

(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
2012 年 10 月 26 日 (26.10.2012) WIPO | PCT



(10) 国际公布号
WO 2012/142943 A1

- (51) 国际专利分类号:
G06F 21/22 (2006.01)
- (21) 国际申请号: PCT/CN2012/074241
- (22) 国际申请日: 2012 年 4 月 18 日 (18.04.2012)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201110100859.6 2011 年 4 月 21 日 (21.04.2011) CN
- (71) 申请人 (对除美国外的所有指定国): 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)。
- (72) 发明人; 及
- (75) 发明人/申请人 (仅对美国): 范纪鎰 (FAN, Jihuang) [CN/CN]; 中国北京市朝阳区建国路 71 号惠通时代广场 D 座, Beijing 100025 (CN)。 潘剑锋 (PAN, Jianfeng) [CN/CN]; 中国北京市朝阳区建国路 71 号惠通时代广场 D 座, Beijing 100025 (CN)。 孙晓骏 (SUN, Xiaojun) [CN/CN]; 中国北京市朝阳区建国路 71 号惠通时代广场 D 座, Beijing 100025 (CN)。 路

健华 (LU, Jianhua) [CN/CN]; 中国北京市朝阳区建国路 71 号惠通时代广场 D 座, Beijing 100025 (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 1116, 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, 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, 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,

[见续页]

(54) Title: METHOD AND DEVICE FOR DEFENSE BY USING SANDBOX, AND SECURE BROWSER

(54) 发明名称: 利用沙箱进行防御的方法、装置及安全浏览器

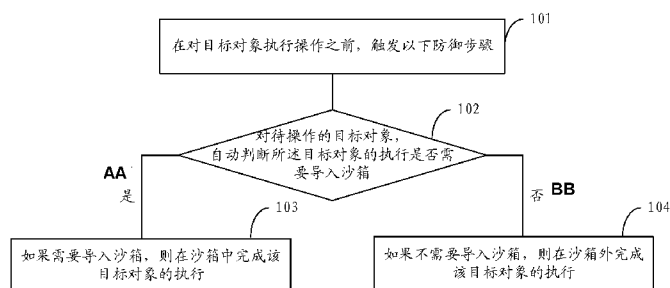


图 1 / FIG. 1

101 Before executing an operation on a target object, triggering of the following defense steps
102 Automatic judgment of whether the execution of the target object to be operated needs to be introduced into a sandbox
103 If the execution of the target object needs to be introduced into the sandbox, completion of the execution of the target object in the sandbox
104 If the execution of the target object does not need to be introduced into the sandbox, completion of the execution of the target object outside the sandbox
AA Yes
BB No

(57) Abstract: This application provides a method and a device for defense by using a sandbox, and a secure browser, so as to solve the problem of a sandbox technology where a user performs selection in the prior art. The method comprises: before executing an operation on a target object, automatically judging whether execution of the target object to be operated needs to be introduced into a sandbox; and if it is determined that the execution of the target object needs to be introduced into the sandbox, introducing the target object into the sandbox and completing the execution of the target object in the sandbox. In this application, before a user executes an operation on a target object, it is automatically judged whether the execution of the target object needs to be introduced into the sandbox, so as to help the user to decide which risky programs need to be run in the sandbox.

[见续页]

WO 2012/142943 A1



RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, 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))。

(57) 摘要:

本申请提供了一种利用沙箱进行防御的方法、装置及安全浏览器,以解决现有技术中由用户自行选择的沙箱技术所存在的问题。其中,所述方法包括:在对目标对象执行操作之前,自动判断待操作的所述目标对象的执行是否需要导入沙箱;若确定需要导入沙箱,则将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行。本申请可以在用户对目标对象执行操作之前,自动判断所述目标对象的执行是否需要导入沙箱,帮助用户决定哪些有风险的程序需要在沙箱内运行。

说 明 书

利用沙箱进行防御的方法、装置及安全浏览器

技术领域

本申请涉及计算机安全技术领域，特别是涉及一种利用沙箱进行防御的方法、装置及一种安全浏览器。

5 背景技术

在计算机安全领域，沙箱(也称为沙盒)是一种程序的隔离运行机制，其目的是限制不可信进程的权限。沙箱技术经常被用于执行未经测试的或不可信的客户程序。为了避免不可信程序可能破坏其它程序的运行，沙箱技术通过为不可信客户程序提供虚拟化的磁盘、内存以及网络资源，而这种虚拟化手段对客户程序来说是透明的。由于沙箱里的资源被虚拟化(或被间接化)，所以沙箱里的不可信程序的恶意行为往往会被限制在沙箱中，从而保护系统原有的状态。

具体来说，沙箱技术可以将一个程序放入沙箱运行，这样该程序所创建、修改、删除的所有文件和注册表都会被虚拟化重定向，也就是说所有操作都是虚拟的，真实的文件和注册表不会被改动，这样可以确保病毒无法对系统关键部位进行改动，破坏系统。

目前沙箱技术提供了两种类型的沙箱：一种是特定型沙箱，例如：Chrome(一种浏览器)利用沙箱技术将渲染引擎或Flash放在沙箱内运行，以保证浏览器的安全；还有一种是通用型沙箱，例如：Sandboxie(另一种浏览器)则提供给用户一个沙箱，让用户自行选择软件程序放入沙箱内运行。

与特定型沙箱相比，上述由用户选择的通用型沙箱为用户提供了更多的灵活性，极大地方便了用户的使用。但是，这种让用户选择的方式存在以下几个问题：

问题一，用户必须自行判断哪些是有风险的程序，需要放在沙箱内运行，如果用户不了解程序的特性，就可能选择错误。

问题二，错误地使用沙箱，如将正在编辑文件的编辑程序放置沙箱内，会导致文件丢失。

问题三，用户自行选择的方式易用性不高，操作复杂，不符合用户的操作习惯。

5 发明内容

本申请提供了一种利用沙箱进行防御的方法、装置及安全浏览器，以解决现有技术中由用户自行选择沙箱技术所存在的上述问题至少之一。

为了解决上述问题，本申请公开了一种利用沙箱进行防御的方法，包括：在对目标对象执行操作之前，自动判断待操作的所述目标对象的执行是否需要导入沙箱；若确定需要导入沙箱，则将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行。

优选地，将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行的步骤包括：如果所述目标对象为目标程序，则将该目标程序导入沙箱，在沙箱中完成该目标程序的运行；如果所述目标对象为目标文件，则将执行该目标文件的关联程序导入沙箱，在沙箱中由所述关联程序运行该目标文件；如果所述目标对象为用户输入的信息，则将接收该用户输入信息的关联程序导入沙箱，在沙箱中根据该用户输入信息运行所述关联程序；所述用户输入的信息包括网址和/或关键词。

优选地，所述在对目标对象执行操作之前，自动判断待操作的所述目标对象的执行是否需要导入沙箱的步骤包括：如果所述目标对象为目标程序，则将所述目标程序下载到客户端后，在客户端运行该目标程序之前，自动判断待操作的所述目标对象的执行是否需要导入沙箱；和/或，在下载所述目标程序之前，自动判断待操作的所述目标对象的执行是否需要导入沙箱；如果所述目标对象为目标文件，则将所述目标文件或执行该目标文件的关联程序下载到客户端后，在客户端运行该目标文件之前，自动判断待操作的所述目标对象的执行是否需要导入沙箱；和/或，在下载所述目标文件或在线执行该目标文件的关联程序之前，自动判断待操作的所述目标对象的执行是否需要

导入沙箱；如果所述目标对象为用户输入的信息，则在用户输入所述信息时，自动判断待操作的所述目标对象的执行是否需要导入沙箱。

优选地，所述自动判断待操作的所述目标对象的执行是否需要导入沙箱的步骤包括：判断所述待操作的目标对象是否符合预置的匹配规则，如果符合，则所述待操作的目标对象的执行需要导入沙箱；如果不符合，则不需要导入沙箱。

10 优选地，在判断所述待操作的目标对象是否符合预置的匹配规则的步骤之前，还包括：创建用于自动判断所述目标对象的执行的进程；判断所述进程的父进程是否在沙箱内，如果是，则执行所述将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行的步骤；如果否，则继续判断所述待操作的目标对象是否符合预置的匹配规则的步骤。

15 优选地，在判断所述待操作的目标对象是否符合预置的匹配规则的步骤之前，还包括：判断用户是否选择将所述待操作的目标对象的执行导入沙箱，如果是，则执行所述将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行的步骤；如果否，则继续判断所述待操作的目标对象是否符合预置的匹配规则的步骤。

20 优选地，在判断所述待操作的目标对象是否符合预置的匹配规则之前，还包括：判断所述待操作的目标对象是否在白名单中，如果不在白名单中，则所述待操作的目标对象是未知对象，继续判断所述待操作的目标对象是否符合预置的匹配规则的步骤；如果在白名单中，则不需要导入沙箱。

25 优选地，在判断所述待操作的目标对象是否符合预置的匹配规则之前，还包括：判断所述待操作的目标对象是否在黑名单中，如果在黑名单中，则执行所述将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行的步骤；如果不在黑名单中，则继续判断所述待操作的目标对象是否符合预置的匹配规则的步骤。

优选地，判断所述待操作的目标对象是否符合预置的匹配规则，包括：查询预置的数据库，将所述待操作的目标对象与该数据库中的预置规则进行比较，如果在该数据库中查询到，则符合匹配规则；如果未查询到，则不符

合匹配规则。

优选地，当所述待操作的目标对象为目标程序和/或目标文件时，判断所述待操作的目标对象是否符合预置的匹配规则，包括：据所述目标对象的信息，判断所述目标对象是否符合预置的匹配规则；和/或，根据所述目标对象的来源程序的信息，判断所述目标对象是否符合预置的匹配规则。

优选地，所述目标对象的信息包括以下至少之一：目标对象的文件路径、加密数据、文件属性、图标特征值、文件特征值、下载来源；所述来源程序的信息包括以下至少之一：来源程序的文件路径、加密数据、文件属性、图标特征值、文件特征值、下载来源。

10 优选地，当所述待操作的目标对象为用户输入的信息时，判断所述待操作的目标对象是否符合预置的匹配规则，包括：判断所述用户输入的信息是否符合预置的匹配规则。

15 优选地，所述自动判断待操作的所述目标对象的执行是否需要导入沙箱的步骤包括：根据客户端的请求，由服务器端自动判断所述待操作的目标对象的执行是否需要导入沙箱；和/或，由客户端自动判断所述待操作的目标对象的执行是否需要导入沙箱。

优选地，如果所述待操作的目标对象的执行需要导入沙箱，则导入沙箱之前，还包括：弹出提示窗提示用户是否导入沙箱，根据所述用户的肯定输入将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行。

20 本申请还提供了一种在其上记录有用于执行上述利用沙箱进行防御的方法的计算机可读记录介质。

本申请还提供了一种利用沙箱进行防御的装置，包括：

判断模块，设置为在对目标对象执行操作之前，自动判断待操作的所述目标对象的执行是否需要导入沙箱；

25 执行模块，设置为若所述判断模块的判断结果为需要导入沙箱，则将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行。

优选地，所述执行模块在将所述目标对象导入所述沙箱并在所述沙箱中

完成该目标对象的执行时，

如果所述目标对象为目标程序，则将该目标程序导入沙箱，在沙箱中完成该目标程序的运行；

如果所述目标对象为目标文件，则将执行该目标文件的关联程序导入沙箱，在沙箱中由所述关联程序运行该目标文件；

如果所述目标对象为用户输入的信息，则将接收该用户输入信息的关联程序导入沙箱，在沙箱中根据该用户输入信息运行所述关联程序；所述用户输入的信息包括网址和/或关键词。

优选地，所述判断模块，设置为：如果所述目标对象为目标程序，则将所述目标程序下载到客户端后在客户端运行该目标程序之前，自动判断待操作的所述目标对象的执行是否需要导入沙箱；和/或，在下载所述目标程序之前，自动判断待操作的所述目标对象的执行是否需要导入沙箱；

如果所述目标对象为目标文件，则将所述目标文件或执行该目标文件的关联程序下载到客户端后在客户端运行该目标文件之前，自动判断待操作的所述目标对象的执行是否需要导入沙箱；和/或，在下载所述目标文件或在线执行该目标文件的关联程序之前，自动判断待操作的所述目标对象的执行是否需要导入沙箱；

如果所述目标对象为用户输入的信息，则在用户输入所述信息时，自动判断待操作的所述目标对象的执行是否需要导入沙箱。

优选地，所述判断模块包括：规则判断模块，设置为在对目标对象执行操作之前，判断所述待操作的目标对象是否符合预置的匹配规则，如果符合，则所述待操作的目标对象的执行需要导入沙箱；如果不符合，则不需要导入沙箱。

优选地，所述判断模块还包括：父进程判断模块，设置为在所述规则判断模块判断所述待操作的目标对象是否符合预置的匹配规则之前，创建用于自动判断所述目标对象的执行的进程后，判断所述进程的父进程是否在沙箱内，如果是，则触发所述执行模块将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行；如果否，则触发所述规则判断模块继续判断所

述待操作的目标对象是否符合预置的匹配规则。

优选地，所述判断模块还包括：用户选择判断模块，设置为判断用户是否选择将所述待操作的目标对象的执行导入沙箱，如果是，则触发所述执行模块将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行；
5 如果否，则触发所述规则判断模块继续判断所述待操作的目标对象是否符合预置的匹配规则。

优选地，所述判断模块还包括：白名单判断模块，设置为判断所述待操作的目标对象是否在白名单中，如果不在白名单中，则所述待操作的目标对象是未知对象，触发所述规则判断模块继续判断所述待操作的目标对象是否
10 符合预置的匹配规则；如果在白名单中，则不需要导入沙箱。

优选地，所述判断模块还包括：黑名单判断模块，设置为判断所述待操作的目标对象是否在黑名单中，如果在黑名单中，则触发所述执行模块将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行；如果不在黑名单中，则触发所述规则判断模块继续判断所述待操作的目标对象是否
15 符合预置的匹配规则。

优选地，所述规则判断模块设置为：当所述待操作的目标对象为目标程序和/或目标文件时，根据所述目标对象的信息，判断所述目标对象是否符合预置的匹配规则；和/或，根据所述目标对象的来源程序的信息，判断所述目标对象是否符合预置的匹配规则；

20 其中，所述目标对象的信息包括以下至少之一：目标对象的文件路径、加密数据、文件属性、图标特征值、文件特征值、下载来源；所述来源程序的信息包括以下至少之一：来源程序的文件路径、加密数据、文件属性、图标特征值、文件特征值、下载来源；

当所述待操作的目标对象为用户输入的信息时，判断所述用户输入的信息
25 是否符合预置的匹配规则。

优选地，所述装置还包括：提示模块，设置为在所述执行模块确定需要导入沙箱之后，将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行之前，弹出提示窗提示用户是否导入沙箱；并根据所述用户的肯定

输入调用所述执行模块将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行。

本申请还提供了一种安全浏览器，包括如上所述的利用沙箱进行防御的装置。

5

与现有技术相比，本申请包括以下优点：

首先，本申请提供了一种智能判定的方法，可以在用户对目标对象执行操作之前，自动判断所述目标对象的执行是否需要导入沙箱，由此带来以下优点：

10 第一，可以帮助用户决定哪些有风险的程序需要在沙箱内运行，而不需要用户自行判断；

第二，避免将安全无风险的程序放置沙箱内运行导致用户数据的丢失；

第三，无需用户的参与，因此不影响用户的操作，易用性高。

其次，本申请所述的目标对象不仅可以是目标程序，还可以是目标文件
15 或用户输入的信息。因此，本申请不仅可以对一些软件程序进行自动判断，还可以对图片等文件的执行是否安全进行自动判断，而且还可以对用户输入的网址、关键词等信息进行自动判断，如果网址或关键词是某电影网站，则打开一个新的浏览器在沙箱内去浏览这个网站。

附图说明

20 图 1 是本申请实施例所述一种利用沙箱进行防御的方法流程图；

图 2 是本申请优选实施例所述一种利用沙箱进行防御的方法流程图；

图 3 是本申请优选实施例所述一种利用沙箱进行防御的装置结构图。

具体实施方式

为使本申请的上述目的、特征和优点能够更加明显易懂，下面结合附图
25 和具体实施方式对本申请作进一步详细的说明。

对于采用了沙箱技术的系统，本申请提供了一种智能判定的方法，可以

在用户对目标对象执行操作之前，自动判断所述目标对象的执行是否需要导入沙箱，从而帮助用户决定哪些有风险的程序需要在沙箱内运行。

下面通过实施例进行详细说明。

5 参照图 1，是本申请实施例所述一种利用沙箱进行防御的方法流程图。

步骤 101，在对目标对象执行操作之前，触发以下防御步骤；

步骤 102，对待操作的目标对象，自动判断所述目标对象的执行是否需要导入沙箱；

如果是，则执行步骤 103；如果否，则执行步骤 104。

10 步骤 103，如果需要导入沙箱，则在沙箱中完成该目标对象的执行。

步骤 104，如果不需要导入沙箱，则在沙箱外完成该目标对象的执行。

即按照正常的处理流程执行该目标对象。

15 优选地，如果所述待操作的目标对象的执行需要导入沙箱，则导入沙箱之前，还可以弹出提示窗提示用户是否导入沙箱，以方便用户根据自动判断的结果进行自由选择。

上述实施例中，所述目标对象包括但不限于目标程序、目标文件和用户输入的信息。下面分别进行详细说明。

(1) 目标程序

20 所述目标程序通常指可执行文件，如电子书、在线播放器、序号生成器等。

用户可通过多种方式触发步骤 102 的执行，触发方式包括但不限于：将目标程序下载到客户端后，通过双击或在右键菜单中点击“打开”等方式在客户端运行该目标程序之前，可触发步骤 102 进行自动判断，从而防止恶意程序的运行破坏系统；和/或，在下载目标程序之前进行触发，从而在将恶意程序下载到客户端之前就提前进行了防御。此外，对于一些可在线运行的目标程序，也可以在运行之前触发防御保护。总之，在对目标程序的任何操作之前都可进行自动判断，以保护系统的安全性。

对于判断为需要导入沙箱执行的目标程序，所述在沙箱中完成该目标程

序的执行是指：将该目标程序导入沙箱，在沙箱中完成该目标程序的运行。
例如，对于某网站上的色情播放器，将该播放器放入沙箱中运行。

(2) 目标文件

所述目标文件通常指图片等不可执行文件，这种目标文件的执行需要由
5 关联程序完成。例如，对于图片，需要启动图片浏览器来浏览，所述图片浏览器即为该图片文件的关联程序。

对于判断为需要导入沙箱执行的目标文件，所述在沙箱中完成该目标文件的执行是指：将执行该目标文件的关联程序导入沙箱，在沙箱中由所述关联程序运行该目标文件。例如，对于不可信的图片文件，可以将图片浏览器
10 导入沙箱来打开该图片。

针对目标文件，用户也可通过多种方式触发步骤 102 的执行，触发方式包括但不限于：将所述目标文件或执行该目标文件的关联程序下载到客户端后，在客户端运行该目标文件之前进行触发；和/或，在下载所述目标文件或在线执行该目标文件的关联程序之前进行触发。总之，在对目标文件的任何
15 操作之前都可进行自动判断，以保护系统的安全性。

(3) 用户输入的信息

用户输入的信息包括用户输入的网址、关键词等信息。

如果所述目标对象为用户输入的信息，则通常在用户输入所述信息时触发步骤 102 进行安全防御，即判断用户输入的网址、关键词等信息是否安全
20 可信，如果不可信，则执行步骤 103。

对于判断为需要导入沙箱执行的用户输入信息，所述在沙箱中完成该用户输入信息的执行是指：将接收该用户输入信息的关联程序导入沙箱，在沙箱中根据该用户输入信息运行所述关联程序。例如，对于存在可疑的网址，在沙箱中新打开一个浏览器来链接到该网址对应的网站，所述浏览器程序即
25 为接收网址输入的关联程序。

结合上述 (1)、(2)、(3)，无论用户要操作的目标对象是哪一种，图 1 所示方法都可以自动判断其执行是否需要导入沙箱。本申请实施例提供的自动判断方法包括但不限于：判断所述待操作的目标对象是否符合预置的匹配

规则，如果符合，则所述待操作的目标对象的执行需要导入沙箱；如果不符合，则不需要导入沙箱。

具体而言，所述判断可以是：查询预置的数据库，将所述待操作的目标对象与该数据库中的预置规则进行比较，如果在该数据库中查询到，则符合匹配规则；如果未查询到，则不符合匹配规则。即数据库中存储了各种判断的规则，或者直接存储了符合匹配规则的对象特征，如果在数据库中查询到所述待操作的目标对象，则表明该目标对象的执行需要导入沙箱。

针对不同的目标对象，相对应的匹配规则也不同：

1) 当所述待操作的目标对象为目标程序和/或目标文件时，判断所述待操作的目标对象是否符合预置的匹配规则，包括：判断所述目标对象的相关信息是否符合预置的匹配规则；和/或，判断所述目标对象的来源程序的相关信息是否符合预置的匹配规则。

其中，所述目标对象的相关信息包括：

目标对象的文件路径，和/或

目标对象的加密数据（如 MD5），和/或

目标对象的文件属性（如产品名称、版本信息、签名发行者、文件大小等），和/或

目标对象的图标特征值（如图标哈希值），和/或

目标对象的文件特征值（如文件哈希值），和/或

目标对象的下载来源（如从哪个网站下载）；

也即，目标对象的相关信息包括上述信息中的至少一个。

相应地，所述来源程序的相关信息包括：

来源程序的文件路径，和/或

来源程序的加密数据（如 MD5），和/或

来源程序的文件属性（如产品名称、版本信息、签名发行者、文件大小等），和/或

来源程序的图标特征值（如图标哈希值），和/或

来源程序的文件特征值（如文件哈希值），和/或

来源程序的下载来源（如从哪个网站下载）；

也即，来源程序的相关信息包括上述信息中的至少一个。

基于上述目标对象的相关信息和来源程序的相关信息，所述匹配规则可以是：

5 例 1：对于网站上的色情播放器，匹配规则如下：

来源程序为：浏览器程序或资源管理器；

目标的文件名：包含“日本 AV”或“情色”...

目标的文件图标：为特定播放器图标；

目标的文件大小：可以限制在一个范围，比如：1MB~10MB；

10 目标的文件描述：比如 xxxx 成人播放器，xxxx 专用播放器。

即符合上述规则的播放器即判定为色情播放器。

例 2：对于未知有风险的电子书，匹配规则如下：

目标文件名称：包含“电子书”的关键字；

目标文件图标的特征值包含：电子书的图标的特征。

15 对于符合上述规则的电子书判定为有风险的电子书。

例 3：对于未知有风险的序号生成器，匹配规则如下：

目标文件名称：有包含“序号生成器”或“keygen”或“cracker”或“破解机”的关键字；

目标文件图标的特征值包含：序号生成器的图标的特征。

20 对符合上述规则的序号生成器可判断为有风险的序号生成器。

除上述列举的几种匹配规则之外，还可以有其他的多种规则，如进行模糊匹配或全文匹配，优先进行文件名称的匹配，等等，视具体应用而定，在此不再一一列举。

2) 当所述待操作的目标对象为用户输入的信息时，判断所述待操作的目标对象是否符合预置的匹配规则，包括：判断所述用户输入的信息是否符合预置的匹配规则。

例如，判断用户输入的网址是否为一些色情网站的网址，或者判断用户输入的关键词是否包含“日本 AV”或“情色”等信息。通过用户输入的信

息,就可以预先判断出用户下一步要浏览的网站或要搜索的网页是否需要放入沙箱。

基于上述列举的各种匹配规则,优选地,在对目标对象进行上述匹配规则的自动判断之前,还可以优先进行如下的自动判断,列举如下:

- 5 1) 在判断所述待操作的目标对象是否符合预置的匹配规则之前:

创建用于自动判断所述目标对象的执行的进程;

判断所述进程的父进程是否在沙箱内,如果是,则所述待操作的目标对象的执行需要导入沙箱;如果否,则继续判断所述待操作的目标对象是否符合预置的匹配规则。

- 10 即如果所述用于自动判断目标对象的执行的进程存在父进程,则该用于自动判断的进程称为子进程。如果父进程已导入沙箱中,说明该父进程不可信,那么该父进程调用的子进程也是不可信的,所以子进程也应该导入沙箱执行。

- 2) 判断所述待操作的目标对象是否符合预置的匹配规则之前:

- 15 判断用户是否选择将所述待操作的目标对象的执行导入沙箱,如果是,则所述待操作的目标对象的执行需要导入沙箱;如果否,则继续判断所述待操作的目标对象是否符合预置的匹配规则。

即用户可参与选择是否放入沙箱,如果用户已主动选择放入沙箱,则不需要进行匹配规则的自动判断。

- 20 3) 判断所述待操作的目标对象是否符合预置的匹配规则之前:

判断所述待操作的目标对象是否在白名单中,如果不在白名单中,则所述待操作的目标对象是未知对象,继续判断所述待操作的目标对象是否符合预置的匹配规则;如果在白名单中,则不需要导入沙箱。

- 25 所述白名单中列出了比较安全的目标对象,白名单中的目标对象可以不导入沙箱而直接执行。如果待操作的目标对象在所述白名单中,则可以免除匹配规则的自动判断。如果待操作的目标对象不在所述白名单中,表明所述待操作的目标对象是未知对象,还需要进一步进行自动判断。

- 4) 判断所述待操作的目标对象是否符合预置的匹配规则之前:

判断所述待操作的目标对象是否在黑名单中，如果在黑名单中，则所述待操作的目标对象的执行需要导入沙箱；如果不在黑名单中，则继续判断所述待操作的目标对象是否符合预置的匹配规则。

5 所述黑名单中列出了一定不可信的目标对象，如果待操作的目标对象在所述黑名单中，则直接导入沙箱执行；但如果不在黑名单中，也不能排除所述待操作的目标对象一定安全，因此还需要继续进行匹配规则的判断。

在实际应用中，如果待操作的目标对象在黑名单中，也可以直接进行拦截而不放入沙箱，这些都可以由用户进行选择。

10 上述 1) 至 4) 可以单独在匹配规则的判断之前使用，也可以组合起来在匹配规则的判断之前使用。

基于上述内容，在实际应用中，本申请实施例还提供了以下两种实现方式：

第一种，根据客户端的请求，由服务器端自动判断所述待操作的目标对象的执行是否需要导入沙箱。

15 具体来说，服务器端存储了自动判断的各种规则，如果待操作的目标程序或目标文件已经下载到了客户端，在用户点击执行时，客户端会将要进行判断的请求发给服务器，由服务器进行自动判断。或者，从服务器上下载目标程序或目标文件之前，服务器根据客户端的下载请求，判断是否导入沙箱下载。或者，在用户输入网址、关键词时，服务器根据用户的输入进行自动
20 判断。

第二种，由客户端自动判断所述待操作的目标对象的执行是否需要导入沙箱。

这种情况下，客户端存储了自动判断的各种规则，并定期从服务器上更新，客户端可在用户对目标对象进行操作之前进行自动判断。

25 综上所述，上述实施例提供了一种智能判定的方法，可以在用户对目标对象执行操作之前，自动判断所述目标对象的执行是否需要导入沙箱，由此带来以下优点：

第一，可以帮助用户决定哪些有风险的程序需要在沙箱内运行，而不需

要用户自行判断;

第二, 避免将安全无风险的程序放置沙箱内运行导致用户数据的丢失;

第三, 无需用户的参与, 因此不影响用户的操作, 易用性高。

5 基于上述内容, 本申请还提供了图 2 所示的优选实施例。

参照图 2, 是本申请优选实施例所述一种利用沙箱进行防御的方法流程图。

以目标对象是目标程序为例, 目标对象是目标文件和用户输入信息的情况与此类似, 不再详述。

10 整个待操作的目标程序自动进入沙箱的判断流程如下:

步骤 201, 创建进程;

步骤 202, 判断父进程是否在沙箱内;

如果父进程在沙箱内, 则跳转到步骤 208;

如果父进程不在沙箱内, 则继续步骤 203。

15 步骤 203, 判断用户是否选择将所述待操作的目标程序的执行导入沙箱;

如果用户已选择将所述待操作的目标程序的执行导入沙箱, 则跳转到步骤 208;

如果用户未选择将所述待操作的目标程序的执行导入沙箱, 则继续步骤 204。

20 步骤 204, 判断所述待操作的目标程序是否在白名单中;

如果在白名单中, 则跳转到步骤 209;

如果不在白名单中, 则是未知程序, 继续步骤 205。

步骤 205, 判断所述待操作的目标对象是否在黑名单中;

如果在黑名单中, 则跳转到步骤 208;

25 如果不在黑名单中, 则继续步骤 206。

步骤 206, 判断所述目标程序是否为特定类型的程序;

即根据各种匹配规则判断是否为特定类型的程序;

如果是, 则继续步骤 207;

如果不是，则跳转到步骤 209。

步骤 207，弹出提示窗提示用户该目标程序将导入沙箱内执行；

如果用户选择导入，则将该目标程序加入沙箱运行列表。

5 步骤 208，开始将目标程序的文件/注册表的写入、删除、修改等操作动作导向沙箱中，判断流程结束。

步骤 209，将目标程序在一般环境下运行(非沙箱模式)，判断流程结束。

需要说明的是，上述步骤 203 至步骤 205 的顺序也可以更换，但都需要在步骤 206 之前。

10 需要说明的是，对于前述的各方法实施例，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，本申请并不受所描述的动作顺序的限制，因为依据本申请，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，所涉及的动作和模块并不一定是本申请所必须的。

15 基于上述内容，本申请还提供了相应的装置实施例，如图 3 所示。

参照图 3，是本申请优选实施例所述一种利用沙箱进行防御的装置结构图。

所述装置可以包括以下模块：

20 判断模块 31，设置为在对目标对象执行操作之前，自动判断待操作的目标对象的执行是否需要导入沙箱；

执行模块 32，设置为若判断模块 31 的判断结果为需要导入沙箱，则将目标对象导入沙箱并在沙箱中完成该目标对象的执行；如果否，则可以在沙箱外完成该目标对象的执行。

25 其中，所述目标对象包括但不限于：目标程序，目标文件，用户输入的信息。

执行模块 32 在将目标对象导入沙箱并在沙箱中完成该目标对象的执行时：

如果所述目标对象为目标程序，则所述执行模块 32 将该目标程序导入

沙箱，在沙箱中完成该目标程序的运行；

如果所述目标对象为目标文件，则所述执行模块 32 将执行该目标文件的关联程序导入沙箱，在沙箱中由所述关联程序运行该目标文件；

如果所述目标对象为用户输入的信息，则所述执行模块 32 将接收该用户输入信息的关联程序导入沙箱，在沙箱中根据该用户输入信息运行所述关联程序；所述用户输入的信息包括网址和/或关键词。

优选地，判断模块 31 设置为：如果所述目标对象为目标程序，则所述判断模块 31 将所述目标程序下载到客户端后在客户端运行该目标程序之前，自动判断待操作的所述目标对象的执行是否需要导入沙箱；和/或，在下载所述目标程序之前，自动判断待操作的所述目标对象的执行是否需要导入沙箱；

如果所述目标对象为目标文件，则所述判断模块 31 将所述目标文件或执行该目标文件的关联程序下载到客户端后在客户端运行该目标文件之前，自动判断待操作的所述目标对象的执行是否需要导入沙箱；和/或，在下载所述目标文件或在线执行该目标文件的关联程序之前，自动判断待操作的所述目标对象的执行是否需要导入沙箱；

如果所述目标对象为用户输入的信息，则所述判断模块 31 在用户输入所述信息时，自动判断待操作的所述目标对象的执行是否需要导入沙箱。

进一步，所述判断模块 31 可以包括：

规则判断模块 311，设置为在对目标对象执行操作之前，判断所述待操作的目标对象是否符合预置的匹配规则，如果符合，则所述待操作的目标对象的执行需要导入沙箱；如果不符合，则不需要导入沙箱。

进一步，当所述待操作的目标对象为目标程序和/或目标文件时，所述规则判断模块 311 判断所述目标对象的相关信息是否符合预置的匹配规则；和/或，判断所述目标对象的来源程序的相关信息是否符合预置的匹配规则；

其中，所述目标对象的相关信息包括目标对象的文件路径、和/或加密数据、和/或文件属性、和/或图标特征值、和/或文件特征值、和/或下载来源，即，上述信息中的至少一个；所述来源程序的相关信息包括来源程序的文件

路径、和/或加密数据、和/或文件属性、和/或图标特征值、和/或文件特征值、和/或下载来源，即，上述信息中的至少一个；

当所述待操作的目标对象为用户输入的信息时，所述规则判断模块 311 判断所述用户输入的信息是否符合预置的匹配规则。

5 优选地，所述判断模块 31 还可以包括：

父进程判断模块 312，设置为在规则判断模块判 311 断所述待操作的目标对象是否符合预置的匹配规则之前，创建用于自动判断所述目标对象的执行的进程后，判断所述进程的父进程是否在沙箱内，如果是，则所述待操作的目标对象的执行需要导入沙箱，触发所述执行模块 32 将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行；如果否，则触发所述规则判断模块 311 继续判断所述待操作的目标对象是否符合预置的匹配规则。

优选地，所述判断模块 31 还可以包括：

15 用户选择判断模块 313，设置为判断用户是否选择将所述待操作的目标对象的执行导入沙箱，如果是，则所述待操作的目标对象的执行需要导入沙箱，触发所述执行模块 32 将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行；如果否，则触发所述规则判断模块 311 继续判断所述待操作的目标对象是否符合预置的匹配规则。

优选地，所述判断模块 31 还可以包括：

20 白名单判断模块 314，设置为判断所述待操作的目标对象是否在白名单中，如果不在白名单中，则所述待操作的目标对象是未知对象，触发所述规则判断模块 311 继续判断所述待操作的目标对象是否符合预置的匹配规则；如果在白名单中，则不需要导入沙箱。

优选地，所述判断模块 31 还可以包括：

25 黑名单判断模块 315，设置为判断所述待操作的目标对象是否在黑名单中，如果在黑名单中，则所述待操作的目标对象的执行需要导入沙箱，触发所述执行模块 32 将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行；如果不在黑名单中，则触发所述规则判断模块 311 继续判断所述待操作的目标对象是否符合预置的匹配规则。

优选地，所述装置还可以包括：

提示模块 33，设置为在所述执行模块 32 确定需要导入沙箱之后，将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行之前，弹出提示窗提示用户是否导入沙箱；并根据所述用户的肯定输入调用所述执行模块 32 将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行。

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。

上述利用沙箱技术进行防御的装置可以部署在服务器端，也可以部署在客户端，在用户对目标对象执行操作之前，自动判断所述目标对象的执行是否需要导入沙箱，帮助用户决定哪些有风险的程序需要在沙箱内运行，避免将安全无风险的程序放置沙箱内运行导致用户数据的丢失，而且由于无需用户的参与，因此不影响用户的操作，易用性高。

基于上述的利用沙箱技术进行防御的装置，本申请实施例还提供了一种安全浏览器，该浏览器包括如上述图 3 实施例所述的用沙箱技术进行系统防御的装置，并可采用图 1 或图 2 所述的方法自动判断待操作的目标对象的执行是否需要导入沙箱。具体描述可参见上述图 1、图 2 和图 3 的相关内容，不再详述。

另外，基于本申请的利用沙箱技术进行防御的方法，本申请实施例还提供了一种在其上记录有执行本申请的利用沙箱技术进行防御的方法的程序的计算机可读记录介质。所述计算机可读记录介质包括用于以计算机可读的形式存储或传送信息的任何机制。例如，机器可读介质包括只读存储器（ROM）、随机存取存储器（RAM）、磁盘存储介质、光存储介质、闪速存储介质、电、光、声或其他形式的传播信号等（例如，载波、红外信号、数据信号等）。

本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。

最后，还需要说明的是，在本文中，诸如第一和第二等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，上文中的“和/或”表示本文既包含了“和”的关系，也包含了“或”
5 的关系，其中：如果方案 A 与方案 B 是“和”的关系，则表示某实施例中可以同时包括方案 A 和方案 B；如果方案 A 与方案 B 是“或”的关系，则表示某实施例中可以单独包括方案 A，或者单独包括方案 B。

以上对本申请所提供的一种利用沙箱进行防御的方法、装置及安全浏览器，进行了详细介绍，本文中应用了具体个例对本申请的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本申请的方法及其核心思想；
10 同时，对于本领域的一般技术人员，依据本申请的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本申请的限制。

权 利 要 求 书

1、一种利用沙箱进行防御的方法，包括：

在对目标对象执行操作之前，自动判断待操作的所述目标对象的执行是否需要导入沙箱；

若确定需要导入沙箱，则将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行。

2、根据权利要求 1 所述的方法，其中，将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行的步骤包括：

如果所述目标对象为目标程序，则将该目标程序导入沙箱，在沙箱中完成该目标程序的运行；

或者，如果所述目标对象为目标文件，则将执行该目标文件的关联程序导入沙箱，在沙箱中由所述关联程序运行该目标文件；

或者，如果所述目标对象为用户输入的信息，则将接收该用户输入信息的关联程序导入沙箱，在沙箱中根据该用户输入信息运行所述关联程序；所述用户输入的信息包括网址和/或关键词。

3、根据权利要求 2 所述的方法，其中，所述在对目标对象执行操作之前，自动判断待操作的所述目标对象的执行是否需要导入沙箱的步骤包括：

如果所述目标对象为目标程序，则将所述目标程序下载到客户端后，在客户端运行该目标程序之前，自动判断待操作的所述目标对象的执行是否需要导入沙箱；和/或，在下载所述目标程序之前，自动判断待操作的所述目标对象的执行是否需要导入沙箱；

或者，如果所述目标对象为目标文件，则将所述目标文件或执行该目标文件的关联程序下载到客户端后，在客户端运行该目标文件之前，自动判断待操作的所述目标对象的执行是否需要导入沙箱；和/或，在下载所述目标文件或在线执行该目标文件的关联程序之前，自动判断待操作的所述目标对象的执行是否需要导入沙箱；

或者，如果所述目标对象为用户输入的信息，则在用户输入所述信息时，自动判断待操作的所述目标对象的执行是否需要导入沙箱。

4、根据权利要求 1 至 3 任一所述的方法，其中，所述自动判断待操作

的所述目标对象的执行是否需要导入沙箱的步骤包括:

判断所述待操作的目标对象是否符合预置的匹配规则, 如果符合, 则所述待操作的目标对象的执行需要导入沙箱; 如果不符合, 则不需要导入沙箱。

5 5、根据权利要求 4 所述的方法, 其中, 在判断所述待操作的目标对象是否符合预置的匹配规则的步骤之前, 还包括: 创建用于自动判断所述目标对象的执行的进程;

判断所述进程的父进程是否在沙箱内, 如果是, 则执行所述将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行的步骤; 如果否, 则继续所述判断所述待操作的目标对象是否符合预置的匹配规则的步骤。

10 6、根据权利要求 4 所述的方法, 其中, 在所述判断所述待操作的目标对象是否符合预置的匹配规则的步骤之前, 还包括:

判断用户是否选择将所述待操作的目标对象的执行导入沙箱, 如果是, 则执行所述将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行的步骤; 如果否, 则继续所述判断所述待操作的目标对象是否符合预置的匹配规则的步骤。
15

7、根据权利要求 4 所述的方法, 其中, 在判断所述待操作的目标对象是否符合预置的匹配规则的步骤之前, 还包括:

判断所述待操作的目标对象是否在白名单中, 如果不在白名单中, 则所述待操作的目标对象是未知对象, 继续所述判断所述待操作的目标对象是否符合预置的匹配规则的步骤; 如果在白名单中, 则不需要将所述待操作的目标对象导入沙箱。
20

8、根据权利要求 4 所述的方法, 其中, 在判断所述待操作的目标对象是否符合预置的匹配规则的步骤之前, 还包括:

判断所述待操作的目标对象是否在黑名单中, 如果在黑名单中, 则执行所述将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行的步骤; 如果不在黑名单中, 则继续所述判断所述待操作的目标对象是否符合预置的匹配规则的步骤。
25

9、根据权利要求 4 所述的方法, 其中, 判断所述待操作的目标对象是

是否符合预置的匹配规则的步骤包括:

查询预置的数据库,将所述待操作的目标对象与该数据库中的预置规则进行比较,如果在该数据库中查询到,则符合匹配规则;如果未查询到,则不符合匹配规则。

- 5 10、根据权利要求4所述的方法,其中,当所述待操作的目标对象为目标程序和/或目标文件时,所述判断所述待操作的目标对象是否符合预置的匹配规则的步骤包括:

根据所述目标对象的信息,判断所述目标对象是否符合预置的匹配规则;

- 10 和/或,根据所述目标对象的来源程序的信息,判断所述目标对象是否符合预置的匹配规则。

11、根据权利要求10所述的方法,其中,

所述目标对象的信息包括以下至少之一:目标对象的文件路径、加密数据、文件属性、图标特征值、文件特征值、下载来源;

- 15 所述来源程序的信息包括以下至少之一:来源程序的文件路径、加密数据、文件属性、图标特征值、文件特征值、下载来源。

12、根据权利要求4所述的方法,其中,当所述待操作的目标对象为用户输入的信息时,所述判断所述待操作的目标对象是否符合预置的匹配规则的步骤包括:

- 20 判断所述用户输入的信息是否符合预置的匹配规则。

13、根据权利要求1至3任一所述的方法,其中,所述自动判断待操作的所述目标对象的执行是否需要导入沙箱的步骤包括:

根据客户端的请求,由服务器端自动判断所述待操作的目标对象的执行是否需要导入沙箱;

- 25 和/或,由客户端自动判断所述待操作的目标对象的执行是否需要导入沙箱。

14、根据权利要求1至3任一所述的方法,其中,在确定需要导入沙箱之后,将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行

之前,还包括:

弹出提示窗提示用户是否导入沙箱;根据所述用户的肯定输入执行所述将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行的步骤。

5 15、一种利用沙箱进行防御的装置,包括:

判断模块,设置为在对目标对象执行操作之前,自动判断待操作的所述目标对象的执行是否需要导入沙箱;

执行模块,设置为若所述判断模块的判断结果为需要导入沙箱,则将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行。

10 16、根据权利要求 15 所述的装置,其中,所述执行模块在将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行时,

如果所述目标对象为目标程序,则将该目标程序导入沙箱,在沙箱中完成该目标程序的运行;

15 或者,如果所述目标对象为目标文件,则将执行该目标文件的关联程序导入沙箱,在沙箱中由所述关联程序运行该目标文件;

或者,如果所述目标对象为用户输入的信息,则将接收该用户输入信息的关联程序导入沙箱,在沙箱中根据该用户输入信息运行所述关联程序;所述用户输入的信息包括网址和/或关键词。

17、根据权利要求 16 所述的装置,其中,所述判断模块,设置为:

20 如果所述目标对象为目标程序,则将所述目标程序下载到客户端后,在客户端运行该目标程序之前,自动判断待操作的所述目标对象的执行是否需要导入沙箱;和/或,在下载所述目标程序之前,自动判断待操作的所述目标对象的执行是否需要导入沙箱;

25 或者,如果所述目标对象为目标文件,则将所述目标文件或执行该目标文件的关联程序下载到客户端后,在客户端运行该目标文件之前,自动判断待操作的所述目标对象的执行是否需要导入沙箱;和/或,在下载所述目标文件或在线执行该目标文件的关联程序之前,自动判断待操作的所述目标对象的执行是否需要导入沙箱;

或者,如果所述目标对象为用户输入的信息,则在用户输入所述信息时,自动判断待操作的所述目标对象的执行是否需要导入沙箱。

18、根据权利要求 15 至 17 任一所述的装置,其中,所述判断模块包括:

5 规则判断模块,设置为在对目标对象执行操作之前,判断所述待操作的目标对象是否符合预置的匹配规则,如果符合,则所述待操作的目标对象的执行需要导入沙箱;如果不符合,则不需要导入沙箱。

19、根据权利要求 18 所述的装置,其中,所述判断模块还包括:

父进程判断模块,设置为在所述规则判断模块判断所述待操作的目标对象是否符合预置的匹配规则之前,创建用于自动判断所述目标对象的执行的
10 进程后,判断所述进程的父进程是否在沙箱内,如果是,则触发所述执行模块将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行;如果否,则触发所述规则判断模块继续判断所述待操作的目标对象是否符合预置的匹配规则。

20、根据权利要求 18 所述的装置,其中,所述判断模块还包括:

15 用户选择判断模块,设置为判断用户是否选择将所述待操作的目标对象的执行导入沙箱,如果是,则触发所述执行模块将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行;如果否,则触发所述规则判断模块继续判断所述待操作的目标对象是否符合预置的匹配规则。

21、根据权利要求 18 所述的装置,其中,所述判断模块还包括:

20 白名单判断模块,设置为判断所述待操作的目标对象是否在白名单中,如果不在白名单中,则所述待操作的目标对象是未知对象,触发所述规则判断模块继续判断所述待操作的目标对象是否符合预置的匹配规则;如果在白名单中,则不需要将所述待操作的目标对象导入沙箱。

22、根据权利要求 18 所述的装置,其中,所述判断模块还包括:

25 黑名单判断模块,设置为判断所述待操作的目标对象是否在黑名单中,如果在黑名单中,则触发所述执行模块将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行;如果不在黑名单中,则触发所述规则判断模块继续判断所述待操作的目标对象是否符合预置的匹配规则。

23、根据权利要求 18 所述的装置，其中，所述规则判断模块设置为：

当所述待操作的目标对象为目标程序和/或目标文件时，根据所述目标对象的信息，判断所述目标对象是否符合预置的匹配规则；和/或，根据所述目标对象的来源程序的信息，判断所述目标对象是否符合预置的匹配规则；

5 其中，所述目标对象的信息包括以下至少之一：目标对象的文件路径、加密数据、文件属性、图标特征值、文件特征值、下载来源；所述来源程序的信息包括以下至少之一：来源程序的文件路径、加密数据、文件属性、图标特征值、文件特征值、下载来源；

10 当所述待操作的目标对象为用户输入的信息时，判断所述用户输入的信息是否符合预置的匹配规则。

24、根据权利要求 15 至 17 任一所述的装置，其中，所述装置还包括：

提示模块，设置为在所述执行模块确定需要导入沙箱之后，将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行之前，弹出提示窗提示用户是否导入沙箱；并根据所述用户的肯定输入调用所述执行模块将所述目标对象导入所述沙箱并在所述沙箱中完成该目标对象的执行。

25、一种安全浏览器，包括如上述权利要求 15 至 24 任一权利要求所述的利用沙箱进行防御的装置。

26、一种在其上记录有用于执行权利要求 1 至 14 任一权利要求所述方法的计算机可读记录介质。

20 27、一种安全浏览器，用于执行权利要求 1 至 14 任一权利要求所述的利用沙箱进行防御的方法。

说明书附图

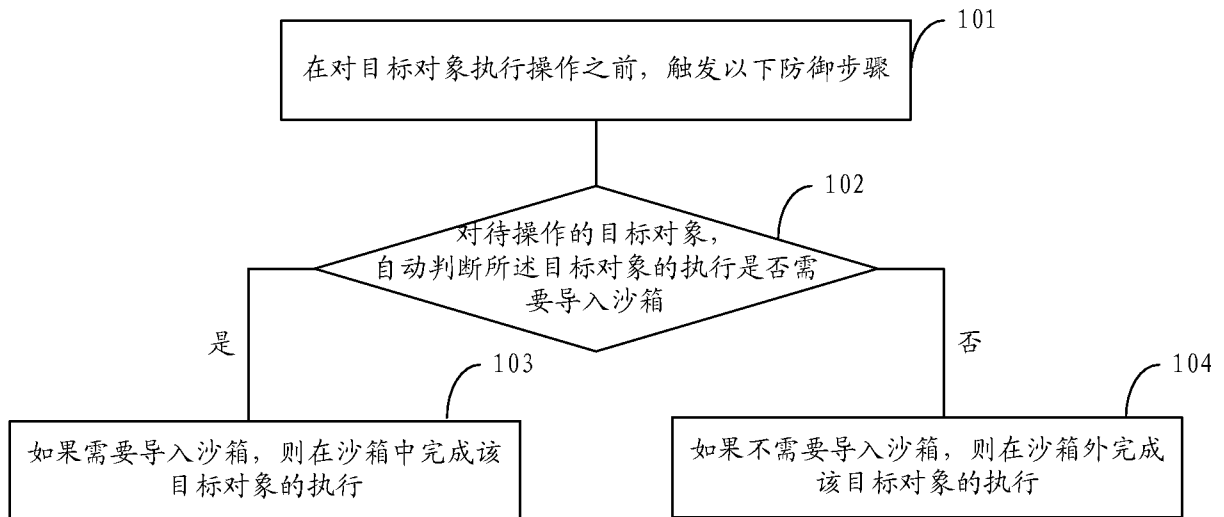


图 1

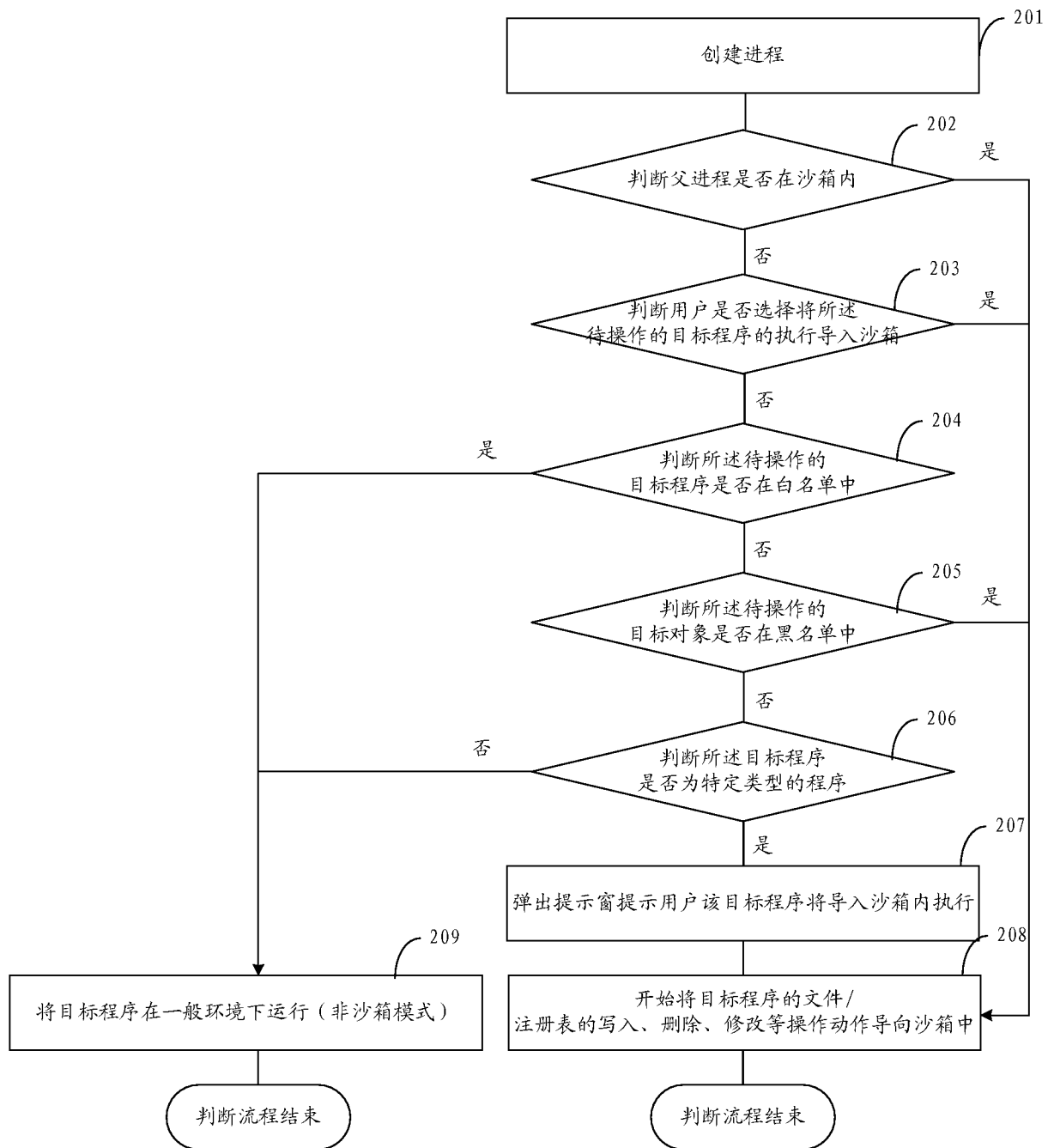


图 2

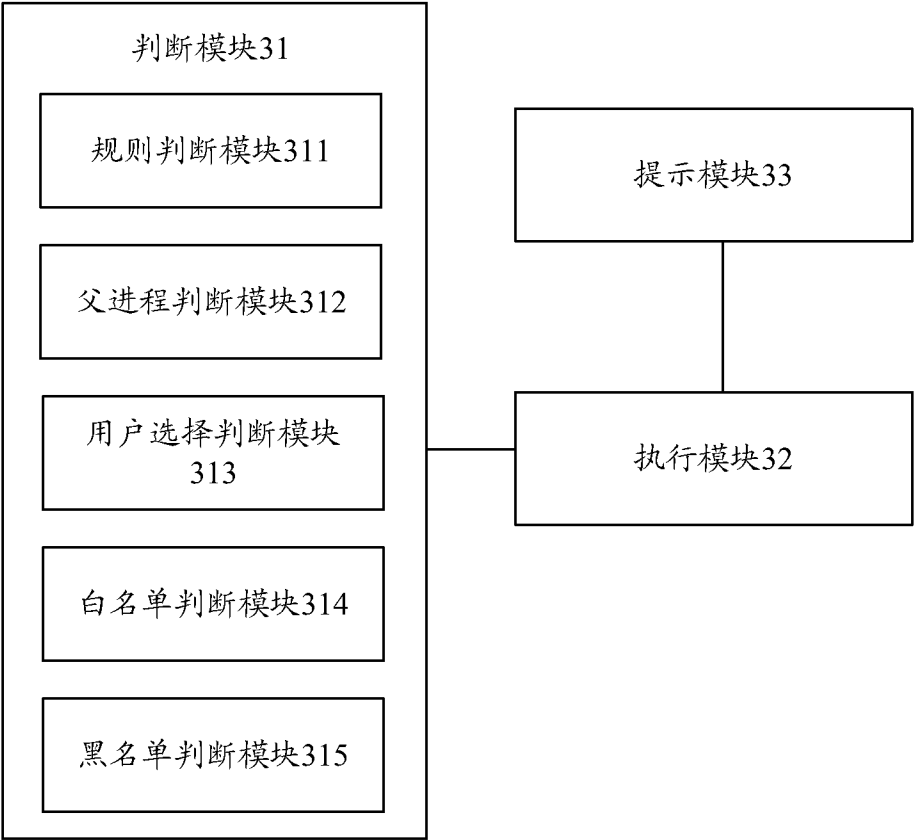


图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2012/074241

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/22 (2006.01) 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)

IPC: 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)

CNPAT; CNKI; WPI; EPODOC

sandbox+, sand box+, sand-box+, program+, software, component, plugin, plug-in, addin, add-in, addon, add-on, file,
automatic+, secur+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN1961272A (INTEL CORP) 09May2007 (09.05.2007) see the claims 32, 34, 36, 38, the description, page 5 lines 1-2, page 6 line 25 to page 7 line 24, page 8 lines 25-29, the figure 3	1-27
X	US2006161982A1 (CHARI Suresh N. et al.) 20Jul.2006 (20.07.2006) see the claims 1-2, 14-16, description, paragraph 23, the description abstract	1-27
X	WO2007113709A1 (KONINK PHILIPS ELECTRONICS NV) 11Oct.2007 (11.10.2007) see the claims 1-10	1-27
P, X	CN102184356A (BEIJING QIZHI SOFTWARE CO LTD OWN) 14Sep.2011 (14.09.2011) see the claims 1-25	1-27
A	WO2010065222A1 (MICROSOFT CORP) 10Jun.2010 (10.06.2010) see the whole document	1-27

☐ 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
12 Jun.2012 (12.06.2012)

Date of mailing of the international search report
05 Jul.2012 (05.07.2012)

Name and mailing address of the ISA
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
WU, Guangping
Telephone No. (86-10) 62411829

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2012/074241

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1961272A	09.05.2007	CN100533334C	26.08.2009
		US2006021029A1	26.01.2006
		WO2006012197A2	02.02.2006
		WO2006012197A3	06.04.2006
		EP1761836A2	14.03.2007
		JP2008500653A	10.01.2008
		JP4599400B2	15.12.2010
		US7908653B2	15.03.2011
US2006161982A1	20.07.2006	WO2006078446A2	27.07.2006
		WO2006078446A3	09.04.2009
		TW200641607A	01.12.2006
		WO2006078446A4	11.06.2009
WO2007113709A1	11.10.2007	NONE	
CN102184356A	14.09.2011	NONE	
WO2010065222A1	10.06.2010	US2010138639A1	03.06.2010
		CA2742121A1	10.06.2010
		EP2356578A1	17.08.2011
		MXPA11005834A	30.06.2011
		KR20110093816A	18.08.2011
		AU2009322881A1	10.06.2010
		CN102232217A	02.11.2011
		MX2011005834A	21.06.2011

A. 主题的分类		
G06F 21/22 (2006.01) 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)		
IPC: 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))		
CNPAT; CNKI; WPI; EPODOC		
沙箱, 沙盒, 程序, 软件, 组件, 构件, 插件, 文件, 自动, 安全, sandbox+, sand box+, sand-box+, program+, software, component, plugin, plug-in, addin, add-in, addon, add-on, file, automatic+, secur+		
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
X	CN1961272A (英特尔公司) 09.5 月 2007 (09.05.2007) 参见权利要求 32、34、36、38, 说明书第 5 页第 1-2 行、第 6 页第 25 行到第 7 页第 24 行、第 8 页第 25-29 行, 图 3	1-27
X	US2006161982A1 (CHARI Suresh N.等) 20.7 月 2006 (20.07.2006) 参见权利要求 1-2、14-16, 说明书第 23 段, 说明书摘要	1-27
X	WO2007113709A1 (KONINK PHILIPS ELECTRONICS NV) 11.10 月 2007 (11.10.2007) 参见权利要求 1-10	1-27
P, X	CN102184356A (奇智软件(北京)有限公司) 14.9 月 2011 (14.09.2011) 参见权利要求 1-25	1-27
A	WO2010065222A1 (MICROSOFT CORP) 10.6 月 2010 (10.06.2010) 参见全文	1-27
☐ 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 12.6 月 2012(12.06.2012)		国际检索报告邮寄日期 05.7 月 2012 (05.07.2012)
ISA/CN 的名称和邮寄地址: 中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号: (86-10)62019451		授权官员 吴广平 电话号码: (86-10) 62411829

国际检索报告

关于同族专利的信息

国际申请号

PCT/CN2012/074241

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN1961272A	09.05.2007	CN100533334C	26.08.2009
		US2006021029A1	26.01.2006
		WO2006012197A2	02.02.2006
		WO2006012197A3	06.04.2006
		EP1761836A2	14.03.2007
		JP2008500653A	10.01.2008
		JP4599400B2	15.12.2010
		US7908653B2	15.03.2011
US2006161982A1	20.07.2006	WO2006078446A2	27.07.2006
		WO2006078446A3	09.04.2009
		TW200641607A	01.12.2006
		WO2006078446A4	11.06.2009
WO2007113709A1	11.10.2007	无	
CN102184356A	14.09.2011	无	
WO2010065222A1	10.06.2010	US2010138639A1	03.06.2010
		CA2742121A1	10.06.2010
		EP2356578A1	17.08.2011
		MXPA11005834A	30.06.2011
		KR20110093816A	18.08.2011
		AU2009322881A1	10.06.2010
		CN102232217A	02.11.2011
		MX2011005834A	21.06.2011