(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 105426758 B
(45)授权公告日 2018.07.27

(21)申请号 201510958935.5

(22)申请日 2015.12.18

(65)同一申请的已公布的文献号
申请公布号 CN 105426758 A

(43)申请公布日 2016.03.23

(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 北京奇安信科技有限公司

(72)发明人 汪圣平 唐青昊

(74)专利代理机构 北京鼎佳达知识产权代理事务所(普通合伙) 11348
代理人 王伟锋 刘铁生

(51)Int.Cl.
G06F 21/55(2013.01)
G06F 11/07(2006.01)

(56)对比文件
CN 103984899 A,2014.08.13,
CN 103023912 A,2013.04.03,
CN 103178988 A,2013.06.26,
CN 103793646 A,2014.05.14,
CN 1737722 A,2006.02.22,
CN 102254111 A,2011.11.23,

审查员 于萍

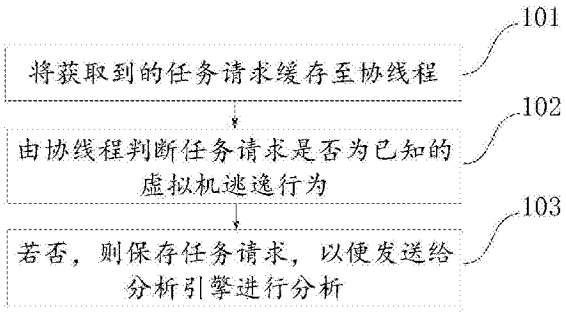
权利要求书3页 说明书10页 附图3页

(54)发明名称

一种虚拟机逃逸的防护方法及装置

(57)摘要

本发明公开了一种虚拟机逃逸的防护方法及装置，涉及计算机技术领域，能够通过建立分析任务的缓存机制来缓解和过滤分析引擎在分析任务高并发状态时的负载压力。本发明主要的技术方案为：将获取到的任务请求缓存至协线程，其中，所述任务请求为分析引擎获取的对虚拟机对外操作行为的分析请求，所述协线程用于协助所述分析引擎缓存所述任务请求；由所述协线程判断所述任务请求是否为已知的虚拟机逃逸行为；若否，则将所述任务请求发送给所述分析引擎进行分析。本发明主要用于防止虚拟逃逸情况的发生。



CN 105426758 B

1.一种虚拟机逃逸的防护方法，其特征在于，所述方法包括：

将获取到的任务请求缓存至协线程，其中，所述任务请求为分析引擎获取的对虚拟机对外操作行为的分析请求，所述协线程用于协助所述分析引擎缓存所述任务请求；

由所述协线程判断所述任务请求是否为已知的虚拟机逃逸行为；

若否，则保存所述任务请求，以便发送给所述分析引擎进行分析。

2.根据权利要求1所述的方法，其特征在于，所述将获取到的任务请求缓存至协线程包括：

创建虚拟机的任务请求队列；

将所述任务请求添加到所述队列中。

3.根据权利要求1所述的方法，其特征在于，由所述协线程判断所述任务请求是否为已知的虚拟机逃逸行为包括：

提取所述任务请求中的操作行为；

将所述操作行为与已知的虚拟机逃逸行为进行匹配。

4.根据权利要求3所述的方法，其特征在于，在由所述协线程判断所述任务请求是否为已知的虚拟机逃逸行为之前，所述方法还包括：

建立虚拟机逃逸行为列表，所述列表中记录有当前已知的所有属于虚拟机逃逸的操作行为特征信息；

根据所述分析引擎的分析结果，更新所述虚拟机逃逸行为列表。

5.根据权利要求4所述的方法，其特征在于，将所述操作行为与已知的虚拟机逃逸行为进行匹配包括：

提取所述操作行为中的特征信息；

遍历所述虚拟机逃逸行为列表，判断所述虚拟机逃逸行为列表中是否存在所述特征信息；

若存在，则确定所述操作行为是虚拟机逃逸行为。

6.根据权利要求5所述的方法，其特征在于，确定所述操作行为是虚拟机逃逸行为包括：

当具有多个特征信息时，计算特征相似度比值，所述特征相似度比值是确定为虚拟机逃逸行为列表中的特征信息占所有特征信息的比值；

当所述特征相似度比值大于预设值时，确定所述操作行为是虚拟机逃逸行为。

7.根据权利要求5所述的方法，其特征在于，提取所述操作行为中的特征信息包括：

根据所述操作行为计算得出的MD5值。

8.根据权利要求1所述的方法，其特征在于，将获取到的任务请求缓存至协线程还包括：

根据所述分析引擎的处理能力，将所述分析引擎无法处理的任务请求缓存至所述协线程。

9.根据权利要求1所述的方法，其特征在于，所述方法还包括：

当所述协线程判断所述任务请求为已知的虚拟机逃逸行为时，所述协线程阻止该任务请求发送给所述分析引擎。

10.根据权利要求1所述的方法，其特征在于，将所述任务请求发送给所述分析引擎进

行分析包括：

获取分析引擎的调取指令；

根据所述调取指令向所述分析引擎发送任务请求。

11.根据权利要求1所述的方法，其特征在于，将所述任务请求发送给所述分析引擎进行分析还包括：

设置预置的时间间隔；

根据所述时间间隔定时向所述分析引擎发送任务请求。

12.一种虚拟机逃逸的防护装置，其特征在于，所述装置包括：

缓存单元，用于将获取到的任务请求缓存至协线程，其中，所述任务请求为分析引擎获取的对虚拟机对外操作行为的分析请求，所述协线程用于协助所述分析引擎缓存所述任务请求；

判断单元，用于由所述协线程判断所述缓存单元缓存的任务请求是否为已知的虚拟机逃逸行为；

保存单元，用于当所述判断单元判断所述任务请求不是虚拟机逃逸行为时，保存所述任务请求，以便发送给所述分析引擎进行分析。

13.根据权利要求12所述的装置，其特征在于，所述缓存单元包括：

创建模块，用于创建虚拟机的任务请求队列；

添加模块，用于将所述任务请求添加到所述创建模块创建的任务请求队列中。

14.根据权利要求12所述的装置，其特征在于，所述判断单元包括：

提取模块，用于提取所述任务请求中的操作行为；

匹配模块，用于将所述提取模块提取的操作行为与已知的虚拟机逃逸行为进行匹配。

15.根据权利要求14所述的装置，其特征在于，所述装置还包括：

建立单元，用于在所述判断单元由所述协线程判断所述任务请求是否为已知的虚拟机逃逸行为之前，建立虚拟机逃逸行为列表，所述列表中记录有当前已知的所有属于虚拟机逃逸的操作行为特征信息；

更新单元，用于根据所述分析引擎的分析结果，更新所述建立单元建立的虚拟机逃逸行为列表。

16.根据权利要求15所述的装置，其特征在于，所述匹配模块包括：

提取子模块，用于提取所述操作行为中的特征信息；

判断子模块，用于遍历所述虚拟机逃逸行为列表，判断所述虚拟机逃逸行为列表中是否存在所述提取子模块提取的特征信息；

确定子模块，用于当所述判断子模块判断所述虚拟机逃逸行为列表中存在所述特征信息时，确定所述操作行为是虚拟机逃逸行为。

17.根据权利要求16所述的装置，其特征在于，所述确定子模块还用于，当具有多个特征信息时，计算特征相似度比值，所述特征相似度比值是确定为虚拟机逃逸行为列表中的特征信息占所有特征信息的比值；当所述特征相似度比值大于预设值时，确定所述操作行为是虚拟机逃逸行为。

18.根据权利要求16所述的装置，其特征在于，所述提取子模块提取的特征信息包括：根据所述操作行为计算得出的MD5值。

19.根据权利要求12所述的装置，其特征在于，所述缓存单元还用于，根据所述分析引擎的处理能力，将所述分析引擎无法处理的任务请求缓存至所述协线程。

20.根据权利要求12所述的装置，其特征在于，所述装置还包括：

阻止单元，用于当所述协线程判断所述任务请求为已知的虚拟机逃逸行为时，所述协线程阻止该任务请求发送给所述分析引擎。

21.根据权利要求12所述的装置，其特征在于，所述保存单元包括：

获取模块，用于获取分析引擎的调取指令；

第一发送模块，用于根据所述获取模块获取的调取指令向所述分析引擎发送任务请求。

22.根据权利要求12所述的装置，其特征在于，所述保存单元还包括：

设置模块，用于设置预置的时间间隔；

第二发送模块，用于根据所述设置模块设置的时间间隔定时向所述分析引擎发送任务请求。

一种虚拟机逃逸的防护方法及装置

技术领域

[0001] 本发明涉及计算机技术领域，尤其涉及一种虚拟机逃逸的防护方法及装置。

背景技术

[0002] 随着计算机软件技术的不断发展，基于Unix系统操作平台的软件开发技术越来越普及，其中，虚拟机逃逸变成研发人员急需解决的问题。虚拟机逃逸是指利用虚拟机软件或者虚拟机中运行的软件的漏洞进行攻击，以达到攻击或控制虚拟机宿主操作系统的目的。

[0003] 目前，虚拟机中的程序只能在虚拟机中运行，当虚拟机系统出现漏洞时，虚拟机中的程序将突破虚拟机的界限，读取虚拟机以外的资源。虚拟机逃逸可以通过虚拟出一个网盘，将逃逸程序携带进宿主机中，对宿主机中的资源进行占用；还可以虚拟出一个仿真指令来携带逃逸程序。为了防止虚拟机逃逸行为的发生，一般是通过行为分析引擎来分析虚拟机的对外操作是否属于虚拟机逃逸行为。然而在宿主机中设置往往会设置有大量的虚拟机，当大量的虚拟机同时产生对外操作或在短时间内进行大量的对外操作时，分析引擎很容易在大负载的情况下死机或崩溃。从而使得整个虚拟机逃逸防护系统失效。

[0004] 可以通过分析引擎对文件行为进行分析，但是在引擎高并发状态时，引擎分析压力大，影响分析结果。

发明内容

[0005] 有鉴于此，本发明提供一种虚拟机逃逸的防护方法及装置，能够通过建立分析任务的缓存机制来缓解和过滤分析引擎在分析任务高并发状态时的负载压力。

[0006] 依据本发明一个方面，提出了一种虚拟机逃逸的防护方法，该方法包括：

[0007] 将获取到的任务请求缓存至协线程，其中，所述任务请求为分析引擎获取的对虚拟机对外操作行为的分析请求，所述协线程用于协助所述分析引擎缓存所述任务请求；

[0008] 由所述协线程判断所述任务请求是否为已知的虚拟机逃逸行为；

[0009] 若否，则将所述任务请求发送给所述分析引擎进行分析。

[0010] 依据本发明另一个方面，还提出了一种虚拟机逃逸的防护装置，该装置包括：

[0011] 缓存单元，用于将获取到的任务请求缓存至协线程，其中，所述任务请求为分析引擎获取的对虚拟机对外操作行为的分析请求，所述协线程用于协助所述分析引擎缓存所述任务请求；

[0012] 判断单元，用于由所述协线程判断所述缓存单元缓存的任务请求是否为已知的虚拟机逃逸行为；

[0013] 发送单元，用于当所述判断单元判断所述任务请求不是虚拟机逃逸行为时，将所述任务请求发送给所述分析引擎进行分析。

[0014] 本发明所采用的虚拟机逃逸的防护方法及装置，用于在高并发分析任务的情况下缓解分析引擎的负载压力。主要通过获取虚拟机对本机以外的宿主机资源所进行的操作，并对该操作以任务请求的方式先缓存至协线程中，由该协线程先对所缓存的任务请求进行

过滤，判断该任务请求中的操作行为是否为虚拟机逃逸行为，若无法确定该任务请求中的操作行为是虚拟机逃逸行为则将该任务请求保留在协线程中，以便发送至分析引擎进行进一步的分析判断。相对于现有技术中直接由分析引擎获取所有虚拟机的任务请求的方式，本发明所采用的虚拟机逃逸的防护方法能够将请求任务在由分析引擎分析之前先进行初步的筛选以减少一部分无需分析的任务请求，通过减少分析引擎的任务处理量达到部分减轻分析引擎负载压力的效果。同时，通过将任务请求先缓存在协线程中，再有序地向分析引擎发送任务请求，能够在面对任务请求高并发状态时起到保护分析引擎，防止分析引擎因负载过大而死机或崩溃的情况发生，从而提高了系统整体的防护稳定性。

[0015] 上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

[0016] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0017] 图1示出了本发明实施例提出的一种虚拟机逃逸的防护方法流程图；

[0018] 图2示出了本发明实施例提出的另一种虚拟机逃逸的防护方法流程图；

[0019] 图3示出了本发明实施例提出的一种虚拟机逃逸的防护装置组成框图；

[0020] 图4示出了本发明实施例提出的另一种虚拟机逃逸的防护装置组成框图。

具体实施方式

[0021] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0022] 本发明实施例提供了一种虚拟机逃逸的防护方法，如图1所示，该方法应用于设置有虚拟机的宿主机中，用于防止虚拟机逃逸的情况发生，具体步骤包括：

[0023] 101、将获取到的任务请求缓存至协线程。

[0024] 要防止虚拟机逃逸的情况发生，首先要能够获取到虚拟机对本机资源以外的宿主机资源或其他虚拟机资源进行的操作行为。根据该行为中的具体特征来判断该操作行为是否构成了虚拟机逃逸。在本实施例中，是由宿主机中的分析引擎获取本机中所有虚拟机的对外操作行为，并将这些行为以任务请求的形式缓存在协线程中。该协线程主要用于辅助分析引擎存储任务请求，以防止多个虚拟机同时产生任务请求或虚拟机在短时间内大量生成任务请求对分析引擎造成的负载过大问题。通过协线程的缓存，分析引擎可以从斜线程中来获取适当数量的任务请求进行分析，从而有效的缓解了分析引擎的处理压力。

[0025] 102、由协线程判断任务请求是否为已知的虚拟机逃逸行为。

[0026] 任务请求缓存至协线程后，协线程将判断该任务请求是否需要由分析引擎进行虚拟机逃逸的行为分析，即判断该任务请求是否为已知的虚拟机逃逸行为。而已知的虚拟机

逃逸行为可以通过分析引擎的分析结果得到，也可以通过管理员设置规定哪些具体的操作行为属于虚拟机逃逸行为，在本实施例中，已知的虚拟机逃逸行为可以是在宿主机中维护的一个列表，在该列表中记录有虚拟机逃逸行为的行为特征。

[0027] 103、若否，则保存任务请求，以便发送给分析引擎进行分析。

[0028] 根据102的判断，当协线程无法确定该任务请求中所携带的操作行为时虚拟机逃逸行为时，说明该任务请求需要由分析引擎进行进一步的具体分析。因此，协线程会将该任务请求保存下来，等待适合的时机发送给分析引擎进行详细的分析判断。

[0029] 通过上述的说明，本发明实施例所提供的一种虚拟机逃逸的防护方法，是通过获取虚拟机对本机以外的宿主机资源所进行的操作，并对该操作以任务请求的方式缓存至协线程中，由该协线程对所缓存的任务请求进行过滤，判断该任务请求中的操作行为是否为虚拟机逃逸行为，若无法确定该任务请求中的操作行为是虚拟机逃逸行为则将该任务请求保留在协线程中，以便发送至分析引擎进行进一步的分析判断。相对于现有技术中直接由分析引擎获取所有虚拟机的任务请求的方式，本发明实施例所采用的虚拟机逃逸的防护方法能够将请求任务在由分析引擎分析之前先进行初步的筛选以减少一部分无需分析的任务请求，通过减少分析引擎的任务处理量达到部分减轻分析引擎负载压力的效果。同时，通过将任务请求先缓存在协线程中，再有序地向分析引擎发送任务请求，能够在面对任务请求高并发状态时起到保护分析引擎，防止分析引擎因负载过大而死机或崩溃的情况发生，从而提高了系统整体的防护稳定性。

[0030] 为了更进一步的说明上述的虚拟机逃逸的防护方法，结合具体的实现方式，本发明实施例还提供了一种虚拟机逃逸的防护方法，如图2所示，该方法包括：

[0031] 201、将获取到的任务请求缓存至协线程。

[0032] 在本发明实施例中，通过建立协线程统一缓存宿主机中所有虚拟机生成的任务请求。具体的实现方式，可以是在该协线程中创建一个队列，将任务请求根据生成的时间添加到该队列中，形成一个任务请求队列。需要说明的是，在根据生成时间进行添加时，在时间精度足够细的前提下基本不可能产生两个相同时间生成的任务请求，但是对于时间的精细程度受到设备硬件条件的限制，在虚拟机高并发任务请求的情况下还是会存在一些同时生成的任务请求，对于同时生成的任务请求，可以通过预置的判断条件再对这些任务请求进行优先排序，例如，通过对虚拟机设置权重值来判断任务请求的优先权，在同时生成的任务请求中，将权重值大的虚拟机生成的任务请求优先添加到队列中。这些预置的判断条件可以通过管理员进行实时的修改设置，对此本实施例不做具体限定。

[0033] 进一步的，还可以将任务请求优先的发送给分析引擎进行处理，当分析引擎的负载到达一定的阈值时，就将任务请求缓存至协线程中等待处理。也就是说，任务请求的数量以及生成的密度在分析引擎的处理能力范围内时，可以不启用斜线程，而当任务请求数量过大出现排队情况时，而这种情况往往是在任务请求高并发是会出现的情况，就启动协线程来缓存多余的任务请求。例如，可以将设置当分析引擎的处理能力在占用率超过90％时，就启动协线程来缓存任务请求；也可以设置一个排队任务请求的阈值，当排队的任务请求达到该阈值时就启动协线程来缓存分析引擎无法处理的任务请求。

[0034] 202、由协线程判断任务请求是否为已知的虚拟机逃逸行为。

[0035] 本发明实施例中，在协线程判断任务请求是否为已知的虚拟机逃逸行为之前，需

要先设定哪些行为是数据虚拟机逃逸行为。具体的实现方式是在宿主机中建立一个虚拟机逃逸行为列表，在该列表中记录有当前已知的所有属于虚拟机逃逸的操作行为，以及该操作行为所具有的相关特征信息。类似于杀毒软件中的病毒特征数据库，该列表也是一个需要实时进行维护的增量型列表，即创建的初期列表中的操作行为以及特征信息较少，但随着分析引擎所分析出的虚拟机逃逸行为的增多，该列表会将新增加的操作行为以及相应的特征信息添加到列表中，逐渐丰富该列表的数据量。随着列表中的特征信息的增加，协线程将能够过滤掉更多的任务请求，以减轻分析引擎的负载。因此，协线程的过滤能力是随着虚拟机逃逸行为列表的更新而动态提高的。

[0036] 在系统中维护有一个虚拟机逃逸行为列表的前提下，协线程将逐一分析任务请求，提取其中虚拟机的操作行为，遍历虚拟机逃逸行为列表，判断该列表中是否具有相同的操作行为信息，若存在则说明该操作行为数据虚拟机逃逸行为；若不存在，则提取该操作行为中的具体的行为特征信息，再遍历虚拟机逃逸行为列表，判断该列表中是否具有相同的行为特征信息，若相同则该操作行为数据虚拟机逃逸行为。进一步的，由于一个操作行为中可能具有多个行为特征信息，在判断一个操作行为时，可能是部分的行为特征为虚拟机逃逸行为的特征信息，因此，在判断操作行为时，可以设置一个预设值，该预设值可以是一个具体数值，根据判断命中的特征信息数量是否达到该值来判断该操作行为是否为虚拟机逃逸行为；也可以使一个比值，该比值用于表示操作行为与虚拟机逃逸行为的特征相似度。在达到该比值的条件下确定该操作行为是虚拟机逃逸行为。例如，设定相似度比值为80％，当一个操作行为具有10个特征时，只有在这10个特征中有8个以上的特征被记录在虚拟机逃逸行为列表中时，才能够确定该操作行为是虚拟机逃逸行为。其中，操作行为中的特征信息可以是由该操作行为计算得出的MD5值等。

[0037] 203、若是，则阻止该任务请求发送给分析引擎。

[0038] 在本实施例中，协线程并不具有像分析引擎对任务请求进行行为分析的能力，而只是判断该任务请求中的操作行为是否为已知的虚拟机逃逸行为，从而对任务请求进行过滤筛选。当协线程判断任务请求中的操作行为是虚拟机逃逸行为时，该任务请求将不需要分析引擎再进行分析判断，因此，会将该任务请求删除出协线程或发送给宿主机中其他的处理虚拟机逃逸行为的单元模块进行处理。

[0039] 204、若否，则保存任务请求，以便发送给分析引擎进行分析。

[0040] 在当协线程无法确定任务请求中的操作行为是虚拟机逃逸行为时，该任务请求就需要分析引擎做进一步的分析判断。因此，协线程将保留该任务请求，在分析引擎具有处理能力时发送给分析引擎做进一步分析判断。对于何时向分析引擎发送任务请求，本实施例中，具体实现方式可以是在分析引擎具有处理能力时向协线程发送一个调取指令，用以告知协线程可以向分析引擎发送任务请求，对于协线程则是接收分析引擎所发送的调取指令，并根据该调取指令向分析引擎发送任务请求；还可以是通过设置一个预置的时间间隔，该时间间隔的取值可以根据计算分析引擎平均处理速度来得到，通过计算处理一个任务请求的平均时长来设置该时间间隔，每过一个时间间隔就向分析引擎主动发送一个任务请求。通过上述的两种实现方式，分析引擎都可以实现与协线程的对接，完成对任务请求的分析，判断宿主机中的虚拟机是否存在虚拟机逃逸行为。

[0041] 进一步的，作为对上述方法的实现，本发明实施例提供了一种虚拟机逃逸的防护

装置，该装置设置于安装有虚拟机的宿主机系统中，如图3所示，该装置具体包括：

[0042] 缓存单元31，用于将获取到的任务请求缓存至协线程，其中，所述任务请求为分析引擎获取的对虚拟机对外操作行为的分析请求，所述协线程用于协助所述分析引擎缓存所述任务请求；

[0043] 判断单元32，用于由所述协线程判断所述缓存单元31缓存的任务请求是否为已知的虚拟机逃逸行为；

[0044] 保存单元33，用于当所述判断单元32判断所述任务请求不是虚拟机逃逸行为时，保存所述任务请求，以便发送给所述分析引擎进行分析。

[0045] 进一步的，如图4所示，所述缓存单元31包括：

[0046] 创建模块311，用于创建虚拟机的任务请求队列；

[0047] 添加模块312，用于将所述任务请求添加到所述创建模块311创建的任务请求队列中。

[0048] 进一步的，如图4所示，所述判断单元32包括：

[0049] 提取模块321，用于提取所述任务请求中的操作行为；

[0050] 匹配模块322，用于将所述提取模块321提取的操作行为与已知的虚拟机逃逸行为进行匹配。

[0051] 进一步的，如图4所示，所述装置还包括：

[0052] 建立单元34，用于在所述判断单元32由所述协线程判断所述任务请求是否为已知的虚拟机逃逸行为之前，建立虚拟机逃逸行为列表，所述列表中记录有当前已知的所有属于虚拟机逃逸的操作行为特征信息；

[0053] 更新单元35，用于根据所述分析引擎的分析结果，更新所述建立单元建立的虚拟机逃逸行为列表。

[0054] 进一步的，如图4所示，所述匹配模块322包括：

[0055] 提取子模块3221，用于提取所述操作行为中的特征信息；

[0056] 判断子模块3222，用于遍历所述虚拟机逃逸行为列表，判断所述虚拟机逃逸行为列表中是否存在所述提取子模块3221提取的特征信息；

[0057] 确定子模块3223，用于当所述判断子模块3222判断所述虚拟机逃逸行为列表中存在所述特征信息时，确定所述操作行为是虚拟机逃逸行为。

[0058] 进一步的，所述确定子模块3223还用于，当具有多个特征信息时，计算特征相似度比值，所述特征相似度比值是确定为虚拟机逃逸行为列表中的特征信息占所有特征信息的比值；当所述特征相似度比值大于预设值时，确定所述操作行为是虚拟机逃逸行为。

[0059] 进一步的，所述提取子模块3221提取的特征信息包括：根据所述操作行为计算得出的MD5值。

[0060] 进一步的，所述缓存单元31还用于，根据所述分析引擎的处理能力，将所述分析引擎无法处理的任务请求缓存至所述协线程。

[0061] 进一步的，如图4所示，所述装置还包括：

[0062] 阻止单元36，用于当所述判断单元32判断所述任务请求为已知的虚拟机逃逸时，所述协线程阻止该任务请求发送给所述分析引擎。

[0063] 进一步的，如图4所示，所述保存单元33包括：

[0064] 获取模块331，用于获取分析引擎的调取指令；

[0065] 第一发送模块332，用于根据所述获取模块331获取的调取指令向所述分析引擎发送任务请求。

[0066] 进一步的，如图4所示，所述保存单元33还包括：

[0067] 设置模块333，用于设置预置的时间间隔；

[0068] 第二发送模块334，用于根据所述设置模块333设置的时间间隔定时向所述分析引擎发送任务请求。

[0069] 综上所述，本实施例提供的一种虚拟机逃逸的防护方法及装置，是通过获取虚拟机对本机以外的宿主机资源所进行的操作，并对该操作以任务请求的方式缓存至协线程中，由该协线程对所缓存的任务请求进行过滤，判断该任务请求中的操作行为是否为虚拟机逃逸行为，若无法确定该任务请求中的操作行为是虚拟机逃逸行为则将该任务请求保留在协线程中，以便发送至分析引擎进行进一步的分析判断。相对于现有技术中直接由分析引擎获取所有虚拟机的任务请求的方式，本发明实施例所采用的虚拟机逃逸的防护方法能够将请求任务在由分析引擎分析之前先进行初步的筛选以减少一部分无需分析的任务请求，通过减少分析引擎的任务处理量达到部分减轻分析引擎负载压力的效果。同时，通过将任务请求先缓存在协线程中，再有序地向分析引擎发送任务请求，能够在面对任务请求高并发状态时起到保护分析引擎，防止分析引擎因负载过大而死机或崩溃的情况发生，从而提高了系统整体的防护稳定性。

[0070] 本发明的实施例公开了：

[0071] A1、一种虚拟机逃逸的防护方法，其特征在于，所述方法包括：

[0072] 将获取到的任务请求缓存至协线程，其中，所述任务请求为分析引擎获取的对虚拟机对外操作行为的分析请求，所述协线程用于协助所述分析引擎缓存所述任务请求；

[0073] 由所述协线程判断所述任务请求是否为已知的虚拟机逃逸行为；

[0074] 若否，则保存所述任务请求，以便发送给所述分析引擎进行分析。

[0075] A2、根据A1所述的方法，其特征在于，所述将获取到的任务请求缓存至协线程包括：

[0076] 创建虚拟机的任务请求队列；

[0077] 将所述任务请求添加到所述队列中。

[0078] A3、根据A1所述的方法，其特征在于，由所述协线程判断所述任务请求是否为已知的虚拟机逃逸行为包括：

[0079] 提取所述任务请求中的操作行为；

[0080] 将所述操作行为与已知的虚拟机逃逸行为进行匹配。

[0081] A4、根据A3所述的方法，其特征在于，在由所述协线程判断所述任务请求是否为已知的虚拟机逃逸行为之前，所述方法还包括：

[0082] 建立虚拟机逃逸行为列表，所述列表中记录有当前已知的所有属于虚拟机逃逸的操作行为特征信息；

[0083] 根据所述分析引擎的分析结果，更新所述虚拟机逃逸行为列表。

[0084] A5、根据A4所述的方法，其特征在于，将所述操作行为与已知的虚拟机逃逸行为进行匹配包括：

[0085] 提取所述操作行为中的特征信息；

[0086] 遍历所述虚拟机逃逸行为列表，判断所述虚拟机逃逸行为列表中是否存在所述特征信息；

[0087] 若存在，则确定所述操作行为是虚拟机逃逸行为。

[0088] A6、根据A5所述的方法，其特征在于，确定所述操作行为是虚拟机逃逸行为包括：

[0089] 当具有多个特征信息时，计算特征相似度比值，所述特征相似度比值是确定为虚拟机逃逸行为列表中的特征信息占所有特征信息的比值；

[0090] 当所述特征相似度比值大于预设值时，确定所述操作行为是虚拟机逃逸行为。

[0091] A7、根据A5所述的方法，其特征在于，提取所述操作行为中的特征信息包括：

[0092] 根据所述操作行为计算得出的MD5值。

[0093] A8、根据A1所述的方法，其特征在于，将获取到的任务请求缓存至协线程还包括：

[0094] 根据所述分析引擎的处理能力，将所述分析引擎无法处理的任务请求缓存至所述协线程。

[0095] A9、根据A1所述的方法，其特征在于，所述方法还包括：

[0096] 当所述协线程判断所述任务请求为已知的虚拟机逃逸行为时，所述协线程阻止该任务请求发送给所述分析引擎。

[0097] A10、根据A1所述的方法，其特征在于，将所述任务请求发送给所述分析引擎进行分析包括：

[0098] 获取分析引擎的调取指令；

[0099] 根据所述调取指令向所述分析引擎发送任务请求。

[0100] A11、根据A1所述的方法，其特征在于，将所述任务请求发送给所述分析引擎进行分析还包括：

[0101] 设置预置的时间间隔；

[0102] 根据所述时间间隔定时向所述分析引擎发送任务请求。

[0103] B12、一种虚拟机逃逸的防护装置，其特征在于，所述装置包括：

[0104] 缓存单元，用于将获取到的任务请求缓存至协线程，其中，所述任务请求为分析引擎获取的对虚拟机对外操作行为的分析请求，所述协线程用于协助所述分析引擎缓存所述任务请求；

[0105] 判断单元，用于由所述协线程判断所述缓存单元缓存的任务请求是否为已知的虚拟机逃逸行为；

[0106] 保存单元，用于当所述判断单元判断所述任务请求不是虚拟机逃逸行为时，保存所述任务请求，以便发送给所述分析引擎进行分析。

[0107] B13、根据B12所述的装置，其特征在于，所述缓存单元包括：

[0108] 创建模块，用于创建虚拟机的任务请求队列；

[0109] 添加模块，用于将所述任务请求添加到所述创建模块创建的任务请求队列中。

[0110] B14、根据B12所述的装置，其特征在于，所述判断单元包括：

[0111] 提取模块，用于提取所述任务请求中的操作行为；

[0112] 匹配模块，用于将所述提取模块提取的操作行为与已知的虚拟机逃逸行为进行匹配。

[0113] B15、根据B14所述的装置，其特征在于，所述装置还包括：

[0114] 建立单元，用于在所述判断单元由所述协线程判断所述任务请求是否为已知的虚拟机逃逸行为之前，建立虚拟机逃逸行为列表，所述列表中记录有当前已知的所有属于虚拟机逃逸的操作行为特征信息；

[0115] 更新单元，用于根据所述分析引擎的分析结果，更新所述建立单元建立的虚拟机逃逸行为列表。

[0116] B16、根据B15所述的装置，其特征在于，所述匹配模块包括：

[0117] 提取子模块，用于提取所述操作行为中的特征信息；

[0118] 判断子模块，用于遍历所述虚拟机逃逸行为列表，判断所述虚拟机逃逸行为列表中是否存在所述提取子模块提取的特征信息；

[0119] 确定子模块，用于当所述判断子模块判断所述虚拟机逃逸行为列表中存在所述特征信息时，确定所述操作行为是虚拟机逃逸行为。

[0120] B17、根据B16所述的装置，其特征在于，所述确定子模块还用于，当具有多个特征信息时，计算特征相似度比值，所述特征相似度比值是确定为虚拟机逃逸行为列表中的特征信息占所有特征信息的比值；当所述特征相似度比值大于预设值时，确定所述操作行为是虚拟机逃逸行为。

[0121] B18、根据B16所述的装置，其特征在于，所述提取子模块提取的特征信息包括：根据所述操作行为计算得出的MD5值。

[0122] B19、根据B12所述的装置，其特征在于，所述缓存单元还用于，根据所述分析引擎的处理能力，将所述分析引擎无法处理的任务请求缓存至所述协线程。

[0123] B20、根据B12所述的装置，其特征在于，所述装置还包括：

[0124] 阻止单元，用于当所述协线程判断所述任务请求为已知的虚拟机逃逸行为时，所述协线程阻止该任务请求发送给所述分析引擎。

[0125] B21、根据B12所述的装置，其特征在于，所述保存单元包括：

[0126] 获取模块，用于获取分析引擎的调取指令；

[0127] 第一发送模块，用于根据所述获取模块获取的调取指令向所述分析引擎发送任务请求。

[0128] B22、根据B12所述的装置，其特征在于，所述保存单元还包括：

[0129] 设置模块，用于设置预置的时间间隔；

[0130] 第二发送模块，用于根据所述设置模块设置的时间间隔定时向所述分析引擎发送任务请求。

[0131] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

[0132] 可以理解的是，上述方法及装置中的相关特征可以相互参考。另外，上述实施例中的“第一”、“第二”等是用于区分各实施例，而并不代表各实施例的优劣。

[0133] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统，装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0134] 在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求

的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

[0135] 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

[0136] 类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

[0137] 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书(包括伴随的权利要求、摘要和附图)中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书(包括伴随的权利要求、摘要和附图)中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0138] 此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0139] 本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器(DSP)来实现根据本发明实施例的发明名称(如确定网站内链接等级的装置)中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序(例如，计算机程序和计算机程序产品)。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

[0140] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项

来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

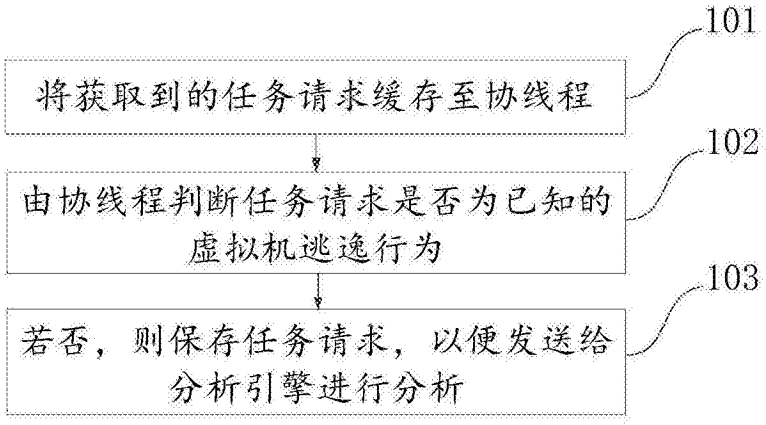

101
将获取到的任务请求缓存至协线程
102
由协线程判断任务请求是否为已知的虚拟机逃逸行为
103
若否，则保存任务请求，以便发送给分析引擎进行分析

图1

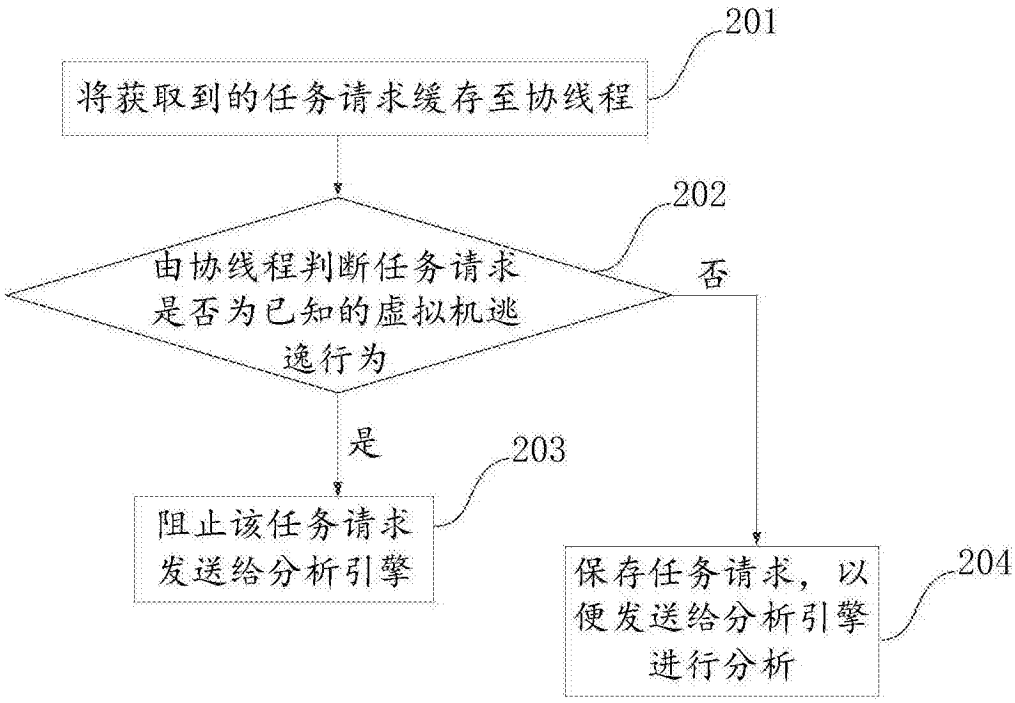

201
将获取到的任务请求缓存至协线程
202
由协线程判断任务请求是否为已知的虚拟机逃逸行为
否
是
203
阻止该任务请求发送给分析引擎
204
保存任务请求，以便发送给分析引擎进行分析

图2

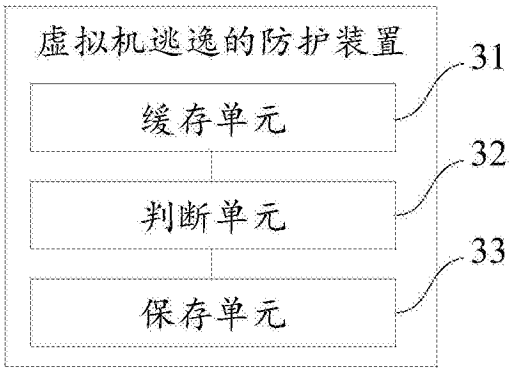


图3

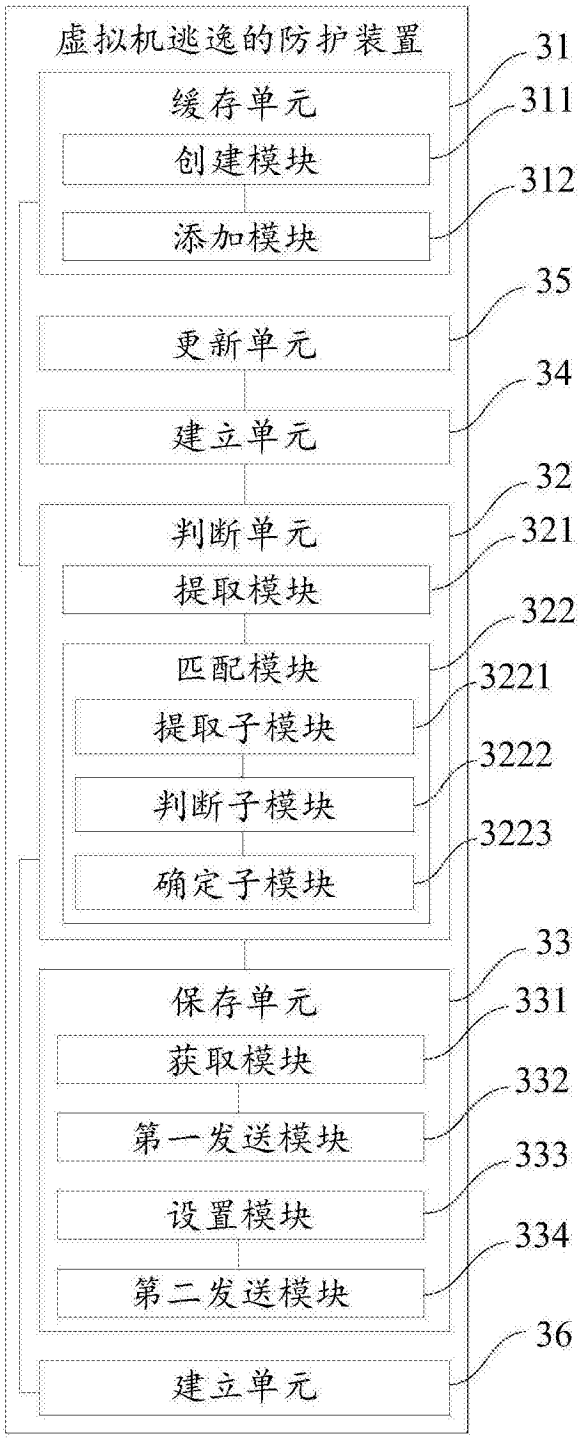

虚拟机逃逸的防护装置
缓存单元
创建模块
添加模块
更新单元
建立单元
判断单元
提取模块
匹配模块
提取子模块
判断子模块
确定子模块
保存单元
获取模块
第一发送模块
设置模块
第二发送模块
建立单元
31
311
312
35
34
32
321
322
3221
3222
3223
33
331
332
333
334
36

图4