(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115481421 A
(43)申请公布日 2022.12.16

(21)申请号 202211212280.3

(22)申请日 2022.09.30

(71)申请人 湖北天融信网络安全技术有限公司
地址 430040 湖北省武汉市临空港经济技术开发区五环大道666号(21)
申请人 北京天融信网络安全技术有限公司
北京天融信科技有限公司
北京天融信软件有限公司

(72)发明人 刘超 胡亚运

(74)专利代理机构 北京超凡宏宇专利代理事务所(特殊普通合伙) 11463
专利代理师 唐正瑜

(51)Int.Cl.
G06F 21/60(2013.01)

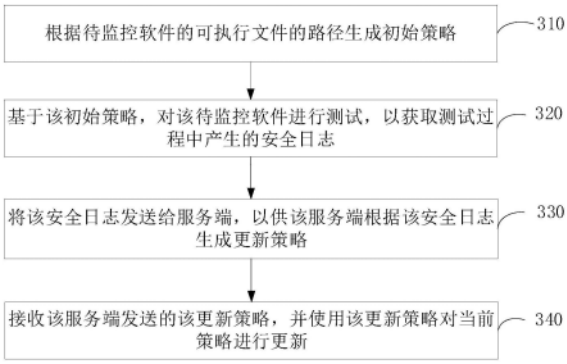
权利要求书3页 说明书13页 附图3页

(54)发明名称

SELinux策略构建方法、装置、电子设备和可读存储介质

(57)摘要

本申请提供了一种SELinux策略构建方法、装置、电子设备和可读存储介质，其中，该方法包括：根据待监控软件的可执行文件的路径生成初始策略；基于该初始策略，对该待监控软件进行测试，以获取测试过程中产生的安全日志；将该安全日志发送给服务端，以供该服务端根据该安全日志生成更新策略；接收该服务端发送的该更新策略，并使用该更新策略对当前策略进行更新，其中，首次对策略进行更新时，该当前策略为该初始策略。



CN 115481421 A

1.一种SELinux策略构建方法,其特征在于,包括:

根据待监控软件的可执行文件的路径生成初始策略;

基于所述初始策略,对所述待监控软件进行测试,以获取测试过程中产生的安全日志;

将所述安全日志发送给服务端,以供所述服务端根据所述安全日志生成更新策略;

接收所述服务端发送的所述更新策略,并使用所述更新策略对当前策略进行更新,其中,首次对策略进行更新时,所述当前策略为所述初始策略。

2.根据权利要求1所述的方法,其特征在于,所述根据待监控软件的可执行文件的路径生成初始策略,包括:

根据待监控软件的可执行文件的路径生成主体初始策略;

根据所述待监控软件的可执行文件所需监控的目标文件的路径,生成客体初始策略。

3.根据权利要求2所述的方法,其特征在于,所述主体初始策略包括主体安全标签;

所述根据待监控软件的可执行文件的路径生成主体初始策略,包括:

根据待监控软件的可执行文件的路径确定出主体进程名;

根据所述主体进程名,确定出所述主体初始策略中的主体安全标签。

4.根据权利要求2所述的方法,其特征在于,所述客体初始策略包括客体安全标签;

所述根据所述待监控软件的可执行文件所需监控的目标文件的路径,生成客体初始策略,包括:

根据所述待监控软件的可执行文件所需监控的目标文件的路径,确定出文件名和一级或多级目录;

根据所述文件名和一级或多级所述目录,确定出客体安全标签。

5.根据权利要求2所述的方法,其特征在于,所述客体初始策略包括客体安全标签;

所述根据所述待监控软件的可执行文件所需监控的目标文件的路径,生成客体初始策略,包括:

若所述待监控软件的可执行文件所需监控的目标文件的路径中的目录数量大于N1,确定出N级的目录,其中,N1为大于1的正整数;

根据所述N级的目录,以及所述N级的目录中的子目录的文件名,确定出客体安全标签。

6.权利要求2所述的方法,其特征在于,所述客体初始策略包括客体安全标签;

所述根据所述待监控软件的可执行文件所需监控的目标文件的路径,生成客体初始策略,包括:

若所述待监控软件的可执行文件所需监控的目标文件的路径中的文件总数大于N2,确定出N3个的目标文件,其中,N2为大于1的正整数,N3为小于或等于N2的正整数;

根据N3个的目标文件的路径,确定出N3个的目标文件对应的客体安全标签。

7.根据权利要求1所述的方法,其特征在于,所述主体初始策略中包括模式字段和风险标志位,所述模式字段用于标记主体初始策略对应的主体的当前运行模式;所述风险标志位用于标记主体初始策略对应的主体的行为处理方式;

所述方法还包括:针对任意一条目标主体初始策略,根据所述模式字段和所述风险标志位的实际值,对所述目标主体初始策略对应的主体行为进行处理。

8.根据权利要求7所述的方法,其特征在于,所述运行模式包括:学习模式、混合模式和强制模式,所述风险标志位的取值包括第一值和第二值;

所述根据所述模式字段和所述风险标志位的实际值，对所述目标主体初始策略对应的目标主体行为进行处理，包括：

若所述目标主体初始策略中的模式字段的实际值表征目标主体处于学习模式，对所述目标主体初始策略对应的目标主体的非法行为放行，并记录安全日志；

若所述目标主体初始策略中的模式字段的实际值表征目标主体处于强制模式，对所述目标主体初始策略对应的目标主体的非法行为进行拦截，并记录安全日志；

若所述目标主体初始策略中的模式字段的实际值表征目标主体处于混合模式，且所述风险标志位的实际值为第一值，对所述目标主体初始策略对应的目标主体的非法行为进行拦截，并记录安全日志；

若所述目标主体初始策略中的模式字段的实际值表征目标主体处于混合模式，且所述风险标志位的实际值为第二值，对所述目标主体初始策略对应的目标主体的非法行为放行，并记录安全日志。

9.一种SELinux策略构建方法，其特征在于，包括：

接收客户端发送的安全日志，其中，所述安全日志为所述客户端基于初始策略对待监控软件进行测试产生的安全日志；

根据所述安全日志生成更新策略，并将所述更新策略发送给所述客户端，以供所述客户端使用所述更新策略对当前策略进行更新。

10.根据权利要求9所述的方法，其特征在于，所述安全日志中携带主体安全标签和客体安全标签；

所述根据所述安全日志生成更新策略，包括：

根据所述主体安全标签和所述客体安全标签，生成更新策略，其中，所述更新策略包括主体信息、客体信息以及主体对客体的动作。

11.一种SELinux策略构建装置，其特征在于，包括：

第一生成模块，用于根据待监控软件的可执行文件的路径生成初始策略；

测试模块，用于基于所述初始策略，对所述待监控软件进行测试，以获取测试过程中产生的安全日志；

第一发送模块，用于将所述安全日志发送给服务端，以供所述服务端根据所述安全日志生成更新策略；

第一接收模块，用于接收所述服务端发送的所述更新策略，并使用所述更新策略对当前策略进行更新，其中，首次对策略进行更新时，所述当前策略为所述初始策略。

12.一种SELinux策略构建装置，其特征在于，包括：

第二接收模块，用于接收客户端发送的安全日志，其中，所述安全日志为所述客户端基于初始策略对待监控软件进行测试产生的安全日志；

第二生成模块，用于根据所述安全日志生成更新策略，并将所述更新策略发送给所述客户端，以供所述客户端使用所述更新策略对当前策略进行更新。

13.一种电子设备，其特征在于，包括：处理器、存储器，所述存储器存储有所述处理器可执行的机器可读指令，当电子设备运行时，所述机器可读指令被所述处理器执行时执行如权利要求1至10任意一项所述的方法的步骤。

14.一种计算机可读存储介质，其特征在于，该计算机可读存储介质上存储有计算机程

序,该计算机程序被处理器运行时执行如权利要求1至10任意一项所述的方法的步骤。

SELinux策略构建方法、装置、电子设备和可读存储介质

技术领域

[0001] 本申请涉及计算机安全领域，具体而言，涉及一种SELinux策略构建方法、装置、电子设备和可读存储介质。

背景技术

[0002] SELinux(Security-Enhanced Linux，安全增强式Linux)是强制访问控制MAC的一种实现方式，SELinux通过策略规则实现对主体行为的控制，目前策略规则的前期开发工作主要依赖SELinux研发人员完成，导致SELinux的策略规则开发、维护难度大的问题。

发明内容

[0003] 本申请的目的在于提供一种SELinux策略构建方法、装置、电子设备和可读存储介质，以改善SELinux的策略规则开发、维护难度大的问题。

[0004] 第一方面，本发明提供一种SELinux策略构建方法，包括：根据待监控软件的可执行文件的路径生成初始策略；基于所述初始策略，对所述待监控软件进行测试，以获取测试过程中产生的安全日志；将所述安全日志发送给服务端，以供所述服务端根据所述安全日志生成更新策略；接收所述服务端发送的所述更新策略，并使用所述更新策略对当前策略进行更新，其中，首次对策略进行更新时，所述当前策略为所述初始策略。

[0005] 在可选的实施方式中，所述根据待监控软件的可执行文件的路径生成初始策略，包括：根据待监控软件的可执行文件的路径生成主体初始策略；根据所述待监控软件的可执行文件所需监控的目标文件的路径，生成客体初始策略。

[0006] 在上述实施方式中，在初始策略中包括主体初始策略和客体初始策略，从而可以更好地对主体和客体进行分别标记，也就能够更好地通过主体初始策略和客体初始策略实现对主体的行为，以及主体行为的作用对象的定位。

[0007] 在可选的实施方式中，所述主体初始策略包括主体安全标签；所述根据待监控软件的可执行文件的路径生成主体初始策略，包括：根据待监控软件的可执行文件的路径确定出主体进程名；根据所述主体进程名，确定出所述主体初始策略中的主体安全标签。

[0008] 在上述实施方式中，可以对主体安全标签中可以直接呈现出进程名，可以更好地对主体进行定位，从而可以在安全日志中记录主体操作。

[0009] 在可选的实施方式中，所述客体初始策略包括客体安全标签；所述根据所述待监控软件的可执行文件所需监控的目标文件的路径，生成客体初始策略，包括：根据所述待监控软件的可执行文件所需监控的目标文件的路径，确定出文件名和一级或多级目录；根据所述文件名和一级或多级所述目录，确定出客体安全标签。

[0010] 在上述实施方式中，可以根据客体安全标签中反推出客体的绝对路径，方便对主体作用的文件的定位，也就能够更准确地分析出主体的操作。

[0011] 在可选的实施方式中，所述客体初始策略包括客体安全标签；所述根据所述待监控软件的可执行文件所需监控的目标文件的路径，生成客体初始策略，包括：若所述待监控

软件的可执行文件所需监控的目标文件的路径中的目录数量大于N1，确定出N1级的目录，其中，N1为大于1的正整数；根据所述N级的目录，以及所述N1级的目录中的子目录的文件名，确定出客体安全标签。

[0012] 在上述实施方式中，，所述客体初始策略包括客体安全标签；

[0013] 所述根据所述待监控软件的可执行文件所需监控的目标文件的路径，生成客体初始策略，包括：若所述待监控软件的可执行文件所需监控的目标文件的路径中的文件总数大于N2，确定出N3个的目标文件，其中，N2为大于1的正整数，N3为小于或等于N2的正整数；根据N3个的目标文件的路径，确定出N3个的目标文件对应的客体安全标签。

[0014] 在上述实施方式中，还可以对客体的文件的路径中的目录数量或者文件总数进行识别，在数量太大时，避免大量的客体安全标签，可以适当提取部分级目录生成客体安全标签，提高初始策略生成效率。

[0015] 在可选的实施方式中，所述主体初始策略中包括模式字段和风险标志位，所述模式字段用于标记主体初始策略对应的主体的当前运行模式；所述风险标志位用于标记主体初始策略对应的主体的行为处理方式；所述方法还包括：针对任意一条目标主体初始策略，根据所述模式字段和所述风险标志位的实际值，对所述目标主体初始策略对应的主体行为进行处理。

[0016] 在上述实施方式中，还可以设置主体的不同运动模式，以适应不同进度下的策略构建，在保持设备安全的情况下，还能够实现策略的完善。

[0017] 在可选的实施方式中，所述运行模式包括：学习模式、混合模式和强制模式，所述风险标志位的取值包括第一值和第二值；

[0018] 所述根据所述模式字段和所述风险标志位的实际值，对所述目标主体初始策略对应的目标主体行为进行处理，包括：

[0019] 若所述目标主体初始策略中的模式字段的实际值表征目标主体处于学习模式，对所述目标主体初始策略对应的目标主体的非法行为放行，并记录安全日志；

[0020] 若所述目标主体初始策略中的模式字段的实际值表征目标主体处于强制模式，对所述目标主体初始策略对应的目标主体的非法行为进行拦截，并记录安全日志；

[0021] 若所述目标主体初始策略中的模式字段的实际值表征目标主体处于混合模式，且所述风险标志位的实际值为第一值，对所述目标主体初始策略对应的目标主体的非法行为进行拦截，并记录安全日志；

[0022] 若所述目标主体初始策略中的模式字段的实际值表征目标主体处于混合模式，且所述风险标志位的实际值为第二值，对所述目标主体初始策略对应的目标主体的非法行为放行，并记录安全日志。

[0023] 在上述实施方式中，可以设置多个运行模式，以及风险标志位的值，可以通过调整目标主体初始策略中的字段，以调整对主体操作的限制，以使用不同场景下的需求。

[0024] 第二方面，本发明提供一种SELinux策略构建方法，包括：

[0025] 接收客户端发送的安全日志，其中，所述安全日志为所述客户端基于初始策略对待监控软件进行测试产生的安全日志；

[0026] 根据所述安全日志生成更新策略，并将所述更新策略发送给所述客户端，以供所述客户端使用所述更新策略对当前策略进行更新。

[0027] 在可选的实施方式中,所述安全日志中携带主体安全标签和客体安全标签;

[0028] 所述根据所述安全日志生成更新策略,包括:根据所述主体安全标签和所述客体安全标签,生成更新策略,其中,所述更新策略包括主体信息、客体信息以及主体对客体的动作。

[0029] 第三方面,本发明提供一种SELinux策略构建装置,包括:

[0030] 第一生成模块,用于根据待监控软件的可执行文件的路径生成初始策略;

[0031] 测试模块,用于基于所述初始策略,对所述待监控软件进行测试,以获取测试过程中产生的安全日志;

[0032] 第一发送模块,用于将所述安全日志发送给服务端,以供所述服务端根据所述安全日志生成更新策略;

[0033] 第一接收模块,用于接收所述服务端发送的所述更新策略,并使用所述更新策略对当前策略进行更新,其中,首次对策略进行更新时,所述当前策略为所述初始策略。

[0034] 第四方面,本发明提供一种SELinux策略构建装置,包括:

[0035] 第二接收模块,用于接收客户端发送的安全日志,其中,所述安全日志为所述客户端基于初始策略对待监控软件进行测试产生的安全日志;

[0036] 第二生成模块,用于根据所述安全日志生成更新策略,并将所述更新策略发送给所述客户端,以供所述客户端使用所述更新策略对当前策略进行更新。

[0037] 第五方面,本发明提供一种电子设备,包括:处理器、存储器,所述存储器存储有所述处理器可执行的机器可读指令,当电子设备运行时,所述机器可读指令被所述处理器执行时执行如前述实施方式任意一项所述的方法的步骤。

[0038] 第六方面,本发明提供一种计算机可读存储介质,该计算机可读存储介质上存储有计算机程序,该计算机程序被处理器运行时执行如前述实施方式任意一项所述的方法的步骤。

[0039] 本申请实施例的有益效果包括:通过自动生成初始策略,可以在SELinux策略构建过程中,降低对研发人员的要求,也能够提高初始策略生成效率。进一步地,还可以基于对待监控软件的测试产生的安全日志,生成更新策略以对SELinux策略进行完善,提高操作系统的安全的情况下,还降低SELinux的策略规则开发和维护的难度。

附图说明

[0040] 为了更清楚地说明本申请实施例的技术方案,下面将对实施例中所需要使用的附图作简单地介绍,应当理解,以下附图仅示出了本申请的某些实施例,因此不应被看作是对范围的限定,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相关的附图。

[0041] 图1为本申请实施例提供的第一终端与第二终端进行交互的示意图;

[0042] 图2为本申请实施例提供的电子设备的方框示意图;

[0043] 图3为本申请实施例提供的SELinux策略构建方法的流程图;

[0044] 图4为本申请实施例提供的SELinux策略构建方法的步骤310的可选流程图;

[0045] 图5为本申请实施例提供的SELinux策略构建装置的功能模块示意图;

[0046] 图6为本申请实施例提供的另一SELinux策略构建方法的流程图;

[0047] 图7为本申请实施例提供的另一SELinux策略构建装置的功能模块示意图。

具体实施方式

[0048] 下面将结合本申请实施例中附图,对本申请实施例中的技术方案进行描述。

[0049] 应注意到:相似的标号和字母在下面的附图中表示类似项,因此,一旦某一项在一个附图中被定义,则在随后的附图中不需要对其进行进一步定义和解释。同时,在本申请的描述中,术语“第一”、“第二”等仅用于区分描述,而不能理解为指示或暗示相对重要性。

[0050] 强制访问控制MAC(mandatory access control,MAC)在计算机安全领域指一种由操作系统约束的访问控制,目标是限制主体访问或对对象执行某种操作的能力。主体通常为一个进程或线程,对象可以是文件、目录、TCP(Transmission Control Protocol,传输控制协议)/UDP(User Datagram Protocol,用户数据报协议)端口、共享内存段、I/O(Input/Output,输入/输出)设备等。其中,SELinux(Security-Enhanced Linux,SELinux)是强制访问控制MAC的一种实现方式。

[0051] SELinux通过策略规则实现对主体行为的控制,SELinux存在学习模式和强制模式两种运行模式。在强制模式下,若进程行为违反策略规则会导致当前行为被拦截;学习模式下违反策略规则的进程行为不会被拦截,但会用SELinux日志记录下来。这些日志记录可以被用于协助开发SELinux策略规则。目前的SELinux策略规则的前期开发工作主要依赖SELinux研发人员完成,开发过程复杂,后期一般基于SELinux日志使用工具开发完成。因为SELinux的“白名单”实现机制(拦截一切未在策略规则中授权的行为),因此策略规则未完全开发完毕时,可能导致设备种一些正常行为但是未被列入白名单,则可能会出现拦截,导致设备存在较多的异常。

[0052] 基于上述研究为了解决SELinux策略的构建与使用复杂的问题,本申请提供的一种SELinux策略构建方法、装置、电子设备和可读存储介质,下面通过一些实施例来描述本申请提供的SELinux策略构建方法。

[0053] 为便于对本实施例进行理解,首先对执行本申请实施例所公开的一种SELinux策略构建方法的运行环境进行详细介绍。

[0054] 如图1所示,是本申请实施例提供的第一终端110与第二终端120进行交互的示意图。该第二终端120通过网络与一个或多个第一终端进行通信连接,以进行数据通信或交互。该第二终端120可以是网络服务器、数据库服务器等,也可以是个人电脑(personal computer,PC)、平板电脑、智能手机、个人数字助理(personal digital assistant,PDA)等。该第一终端110可以是个人电脑(personal computer,PC)、平板电脑、智能手机、个人数字助理(personal digital assistant,PDA)等。

[0055] 本实施例中,该第一终端110中可以存储有最新的SELinux策略,该第一终端可以基于该SELinux策略对第一终端的主体行为进行控制。该第一终端中还可以部署客户端。该客户端可以接收SELinux策略并对本地策略进行更新。

[0056] 该第二终端120中可以部署有服务端,该客户端与服务端可以建立链接后,客户端可以将SELinux安全日志发送给服务端。

[0057] 在一个实例中,该第一终端110部署的客户端可以是rsyslogd客户端,在第二终端120部署的服务端可以是rsyslogd服务端。该rsyslogd客户端与rsyslogd服务端建立链接

后,SELinux的安全日志能通过rsyslogd客户端发送到rsyslogd服务端。

[0058] 图1所示的第一终端110和第二终端120可以是具有存储功能和处理功能的电子设备。如图2所示,电子设备200可以包括存储器211、处理器213。本领域普通技术人员可以理解,图2所示的结构仅为示意,其并不对电子设备200的结构造成限定。例如,电子设备200还可包括比图2中所示更多或者更少的组件,或者具有与图2所示不同的配置。

[0059] 上述的存储器211、处理器213各元件相互之间直接或间接地电性连接,以实现数据的传输或交互。例如,这些元件相互之间可通过一条或多条通讯总线或信号线实现电性连接。上述的处理器213用于执行存储器中存储的可执行模块。

[0060] 其中,存储器211可以是,但不限于,随机存取存储器(Random Access Memory,简称RAM),只读存储器(Read Only Memory,简称ROM),可编程只读存储器(Programmable Read-Only Memory,简称PROM),可擦除只读存储器(Erasable Programmable Read-Only Memory,简称EPROM),电可擦除只读存储器(Electric Erasable Programmable Read-Only Memory,简称EEPROM)等。其中,存储器211用于存储程序,该处理器213在接收到执行指令后,执行该程序,本申请实施例任一实施例揭示的过程定义的电子设备200所执行的方法可以应用于处理器213中,或者由处理器213实现。

[0061] 上述的处理器213可能是一种集成电路芯片,具有信号的处理能力。上述的处理器213可以是通用处理器,包括中央处理器(Central Processing Unit,简称CPU)、网络处理器(Network Processor,简称NP)等;还可以是数字信号处理器(digital signal processor,简称DSP)、专用集成电路(Application Specific Integrated Circuit,简称ASIC)、现场可编程门阵列(FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

[0062] 本实施例中的电子设备200可以用于执行本申请实施例提供的各个方法中的各个步骤。下面通过几个实施例详细描述SELinux策略构建方法的实现过程。

[0063] 请参阅图3,是本申请实施例提供的SELinux策略构建方法的流程图。本实施例的方法中的步骤可以由于图1所示的第一终端执行,也可以由第一终端中运行的客户端执行。下面将对图3所示的具体流程进行详细阐述。

[0064] 步骤310,根据待监控软件的可执行文件的路径生成初始策略。

[0065] 本实施例中,该初始策略可以包括需要监控的待监控软件的进程的主体初始策略。该初始策略还可以包括待监控软件需要操作的对象的客体初始策略。该对象可以是该待监控软件所需操作的文件、目录等。

[0066] 可选地,可以使用策略生成工具,根据待监控软件的可执行文件的路径生成初始策略。示例性地,该待监控软件的可执行文件的路径可以是待监控软件的可执行文件的绝对路径。

[0067] 示例性地,该策略生成工具可以是get_policy_1.0,通过将待监控软件的可执行文件的路径将存入指定文件中,然后执行策略生成工具get_policy_1.0,该策略生成工具get_policy_1.0可以根据指定文件中的待监控软件的可执行文件的路径生成初始策略。

[0068] 在一个实例中,该指定文件可以是selinux_process.conf,该指定文件selinux_process.conf可以接收需要监控的所有软件的可执行文件的路径。该指定文件selinux_

process.conf中配置的路径可以按需设置。

[0069] 步骤320,基于该初始策略,对该待监控软件进行测试,以获取测试过程中产生的安全日志。

[0070] 示例性地,可以使用测试用例,对待监控软件进行测试,以在测试过程中产生安全日志。该安全日志中可以记录有待监控软件的进程信息,以及该进程执行的操作等。

[0071] 示例性地,该安全日志可以是SELinux拦截日志。

[0072] 步骤330,将该安全日志发送给服务端,以供该服务端根据该安全日志生成更新策略。

[0073] 示例性地,服务端接收到安全日志后可以根据安全日志生成更新策略。

[0074] 在一个实例中,可以使用audit2allow工具,根据安全日志生成特定策略规则。

[0075] 步骤340,接收该服务端发送的该更新策略,并使用该更新策略对当前策略进行更新。

[0076] 其中,首次对策略进行更新时,该当前策略为该初始策略。随着客户端中的策略的更新,当前策略也可以不断完善。

[0077] 在本实施例中,通过自动生成初始策略,可以在SELinux策略构建过程中,降低对研发人员的要求,也能够提高初始策略生成效率。进一步地,还可以基于对待监控软件的测试产生的安全日志,生成更新策略以对SELinux策略进行完善,提高操作系统的安全的情况下,还降低SELinux的策略规则开发和维护的难度。

[0078] 考虑待监控软件中运行的各个功能,除了执行主体的作用,还包括执行主体作用下的对象。基于此,在初始策略可以包括主体初始策略和客体初始策略。如图4所示,步骤310可以包括步骤311和步骤312。

[0079] 步骤311,根据待监控软件的可执行文件的路径生成主体初始策略。

[0080] 示例性地,主体初始策略包括主体安全标签。

[0081] 上述的步骤311可以包括:根据待监控软件的可执行文件的路径确定出主体进程名;根据该主体进程名,确定出该主体初始策略中的主体安全标签。

[0082] 在一个实例中,待监控软件的可执行文件的路径可以包括/usr/sbin/ntpd、/usr/local/sbin/sshd。

[0083] 在实例/usr/sbin/ntpd可以提取出的主体进程名为ntpd,则可以根据该进程名ntpd生成主体安全标签。在实例/usr/local/sbin/sshd可以提取出的主体进程名为sshd,则可以根据该进程名sshd生成主体安全标签。

[0084] 示例性地,可以在进程名的基础上添加指定字符,以得到主体安全标签。在一个实例中,该指定字符可以是proc_t。

[0085] 以上面两个实例为例,则可以得到的主体安全标签分别为ntpd_proc_t、sshd_proc_t。

[0086] 本实施例中,可以使用策略生成工具get_policy_1.0,可以基于“主体安全标签=进程名+proc_t”的规则为待监控软件的进程自动生成安全标签,同时生成策略规则。

[0087] 在一个实例中策略规则可以为:type_transition source_type target_type:process process_type;

[0088] 其中,source_type表示系统中所有进程安全标签的集合,target_type表示进程

对应可执行文件安全标签;process_type表示进程安全标签。

[0089] 通过上述安全标签配置,可以使任何父进程执行指定可执行程序时都能保证主体进程使用预期安全标签。

[0090] 步骤312,根据该待监控软件的可执行文件所需监控的目标文件的路径,生成客体初始策略。

[0091] 本实施例中,客体初始策略包括客体安全标签。

[0092] 可选地,可以将需要设置客体安全标签的文件的绝对路径配置在指定文件中,从而可以使用策略生成工具get_policy_1.0可以自动扫描指定文件中的绝对路径,生成各个文件对应的客体安全标签。

[0093] 在一种实施方式中,步骤312可以包括:根据该待监控软件的可执行文件所需监控的目标文件的路径,确定出文件名和一级或多级目录;根据该文件名和一级或多级该目录,确定出客体安全标签。

[0094] 其中,目标文件的目录的级数,根据该目标文件存放位置确定。

[0095] 可选地,策略生成工具get_policy_1.0可以自动扫描待监控软件所涉及的文件的绝对路径自动生成客体初始策略。可选地,策略生成工具get_policy_1.0可以自动扫描待监控软件所需监控的文件的绝对路径自动生成客体初始策略。

[0096] 示例性地,客体安全标签=文件名称根目录-文件名称次级根目-...-文件名称,其中,文件目录的层级可以根据文件存储位置确定。

[0097] 例如,需监控的一个文件的绝对路径为:/etc/passwd,则该文件的客体安全标签为:etc-passwd。再例如,需要监控的一个文件的绝对路径:/etc/ssh/ssh_config,则该文件的客体安全标签为:etc-ssh-ssh_config。

[0098] 可选地,需监控的文件的绝对路径可以预先被配置在指定文件中,策略生成工具get_policy_1.0可以自动扫描该指定文件中的各文件的绝对路径,以自动生成客体初始策略。该指定文件为selinux_file.conf。

[0099] 可选地,针对父目录下的文件名未被写入指定文件中时,父目录下的文件可以默认使用基于父目录名称的安全标签。

[0100] 在一个实例中,一父目录下包括多个文件,多个文件分别为A/B/F1/f11,A/B/F1/f12,A/B/F1/f13。但是f11、f12、f13的绝对路径未被配置入指定文件中,则可以不生成文件f11、f12、f13定的客体安全标签,可以仅生成其父目录A/B/F1的客体安全标签。父目录A/B/F1的客体安全标签可以表示为:A-B-F1。父目录A/B/F1下的子文件可以均使用该父目录的客体安全标签。

[0101] 在一些实际场景中,待监控软件所涉及的文件的数量可能比较大,或者,所涉及的文件所在目录层级比较深,如果针对所有文件均设置客体安全标签,可能会导致配置量较大,生成的客体安全标签较多。基于此,步骤312可以包括:若该待监控软件的可执行文件所需监控的目标文件的路径中的目录数量大于N1,确定出N1级的目录,根据该N1级的目录,以及该N级的目录中的子目录的文件名,确定出客体安全标签。

[0102] 其中,N1为大于1的正整数。该N1可以按需设置,例如,该N1的取值可以是5、6、7等值。

[0103] 示例性地,该N级的目录中若包括M个子目录,则可以在该N级目录下生成M个客体

安全标签。

[0104] 若M个子目录下还包括多个目录或文件,则该M个子目录下还包括多个目录或文件均使用该M个客体安全标签。

[0105] 在一实施方式中,步骤312可以包括:若该待监控软件的可执行文件所需监控的目标文件的路径中的文件总数大于N2,确定出N3个的目标文件,其中,N2为大于1的正整数,N3为小于或等于N2的正整数;根据N3个的目标文件的路径,确定出N3个的目标文件对应的客体安全标签。

[0106] 针对其余除了上述的N3个的目标文件之外的目标文件,则可以使用其父目录的客体安全标签。

[0107] 其中,上述的N2可以按需设置,例如,该N2可以为20、50、100、150等值。

[0108] 示例性地,该N3个的目标文件的选择可以是用户根据实际访问频率或访问需求设置的。例如,用户可以将该N3个的目标文件配置在指定文件中。策略生成工具get_policy_1.0可以自动扫描该指定文件中的各N3个的目标文件的绝对路径,以自动生成客体安全标签。

[0109] 示例性地,N3个的目标文件也可以是按照其它标准确定出的。例如,可以先从根目录开始选,依次深入目录,直到选出N3个的目标文件。再例如,也可以随机选出N3个的目标文件。实际情况下,可以根据需求设置选出N3个的目标文件的方式。

[0110] 在一实施方式中,步骤312可以包括:针对任意待监控软件所需监控的指定目录,若指定目录下的文件数量大于设定数量,则可以为该指定目录设置一个客体安全标签。

[0111] 该指定目录下的文件或子目录可以均使用该指定目录的客体安全标签。

[0112] 通过上述配置方式,可以为对客体的文件设置适量的客体安全标签,避免大量的客体安全标签,可以适当提取部分级目录生成客体安全标签,提高初始策略生成效率。

[0113] 为了使SELinux策略构建方法能够适应更多的应用场景,例如,针对一些已经完善策略规则的进程可以采用强制模式,以使使用SELinux策略的设备的安全性具有保障,对于一些还需要完善的进程可以使用学习模式,可以使这类进程还是可以不断完善策略规则,且不会导致使用SELinux策略的设备出现针对该类进程的异常拦截。因此,还可以为SELinux策略设置多种运行模式。

[0114] 可选地,主体初始策略中包括模式字段和风险标志位,该模式字段用于标记主体初始策略对应的主体的当前运行模式;该风险标志位用于标记主体初始策略对应的主体的行为处理方式。

[0115] 本实施例中的SELinux策略构建方法还可以包括:针对任意一条目标主体初始策略,根据该模式字段和该风险标志位的实际值,对该目标主体初始策略对应的主体行为进行处理。

[0116] 示例性地,该运行模式包括:学习模式、混合模式和强制模式,该风险标志位的取值包括第一值和第二值。

[0117] 在一个实例中,模式字段可以表示为:is_mixed。

[0118] 若该目标主体初始策略中的模式字段的实际值表征目标主体处于学习模式,对该目标主体初始策略对应的目标主体的非法行为放行,并记录安全日志。

[0119] 若该目标主体初始策略中的模式字段的实际值表征目标主体处于强制模式,对该

目标主体初始策略对应的目标主体的非法行为进行拦截,并记录安全日志。

[0120] 示例性地,可以将部分策略规则学习完毕的进程配置成强制模式。例如,可以在指定文件中配置强制模式。例如,在selinux_process.conf文件中进程的绝对路径中配置:/usr/sbin/ntpd enforce。此时,该进程ntpd被设置为强制模式,可以对该进程产品的非法行为进行拦截,并产生拦截日志。

[0121] 若该目标主体初始策略中的模式字段的实际值表征目标主体处于混合模式,且该风险标志位的实际值为第一值,对该目标主体初始策略对应的目标主体的非法行为进行拦截,并记录安全日志。

[0122] 若该目标主体初始策略中的模式字段的实际值表征目标主体处于混合模式,且该风险标志位的实际值为第二值,对该目标主体初始策略对应的目标主体的非法行为放行,并记录安全日志。

[0123] 在一个实例中,上述的第一值可以是1,该第二值可以是0。

[0124] 可选地,上述模式字段的实际值可以为三个值,每一个值对应一个运行模式。在一个实例中,模式字段的实际值为0时,则表示运行模式为学习模式;模式字段的实际值为1时,则表示运行模式为混合模式;模式字段的实际值为2时,则表示运行模式为强制模式。

[0125] 下面通过一个表格来表示不同模式下对主体的非法行为处理方式:

[0126]

is_mixed值	高风险标志位	非法行为处理结果
0(学习模式)	0	产生SElinux安全日志,放行非法行为
0(学习模式)	1	产生SElinux安全日志,放行非法行为
1(混合模式)	0	产生SElinux安全日志,放行非法行为
1(混合模式)	1	产生SElinux安全日志,拦截非法行为
2(强制模式)	0	产生SElinux安全日志,拦截非法行为
2(强制模式)	1	产生SElinux安全日志,拦截非法行为

[0127] 可选地,在混合模式下产生的安全日志可以分为拦截日志和学习日志,例如,针对高风险标志位为0的进程产生的日志确定为学习日志,例如,针对高风险标志位为1的进程产生的日志确定为拦截日志。

[0128] 其中,学习日志可以用于继续完善策略规则,还可以基于拦截日志分析进程的具体非法行为。

[0129] 可以重复上述流程,直到待监控软件的所有进程的策略规则均完善。

[0130] 本实施例的SELinux策略构建方法可应用于所有基于linux内核的操作系统。

[0131] 本实施例中,需要当前操作系统的进行安全加固,可以先筛选出需要在设备上长时间运行的进程进行行为控制,然后在可以在指定文件selinux_process.conf中配置需要被监控的进程对应的可执行文件的绝对路径,最后基于日常测试产生的拦截行为日志,使用工具audit2allow工具基于拦截行为日志自动生成这些进程的策略规则。可以降低用户对SElinux策略的需求,也就降低了研发人员对工具学习成本,降低SELinux策略规则的开发难度,降低了SELinux工具的使用成本。

[0132] 在一些情况中,若无法保证所有进程的策略规则均已开发完毕,但又需要将一些风险较高的进程(比如sshd nginx mysql等)配置成强制模式,以提高使用SELinux策略的设备的安全性,则可以将SELinux模式配置为混合模式,将sshd、nginx、mysql这些进程配置

为强制模式，其它进程继续以学习模式运行，这样既可以保证使用SELinux策略的设备的安全性，又能避免设备因缺少策略规则导致设备异常。混合模式能同时兼顾安全性和稳定性，同时增加了SELinux的灵活性，可以让用户根据系统安全级别调整SELinux的使用方式。

[0133] 通过混合模式的设置，可以从内核层面限制sshd、nginx、mysql的行为，若远程攻击者入侵sshd、nginx、mysql进程访问设备上的其它机密文件，这些异常行为均会被SELinux策略拦截，用户同时还能通过日志迅速定位攻击者的具体行为。

[0134] 进一步地，由于为各个主体和客体设置了安全标签，通过安全日志中的安全标签可以准确定位主体作用的客体的绝对路径，准确定位被访问文件具体信息。

[0135] 基于同一申请构思，本申请实施例中还提供了与SELinux策略构建方法对应的SELinux策略构建装置，由于本申请实施例中的装置解决问题的原理与前述的SELinux策略构建方法实施例相似，因此本实施例中的装置的实施可以参见上述方法的实施例中的描述，重复之处不再赘述。

[0136] 请参阅图5，是本申请实施例提供的SELinux策略构建装置的功能模块示意图。本实施例中的SELinux策略构建装置中的各个模块用于执行上述方法实施例中的各个步骤。SELinux策略构建装置包括：第一生成模块410、测试模块420、第一发送模块430以及第一接收模块440；其中各个模块的内容如下所示：

[0137] 第一生成模块410，用于根据待监控软件的可执行文件的路径生成初始策略；

[0138] 测试模块420，用于基于该初始策略，对该待监控软件进行测试，以获取测试过程中产生的安全日志；

[0139] 第一发送模块430，用于将该安全日志发送给服务端，以供该服务端根据该安全日志生成更新策略；

[0140] 第一接收模块440，用于接收该服务端发送的该更新策略，并使用该更新策略对当前策略进行更新，其中，首次对策略进行更新时，该当前策略为该初始策略。

[0141] 一种可能的实施方式中，第一生成模块410，包括第一生成单元和第二生成单元：

[0142] 第一生成单元，用于根据待监控软件的可执行文件的路径生成主体初始策略；

[0143] 第二生成单元，用于根据该待监控软件的可执行文件所需监控的目标文件的路径，生成客体初始策略。

[0144] 一种可能的实施方式中，该主体初始策略包括主体安全标签；

[0145] 第一生成单元，用于根据待监控软件的可执行文件的路径确定出主体进程名；根据该主体进程名，确定出该主体初始策略中的主体安全标签。

[0146] 一种可能的实施方式中，该客体初始策略包括客体安全标签；

[0147] 第二生成单元，用于根据该待监控软件的可执行文件所需监控的目标文件的路径，确定出文件名和一级或多级目录；根据该文件名和一级或多级该目录，确定出客体安全标签。

[0148] 一种可能的实施方式中，第二生成单元，用于若该待监控软件的可执行文件所需监控的目标文件的路径中的目录数量大于N1，确定出N1级的目录，其中，N1为大于1的正整数；根据该N1级的目录，以及该N1级的目录中的子目录的文件名，确定出客体安全标签。

[0149] 一种可能的实施方式中，第二生成单元，用于若该待监控软件的可执行文件所需监控的目标文件的路径中的文件总数大于N2，确定出N3个的目标文件，其中，N2为大于1的

正整数,N3为小于或等于N2的正整数;根据N3个的目标文件的路径,确定出N3个的目标文件对应的客体安全标签。

[0150] 一种可能的实施方式中,该主体初始策略中包括模式字段和风险标志位,该模式字段用于标记主体初始策略对应的主体的当前运行模式;该风险标志位用于标记主体初始策略对应的主体的行为处理方式;

[0151] 本实施例的SELinux策略构建装置还可以包括:处理模块,用于针对任意一条目标主体初始策略,根据该模式字段和该风险标志位的实际值,对该目标主体初始策略对应的主体行为进行处理。

[0152] 一种可能的实施方式中,该运行模式包括:学习模式、混合模式和强制模式,该风险标志位的取值包括第一值和第二值;

[0153] 处理模块,用于若该目标主体初始策略中的模式字段的实际值表征目标主体处于学习模式,对该目标主体初始策略对应的目标主体的非法行为放行,并记录安全日志;若该目标主体初始策略中的模式字段的实际值表征目标主体处于强制模式,对该目标主体初始策略对应的目标主体的非法行为进行拦截,并记录安全日志;若该目标主体初始策略中的模式字段的实际值表征目标主体处于混合模式,且该风险标志位的实际值为第一值,对该目标主体初始策略对应的目标主体的非法行为进行拦截,并记录安全日志;若该目标主体初始策略中的模式字段的实际值表征目标主体处于混合模式,且该风险标志位的实际值为第二值,对该目标主体初始策略对应的目标主体的非法行为放行,并记录安全日志。

[0154] 请参阅图6,是本申请实施例提供的SELinux策略构建方法的流程图。本实施例的方法中的步骤可以由于图1所示的第二终端执行,也可以由第二终端中运行的服务端执行。下面将对图6所示的具体流程进行详细阐述。

[0155] 步骤510,接收客户端发送的安全日志。

[0156] 其中,该安全日志为该客户端基于初始策略对待监控软件进行测试产生的安全日志。

[0157] 可选地,该第二终端的服务端可以接收该第一终端的客户端传输的安全日志。

[0158] 步骤520,根据该安全日志生成更新策略,并将该更新策略发送给该客户端,以供该客户端使用该更新策略对当前策略进行更新。

[0159] 可选地,可以从安全日志中提取出,主体信息、客体信息以及主体对客体进行的操作信息。

[0160] 可以根据该主体信息、客体信息以及主体对客体进行的操作信息,生成更新策略。

[0161] 示例性地,安全日志中携带主体安全标签和客体安全标签。

[0162] 步骤520可以包括:根据该主体安全标签和该客体安全标签,生成更新策略。其中,该更新策略包括主体信息、客体信息以及主体对客体的动作。

[0163] 可选地,可以使用指定策略生成工具对安全日志进行分析,得到更新策略。例如,该指定策略生成工具可以为audit2allow工具。

[0164] 可选地,可以根据客体安全标签确定出客体的绝对路径,可以根据该主体安全标签可以确定出主体进程。

[0165] 在一个实例中,安全日志可以如下所示:

[0166] 2022-05-05T11:23:27+08:00localhost kernel:audit:type＝1400audit

(1651721007.306:1698887):avc:denied{open read}for pid＝27463comm＝"sshd"name＝"ssh_config"dev＝"rootfs"ino＝2019scontext＝system_u:system_r:sshd_proc_t:s0 tcontext＝system_u:object_r:etc-ssh-ssh_config:s0 tclass＝file permissive＝1

[0167] 2022-05-05T11:23:20+08:00localhost kernel:audit:type＝1400audit(1651721001.009:1698868):avc:denied{open}for pid＝14884comm＝"sshd"name＝"passwd"dev＝"rootfs"ino＝2019scontext＝system_u:system_r:service_sshd:s0 tcontext＝system_u:object_r:etc-passwd:s0 tclass＝file permissive＝1

[0168] 通过对上述安全日志的分析,可以确定出主体安全标签为:sshd_proc_t,客体安全标签为:etc-ssh-ssh_confi和etc-passwd。

[0169] 基于上述两条日志中,使用audit2allow工具得到两条更新策略规则如下:

[0170] allow sshd_proc_t etc-ssh-ssh_config:file{open read};

[0171] allow sshd_proc_t etc-passwd:file{open}。

[0172] 可选地,还可以基于安全日志中的主体安全标签和客体安全标签,确定出主体所指定的具体动作。

[0173] 通过上述策略规则中主体安全标签:sshd_proc_t和客体安全标签:etc-ssh-ssh_confi、etc-passwd分析出进程shhd对文件/etc/ssh/ssh_config和/etc/passwd进行了open和read操作。

[0174] 通过第二终端对安全日志的分析,可以确定出更新策略,以实现动态地更新SELinux策略,完善SELinux策略,提高SELinux策略的有效性,以及降低SELinux策略使用难度。

[0175] 基于同一申请构思,本申请实施例中还提供了与SELinux策略构建方法对应的SELinux策略构建装置,由于本申请实施例中的装置解决问题的原理与前述的SELinux策略构建方法实施例相似,因此本实施例中的装置的实施可以参见上述方法的实施例中的描述,重复之处不再赘述。

[0176] 请参阅图7,是本申请实施例提供的SELinux策略构建装置的功能模块示意图。本实施例中的SELinux策略构建装置中的各个模块用于执行上述方法实施例中的各个步骤。SELinux策略构建装置包括:第二接收模块610和第二生成模块620;其中各模块的内容如下所示:

[0177] 第二接收模块610,用于接收客户端发送的安全日志,其中,该安全日志为该客户端基于初始策略对待监控软件进行测试产生的安全日志;

[0178] 第二生成模块620,用于根据该安全日志生成更新策略,并将该更新策略发送给该客户端,以供该客户端使用该更新策略对当前策略进行更新。

[0179] 一种可能的实施方式中,该安全日志中携带主体安全标签和客体安全标签;

[0180] 第二生成模块620,用于根据该主体安全标签和该客体安全标签,生成更新策略,其中,该更新策略包括主体信息、客体信息以及主体对客体的动作。

[0181] 此外,本申请实施例还提供一种计算机可读存储介质,该计算机可读存储介质上存储有计算机程序,该计算机程序被处理器运行时执行上述方法实施例中所述的SELinux策略构建方法的步骤。

[0182] 本申请实施例所提供的SELinux策略构建方法的计算机程序产品，包括存储了程序代码的计算机可读存储介质，所述程序代码包括的指令可用于执行上述方法实施例中所述的SELinux策略构建方法的步骤，具体可参见上述方法实施例，在此不再赘述。

[0183] 在本申请所提供的几个实施例中，应该理解到，所揭露的装置和方法，也可以通过其它的方式实现。以上所描述的装置实施例仅仅是示意性的，例如，附图中的流程图和框图显示了根据本申请的多个实施例的装置、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段或代码的一部分，所述模块、程序段或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现方式中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个连续的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以用执行规定的功能或动作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0184] 另外，在本申请各个实施例中的各功能模块可以集成在一起形成一个独立的部分，也可以是各个模块单独存在，也可以两个或两个以上模块集成形成一个独立的部分。

[0185] 所述功能如果以软件功能模块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。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，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0186] 以上所述仅为本申请的优选实施例而已，并不用于限制本申请，对于本领域的技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。应注意到:相似的标号和字母在下面的附图中表示类似项，因此，一旦某一项在一个附图中被定义，则在随后的附图中不需要对其进行进一步定义和解释。

[0187] 以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以权利要求的保护范围为准。

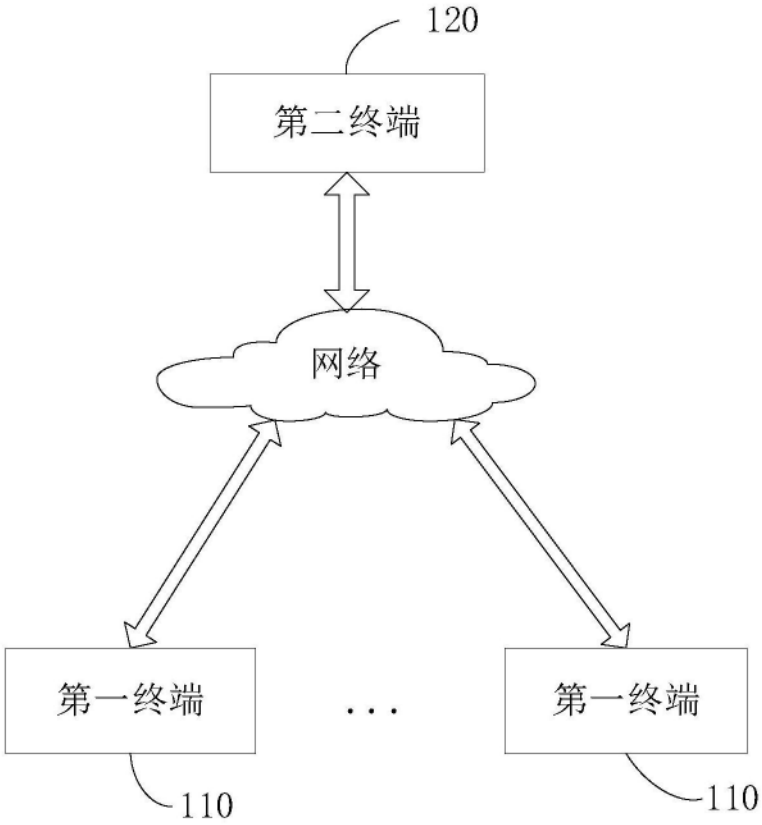


图1

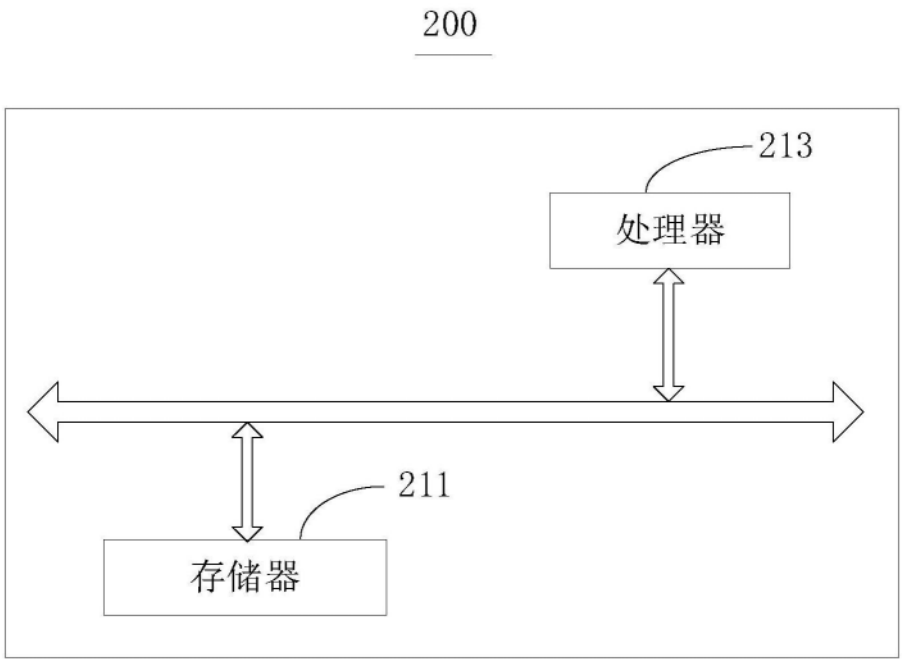


图2

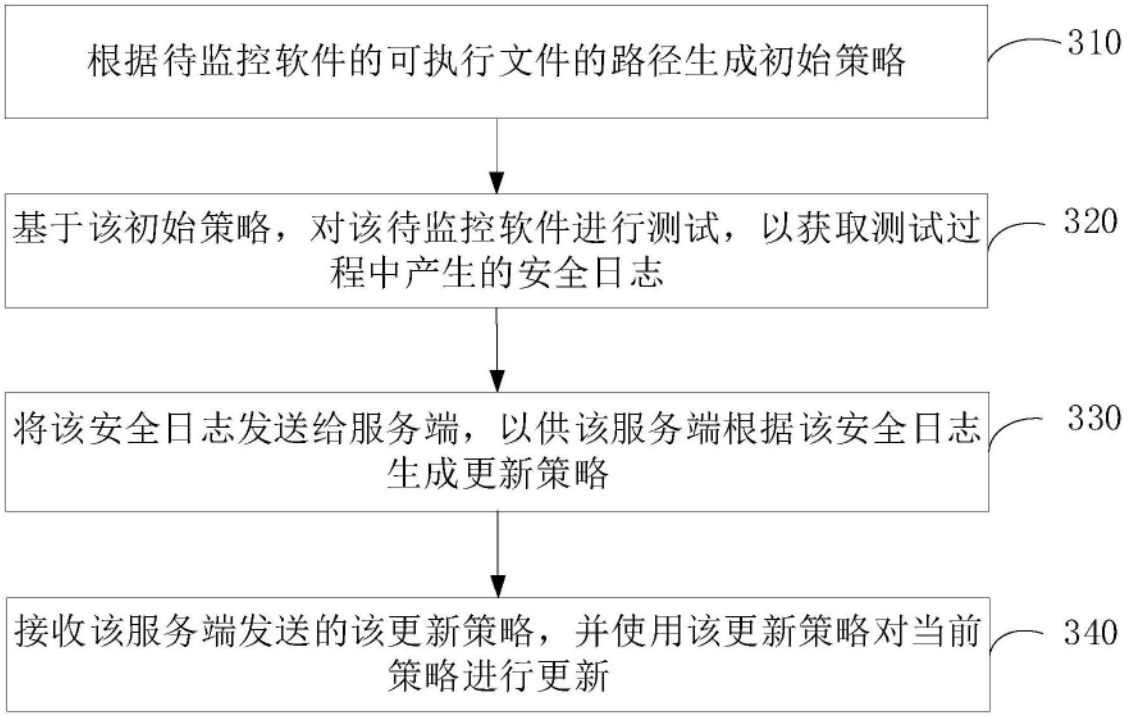

根据待监控软件的可执行文件的路径生成初始策略
310
基于该初始策略，对该待监控软件进行测试，以获取测试过程中产生的安全日志
320
将该安全日志发送给服务端，以供该服务端根据该安全日志生成更新策略
330
接收该服务端发送的该更新策略，并使用该更新策略对当前策略进行更新
340

图3

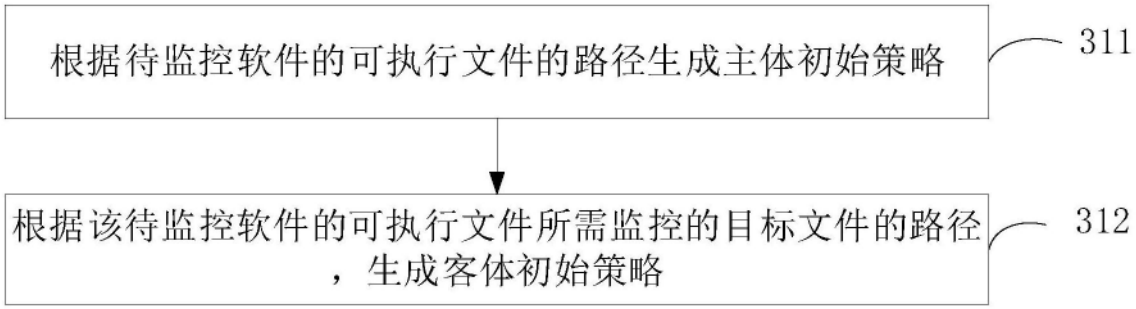

根据待监控软件的可执行文件的路径生成主体初始策略
311
根据该待监控软件的可执行文件所需监控的目标文件的路径，生成客体初始策略
312

图4

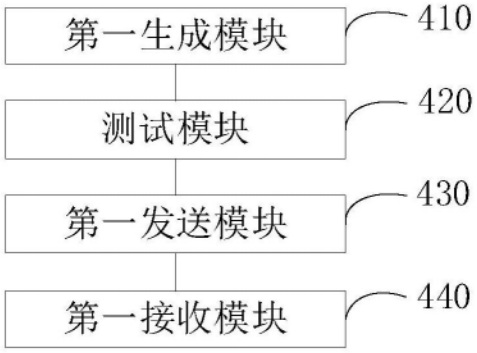

第一生成模块
410
测试模块
420
第一发送模块
430
第一接收模块
440

图5

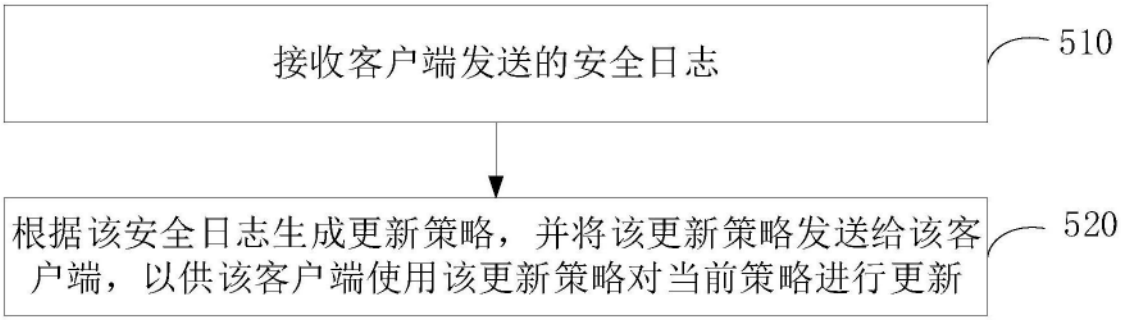

接收客户端发送的安全日志
510
根据该安全日志生成更新策略，并将该更新策略发送给该客户端，以供该客户端使用该更新策略对当前策略进行更新
520

图6


第二接收模块
610
第二生成模块
620

图7