

(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
2020 年 7 月 2 日 (02.07.2020)



(10) 国际公布号
WO 2020/132876 A1

(51) 国际专利分类号:
G06F 21/33 (2013.01)

(21) 国际申请号: PCT/CN2018/123534

(22) 国际申请日: 2018 年 12 月 25 日 (25.12.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 奇安信安全技术(珠海)有限公司(QI AN XIN SECURITY TECHNOLOGY (ZHUHAI) CO., LTD.) [CN/CN]; 中国广东省珠海市高新区唐家湾镇金唐路1号港湾1号科创园14栋501、601号, Guangdong 519000 (CN)。奇安信科技集团股份有限公司(QI AN XIN TECHNOLOGY GROUP INC.) [CN/CN]; 中国北京市西城区新街口外大街28号102号楼3层332号, Beijing 100088 (CN)。

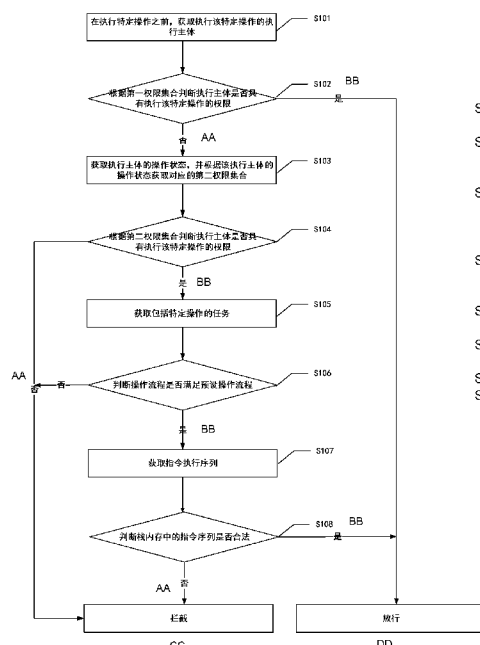
(72) 发明人: 徐贵斌(XU, Guibin); 中国广东省珠海市高新区唐家湾镇金唐路1号港湾1号科创园14栋501、601号, Guangdong 519000 (CN)。

(74) 代理人: 中科专利商标代理有限公司(CHINA SCIENCE PATENT & TRADEMARK AGENT LTD.); 中国北京市海淀区西三环北路87号4-1105室, Beijing 100089 (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,

(54) Title: OPERATION DETECTION METHOD AND SYSTEM, AND ELECTRONIC DEVICE

(54) 发明名称: 一种操作检测方法、系统及电子设备



S101 Before executing a specific operation, obtain an execution subject executing the specific operation
S102 Determine, according to a first permission set, whether the execution subject has the permission to execute the specific operation
S103 Obtain the operation state of the execution subject, and according to the operation state of the execution subject, obtain a corresponding second permission set
S104 Determine, according to the second permission set, whether the execution subject has the permission to execute the specific operation
S105 Obtain a task comprising the specific operation
S106 Determine whether an operation process satisfies a preset operation process
S107 Obtain an instruction execution sequence
S108 Determine whether an instruction sequence in a stack memory is valid
AA No
BB Yes
CC Intercept
DD Release

图 1

(57) Abstract: An operation detection method, comprising: S1, obtaining an execution subject executing a specific operation; S2, determining, according to a first permission set, whether the execution subject has the permission to execute the specific operation; S3, obtaining the operation state of the execution subject and a corresponding second permission set; S4, determining, according to the second permission set, whether the execution subject has the permission to execute the specific operation, if yes, executing operation S5, and if not, processing the execution subject; S5, obtaining a task comprising the specific operation, the task corresponding to an

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))。

operation process; S6, determining whether the operation process satisfies a preset operation process, and if not, processing the execution subject; S7, obtaining an instruction execution sequence corresponding to at least one operation in the task; and S8, determining whether the instruction execution sequence matches a preset instruction execution sequence, and if not, processing the execution subject. Also provided are an operation detection system and an electronic device.

(57) 摘要: 一种操作检测方法, 包括: S1, 获取执行该特定操作的执行主体; S2, 根据第一权限集合判断执行主体是否具有执行该特定操作的权限; S3, 获取执行主体的操作状态及其对应的第二权限集合; S4, 根据第二权限集合判断执行主体是否具有执行特定操作的权限, 若是, 则执行操作S5, 若否, 则对执行主体进行处理; S5, 获取包括特定操作的任务, 该任务对应的操作流程; S6, 判断所述操作流程是否满足预设操作流程, 若否, 则对所述执行主体进行处理; S7, 获取任务中至少一个操作所对应的指令执行序列; S8, 判断指令执行序列与预设指令执行序列是否匹配, 若否, 则对所述执行主体进行处理。还提供一种操作检测系统及电子设备。

一种操作检测方法、系统及电子设备

技术领域

本公开属于网络安全领域，具体涉及一种操作检测方法、系统及电子设备。

5

背景技术

随着计算机网络的发展，网络安全越来越受到业界的重视。对于计算机网络被黑客攻击的情况，人们希望能在攻击发生的过程中或者危害结果发生之前发现此攻击，以在最大程度上避免侵害。现有技术中所采用的网络安全手段有多种，例如：“恶意软件检测”、“攻击发现”、“恶意行为检测”等等，这些技术虽然能够进行安全防护，但随着攻击手段的提高，已不能满足日益增长的网络安全需求。

10

发明内容

15

本公开的一个方面提供了一种操作检测方法，包括：S1，在执行特定操作之前，获取执行该特定操作的执行主体；S2，根据第一权限集合判断所述执行主体是否具有执行该特定操作的权限，若否，则执行操作S3；S3，获取所述执行主体的操作状态，并根据该执行主体的操作状态获取对应的第二权限集合；S4，根据第二权限集合判断所述执行主体是否具有执行该特定操作的权限，若是，则执行操作S5，若否，则对所述执行主体进行处理；S5，获取包括所述特定操作的任务，该任务对应执行至少一个操作的操作流程；S6，判断所述操作流程是否满足预设操作流程，若是，则执行操作S7；若否，则对执行主体进行处理；S7，获取任务中至少一个操作所对应的指令执行序列；S8，判断指令执行序列与预设指令执行序列是否匹配，若否，则对执行主体进行处理。

20

25

可选地，步骤S6中，判断所述操作流程是否满足预设操作流程，

包括：获取所述操作流程所对应的至少一个操作；判断所述至少一个操作中每个操作是否与所述预设操作流程中所对应的操作一致。

可选地，所述判断所述至少一个操作中每个操作是否与所述预设操作流程中所对应操作一致，包括：判断所述至少一个操作中每个操作的
5 执行主体是否与预设操作流程所对应操作的执行主体一致。

可选地，在所述步骤 S1 之前，还包括：S0，创建第一权限集合，所述第一权限集合包括至少一个执行主体在任意操作状态下的操作权限。

可选地，在所述步骤 S1 之前，还包括：S0'，创建至少一个第二权限集合，其中，每个所述第二权限集合对应一个执行主体的一个操作状态，并且，每个所述第二权限集合包括对应执行主体在对应操作状态下的操作权限。
10

可选地，所述至少一个第二权限集合存储在远端，所述步骤 S3 中，根据该执行主体的操作状态获取对应的第二权限集合，包括：向远端发送请求，所述请求包括所述执行主体信息及其操作状态；获取远端发送的第二权限集合，其中，该第二权限集合是由所述远端响应所述请求而返回。
15

可选地，步骤 S3 中，获取所述执行主体的操作状态，至少包括：根据所述执行主体的调用方式确定所述执行主体的操作状态，其中，所述执行主体是由用户直接调用时，确定所述执行主体的操作状态为第一操作状态，当所述执行主体是由其他执行主体调用时，确定所述执行主体的操作状态为第二操作状态。
20

可选地，步骤 S8 中，判断所述指令执行序列与预设指令执行序列是否匹配，包括：获取所述指令执行序列中的函数调用信息，所述函数调用信息包括函数调用次数和/或函数调用顺序；判断所述指令执行序列中的函数调用信息与预设指令执行序列中的函数调用信息是否匹配。
25

可选地，步骤 S7 中，获取所述任务中至少一个操作所对应的指令执行序列，包括：从栈内存中获取所述任务中至少一个操作所对应的指令执行序列。

本公开的另一方面提供了一种操作检测系统，包括：第一获取模块，用于在执行特定操作之前，获取执行特定操作的执行主体；第一判断模块，用于根据第一权限集合判断所述执行主体是否具有执行该特定操作的权限，若否，则执行第二获取模块；第二获取模块，用于获取所述执行主体的操作状态，并根据该执行主体的操作状态获取对应的第二权限集合；第二判断模块，用于根据第二权限集合判断所述执行主体是否具有执行该特定操作的权限，若是，则执行第三获取模块，若否，则对所述执行主体进行处理；第三获取模块，用于获取包括所述特定操作的任务，该任务对应有执行至少一个操作的操作流程；第三判断模块，用于判断所述操作流程是否满足预设操作流程，若是，则执行第四获取模块，若否，则对执行主体进行处理；第四获取模块，用于获取任务中至少一个操作所对应的指令执行序列；第四判断模块，用于判断指令执行序列与预设指令执行序列是否匹配，若否，则对执行主体进行处理。

可选地，第三判断模块中，判断所述操作流程是否满足预设操作流程，包括：获取所述操作流程所对应的至少一个操作；判断所述至少一个操作中每个操作是否与所述预设操作流程中所对应的操作一致。

可选地，第三判断模块判断所述至少一个操作中每个操作是否与所述预设操作流程中所对应操作一致，包括：判断所述至少一个操作中每个操作的执行主体是否与预设操作流程所对应操作的执行主体一致。

可选地，操作检测系统还包括：第一创建模块，用于创建第一权限集合，所述第一权限集合包括至少一个执行主体在任意操作状态下的操作权限。

可选地，操作检测系统，还包括：第二创建模块，用于创建至少一个第二权限集合，其中，每个所述第二权限集合对应一个执行主体的一个操作状态，并且，每个所述第二权限集合包括对应执行主体在对应操作状态下的操作权限。

可选地，至少一个第二权限集合存储在远端，所述第二获取模块根据该执行主体的操作状态获取对应的第二权限集合，包括：向远端发送请求，所述请求包括所述执行主体信息及其操作状态；获取远端发送的

第二权限集合，其中，该第二权限集合是由所述远端响应所述请求而返回。

可选地，第二获取模块获取所述执行主体的操作状态，至少包括：根据所述执行主体的调用方式确定所述执行主体的操作状态，其中，所述执行主体是由用户直接调用时，确定所述执行主体的操作状态为第一操作状态，当所述执行主体是由其他执行主体调用时，确定所述执行主体的操作状态为第二操作状态。

可选地，第四判断模块判断指令执行序列与预设指令执行序列是否匹配，包括：获取指令执行序列中的函数调用信息，函数调用信息包括函数调用次数和/或函数调用顺序；判断指令执行序列中的函数调用信息与预设指令执行序列中的函数调用信息是否匹配。

可选地，第四获取模块获取任务中至少一个操作所对应的指令执行序列，包括：从栈内存中获取任务中至少一个操作所对应的指令执行序列。

本公开的另一方面提供了一种电子设备，包括：处理器；存储器，存储有计算机可执行指令，该计算机可执行指令在被所述处理器执行时，使得所述处理器执行：S1，在执行特定操作之前，获取执行该特定操作的执行主体；S2，根据第一权限集合判断所述执行主体是否具有执行该特定操作的权限，若否，则执行操作 S3；S3，获取所述执行主体的操作状态，并根据该执行主体的操作状态获取对应的第二权限集合；S4，根据第二权限集合判断所述执行主体是否具有执行该特定操作的权限，若是，则执行操作 S5，若否，则对所述执行主体进行处理；S5，获取包括所述特定操作的任务，该任务对应有执行至少一个操作的操作流程；S6，判断所述操作流程是否满足预设操作流程，若是，则执行操作 S7；若否，则对执行主体进行处理；S7，获取任务中至少一个操作所对应的指令执行序列；S8，判断指令执行序列与预设指令执行序列是否匹配，若否，则对执行主体进行处理。

可选地，处理器在执行步骤 S6 时，判断所述操作流程是否满足预设操作流程，包括：获取所述操作流程所对应的至少一个操作；判断所

述至少一个操作中每个操作是否与所述预设操作流程中所对应的操作一致。

可选地，处理器判断所述至少一个操作中每个操作是否与所述预设操作流程中所对应操作一致，包括：判断所述至少一个操作中每个操作的执行主体是否与预设操作流程所对应操作的执行主体一致。

可选地，处理器在执行所述步骤 S1 之前，还执行：S0，创建第一权限集合，所述第一权限集合包括至少一个执行主体在任意操作状态下的操作权限。

可选地，处理器在执行所述步骤 S1 之前，还执行：S0'，创建至少一个第二权限集合，其中，每个所述第二权限集合对应一个执行主体的一个操作状态，并且，每个所述第二权限集合包括对应执行主体在对应操作状态下的操作权限。

可选地，至少一个第二权限集合存储在远端，所述处理器在执行所述步骤 S3 时，根据该执行主体的操作状态获取对应的第二权限集合，包括：向远端发送请求，所述请求包括所述执行主体信息及其操作状态；获取远端发送的第二权限集合，其中，该第二权限集合是由所述远端响应所述请求而返回。

可选地，处理器在执行所述步骤 S3 时，获取所述执行主体的操作状态，至少包括：根据所述执行主体的调用方式确定所述执行主体的操作状态，其中，所述执行主体是由用户直接调用时，确定所述执行主体的操作状态为第一操作状态，当所述执行主体是由其他执行主体调用时，确定所述执行主体的操作状态为第二操作状态。

可选地，处理器在执行步骤 S8 时，判断指令执行序列与预设指令执行序列是否匹配，包括：获取指令执行序列中的函数调用信息，函数调用信息包括函数调用次数和/或函数调用顺序；判断指令执行序列中的函数调用信息与预设指令执行序列中的函数调用信息是否匹配。

可选地，处理器在执行步骤 S7 时，获取任务中至少一个操作所对应的指令执行序列，包括：从栈内存中获取任务中至少一个操作所对应的指令执行序列。

本公开的另一方面提供了一种计算机可读介质，存储有计算机可执行指令，所述指令在被执行时用于实现如上任一项所述的方法。

本公开的另一方面提供了一种计算机程序，所述计算机程序包括计算机可执行指令，所述指令在被执行时用于实现如上任一项所述的方法。

5

附图说明

图 1 示意性示出了根据本公开实施例的操作检测方法的流程图。

图 2 示意性示出了本公开实施例中“远程启动 Shell 程序 cmd.exe”的合法操作流程图。

10 图 3 示意性示出了本公开实施例中“远程启动 Shell 程序 cmd.exe”的非法操作流程图。

图 4 示意性示出了根据本公开实施例的操作检测系统的框图。

图 5 示意性示出了根据本公开另一实施例的电子设备的框图。

15 具体实施方式

以下，将参照附图来描述本公开的实施例。但是应该理解，这些描述只是示例性的，而并非要限制本公开的范围。此外，在以下说明中，省略了对公知结构和技术的描述，以避免不必要地混淆本公开的概念。

20 在此使用的术语仅仅是为了描述具体实施例，而并非意在限制本公开。这里使用的词语“一”、“一个（种）”和“该”等也应包括“多个”、“多种”的意思，除非上下文另外明确指出。此外，在此使用的术语“包括”、“包含”等表明了所述特征、步骤、操作和/或部件的存在，但是并不排除存在或添加一个或多个其他特征、步骤、操作或部件。

25 在此使用的所有术语（包括技术和科学术语）具有本领域技术人员通常所理解的含义，除非另外定义。应注意，这里使用的术语应解释为具有与本说明书的上下文相一致的含义，而不应以理想化或过于刻板的方式来解释。

附图中示出了一些方框图和/或流程图。应理解，方框图和/或流程图的一些方框或其组合可以由计算机程序指令来实现。这些计算机程序指令可以提供给通用计算机、专用计算机或其他可编程数据处理装置的处理器，从而这些指令在由该处理器执行时可以创建用于实现这些方框图和/或流程图中所说明的功能/操作的装置。

因此，本公开的技术可以硬件和/或软件（包括固件、微代码等）的形式来实现。另外，本公开的技术可以采取存储有指令的计算机可读介质上的计算机程序产品的形式，该计算机程序产品可供指令执行系统使用或者结合指令执行系统使用。在本公开的上下文中，计算机可读介质可以是能够包含、存储、传送、传播或传输指令的任意介质。例如，计算机可读介质可以包括但不限于电、磁、光、电磁、红外或半导体系统、装置、器件或传播介质。计算机可读介质的具体示例包括：磁存储装置，如磁带或硬盘（HDD）；光存储装置，如光盘（CD-ROM）；存储器，如随机存取存储器（RAM）或闪存；和/或有线/无线通信链路。

图 1 示意性示出了根据本公开实施例的操作检测方法的流程图。

具体地，如图 1 所示，本公开实施例的操作检测方法包括以下操作：
S101，在执行特定操作之前，获取执行该特定操作的执行主体。

在操作系统中为了完成任务，会执行各种各样的操作，这些操作经常会涉及到系统中的服务、程序、文件、数据等。本公开的“特定操作”是指一些敏感的、有可能导致危险后果的操作，其包括但不限于可执行文件加载、内存操作、文件操作、网络访问、端口监听、注册表项操作、敏感窗口消息发送等等。

本公开在操作系统中会实时对上述的特定操作进行监控，其监控手段可以有多种。例如可以采用“挂钩（HOOK）技术”，“挂钩”是计算机安全领域常用的一种安全监控方法，可以对一些应用程序编程接口（Application Programming Interface, API）进行挂钩，当系统执行特定操作时，就会进入到 HOOK 处理流程中；又例如可以采用操作系统提供的各类的功能过滤驱动，比如：文件过滤驱动、网络过滤驱动等等，可以对涉及相应文件、网络等的特定操作进行监控。

本公开所提及的“执行该特定操作的执行主体”包括但不限于操作系统本身、安装在操作系统上的应用程序等。当执行主体在执行特定操作之前，会通过上述监控手段获取该执行主体的信息，包括但不限于执行主体的名称、创建时间、位置索引等等。

5 S102，根据第一权限集合判断执行主体是否具有执行该特定操作的权限，若是，则对该特定操作放行，若否，则执行操作 S103。

由于目前的应用程序繁多，其中，Windows10 平台拥有 3500 万个应用程序、IOS 平台拥有 210 万个应用程序、安卓平台拥有 260 万个应用程序，这些应用程序所涉及的操作更是不计其数，若通过黑名单或者
10 白名单的方式对每个应用程序的特定操作都进行判定，需要耗费巨大的资源收集每个应用程序的特定操作及合法性。

本公开出于上述考虑，在执行上述操作 S101 之前，会创建第一权限集合，称之为“最小行为权限集合”，该集合包括至少一个执行主体在任意操作状态下的操作权限。其中，本公开中执行主体的操作状态是指执行主体在执行该特定操作时所处于的状态，例如执行主体为
15 winword 程序，其在运行时可以打开 word 文档，如果该 winword 程序是用户主动运行的，那么其操作状态为主动运行状态，如果该 winword 程序是被其他程序调用所运行的，那么其操作状态为被动运行状态。还是以 winword 程序为例，若其打开的 word 文档会以一个窗口的形式进行
20 显示，那么其操作状态为窗口状态，若其打开的 word 文档会只在后台运行并不显示，那么其操作状态为非窗口状态。本公开中第一权限集合只涉及执行主体在“任意操作状态下”的操作权限，其“不同操作状态下”的操作权限将在后文中描述。

本公开所提供的第一权限集合至少包括如下执行主体在任意操作
25 状态下的操作权限：

- 非特定的应用程序的运行方式为非自动运行

解释：一般的应用程序不可以自动运行，只能由用户手动执行，特定的需要自动运行的程序由程序专属行为集合进行处理；

- 应用程序只能操作自身直接和/或间接创建的文件

解释：应用程序只可以全权操作（读、写、打开、删除等）自己创建的或与自己一起由同一安装包直接或间接创建的文件；

- 应用程序对操作系统文件仅有只读的权限；
- 应用程序不能操作除了自身直接和/或间接创建的文件外的非系统

5 文件

解释：应用程序不可以操作（读、写、打开、删除等）除自身直接和/或间接创建的文件外的、任何非系统的文件；

- 应用程序不允许访问内外网络及网内设备节点
- 在非用户操作时，应用程序不允许对其它进程进行跨进程操作；
- 操作系统本身及应用程序，不允许不通过文件系统而直接操作磁

盘；

• 在非用户操作时，操作系统及应用程序不允许下载或执行另一个程序，不可以加载驱动；

- 在非用户操作时，操作系统及应用程序不允许读写用户私有数据

15 解释：用户私有数据包括但不限于文档、照片等；

• 在用户操作时，只有数据所对应的默认编辑程序可以操作对应数据类型文档

解释：默认编辑程序以操作系统注册表中的登记为准，例如，word 文档只允许 winword 程序或 WPS 操作；

20 • 在用户操作时，对应的行为主体，只有对单一客体进行操作的权限

解释：比如用户调用 winword 程序打开了 word 文档 A，那 winword 程序将拥有对 A 的操作权限，但对用户并没有显示主动打开的 word 文档 B，winword 程序并不具备操作权限；

25 • 在非用户操作时，操作系统及应用程序不具备添加账户的权限；

• 在非用户操作时，操作系统及应用程序不具备写关键注册表项的权限

解释：关键注册表项包括但不限于浏览器主页、自启动项、各类型文件的默认程序设置、系统启动设置等；

- 在非用户操作时，操作系统本身及应用程序不具备调用系统功能类程序的权限

解释：系统功能类程序包括但不限于 shell 程序、注册表编辑器、计划任务、磁盘文件注册表的权限更改类程序；

- 5 • 在非用户操作时，操作系统及应用程序不具备创建并执行脚本文件的权限。

通过上述第一权限集合的设定，能够有效判定大多数的执行主体是否具有执行该特定操作的权限，无需对每个执行主体及相应的特定操作建立黑名单或者白名单，从而节省了系统开销。在本操作中，若执行主体所执行的特定操作符合上述第一权限集合，则对该特定操作放行，并使该特定操作执行，若执行主体所执行的特定操作不符合上述第一权限集合，则执行操作 S103，以对其进行进一步判定。

10

S103，获取执行主体的操作状态，并根据该执行主体的操作状态获取对应的第二权限集合。

- 15 在上述操作 S102 中已解释了执行主体的操作状态，在此就不再赘述。另外，上述操作 S102 所设定的第一权限集合能够对任何有风险的操作进行过滤。然而，对于一些特殊的应用程序，其在正常运行时即会超出第一权限集合所限制的权限，比如：安全软件，它有检测全系统可执行文件是否被病毒感染的操作，但受限于第一权限集合的限制，其并不能操作其它的应用程序。因此，如果仅采用本公开的第一权限集合来进行判定，会对例如安全软件等一些特殊的应用程序产生“误报”。对于上述情形，本公开需要对不满足第一权限集合的执行主体进行进一步判定，由此引入本公开的第二权限集合。
- 20

- 25 本公开出于上述考虑，在执行上述操作 S101 之前，还会创建一个以上的第二权限集合，其中，每个第二权限集合对应一个执行主体的一个操作状态，并且，每个第二权限集合包括对应执行主体在对应操作状态下的操作权限。

例如，针对 winword 程序，第二权限集合规定：

- 用户主动执行 winword 程序时，拥有操作对应客体的权限，即：

用户主动通过 winword 程序打开 word 文档 A 时，winword 程序即拥有 word 文档 A 的操作权限。(注：双击 word 文档，由操作系统调用 winword 程序来打开；与双击 winword 程序再通过菜单或拖拽操作打开文档，都是因用户操作触发的行为，都被视为“主动运行状态”)

5 • 非用户主动执行 winword 程序时（被动运行状态），并不具备操作 word 文档的权限。

• 用户主动执行 winword 程序时，也并不具备操作非对应客体的权限，即：打开 word 文档 A 时，winword 程序只具备操作 A 的单一权限，并不具备操作 B、C 等其它 word 文档或非 word 文档的权限。

10 通过上述例子可以看出，第二权限集合规定了 winword 程序在“主动运行状态”及“被动运行状态”这两种操作状态下的不同权限。

在本公开操作 S103 中，可以通过不同的方式确定执行主体的不同操作状态。

15 根据本公开的一种实施方式，可以根据执行主体的调用方式确定执行主体的操作状态，其中，执行主体是由用户直接调用时，确定执行主体的操作状态为主动运行状态，当执行主体是由其他执行主体调用时，确定执行主体的操作状态为被动运行状态。

20 根据本公开的另一种实施方式，可以根据执行主体对执行客体的操作方式来确定执行主体的操作状态，例如，winword 程序为例，若其打开的 word 文档会以一个窗口的形式进行显示，那么其操作状态为窗口状态，若其打开的 word 文档会只在后台运行并不显示，那么其操作状态为非窗口状态。

25 上述实施方式仅为说明执行主体的不同操作状态而举出的例子，其操作状态并不限定于上述两种实施方式。另外，操作 S103 中所获取的操作状态并不局限于一种操作状态，也可以针对同一执行主体同时获取多个其所属的操作状态（例如可以同时获取的 winword 程序为主动执行状态及窗口状态），用于后续判定。

另外还需要说明的是，每一个第二权限集合对应一个执行主体的至少一个操作状态，所以说第二权限集合的数量极为庞大。因此，本公开

可将创建的第二权限集合存储在远端（例如服务器端、云端等），客户端在实施本公开时，向远端发送请求，该请求包括执行主体信息及其操作状态，远端响应请求，根据执行主体信息及其操作状态检索出对于的第二权限集合，并发送给客户端。更进一步地，客户端在获取到第二权限集合后，可以将此第二权限集合联合对于的执行主体信息及其操作状态进行本地缓存。当客户端再次需要获取该第二权限集合后，可以先从本地缓存中进行查询，若不存在，再向远端发送请求。在本公开的另外一种实施方式中，客户端在安装应用程序（或其他执行主体）时，即从远端获取应用程序（或其他执行主体）所对应的各种操作状态的第二权限集合，并进行本地保存。这样在后续获取第二权限集合时，即可直接从本地调用。

S104，根据第二权限集合判断执行主体是否具有执行该特定操作的权限，若是，则执行操作 S105，若否，则对执行主体进行处理。

以上已经介绍了第二权限集合包括对应执行主体在对应操作状态下的操作权限，因此容易理解操作 S104 中的判断流程，在此就不再赘述。但需要强调的是，本公开从执行主体的操作状态层面上进行了权限判定，不再局限于“应用程序本身行为、应用程序功能与种类”，能够较为准确地判定执行主体的“越权行为”。

再以上述安全软件为例，其由于在正常运行时会检测全系统可执行文件是否被病毒感染的操作，故需要有无需用户干预自动进行安全检测的功能，且进行安全检测时一般都需要连接云端的病毒特征库，这些功能显然已经超出了上述第一权限集合所规定的权限。因此，其必定不能通过第一权限集合的判定，此时，需要第二权限集合对其进行进一步判定。在安全软件的任意操作状态下，其对应的第二权限集合规定了其具有“可以自动运行、可以非经用户操作连接网络”的权限，所以其能通过第二权限集合的判定。通过上例可以看出，第二权限集合的设定可以避免第一权限集合对一些特定执行主体的“误报”。

另外，本公开设定第二权限集合一方面不仅仅是防止了第一权限集合的“误报”，另一方面还加强了对执行主体的权限划分，以使得执行

主体能够不被第一权限集合的“误报”影响其正常功能，又能限制其进行其他具有安全威胁的特定操作。以 Xshell 为例，其多被用来远程管理服务器，但在其多个版本中存在后门，使用时会偷偷上传用户服务器账户与密码。Xshell 在由本公开第一权限集合判定时，由于第一权限集合规定了“应用程序不允许访问内外网络及网内设备节点”，故其不符合第一权限集合的判定。对于本公开的第二权限集合，其可以根据应用程序类型确定不同的网络连接权限，以使得不同应用程序能够精确地连接某一类或某一个或多个网络。例如，打印机、摄像头等只可以连接固定的 IP 地址；内网通信用应用程序只可以连接内网；xshell 类的服务器管理工具只可以连接用户本次操作所连接的网络；应用程序只可以使用特定的网络协议连接网络等。再以 Xshell 为例，其在各种操作状态下的第二权限集合为：

- 在用户主动执行、且具备交互窗口的双状态下，拥有与指定网络地址（主动连接的服务器 IP 或域名）进行网络通信的权限
- 非用户主动执行、或无窗口都不可进行网络通信
- 不可与本次用户操作所指向管理的服务器地址无关的网络地址通信

基于上述第二权限集合判定 Xshell 时，其不允许 Xshell 访问用户本次操作所连接的网络之外的其他网络，切断了其上传用户服务器账户与密码的网络通路，避免了安全威胁。

通过上述例子可以看出，根据第一权限集合的判定对其进行了“拦截”后，再由第二权限集合对其判定，对于远程管理服务器等正常功能进行“放行”，对于非法连接其他网络进行“拦截”，实现了更精准的权限控制。

当执行主体在对应操作状态下不满足所规定的第二权限集合，则可以充分认定该执行主体或其对应的特定操作具有安全威胁，即对该执行主体进行拦截，以中断其即将执行的特定操作。

但是，当执行主体在对应操作状态下满足所规定的第二权限集合（其已经操作 S102 中判定该执行主体不满足第一权限集合）时，即可

认定通过第一权限集合进行判定的结果存在“误报”的可能，需要在后续进行进一步的判定。

S105，获取包括特定操作的任务，该任务对应有执行至少一个操作的操作流程。

- 5 在操作系统中“任务”是实现对应功能的最小单元，每个任务包括有一个或多个按顺序执行的操作（包括特定操作），以固定的顺序执行这些操作以完成任务即是该任务的操作流程。

10 在操作 S105 中，获取的任务可以具体包括：任务所包含的一个或多个操作，一个或多个操作的执行顺序、每个操作的执行客体（例如，通过 winword 程序打开 word 文档，word 文档即为执行客体）。通过上述的信息即可判定任务的操作流程是否合法。

S106，判断操作流程是否满足预设操作流程，若是，则执行操作 S7，若否，则对执行主体进行处理。

15 本公开判定任务的操作流程是否合法是通过判定其是否符合预设操作流程，每个任务为了实现对应的功能都应具备一套合法的操作流程，即为本公开所提及的预设操作流程。下面以“远程启动 Shell 程序 cmd.exe”为例，来解释本公开的合法操作流程及非法操作流程。

20 图 2 绘示出本公开实施例中“远程启动 Shell 程序 cmd.exe”的合法操作流程。如图 2 所示，在正常远控机 A 产生一任务为“启动目标服务器 B 上的 Shell 程序 cmd.exe”，该任务执行的操作流程为：

S201，在正常远控机 A 上启动 Telnet.exe 程序；

S202，在正常远控机上 A，通过 Telnet.exe 程序发送与目标服务器 B 建立远程连接的请求；

25 S203，在目标服务器 B 上通过 tlntsvr.exe 接收正常远控机 A 发送的远程连接的请求；

S204，在目标服务器 B 上，通过 tlntsvr.exe 启动 tlntsess.exe，以建立与正常远控机 A 的连接；

S205，在正常远控机 A 上发送启动 Shell 程序 cmd.exe 的指令；

S206，在目标服务器 B 上通过 tlntsess.exe 接收到上述指令；

S207,在目标服务器 B 上通过 tlntsess.exe 启动 Shell 程序 cmd.exe。

图 3 绘示出本公开实施例中“远程启动 Shell 程序 cmd.exe”的非法操作流程图。如图 3 所示,在黑客远控机 A 产生一任务为“启动目标服务器 B 上的 Shell 程序 cmd.exe”,该任务执行的操作流程为:

5 S301,在黑客远控机 A 上,通过 ms17-010 漏洞(此漏洞为勒索者病毒 Wannacry 实际使用的漏洞)向目标服务器 B 发送数据包(该数据包为特殊构建的、包含有勒索者病毒的攻击代码);

S302,在目标服务器 B 上,由于 ms17-010 漏洞存在,执行数据包中的勒索者病毒的攻击代码;

10 S303,在目标服务器 B 上,勒索者病毒的攻击代码,将启动 shell 的指令注入到 spoolsv.exe 中;

S304,在目标服务器 B 上,通过 spoolsv.exe 启动 Shell 程序 cmd.exe。

从本公开的图 2~图 3 可以看出,两个同样地任务,实现的功能均是启动 Shell 程序 cmd.exe,但是其执行的操作流程不一样。

15 但合法操作流程是:“系统专用的远程管理服务程序:tlntsvr.exe、tlntsess.exe”共同完成了任务的执行,tlntsvr.exe 接受连接进行身份认证,然后启动 tlntsess.exe 来接受用户的命令,最终启动 cmd.exe。

而非法操作流程是:通过“打印机管理服务程序:spoolsv.exe”启动 cmd.exe。

20 显然地,本公开操作 S106 中,通过判定任务的操作流程是否合法是通过判定其是否符合预设操作流程,能够判定特定操作所属的任务是否合法。具体地,本公开在判定操作流程时,首先获取操作流程所对应的操作,然后需要判定每个操作是否与预设操作流程中所对应的操作一致。

25 以图 2~图 3 为例,非法操作流程中有“启动 spoolsv.exe”、“spoolsv.exe 启动 Shell 程序 cmd.exe”;其对应的合法操作流程为“tlntsvr.exe 启动 tlntsess.exe”、“tlntsess.exe 启动 Shell 程序 cmd.exe”。虽然两者都有“启动 Shell 程序 cmd.exe”这个操作,但缺少“tlntsvr.exe 启动 tlntsess.exe”环节,而且“spoolsv.exe 启动 cmd.exe”也与预设任务流程中的 tlntsess.exe

启动 Shell 程序 `cmd.exe` 不一致, 因此图 3 所示的任务操作流程不符合预设操作流程, 进而不合法。

另外, 假如恶意攻击代码不是选择注入 `spoolsv.exe` 而是启动并注入到 `tlntsess.exe` 中, 再执行启动 shell 程序 `cmd.exe` 的操作, 是否就能判定此操作合法呢? 仍然不能, 因为 `tlntsess.exe` 在预设的合法流程中, 必须由 `tlntsvr.exe` 启动才是合法的, 而不是任何其它的服务或程序。

因此, 本公开在操作 S106 中, 还需要判断每个操作的执行主体是否与预设操作流程所对应操作的执行主体一致, 如果不一致, 则认为整个操作流程不合法。

10 为了更加准确地判定操作流程是否合法, 还可以增加“判定每个操作的执行客体是否”合法的步骤, 其原理与“判断每个操作的执行主体是否与预设操作流程所对应操作的执行主体一致”一样, 在此就不再赘述。

通过本公开的操作 S106, 可以将“未通过第一权限集合的判定”, 但又“通过了第二权限集合的判断”的执行主体及特定操作进行准确甄别, 以确定其是“误报”还是“确实存在安全威胁”。因此, 在判定出操作流程不满足预设操作流程时, 可充分认定该执行主体或其对应的特定操作具有安全威胁, 即对该执行主体进行拦截, 以中断其即将执行的特定操作; 在判定出操作流程满足预设操作流程时, 可充分认定在操作 S102 中存在“误报”现象, 对该执行主体及对应的特定操作进行“放行”, 20 以使该执行主体执行该特定操作。

然而基于图 2 及图 3 的示例, 如果黑客远程攻击完成后, 先控制 `tlntsvr.exe`, 再通过 `tlntsvr.exe` 调用 `tlntsess.exe`, 然后再控制 `tlntsess.exe` 来启动 Shell, 进而绕过了上述操作 S106 的操作流程判定。因此, 本公开进一步引入操作 S107~S108。

S107, 获取任务中至少一个操作所对应的指令执行序列。

本公开操作 S107 中的“任务”即本公开之前所提及的包括特定操作的任务。本公开从该任务中获取至少一个操作 (该操作可以是特定操作, 也可以是任务中的其他操作), 并获取执行该操作所对应的指令执

行序列。具体地，本公开指令执行序列是从操作系统中的栈内存（栈内存由操作系统自动申请分配、使用以及回收，用户无法控制）中获取的。

S108，判断指令执行序列与预设指令执行序列是否匹配，若否，则对执行主体进行处理。

- 5 本公开操作 S108 中的预设指令执行序列是指合法的指令执行序列。将从栈内存中获取的指令执行序列与预设指令执行序列进行匹配，以确定从栈内存中获取的指令执行序列是否合法，进而判定其对应的操作是否合法。具体地，在匹配过程中，本公开的一种实施方式为，获取指令执行序列中的函数调用信息，函数调用信息包括函数调用次数（若某一函数被调用 0 次时，表示该函数未被调用）和/或函数调用顺序，判断指令执行序列中的函数调用信息与预设指令执行序列中的函数调用信息是否匹配。如果匹配成功，则对执行主体进行的特定操作进行放行，否则，对执行主体进行的特定操作进行拦截。

- 15 表 1 示意性示出了本公开实施例中“远程启动 Shell 程序 cmd.exe”合法的指令执行序列：

tlntsvr.exe 启动 tlntsess.exe 时的指令执行序列 1	tlntsess.exe 启动 cmd.exe 时的指令执行序列 2
ntdll!RtlUserThreadStart	ntdll!RtlUserThreadStart
kernel32!BaseThreadInitThunk	kernel32!BaseThreadInitThunk
sechost!ScSvcctrlThreadA	tlntsess!LsaFreeMemory
tlntsvr!CServiceModule::_ServiceMain	tlntsess!main
tlntsvr!CServiceModule::Run	tlntsess!CSession::WaitForIo
tlntsvr!TelnetServiceThread	tlntsess!CioHandler::OnDataFromSocket
tlntsvr!CTelnetService::ListenerThread	tlntsess!CioHandler::ProcessDataFromSocket
tlntsvr!CTelnetService::CreateClient	tlntsess!CShell::StartUserSession
tlntsvr!CTelnetService::CreateSessionProcess	tlntsess!CShell::StartProcess
kernel32!CreateProcessW	ADVAPI32!CreateProcessAsUserWStub
kernel32!CreateProcessInternalW	kernel32!CreateProcessAsUserW
ntdll!ZwCreateUserProcess	

nt!KiSystemServiceCopyEnd
nt!NtCreateUserProcess

表 1

需要说明的是，指令执行序列存储在栈内存中时的顺序与其执行的顺序相反，为了方便说明，表 1 即按执行顺序从上至下来描述，下面针对表 1 中的指令执行序列 1 和指令执行序列 2，对其中一些关键性的指令进行说明，如表 2 所示：

5 指令进行说明，如表 2 所示：

指令执行序列 1	tlntsvr!CServiceModule::_ServiceMain	tlntsvr.exe 服务本身启动并执行自己的服务主函数
	tlntsvr!CTelnetService::ListenerThread	创建监听线程等待来自用户的远程连接
	tlntsvr!CTelnetService::CreateSessionProcess	用户连接成功后，tlntsvr 服务为此用户创建 tlntsess.exe 进程
指令执行序列 2	tlntsess!main	进程成功启动，并执行主函数
	tlntsess!CSession::WaitForIo	在等待接收来自用户的任务指令
	tlntsess!CShell::StartProcess	接收到启动 Shell 的指令后开始启动 Shell

表 2

通过表 1 和表 2 可以看出，当（合法的）操作执行时，其指令执行序列是脉络清晰的。每次调用都是来自 tlntsvr 及 tlntsess 本身或系统 API 调用，从调用栈的各层指令执行序列中，可以清晰的看到每个服务或程序中的各个关键环节、关键任务的启动、上下间的关系衔接、及流程进行的脉络。

然而，对于同样是完成任务“远程启动 Shell 程序 cmd.exe”，黑客通过漏洞攻击，远程获取服务器的系统控制权后，通过 tlntsvr.exe 调用 tlntsess.exe，然后再控制 tlntsess.exe 来启动 Shell 程序 cmd.exe，如表 3 所示，表 3 示意性示出了本公开实施例中“远程启动 Shell 程序 cmd.exe”非法的指令执行序列：

tlntsvr.exe 启动 tlntsess.exe 时的指令执行序列 3	tlntsess.exe 启动 cmd.exe 时的指令执行序列 4
ntdll!RtlInitializeExceptionChain	ntdll!RtlInitializeExceptionChain
ntdll!RtlInitializeExceptionChain	ntdll!RtlInitializeExceptionChain
kernel32!BaseThreadInitThunk	kernel32!BaseThreadInitThunk
0x70ce1163	0x730711b0
kernel32!CreateProcessW	kernel32!CreateProcessW

表 3

通过对比表 1 和表 3 可以清楚的看到,表 1 所示出的“远程启动 Shell 程序 cmd.exe” 需要进行“tlntsvr.exe 启动 tlntsess.exe”、“tlntsess.exe 启动 cmd.exe”两个操作。而表 3 所示出的“远程启动 Shell 程序 cmd.exe”,

5 恶意攻击者为了模拟正常的任务流程完成任务“远程启动 Shell 程序 cmd.exe”, 同样需要进行“tlntsvr.exe 启动 tlntsess.exe”、“tlntsess.exe 启动 cmd.exe”两个操作, 其在操作流程上是一致的。但通过分析栈内存中的指令执行序列, 两者完全不一样, 甚至没有任何相同之处。又从表 3 可以看出, 非法的指令执行序列直接是一个单独的线程启动, 然后从

10 一个非系统代码的空间地址中启动了对应的程序, 从中完全无法看出正常操作发生时应该有的指令及调用序列, 其中的非法与异常清晰可辨。

再参见表 1 所示的合法的指令执行序列 1 中, 其中一条指令为“kernel32!CreateProcessW”, 其代表的含义是: “在“kernel32.dll”这个动态链接库中的函数“CreateProcessW”被调用了一次, 而调用这个函数

15 的作用是“启动某一指定的程序”。因此, 本公开在判断指令执行序列与预设指令执行序列是否匹配时, 可以通过各自序列中的函数调用信息来匹配, 包括不同作用的函数是否被调用过、调用的次数及调用的顺序等。

通过本公开实施例的操作 S107~S108 可以看出, 任务的操作流程通

20 过了 S106 的判定后, 还进一步地对任务的指令执行序列进行合法性判定, 在指令执行序列通过判定时, 即认为最初的 S101 中的执行主体及其特定操作合法, 进而对其放行; 否则, 对执行主体及其特定操作进行

拦截。因此，S107~S108 进一步保证了操作的安全性。图 4 示意性示出了根据本公开实施例的操作检测系统的框图。

如图 4 所示，操作检测系统 400 包括第一获取模块 410、第一判断模块 420、第二获取模块 430、第二判断模块 440、第三获取模块 450、第三判断模块 460、第四获取模块 470 及第四判断模块 480。该操作检测系统 400 可以执行上面参考图 1 描述的方法，以实现对特定操作的检测。

具体地，第一获取模块 410 用于在执行特定操作之前，获取执行特定操作的执行主体；第一判断模块 420 用于根据第一权限集合判断所述执行主体是否具有执行该特定操作的权限，若否，则执行第二获取模块 430；第二获取模块 430 用于获取执行主体的操作状态，并根据该执行主体的操作状态获取对应的第二权限集合；第二判断模块 440 用于根据第二权限集合判断执行主体是否具有执行该特定操作的权限，若是，则执行第三获取模块 450，若否，则对所述执行主体进行处理；第三获取模块 450 用于获取包括特定操作的任务，该任务对应有执行至少一个操作的操作流程；第三判断模块用于判断所述操作流程是否满足预设操作流程，若是，则执行第四获取模块，若否，则对所述执行主体进行处理；第四获取模块用于获取任务中至少一个操作所对应的指令执行序列；第四判断模块，用于判断指令执行序列与预设指令执行序列是否匹配，若否，则对执行主体进行处理。

可以理解的是，第一获取模块 410、第一判断模块 420、第二获取模块 430、第二判断模块 440、第三获取模块 450、第三判断模块 460、第四获取模块 470 及第四判断模块 480 可以合并在一个模块中实现，或者其中的任意一个模块可以被拆分成多个模块。或者，这些模块中的一个或多个模块的至少部分功能可以与其他模块的至少部分功能相结合，并在一个模块中实现。根据本发明的实施例，第一获取模块 410、第一判断模块 420、第二获取模块 430、第二判断模块 440、第三获取模块 450、第三判断模块 460、第四获取模块 470 及第四判断模块 480 中的至少一个可以至少被部分地实现为硬件电路，例如现场可编程门阵列

(FPGA)、可编程逻辑阵列 (PLA)、片上系统、基板上的系统、封装上的系统、专用集成电路 (ASIC)，或可以以对电路进行集成或封装的任何其他的合理方式等硬件或固件来实现，或以软件、硬件以及固件三种实现方式的适当组合来实现。或者，第一获取模块 410、第一判断模块 420、第二获取模块 430、第二判断模块 440、第三获取模块 450、第三判断模块 460、第四获取模块 470 及第四判断模块 480 中的至少一个可以至少被部分地实现为计算机程序模块，当该程序被计算机运行时，可以执行相应模块的功能。

图 5 示意性示出了根据本公开另一实施例的电子设备的框图。

如图 5 所示，电子设备 500 包括处理器 510、计算机可读存储介质 520。该电子设备 500 可以执行上面参考图 1 描述的方法，以实现对待检测操作的检测。

具体地，处理器 510 例如可以包括通用微处理器、指令集处理器和/或相关芯片组和/或专用微处理器（例如，专用集成电路 (ASIC)），等等。处理器 510 还可以包括用于缓存用途的板载存储器。处理器 510 可以是用于执行参考图 1 描述的根据本公开实施例的方法流程的不同动作的单一处理单元或者是多个处理单元。

计算机可读存储介质 520，例如可以是能够包含、存储、传送、传播或传输指令的任意介质。例如，可读存储介质可以包括但不限于电、磁、光、电磁、红外或半导体系统、装置、器件或传播介质。可读存储介质的具体示例包括：磁存储装置，如磁带或硬盘 (HDD)；光存储装置，如光盘 (CD-ROM)；存储器，如随机存取存储器 (RAM) 或闪存；和/或有线/无线通信链路。

计算机可读存储介质 520 可以包括计算机程序 521，该计算机程序 521 可以包括代码/计算机可执行指令，其在由处理器 510 执行时使得处理器 510 执行例如上面结合图 1 所描述的方法流程及其任何变形。

计算机程序 521 可被配置为具有例如包括计算机程序模块的计算机程序代码。例如，在示例实施例中，计算机程序 521 中的代码可以包括一个或多个程序模块，例如包括 521A、模块 521B、……。应当注意，

模块的划分方式和个数并不是固定的，本领域技术人员可以根据实际情况使用合适的程序模块或程序模块组合，当这些程序模块组合被处理器 510 执行时，使得处理器 510 可以执行例如上面结合图 2~图 3D 所描述的方法流程及其任何变形。

- 5 根据本发明的实施例，第一获取模块 410、第一判断模块 420、第二获取模块 430、第二判断模块 440、第三获取模块 450 及第三判断模块 460 中的至少一个可以实现为参考图 5 描述的计算机程序模块，其在被处理器 510 执行时，可以实现上面描述的相应操作。

- 10 本领域技术人员可以理解，本公开的各个实施例和/或权利要求中记载的特征可以进行多种组合或/或结合，即使这样的组合或结合没有明确记载于本公开中。特别地，在不脱离本公开精神和教导的情况下，本公开的各个实施例和/或权利要求中记载的特征可以进行多种组合和/或结合。所有这些组合和/或结合均落入本公开的范围。

- 15 尽管已经参照本公开的特定示例性实施例示出并描述了本公开，但是本领域技术人员应该理解，在不背离所附权利要求及其等同物限定的本公开的精神和范围的情况下，可以对本公开进行形式和细节上的多种改变。因此，本公开的范围不应该限于上述实施例，而是应该不仅由所附权利要求来进行确定，还由所附权利要求的等同物来进行限定。

权利要求

1、一种操作检测方法，包括：

S1，在执行特定操作之前，获取执行该特定操作的执行主体；

5 S2，根据第一权限集合判断所述执行主体是否具有执行该特定操作的权限，若否，则执行操作 S3；

S3，获取所述执行主体的操作状态，并根据该执行主体的操作状态获取对应的第二权限集合；

S4，根据第二权限集合判断所述执行主体是否具有执行该特定操作的权限，若是，则执行操作 S5，若否，则对所述执行主体进行处理；

10 S5，获取包括所述特定操作的任务，该任务对应有执行至少一个操作的操作流程；

S6，判断所述操作流程是否满足预设操作流程，若是，则执行操作 S7；若否，则对所述执行主体进行处理；

S7，获取所述任务中至少一个操作所对应的指令执行序列；

15 S8，判断所述指令执行序列与预设指令执行序列是否匹配，若否，则对所述执行主体进行处理。

2、根据权利要求 1 所述的操作检测方法，其中，所述步骤 S6 中，判断所述操作流程是否满足预设操作流程，包括：

获取所述操作流程所对应的至少一个操作；

20 判断所述至少一个操作中每个操作是否与所述预设操作流程中所对应的操作一致。

3、根据权利要求 2 所述的操作检测方法，其中，所述判断所述至少一个操作中每个操作是否与所述预设操作流程中所对应操作一致，包括：

25 判断所述至少一个操作中每个操作的执行主体是否与预设操作流程所对应操作的执行主体一致。

4、根据权利要求 1-3 任意一项所述的操作检测方法，其中，在所述步骤 S1 之前，还包括：

S0, 创建第一权限集合, 所述第一权限集合包括至少一个执行主体在任意操作状态下的操作权限。

5、根据权利要求 1-4 任意一项所述的操作检测方法, 其中, 在所述步骤 S1 之前, 还包括:

5 S0', 创建至少一个第二权限集合, 其中, 每个所述第二权限集合对应一个执行主体的一个操作状态, 并且, 每个所述第二权限集合包括对应执行主体在对应操作状态下的操作权限。

6、根据权利要求 5 所述的操作检测方法, 其中, 所述至少一个第二权限集合存储在远端, 所述步骤 S3 中, 根据该执行主体的操作状态
10 获取对应的第二权限集合, 包括:

向远端发送请求, 所述请求包括所述执行主体信息及其操作状态;
获取远端发送的第二权限集合, 其中, 该第二权限集合是由所述远端响应所述请求而返回。

7、根据权利要求 1-6 任意一项所述的操作检测方法, 其中, 所述步骤 S3 中, 获取所述执行主体的操作状态, 至少包括:

根据所述执行主体的调用方式确定所述执行主体的操作状态, 其中, 所述执行主体是由用户直接调用时, 确定所述执行主体的操作状态为第一操作状态, 当所述执行主体是由其他执行主体调用时, 确定所述执行主体的操作状态为第二操作状态。

8、根据权利要求 1 所述的操作检测方法, 其中, 所述步骤 S8 中, 判断所述指令执行序列与预设指令执行序列是否匹配, 包括:

获取所述指令执行序列中的函数调用信息, 所述函数调用信息包括函数调用次数和/或函数调用顺序;

判断所述指令执行序列中的函数调用信息与预设指令执行序列中的函数调用信息是否匹配。
25

9、根据权利要求 1-7 任意一项所述的操作检测方法, 其中, 所述步骤 S7 中, 获取所述任务中至少一个操作所对应的指令执行序列, 包括:

从栈内存中获取所述任务中至少一个操作所对应的指令执行序列。

10、一种操作检测系统, 包括:

第一获取模块，用于在执行特定操作之前，获取执行特定操作的执行主体；

第一判断模块，用于根据第一权限集合判断所述执行主体是否具有执行该特定操作的权限，若否，则执行第二获取模块；

5 第二获取模块，用于获取所述执行主体的操作状态，并根据该执行主体的操作状态获取对应的第二权限集合；

第二判断模块，用于根据第二权限集合判断所述执行主体是否具有执行该特定操作的权限，若是，则执行第三获取模块，若否，则对所述执行主体进行处理；

10 第三获取模块，用于获取包括所述特定操作的任务，该任务对应有执行至少一个操作的操作流程；

第三判断模块，用于判断所述操作流程是否满足预设操作流程，若是，则执行第四获取模块，若否，则对所述执行主体进行处理；

15 第四获取模块，用于获取所述任务中至少一个操作所对应的指令执行序列；

第四判断模块，用于判断所述指令执行序列与预设指令执行序列是否匹配，若否，则对所述执行主体进行处理。

11、根据权利要求 10 所述的操作检测系统，其中，所述第三判断模块中，判断所述操作流程是否满足预设操作流程，包括：

20 获取所述操作流程所对应的至少一个操作；

判断所述至少一个操作中每个操作是否与所述预设操作流程中所对应的操作一致。

12、根据权利要求 11 所述的操作检测系统，其中，所述第三判断模块判断所述至少一个操作中每个操作是否与所述预设操作流程中所对应操作一致，包括：

25 判断所述至少一个操作中每个操作的执行主体是否与预设操作流程所对应操作的执行主体一致。

13、根据权利要求 10-12 任意一项所述的操作检测系统，还包括：

第一创建模块，用于创建第一权限集合，所述第一权限集合包括至

少一个执行主体在任意操作状态下的操作权限。

14、根据权利要求 9-13 任意一项所述的操作检测系统，还包括：

第二创建模块，用于创建至少一个第二权限集合，其中，每个所述第二权限集合对应一个执行主体的一个操作状态，并且，每个所述第二权限集合包括对应执行主体在对应操作状态下的操作权限。

15、根据权利要求 14 所述的操作检测系统，其中，所述至少一个第二权限集合存储在远端，所述第二获取模块根据该执行主体的操作状态获取对应的第二权限集合，包括：

向远端发送请求，所述请求包括所述执行主体信息及其操作状态；
获取远端发送的第二权限集合，其中，该第二权限集合是由所述远端响应所述请求而返回。

16、根据权利要求 10-15 任意一项所述的操作检测系统，其中，所述第二获取模块获取所述执行主体的操作状态，至少包括：

根据所述执行主体的调用方式确定所述执行主体的操作状态，其中，所述执行主体是由用户直接调用时，确定所述执行主体的操作状态为第一操作状态，当所述执行主体是由其他执行主体调用时，确定所述执行主体的操作状态为第二操作状态。

17、根据权利要求 10 所述的操作检测系统，其中，所述第四判断模块判断所述指令执行序列与预设指令执行序列是否匹配，包括：

获取所述指令执行序列中的函数调用信息，所述函数调用信息包括函数调用次数和/或函数调用顺序；

判断所述指令执行序列中的函数调用信息与预设指令执行序列中的函数调用信息是否匹配。

18、根据权利要求 10-17 任意一项所述的操作检测系统，其中，所述第四获取模块获取所述任务中至少一个操作所对应的指令执行序列，包括：

从栈内存中获取所述任务中至少一个操作所对应的指令执行序列。

19、一种电子设备，包括：

处理器：

存储器，存储有计算机可执行指令，该计算机可执行指令在被所述处理器执行时，使得所述处理器执行：

S1，在执行特定操作之前，获取执行该特定操作的执行主体；

S2，根据第一权限集合判断所述执行主体是否具有执行该特定操作的权限，若否，则执行操作 S3；

S3，获取所述执行主体的操作状态，并根据该执行主体的操作状态获取对应的第二权限集合；

S4，根据第二权限集合判断所述执行主体是否具有执行该特定操作的权限，若是，则执行操作 S5，若否，则对所述执行主体进行处理；

S5，获取包括所述特定操作的任务，该任务对应有执行至少一个操作的操作流程；

S6，判断所述操作流程是否满足预设操作流程，若是，则执行操作 S7；若否，则对所述执行主体进行处理；

S7，获取所述任务中至少一个操作所对应的指令执行序列；

S8，判断所述指令执行序列与预设指令执行序列是否匹配，若否，则对所述执行主体进行处理。

20、根据权利要求 19 所述的电子设备，其中，所述处理器在执行步骤 S6 时，判断所述操作流程是否满足预设操作流程，包括：

获取所述操作流程所对应的至少一个操作；

判断所述至少一个操作中每个操作是否与所述预设操作流程中所对应的操作一致。

21、根据权利要求 20 所述的电子设备，其中，所述处理器判断所述至少一个操作中每个操作是否与所述预设操作流程中所对应操作一致，包括：

判断所述至少一个操作中每个操作的执行主体是否与预设操作流程所对应操作的执行主体一致。

22、根据权利要求 19-21 任意一项所述的电子设备，其中，所述处理器在执行所述步骤 S1 之前，还执行：

S0，创建第一权限集合，所述第一权限集合包括至少一个执行主体

在任意操作状态下的操作权限。

23、根据权利要求 19-22 任意一项所述的电子设备，其中，所述处理器在执行所述步骤 S1 之前，还执行：

5 S0'，创建至少一个第二权限集合，其中，每个所述第二权限集合对应一个执行主体的一个操作状态，并且，每个所述第二权限集合包括对应执行主体在对应操作状态下的操作权限。

24、根据权利要求 23 所述的电子设备，其中，所述至少一个第二权限集合存储在远端，所述处理器在执行所述步骤 S3 时，根据该执行主体的操作状态获取对应的第二权限集合，包括：

10 向远端发送请求，所述请求包括所述执行主体信息及其操作状态；
获取远端发送的第二权限集合，其中，该第二权限集合是由所述远端响应所述请求而返回。

25、根据权利要求 19-24 任意一项所述的电子设备，其中，所述处理器在执行所述步骤 S3 时，获取所述执行主体的操作状态，至少包括：

15 根据所述执行主体的调用方式确定所述执行主体的操作状态，其中，所述执行主体是由用户直接调用时，确定所述执行主体的操作状态为第一操作状态，当所述执行主体是由其他执行主体调用时，确定所述执行主体的操作状态为第二操作状态。

20 26、根据权利要求 19 所述的电子设备，其中，所述处理器在执行步骤 S8 时，判断所述指令执行序列与预设指令执行序列是否匹配，包括：

获取所述指令执行序列中的函数调用信息，所述函数调用信息包括函数调用次数和/或函数调用顺序；

25 判断所述指令执行序列中的函数调用信息与预设指令执行序列中的函数调用信息是否匹配。

27、根据权利要求 19-26 任意一项所述的电子设备，其中，所述处理器在执行步骤 S7 时，获取所述任务中至少一个操作所对应的指令执行序列，包括：

从栈内存中获取所述任务中至少一个操作所对应的指令执行序列。

28、一种计算机可读介质，存储有计算机可执行指令，所述指令在被执行时用于实现如权利要求 1-9 任意一项所述的方法。

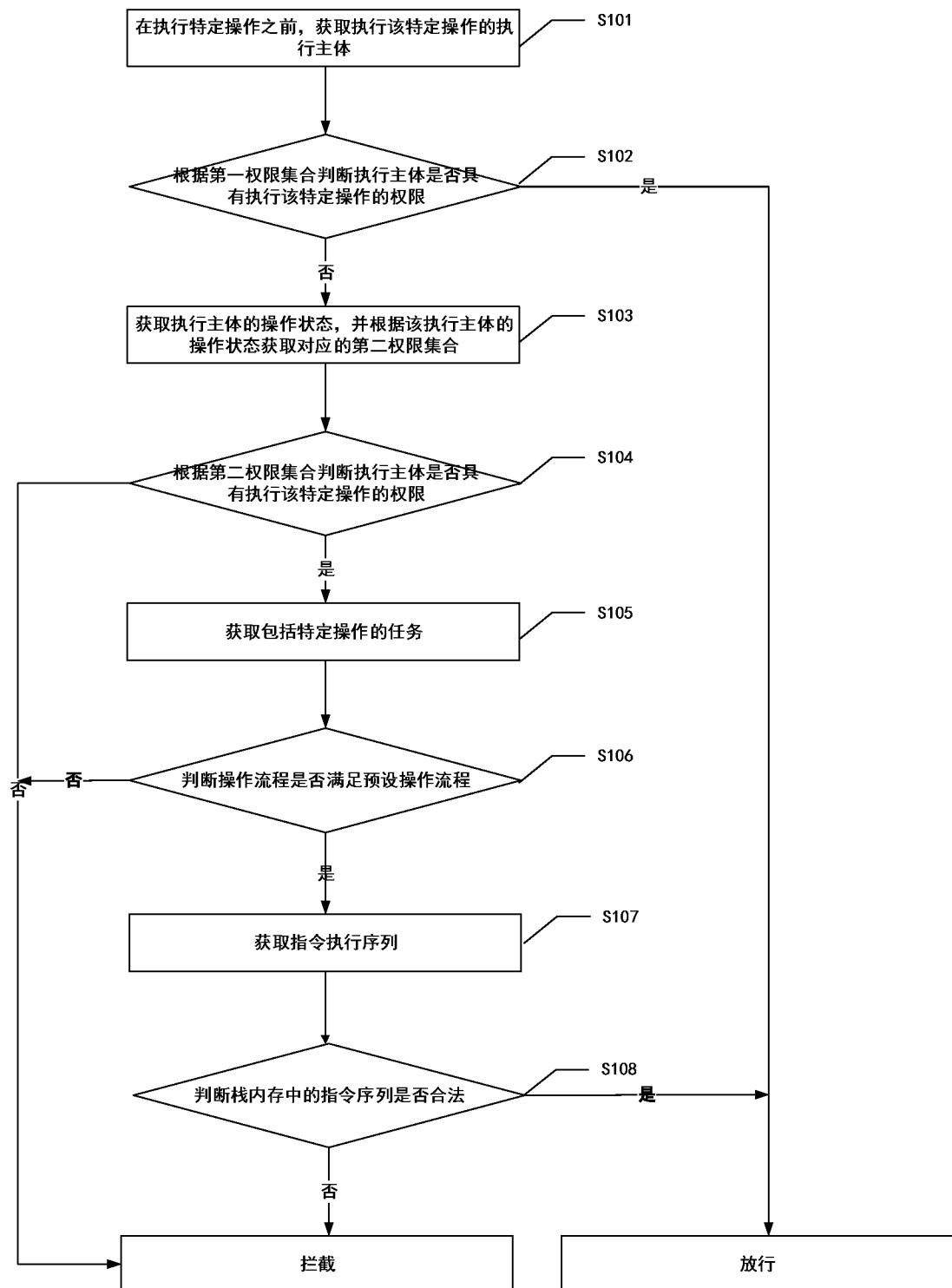


图 1

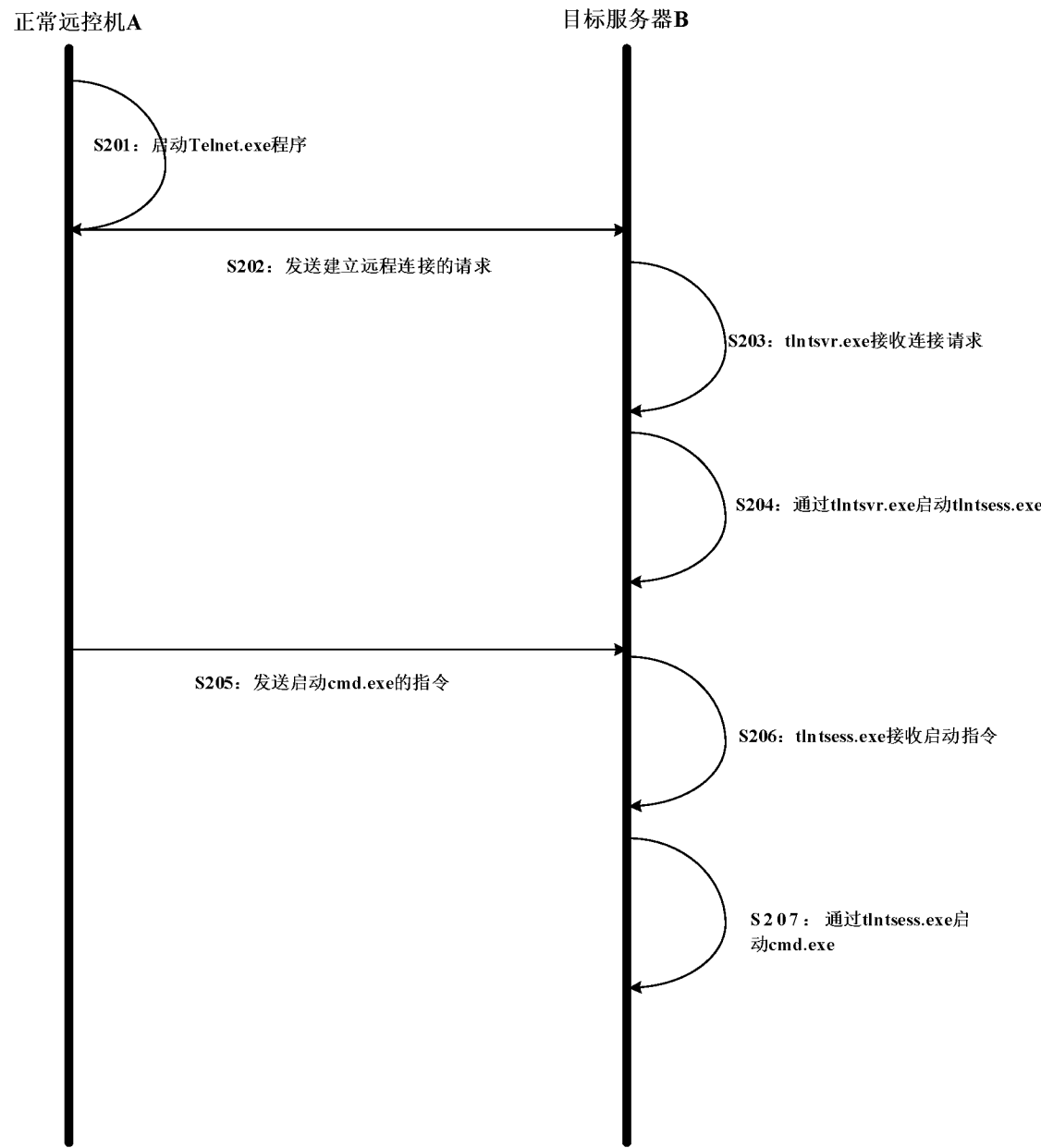


图 2

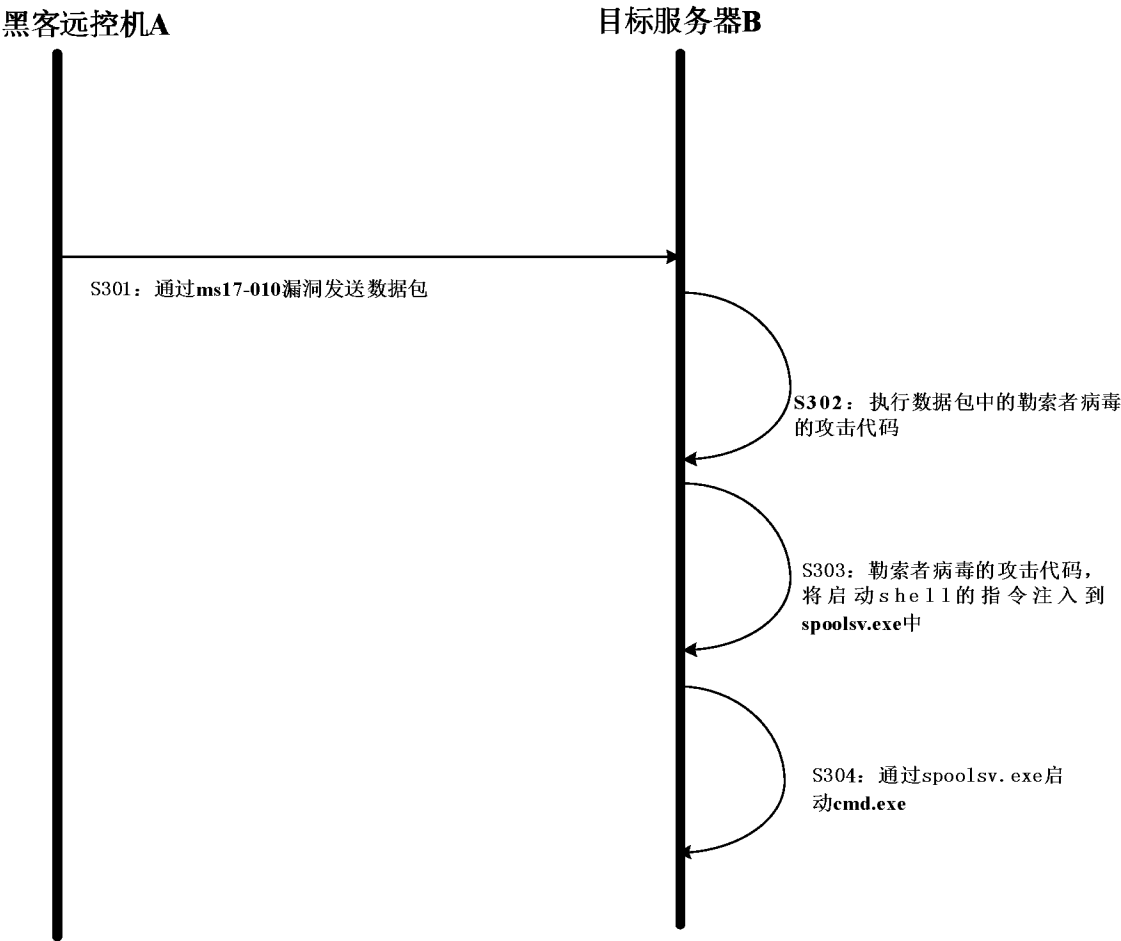


图 3

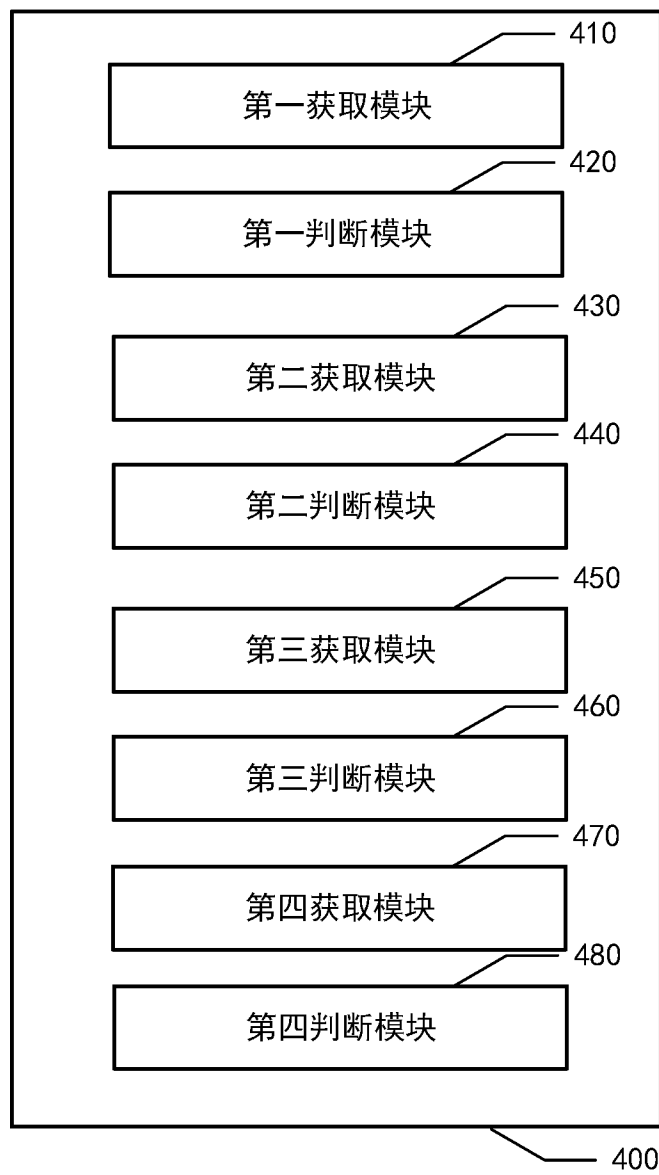


图 4

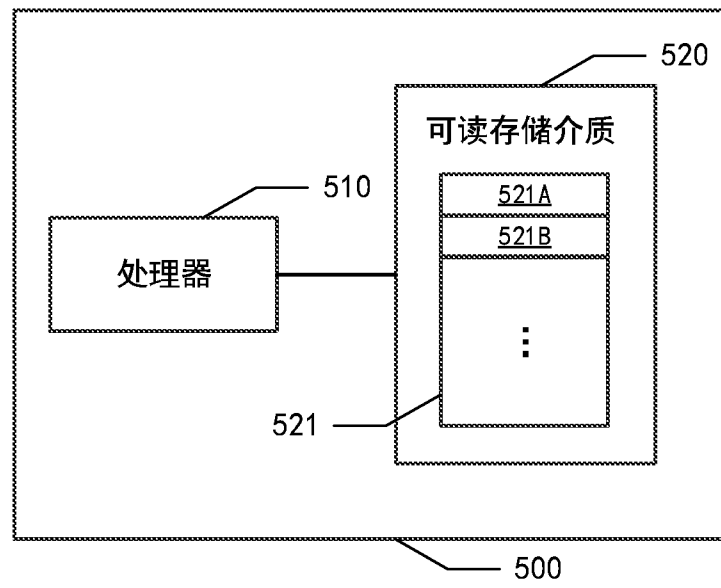


图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/123534

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/33(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

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)

WPI; EPODOC; CNPAT; CNKI; IEEE: 操作, 检测, 权限, 执行, 主体, 状态, 获取, 程序, 判断, operate, detect, purview, estate, obtain, program, judgement

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 104166818 A (BAIDU ONLINE NETWORK TECHNOLOGY (BEIJING) CO., LTD.) 26 November 2014 (2014-11-26) description, paragraphs [0033]-[0196]	1-28
A	CN 103067911 A (CHINA UNITED NETWORK COMMUNICATIONS GROUP CO., LTD.) 24 April 2013 (2013-04-24) entire document	1-28
A	CN 107944258 A (GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CO., LTD.) 20 April 2018 (2018-04-20) entire document	1-28
A	US 2016098570 A1 (HUAWEI DEVICE CO., LTD.) 07 April 2016 (2016-04-07) entire document	1-28



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

20 August 2019

Date of mailing of the international search report

24 September 2019

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

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2018/123534

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	104166818	A	26 November 2014	None			
CN	103067911	A	24 April 2013	None			
CN	107944258	A	20 April 2018	None			
US	2016098570	A1	07 April 2016	EP	2993603	A1	09 March 2016
				CN	104424423	A	18 March 2015
				WO	2015027846	A1	05 March 2015

国际检索报告

国际申请号

PCT/CN2018/123534

A. 主题的分类 G06F 21/33 (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) G06F 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)) WPI; EPDOC; CNPAT; CNKI; IEEE: 操作, 检测, 权限, 执行, 主体, 状态, 获取, 程序, 判断, operate, detect, purview, estate, obtain, program, judgement																	
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>A</td> <td>CN 104166818 A (百度在线网络技术北京有限公司) 2014年 11月 26日 (2014 - 11 - 26) 说明书第[0033]-[0196]段</td> <td>1-28</td> </tr> <tr> <td>A</td> <td>CN 103067911 A (中国联合网络通信集团有限公司) 2013年 4月 24日 (2013 - 04 - 24) 全文</td> <td>1-28</td> </tr> <tr> <td>A</td> <td>CN 107944258 A (广东欧珀移动通信有限公司) 2018年 4月 20日 (2018 - 04 - 20) 全文</td> <td>1-28</td> </tr> <tr> <td>A</td> <td>US 2016098570 A1 (HUAWEI DEVICE CO., LTD.) 2016年 4月 7日 (2016 - 04 - 07) 全文</td> <td>1-28</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	A	CN 104166818 A (百度在线网络技术北京有限公司) 2014年 11月 26日 (2014 - 11 - 26) 说明书第[0033]-[0196]段	1-28	A	CN 103067911 A (中国联合网络通信集团有限公司) 2013年 4月 24日 (2013 - 04 - 24) 全文	1-28	A	CN 107944258 A (广东欧珀移动通信有限公司) 2018年 4月 20日 (2018 - 04 - 20) 全文	1-28	A	US 2016098570 A1 (HUAWEI DEVICE CO., LTD.) 2016年 4月 7日 (2016 - 04 - 07) 全文	1-28
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求															
A	CN 104166818 A (百度在线网络技术北京有限公司) 2014年 11月 26日 (2014 - 11 - 26) 说明书第[0033]-[0196]段	1-28															
A	CN 103067911 A (中国联合网络通信集团有限公司) 2013年 4月 24日 (2013 - 04 - 24) 全文	1-28															
A	CN 107944258 A (广东欧珀移动通信有限公司) 2018年 4月 20日 (2018 - 04 - 20) 全文	1-28															
A	US 2016098570 A1 (HUAWEI DEVICE CO., LTD.) 2016年 4月 7日 (2016 - 04 - 07) 全文	1-28															
☐ 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 2019年 8月 20日		国际检索报告邮寄日期 2019年 9月 24日															
ISA/CN的名称和邮寄地址 中国国家知识产权局 (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 李萌 电话号码 86-(10)-53961536															

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2018/123534

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	104166818	A	2014年 11月 26日	无			
CN	103067911	A	2013年 4月 24日	无			
CN	107944258	A	2018年 4月 20日	无			
US	2016098570	A1	2016年 4月 7日	EP	2993603	A1	2016年 3月 9日
				CN	104424423	A	2015年 3月 18日
				WO	2015027846	A1	2015年 3月 5日