(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103942488 B
(45)授权公告日 2017.06.23

(21)申请号 201410058386.1

(22)申请日 2011.04.21

(65)同一申请的已公布的文献号
申请公布号 CN 103942488 A

(43)申请公布日 2014.07.23

(62)分案原申请数据
201110100859.6 2011.04.21

(73)专利权人 北京奇虎科技有限公司
地址 100088 北京市西城区新街口外大街28号D座112室(德胜园区)
专利权人 奇智软件(北京)有限公司

(72)发明人 范纪鍠 潘剑锋 孙晓骏 路健华

(74)专利代理机构 北京润泽恒知识产权代理有限公司 11319
代理人 苏培华

(51)Int.Cl.
G06F 21/53(2013.01)

(56)对比文件
US 5974549 A,1999.10.26,摘要16-21行,图1,11.
US 2010/0138639 A1,2010.06.03,说明书第0022-0078段.
US 2003/0055991 A1,2003.03.20,全文.
CN 1961272 A,2007.05.09,说明书第6-9页,权利要求1.

审查员 陈玲

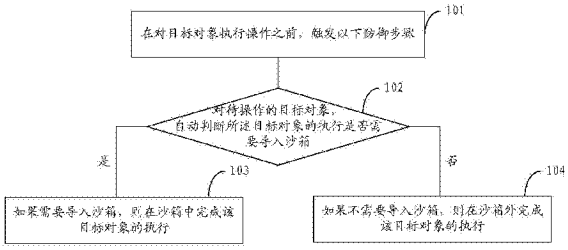
权利要求书3页 说明书11页 附图3页

(54)发明名称

利用沙箱技术进行防御的方法、装置及安全浏览器

(57)摘要

本发明提供了一种利用沙箱技术进行防御的方法、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。所述方法包括:在对目标对象执行操作之前,触发以下防御步骤: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,则在沙箱中完成该目标对象的执行;如果否,则在沙箱外完成该目标对象的执行。本发明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。



CN 103942488 B

1.一种利用沙箱技术进行防御的方法,其特征在于,包括:

在对目标对象执行操作之前,触发以下防御步骤:

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,则在沙箱中完成该目标对象的执行;如果否,则在沙箱外完成该目标对象的执行;

所述自动判断包括: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;

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:

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;

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;

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。

2.根据权利要求1所述的方法,其特征在于,当自动判断所述目标对象的执行需要导入沙箱时:

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。

3.根据权利要求2所述的方法,其特征在于,所述在对目标对象执行操作之前触发防御步骤,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触发防御步骤;和/或,在下载所述目标程序之前触发防御步骤;

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触发防御步骤;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触发防御步骤;

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触发防御步骤。

4.根据权利要求1所述的方法,其特征在于,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。

5.根据权利要求1所述的方法,其特征在于,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。

6.根据权利要求5所述的方法，其特征在于：

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；

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。

7.根据权利要求1所述的方法，其特征在于，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。

8.根据权利要求1至3任一所述的方法，其特征在于：

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。

9.根据权利要求1至3任一所述的方法，其特征在于，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。

10.一种利用沙箱技术进行防御的装置，其特征在于，包括：

判断触发模块，用于在对目标对象执行操作之前，触发自动判断模块；

自动判断模块，用于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，则在沙箱中完成该目标对象的执行；如果否，则在沙箱外完成该目标对象的执行；

所述自动判断包括：规则判断子模块，用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；

所述自动判断模块还包括：父进程判断子模块，用于在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；如果否，则触发所述规则判断子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；白名单判断子模块，用于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，触发所述规则判断子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，则不需要导入沙箱；黑名单判断子模块，用于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，则触发所述规则判断子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。

11.根据权利要求10所述的装置，其特征在于，当自动判断所述目标对象的执行需要导入沙箱时：

如果所述目标对象为目标程序，则所述自动判断模块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，则所述自动判断模块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，则所述自动判断模块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。

12.根据权利要求11所述的装置，其特征在于：

如果所述目标对象为目标程序，则所述判断触发模块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触发自动判断模块；和/或，在下载所述目标程序之前触发自动判断模块；

如果所述目标对象为目标文件，则所述判断触发模块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触发自动判断模块；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触发自动判断模块；

如果所述目标对象为用户输入的信息，则所述判断触发模块在用户输入所述信息时触发自动判断模块。

13.根据权利要求10所述的装置，其特征在于，所述自动判断模块还包括：

用户选择判断子模块，用于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，则触发所述规则判断子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。

14.根据权利要求10所述的装置，其特征在于：

当所述待操作的目标对象为目标程序和/或目标文件时，所述规则判断子模块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；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；

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

15.根据权利要求10至12任一所述的装置，其特征在于，还包括：

提示模块，用于当所述待操作的目标对象的执行需要导入沙箱时，在导入沙箱之前，弹出提示窗提示用户是否导入沙箱。

利用沙箱技术进行防御的方法、装置及安全浏览器

[0001] 本发明专利申请是申请日为2011年4月21日、申请号为201110100859.6、名称为“利用沙箱技术进行防御的方法、装置及安全浏览器”的中国发明专利申请的分案申请。

技术领域

[0002] 本发明涉及计算机安全技术领域，特别是涉及一种利用沙箱技术进行防御的方法、装置及一种安全浏览器。

背景技术

[0003] 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。

[0004] 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。

[0005] 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。

[0006] 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：

[0007] 第一，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；

[0008] 第二，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；

[0009] 第三，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。

发明内容

[0010] 本发明所要解决的技术问题是提供一种利用沙箱技术进行防御的方法、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。

[0011] 为了解决上述问题，本发明公开了一种利用沙箱技术进行防御的方法，包括：

[0012] 在对目标对象执行操作之前，触发以下防御步骤：

[0013] 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，则在沙箱中完成该目标对象的执行；如果否，则在沙箱外完成该目标对象的执行。

[0014] 其中，当自动判断所述目标对象的执行需要导入沙箱时：

[0015] 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；

[0016] 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；

[0017] 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。

[0018] 其中，所述在对目标对象执行操作之前触发防御步骤，包括：

[0019] 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触发防御步骤；和/或，在下载所述目标程序之前触发防御步骤；

[0020] 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触发防御步骤；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触发防御步骤；

[0021] 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触发防御步骤。

[0022] 优选的，所述自动判断包括：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。

[0023] 优选的，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：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。

[0024] 优选的，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。

[0025] 优选的，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；如果在白名单中，则不需要导入沙箱。

[0026] 优选的，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。

[0027] 优选的，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。

[0028] 优选的，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。

[0029] 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；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。

[0030] 优选的，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。

[0031] 优选的，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。

[0032] 优选的，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。

[0033] 本发明还提供了一种利用沙箱技术进行防御的装置，包括：

[0034] 判断触发模块，用于在对目标对象执行操作之前，触发所述自动判断模块；

[0035] 自动判断模块，用于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，则在沙箱中完成该目标对象的执行；如果否，则在沙箱外完成该目标对象的执行。

[0036] 其中，当自动判断所述目标对象的执行需要导入沙箱时：

[0037] 如果所述目标对象为目标程序，则所述自动判断模块将该目标程序导入沙箱，在沙箱中完成该目标程序的运行；

[0038] 如果所述目标对象为目标文件，则所述自动判断模块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；

[0039] 如果所述目标对象为用户输入的信息，则所述自动判断模块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。

[0040] 其中，如果所述目标对象为目标程序，则所述判断触发模块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触发自动判断模块；和/或，在下载所述目标程序之前触发自动判断模块；

[0041] 如果所述目标对象为目标文件，则所述判断触发模块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触发自动判断模块；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触发自动判断模块；

[0042] 如果所述目标对象为用户输入的信息，则所述判断触发模块在用户输入所述信息时触发自动判断模块。

[0043] 优选的，所述自动判断模块包括：规则判断子模块，用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。

[0044] 优选的，所述自动判断模块还包括：父进程判断子模块，用于在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；如果否，则触发所述规则判断子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。

[0045] 优选的，所述自动判断模块还包括：用户选择判断子模块，用于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，则触发所述规则判断子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。

[0046] 优选的，所述自动判断模块还包括：白名单判断子模块，用于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，触发所述规则判断子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，则不需要导入沙箱。

[0047] 优选的，所述自动判断模块还包括：黑名单判断子模块，用于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，则触发所述规则判断子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。

[0048] 优选的，当所述待操作的目标对象为目标程序和/或目标文件时，所述规则判断子模块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；

[0049] 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；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；

[0050] 当所述待操作的目标对象为用户输入的信息时，所述规则判断子模块判断所述用户输入的信息是否符合预置的匹配规则。

[0051] 优选的，所述装置还包括：提示模块，用于当所述待操作的目标对象的执行需要导入沙箱时，在导入沙箱之前，弹出提示窗提示用户是否导入沙箱。

[0052] 本发明还提供了一种安全浏览器，包括如上所述的利用沙箱技术进行防御的装置。

[0053] 与现有技术相比，本发明包括以下优点：

[0054] 首先，本发明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：

[0055] 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；

[0056] 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；

[0057] 第三，无需用户的参与，因此不影响用户的操作，易用性高。

[0058] 其次，本发明所述的目标对象不仅可以是目标程序，还可以是目标文件或用户输入的信息。因此，本发明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是，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

[0059] 图1是本发明实施例所述一种利用沙箱技术进行防御的方法流程图；

[0060] 图2是本发明优选实施例所述一种利用沙箱技术进行防御的方法流程图；

[0061] 图3是本发明优选实施例所述一种利用沙箱技术进行防御的装置结构图。

具体实施方式

[0062] 为使本发明的上述目的、特征和优点能够更加明显易懂，下面结合附图和具体实施方式对本发明作进一步详细的说明。

[0063] 对于采用了沙箱技术的系统，本发明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。

[0064] 下面通过实施例进行详细说明。

[0065] 参照图1，是本发明实施例所述一种利用沙箱技术进行防御的方法流程图。

[0066] 步骤101，在对目标对象执行操作之前，触发以下防御步骤；

[0067] 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；

[0068] 如果是，则执行步骤103；如果否，则执行步骤104。

[0069] 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。

[0070] 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。

[0071] 即按照正常的处理流程执行该目标对象。

[0072] 优选的，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。

[0073] 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。

[0074] (1)目标程序

[0075] 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。

[0076] 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。

[0077] 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。

[0078] (2)目标文件

[0079] 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。

[0080] 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，可以将图片浏览器导入沙箱来打开该图片。

[0081] 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操作之前都可进行自动判断，以保护系统的安全性。

[0082] (3)用户输入的信息

[0083] 用户输入的信息包括用户输入的网址、关键词等信息。

[0084] 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可信，如果不可信，则执行步骤103。

[0085] 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，所述浏览器程序即为接收网址输入的关联程序。

[0086] 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。本发明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。

[0087] 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的特征，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。

[0088] 针对不同的目标对象，相对应的匹配规则也不同：

[0089] 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。

[0090] 其中，所述目标对象的相关信息包括：

[0091] 目标对象的文件路径，和/或

[0092] 加密数据(如MD5)，和/或

[0093] 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

[0094] 图标特征值(如图标哈希值)，和/或

[0095] 文件特征值(如文件哈希值)，和/或

[0096] 下载来源(如从哪个网站下载)；

[0097] 相应的，所述来源程序的相关信息包括：

[0098] 来源程序的文件路径，和/或

[0099] 加密数据(如MD5)，和/或

[0100] 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

[0101] 图标特征值(如图标哈希值),和/或

[0102] 文件特征值(如文件哈希值),和/或

[0103] 下载来源(如从哪个网站下载)。

[0104] 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:

[0105] 例1:对于网站上的色情播放器,匹配规则如下:

[0106] 来源程序为:浏览器程序或资源管理器;

[0107] 目标的文件名:包含“日本AV”或“情色”…;

[0108] 目标的文件图标:为特定播放器图标;

[0109] 目标的文件大小:可以限制在一个范围,比如:1MB～10MB;

[0110] 目标的文件描述:比如xxxx成人播放器,xxxx专用播放器。

[0111] 即符合上述规则的播放器即判定为色情播放器。

[0112] 例2:对于未知有风险的电子书,匹配规则如下:

[0113] 目标文件名称:包含“电子书”的关键字;

[0114] 目标文件图标的特征值包含:电子书的图标的特征。

[0115] 对于符合上述规则的电子书判定为有风险的电子书。

[0116] 例3:对于未知有风险的序号生成器,匹配规则如下:

[0117] 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;

[0118] 目标文件图标的特征值包含:序号生成器的图标的特征。

[0119] 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。

[0120] 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。

[0121] 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。

[0122] 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。

[0123] 基于上述列举的各种匹配规则,优选的,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:

[0124] 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:

[0125] 创建用于自动判断所述目标对象的执行的进程;

[0126] 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。

[0127] 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。

[0128] 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:

[0129] 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。

[0130] 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。

[0131] 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：

[0132] 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。

[0133] 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，标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。

[0134] 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：

[0135] 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。

[0136] 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。

[0137] 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。

[0138] 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。

[0139] 基于上述内容，在实际应用中，本发明实施例还提供了以下两种实现方式：

[0140] 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；

[0141] 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判断。

[0142] 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。

[0143] 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。

[0144] 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：

[0145] 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；

[0146] 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；

[0147] 第三，无需用户的参与，因此不影响用户的操作，易用性高。

[0148] 基于上述内容，本发明还提供了图2所示的优选实施例。

[0149] 参照图2，是本发明优选实施例所述一种利用沙箱技术进行防御的方法流程图。

[0150] 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。

[0151] 整个待操作的目标程序自动进入沙箱的判断流程如下：

[0152] 步骤201，创建进程；

[0153] 步骤202，判断父进程是否在沙箱内；

[0154] 如果父进程在沙箱内，则跳转到步骤208；

[0155] 如果父进程不在沙箱内，则继续步骤203。

[0156] 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；

[0157] 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；

[0158] 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。

[0159] 步骤204，判断所述待操作的目标程序是否在白名单中；

[0160] 如果在白名单中，则跳转到步骤209；

[0161] 如果不在白名单中，则是未知程序，继续步骤205。

[0162] 步骤205，判断所述待操作的目标对象是否在黑名单中；

[0163] 如果在黑名单中，则跳转到步骤208；

[0164] 如果不在黑名单中，则继续步骤206。

[0165] 步骤206，判断所述目标程序是否为特定类型的程序；

[0166] 即根据各种匹配规则判断是否为特定类型的程序；

[0167] 如果是，则继续步骤207；

[0168] 如果不是，则跳转到步骤209。

[0169] 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；

[0170] 如果用户选择导入，则将该目标程序加入沙箱运行列表。

[0171] 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。

[0172] 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。

[0173] 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。

[0174] 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，本发明并不受所描述的动作顺序的限制，因为依据本发明，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发明所必须的。

[0175] 基于上述内容，本发明还提供了相应的装置实施例，如图3所示。

[0176] 参照图3，是本发明优选实施例所述一种利用沙箱技术进行防御的装置结构图。

[0177] 所述装置可以包括以下模块：

[0178] 判断触发模块31，用于在对目标对象执行操作之前，触发所述自动判断模块32；

[0179] 自动判断模块32，用于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，则在沙箱中完成该目标对象的执行；如果否，则在沙箱外完成该目标对象的执行。

[0180] 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。

[0181] 当自动判断所述目标对象的执行需要导入沙箱时：

[0182] 如果所述目标对象为目标程序，则所述自动判断模块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；

[0183] 如果所述目标对象为目标文件，则所述自动判断模块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；

[0184] 如果所述目标对象为用户输入的信息，则所述自动判断模块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。

[0185] 并且，如果所述目标对象为目标程序，则所述判断触发模块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触发自动判断模块32；和/或，在下载所述目标程序之前触发自动判断模块32；

[0186] 如果所述目标对象为目标文件，则所述判断触发模块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触发自动判断模块32；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触发自动判断模块32；

[0187] 如果所述目标对象为用户输入的信息，则所述判断触发模块31在用户输入所述信息时触发自动判断模块32。

[0188] 进一步，所述自动判断模块32可以包括：

[0189] 规则判断子模块321，用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。

[0190] 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，所述规则判断子模块321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；

[0191] 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；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；

[0192] 当所述待操作的目标对象为用户输入的信息时，所述规则判断子模块321判断所述用户输入的信息是否符合预置的匹配规则。

[0193] 优选的，所述自动判断模块32还可以包括：

[0194] 父进程判断子模块322，用于在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；如果否，则触发所述规则判断子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。

[0195] 优选的，所述自动判断模块32还可以包括：

[0196] 用户选择判断子模块323，用于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，则触发所述规则判断子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。

[0197] 优选的，所述自动判断模块32还可以包括：

[0198] 白名单判断子模块324，用于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，触发所述规则判断子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，则不需要导入沙箱。

[0199] 优选的，所述自动判断模块32还可以包括：

[0200] 黑名单判断子模块325，用于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，则触发所述规则判断子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。

[0201] 优选的，所述装置还可以包括：

[0202] 提示模块33，用于当所述待操作的目标对象的执行需要导入沙箱时，在导入沙箱之前，弹出提示窗提示用户是否导入沙箱。

[0203] 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。

[0204] 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。

[0205] 基于上述的利用沙箱技术进行防御的装置，本发明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。

[0206] 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。

[0207] 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。

[0208] 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”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。

[0209] 以上对本发明所提供的一种利用沙箱技术进行防御的方法、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发明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发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，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发明的限制。

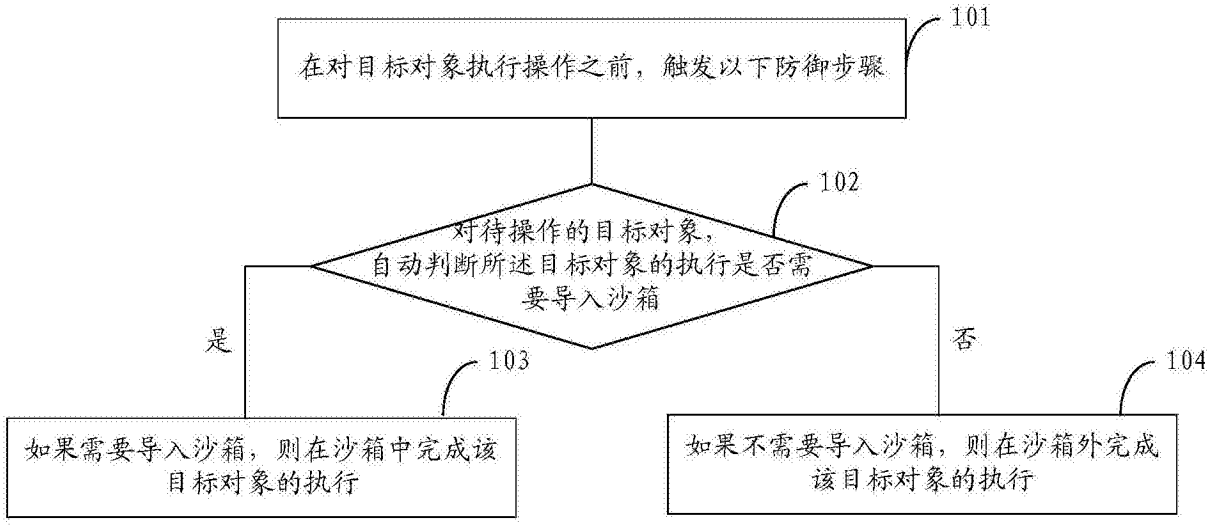

101
在对目标对象执行操作之前，触发以下防御步骤
102
对待操作的目标对象，
自动判断所述目标对象的执行是否需
要导入沙箱
是
否
103
如果需要导入沙箱，则在沙箱中完成该
目标对象的执行
104
如果不需要导入沙箱，则在沙箱外完成
该目标对象的执行

图1

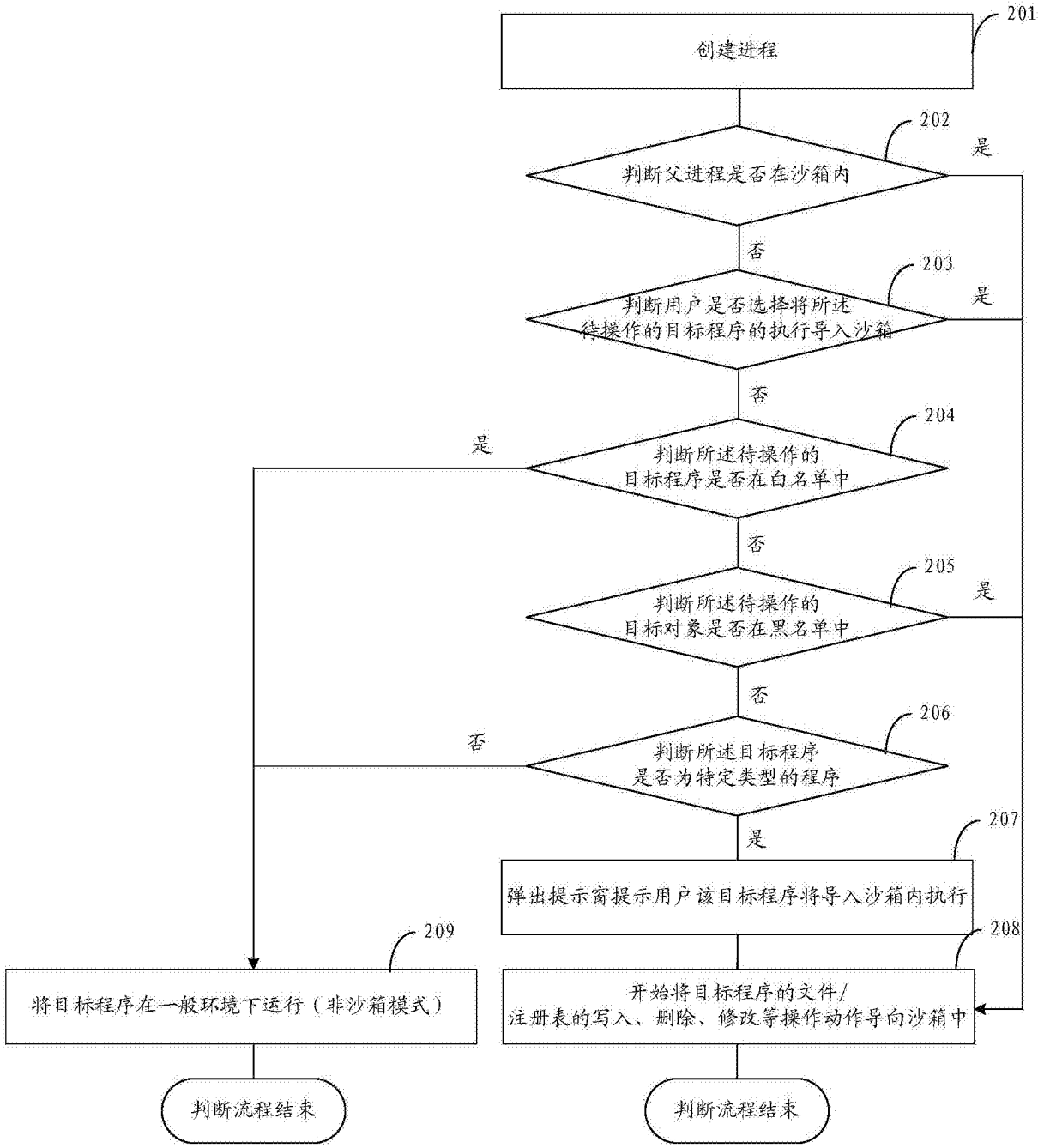

201
创建进程
202
判断父进程是否在沙箱内
是
否
203
判断用户是否选择将所述
待操作的目标程序的执行导入沙箱
是
否
204
判断所述待操作的
目标程序是否在白名单中
是
否
205
判断所述待操作的
目标对象是否在黑名单中
是
否
206
判断所述目标程序
是否为特定类型的程序
否
是
207
弹出提示窗提示用户该目标程序将导入沙箱内执行
208
开始将目标程序的文件/
注册表的写入、删除、修改等操作动作导向沙箱中
209
将目标程序在一般环境下运行（非沙箱模式）
判断流程结束
判断流程结束

图2

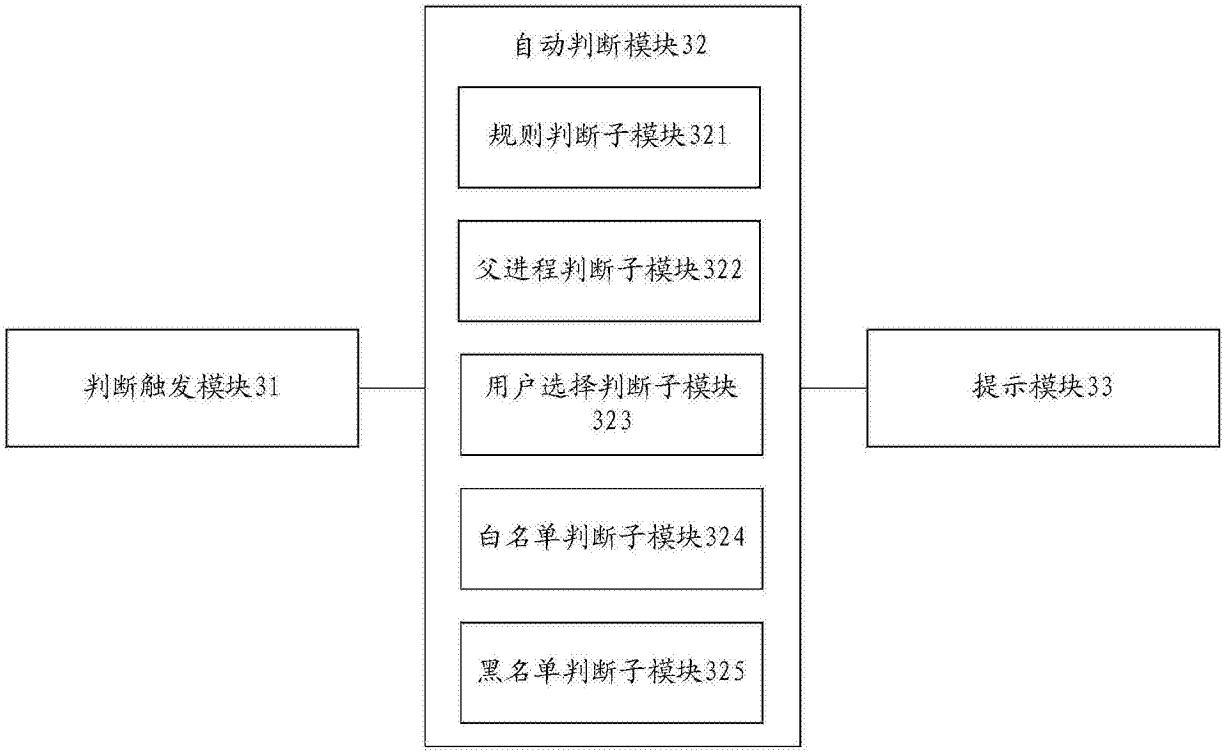

自动判断模块32
规则判断子模块321
父进程判断子模块322
判断触发模块31
用户选择判断子模块323
提示模块33
白名单判断子模块324
黑名单判断子模块325

图3