(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 108459899 B
(45)授权公告日 2021.06.01

(21)申请号 201710093800.6
(22)申请日 2017.02.21
(65)同一申请的已公布的文献号
申请公布号 CN 108459899 A
(43)申请公布日 2018.08.28
(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
(72)发明人 夏虞斌 袁劲枫
(74)专利代理机构 北京三高永信知识产权代理有限责任公司 11138
代理人 罗振安
(51)Int.Cl.
G06F 9/455(2006.01)

(56)对比文件
US 2012255013 A1,2012.10.04
CN 104468568 A,2015.03.25
CN 105956465 A,2016.09.21

审查员 张文全

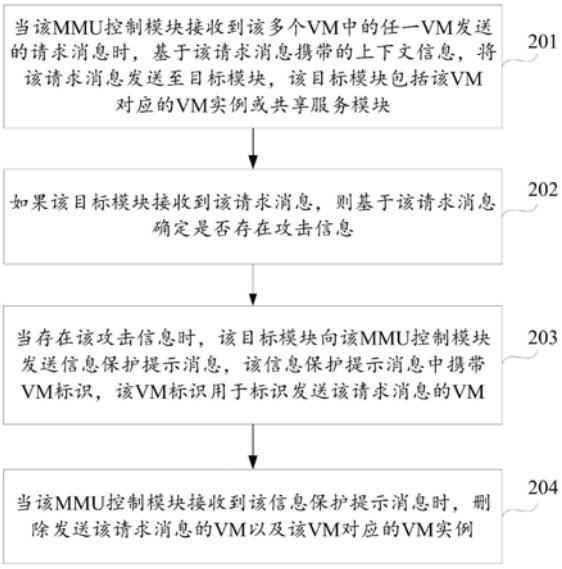
权利要求书3页 说明书12页 附图4页

(54)发明名称

信息保护方法及装置

(57)摘要

本发明实施例公开了一种信息保护方法及装置，属于虚拟化技术领域。应用于信息保护装置，该信息保护装置包括：VMM和多个VM；该VMM包括MMU控制模块、多个VM实例和共享服务模块，该多个VM实例与多个VM一一对应。当MMU控制模块接收到多个VM中的任一VM发送的请求消息时，可以基于该请求消息携带的上下文信息，将该请求消息发送至VM对应的VM实例或共享服务模块；如果VM实例或共享服务模块确定存在攻击信息，则可以向MMU控制模块发送信息保护提示消息，以使MMU控制模块在接收到该信息保护提示消息时，删除发送该请求消息的VM以及该VM对应的VM实例，从而避免了攻击信息影响到其它模块，达到了信息保护的目的。



CN 108459899 B

1.一种信息保护方法,其特征在于,应用于信息保护装置,所述信息保护装置包括:虚拟机监视器VMM和多个虚拟机VM;所述VMM包括内存管理MMU控制模块、多个VM实例和共享服务模块,所述多个VM实例与所述多个VM一一对应,且所述MMU控制模块、所述多个VM和所述共享服务模块之间均相互独立且相互隔离,所述多个VM实例中的任一VM实例用于存储对应的VM的运行信息,所述MMU控制模块用于管理控制所述共享服务模块和所述多个VM实例的数据,以确保所述共享服务模块和所述多个VM实例之间的相互隔离;

所述方法包括:

当所述MMU控制模块接收到所述多个VM中的任一VM发送的请求消息时,基于所述请求消息携带的上下文信息,向目标模块发送所述请求消息,所述目标模块包括所述VM对应的VM实例或所述共享服务模块;

如果所述目标模块接收到所述MMU控制模块发送的所述请求消息,则基于所述请求消息确定是否存在攻击信息;

当存在所述攻击信息时,所述目标模块向所述MMU控制模块发送信息保护提示消息,所述信息保护提示消息中携带VM标识,所述VM标识用于标识发送所述请求消息的VM;

当所述MMU控制模块接收到所述信息保护提示消息时,删除发送所述请求消息的VM以及所述VM对应的VM实例。

2.根据权利要求1所述的方法,其特征在于,所述MMU控制模块包括检测单元;

所述当所述MMU控制模块接收到所述多个VM中的任一VM发送的请求消息时,基于所述请求消息携带的上下文信息,向目标模块发送所述请求消息,包括:

当所述检测单元接收到所述多个VM中任一VM发送的请求消息时,将所述请求消息携带的上下文信息进行解析,以确定所述请求消息所请求的事件的事件类型;

基于所述事件类型,从所述VM对应的VM实例和所述共享服务模块中确定目标模块,并将向所述目标模块发送所述请求消息。

3.根据权利要求2所述的方法,其特征在于,所述将所述请求消息携带的上下文信息进行解析之后,还包括:

判断所述请求消息是否满足安全规则,所述安全规则用于描述访问所述VMM的条件;

当所述请求消息满足所述安全规则时,基于所述事件类型,从所述VM对应的VM实例和所述共享服务模块中确定目标模块,并将所述请求消息输出至所述目标模块;

当所述请求消息不满足所述安全规则时,向发送所述请求消息的VM发送出错提示信息,以将所述请求消息的出错原因提示给所述VM。

4.根据权利要求3所述的方法,其特征在于,所述安全规则为所述请求消息中携带安全验证信息;

所述判断所述请求消息是否满足安全规则,包括:

判断所述请求消息携带的上下文信息中是否包括安全验证信息;

当所述上下文信息中包括所述安全验证信息时,确定所述请求消息满足所述安全规则;

当所述上下文信息中不包括所述安全验证信息时,确定所述请求消息不满足所述安全规则。

5.根据权利要求3所述的方法,其特征在于,所述安全规则为所述请求消息中未携带指

定参数,所述指定参数为所述VMM无法处理的参数;

所述判断所述请求消息是否满足安全规则,包括:

判断所述请求消息的上下文信息中是否携带所述指定参数;

当所述请求消息中未携带所述指定参数时,确定所述请求消息满足所述安全规则;

当所述请求消息中携带所述指定参数时,确定所述请求消息不满足所述安全规则。

6.根据权利要求1-5任一所述的方法,其特征在于,所述目标模块为所述共享服务模块且所述共享服务模块;所述基于所述请求消息确定是否存在攻击信息,包括:

对所述请求消息进行处理以确定所述请求消息中是否包含指定数据的更新操作;

当确定所述请求消息中包含指定数据的更新操作时,确定存在攻击信息。

7.根据权利要求1-5任一所述的方法,其特征在于,所述目标模块为VM实例;所述基于所述请求消息确定是否存在攻击信息,包括:对所述请求消息进行处理;

当所述VM实例在对所述请求消息进行处理的过程中运行错误时,确定存在攻击信息。

8.根据权利要求7所述的方法,其特征在于,所述对所述请求消息进行处理,包括:

当所述上下文信息用于指示所述VM实例访问所述多个VM实例共享的信息时,所述VM实例对所述请求消息进行处理,得到第一更新请求消息;

相应地,所述对所述请求消息进行处理之后,还包括:

当所述VM实例在对所述请求消息进行处理的过程中未运行错误时,将所述第一更新请求消息发送至所述共享服务模块;

所述共享服务模块接收所述第一更新请求消息,并对所述第一更新请求消息进行处理;

在对所述第一更新请求消息进行处理过程中,当所述共享服务模块检测到指定数据的更新操作时,确定存在攻击信息。

9.根据权利要求7所述的方法,其特征在于,所述对所述请求消息进行处理,包括:

当所述上下文信息用于指示所述VM实例访问所述MMU控制模块所控制的硬件信息时,所述VM实例对所述请求消息进行处理,得到第二更新请求消息;

相应地,所述对所述请求消息进行处理之后,还包括:

当所述VM实例在对所述请求消息进行处理的过程中未运行错误时,将所述第二更新请求消息发送至所述MMU控制模块;

所述MMU控制模块接收所述第二更新请求消息,并对所述第二更新请求消息进行处理;

在所述MMU控制模块对所述第二更新请求消息进行处理的过程中,判断所述第二更新请求消息是否满足安全规则;

当所述第二更新请求消息不满足所述安全规则时,所述MMU控制模块确定存在所述攻击信息。

10.一种信息保护装置,其特征在于,所述信息保护装置包括:虚拟机监视器VMM和多个虚拟机VM;所述VMM包括内存管理MMU控制模块、多个VM实例和共享服务模块,所述多个VM实例与所述多个VM一一对应,且所述MMU控制模块、所述多个VM和所述共享服务模块之间均相互独立且相互隔离,所述多个VM实例中的任一VM实例用于存储对应的VM的运行信息;

所述MMU控制模块,用于管理控制所述共享服务模块和所述多个VM实例的数据,以确保所述共享服务模块和所述多个VM实例之间的相互隔离,并用于对VM到VMM的控制流进行检

测和转发；

其中，所述多个VM中每个VM在所述VMM中都对应一个VM实例；

其中，所述共享服务模块包含不能被放入VM实例中的、所有VM共享的数据，和操作这些数据的代码；

其中，所述共享服务模块拥有独立的地址空间，受到MMU控制模块的隔离保护。

11.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质中存储有计算机指令，当所述计算机指令在被处理器运行时实现如权利要求1至权利要求9中任一项所述的信息保护方法。

12.一种物理主机，其特征在于，所述物理主机包括：发射器、接收器、存储器和处理器，所述存储器、所述发送器和所述接收器分别与所述处理器连接，所述存储器存储有计算机程序指令，所述处理器运行所述计算机程序指令以执行权利要求1至权利要求9中任一项所述的信息保护方法。

信息保护方法及装置

技术领域

[0001] 本发明实施例涉及虚拟化技术领域,特别涉及一种信息保护方法及装置。

背景技术

[0002] 虚拟化技术涉及的系统架构通常包括如图1A所示的物理硬件1、虚拟机监控器2(Virtual Machine Monitor,VMM)和多个虚拟机3(Virtual Machine,VM)。其中,物理硬件1一般是物理主机中的硬件资源,该VMM2可以负责所有硬件资源的管理和分配,并为运行的多个VM3提供相互间的隔离,从而实现单台物理主机上运行多个操作系统的目的,提高硬件资源的利用率。另外,由于该VMM具备系统最高的特权级,因此,一旦VMM存在漏洞或者错误,又或者受到攻击时,将会对整个物理主机造成严重的安全威胁,比如,拒绝服务攻击、VM逃逸、信息泄露等等。

[0003] 目前,为了避免VMM存在漏洞或错误,或者在VMM受到攻击时,导致整个物理主机的信息安全受到威胁,该物理主机在创建VM时,会为该VM分配好CPU、内存、虚拟设备等资源,并通过扩展页表(Extended Page Table,EPT)隔离不同VM的内存,用硬件提供的虚拟硬件功能隔离输入/输出(Input/Output,I/O),使每个VM启动后完全依靠硬件提供的功能相互隔离、独立运转。

[0004] 但是,由于对该多个VM的隔离是通过硬件功能实现的,使用的限制较大。另外,支持VM运行的资源是事先分配好的,导致后续进行资源调度的灵活性下降,比如,物理CPU之间无法做负载均衡,不能动态的分配内存,降低了资源的利用率,从而失去了虚拟化平台最大的优势。

发明内容

[0005] 为了避免VMM存在漏洞或错误,或者在VMM受到攻击时,导致整个物理主机的信息安全受到威胁,本发明实施例提供了一种信息保护方法及装置。所述技术方案如下:

[0006] 第一方面,提供了一种信息保护方法,应用于信息保护装置,所述信息保护装置包括:VMM和多个VM;所述VMM包括内存管理(Memory Management Unite,MMU)控制模块、多个VM实例和共享服务模块,所述多个VM实例与所述多个VM一一对应,且所述MMU控制模块、所述多个VM和所述共享服务模块之间均相互独立且相互隔离;

[0007] 所述方法包括:

[0008] 当所述MMU控制模块接收到所述多个VM中的任一VM发送的请求消息时,基于所述请求消息携带的上下文信息,将所述请求消息发送至目标模块,所述目标模块包括所述VM对应的VM实例或所述共享服务模块;

[0009] 如果所述目标模块接收到所述请求消息,则基于所述请求消息确定是否存在攻击信息;

[0010] 当存在所述攻击信息时,所述目标模块向所述MMU控制模块发送信息保护提示消息,所述信息保护提示消息中携带VM标识,所述VM标识用于标识发送所述请求消息的VM;

[0011] 当所述MMU控制模块接收到所述信息保护提示消息时，删除发送所述请求消息的VM以及所述VM对应的VM实例。

[0012] 需要说明的是，该上下文信息中可以包括个寄存器的值、事件参数等等。另外，该VM标识用于唯一标识VM，且该VM标识可以为VM的地址信息、VM的名称等等。

[0013] 值得说明的是，本发明实施例通过将VMM划分成多个相互独立和相互隔离的模块，也即是，将该VMM划分为共享服务模块、MMU控制模块和多个VM实例，且共享服务模块、MMU控制模块和多个VM实例之间均相互独立且相互隔离，从而将VMM中出现的攻击信息限制在单个独立的模块当中，避免影响到其它域模块，进而达到了信息保护的目的。

[0014] 可选地，所述MMU控制模块包括检测单元；

[0015] 所述当所述MMU控制模块接收到所述多个VM中的任一VM发送的请求消息时，基于所述请求消息携带的上下文信息，将所述请求消息发送至目标模块，包括：

[0016] 当所述检测单元接收到所述多个VM中任一VM发送的请求消息时，将所述请求消息携带的上下文信息进行解析，以确定所述请求消息所请求的事件的事件类型；

[0017] 基于所述事件类型，从所述VM对应的VM实例和所述共享服务模块中确定目标模块，并将所述请求消息输出至所述目标模块。

[0018] 需要说明的是，该检测单元可以包括Gatekeeper，该Gatekeeper即为MMU控制模块对外提供的一个消息入口。

[0019] 可选地，所述将所述请求消息携带的上下文信息进行解析之后，还包括：

[0020] 判断所述请求消息是否满足安全规则，所述安全规则用于描述访问所述VMM的条件；

[0021] 当所述请求消息满足所述安全规则时，执行所述基于所述事件类型，从所述VM对应的VM实例和所述共享服务模块中确定目标模块，并将所述请求消息输出至所述目标模块的操作；

[0022] 当所述请求消息不满足所述安全规则时，向发送所述请求消息的VM发送出错提示信息，以将所述请求消息的出错原因提示给所述VM。

[0023] 需要说明的是，该安全规则可以事先设置，比如，该安全规则为请求消息中未携带指定参数、该请求消息中携带安全验证信息等等。

[0024] 可选地，所述安全规则为所述请求消息中携带安全验证信息；

[0025] 所述判断所述请求消息是否满足安全规则，包括：

[0026] 判断所述请求消息携带的上下文信息中是否包括安全验证信息；

[0027] 当所述上下文信息中包括所述安全验证信息时，确定所述请求消息满足所述安全规则；

[0028] 当所述上下文信息中不包括所述安全验证信息时，确定所述请求消息不满足所述安全规则。

[0029] 可选地，所述安全规则为所述请求消息中未携带指定参数，所述指定参数为所述VMM无法处理的参数；

[0030] 所述判断所述请求消息是否满足安全规则，包括：

[0031] 判断所述请求消息的上下文信息中是否携带所述指定参数；

[0032] 当所述请求消息中未携带所述指定参数时，确定所述请求消息满足所述安全规

则；

[0033] 当所述请求消息中携带所述指定参数时，确定所述请求消息不满足所述安全规则。

[0034] 可选地，所述基于所述请求消息确定是否存在攻击信息，包括：

[0035] 对所述请求消息进行处理；

[0036] 当所述目标模块为所述共享服务模块且所述共享服务模块在对所述请求消息进行处理的过程中检测到指定数据的更新操作时，确定存在攻击信息。

[0037] 所述对所述请求消息进行处理之后，还包括：

[0038] 当所述目标模块为VM实例且所述VM实例在对所述请求消息进行处理的过程中运行错误时，确定存在攻击信息。

[0039] 其中，在该共享服务模块中，该指定数据为共享服务模块独占的数据，该指定数据在共享服务模块中为只读模式，也即是，该指定该数据为不可更改的数据，因此，当该共享服务模块在对该请求消息进行处理的过程中检测到指定数据的更新操作时，可以确定存在攻击信息。

[0040] 需要说明的是，该指定数据可以事先设置，比如，该指定数据可以为中断向量表、数据结构的映射、错误处理函数、页表权限的设置信息等等。

[0041] 可选地，当该目标模块为该共享服务模块且该共享服务模块在对该请求消息进行处理的过程中未检测到指定数据的更新操作时，确定不存在攻击信息，此时该共享服务模块可以根据请求消息的上下文信息，将对请求消息处理的结果发送至VM实例或MMU控制模块。

[0042] 可选地，所述对所述请求消息进行处理，包括：

[0043] 当所述目标模块为VM实例且所述上下文信息用于指示所述VM实例访问所述多个VM实例共享的信息时，所述VM实例对所述请求消息进行处理，得到第一更新请求消息；

[0044] 相应地，所述对所述请求消息进行处理之后，还包括：

[0045] 当所述VM实例在对所述请求消息进行处理的过程中未运行错误时，将所述第一更新请求消息发送至所述共享服务模块；

[0046] 所述共享服务模块接收所述第一更新请求消息，并对所述第一更新请求消息进行处理；

[0047] 在对所述第一更新请求消息进行处理过程中，当所述共享服务模块检测到指定数据的更新操作时，确定存在攻击信息。

[0048] 由于共享服务模块可能会同时接收到多个更新请求消息，因此，为了方便后续MMU控制模块的操作，该共享服务模块可以通过错误处理函数确定存在攻击信息的模块。

[0049] 可选地，该共享服务模块接收该第一更新请求消息，并对该第一更新请求消息进行处理；在对该第一更新请求消息进行处理过程中，该共享服务模块未检测到指定数据的更新操作时，可以确定不存在攻击信息。此时，该共享服务模块可以根据第一更新请求消息的上下文信息，将对第一更新请求消息处理的结果发送至VM实例或MMU控制模块。

[0050] 可选地，所述对所述请求消息进行处理，包括：

[0051] 当所述目标模块为VM实例且所述上下文信息用于指示所述VM实例访问所述MMU控制模块所控制的硬件信息时，所述VM实例对所述请求消息进行处理，得到第二更新请求消

息；

[0052] 相应地，所述对所述请求消息进行处理之后，还包括：

[0053] 当所述VM实例在对所述请求消息进行处理的过程中未运行错误时，将所述第二更新请求消息发送至所述MMU控制模块；

[0054] 所述MMU控制模块接收所述第二更新请求消息，并对所述第二更新请求消息进行处理；

[0055] 在所述MMU控制模块对所述第二更新请求消息进行处理的过程中，判断所述第二更新请求消息是否满足安全规则；

[0056] 当所述第二更新请求消息不满足所述安全规则时，所述MMU控制模块确定存在所述攻击信息。

[0057] 由于该MMU控制模块为本发明实施例中的TCB(Trusted Computing Base，可信计算基)，为了保证信息的安全，该MMU控制模块可以对接收到的任何一个请求消息进行安全性检测，因此，该MMU控制模块对该第二更新请求消息进行处理时，可以判断该第二更新请求消息是否满足安全规则。其中，可信计算基，是指为实现计算基系统安全保护的所有安全保护机制的集合，被认为是系统唯一安全和可信的模块。

[0058] 可选地，当该第二更新请求消息满足该安全规则时，该MMU控制模块确定不存在该攻击信息，此时该MMU控制模块可以完成对第二更新请求消息的处理。

[0059] 第二方面，提供了一种信息保护装置，所述信息保护装置具有实现上述第一方面中信息保护方法行为的功能。该息保护装置包括至少一个模块，该至少一个模块用于实现上述第一方面所提供的信息保护方法。

[0060] 第三方面，提供了一种物理主机，该物理主机包括：发射器、接收器、存储器和处理器，所述存储器、所述发送器和所述接收器分别与所述处理器连接，所述存储器存储有程序代码，所述处理器用于调用程序代码，执行上述第一方面所述的息保护方法。

[0061] 第四方面，提供了一种计算机存储介质，用于储存为上述第三方面提供的物理主机所用的计算机软件指令，其包含用于执行上述第一方面所设计的程序。

[0062] 本发明实施例提供的技术方案带来的有益效果是：本发明实施例中，由于VMM包括共享服务模块、MMU控制模块和多个VM实例，且共享服务模块、MMU控制模块和多个VM实例之间均相互独立且相互隔离，因此，当该VMM接收到多个VM中任一VM发送的请求消息，并确定存在攻击信息时，该MMU控制模块可以直接将发送该请求消息的VM和与该VM对应的VM实例进行删除，从而避免了攻击信息影响到其它模块，达到了信息保护的目的。

附图说明

[0063] 图1A是本发明实施例提供的一种虚拟化技术的系统架构的结构示意图；

[0064] 图1B是本发明实施例提供的一种信息保护系统架构的结构示意图；

[0065] 图1C是本发明实施例提供的一种请求消息处理方向的示意图；

[0066] 图1D是本发明实施例提供的一种物理主机的结构示意图；

[0067] 图2是本发明实施例提供的一种信息保护方法流程图；

[0068] 图3A是本发明实施例提供的一种信息保护装置结构示意图；

[0069] 图3B是本发明实施例提供的另一种信息保护装置结构示意图。

具体实施方式

[0070] 为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明实施方式作进一步地详细描述。

[0071] 在对本发明实施例进行详细地解释说明之前，先对本发明实施例的系统架构予以说明。图1B是本发明实施例提供的一种信息保护系统架构，该系统架构用于物理主机中，包括VMM2和多个VM。该VMM2包括MMU控制模块21、共享服务模块22和多个VM实例23，该多个VM实例与该多个VM一一对应，该MMU控制模块、该多个VM和该共享服务模块之间均相互独立且相互隔离，且该多个实例可以包括XEN实例、KVM实例等等。在图示1A和图示1B中，分别以3个VM和3个VM实例为例进行说明，并不对本发明实施例构成限定。比如，如图1B所示，该VM实例23A与VM3A对应，该VM实例23B与VM3B对应，该VM实例23C与VM3C对应。

[0072] 其中，本发明实施例中，可以通过嵌套MMU虚拟化技术在VMM中，划分出MMU控制模块、共享服务模块和多个VM实例。该MMU控制模块负责整个VMM中各个模块之间的相互隔离，该MMU控制模块包括对于MMU进行更新操作的访问控制代码，也即是，该MMU控制模块中可以包括物理硬件相关的硬件信息，且该MMU控制模块可以对共享服务模块和该多个VM实例的数据进行管理控制；该MMU控制模块为本发明实施例中的可信计算基(Trusted Computing Base，TCB)，该MMU控制模块为唯一安全且可信的模块。共享服务模块中存储该多个VM实例共享的信息，比如，该共享的信息可以包括用于记录物理内存相关信息的全局物理页描述数组等，且该多个VM实例共享的信息可以为多个VM实例对应的多个VM在创建过程中映射至该共享服务模块得到。因此，该共享服务模块能够向该多个VM实例提供共享服务，该共享服务可以包括VM调度、多个VM之间的通信或多个VM的物理内存分配及管理等等。该多个VM实例中的任一VM实例用于存储对应的VM的运行信息，比如，指令模拟功能，I/O请求处理、异常处理、虚拟机页表更新等等。多个VM实例之间同样由MMU控制模块保证相互之间的隔离。

[0073] 另外，在不存在攻击信息的情况下，该VM实例向VMM发送请求消息后，该请求消息的处理方向可以参见图1C，该图1C中以一个VM实例2和一个VM3为例进行说明。该MMU控制模块21可以将该请求消息发送至共享服务模块22或者该VM3对应的VM实例2。如果该VM实例2接收到该请求消息，并对该请求消息处理后，可以基于该请求消息的上下文信息，将该请求消息的处理结果发送至MMU控制模块21，使MMU控制模块21进行更新操作；或者，将该请求消息的处理结果发送至MMU控制模块21，由MMU控制模块将该请求消息的处理结果转发至该VM3；或者，该VM实例可以将该请求消息的处理结果发送至共享服务模块，以获取共享服务模块中共享的信息。如果该共享服务模块接收到该请求消息，并对该请求消息处理后，将该请求消息的处理结果发送至MMU控制模块，使MMU控制模块进行更新操作；或者，将该请求消息的处理结果发送至MMU控制模块，由MMU控制模块将该请求消息的处理结果转发至该VM；或者，将该请求消息的处理结果发送至VM实例，使该VM实例继续基于该请求消息的处理结果进行相关处理操作。

[0074] 图1D是本发明实施例提供的一种物理主机的结构示意图，该物理主机主要包括有一个或者一个以上处理核心的处理器110、包括有一个或一个以上计算机可读存储介质的存储器120、通信总线130、发射机140以及接收机150等，且该存储器120、发射机140和接收机150分别通过通信总线130与处理器110连接。本领域技术人员可以理解，图1D中示出的物理主机的结构并不构成对物理主机的限定，可以包括比图示更多或更少的部件，或者组合

某些部件,或者不同的部件布置,本发明实施例对此不做限定。

[0075] 其中,该处理器110是该物理主机的控制中心,该处理器110可以一个通用中央处理器(Central Processing Unit,CPU),微处理器,特定应用集成电路(application-specific integrated circuit,ASIC),或一个或多个用于控制本发明方案程序执行的集成电路。其中,该处理器110可以通过运行或执行存储在存储器120内的软件程序和/或模块,以及调用存储在存储器120内的数据,来实现下文图2实施例所提供的信息保护方法。

[0076] 其中,该存储器120可以是只读存储器(read-only memory,ROM)或可存储静态信息和指令的其它类型的静态存储设备,随机存取存储器(random access memory,RAM))或者可存储信息和指令的其它类型的动态存储设备,也可以是电可擦可编程只读存储器(Electrically Erasable Programmable Read-Only Memory,EEPROM)、只读光盘(Compact Disc Read-Only Memory,CD-ROM)或其它光盘存储、光碟存储(包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等)、磁盘存储介质或者其它磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由集成电路存取的任何其它介质,但不限于此。存储器120可以是独立存在,通过通信总线130与处理器110相连接。存储器120也可以和处理器110集成在一起。

[0077] 发射机140和接收机150,使用任何收发器一类的装置,用于与其它设备或通信网络通信,比如,无线局域网(Wireless LocalAreaNetworks,WLAN)等。

[0078] 另外,上述通信总线130可包括一通路,在上述处理器110、存储器120发射机140和接收机150之间传送信息。

[0079] 图2是本发明实施例提供的一种信息保护方法的流程图,参见图2,该方法用于信息保护装置,该信息保护装置包括:VMM和多个VM;该VMM包括MMU控制模块、多个VM实例和共享服务模块,该多个VM实例与该多个VM一一对应,且该MMU控制模块、该多个VM和该共享服务模块之间均相互独立且相互隔离;该方法包括如下步骤。

[0080] 步骤201:当该MMU控制模块接收到该多个VM中的任一VM发送的请求消息时,基于该请求消息携带的上下文信息,将该请求消息发送至目标模块,该目标模块包括该VM对应的VM实例或共享服务模块。

[0081] 通常情况下,多个VM与多个VM实例一一对应时,由于该多个VM之间实现的功能互不相同,因此,该VMM需要对外提供多个消息入口以接收不同功能的VM发送的请求消息。本发明实施例中,为了使MMU控制模块可以统一对该请求消息进行管理,可以将该多个不同的消息入口替换为MMU控制模块对外提供的一个消息入口。比如,将中断描述符表(Interrupt Descriptor Table,IDT)进行修改,使该多个VM中所有中断和异常的处理函数的多个消息入口均替换为MMU控制模块对外提供的一个消息入口,修改虚拟机控制结构(Virtual-Machine Control Structure,VMCS)的接口字段,使该接口字段执行MMU控制模块对外提供的一个消息入口等等,从而该MMU控制模块接收到请求消息时,可以基于该请求消息携带的上下文信息,将该请求消息发送至目标模块。

[0082] 值得说明的是,将该多个消息入口替换为一个消息入口之后,可以保证只能通过该一个消息入口进行对VMM的访问和对MMU的更新操作,从而提高了信息的安全性。

[0083] 需要说明的是,该上下文信息中可以包括寄存器的值、事件参数等等。

[0084] 其中,由于该上下文信息中包括寄存器的值、事件参数等可以指示事件类型,每个

事件类型对应一个模块。因此，当该MMU控制模块接收到该请求消息时，可以对该上下文信息进行解析，以确定该请求消息所请求的事件类型；根据该事件类型可以确定该事件类型对应的模块，并将该事件类型对应的模块确定为目标模块；之后，将该请求消息发送至该目标模块中。

[0085] 由于MMU控制模块可以包括检测单元，因此，当该MMU控制模块接收到该多个VM中的任一VM发送的请求消息时，基于该请求消息携带的上下文信息，将该请求消息发送至目标模块的操作可以为：当该检测单元接收到该多个VM中任一VM发送的请求消息时，将该请求消息携带的上下文信息进行解析，以确定该请求消息所请求的事件的事件类型；基于该事件类型，从该VM对应的VM实例和该共享服务模块中确定目标模块，并将该请求消息输出至该目标模块。

[0086] 需要说明的是，该检测单元可以包括Gatekeeper，该Gatekeeper即为MMU控制模块对外提供的消息入口。

[0087] 比如，当该多个VM中任一VM向VMM发送请求消息时，该检测单元可以对该请求消息的上下文信息进行解析，以确定该请求消息所请求的事件的事件类型。当该事件类型为访问VM实例的内部数据结构时，将该VM实例确定为目标模块，检测单元将该请求消息输出至该VM实例。当该事件类型为获取共享服务模块中多个VM实例共享的信息时，将该共享服务模块确定为目标模块，检测单元将该请求消息输出至该共享服务模块。

[0088] 进一步地，将该请求消息携带的上下文信息进行解析之后，该检测单元还可以判断该请求消息是否满足安全规则，该安全规则用于描述访问该VMM的条件；当该请求消息满足该安全规则时，执行基于该事件类型，从该VM对应的VM实例和该共享服务模块中确定目标模块，并将该请求消息输出至该目标模块的操作；当该请求消息不满足该安全规则时，向发送该请求消息的VM发送出错提示信息，以将该请求消息的出错原因提示给该VM。

[0089] 需要说明的是，该安全规则可以事先设置，比如，该安全规则为请求消息中未携带该VMM无法处理的指定参数、该请求消息中携带安全验证信息等等。

[0090] 在一种可能的实现方式中，当该安全规则为该请求消息中携带安全验证信息时，该检测单元可以判断该请求消息携带的上下文信息中是否包括安全验证信息；当该上下文信息中包括该安全验证信息时，确定该请求消息满足该安全规则；当该上下文信息中不包括该安全验证信息时，确定该请求消息不满足该安全规则。

[0091] 在另一种可能的实现方式中，当该安全规则为该请求消息中未携带指定参数时，该检测单元可以判断该请求消息的上下文信息中是否携带该指定参数；当该请求消息中未携带该指定参数时，确定该请求消息满足该安全规则；当该请求消息中携带该指定参数时，确定该请求消息不满足该安全规则。

[0092] 步骤202：如果该目标模块接收到该请求消息，则基于该请求消息确定是否存在攻击信息。

[0093] 具体地，如果该目标模块接收到该请求消息，则对该请求消息进行处理；当该目标模块为该共享服务模块且该共享服务模块在对该请求消息进行处理的过程中检测到指定数据的更新操作时，确定存在攻击信息；当该目标模块为VM实例且该VM实例在对该请求消息进行处理的过程中运行错误时，确定存在攻击信息。

[0094] 在一种可能的实现方式中，当该目标模块为VM实例时，在通常情况下，该VM实例可

以对请求消息进行处理，得到对该请求消息的处理结果，该VM实例可以将该请求消息的处理结果发送至MMU控制模块，该MMU控制模块可以将该请求消息的处理结果转发至该VM实例对应的VM。由于在上述过程中所有操作均只涉及到VM及VM对应的实例，因此当存在攻击信息并造成VM实例的运行错误时，仅仅只会影响到该VM实例，对其他模块并未产生影响。

[0095] 在另一种可能的实现方式中，当该目标模块为共享服务模块时，由于在在该共享服务模块中，该指定数据为共享服务模块独占的数据，该指定数据为共享服务模块最初创建时，向MMU控制模块申请独占内存后得到。另外，由于该指定数据在共享服务模块中为只读模式，也即是，该指定该数据为不可更改的数据，因此，当该共享服务模块在对该请求消息进行处理的过程中检测到指定数据的更新操作时，可以确定存在攻击信息。同时，由于该指定数据为只读模式，因此，该攻击信息无法对该指定数据造成影响，从而保护了该共享服务模块中的信息。

[0096] 需要说明的是，该指定数据可以事先设置，比如，该指定数据可以为中断向量表、数据结构的映射、错误处理函数、页表权限的设置信息等等。另外，对指定数据的更新操作可以包括对指定数据的更改、增加、删除等操作。

[0097] 另外，当该目标模块为该共享服务模块且该共享服务模块在对该请求消息进行处理的过程中未检测到指定数据的更新操作时，确定不存在攻击信息，此时该共享服务模块可以根据请求消息的上下文信息，将对请求消息处理的结果发送至VM实例或MMU控制模块。

[0098] 由于当目标模块为VM实例时，在VM实例对该请求消息处理的过程中，攻击信息可能已经对该VM实例进行了攻击，但是该攻击程度不足以使VM实例运行错误，此时，VM实例无法确定是否存在攻击信息，因此，该VM实例依旧可以将对请求消息处理后的结果发送至共享服务模块或者MMU控制模块，具体可以包括如下两种情况。

[0099] 第一种情况，当该目标模块为VM实例且该上下文信息用于指示该VM实例访问该多个VM实例共享的信息时，该VM实例对该请求消息进行处理，得到第一更新请求消息；当该VM实例在对该请求消息进行处理的过程中未运行错误时，可以将该第一更新请求消息发送至该共享服务模块；该共享服务模块接收该第一更新请求消息，并对该第一更新请求消息进行处理；在对该第一更新请求消息进行处理过程中，当该共享服务模块检测到指定数据的更新操作时，确定存在攻击信息。

[0100] 下面以保护中断向量表为例进行说明。

[0101] 在通常情况下，由于中断向量表为记录每个中断的处理函数的关键数据结构，当中断向量表遭到攻击信息的攻击时，为了保护数据可能会直接清空中断向量表，从而造成的信息的损失。为了避免此情况的发生，本发明实施例通过下述方式进行信息保护，具体过程如下：

[0102] 当MMU控制模块接收到VM创建请求时，从共享服务模块中复制一份地址空间作为该VM对应的XEN实例的地址空间，并改变需要保护的数据结构的映射，比如，需要保护的数据结构为中断向量表。

[0103] 其中，由于关于中断向量表的操作由共享服务模块负责，且共享服务模块独占中断向量表的内存页，也即是，该中断向量表在共享服务模块中为只读模式。因此，当该VM实施例接收到的请求消息为访问XEN实例的内部数据结构时，该XEN实例对该请求消息进行处理后，可能会生成对共享服务模块中的中断向量表进行更新的第一更新请求消息，之后该

XEN实例可以将该第一更新请求消息发送至共享服务模块;该共享服务模块在对该第一更新请求消息进行处理的过程中,检测到中断向量表的虚拟地址中有垃圾消息写入,此时,由于该中断向量表的虚拟地址为只读模式,因此,该垃圾消息将无法写入到该中断向量表的虚拟地址中,从而保护了该中断向量表,同时该共享服务模块可以确定存在攻击信息。

[0104] 另外,由于共享服务模块可能会同时接收到多个更新请求消息,因此,为了方便后续MMU控制模块的操作,该共享服务模块可以通过错误处理函数确定存在攻击信息的模块。

[0105] 再者,该共享服务模块接收该第一更新请求消息,并对该第一更新请求消息进行处理;在对该第一更新请求消息进行处理过程中,该共享服务模块未检测到指定数据的更新操作时,可以确定不存在攻击信息。此时,该共享服务模块可以根据第一更新请求消息的上下文信息,将对第一更新请求消息处理的结果发送至VM实例或MMU控制模块。

[0106] 第二种情况,当该目标模块为VM实例且该上下文信息用于指示该VM实例访问该MMU控制模块所控制的硬件信息时,VM实例对请求消息进行处理,得到第二更新请求消息;当该VM实例在对请求消息进行处理的过程中未运行错误时,将该第二更新请求消息发送至该MMU控制模块;该MMU控制模块接收该第二更新请求消息,并对该第二更新请求消息进行处理;在该MMU控制模块对该第二更新请求消息进行处理的过程中,判断该第二更新请求消息是否满足安全规则;当该第二更新请求消息不满足该安全规则时,该MMU控制模块确定存在该攻击信息。

[0107] 其中,由于该MMU控制模块为本发明实施例中的TCB,为了保证信息的安全,该MMU控制模块可以对接收到的任何一个请求消息进行安全性检测,因此,该MMU控制模块对该第二更新请求消息进行处理时,可以判断该第二更新请求消息是否满足安全规则。

[0108] 另外,当该第二更新请求消息满足该安全规则时,该MMU控制模块确定不存在该攻击信息,此时该MMU控制模块可以完成对第二更新请求消息的处理。

[0109] 进一步地,攻击信息不仅可以体现在对指定数据的更新,或者处理结果不满足安全规则上,还可以体现在计算资源的滥用,为了对本发明实施例进行更详细地说明,下面以解决计算资源滥用为例进行说明。

[0110] 由于VMM中存在不可打断且耗时长的操作,如果VM可以任意触发这些操作,则攻击信息可能会高频率的触发这些操作,从而使大量计算资源耗费在这些操作上,造成资源浪费,严重情况下可能会使CPU失去响应。为了避免上述情况的发生,本发明实施例通过下述方式进行信息保护,具体过程如下:

[0111] 由于在创建XEN实例时,MMU控制模块可以将该XEN实例对应的VM标识以只读的形式映射到其地址空间的固定位置中;当该VM实施例接收到的请求消息为访问XEN实例的内部数据结构时,该XEN实例对该请求消息进行处理后,可能会生成触发不可屏蔽的中断,该XEN实例可能会不断向MMU控制模块或者共享服务模块发送更新请求消息。但是由于该XEN实例对应的VM标识为只读模式,因此,该MMU控制模块或该共享服务模块可以根据该VM标识确定存在攻击信息的XEN实例。

[0112] 需要说明的是,该VM标识用于唯一标识VM,且该VM标识可以为VM的地址信息、VM的名称等等。

[0113] 步骤203:当存在该攻击信息时,该目标模块向该MMU控制模块发送信息保护提示消息,该信息保护提示消息中携带VM标识,该VM标识用于标识发送该请求消息的VM。

[0114] 其中，当存在攻击信息的攻击时，该MMU控制模块可能还会触发内存页错误提示信息，以提示用户存在攻击信息。

[0115] 步骤204：当该MMU控制模块接收到该信息保护提示消息时，删除发送该请求消息的VM以及该VM对应的VM实例。

[0116] 由于当该MMU控制模块接收到该信息保护提示消息时，证明存在攻击信息，为了保证VMM中其他模块中数据的安全性，该VMM可以删除发送该请求消息的VM以及该VM对应的VM实例。

[0117] 进一步地，当该MMU控制模块删除发送该请求消息的VM以及该VM对应的VM实例之后，可以重新创建与该删除的VM功能相同的VM及对应的VM实例。

[0118] 本发明实施例中，通过将VMM划分成多个相互独立和相互隔离的模块，也即是，将该VMM划分为共享服务模块、MMU控制模块和多个VM实例，且共享服务模块、MMU控制模块和多个VM实例之间均相互独立且相互隔离。当该多个VM中任一VM发送请求消息时，该MMU控制模块可以基于该请求消息的上下文信息将该请求消息发送至对应VM实例或共享服务模块，该VM实例或者共享服务模块可以对该请求消息进行处理，以确定是否存在攻击信息，并当存在攻击信息时，向MMU控制模块发送信息保护提示消息，当MMU控制模块接收到信息保护提示消息时，可以直接删除发送请求消息的VM以及VM对应的VM实例，从而将VMM中出现的攻击信息限制在单个独立的模块当中，避免了影响到其它的模块，从而达到了信息保护的目的。

[0119] 图3A是本发明实施例提供的一种信息保护装置的结构示意图，参见图3A，该信息保护装置包括：VMM301和多个VM302；该VMM301包括MMU控制模块3011、多个VM实例3012和共享服务模块3013，该多个VM实例3012与该多个VM302一一对应；

[0120] 该MMU控制模块3011，用于执行图2实施例中的步骤201；

[0121] 该目标模块303，用于执行图2实施例中的步骤202；

[0122] 该目标模块303，用于执行图2实施例中的步骤203；

[0123] 该MMU控制模块3011，用于执行图2实施例中的步骤204。

[0124] 可选地，参见图3B，该MMU控制模块3011包括检测单元30111；

[0125] 该检测单元30111用于：

[0126] 当接收到该多个VM中任一VM发送的请求消息时，将该请求消息携带的上下文信息进行解析，以确定该请求消息所请求的事件的事件类型；

[0127] 基于该事件类型，从该VM对应的VM实例和该共享服务模块中确定目标模块，并将该请求消息输出至该目标模块。

[0128] 可选地，该检测单元30111还用于：

[0129] 判断该请求消息是否满足安全规则，该安全规则用于描述访问该VMM的条件；

[0130] 当该请求消息满足该安全规则时，执行该基于该事件类型，从该VM对应的VM实例和该共享服务模块中确定目标模块，并将该请求消息输出至该目标模块的操作；

[0131] 当该请求消息不满足该安全规则时，向发送该请求消息的VM发送出错提示信息，以将该请求消息的出错原因提示给该VM。

[0132] 可选地，该安全规则为该请求消息中携带安全验证信息；

[0133] 该检测单元30111用于：

[0134] 判断该请求消息携带的上下文信息中是否包括安全验证信息；

[0135] 当该上下文信息中包括该安全验证信息时，确定该请求消息满足该安全规则；

[0136] 当该上下文信息中不包括该安全验证信息时，确定该请求消息不满足该安全规则。

[0137] 可选地，该安全规则为该请求消息中未携带指定参数，该指定参数为该VMM无法处理的参数；

[0138] 该检测单元30111用于：

[0139] 判断该请求消息的上下文信息中是否携带该指定参数；

[0140] 当该请求消息中未携带该指定参数时，确定该请求消息满足该安全规则；

[0141] 当该请求消息中携带该指定参数时，确定该请求消息不满足该安全规则。

[0142] 可选地，该目标模块303用于：

[0143] 对该请求消息进行处理；

[0144] 当该目标模块为该共享服务模块且该共享服务模块在对该请求消息进行处理的过程中检测到指定数据的更新操作时，确定存在攻击信息；

[0145] 可选地，该目标模块303还用于：

[0146] 当该目标模块为VM实例且该VM实例在对该请求消息进行处理的过程中运行错误时，确定存在攻击信息。

[0147] 可选地，该目标模块303用于：

[0148] 当该目标模块为VM实例且该上下文信息用于指示该VM实例访问该多个VM实例共享的信息时，该VM实例对该请求消息进行处理，得到第一更新请求消息；

[0149] 相应地，

[0150] 该目标模块303，还用于当该VM实例在对该请求消息进行处理的过程中未运行错误时，将该第一更新请求消息发送至该共享服务模块；

[0151] 该共享服务模块3013，还用于接收该第一更新请求消息，并对该第一更新请求消息进行处理；

[0152] 该共享服务模块3013，还用于在对该第一更新请求消息进行处理过程中，当检测到指定数据的更新操作时，确定存在攻击信息。

[0153] 可选地，该目标模块303用于：

[0154] 当该目标模块为VM实例且该上下文信息用于指示该VM实例访问该MMU控制模块所控制的硬件信息时，该VM实例对该请求消息进行处理，得到第二更新请求消息；

[0155] 相应地，

[0156] 该目标模块303，还用于当该VM实例在对该请求消息进行处理的过程中未运行错误时，将该第二更新请求消息发送至该MMU控制模块；

[0157] 该MMU控制模块3011，还用于接收该第二更新请求消息，并对该第二更新请求消息进行处理；

[0158] 该MMU控制模块3011，还用于对该第二更新请求消息进行处理的过程中，判断该第二更新请求消息是否满足安全规则；

[0159] 该MMU控制模块3011，还用于当该第二更新请求消息不满足该安全规则时，该MMU控制模块确定存在该攻击信息。

[0160] 本发明实施例中，通过将VMM划分成多个相互独立和相互隔离的模块，也即是，将该VMM划分为共享服务模块、MMU控制模块和多个VM实例，且共享服务模块、MMU控制模块和多个VM实例之间均相互独立且相互隔离。当该多个VM中任一VM发送请求消息时，该MMU控制模块可以基于该请求消息的上下文信息将该请求消息发送至对应VM实例或共享服务模块，该VM实例或者共享服务模块可以对该请求消息进行处理，以确定是否存在攻击信息，并当存在攻击信息时，向MMU控制模块发送信息保护提示消息，当MMU控制模块接收到信息保护提示消息时，可以直接删除发送请求消息的VM以及VM对应的VM实例，从而将VMM中出现的攻击信息限制在单个独立的模块当中，避免了影响到其它的模块，从而达到了信息保护的目的。

[0161] 需要说明的是：上述实施例提供的信息保护装置在进行信息保护时，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将装置的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。另外，上述实施例提供的信息保护装置与信息保护方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

[0162] 本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成，也可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[0163] 在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时，全部或部分地产生按照本发明实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线(例如同轴电缆、光线、数字用户线(Digital Subscriber Line,DSL))或无限(例如红外、无线、微波等)方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质，(例如，软盘、硬盘、磁带)、光介质(例如，数字化视频光盘(Digital Video Disk,DVD))、或者半导体介质(例如固态硬盘(Solid State Disk,SSD))等。

[0164] 以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。


VM
VM
VM
3
VMM
2
物理硬件
1

图1A

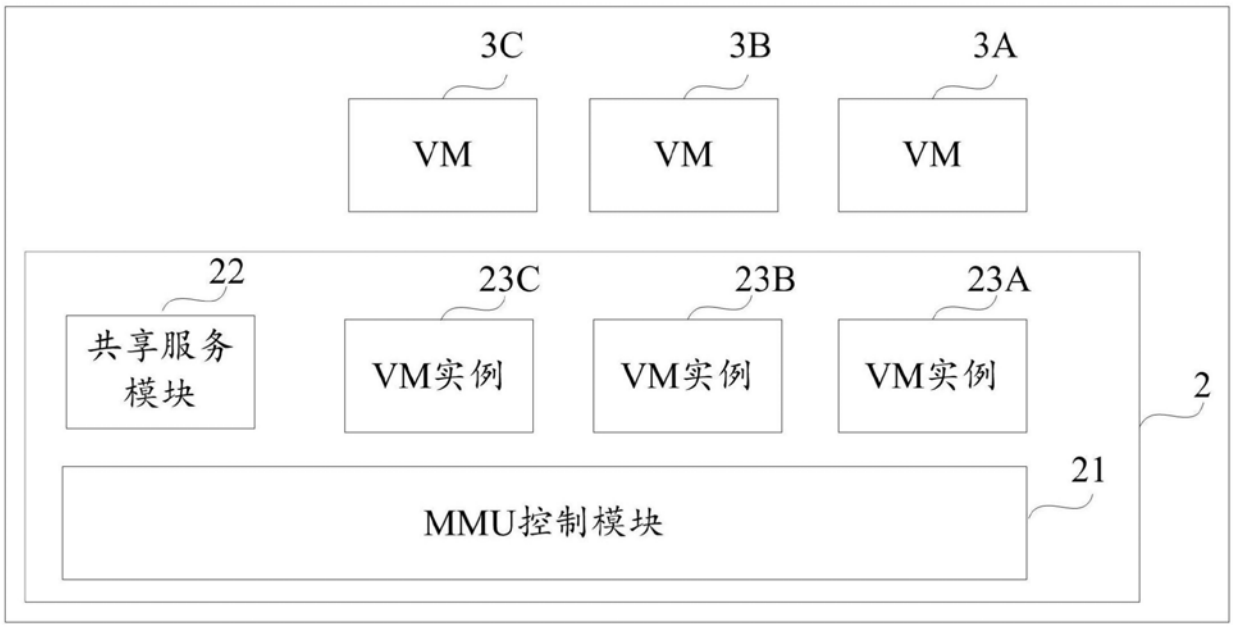

3C
3B
3A
VM
VM
VM
22
23C
23B
23A
共享服务模块
VM实例
VM实例
VM实例
2
21
MMU控制模块

图1B

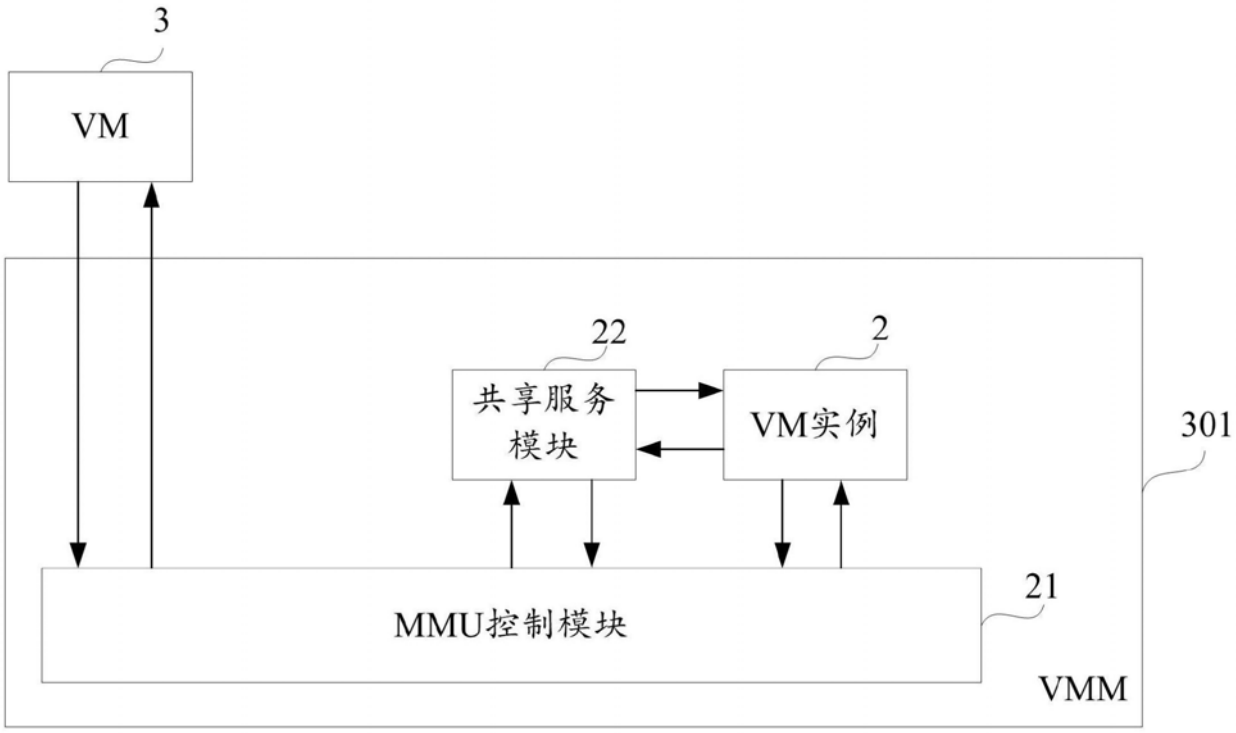

3
VM
22
共享服务模块
2
VM实例
301
21
MMU控制模块
VMM

图1C

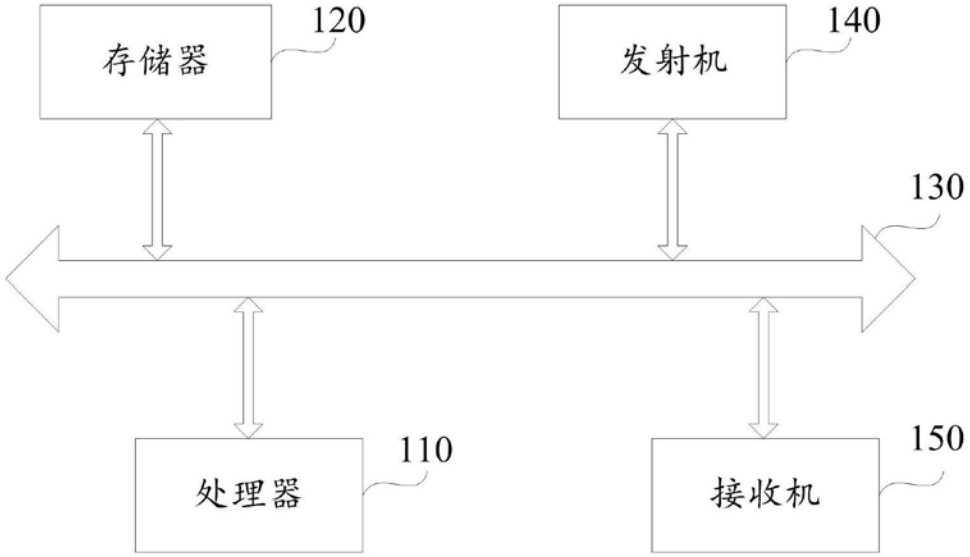

存储器
120
发射机
140
130
处理器
110
接收机
150

图1D

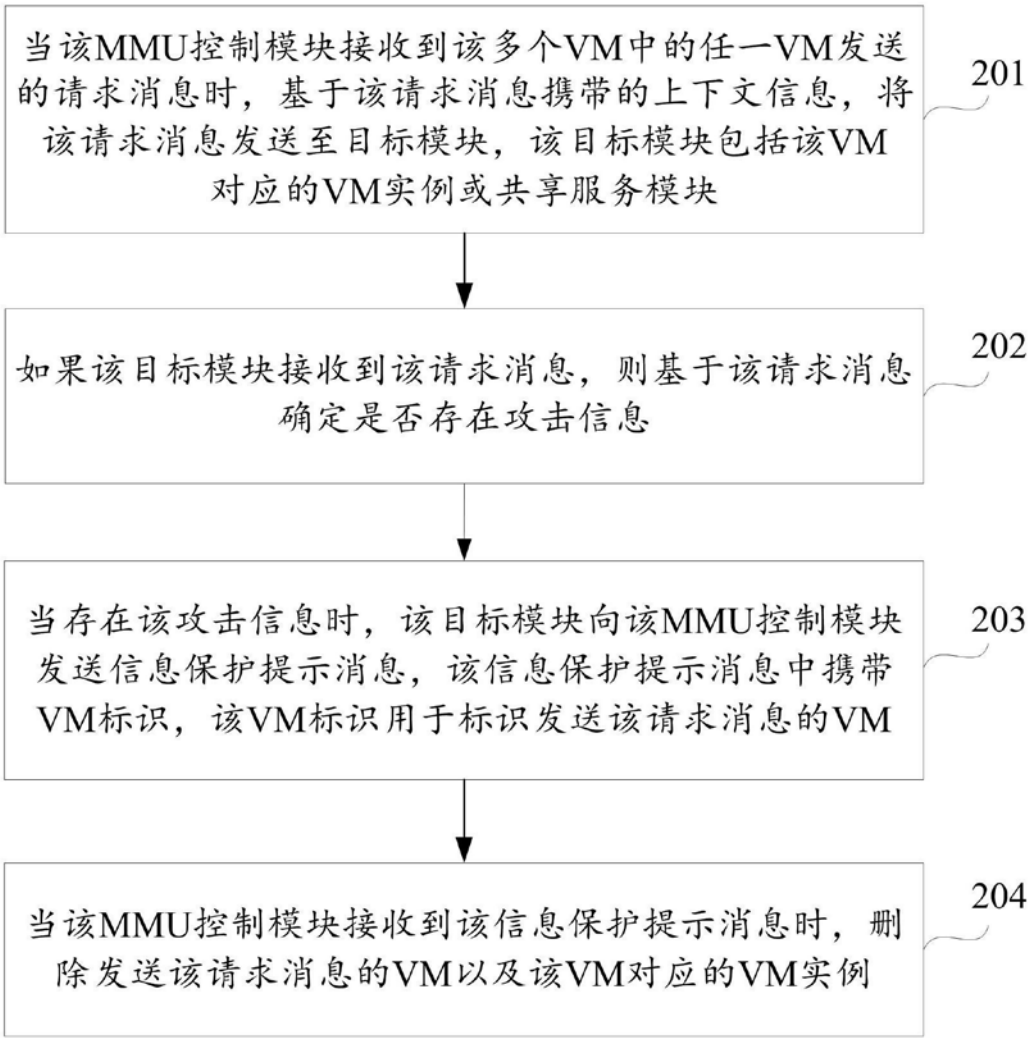

当该MMU控制模块接收到该多个VM中的任一VM发送的请求消息时，基于该请求消息携带的上下文信息，将该请求消息发送至目标模块，该目标模块包括该VM对应的VM实例或共享服务模块
201
如果该目标模块接收到该请求消息，则基于该请求消息确定是否存在攻击信息
202
当存在该攻击信息时，该目标模块向该MMU控制模块发送信息保护提示消息，该信息保护提示消息中携带VM标识，该VM标识用于标识发送该请求消息的VM
203
当该MMU控制模块接收到该信息保护提示消息时，删除发送该请求消息的VM以及该VM对应的VM实例
204

图2

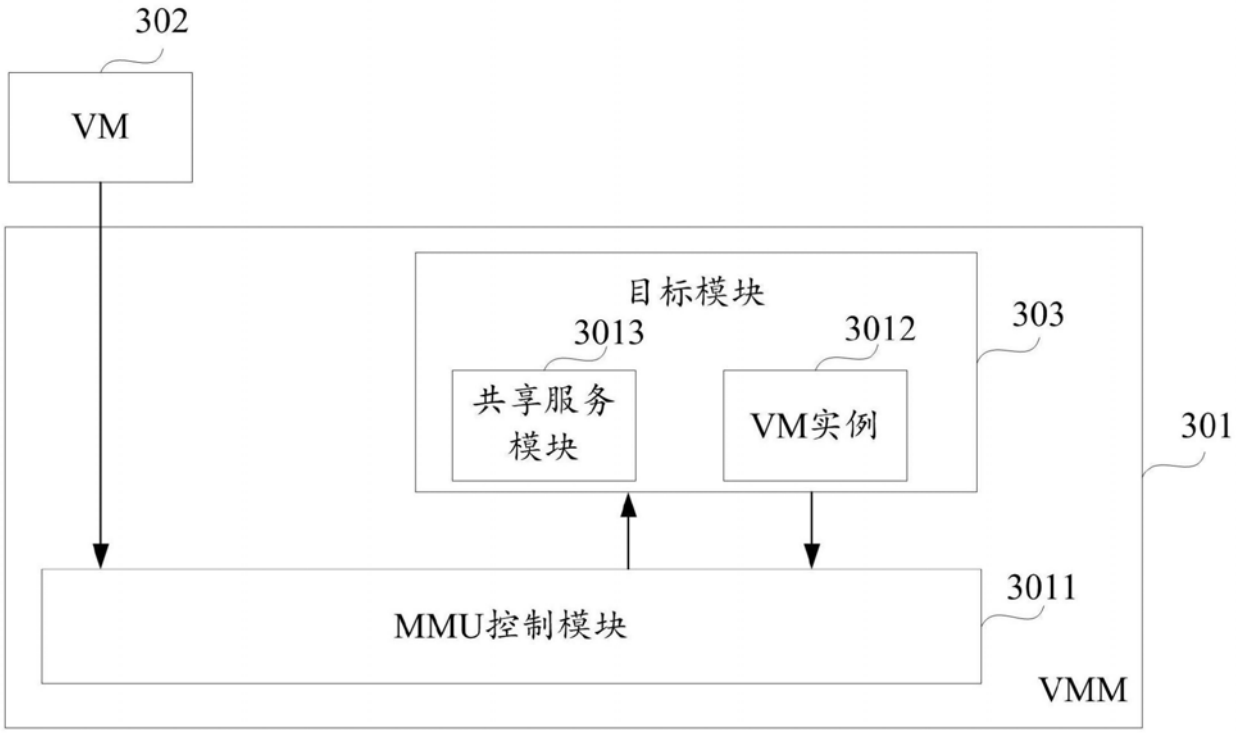

302
VM
目标模块
3013
3012
303
共享服务模块
VM实例
301
3011
MMU控制模块
VMM

图3A

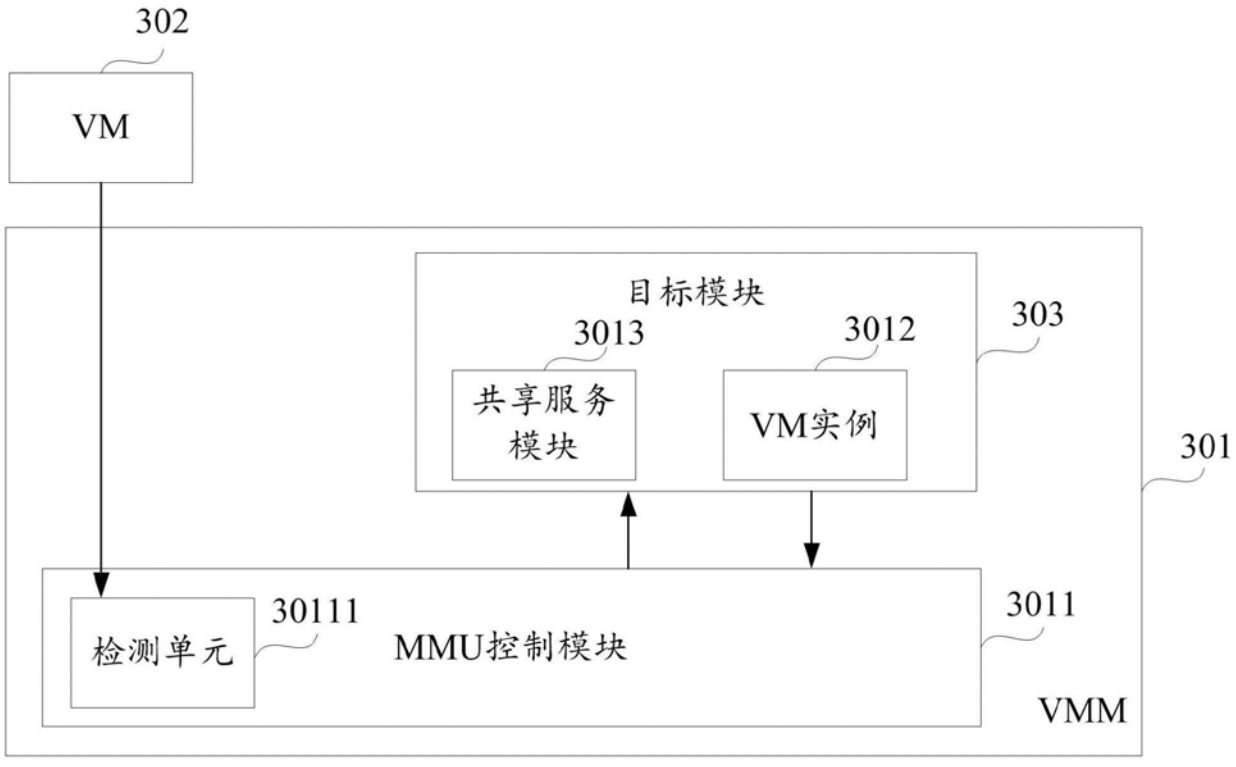

302
VM
目标模块
3013
3012
303
共享服务模块
VM实例
301
检测单元
30111
3011
MMU控制模块
VMM

图3B