(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
2022 年 5 月 19 日 (19.05.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/100660 A1

(51) 国际专利分类号:
G06F 21/52 (2013.01)

(21) 国际申请号: PCT/CN2021/130041

(22) 国际申请日: 2021 年 11 月 11 日 (11.11.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202011272230.5 2020年11月13日 (13.11.2020) CN

(71) 申请人: 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)。 奇安信安全技术（珠海）有限公司(QI AN XIN SAFETY TECHNOLOGY (ZHUHAI) LTD., CO) [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 519085 (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 519085 (CN)。

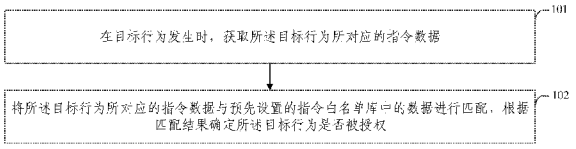
(74) 代理人: 北京路浩知识产权代理有限公司(CN-KNOWHOW INTELLECTUAL PROPERTY AGENT LIMITED); 中国北京市海淀区苏州街29号维亚大厦12层12130室, Beijing 100080 (CN)。

(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, IT, 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, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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,

(54) **Title:** BEHAVIOR CONTROL METHOD, APPARATUS, ELECTRONIC DEVICE, AND STORAGE MEDIUM

(54) **发明名称**: 行为控制方法、装置、电子设备及存储介质



101 When target behavior occurs, obtain instruction data corresponding to target behavior

102 Perform matching on instruction data corresponding to target behavior with data within preconfigured instruction white list library, and determine whether target behavior is authorized according to matching result

图 1

(57) **Abstract:** A behavior control method, an apparatus, an electronic device, and a storage medium. The method comprises: when a target behavior occurs, obtaining instruction data corresponding to the target behavior (101); performing matching on the instruction data corresponding to the target behavior with data within a preconfigured instruction white list library, and determining whether the target behavior is authorized according to a matching result (102); wherein the instruction white list library is used for storing instruction data corresponding to authorized behavior. By means of generating instruction data corresponding to a target behavior, performing matching of said data with data in an instruction white list library, and determining whether the target behavior is legitimate according to a matching result, the behavior control method, the apparatus, the electronic device, and the storage medium thereby implement behavior control at a code instruction level, which is more secure than an existing process-based behavior control method.

(57) **摘要**: 一种行为控制方法、装置、电子设备及存储介质；方法包括：在目标行为发生时，获取所述目标行为所对应的指令数据（101）；将所述目标行为所对应的指令数据与预先设置的指令白名单库中的数据进行匹配，根据匹配结果确定所述目标行为是否被授权（102）；其中，所述指令白名单库用于存储被授权行为所对应的指令数据。所述行为控制方法、装置、电子设备及存储介质通过生成目标行为所对应的指令数据，将其与指令白名单库中的数据进行匹配，根据匹配结果确定目标行为是否合法，从而在代码指令层次实现行为控制，较现有的基于进程的行为控制方法安全性更高。

WO 2022/100660 A1

[见续页]

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))。

行为控制方法、装置、电子设备及存储介质

相关申请的交叉引用

本申请要求于 2020 年 11 月 13 日提交的申请号为 202011272230.5，名称为“行为控制方法、装置、电子设备及存储介质”的中国专利申请的优先权，其通过引用方式全部并入本文。

技术领域

本申请涉及计算机技术领域，尤其涉及一种行为控制方法、装置、电子设备及存储介质。

背景技术

强制访问控制（Mandatory Access Control，MAC）是一种由计算机操作系统约束的访问控制，目标是限制“主体”对“客体”执行某种行为的能力。其中，“主体”可以是用户和/或进程，客体是指各类需要被保护的对象，如文件、目录、网络端口、内存、IO 设备等。

根据现有的 MAC 机制，进程是对“主体”进行权限约束的最小单元。可以想象，即使只允许某一特定的进程 A 才能对某一特定的被保护对象 B 进行操作，依据现有技术，也能够将一组“攻击”代码注入具有操作权限的特定进程 A 中，从而实现对被保护对象 B 的攻击。

因此，现有技术中基于 MAC 机制所实现的行为控制方法存在一定的安全隐患。

发明内容

针对现有技术中存在的问题，本申请实施例提供一种行为控制方法、装置、电子设备及存储介质。

本申请第一方面实施例提供一种行为控制方法，包括：

在目标行为发生时，获取所述目标行为所对应的指令数据；

将所述目标行为所对应的指令数据与预先设置的指令白名单库中的数据进行匹配，根据匹配结果确定所述目标行为是否被授权；其中，

所述指令白名单库用于存储被授权行为所对应的指令数据。

上述技术方案中，所述指令数据包括：指令执行序列；所述指令执行序列用于描述 API 调用序列中各层级的偏移地址及调用顺序；

相应地，所述将所述目标行为所对应的指令数据与预先设置的指令白名单库中的数据进行匹配，包括：

将所述目标行为的指令执行序列与指令白名单库中的指令执行序列进行匹配。

上述技术方案中，所述指令数据还包括：行为类型和/或 API 信息；

相应地，所述将所述目标行为所对应的指令数据与预先设置的指令白名单库中的数据进行匹配，还包括：

将所述目标行为的行为类型与所述指令白名单库中的行为类型进行匹配；

和/或，

将所述目标行为的API信息与所述指令白名单库中的API信息进行匹配。

上述技术方案中，所述指令数据还包括：程序名称以及程序版本号；

相应地，所述将所述目标行为所对应的指令数据与预先设置的指令白名单库中的数据进行匹配，还包括：

根据目标行为所属进程的信息确定目标行为所属程序的程序名称与版本号，根据所述程序名称与版本号确定指令白名单库。

上述技术方案中，所述将所述目标行为的第一指令执行序列与指令白名单库中的指令执行序列进行匹配，包括：

按照预先设定的匹配顺序，将所述目标行为的指令执行序列中各层的偏移地址与指令白名单库中的指令执行序列中各层的偏移地址按照层级依次进行匹配，直至已匹配的层级数量达到预先设置的匹配层数。

上述技术方案中，所述获取所述目标行为所对应的指令数据，包括：

获取所述目标行为所对应的线程的栈数据；

根据所述栈数据还原所述目标行为发生时的指令执行序列。

上述技术方案中，方法还包括：

对程序以及其所使用的动态库进行分析，确定所述程序中与被授权行

为相对应的指令数据;

根据被授权行为相对应的指令数据，生成指令白名单库。

上述技术方案中，所述确定所述程序中与被授权行为相对应的指令数据，包括:

确定与所述被授权行为相对应的第一 API;

确定用于调用所述第一 API 的指令执行序列;

根据所述用于调用所述第一 API 的指令执行序列，确定所述程序中与被授权行为相对应的指令执行序列;

根据所述程序中与被授权行为相对应的指令执行序列，确定所述程序中与被授权行为相对应的指令数据。

上述技术方案中，所述根据所述用于调用所述第一 API 的指令执行序列，确定所述程序中与被授权行为相对应的指令执行序列，包括:

将所述用于调用所述第一 API 的指令执行序列的全部作为程序中与被授权行为相对应的指令执行序列;

或，将所述用于调用所述第一 API 的指令执行序列的一部分作为程序中与被授权行为相对应的指令执行序列。

本申请第二方面实施例提供一种行为控制装置，包括:

指令数据获取模块，用于在目标行为发生时，获取所述目标行为所对应的指令数据;

匹配模块，用于将所述目标行为所对应的指令数据与预先设置的指令白名单库中的数据进行匹配，根据匹配结果确定所述目标行为是否被授权; 其中，

所述指令白名单库用于存储被授权行为所对应的指令数据。

本申请第三方面实施例提供一种电子设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现如本申请第一方面实施例所述行为控制方法的步骤。

本申请第四方面实施例提供一种非暂态计算机可读存储介质，其上存储有计算机程序，该计算机程序被处理器执行时实现如本申请第一方面实施例所述行为控制方法的步骤。

本申请第五方面实施例提供一种计算机程序产品，所述计算机程序产

品包括计算机可执行指令，所述指令在被执行时用于实现如本申请第一方面实施例所述行为控制方法的步骤。

本申请实施例提供的行为控制方法、装置、电子设备及存储介质通过生成目标行为所对应的指令数据，将其与指令白名单库中的数据进行匹配，根据匹配结果确定目标行为是否合法，从而在代码指令层次实现行为控制，较现有的基于进程的行为控制方法安全性更高。

附图说明

为了更清楚地说明本申请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一简单地介绍，显而易见地，下面描述中的附图是本申请的一些实施例，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。

图 1 为本申请实施例提供的行为控制方法的流程图；

图 2 为本申请实施例提供的行为控制装置的示意图；

图 3 为本申请实施例所涉及的电子设备的实体结构示意图。

具体实施方式

为使本申请实施例的目的、技术方案和优点更加清楚，下面将结合本申请实施例中的附图，对本申请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申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

为了便于理解本申请实施例提供的行为控制方法，下面结合一个具体的场景对现有技术中基于 MAC 机制所实现的行为控制方法进行说明。

假设有这样一个场景：在一个文本文件“a.txt”（扩展名为.txt 的纯文本文档）中存储了重要的信息；为了保护这些重要的信息，对该文件设定了访问权限，只允许作为系统文本编辑器的记事本程序（notepad.exe）可以打开这个文本文件。

所对应的规则为：只有 notepad.exe 可以打开 a.txt。

其中，主体是 notepad.exe，客体是 a.txt，行为是“文件打开”，而可以打开 a.txt 的权限被赋予了 notepad.exe。

然后，每当有“文件打开”这个行为发生时，MAC 系统中的安全策略执行组件就会对主客体的权限进行检测，如果客体是 a.txt，那主体必须是 notepad.exe，打开文件的行为才会被允许，否则将被拒绝。

从整个过程中可以看出，“指令”并未参于到实际的规则判断之中，判断的仅仅是“进程”是否是“notepad.exe”，但实质上“打开文件”这个行为是由一组指令触发的，进程仅仅是一个容器。

在现有技术中存在着多种方法可以将一组指令放到任意进程中去执行，从而绕过基于进程识别的权限管控，例如以下方式中的任意一种：

a、进程中有漏洞，可导致任意远程代码执行；

b、通过线程注入的方式，注入一段代码到目标进程内执行；

c、加载一个模块到目标进程内并执行模块内的代码。

从上述场景的描述中可以看出，现有技术中基于 MAC 机制所实现的行为控制方法存在安全漏洞，并不能万无一失地实现对行为的控制。只有进入到代码指令识别的层次，才能真正的区分行为的发生真的是由 notepad.exe 触发，还是由一段非 notepad.exe 的异常指令触发。

为此，本申请实施例提供了一种在代码指令层次实现行为控制的方法。

图 1 为本申请实施例提供的行为控制方法的流程图，如图 1 所示，本申请实施例提供的行为控制方法，包括：

步骤 101、在目标行为发生时，获取所述目标行为所对应的指令数据。

在本申请实施例中，目标行为是指需要被控制的行为。例如，前述的对文本文件“a.txt”的“打开文件”的行为。对目标行为的控制既有可能是允许执行目标行为，也有可能是禁止执行目标行为。

在计算机操作系统中，一个行为由一条指令或多条指令实现。在本申请实施例中，若某一指令集合用于实现目标行为，则将与该指令集合相关的数据称为目标行为所对应的指令数据。

在本申请实施例中，所述指令数据包括指令执行序列。

指令执行序列用于描述 API（Application Programming Interface，应用

程序接口）调用序列中各层级的偏移地址及调用顺序。API 调用序列按程序的不同、功能的不同、分支的不同，可能会有不同的层深。例如，Local_A 函数调用 Local_B 函数、Local_B 函数调用 Local_C 函数、Local_C 函数调用系统 API CreateFileW 来打开一个文件。在这个例子中，API 调用序列为三层调用。各层 API 调用序列所对应的内存中的指令相对于程序基地址的偏移是不一样的，API 调用序列中各层级的偏移地址记录了各层 API 调用序列所对应的内存中的指令相对于程序基地址的偏移。例如，Local_A 函数在内存中的指令相对于程序基地址的偏移量为 010000（仅为示例说明之用，真实的地址偏移量可以与之不同），Local_B 函数在内存中的指令相对于程序基地址的偏移量为 020000，Local_C 函数在内存中的指令相对于程序基地址的偏移量为 030000，CreateFileW 在内存中的指令相对于程序基地址的偏移量为 040000。这些偏移地址一般用十六进制的数字表示，并按照执行的先后顺序依次排列，如形成诸如 010000020000030000040000 的序列。API 调用序列中各层级的偏移地址在指令执行序列中的顺序反映了调用顺序。

需要说明的是，同一类型的系统 API，其在内存中的指令相对于程序基地址的偏移量有可能是不一样的。例如，notepad.exe 中源于 NPCommand 指令执行序列中的 CreateFileW 调用指令，与源于 UpdateEncoding 指令执行序列中的 CreateFileW 调用指令均可实现文件打开操作。但源于 NPCommand 指令执行序列中的 CreateFileW 调用指令是在偏移 0x2323 处的上一条指令；源于 UpdateEncoding 指令执行序列中的 CreateFileW 调用指令是在偏移 0x1300 处的上一条指令。由此可见，即使同样是 CreateFileW 调用指令，也可能会有不同的地址偏移量。

在本申请的其他实施例中，所述指令数据还包括行为类型和/或 API 信息。

行为类型是指目标行为的类型。例如，典型的行为类型有打开文件、删除文件、保存文件、修改文件等。

API 信息是指目标行为在执行时所调用的 API 的信息。API 是一组定义、程序及协议的集合，它是程序与操作系统之间的接口，是程序能取得操作系统服务的唯一途径。程序的行为通常需要调用系统 API 来实现，例

如，在 windows 系统中，调用系统 API CreateFileW 创建或打开文件、调用系统 API CreateProcess 来创建进程、调用系统 API LoadLibrary 来加载模块。各个行为所对应的 API 的具体类型存在差异，因此指令数据中的 API 信息需要描述目标行为在执行时所调用的 API 的名称。

目标行为所对应的指令数据可能是合法的（得到授权），也可能是非法的（未得到授权）。在本申请实施例的后续步骤中，通过对目标行为所对应的指令数据的校验来确定目标行为是否被允许执行。

在与目标行为相关的进程触发所述目标行为时，通过对目标行为的拦截能够获知目标行为的发生。所述对目标行为的拦截可以采用现有 MAC 机制中的行为拦截功能，如通过以下技术中的任意一种实现：文件系统过滤驱动、系统回调接口、HOOK 技术。

通过对程序代码的分析可以知道，程序中与目标行为相关的指令数据是特定的，除了这些特定的指令数据外，其他的指令数据都与目标行为无关。

以指令执行序列为例，通过对 notepad.exe 程序进行分析可以知道，“打开文件”的行为在 notepad.exe 中有两组指令执行序列来实现：

第一组源于 NPCommand，中间经一系列调用，最终调用系统 API CreateFileW 来实现文件打开操作；

第二组源于 UpdateEncoding，中间经过一系列调用，最终调用系统 API CreateFileW 来实现文件打开操作。

除此之外，在 notepad.exe 中再无任何有关“打开文件”相关的指令存在。

也就是说，如果采用 notepad.exe 打开文件，那么内存中的指令执行序列必然是以上两条指令执行序列之一，任何产生“文件打开”操作的其它指令执行序列的调用都是非法的。

基于上述特点，在本步骤中，确定目标行为发生后，需要进一步获取目标行为所对应的指令数据，以在后续步骤中实现对目标行为的控制。

具体的说，在对目标行为的拦截时可以知道目标行为的行为类型。在之前的描述中已经对如何实现目标行为的拦截做了充分说明，因此不在此处重复。

由于行为与行为所调用的 API 之间的映射关系是固定且可穷举的，因此在确定目标行为的类型后，通过行为与 API 之间的映射关系能够得到目标行为的 API 信息。

在本申请实施例中，可通过栈数据获取目标行为所对应的指令执行序列。

“栈”是计算机系统中的一种具有特殊数据结构的动态内存。操作系统为每一个线程都维护了一个栈内存空间，在栈内存空间内保存的是此线程的函数调用信息，包括：函数调用的返回地址及参数。

由于函数调用信息在“栈”中按照先后顺序依次存放，因此基于栈数据可以还原任一线程的函数调用序列。

基于“栈”的前述特性，可以获得目标行为所对应的线程的栈数据，然后依据栈数据还原目标行为发生时的指令执行序列。如何依据栈数据还原目标行为发生时的指令执行序列是本领域技术人员的公知常识，因此不在此处做重复说明。

由于在不同的程序中，同类型的行为所对应的指令数据可能存在差异。因此，在另一个实施例中，目标行为的指令数据包括：程序名称、版本号、行为类型、API 信息、指令执行序列。

其中，程序名称是指目标行为所属程序的名称。例如，前述打开文本文件“a.txt”的行为是由名称为 notepad.exe 的程序触发的，则指令数据中的程序名称就是 notepad.exe。

版本号是指目标行为所属的程序的版本号。应用程序通常会有多次迭代更新，为了区分不同版本的应用程序，会为应用程序设置版本号。例如，应用程序 notepad.exe 有 1.0、2.0、3.0 等多个版本，若目标行为只在 2.0 之后的版本出现，则指令数据的版本号中只包含 2.0 之后的版本号（如 2.0、3.0）。

目标行为所述程序的程序名称以及版本号可通过现有技术获取，在本申请实施例中不对其获取过程做详细描述。

行为类型、API 信息以及指令执行序列在之前的描述中已经有详细的说明，因此不在此处重复。

通过前述的程序名称、版本号、行为类型、API 信息、指令执行序列，

可以精确地描述目标行为所对应的指令数据。

步骤 102、将所述目标行为所对应的指令数据与预先设置的指令白名单库中的数据进行匹配，根据匹配结果确定所述目标行为是否被授权。

在本申请实施例中，指令白名单库用于存储被授权行为所对应的指令数据。其中，被授权行为是指被允许执行的行为。

在不同的操作系统中，实现特定功能（即行为的执行结果）需要调用的 API 是固定不变的，这是由操作系统提供的标准接口规范所决定的。特定功能与所要调用的 API 之间的映射关系是固定且可穷举的，而非可随机变化的。因此，在本申请实施例中，将被授权的行为及其所要调用的指令执行序列之间的映射关系通过指令白名单库的方式予以存储。

具体的说，在一个实施例中，指令数据包括：指令执行序列。

指令执行序列用于描述 API 调用序列中各层级的偏移地址及调用顺序。

在本申请另一个实施例中，指令数据还包括：行为类型及 API 信息。

行为类型是指被授权的行为的类型。例如，典型的行为类型有打开文件、删除文件、保存文件、修改文件等。

API 信息是指被授权的行为在执行时所调用的 API 的信息。

关于行为类型、API 信息以及指令执行序列的详细内容在之前的描述中已经有较为充分的说明，因此不在此处重复。

在本申请的另一个实施例中，指令数据包括：程序名称、版本号、行为类型、API 信息、指令执行序列。

被授权行为的指令数据在存储时，可以有多种存储方式。一种常见的存储方式是：程序名称及版本号均相同的程序内的所有被授权行为的数据（行为类型、API 信息、指令执行序列）存储在一个指令白名单库中，不同的程序（不同的程序包含：名称不同的程序，名称相同但版本号不同的程序）会有各自对应的指令白名单库。在其他实施例中，也可以将不同程序内的被授权行为的指令数据都存储在一个指令白名单库中。

在本申请实施例中，指令白名单库是预先设置的，可直接使用指令白名单库中的数据。在本申请的其他实施例中，将对指令白名单库的生成过程进行说明。

当程序名称及版本号均相同的程序内的所有被授权行为的指令数据存储在一个指令白名单库中，且所述指令白名单库已经确定时，根据目标行为的指令数据就可以与指令白名单库中的数据进行匹配。

如在一个实施例中，将所述目标行为的指令数据与指令白名单库中的指令数据进行匹配，包括:

将所述目标行为的指令执行序列与指令白名单库中的指令执行序列进行匹配。

其中，在将目标行为的指令执行序列中各层级的偏移地址与指令白名单库中的指令执行序列中各层级的偏移地址进行匹配时，需要按照预先设定的匹配顺序进行匹配操作。所述预先设定的匹配顺序可以与调用顺序反方向，也可以与调用顺序同方向。

以匹配顺序与调用顺序反方向为例，在 Local_A 函数调用 Local_B 函数、Local_B 函数调用 Local_C 函数、Local_C 函数调用系统 API CreateFileW 来打开一个文件的例子中，调用顺序为 Local_A—Local_B—Local_C—CreateFileW。而匹配操作的顺序则为 CreateFileW—Local_C—Local_B—Local_A。

作为一种可选的实现方式，偏移地址做匹配时，可以根据实际需要（如具体的应用场景）设置匹配层数。例如，若匹配操作的顺序为 CreateFileW—Local_C—Local_B—Local_A，若只做一层匹配，那么只需要比较 CreateFileW 这一层的指令偏移地址是否一致；若需要做二层匹配，那么需要同时比较 CreateFileW 这一层的指令偏移地址以及 Local_C 这一层的指令偏移地址是否一致；若需要做三层匹配，那么需要同时比较 CreateFileW 这一层的指令偏移地址、Local_C 这一层的指令偏移地址以及 Local_B 这一层的指令偏移地址是否一致。依次类推，直至分层匹配的层数达到预先设置的匹配层数。

若匹配成功，认为目标行为所对应的指令数据与预先设置的指令白名单库中的数据匹配成功。反之，若匹配失败，就认为目标行为所对应的指令数据与预先设置的指令白名单库中的数据匹配失败。

在另一个实施例中，将所述目标行为所对应的指令数据与预先设置的指令白名单库中的数据进行匹配，还包括:

将所述目标行为的行为类型与所述指令白名单库中的行为类型进行匹配;

和/或,

将所述目标行为的API信息与所述指令白名单库中的API信息进行匹配。

也就是说,在该实施例中,需要同时对指令执行序列以及行为类型和/或 API 信息进行匹配。

以需要同时对指令执行序列、行为类型以及 API 信息进行匹配为例,具体包括:

将所述目标行为的行为类型与所述指令白名单库中的行为类型进行第一次匹配;

当所述第一次匹配成功后,将所述目标行为的 API 信息与所述指令白名单库中的 API 信息进行第二次匹配;

当所述第二次匹配成功后,将所述目标行为的指令执行序列与指令白名单库中的指令执行序列进行第三次匹配。

只有前述三次匹配全部匹配成功,才认为目标行为所对应的指令数据与预先设置的指令白名单库中的数据匹配成功。反之,只要有任意一项的匹配失败,就认为目标行为所对应的指令数据与预先设置的指令白名单库中的数据匹配失败。

当程序名称及版本号均相同的程序内的所有被授权行为的指令数据(行为类型、API 信息、指令执行序列中)存储在一个指令白名单库中,且所述指令白名单库尚未确定时,需要根据目标行为所属程序的程序名称、版本号、目标行为的行为类型、API 信息以及指令执行序列中就可以与指令白名单库中的数据进行匹配。

具体包括:

首先,根据目标行为所属进程的信息确定目标行为所属程序的程序名称与版本号,根据所述程序名称与版本号确定指令白名单库。

由于不同的程序会有各自对应的指令白名单库,因此需要根据目标行为所属程序的程序名称与版本号确定指令白名单库。

接着,将所述目标行为的第一行为类型与所述指令白名单库中的第二

行为类型进行第一次匹配;

当所述第一次匹配成功后，将所述目标行为的 API 信息与所述指令白名单库中的 API 信息进行第二次匹配;

当所述第二次匹配成功后，将所述目标行为的第指令执行序列与指令白名单库中的指令执行序列进行第三次匹配。

上述的第一次匹配、第二次匹配以及第三次匹配的实现过程在之前的描述中已经有详细说明，因此不在此处重复。

在得到匹配结果后，根据匹配结果可以确定目标行为是否被允许。如果匹配成功，则说明目标行为所对应的指令数据事先已经得到授权，该目标行为是合法的行为，可以正常执行。如果匹配失败，则说明目标行为所对应的指令数据事先并未得到授权，该目标行为可能是非法的行为，将阻止其被执行。

本申请实施例提供的行为控制方法通过生成目标行为所对应的指令数据，然后将其与指令白名单库中的数据进行匹配，根据匹配结果确定目标行为是否合法，从而在代码指令层次实现行为控制，较现有的基于进程的行为控制方法安全性更高。

基于上述任一实施例，在本申请实施例中，方法还包括:

对程序以及其所使用的动态库进行分析，确定所述程序中与被授权行为相对应的指令数据;

根据被授权行为相对应的数据，生成指令白名单库。

在本申请实施例中，被授权行为是指被允许执行的行为。在程序中，一般只允许少量指令执行序列实现被授权行为。

例如，通过对 notepad.exe 的代码进行分析可以知道，“打开文件”的行为在 notepad.exe 中有两组指令执行序列来实现:

第一组源于 NPCommand，中间经一系列调用，最终调用系统 API CreateFileW 来实现文件打开操作;

第二组源于 UpdateEncoding，中间经过一系列调用，最终调用系统 API CreateFileW 来实现文件打开操作。

除了这两组指令执行序列外，notepad.exe 中的其余指令不能执行“打开文件”的行为。

因此，在本申请实施例中，需要确定程序中与被授权行为相对应的指令数据。具体的说，

首先，确定与被授权行为相对应的第一 API。

与被授权行为相对应的 API 可以有一个，也可以有多个，例如，“打开文件”的行为，既可以调用系统 API OpenFile 来实现，也可以调用系统 API CreateFileW 来实现。因此，在本步骤中需要确定与被授权行为相对应的 API，将这一 API 记为第一 API。

由于行为与行为所调用的 API 之间的映射关系是固定且可穷举的，因此在确定被授权行为的类型后，通过行为与 API 之间的映射关系能够得到所述第一 API。

例如，可将行为与行为所调用的 API 之间的映射关系通过表格的方式予以存储。在确定第一 API 时，根据被授权行为的行为类型查找表格，所得到的查找结果即为第一 API。

接着，确定用于调用所述第一 API 的指令执行序列。

在本申请实施例中，可通过反汇编引擎，确定用于调用所述第一 API 的指令执行序列。

再接着，根据用于调用所述第一 API 的指令执行序列，确定所述程序中与被授权行为相对应的指令执行序列。

调用 API 的指令执行序列可以有多层，如 Local_A 函数调用 Local_B 函数，Local_B 函数调用 Local_C 函数，Local_C 函数调用系统 API CreateFileW 来打开一个文件。在这个例子中，调用系统 API CreateFileW 的指令执行序列有三层。

在根据调用所述第一 API 的指令执行序列，确定所述程序中与被授权行为相对应的指令执行序列的过程中，可以将用于调用所述第一 API 的指令执行序列的全部作为程序中与被授权行为相对应的指令执行序列，也可以将用于调用所述第一 API 的指令执行序列的一部分作为程序中与被授权行为相对应的指令执行序列。

例如，完整的调用系统 API CreateFileW 的指令执行序列为：Local_A—Local_B—Local_C—CreateFileW。可以将这整个指令执行序列作为程序中与被授权行为相对应的指令执行序列，也可以将该指令执行序

列的一部分，如 Local_B—Local_C—CreateFileW，作为程序中与被授权行为相对应的指令执行序列。

在确定所述程序中与被授权行为相对应的指令执行序列时，具体从调用所述第一 API 的指令执行序列选取多少层可以根据实际需要确定。理论上来说，哪怕只选取一层，也可以识别出绝大多数的正常调用与异常调用。当然，选取的层数越多，就越难以被伪造，选取的层数越少，伪造就越容易。

最后，根据所述程序中与被授权行为相对应的指令执行序列，确定所述程序中与被授权行为相对应的指令数据。

在确定程序中与被授权行为相对应的指令执行序列后，再获得被授权行为所属程序的程序名称、版本号、行为类型以及 API 信息等数据，就能够确定所述程序中与被授权行为相对应的指令数据，进而生成指令白名单库。

本申请实施例提供的行为控制方法通过对程序以及其所使用的动态库进行分析，确定所述程序中与被授权行为相对应的指令数据；根据被授权行为相对应的指令数据，生成指令白名单库，根据所述指令白名单库可对目标行为所对应的指令数据进行匹配操作，根据匹配结果确定目标行为是否合法，从而在代码指令层次实现行为控制，较现有的基于进程的行为控制方法安全性更高。

基于上述任一实施例，在本申请实施例中，方法还包括：

对所述目标行为所属进程的权限以及所述目标行为所要处理对象的权限进行校验。

目标行为所属进程对应于程序，即 MAC 机制中的主体；目标行为所要处理对象对应于文件，即 MAC 机制中的客体。

在目标行为所对应的指令数据进行校验前，可以首先对所述目标行为所属进程的权限以及所述目标行为所要处理对象的权限进行校验，只有通过校验才会进一步对目标行为所对应的指令执行序列进行校验。

如何校验目标行为所属进程的权限以及目标行为所要处理对象的权限，在 MAC 机制中已经有详细的说明，因此不在本申请实施例中做详细说明。

本申请实施例提供的行为控制方法通过对目标行为所属进程的权限以及所述目标行为所要处理对象的权限进行校验，可以过滤明显的非法行为，有助于减轻对计算机系统的资源负载。

基于上述任一实施例，图 2 为本申请实施例提供的行为控制装置的示意图，如图 2 所示，本申请实施例提供的行为控制装置，包括:

指令数据获取模块 201，用于在目标行为发生时，获取所述目标行为所对应的指令数据;

匹配模块 202，用于将所述目标行为所对应的指令数据与预先设置的指令白名单库中的数据进行匹配，根据匹配结果确定所述目标行为是否被授权；其中，

所述指令白名单库用于存储被授权行为所对应的指令数据。

本申请实施例提供的行为控制装置通过生成目标行为所对应的指令数据，然后将其与指令白名单库中的数据进行匹配，根据匹配结果确定目标行为是否合法，从而在代码指令层次实现行为控制，较现有的基于进程的行为控制装置安全性更高。

图 3 为本申请实施例所涉及的电子设备的实体结构示意图，如图 3 所示，该电子设备可以包括: 处理器(processor)310、通信接口(Communications Interface)320、存储器(memory)330 和通信总线 340，其中，处理器 310，通信接口 320，存储器 330 通过通信总线 340 完成相互间的通信。处理器 310 可以调用存储器 330 中的逻辑指令，以执行如下方法:

在目标行为发生时，获取所述目标行为所对应的指令数据;

将所述目标行为所对应的指令数据与预先设置的指令白名单库中的数据进行匹配，根据匹配结果确定所述目标行为是否被授权；其中，

所述指令白名单库用于存储被授权行为所对应的指令数据。

此外，上述的存储器 330 中的逻辑指令可以通过软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本申请各个

实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介质。

另一方面，本申请实施例还提供一种非暂态计算机可读存储介质，其上存储有计算机程序，该计算机程序被处理器执行时实现以执行上述各实施例提供的方法，例如包括：

在目标行为发生时，获取所述目标行为所对应的指令数据；

将所述目标行为所对应的指令数据与预先设置的指令白名单库中的数据进行匹配，根据匹配结果确定所述目标行为是否被授权；其中，

所述指令白名单库用于存储被授权行为所对应的指令数据。

以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性的劳动的情况下，即可以理解并实施。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到各实施方式可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件。基于这样的理解，上述技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在计算机可读存储介质中，如ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行各个实施例或者实施例的某些部分所述的方法。

最后应说明的是：以上实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的精神和范围。

权 利 要 求 书

1、一种行为控制方法，其特征在于，包括:

在目标行为发生时，获取所述目标行为所对应的指令数据;

将所述目标行为所对应的指令数据与预先设置的指令白名单库中的数据进行匹配，根据匹配结果确定所述目标行为是否被授权；其中，

所述指令白名单库用于存储被授权行为所对应的指令数据。

2、根据权利要求 1 所述的行为控制方法，其特征在于，所述指令数据包括: 指令执行序列; 所述指令执行序列用于描述 API 调用序列中各层级的偏移地址及调用顺序;

相应地，所述将所述目标行为所对应的指令数据与预先设置的指令白名单库中的数据进行匹配，包括:

将所述目标行为的指令执行序列与指令白名单库中的指令执行序列进行匹配。

3、根据权利要求 2 所述的行为控制方法，其特征在于，所述指令数据还包括: 行为类型和/或 API 信息;

相应地，所述将所述目标行为所对应的指令数据与预先设置的指令白名单库中的数据进行匹配，还包括:

将所述目标行为的行为类型与所述指令白名单库中的行为类型进行匹配;

和/或，

将所述目标行为的API信息与所述指令白名单库中的API信息进行匹配。

4、根据权利要求 3 所述的行为控制方法，其特征在于，所述指令数据还包括: 程序名称以及程序版本号;

相应地，所述将所述目标行为所对应的指令数据与预先设置的指令白名单库中的数据进行匹配，还包括:

根据目标行为所属进程的信息确定目标行为所属程序的程序名称与版本号，根据所述程序名称与版本号确定指令白名单库。

5、根据权利要求 2 所述的行为控制方法，其特征在于，所述将所述目标行为的指令执行序列与指令白名单库中的指令执行序列进行匹配，包

括:

按照预先设定的匹配顺序，将所述目标行为的指令执行序列中各层的偏移地址与指令白名单库中的指令执行序列中各层的偏移地址按照层级依次进行匹配，直至已匹配的层级数量达到预先设置的匹配层数。

6、根据权利要求 2 所述的行为控制方法，其特征在于，所述获取所述目标行为所对应的指令数据，包括:

获取所述目标行为所对应的线程的栈数据;

根据所述栈数据还原所述目标行为发生时的指令执行序列。

7、根据权利要求 1 至 6 任一项所述的行为控制方法，其特征在于，所述方法还包括:

对程序以及其所使用的动态库进行分析，确定所述程序中与被授权行为相对应的指令数据;

根据被授权行为相对应的指令数据，生成指令白名单库。

8、根据权利要求 7 所述的行为控制方法，其特征在于，所述确定所述程序中与被授权行为相对应的指令数据，包括:

确定与所述被授权行为相对应的第一 API;

确定用于调用所述第一 API 的指令执行序列;

根据所述用于调用所述第一 API 的指令执行序列，确定所述程序中与被授权行为相对应的指令执行序列;

根据所述程序中与被授权行为相对应的指令执行序列，确定所述程序中与被授权行为相对应的指令数据。

9、根据权利要求 8 所述的行为控制方法，其特征在于，所述根据所述用于调用所述第一 API 的指令执行序列，确定所述程序中与被授权行为相对应的指令执行序列，包括:

将所述用于调用所述第一 API 的指令执行序列的全部作为程序中与被授权行为相对应的指令执行序列;

或，将所述用于调用所述第一 API 的指令执行序列的一部分作为程序中与被授权行为相对应的指令执行序列。

10、一种行为控制装置，其特征在于，包括:

指令数据获取模块，用于在目标行为发生时，获取所述目标行为所对

应的指令数据；

匹配模块，用于将所述目标行为所对应的指令数据与预先设置的指令白名单库中的数据进行匹配，根据匹配结果确定所述目标行为是否被授权；其中，

所述指令白名单库用于存储被授权行为所对应的指令数据。

11、一种电子设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述程序时实现如权利要求 1 至 9 任一项所述行为控制方法的步骤。

12、一种非暂态计算机可读存储介质，其上存储有计算机程序，其特征在于，该计算机程序被处理器执行时实现如权利要求 1 至 9 任一项所述行为控制方法的步骤。

13、一种计算机程序产品，所述计算机程序产品包括计算机可执行指令，其特征在于，所述指令在被执行时用于实现如权利要求 1 至 9 任一项所述行为控制方法的步骤。

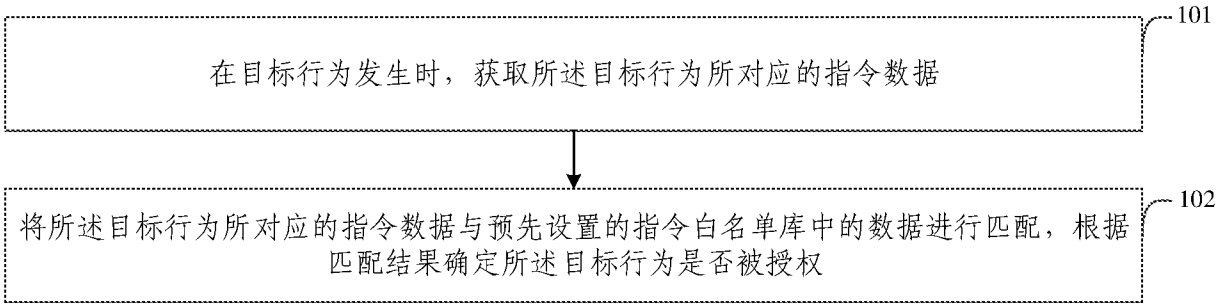

101
在目标行为发生时，获取所述目标行为所对应的指令数据
102
将所述目标行为所对应的指令数据与预先设置的指令白名单库中的数据进行匹配，根据匹配结果确定所述目标行为是否被授权

图 1

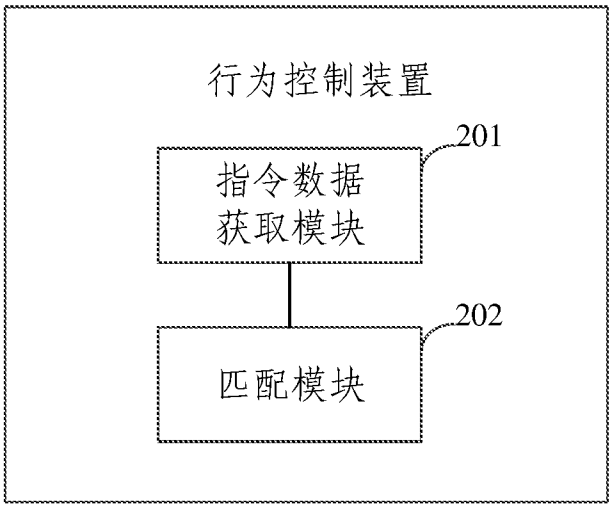

行为控制装置
201
指令数据获取模块
202
匹配模块

图 2

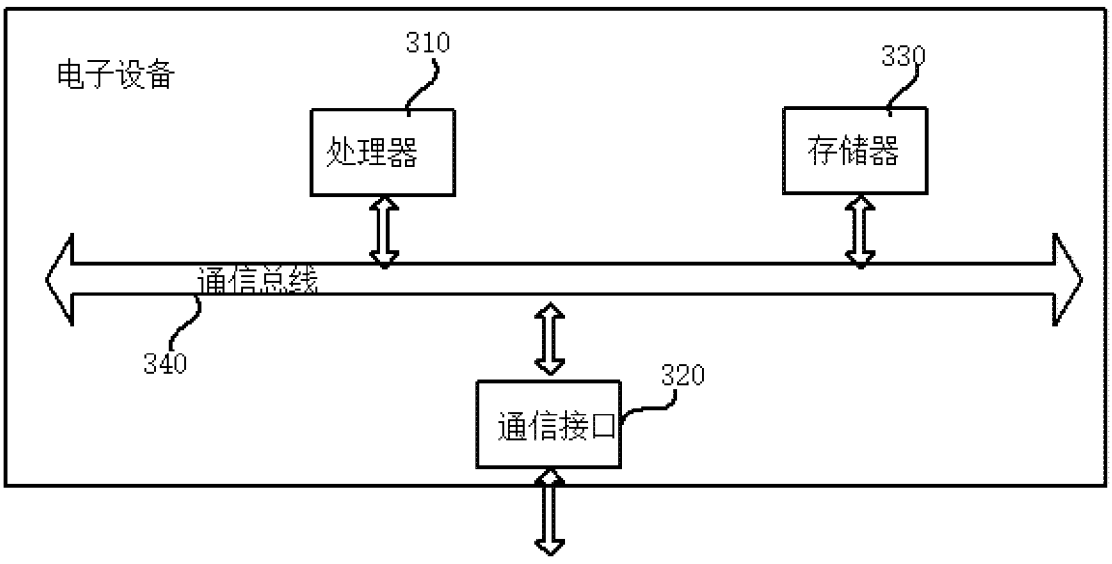

电子设备
310
处理器
330
存储器
通信总线
340
320
通信接口

图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/130041

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

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: 指令, 白名单, 序列, 授权, 访问控制, instructions, white list, sequence, array, authorization, access, control, API, MAC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 112817822 A (SHENZHEN THINKIVE INFORMATION TECHNOLOGY CO., LTD.) 18 May 2021 (2021-05-18) description, paragraphs [0047]-[0055]	1-13
PX	CN 112395593 A (QI AN XIN SECURITY TECHNOLOGY (ZHUHAI) CO., LTD. et al.) 23 February 2021 (2021-02-23) description, paragraphs [0056]-[0065]	1-13
Y	CN 109726548 A (360 ENTERPRISE SECURITY TECHNOLOGY (ZHUHAI) CO., LTD. et al.) 07 May 2019 (2019-05-07) description, paragraph [0003]	1-13
Y	US 2020175155 A1 (EBAY INC.) 04 June 2020 (2020-06-04) claims 1 and 7	1-13
A	CN 109508536 A (HUAWEI TECHNOLOGIES CO., LTD.) 22 March 2019 (2019-03-22) entire document	1-13
A	CN 103279706 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.) 04 September 2013 (2013-09-04) entire document	1-13

☑ 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
24 January 2022	**10 February 2022**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088, China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/130041

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 103020527 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.) 03 April 2013 (2013-04-03) entire document	1-13

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2021/130041

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 112817822 A	18 May 2021	None	
CN 112395593 A	23 February 2021	None	
CN 109726548 A	07 May 2019	None	
US 2020175155 A1	04 June 2020	CN 113168463 A	23 July 2021
		EP 3891632 A1	13 October 2021
		WO 2020117314 A1	11 June 2020
CN 109508536 A	22 March 2019	None	
CN 103279706 A	04 September 2013	None	
CN 103020527 A	03 April 2013	None	

国际检索报告

国际申请号
PCT/CN2021/130041

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)

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, EPODOC, CNPAT, CNKI, IEEE: 指令, 白名单, 序列, 授权, 访问控制, instructions, white list, sequence, array, authorization, access, control, API, MAC

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 112817822 A (深圳市思迪信息技术股份有限公司) 2021年5月18日 (2021-05-18) 说明书第[0047]-[0055]段	1-13
PX	CN 112395593 A (奇安信安全技术珠海有限公司 等) 2021年2月23日 (2021-02-23) 说明书第[0056]-[0065]段	1-13
Y	CN 109726548 A (360企业安全技术珠海有限公司 等) 2019年5月7日 (2019-05-07) 说明书第[0003]段	1-13
Y	US 2020175155 A1 (EBAY INC.) 2020年6月4日 (2020-06-04) 权利要求1、7	1-13
A	CN 109508536 A (华为技术有限公司) 2019年3月22日 (2019-03-22) 全文	1-13
A	CN 103279706 A (北京奇虎科技有限公司 等) 2013年9月4日 (2013-09-04) 全文	1-13
A	CN 103020527 A (北京奇虎科技有限公司 等) 2013年4月3日 (2013-04-03) 全文	1-13

☐ 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
2022年1月24日	2022年2月10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 赵婷 电话号码 86-(10)-53961350

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2021/130041

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	112817822	A	2021年5月18日	无			
CN	112395593	A	2021年2月23日	无			
CN	109726548	A	2019年5月7日	无			
US	2020175155	A1	2020年6月4日	CN	113168463	A	2021年7月23日
				EP	3891632	A1	2021年10月13日
				WO	2020117314	A1	2020年6月11日
CN	109508536	A	2019年3月22日	无			
CN	103279706	A	2013年9月4日	无			
CN	103020527	A	2013年4月3日	无			