(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
2016 年 6 月 23 日 (23.06.2016)

WIPO | PCT

(10) 国际公布号
WO 2016/095673 A1

(51) 国际专利分类号:
G06F 21/52 (2013.01)

(21) 国际申请号: PCT/CN2015/095454

(22) 国际申请日: 2015 年 11 月 24 日 (24.11.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
2014107847269 2014 年 12 月 16 日 (16.12.2014) CN

(71) 申请人: **北京奇虎科技有限公司 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED)** [CN/CN]; 中国北京市西城区新街口外大街 28 号 D 座 112 室（德胜园区）, Beijing 100088 (CN)。 **奇智软件（北京）有限公司 (QIZHI SOFTWARE (BEIJING) COMPANY LIMITED)** [CN/CN]; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼 B 座 2 层、3 层 301-306 室, Beijing 100015 (CN)。

(72) 发明人: **张皓秋 (ZHANG, Haoqiu)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。

(74) 代理人: **北京润泽恒知识产权代理有限公司 (BEIJING RISEHIGH INTELLECTUAL PROPERTY LAW FIRM)**; 中国北京市海淀区中关村南大街 31 号神舟大厦 702, Beijing 100081 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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。

(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))。

(54) **Title**: APPLICATION-BASED BEHAVIOR PROCESSING METHOD AND DEVICE

(54) **发明名称**: 一种基于应用程序的行为处理方法和装置

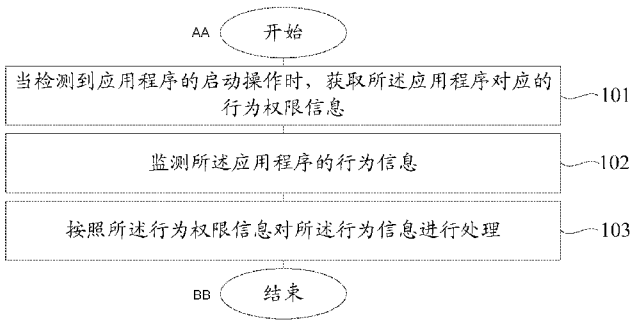

图 1 / FIG. 1

101 WHEN AN OPERATION OF STARTING UP AN APPLICATION IS DETECTED, ACQUIRE BEHAVIOR PERMISSION INFORMATION CORRESPONDING TO THE APPLICATION
102 MONITOR BEHAVIOR INFORMATION OF THE APPLICATION
103 PROCESS THE BEHAVIOR INFORMATION ACCORDING TO THE BEHAVIOR PERMISSION INFORMATION
AA START
BB END

(57) **Abstract**: Disclosed are an application-based behavior processing method and device. The method comprises: acquiring, when an operation of starting up an application is detected, behavior permission information corresponding to the application; monitoring behavior information of the application; and processing the behavior information according to the behavior permission information. According to the embodiments of the present invention, behavior permission information is configured for behaviors, and applications are monitored by taking a single behavior as a permission unit, which avoids monitoring vulnerabilities caused by configuration of uniform permissions for applications based on black and white name lists, and achieve fine-granularity permission control, thereby improving the protection strength, reducing potential threats and lowering the possibility of false positives.

(57) **摘要**: 本发明公开了一种基于应用程序的行为处理方法和装置，所述方法包括：当检测到应用程序的启动操作时，获取所述应用程序对应的行为权限信息；监测所述应用程序的行为信息；以及按照所述行为权限信息对所述行为信息进行处理。本发明实施例通过为行为配置行为权限信息，以单个行为作为权限单位，对应用程序进行监控，避免了黑白名单对应用程序配置统一权限带来的监控漏洞，实现了细粒度权限控制，增强了保护的强度，降低潜在威胁，亦可以减少误报率。

WO 2016/095673 A1

一种基于应用程序的行为处理方法和装置

技术领域

本发明涉及应用程序技术领域，尤其涉及一种基于应用程序的行为处理方法和一种基于应用程序的行为处理装置。

背景技术

随着互联网技术的不断发展，人们开发了各种功能丰富的应用程序，例如，即时通讯工具、音频播放器、视频播放器、日历工具等等，给人们的生活带来许多便利。

由于种种原因，应用程序总是会存在着某些漏洞，利用这些漏洞，病毒、木马或恶意代码可以操纵这些应用程序进行非法滥用，又或者，应用程序本身出于某些非法目的，进行某些危险的行为。

进而，这些应用程序的行为可能会危及数据的完整性、保密性、可用性和可控性，最终表现为应用程序在运行的过程中偏离了正常的轨道，即产生异常行为。

为了保护数据的安全，用户一般在操作系统中安装安全工具，例如，防火墙、杀毒工具等等，这些安全工具，一般会设置有黑名单和白名单，采用 “非白即黑”的核心理念保护操作系统。

具体而言，对于白名单中信任的应用程序，一律允许其执行操作；对于黑名单中不信任的应用程序，就会对其行为进行审核，若出现敏感行为，就会以弹窗形式提示用户。

对于黑白名单机制，添加进白名单的应用程序，该应用程序的所有行为就全部信任，容易出现漏洞。若不添加进白名单，则可能会有很多行为被误报病毒，误操作多，浪费系统资源。

例如，某应用程序为文字编辑程序，主要用于编辑，保存和打印文档，它的正常行为表现为读写它所支持的文档格式的文档，操作打印机进行打印，如果发现该应用程序通过网络下载了一个可执行程序并通过修改注册表把它设置为开机自动运行，这显然是一个异常行为，这个异常行为有可能是由于受到了宏病毒或者木马程序的攻击所造成的，又或者，出于强行推广应用程序的目的，该应用程序本身具有这个异常行为。

若将该文字编辑程序添加进白名单，则上述异常行为也是允许的，会

导致安全漏洞。若不添加到白名单，则日常的文档读写、打印机打印等行为又容易被误报病毒。

发明内容

鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决或减缓上述问题的一种基于应用程序的行为处理方法和相应的一种基于应用程序的行为处理装置。

根据本发明的一个方面，提供了一种基于应用程序的行为处理方法，包括步骤:

当检测到应用程序的启动操作时，获取所述应用程序对应的行为权限信息;

监测所述应用程序的行为信息；以及

按照所述行为权限信息对所述行为信息进行处理。

根据本发明的另一方面，提供了一种基于应用程序的行为处理装置，包括:

权限信息获取模块，适于在检测到应用程序的启动操作时，获取所述应用程序对应的行为权限信息;

行为信息监测模块，适于监测所述应用程序的行为信息；以及

处理模块，适于按照所述行为权限信息对所述行为信息进行处理。

根据本发明的又一个方面，提供了一种计算机程序，其包括计算机可读代码，当所述计算机可读代码在计算设备上运行时，导致所述计算设备执行如上文所述的基于应用程序的行为处理方法。

根据本发明的再一个方面，提供了一种计算机可读介质，其中存储了上述的计算机程序。

本发明的有益效果为:

本发明实施例在检测到应用程序的启动操作时，获取该应用程序对应的行为权限信息，对监测到的应用程序的行为信息，按照该行为权限信息进行处理，通过为行为配置行为权限信息，以单个行为作为权限单位，对

应用程序进行监控，避免了黑白名单对应用程序配置统一权限带来的监控漏洞，实现了细粒度权限控制，增强了保护的强度，降低潜在威胁，亦可以减少误报率。

本发明实施例在服务器更新和维护应用程序的行为权限信息，无需在本地配置不同应用程序的行为权限信息，减少了本地系统的资源占用，服务器可以快速对应用程序的行为变化做出反应对行为权限信息进行修改，保证了行为权限信息的准确性。

本发明实施例在本地配置行为权限基础信息，由服务器发送的行为权限配置信息进行配置，以获得应用程序的行为权限信息，一方面，由于从服务器获取权限组标识可以获得本地的权限基础信息，无需重复从服务器获取部分的行为权限信息，大大减少了数据的传输量，减少带宽的占用，加快数据的传输速度；另一方面，服务器可以及时对应用程序的行为变化做出反馈，修改行为权限配置信息，保证了应用程序的行为权限信息的准确性。

本发明实施例通过白名单行为信息和黑名单行为信息对应用程序的行为进行可信和不可信操作，进一步细化权限的层次，提高了行为监控的准确性。

本发明实施例通过将未标记的行为进行提示，或，由服务器进行分析，进一步提高了行为监控的准确性和全面性。

上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

图 1 示意性地示出了根据本发明一个实施例的一种基于应用程序的行为处理方法实施例的步骤流程示意图；

图 2 示意性地示出了根据本发明一个实施例的一种基于应用程序的行为

处理装置实施例的方块示意图;

图 3 示意性地示出了用于执行根据本发明的方法的计算设备的框图;以及

图 4 示意性地示出了用于保持或者携带实现根据本发明的方法的程序代码的存储单元。

具体实施例

下面结合附图和具体的实施方式对本发明作进一步的描述。

参照图 1，示出了根据本发明一个实施例的一种基于应用程序的行为处理方法实施例的步骤流程图，具体可以包括如下步骤:

步骤 101，当检测到应用程序的启动操作时，获取所述应用程序对应的行为权限信息;

本发明实施例中，当前启动的应用程序可以是由用户的操作进行触发的，例如，用户通过鼠标双击快捷方式触发应用程序的启动；也可以由其他应用程序或服务所触发，例如，当下载工具下载文件完成时，可以调用安全工具对该文件进行安全扫描；还可以通过其他方式触发启动，本发明实施例对此不加以限制。

在具体实现中，可以通过回调操作系统中指定的系统函数，如PsSetCreateProcessNotifyRoutine等，让操作系统通知该系统函数，以获知应用程序的进程启动、退出等信息。

当然，本发明实施例中还可以挂钩（Hook）CreateProcess 等系统函数获取到应用程序的进程启动的时机和信息，本发明实施例对此不加以限制。

客户端在检测应用程序启动时，可以获取该应用程序对应的行为权限信息，以对该应用程序的行为进行控制。其中，该行为权限信息可以用于记录对应的应用程序的行为的权限。

在本发明的一种可选实施例中，步骤 101 可以包括如下子步骤:

子步骤 S11，提取所述应用程序的第一特征信息;

客户端在检测应用程序启动时，可以提取其第一特征信息。

第一特征信息，可以为表征当前启动的应用程序的特征的信息，具体可以包括 ID（Identity，身份标识号码）、数字签名、hash（哈希值）等等。

子步骤 S12，将所述第一特征信息发送至服务器;

应用本发明实施例，可以预先提取待检测的应用程序的第二特征信

息，该第二特征信息可以为表征待检测的应用程序的特征的信息，具体可以包括ID（Identity，身份标识号码）、数字签名、hash（哈希值）等等。

此外，可以预先/实时对该待检测的应用程序的行为进行分析，根据分析结果，对该应用程序的第二特征信息配置行为权限信息。在该行为权限信息中可以记录该第二特征信息对应的应用程序的行为所拥有的权限。该权限行为信息可以用于对该应用程序的行为进行监控。

具体而言，行为权限信息可以包括白名单行为信息和黑名单行为信息中的至少一个。当然，对于某些应用程序，其行为权限信息可以只包括白名单行为信息，或者，可以只包括黑名单行为信息，本发明实施例对此不加以限制。

若分析出该待检测的应用程序的行为可信时，将该行为的行为信息作为特征行为信息，添加到其第二特征信息对应的白名单行为信息中，即白名单行为信息可以为某个应用程序的可信的行为的集合。

若分析出该待检测的应用程序的行为不可信时，将该行为的行为信息作为特征行为信息，添加到其第二特征信息对应的黑名单行为信息中，即黑名单行为信息可以为某个应用程序的不可信的行为的集合。

在实际应用中，该待检测的应用程序可以包括用户上传的、出现报警行为的应用程序。将该待检测的应用程序置于虚拟机中运行，复现出现报警的行为，若没有发现异常行为时，则可以将当时表现出来的会被报警的行为添加到该应用程序的第二特性信息对应的白名单行为信息中。

当然，本领域技术人员也可以主动收集不同的应用程序进行分析，本发明实施例对此不加以限制。

子步骤S13，接收所述服务器在判断所述第一特征信息与预置的第二特征信息匹配时，返回的所述第二特征信息对应的行为权限列表。

本发明实施例中，客户端可以将第一特征信息发送至服务器，由服务器检测第一特征信息与预置的第二特征信息是否匹配。

当第一特征信息与第二特征信息匹配时，可以表示在先已经对当前启动的应用程序进行了分析，存储有行为权限信息。

服务器将该第二特征信息对应的行为权限信息发送至客户端，由客户端对当前启动的应用程序的行为进行监控。

本发明实施例在服务器更新和维护应用程序的行为权限信息，无需在

本地配置不同应用程序的行为权限信息，减少了本地系统的资源占用，服务器可以快速对应用程序的行为变化做出反应对行为权限信息进行修改，保证了行为权限信息的准确性。

在本发明的另一种可选实施例中，步骤 101 可以包括如下子步骤:

子步骤 S21，提取所述应用程序的第一特征信息;

子步骤 S22，将所述第一特征信息发送至服务器;

子步骤 S23，接收所述服务器在判断所述第一特征信息与预置的第二特征信息匹配时，返回的所述第二特征信息对应的行为权限配置信息和权限组标识;

子步骤 S24，查找在本地预置的，所述权限组标识对应的行为权限基础信息；以及

子步骤 S25，利用所述行为权限配置信息对所述行为权限基础信息进行配置，以获得行为权限信息。

在本发明实施例中，可以对应用程序划分一个或多个权限组，每个权限组具有唯一的权限组标识进行识别。

在每个权限组中的应用程序，可能具有相同或相似的行为，但是每个应用程序的行为一般又具有差异性。

例如，下载工具A和下载工具B，都会主动修改开机启动项，也会在后台上传数据，但是下载工具 A 通过 80 端口上传，下载工具 B 通过 21 端口上传，此外，下载工具 B 还会调用安全工具对下载的文件进行安全扫描。因此，下载工具 A 和下载工具 B 可以归属于同一个权限组。

因此，一方面，可以针对每个权限组配置行为权限基础信息，在该行为权限基础信息中可以记录该权限组中的应用程序的相同或相似的行为所拥有的权限。

具体而言，所述行为权限基础信息可以包括白名单行为基础信息和黑名单行为基础信息中的至少一种。

其中，白名单行为基础信息可以为该权限组中应用程序的不可信的、相同或相似的行为的集合；黑名单行为基础信息可以为该权限组中应用程序的不可信的行为的、相同或相似的行为的集合。

例如，对于下载工具 A 和下载工具 B，由于上传数据一般是用于 P2P（Peer-to-Peer，对等网络）数据传输，因此，上传数据都是可信的；主动修

改开机启动项不是用户主动请求的，且会占用系统资源降低开机速度，因此，主动修改开机启动项都是不可信的。对于下载工具 A 和下载工具 B 所属的权限组，上传数据可以写入白名单行为基础信息，主动修改开机启动项可以写入黑名单行为基础信息。

需要说明的是，本领域技术人员可以根据实际情况对白名单行为基础信息和黑名单行为基础信息进行设置，例如，对于下载工具 B 的调用安全工具的行为，是可信的，若该权限组的其他应用程序大多数具有该行为，则可以写入白名单行为基础信息，若该权限组的其他应用程序大多数不具有该行为，则可以不写入白名单行为基础信息，本发明实施例对此不加以限制。

另一方面，可以针对特定的应用程序配置行为权限配置信息，在该行为权限配置信息中可以记录如何对该特定的应用程序所属的权限组的行为权限基础信息进行配置，以获得该特定应用程序的行为权限信息。

具体而言，所述行为权限配置信息包括白名单行为添加信息、白名单行为删除信息、白名单行为修改信息、黑名单行为添加信息、黑名单行为删除信息、黑名单行为修改信息中的至少一种。

其中，白名单行为添加信息可以指示在白名单行为基础信息中添加指定的特征行为信息;

白名单行为删除信息可以指示在白名单行为基础信息中删除指定的特征行为信息;

白名单行为修改信息可以指示在白名单行为基础信息中修改指定的特征行为信息;

黑名单行为添加信息可以指示在黑名单行为基础信息中添加指定的特征行为信息;

黑名单行为删除信息可以指示在黑名单行为基础信息中删除指定的特征行为信息;

黑名单行为修改信息可以指示在黑名单行为基础信息中修改指定的特征行为信息。

例如，若下载工具 A 和下载工具 B 所属的权限组的行为权限基础信息如下:

白名单行为基础信息：上传数据（*端口）；

黑名单行为基础信息：主动修改开机启动项；

其中，*为通配符，上传数据（*端口）可以表示允许用任意端口上传数据。

则对于下载工具 A，可以在该行为权限基础信息上，需要配置一白名单行为修改信息，以将“上传数据（*端口）”修改为“上传数据（80 端口）”，即信任使用 80 端口上传数据；对于下载工具 B，可以在该行为权限基础信息上，需要配置一白名单行为修改信息，以将“上传数据（*端口）”修改为上传“数据（21 端口）”，即信任使用 21 端口上传数据，同时配置一白名单行为添加信息，在白名单行为基础信息添加调用“调用安全工具”，以信任调用安全工具对下载的文件进行安全扫描的行为。

本发明实施例在本地配置行为权限基础信息，由服务器发送的行为权限配置信息进行配置，以获得应用程序的行为权限信息，一方面，由于从服务器获取权限组标识可以获得本地的权限基础信息，无需重复从服务器获取部分的行为权限信息，大大减少了数据的传输量，减少带宽的占用，加快数据的传输速度；另一方面，服务器可以及时对应用程序的行为变化做出反馈，修改行为权限配置信息，保证了应用程序的行为权限信息的准确性。

在本发明实施例的一种可选示例中，子步骤 S25 可以包括如下子步骤：

子步骤 S251，在所述白名单行为基础信息中添加所述白名单行为添加信息对应的特征行为信息。

在本发明实施例中，若接收到白名单行为添加信息，则可以在白名单行为基础信息添加指定的行为信息（即特征行为信息）。

例如，若白名单行为添加信息为“w+修改启动项”，“w”可以指示白名单行为基础信息，“+”可以指示添加操作，“修改启动项”可以为特征行为信息，则在白名单行为基础信息中添加修改启动项的行为。

在本发明实施例的一种可选示例中，子步骤 S25 可以包括如下子步骤：

子步骤 S252，在所述白名单行为基础信息中删除所述白名单行为删除信息对应的特征行为信息。

在本发明实施例中，若接收到白名单行为删除信息，则可以在白名单

行为基础信息删除指定的行为信息（即特征行为信息）。

例如，若白名单行为添加信息为“w-修改com接口”，“w”可以指示白名单行为基础信息，“-”可以指示删除操作，“修改 com 接口”可以为特征行为信息，则在白名单行为基础信息中删除修改com接口的行为。

在本发明实施例的一种可选示例中，子步骤 S25 可以包括如下子步骤：

子步骤 S253，按照所述白名单行为修改信息对所述白名单行为基础信息中的特征行为信息进行修改。

在本发明实施例中，若接收到白名单行为修改信息，则可以对白名单行为基础信息中指定的行为信息（即特征行为信息）进行修改。

例如，若白名单行为基础信息包括访问网络(url:*)，白名单行为修改信息为“w|访问网络(url: hao.360.cn)”，“w”可以指示白名单行为基础信息，“|”可以指示修改操作，“访问网络(url: hao.360.cn)”可以为修改的信息，则在白名单行为基础信息中将访问网络(url:*)的行为修改为访问网络(url: hao.360.cn)。

在本发明实施例的一种可选示例中，子步骤 S25 可以包括如下子步骤：

子步骤 S254，在所述黑名单行为基础信息中添加所述黑名单行为添加信息对应的特征行为信息。

在本发明实施例中，若接收到黑名单行为添加信息，则可以在黑名单行为基础信息添加指定的行为信息（即特征行为信息）。

例如，若白名单行为添加信息为“b+添加驱动程序”，“b”可以指示黑名单行为基础信息，“+”可以指示添加操作，“添加驱动程序”可以为特征行为信息，则在黑名单行为基础信息中添加添加驱动程序的行为。

在本发明实施例的一种可选示例中，子步骤 S25 可以包括如下子步骤：

子步骤 S255，在所述黑名单行为基础信息中删除所述黑名单行为删除信息对应的特征行为信息。

在本发明实施例中，若接收到黑名单行为删除信息，则可以在黑名单行为基础信息删除指定的行为信息（即特征行为信息）。

例如，若白名单行为添加信息为“b-发送邮件”，“b”可以指示黑名

单行为基础信息，“-”可以指示删除操作，“发送邮件”可以为特征行为信息，则在黑名单行为基础信息中删除发送邮件的行为。

在本发明实施例的一种可选示例中，子步骤 S25 可以包括如下子步骤:

子步骤 S256，按照所述黑名单行为修改信息对所述黑名单行为基础信息中的特征行为信息进行修改。

在本发明实施例中，若接收到黑名单行为修改信息，则可以对黑名单行为基础信息中指定的行为信息（即特征行为信息）进行修改。

例如，若黑名单行为基础信息包括删除应用程序(Id:*)，白名单行为添加信息为“b|删除应用程序(Id:安全工具)”，“b”可以指示黑名单行为基础信息，“|”可以指示修操作，“删除应用程序”可以为特征行为信息，则在黑名单行为基础信息中将删除应用程序(Id:*)的行为修改为删除应用程序(Id:安全工具)。

当然，上述行为权限配置信息只是作为示例，在实施本发明实施例时，可以根据实际情况设置其他行为权限配置信息，本发明实施例对此不加以限制。另外，除了上述行为权限配置信息外，本领域技术人员还可以根据实际需要采用其它行为权限配置信息，本发明实施例对此也不加以限制。

需要说明的是，本领域技术人员可以根据实际情况信任哪些应用程序的行为，不信任哪些应用程序的行为，本发明实施例对此不加以限制。

步骤 102，监测所述应用程序的行为信息;

在实际应用中，由于应用程序的进程一般是通过操作系统提供的 API（Application Program Interface，应用程序编程接口）函数来对注册表、文件和创建其他进程等资源来实施操作的，通过对进程调用的这些 API 进行 Hook（挂钩）则可以达到监测的目的。

为使本领域技术人员更好地理解本发明实施例，以下将 windows 操作系统作为 API Hook 和服务系统 Hook 的一种示例进行说明。

通常，Hook 可以分为用户模式 API Hook 和服务系统 Hook。

对于 API Hook:

IAT（import address table，导入地址表）是 windows 平台下的可移植的执行体（Portable Executable，PE）格式文件里的一个重要组成部分，其中存

放着本 PE 文件执行过程可能调用到的所有系统 API 的名称。当应用程序的进程运行时，它的可执行文件被调入内存，同时其 IAT 表的 PAI 名字会被映射到相应的 API 在当前进程控件中的函数体入口地址，以后该进程所发出的 API 调用通过 IAT 表转跳到相应的 API 函数体上。

因此，可以在进程载入时修改 IAT 表，将要截取的 API 的入口地址转向新的一段代码，这段代码首先将此 API 调用的函数名和参数记录下来，再转到原来的 API 真实地址继续执行。即通过修改应用程序内存映像的 IAT 中 API 函数的入口地址，就可以达到重定向 API 的目的。

例如，操作注册表、文件和创建其他进程的 API 函数如表 1 所示。

表 1

对象	操作	API 函数
注册表	创建、打开注册表	RegCreateKeyEx,RegOpenKeyEx
	读注册表	RegQueryInfoKey,RegQueryValue
	写注册表	RegSetValueEx
	删除注册表	RegDeleteKey,RegDeleteValue
文件	创建、打开文件	CreatFile
	读、写文件	ReadFile,WriteFile
	文件删除	DeleteFile
	文件重命名	SHFileOperation
进程	创建进程	CreateProcess
	打开进程	OpenProcess

对于服务系统 Hook:

Windows 工作模式分为用户模式和内核模式，用户模式的应用程 API 调用都是通过调用基于 NTDLL.dll 的本地系统服务，进入内核模式，由系统服务调度表根据所传入系统服务号在相应的系统服务表中查找所需的服务函数入口地址，最终调用内核模式中的系统服务来完成真正操作的。

因此，Hook 系统服务表中所需要监控的系统服务，修改系统服务表中需要监控的系统服务函数指针来指向自定义的系统服务函数，则可以达到对整个系统范围内的访问控制。

例如，操作注册表、文件和创建其他进程的服务函数如表 2 所示。

表 2

对象	操作	API 函数

注册表	创建、打开注册表	ZwCreateKey, ZwOpenKey
	读注册表	ZwQueryInfoKey, ZwQueryValue
	写注册表	ZwSetValueEx
	删除注册表	ZwDeleteKey, ZwDeleteValue
文件	创建、打开文件	ZwCreatFile, ZwOpenFile
	读、写文件	ZwReadFile, ZwWriteFile
	文件删除	ZwSetInformationFile
	文件重命名	ZwSetInformationFile
进程	创建进程	ZwCreateProcess, ZwCreateProcess
	打开进程	ZwOpenProcess

步骤 103，按照所述行为权限信息对所述行为信息进行处理。

在本发明实施例中，客户端接收到服务器返回的行为权限信息，则可以按照行为权限信息中对行为的权限的配置，针对应用进程的行为进行监控。

在本发明的一种可选实施例中，步骤 103 可以包括如下子步骤:

子步骤 S31，当所述行为信息与所述行为权限信息中的特征行为信息匹配时，执行所述特征行为信息对应的操作。

应用本发明实施例，可以预先为应用程序的特征行为信息配置对应的处理方式。

当检测出与特征行为信息对应的行为信息时，可以按照预先设定的安理方式进行处理。

在本发明实施例的一种可选示例中，子步骤 S31 可以包括如下子步骤:

子步骤 S311，当所述行为信息与所述白名单行为信息中的特征行为信息匹配时，允许所述行为信息的执行。

在本发明实施例中，白名单行为信息中记录可信行为的特征行为信息，其具有可执行的权限。

当检测出当前应用程序的行为与白名单行为信息中的特征行为信息匹配时，按照可执行的权限，放行该行为的执行。

在本发明实施例的一种可选示例中，子步骤 S31 可以包括如下子步

骤:

子步骤 S312，当所述行为信息与所述黑名单行为信息中的特征行为信息匹配时，生成针对所述行为信息的第一提示信息。

在本发明实施例中，黑名单行为信息中记录不可信行为的特征行为信息，其具有不可执行的权限。

当检测出当前应用程序的行为与黑名单行为信息中的特征行为信息匹配时，按照不可执行的权限，拦截该行为的执行，并生成第一提示信息，例如，生成“应用程序 C 在发送邮件，可能盗取密码，是否阻止”的文字信息，并配置红色的底色和控件“是”和“否”，以提示用户具有危险性的行为在执行。

若接收到针对该第一提示信息返回的允许执行的操作指示，例如，用户点击上述控制“否”，则可以允许该行为的执行。

若接收到针对该第一提示信息返回的禁止执行的操作指示，例如，用户点击上述控件“是”，则可以阻断该行为的执行。

本发明实施例通过白名单行为信息和黑名单行为信息对应用程序的行为进行可信和不可信操作，进一步细化权限的层次，提高了行为监控的准确性。

在本发明的一种可选实施例中，步骤 103 可以包括如下子步骤:

子步骤 S41，当所述行为信息未与所述行为权限信息中的特征行为信息匹配时，生成针对所述行为信息的第二提示信息。

在本发明实施中，若在先未在行为权限信息中记录有该应用程序的行为，如与白名单行为信息中的特征行为信息不匹配，也与黑名单行为信息中的特征行为信息不匹配，则客户端可以生成针对该行为的第二提示信息，例如，“应用程序 D 正在修改系统敏感启动项，是否阻止”，以提示用户敏感的行为在执行。

若接收到针对该第二提示信息返回的允许执行的操作指示，例如，用户点击上述控制“否”，则可以允许该行为的执行。

若接收到针对该第二提示信息返回的禁止执行的操作指示，例如，用户点击上述控件“是”，则可以阻断该行为的执行。

在本发明的一种可选实施例中，步骤 103 可以包括如下子步骤:

子步骤 S51，当所述行为信息未与所述行为权限信息中的特征行为信息

匹配时，将所述应用程序的信息和所述行为信息发送至服务器；

子步骤 S52，接收所述服务器返回的，针对所述应用程序的信息和所述行为信息的操作信息；以及

子步骤 S53，按照所述操作信息进行操作。

在本发明实施中，若在先未在行为权限信息中记录有该应用程序的行为，如与白名单行为信息中的特征行为信息不匹配，也与黑名单行为信息中的特征行为信息不匹配，则客户端将该行为的相关情况上传至服务器，由服务器进行处理并返回操作信息，客户端根据返回的操作信息进行操作。

例如，当服务器分析获得当前行为可能读取用户的账号密码，具有较高的危险性，则可以返回 block（冻结、锁定行为的示例），客户端根据该 block 阻断该行为的执行。

本发明实施例通过将未标记的行为进行提示，或，由服务器进行分析，进一步提高了行为监控的准确性和全面性。

本发明实施例在检测到应用程序的启动操作时，获取该应用程序对应的行为权限信息，对监测到的应用程序的行为信息，按照该行为权限信息进行处理，通过为行为配置行为权限信息，以单个行为作为权限单位，对应用程序进行进行监控，避免了黑白名单对应用程序配置统一权限带来的监控漏洞，实现了细粒度权限控制，增强了保护的强度，降低潜在威胁，亦可以减少误报率。

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

参照图 2，示出了根据本发明一个实施例的一种基于应用程序的行为处理装置实施例的结构框图，具体可以包括如下模块：

权限信息获取模块 201，适于在检测到应用程序的启动操作时，获取所述应用程序对应的行为权限信息；

行为信息监测模块 202，适于监测所述应用程序的行为信息；以及

处理模块 203，适于按照所述行为权限信息对所述行为信息进行处理。

在本发明的一种可选实施例中，所述权限信息获取模块 201 还可以适于:

提取所述应用程序的第一特征信息;

将所述第一特征信息发送至服务器; 以及

接收所述服务器在判断所述第一特征信息与预置的第二特征信息匹配时，返回的所述第二特征信息对应的行为权限信息。

在本发明的一种可选实施例中，所述权限信息获取模块 201 还可以适于:

提取所述应用程序的第一特征信息;

将所述第一特征信息发送至服务器;

接收所述服务器在判断所述第一特征信息与预置的第二特征信息匹配时，返回的所述第二特征信息对应的行为权限配置信息和权限组标识;

查找在本地预置的，所述权限组标识对应的行为权限基础信息; 以及

利用所述行为权限配置信息对所述行为权限基础信息进行配置，以获得行为权限信息。

在本发明实施例的一种可选示例中，所述行为权限信息可以包括白名单行为信息和黑名单行为信息中的至少一种;

所述行为权限配置信息可以包括白名单行为添加信息、白名单行为删除信息、白名单行为修改信息、黑名单行为添加信息、黑名单行为删除信息、黑名单行为修改信息中的至少一种;

所述行为权限基础信息可以包括白名单行为基础信息和黑名单行为基础信息中的至少一种。

在本发明实施例的一种可选示例中，所述权限信息获取模块201还可以适于:

在所述白名单行为基础信息中添加所述白名单行为添加信息对应的特征行为信息。

在本发明实施例的一种可选示例中，所述权限信息获取模块201还可以适于:

在所述白名单行为基础信息中删除所述白名单行为删除信息对应的特征行为信息。

在本发明实施例的一种可选示例中，所述权限信息获取模块201还可以

适于:

按照所述白名单行为修改信息对所述白名单行为基础信息中的特征行为信息进行修改。

在本发明实施例的一种可选示例中，所述权限信息获取模块201还可以适于:

在所述黑名单行为基础信息中添加所述黑名单行为添加信息对应的特征行为信息。

在本发明实施例的一种可选示例中，所述权限信息获取模块201还可以适于:

在所述黑名单行为基础信息中删除所述黑名单行为删除信息对应的特征行为信息。

在本发明实施例的一种可选示例中，所述权限信息获取模块201还可以适于:

按照所述黑名单行为修改信息对所述黑名单行为基础信息中的特征行为信息进行修改。

在本发明的一种可选实施例中，所述处理模块203还可以适于:

当所述行为信息与所述行为权限信息中的特征行为信息匹配时，执行所述特征行为信息对应的操作。

在本发明的一种可选实施例中，所述处理模块203还可以适于:

当所述行为信息与所述白名单行为信息中的特征行为信息匹配时，允许所述行为信息的执行。

在本发明的一种可选实施例中，所述处理模块203还可以适于:

当所述行为信息与所述黑名单行为信息中的特征行为信息匹配时，生成针对所述行为信息的第一提示信息。

在本发明的一种可选实施例中，所述处理模块203还可以适于:

当所述行为信息未与所述行为权限信息中的特征行为信息匹配时，生成针对所述行为信息的第二提示信息。

在本发明的一种可选实施例中，所述处理模块203还可以适于:

当所述行为信息未与所述行为权限信息中的特征行为信息匹配时，将所述应用程序的信息和所述行为信息发送至服务器;

接收所述服务器返回的，针对所述应用程序的信息和所述行为信息的

操作信息；以及

按照所述操作信息进行操作。

对于装置实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的基于应用程序的行为处理设备中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

例如，图 3 示出了可以实现根据本发明的基于应用程序的行为处理计算设备，例如应用服务器。该计算设备传统上包括处理器 310 和以存储器 320 形式的计算机程序产品或者计算机可读介质。存储器 320 可以是诸如闪存、EEPROM（电可擦除可编程只读存储器）、EPROM、硬盘或者 ROM 之类的电子存储器。存储器 320 具有存储用于执行上述方法中的任何方法步骤的程序代码 331 的存储空间 330。例如，存储程序代码的存储空间 330 可以包括分别用于实现上面的方法中的各种步骤的各个程序代码 331。这些程序代码可以从一个或者多个计算机程序产品中读出或者写入到这一个或者多个计算机程序产品中。这些计算机程序产品包括诸如硬盘，紧致盘（CD）、存储卡或者软盘之类的程序代码载体。这样的计算机程序产品通常为例如图 4 所示的便携式或者固定存储单元。该存储单元可以具有与图 3 的计算设备中的存储器 320 类似布置的存储段、存储空间等。程序代码可以例如以适当形式进行压缩。通常，存储单元包括用于执行根据本发明的方法步骤的计算机可读代码 331’，即可以由诸如 310 之类的处理器读取的代码，当这些代码由计算设备运行时，导致该计算设备执行上面所描述的方法中的各个步骤。

本文中所称的“一个实施例”、“实施例”或者“一个或者多个实施

例”意味着，结合实施例描述的特定特征、结构或者特性包括在本发明的至少一个实施例中。此外，请注意，这里“在一个实施例中”的词语例子不一定全指同一个实施例。

在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下被实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

此外，还应当注意，本说明书中使用的语言主要是为了可读性和教导的目的而选择的，而不是为了解释或者限定本发明的主题而选择的。因此，在不偏离所附权利要求书的范围和精神的情况下，对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。对于本发明的范围，对本发明所做的公开是说明性的，而非限制性的，本发明的范围由所附权利要求书限定。

权 利 要 求 书

1、一种基于应用程序的行为处理方法，包括步骤:

当检测到应用程序的启动操作时，获取所述应用程序对应的行为权限信息;

监测所述应用程序的行为信息；以及

按照所述行为权限信息对所述行为信息进行处理。

2、如权利要求 1 所述的方法，其中，所述获取所述应用程序对应的行为权限列表的步骤包括:

提取所述应用程序的第一特征信息;

将所述第一特征信息发送至服务器；以及

接收所述服务器在判断所述第一特征信息与预置的第二特征信息匹配时，返回的所述第二特征信息对应的行为权限信息。

3、如权利要求 1 所述的方法，其中，所述获取所述应用程序对应的行为权限列表的步骤包括:

提取所述应用程序的第一特征信息;

将所述第一特征信息发送至服务器;

接收所述服务器在判断所述第一特征信息与预置的第二特征信息匹配时，返回的所述第二特征信息对应的行为权限配置信息和权限组标识;

查找在本地预置的，所述权限组标识对应的行为权限基础信息；以及

利用所述行为权限配置信息对所述行为权限基础信息进行配置，以获得行为权限信息。

4、如权利要求 3 所述的方法，其中，所述行为权限信息包括白名单行为信息和黑名单行为信息中的至少一种;

所述行为权限配置信息包括白名单行为添加信息、白名单行为删除信息、白名单行为修改信息、黑名单行为添加信息、黑名单行为删除信息、黑名单行为修改信息中的至少一种；以及

所述行为权限基础信息包括白名单行为基础信息和黑名单行为基础信息中的至少一种。

5、如权利要求 4 所述的方法，其中，所述采用所述行为权限配置信息对所述行为权限基础信息进行配置，获得行为权限信息的步骤包括:

在所述白名单行为基础信息中添加所述白名单行为添加信息对应的特

征行为信息。

6、如权利要求 4 所述的方法，其中，所述采用所述行为权限配置信息对所述行为权限基础信息进行配置，获得行为权限信息的步骤包括:

在所述白名单行为基础信息中删除所述白名单行为删除信息对应的特征行为信息。

7、如权利要求 4 所述的方法，其中，所述采用所述行为权限配置信息对所述行为权限基础信息进行配置，获得行为权限信息的步骤包括:

按照所述白名单行为修改信息对所述白名单行为基础信息中的特征行为信息进行修改。

8、如权利要求 4 所述的方法，其中，所述采用所述行为权限配置信息对所述行为权限基础信息进行配置，获得行为权限信息的步骤包括:

在所述黑名单行为基础信息中添加所述黑名单行为添加信息对应的特征行为信息。

9、如权利要求 4 所述的方法，其中，所述采用所述行为权限配置信息对所述行为权限基础信息进行配置，获得行为权限信息的步骤包括:

在所述黑名单行为基础信息中删除所述黑名单行为删除信息对应的特征行为信息。

10、如权利要求 4 所述的方法，其中，所述采用所述行为权限配置信息对所述行为权限基础信息进行配置，获得行为权限信息的步骤包括:

按照所述黑名单行为修改信息对所述黑名单行为基础信息中的特征行为信息进行修改。

11、如权利要求 1-10 任一项所述的方法，其中，所述按照所述行为权限信息对所述行为信息进行处理的步骤包括:

当所述行为信息与所述行为权限信息中的特征行为信息匹配时，执行所述特征行为信息对应的操作。

12、如权利要求 11 所述的方法，其中，所述当所述行为信息与所述行为权限信息中的特征行为信息匹配时，执行所述特征行为信息对应的操作的步骤包括:

当所述行为信息与所述白名单行为信息中的特征行为信息匹配时，允许所述行为信息的执行。

13、如权利要求 11 所述的方法，其中，所述当所述行为信息与所述特

征行为信息匹配时，执行所述特征行为信息对应的操作的步骤包括:

当所述行为信息与所述黑名单行为信息中的特征行为信息匹配时，生成针对所述行为信息的第一提示信息。

14、如权利要求 1-10 任一项所述的方法，其中，所述按照所述行为权限信息对所述行为信息进行处理的步骤包括:

当所述行为信息未与所述行为权限信息中的特征行为信息匹配时，生成针对所述行为信息的第二提示信息。

15、如权利要求 1-10 任一项所述的方法，其中，所述按照所述行为权限信息对所述行为信息进行处理的步骤包括:

当所述行为信息未与所述行为权限信息中的特征行为信息匹配时，将所述应用程序的信息和所述行为信息发送至服务器;

接收所述服务器返回的，针对所述应用程序的信息和所述行为信息的操作信息；以及

按照所述操作信息进行操作。

16、一种基于应用程序的行为处理装置，包括:

权限信息获取模块，适于在检测到应用程序的启动操作时，获取所述应用程序对应的行为权限信息;

行为信息监测模块，适于监测所述应用程序的行为信息；以及

处理模块，适于按照所述行为权限信息对所述行为信息进行处理。

17、如权利要求16所述的装置，其中，所述权限信息获取模块还适于:

提取所述应用程序的第一特征信息;

将所述第一特征信息发送至服务器；以及

接收所述服务器在判断所述第一特征信息与预置的第二特征信息匹配时，返回的所述第二特征信息对应的行为权限信息。

18、如权利要求16所述的装置，其中，所述权限信息获取模块还适于:

提取所述应用程序的第一特征信息;

将所述第一特征信息发送至服务器;

接收所述服务器在判断所述第一特征信息与预置的第二特征信息匹配时，返回的所述第二特征信息对应的行为权限配置信息和权限组标识;

查找在本地预置的，所述权限组标识对应的行为权限基础信息；以及

利用所述行为权限配置信息对所述行为权限基础信息进行配置，以获

得行为权限信息。

19、如权利要求 18 所述的装置，其中，所述行为权限信息包括白名单行为信息和黑名单行为信息中的至少一种;

所述行为权限配置信息包括白名单行为添加信息、白名单行为删除信息、白名单行为修改信息、黑名单行为添加信息、黑名单行为删除信息、黑名单行为修改信息中的至少一种; 以及

所述行为权限基础信息包括白名单行为基础信息和黑名单行为基础信息中的至少一种。

20、如权利要求19所述的装置，其中,所述权限信息获取模块还适于:

在所述白名单行为基础信息中添加所述白名单行为添加信息对应的特征行为信息。

21、如权利要求19所述的装置，其中,所述权限信息获取模块还适于:

在所述白名单行为基础信息中删除所述白名单行为删除信息对应的特征行为信息。

22、如权利要求19所述的装置，其中,所述权限信息获取模块还适于:

按照所述白名单行为修改信息对所述白名单行为基础信息中的特征行为信息进行修改。

23、如权利要求19所述的装置，其中,所述权限信息获取模块还适于:

在所述黑名单行为基础信息中添加所述黑名单行为添加信息对应的特征行为信息。

24、如权利要求19所述的装置，其中,所述权限信息获取模块还适于:

在所述黑名单行为基础信息中删除所述黑名单行为删除信息对应的特征行为信息。

25、如权利要求19所述的装置，其中,所述权限信息获取模块还适于:

按照所述黑名单行为修改信息对所述黑名单行为基础信息中的特征行为信息进行修改。

26、如权利要求 16-25 任一项所述的装置，所述处理模块还适于:

当所述行为信息与所述行为权限信息中的特征行为信息匹配时，执行所述特征行为信息对应的操作。

27、如权利要求 26 所述的装置，其中，所述处理模块还适于:

当所述行为信息与所述白名单行为信息中的特征行为信息匹配时，允

许所述行为信息的执行。

28、如权利要求 26 所述的装置，其中，所述处理模块还适于:

当所述行为信息与所述黑名单行为信息中的特征行为信息匹配时，生成针对所述行为信息的第一提示信息。

29、如权利要求 16-25 任一项所述的装置，其中，所述处理模块还适于:

当所述行为信息未与所述行为权限信息中的特征行为信息匹配时，生成针对所述行为信息的第二提示信息。

30、如权利要求 16-25 任一项所述的装置，其中，所述处理模块还适于:

当所述行为信息未与所述行为权限信息中的特征行为信息匹配时，将所述应用程序的信息和所述行为信息发送至服务器;

接收所述服务器返回的，针对所述应用程序的信息和所述行为信息的操作信息；以及

按照所述操作信息进行操作。

31 、一种计算机程序，包括计算机可读代码，当所述计算机可读代码在计算设备上运行时，导致所述计算设备执行根据权利要求 1-15 中的任一个所述的基于应用程序的行为处理方法。

32、一种计算机可读介质，其中存储了如权利要求 31 所述的计算机程序。

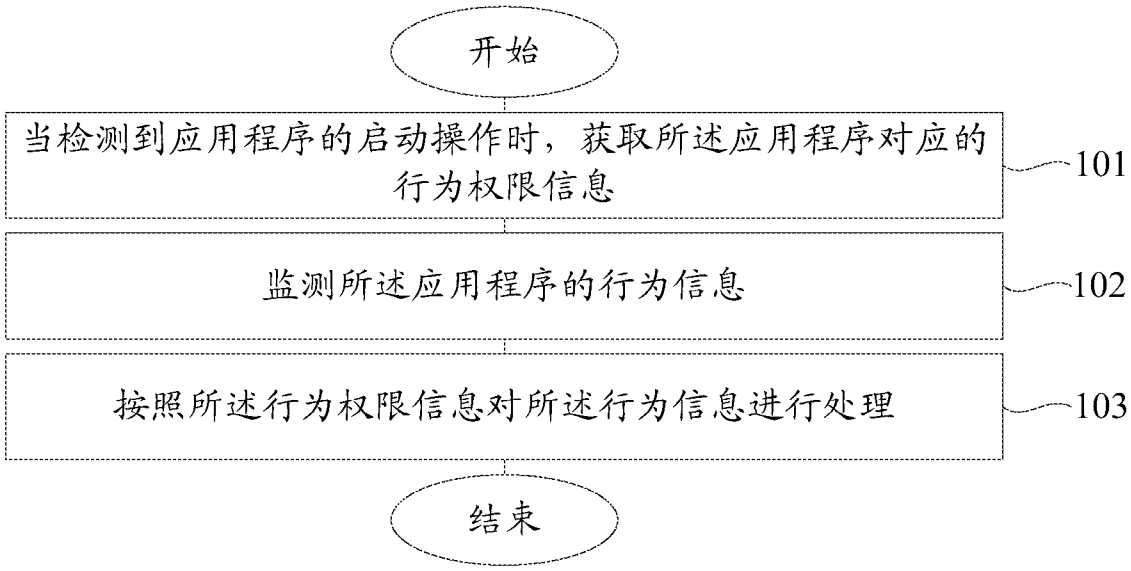
开始
当检测到应用程序的启动操作时，获取所述应用程序对应的行为权限信息
101
监测所述应用程序的行为信息
102
按照所述行为权限信息对所述行为信息进行处理
103
结束

图 1

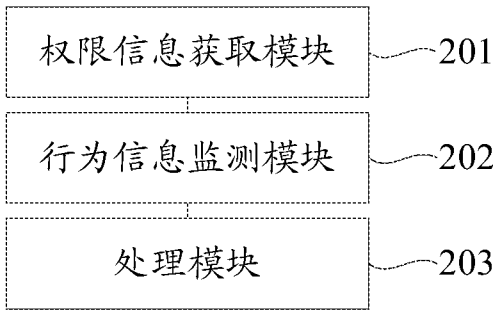
权限信息获取模块
201
行为信息监测模块
202
处理模块
203

图 2

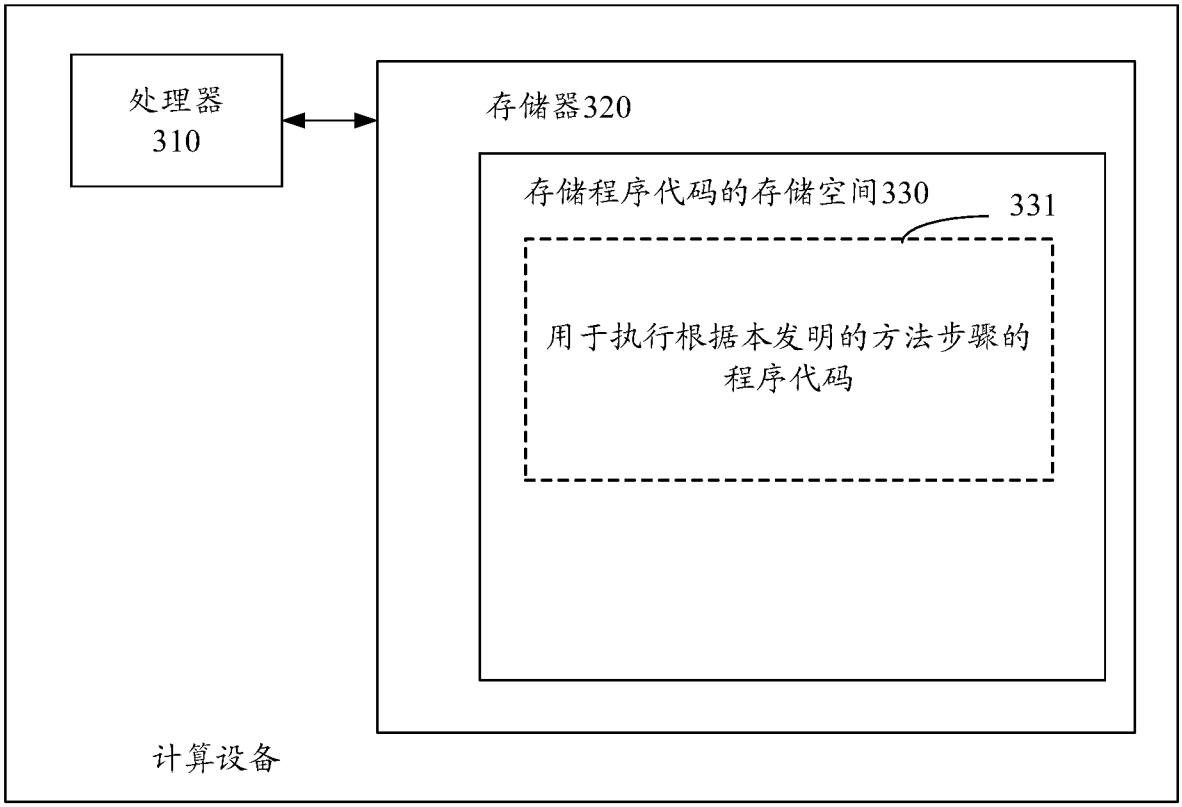
处理器
310
存储器320
存储程序代码的存储空间330
331
用于执行根据本发明的方法步骤的
程序代码
计算设备

图 3

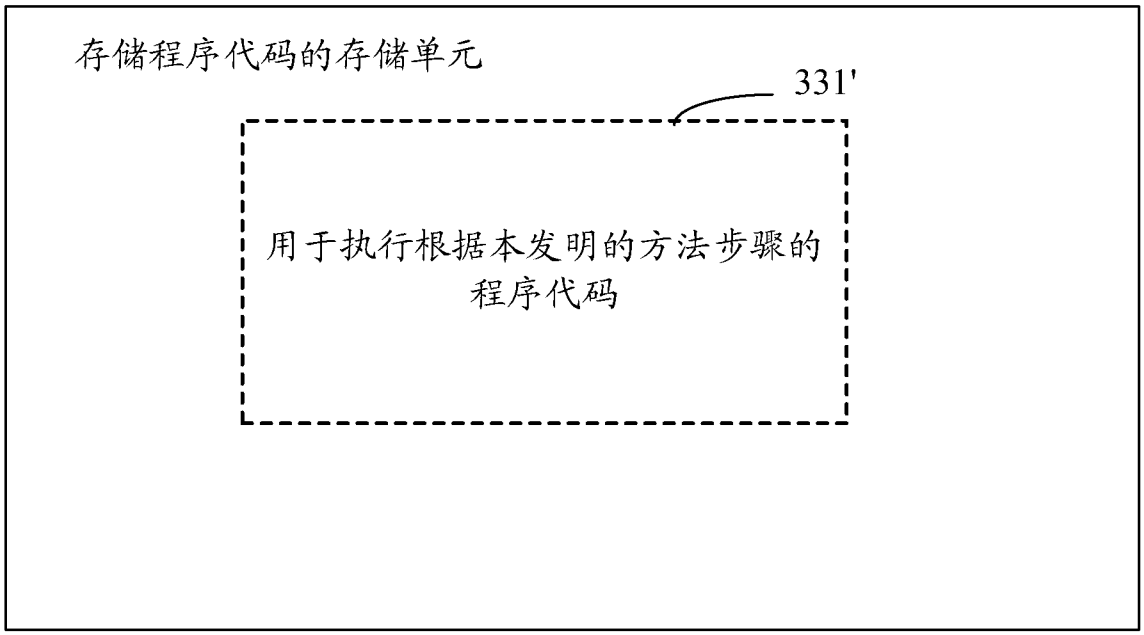
存储程序代码的存储单元
331'
用于执行根据本发明的方法步骤的
程序代码

图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/095454

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/52 (2013.01) 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)

G06F 21

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, CNTXT, VEN: software, behaviour, operation, action, black list, white list, application, act, authori+, permit, permission, trust, white, black, list

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 104484599 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 01 April 2015 (01.04.2015), description, paragraphs 275-358	1-32
X	CN 103890770 A (MCAFEE INC.), 25 June 2014 (25.06.2014), description, paragraphs 5-7, 26-32, 44-45 and 68, and figures 3 and 6C	1-2, 11-15, 16-17, 26-30, 31-32
X	CN 103218552 A (HUAWEI DEVICE CO., LTD.), 24 July 2013 (24.07.2013), description, paragraphs 25-63, and figures 1-2	1-2, 11, 14-15, 16-17, 26, 29-30, 31-32
A	US 2014090077 A1 (SAMSUNG ELECTRONICS CO., LTD.), 27 March 2014 (27.03.2014), the whole document	1-32
A	CN 103761472 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 30 April 2014 (30.04.2014), the whole 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
15 January 2016 (15.01.2016)	**25 January 2016 (25.01.2016)**
Name and mailing address of the ISA/CN: 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 **XU, Feifei** Telephone No.: (86-10) **62411752**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/095454

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104484599 A	01 April 2015	None	
CN 103890770 A	25 June 2014	US 2013097660 A1	18 April 2013
		US 2015180908 A1	25 June 2015
		EP 2769327 A1	27 August 2014
		EP 2769327 A4	01 July 2015
		WO 2013059138 A1	25 April 2013
CN 103218552 A	24 July 2013	None	
US 2014090077 A1	27 March 2014	KR 20140044991 A	16 April 2014
CN 103761472 A	30 April 2014	WO 2015124018 A1	27 August 2015

国际检索报告

国际申请号 PCT/CN2015/095454

A. 主题的分类

G06F 21/52(2013.01)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)

G06F21

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,CNTXT,VEN:应用，软件，行为，操作，动作，权限，信任，黑名单，白名单，application,act,authori+,permit,permission,trust,white,black,list

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
PX	CN 104484599 A (北京奇虎科技有限公司等) 2015年 4月 1日 (2015-04-01) 说明书第275-358段	1-32
X	CN 103890770 A (迈可菲公司) 2014年 6月 25日 (2014-06-25) 说明书第5-7，26-32，44-45，68段，图3，6C	1-2，11-15，16-17，26-30，31-32
X	CN 103218552 A (华为终端有限公司) 2013年 7月 24日 (2013-07-24) 说明书第25-63段，图1-2	1-2，11，14-15，16-17，26，29-30，31-32
A	US 2014090077 A1 (SAMSUNG ELECTRONICS CO LTD) 2014年 3月 27日 (2014-03-27) 全文	1-32
A	CN 103761472 A (北京奇虎科技有限公司等) 2014年 4月 30日 (2014-04-30) 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
2016年 1月 15日	2016年 1月 25日
ISA/CN的名称和邮寄地址 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 传真号 (86-10)62019451	受权官员 许菲菲 电话号码 (86-10)62411752

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/095454

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	104484599	A	2015年 4月 1日		无		
CN	103890770	A	2014年 6月 25日	US	2013097660	A1	2013年 4月 18日
				US	2015180908	A1	2015年 6月 25日
				EP	2769327	A1	2014年 8月 27日
				EP	2769327	A4	2015年 7月 1日
				WO	2013059138	A1	2013年 4月 25日
CN	103218552	A	2013年 7月 24日		无		
US	2014090077	A1	2014年 3月 27日	KR	20140044991	A	2014年 4月 16日
CN	103761472	A	2014年 4月 30日	WO	2015124018	A1	2015年 8月 27日