] 进一步的，用户可结合每一个第一应用程序本身的特性合理设置至少一个第一应用程序的文件访问规则；举例来说，在文件访问规则中将当前第一应用程序在正常工作时必须访问的文件对象设置为当前第一应用程序可以访问的文件对象，如果当前第一应用程序在设定的时间段内频繁请求访问其正常工作时并不需要访问的其他文件对象时，则说明当前第一应用程序可能存在漏洞，且已经被入侵者控制；相应的，本发明一个优选实施例中，在所述拦截所述文件访问请求之后，还包括：

[0075] 记录在设定时间长度的一个检测周期内拦截的对应所述目标应用程序的文件访问请求的拦截数量，当所述拦截数量大于预先设定的标准参数时，产生告警信息，并将所述告警信息发送至外部告警系统，以使外部告警系统进行告警。

[0076] 本发明上述实施例中，对应目标应用程序的文件访问请求的拦截数量，即为目标应用程序在设定时间长度的一个检测周期内请求访问其正常工作时并不需要访问的其他文件对象的次数，检测周期的时间长度以及标准参数可以通过相应数量的样本分析来确定，在该次数大于预先设定的标准参数时，则说明目标应用程序可能存在漏洞，且已经被入侵者控制，产生告警信息并发送至外部告警系统，外部告警系统根据该告警信息进行告警，可提醒工作人员及时针对该目标应用程序进行相应的处理。

[0077] 进一步的，由于操作系统在不同工作状态时，其本身的安全程度并不相同，比如，在一个利用一台服务器和多个终端设备搭建的数据管理系统中，服务器可实时监控并维护各个终端设备的运行状态，服务器监控到终端设备的操作系统被非法入侵时，可及时修复被入侵的操作系统，以防止被入侵的操作系统被进一步破坏，安全性较高；相反地，服务器与终端设备断开连接时，终端设备中操作系统的安全性较低；因此，在操作系统处于不同安全程度的工作状态时，同一个应用程序可对应不同的文件访问规则，相应的，本发明一个优选实施例中，所述预先设置至少一个第一应用程序的文件访问规则，包括：预先设置至少一个第一应用程序分别对应的至少两个权限维度；其中，每一个所述权限维度分别与所述操

作系统的至少一种工作状态相对应；

[0078] 所述根据所述文件访问规则判断所述目标应用程序是否可以访问所述目标文件对象，包括：

[0079] 获取所述操作系统的运行参数；

[0080] 根据所述运行参数确定所述操作系统的至少一种目标工作状态；

[0081] 确定所述目标应用程序在所述操作系统处于所述至少一种目标工作状态时对应的目标权限维度；

[0082] 根据所述目标权限维度判断所述目标应用程序是否可以访问所述目标访问对象。

[0083] 具体的，本发明一个优选实施例中，所述操作系统的至少一种工作状态包括如下工作状态中的一种或多种：

[0084] 安装所述操作系统的终端设备与外部网络相连通、安装所述操作系统的终端设备与外部网络未连通、所述目标应用程序在设定时间长度的一个检测周期内访问所述操作系统的系统文件的次数大于预先设定的阈值。

[0085] 举例来说，安装操作系统的终端设备与外部网络未连通时，即终端设备处于离线状态时，其安全性较低，可设置应用程序A在安装操作系统的终端设备处于离线状态时对应的一个权限维度a1中，应用程序A具备n个方向上的访问权限，即访问n种资源(n种类型的文件对象或n个文件对象)；相反的，在安装操作系统的终端设备通过外部网络与对应的服务器相连通时，其安全性较高，可设置应用程序A在安装操作系统的终端设备处于联网状态时对应的另一个权限维度a2中，应用程序A具备n+m个方向上的访问权限，即在操作系统本身的安全等级较高时，可为其开放更多的访问权限，使得应用程序可访问n+m种资源。

[0086] 本发明一实施例中，操作系统的运行参数可以包括安装当前操作系统的终端设备中，用于连接其对应的服务器的网络端口的工作参数，该参数应当反应当前终端设备是否通过外部网络与对应的服务器相连通。

[0087] 为了进一步提高操作系统的安全性，防止入侵者通过截获的用户账号入侵操作系统，还可以对不同用户分别对应的管理权限做进一步限定，即为不同的用户分配不同的权限管理维度以限定当前用户登录操作系统时，操作系统可以运行的应用程序；具体地，本发明一个优选实施例中，还包括：预先设置至少一个第二应用程序的用户启动规则；

[0088] 截获对应所述至少一个第二应用程序的运行指令；

[0089] 获取在当前时刻已经登录所述操作系统的登录用户的用户信息；

[0090] 根据所述用户信息及所述用户启动规则，确定所述至少一个第二应用程序是否包括所述登录用户可以启动的至少一个第一应用程序，如果是，则释放所述运行指令，以使所述操作系统运行所述至少一个第一应用程序；否则，拦截所述运行指令。

[0091] 举例来说，安装在操作系统中的应用程序包括A、B和C，对应的用户启动规则为：用户user可控制应用程序A运行，用户administrator可控制应用程序A、B运行，与安装当前操作系统的终端设备相连的服务器可控制应用程序A、B和C运行；那么，在截获到对应应用程序B的运行指令后，如果在当前时刻已经登陆操作系统的用户为guest，则拦截该运行指令，如果在当前时刻已经登陆操作系统的用户为administrator，则释放该运行指令。需要说明的是，在用户登录操作系统时，还可以识别该登录请求，如果预先设置的用户启动规则中，并不存在针对该登录请求对应的用户的权限限定，则拦截该登录请求；举例来说，如果数据

库的管理员账号为root，入侵者使用非法手段获得了root账号的权限并试图登录以访问数据库，当预先设置的用户启动规则中并不存在root用户的相关权限限定时，则拦截该登录请求，以拒绝root账号的登录。如此，防止入侵者通过截获的用户账号登录操作系统，越权启动相应的应用程序以威胁操作系统安全。

[0092] 综上所述，本发明上述实施例中所述的应用程序管理方法，可实现根据操作系统所处的当前工作状态，对安装在操作系统中的各个应用程序能否在操作系统中运行进行限定，且同时对能够运行在操作系统中的应用程序的文件访问权限进行限定；如此，通过限制安装在操作系统中的应用程序的越权运行和越权访问，可避免应用程序本身被入侵者利用而威胁操作系统安全。

[0093] 如图2所示，本发明实施例提供了一种应用程序管理方法，该方法可以包括如下步骤：

[0094] 步骤201，设置操作系统中需要监控的至少一个应用程序的用户启动规则。

[0095] 举例来说，当用户需要监控的应用程序包括应用程序A、B、C，且当前操作系统存在用户guest、user和administrator，可设置用户启动规则为：administrator可启动应用程序A、B、C，user可启动应用程序A、B。

[0096] 步骤202，设置每一个应用程序在操作系统处于至少一种工作状态时，分别对应的权限维度。

[0097] 举例来说，可以设置安装操作系统的终端设备处于离线工作状态时，应用程序A对应的一个权限维度a1中，应用程序A具备n个方向上的访问权限，即访问n种资源(n种类型的文件对象或n个文件对象)；相反的，在安装操作系统的终端设备处于联网工作状态时，应用程序A对应的另一个权限维度a2中，应用程序A具备n+m个方向上的访问权限。

[0098] 本发明实施例中，在操作系统本身的安全程度较高时，可为其开放更多的访问权限。

[0099] 本发明实施例中，还可以设置一个文件访问规则链表，该文件访问规则链表用于记录应用程序A、B和C在操作系统处于离线防止状态和联网工作状态时分别对应的权限维度，每一个权限维度下存储一个应用程序与至少一个文件对象之间的对应关系。

[0100] 步骤203，截获对应至少一个第二应用程序的运行指令。

[0101] 步骤204，获取在当前时刻已经登录操作系统的登录用户的用户信息。

[0102] 需要说明的是，在用户登录当前操作系统时，还可以识别对应的登录请求，如果预先设置的用户启动规则中，并不存在针对该登录请求对应的用户的权限限定，则拦截该登录请求；比如，数据库的管理员账号为root，入侵者使用非法手段获得了root账号的权限并试图登录以访问数据库，当预先设置的用户启动规则中并不存在root用户的相关权限设置时，则拦截该登录请求，以拒绝root账号的登录。

[0103] 步骤205，根据用户信息及用户启动规则，判断至少一个第二应用程序是否包括登录用户可以启动的至少一个第一应用程序，如果是，则执行步骤206；否则，执行步骤215。

[0104] 举例来说，当运行指令对应的第二应用程序为应用程序A，且登录当前操作系统的登录用户为administrator或user，则执行步骤206；反之，当运行指令对应的第二应用程序为C，且登录操作系统的登录用户为guest或user时，根据预先设置的用户启动规则，应用程序C为登录用户guest或user所不能启动的第一应用程序，执行步骤215。

[0105] 步骤206，释放截获的运行指令。

[0106] 本发明实施例中，在释放截获的运行指令后，可使操作系统响应该运行指令，以在当前操作系统中运行该运行指令对应的第一应用程序。

[0107] 步骤207，在操作系统运行至少一个第一应用程序之后，截获每一个第一应用程序发起的文件访问请求。

[0108] 步骤208，解析截获的文件访问请求以确定该文件访问请求对应的目标应用程序和目标文件对象。

[0109] 步骤209，获取当前操作系统的运行参数。

[0110] 步骤210，根据获取的运行参数确定操作系统的目标工作状态。

[0111] 本发明实施例中，运行参数可以包括安装当前操作系统的终端设备中，用于连接其对应的服务器的网络端口的工作参数，通过该参数可以判断出安装当前操作系统的终端设备是否处于联网状态。

[0112] 当然，步骤209中还可以获取当前操作系统的其他运行参数以确定当前操作系统的目标工作状态，比如，获取相应运行参数以确定当前操作系统是否处于锁定状态等。

[0113] 步骤211，确定目标应用程序在操作系统处于目标工作状态时对应的目标权限维度。

[0114] 举例来说，当步骤208中确定的目标应用程序为A时，且在步骤210中确定出安装当前操作系统的终端设备处于离线状态时，则可通过查询步骤202中构建的文件访问规则链表确定出目标权限维度为a1。

[0115] 步骤212，判断目标权限维度下是否存在目标应用程序与目标文件对象之间的对应关系，如果是，则执行步骤216；否则，执行步骤213。

[0116] 这里，即通过查询文件访问规则链表以判断目标权限维度a1中，是否存在目标应用程序A与步骤208中确定的目标文件对象之间的对应关系。

[0117] 步骤213，拦截该文件访问请求。

[0118] 步骤214，记录在设定时间长度的一个检测周期内拦截的对应目标应用程序的文件访问请求的拦截数量，当拦截数量大于预先设定的标准参数时，产生告警信息，并将告警信息发送至外部告警系统，以使外部告警系统进行告警。

[0119] 步骤215，拦截该运行指令。

[0120] 步骤216，释放该文件访问请求。

[0121] 如图3所示，本发明实施例提供了一种应用程序管理装置，包括：

[0122] 设置模块301，用于预先设置至少一个第一应用程序的文件访问规则；

[0123] 文件层过滤模块302，用于在操作系统运行所述至少一个第一应用程序之后，截获所述至少一个第一应用程序发起的文件访问请求；

[0124] 解析模块303，用于解析所述文件访问请求以确定所述文件访问请求对应的目标应用程序和目标文件对象；

[0125] 第一处理模块304，用于根据所述文件访问规则判断所述目标应用程序是否可以访问所述目标文件对象，如果是，则释放所述文件访问请求，以使所述操作系统响应所述文件访问请求；否则，拦截所述文件访问请求。

[0126] 进一步的，为了方便用户及时针对已经被入侵者控制的应用程序进行及时处理，

如图4所示，本发明一个优选实施例中，还包括：告警处理模块401，用于记录在设定时间长度的一个检测周期内拦截的对应所述目标应用程序的文件访问请求的拦截数量，当所述拦截数量大于预先设定的标准参数时，产生告警信息，并将所述告警信息发送至外部告警系统，以使外部告警系统进行告警。

[0127] 进一步的，为了提高用户体验，本发明一个优选实施例中，所述设置模块301，用于预先设置文件访问规则链表，其中，所述文件访问规则链表用于存储所述至少一个第一应用程序与至少一个文件对象之间的对应关系；

[0128] 所述第一处理模块304，用于查询所述文件访问规则链表，判断所述文件访问规则链表中是否存在所述目标应用程序与所述目标文件对象之间的对应关系。

[0129] 进一步的，为了实现控制同一个应用程序在当前操作系统处于不同安全程度的工作状态时，该应用程序可以具备不同的文件访问权限，如图5所示，本发明一个优选实施例中，所述设置模块301，用于预先设置至少一个第一应用程序分别对应的至少两个权限维度；其中，每一个所述权限维度分别与所述操作系统的至少一种工作状态相对应；

[0130] 所述第一处理模块304，包括：

[0131] 获取子单元3041，用于获取所述操作系统的运行参数；

[0132] 第一确定子单元3042，用于根据所述运行参数确定所述操作系统的至少一种目标工作状态；

[0133] 第二确定子单元3043，用于确定所述目标应用程序在所述操作系统处于所述至少一种目标工作状态时对应的目标权限维度；

[0134] 处理子单元3044，用于根据所述目标权限维度判断所述目标应用程序是否可以访问所述目标访问对象。

[0135] 进一步的，为了进一步提高操作系统的安全性，防止入侵者通过截获的用户账号入侵操作系统中的应用程序，如图6所示，本发明一个优选实施例中，所述设置模块301，进一步用于预先设置至少一个第二应用程序的用户启动规则；

[0136] 还包括：应用层过滤模块601、获取模块602和第二处理模块603；其中，

[0137] 所述应用层过滤模块601，用于截获对应所述至少一个第二应用程序的运行指令；

[0138] 所述获取模块602，用于获取在当前时刻已经登录所述操作系统的登录用户的用户信息；

[0139] 所述第二处理模块603，用于根据所述用户信息及所述用户启动规则，确定所述至少一个第二应用程序是否包括所述登录用户可以启动的至少一个第一应用程序，如果是，则释放所述运行指令，以使所述操作系统运行所述至少一个第一应用程序；否则，拦截所述运行指令。

[0140] 上述装置内的各模块之间的信息交互、执行过程等内容，由于与本发明方法实施例基于同一构思，具体内容可参见本发明方法实施例中的叙述，此处不再赘述。

[0141] 本发明各个实施例至少具有如下有益效果：

[0142] 1、通过预先设置至少一个第一应用程序的文件访问规则，在操作系统运行第一应用程序后，截获每一个第一应用程序发起的文件访问请求，解析截获的文件访问请求以确定当前文件访问请求对应的目标应用程序和目标文件对象(比如操作系统的系统文件、日志文件等)，即确定发起该文件访问请求的目标应用程序以及该目标应用程序执行本次数

据访问任务时需要访问的目标文件对象，进而根据预先设定的文件访问规则判断目标应用程序是否可以访问目标文件对象，只有预先设定的文件访问规则中允许目标应用程序访问目标文件对象时，才释放截获的文件访问请求，使得操作系统响应该文件访问请求(比如在目标文件对象内读写业务数据)，否则，拦截该文件访问请求，使得操作系统不会响应该文件访问请求；综上可见，本发明实施例提供的技术方案中，通过限定应用程序可访问的文件对象的范围，使得入侵者不能访问不在当前应用程序可访问的文件对象范围内的其他文件对象，避免应用程序在被入侵者控制后，通过该应用程序继续入侵操作系统，可提高操作系统的安全性。

[0143] 2、本发明一实施例中，通过设置文件访问规则链表，工作人员仅需要向文件访问规则链表填充应用程序与文件对象之间的对应关系，在截获到文件访问请求后，在不改变操作系统原本的权限配置信息的前提下，即可根据该文件访问规则链表来实现控制释放或拦截已经截获的文件访问请求；同时，文件访问规则链表中仅存储应用程序与文件对象之间的对应关系，无需向文件访问规则链表中写入每一个文件对象的详细路径，用户体验较好。

[0144] 3、本发明一个优选实施例中，记录在设定时间长度的一个检测周期内拦截的对应目标应用程序的文件访问请求的拦截数量，当拦截数量大于预先设定的标准参数时，表征目标应用程序可能存在漏洞，且已经被入侵者控制，相应的，产生告警信息，并将告警信息发送至外部告警系统，以使外部告警系统进行告警；可提醒工作人员及时针对该目标应用程序进行相应的处理。

[0145] 4、本发明一实施例中，针对同一个应用程序，可根据操作系统所处工作状态的安全程度合理设置当前应用程序对应的多个权限维度，在操作系统处于不同的工作状态时，通过不同的权限维度限定当前应用程序的文件对象访问范围。

[0146] 5、本发明一实施例中，通过设置应用程序对应的用户启动规则，使得相应的应用程序只能被登录操作系统的指定用户启动，防止入侵者通过截获的用户账号登录操作系统，越权启动相应的应用程序以威胁操作系统安全。

[0147] 需要说明的是，在本文中，诸如第一和第二之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个〃·····”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同因素。

[0148] 本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储在计算机可读取的存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质中。

[0149] 最后需要说明的是：以上所述仅为本发明的较佳实施例，仅用于说明本发明的技术方案，并非用于限定本发明的保护范围。凡在本发明的精神和原则之内所做的任何修改、等同替换、改进等，均包含在本发明的保护范围内。

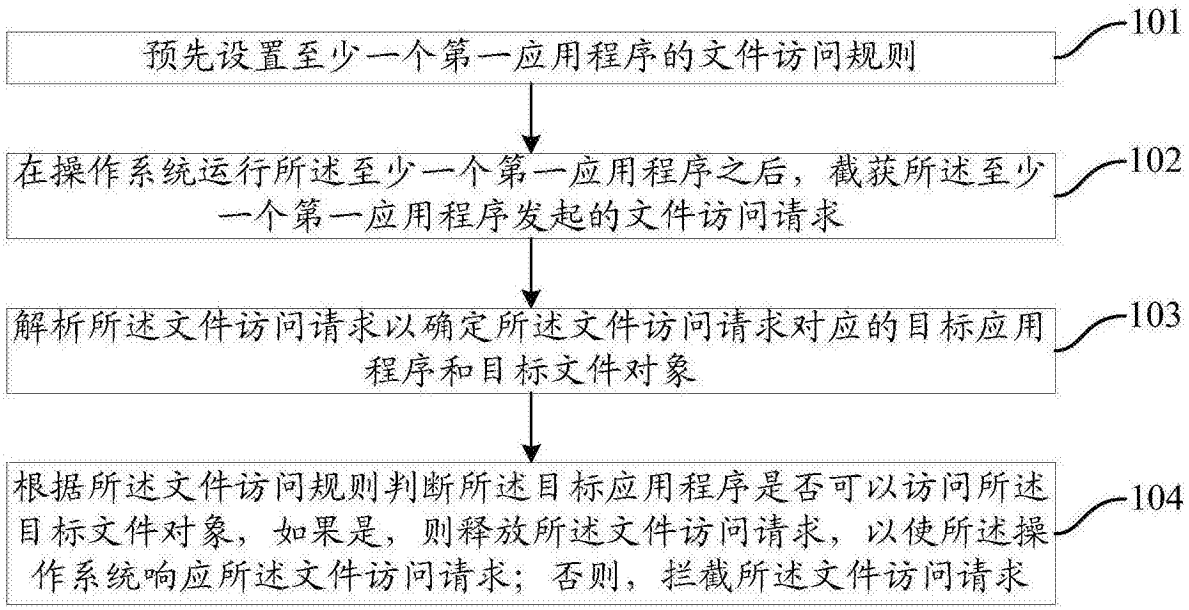

预先设置至少一个第一应用程序的文件访问规则
101
在操作系统运行所述至少一个第一应用程序之后，截获所述至少一个第一应用程序发起的文件访问请求
102
解析所述文件访问请求以确定所述文件访问请求对应的目标应用程序和目标文件对象
103
根据所述文件访问规则判断所述目标应用程序是否可以访问所述目标文件对象，如果是，则释放所述文件访问请求，以使所述操作系统响应所述文件访问请求；否则，拦截所述文件访问请求
104

图1

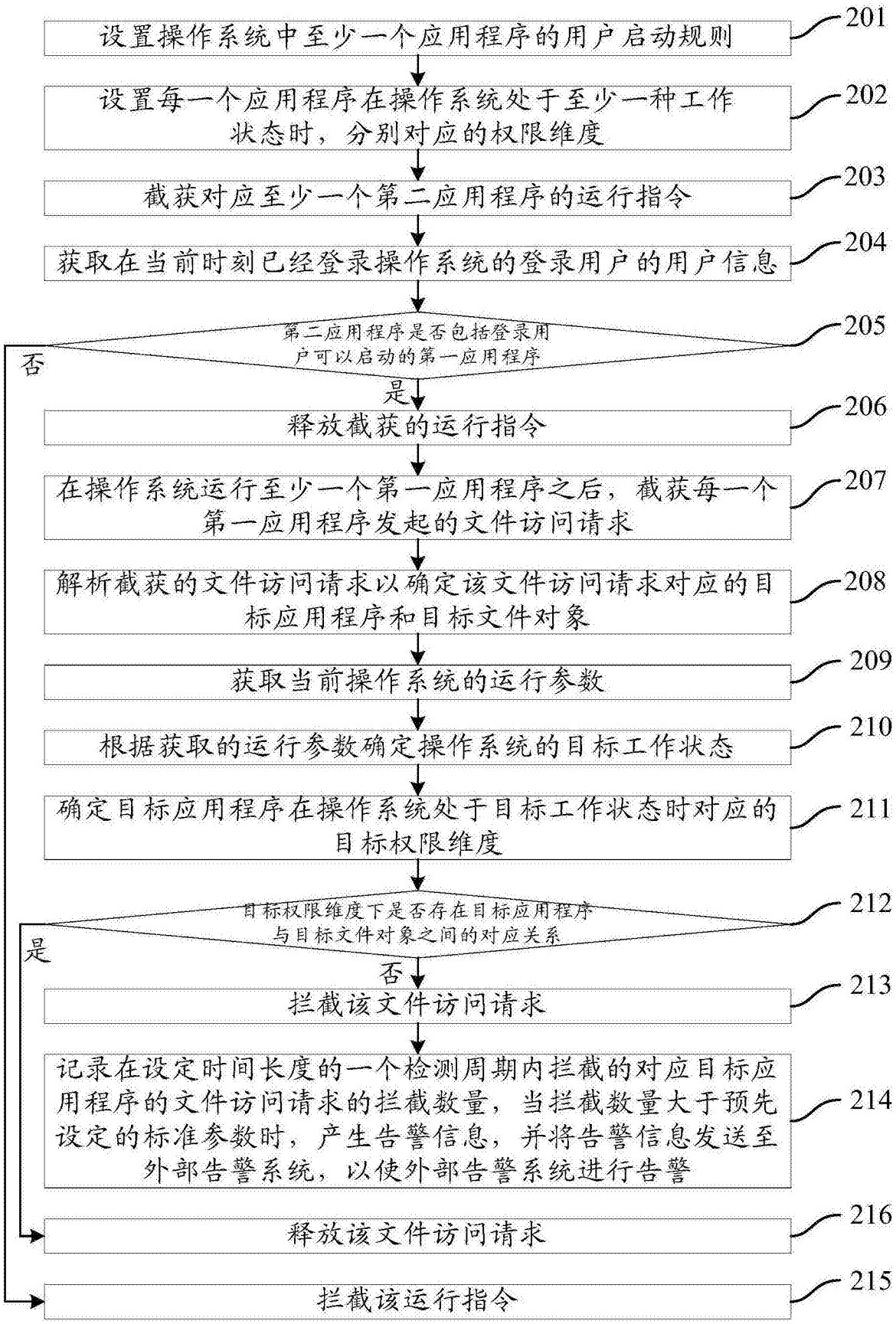

设置操作系统中至少一个应用程序的用户启动规则
201
设置每一个应用程序在操作系统处于至少一种工作状态时，分别对应的权限维度
202
截获对应至少一个第二应用程序的运行指令
203
获取在当前时刻已经登录操作系统的登录用户的用户信息
204
第二应用程序是否包括登录用户可以启动的第一应用程序
205
否
是
释放截获的运行指令
206
在操作系统运行至少一个第一应用程序之后，截获每一个第一应用程序发起的文件访问请求
207
解析截获的文件访问请求以确定该文件访问请求对应的目标应用程序和目标文件对象
208
获取当前操作系统的运行参数
209
根据获取的运行参数确定操作系统的目标工作状态
210
确定目标应用程序在操作系统处于目标工作状态时对应的目标权限维度
211
目标权限维度下是否存在目标应用程序与目标文件对象之间的对应关系
212
是
否
拦截该文件访问请求
213
记录在设定时间长度的一个检测周期内拦截的对应目标应用程序的文件访问请求的拦截数量，当拦截数量大于预先设定的标准参数时，产生告警信息，并将告警信息发送至外部告警系统，以使外部告警系统进行告警
214
释放该文件访问请求
216
拦截该运行指令
215

图2

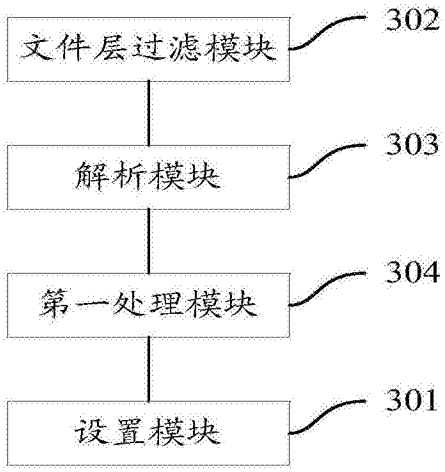

文件层过滤模块
302
解析模块
303
第一处理模块
304
设置模块
301

图3

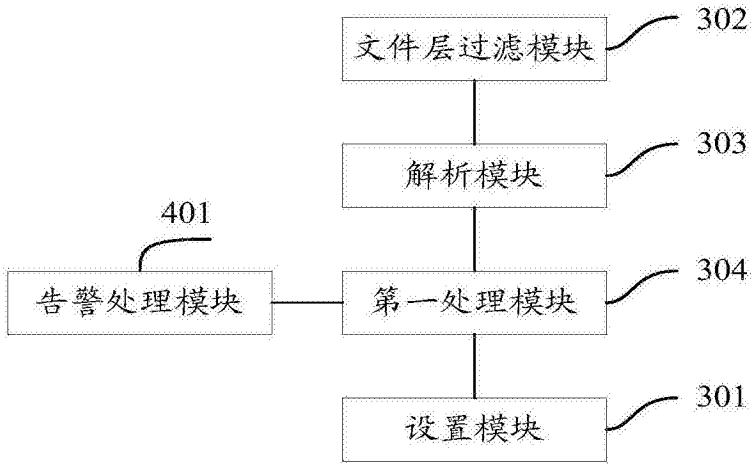

文件层过滤模块
302
解析模块
303
401
告警处理模块
第一处理模块
304
设置模块
301

图4

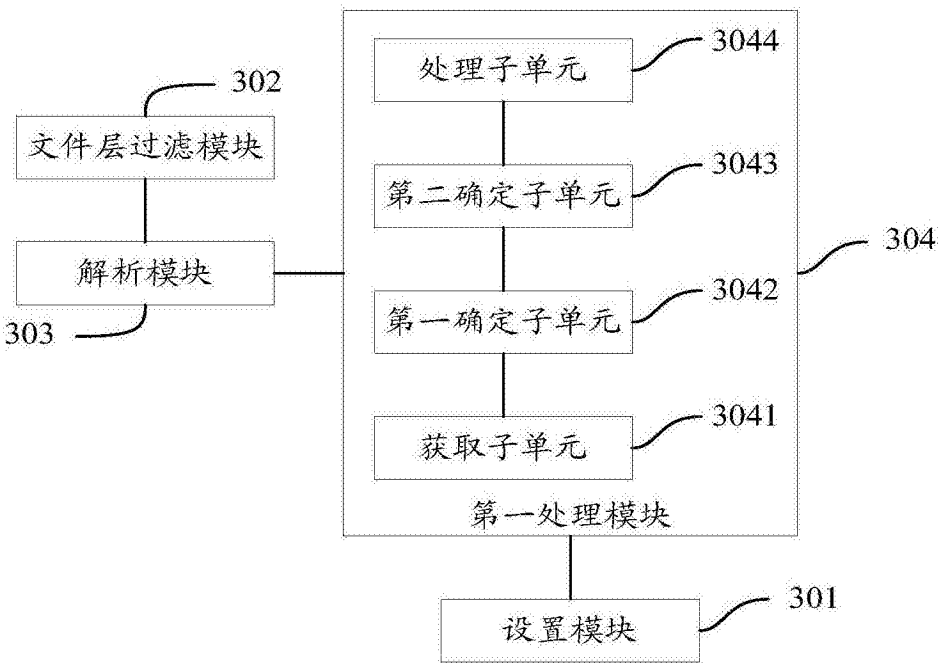

处理子单元
3044
302
第二确定子单元
3043
文件层过滤模块
304
解析模块
第一确定子单元
3042
303
获取子单元
3041
第一处理模块
设置模块
301

图5

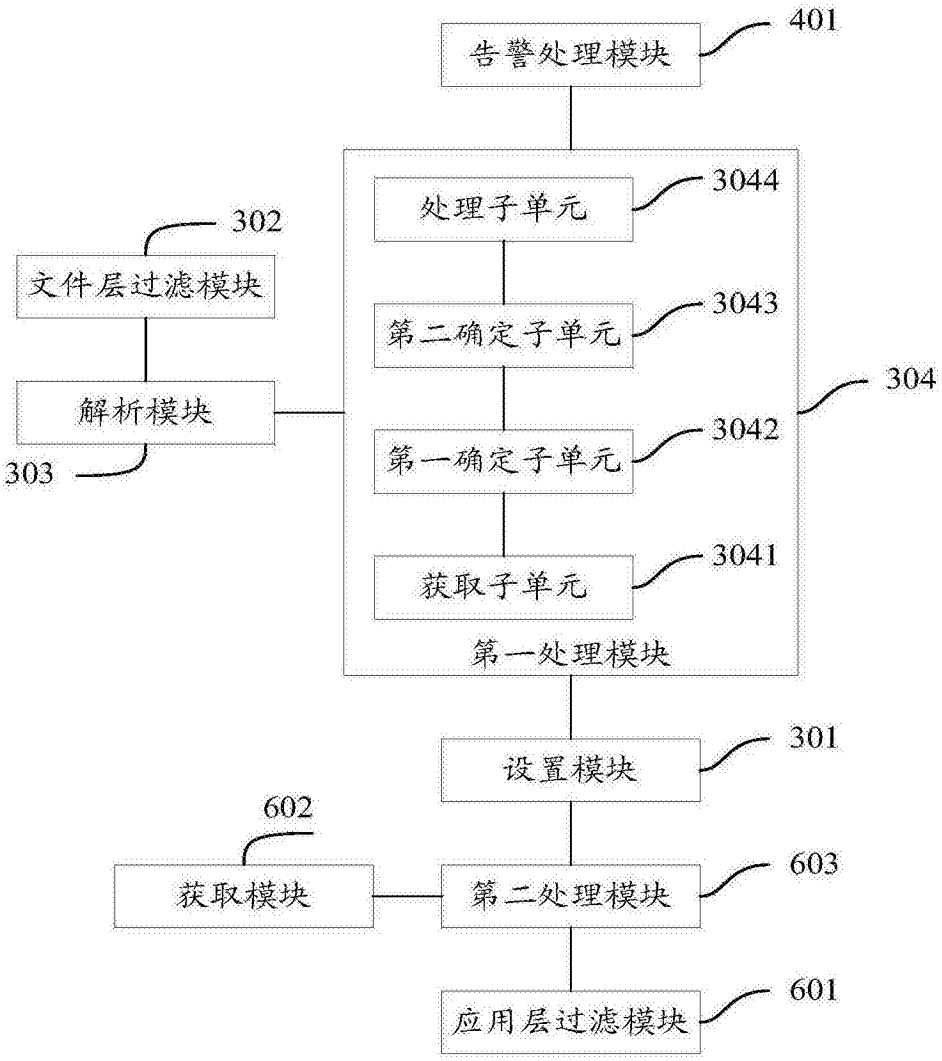

告警处理模块
401
处理子单元
3044
第二确定子单元
3043
第一确定子单元
3042
获取子单元
3041
第一处理模块
304
文件层过滤模块
302
解析模块
303
设置模块
301
获取模块
602
第二处理模块
603
应用层过滤模块
601

图6