(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 120523553 A
(43)申请公布日 2025.08.22

(21)申请号 202510544837.0

(22)申请日 2025.04.28

(71)申请人 南方科技大学
地址 518055 广东省深圳市南山区桃源街道学苑大道1088号

(72)发明人 张锋巍 卢琨

(74)专利代理机构 广州嘉权专利商标事务所有限公司 44205
专利代理师 廖慧贤

(51)Int.Cl.
G06F 9/455(2018.01)
G06F 9/50(2006.01)
G06F 21/57(2013.01)

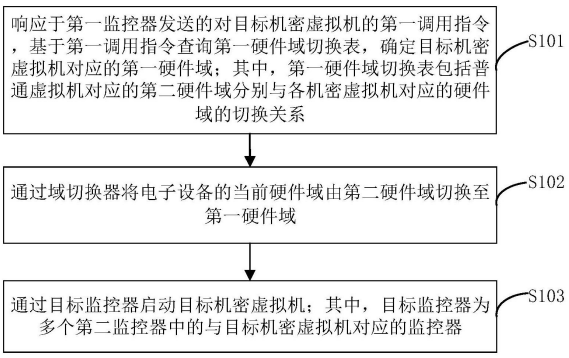
权利要求书2页 说明书12页 附图3页

(54)发明名称

一种机密虚拟机的调用方法及其相关产品

(57)摘要

本申请提供一种机密虚拟机的调用方法及其相关产品,应用于电子设备,电子设备包括普通虚拟机对应的第一监控器,域切换器,以及与多个机密虚拟机一一对应的多个第二监控器;电子设备通过第一监控器与云服务提供商通信;方法包括:响应于第一监控器发送的对目标机密虚拟机的第一调用指令,基于第一调用指令查询第一硬件域切换表,确定目标机密虚拟机对应的第一硬件域;通过域切换器将电子设备的当前硬件域由普通虚拟机对应的第二硬件域切换至第一硬件域;通过多个第二监控器中的目标监控器启动目标机密虚拟机。本申请可使机密虚拟机脱离云服务提供商的控制,可从根本上消除机密虚拟机的攻击原语,能够提高机密虚拟机的防攻击效果。



CN 120523553 A

1.一种机密虚拟机的调用方法,应用于电子设备,所述电子设备包括普通虚拟机对应的第一监控器,域切换器,以及与多个机密虚拟机一一对应的多个第二监控器;所述电子设备通过所述第一监控器与云服务提供商通信;所述调用方法包括:

响应于所述第一监控器发送的对目标机密虚拟机的第一调用指令,基于所述第一调用指令查询第一硬件域切换表,确定所述目标机密虚拟机对应的第一硬件域;其中,所述第一硬件域切换表包括所述普通虚拟机对应的第二硬件域分别与各机密虚拟机对应的硬件域的切换关系;

通过所述域切换器将所述电子设备的当前硬件域由所述第二硬件域切换至所述第一硬件域;

通过目标监控器启动所述目标机密虚拟机;其中,所述目标监控器为所述多个第二监控器中的与所述目标机密虚拟机对应的监控器。

2.如权利要求1所述的调用方法,其特征在于,所述通过所述域切换器将所述电子设备的当前硬件域由所述第二硬件域切换至所述第一硬件域,包括:

向所述域切换器发送第一硬件域切换指令;其中,所述第一硬件域切换指令用于指示将所述当前硬件域由所述第二硬件域切换至所述第一硬件域;

通过所述域切换器对所述第二硬件域的上下文进行存储,以及对所述第一硬件域的上下文进行调用,完成所述第一硬件域切换指令。

3.如权利要求1所述的调用方法,其特征在于,在所述通过目标监控器启动所述目标机密虚拟机之后,所述调用方法还包括:

响应于所述目标监控器发送的对目标设备的数据传输指令,基于所述数据传输指令查询第二硬件域切换表,确定所述目标设备对应的第三硬件域;其中,所述数据传输指令通过所述目标监控器基于所述目标机密虚拟机对所述目标设备的数据传输请求生成;所述第二硬件域切换表包括各机密虚拟机对应的硬件域分别与各设备对应的硬件域之间的切换关系;

通过所述域切换器将所述目标机密虚拟机的当前硬件域由所述第一硬件域切换至所述第三硬件域;

通过所述目标监控器对所述目标设备执行与所述数据传输指令对应的操作,并向所述目标机密虚拟机反馈与所述数据传输指令对应的操作结果。

4.如权利要求1所述的调用方法,其特征在于,在所述通过目标监控器启动所述目标机密虚拟机之后,所述调用方法还包括:

通过所述目标监控器运行于用户态,执行所述目标机密虚拟机对应的操作;其中,所述目标机密虚拟机对应的操作包括异常退出处理、超级调用中的至少一项。

5.如权利要求1所述的调用方法,其特征在于,在所述通过目标监控器启动所述目标机密虚拟机之后,所述调用方法还包括:

响应于所述目标监控器发送的对所述普通虚拟机的第二调用指令,基于所述第二调用指令查询所述第一硬件域切换表,确定所述第二硬件域;

通过所述域切换器将所述电子设备的当前硬件域由所述第一硬件域切换至所述第二硬件域;

通过所述第一监控器启动所述普通虚拟机。

6.如权利要求1所述的调用方法,其特征在于,所述第一调用指令包括所述第一硬件域与所述第二硬件域的切换关系的第一索引信息;

在所述基于所述第一调用指令查询第一硬件域切换表,确定所述目标机密虚拟机对应的第一硬件域之前,所述调用方法还包括:

响应于所述目标机密虚拟机的创建信息,通过所述电子设备的安全监控器生成所述第一硬件域与所述第二硬件域的切换关系,及所述第一索引信息;

通过所述安全监控器将所述第一硬件域与所述第二硬件域的切换关系,以及所述第一索引信息,更新至所述第一硬件域切换表。

7.一种机密虚拟机的调用装置,其特征在于,所述调用装置应用于电子设备,所述电子设备包括普通虚拟机对应的第一监控器,域切换器,以及与多个机密虚拟机一一对应的多个第二监控器;所述电子设备通过所述第一监控器与云服务提供商通信;所述调用装置包括查询模块、切换模块及调用模块;

所述查询模块用于响应于所述第一监控器发送的对目标机密虚拟机的第一调用指令,基于所述第一调用指令查询第一硬件域切换表,确定所述目标机密虚拟机对应的第一硬件域;其中,所述第一硬件域切换表包括所述普通虚拟机对应的第二硬件域分别与各机密虚拟机对应的硬件域的切换关系;

所述切换模块用于通过所述域切换器将所述电子设备的当前硬件域由所述第二硬件域切换至所述第一硬件域;

所述启动模块用于通过目标监控器启动所述目标机密虚拟机;其中,所述目标监控器为所述多个第二监控器中的与所述目标机密虚拟机对应的监控器。

8.一种电子设备,其特征在于,所述电子设备包括存储器和处理器,所述存储器存储有计算机程序,所述处理器执行所述计算机程序时实现如权利要求1至6中任一项所述的调用方法。

9.一种计算机可读存储介质,所述计算机可读存储介质存储有计算机程序,其特征在于,所述计算机程序被处理器执行时实现如权利要求1至6中任一项所述的调用方法。

10.一种计算机程序产品,其特征在于,所述计算机程序产品被存储在存储介质中,所述计算机程序产品被至少一个处理器执行时实现如权利要求1至6中任一项所述的调用方法。

一种机密虚拟机的调用方法及其相关产品

技术领域

[0001] 本申请涉及虚拟机技术领域,具体涉及一种机密虚拟机的调用方法及其相关产品。

背景技术

[0002] 机密虚拟机作为可信执行环境的一种类型,提供了一种隔离框架,使云租户能够在云服务提供商不完全可信的情况下安全地访问其服务。然而,目前机密虚拟机的监控器受云服务提供商的控制,存在引入潜在攻击原语的风险,例如异常注入和地址空间标识符滥用。

[0003] 目前针对机密虚拟机的攻击原语已经十分成熟,攻击者可以利用现成的攻击原语对机密虚拟机发起更加具体的攻击。然而,现有的防御方案大都是针对具体攻击提出具体的防御补丁,未从根本上消除这些攻击原语,导致机密虚拟机的防攻击效果不佳。

发明内容

[0004] 本申请实施例的主要目的在于提出一种机密虚拟机的调用方法及其相关产品,旨在提高机密虚拟机的防攻击效果。

[0005] 本申请实施例提供了一种机密虚拟机的调用方法,应用于电子设备,所述电子设备包括普通虚拟机对应的第一监控器,域切换器,以及与多个机密虚拟机一一对应的多个第二监控器;所述电子设备通过所述第一监控器与云服务提供商通信;所述调用方法包括:响应于所述第一监控器发送的对目标机密虚拟机的第一调用指令,基于所述第一调用指令查询第一硬件域切换表,确定所述目标机密虚拟机对应的第一硬件域;其中,所述第一硬件域切换表包括所述普通虚拟机对应的第二硬件域分别与各机密虚拟机对应的硬件域的切换关系;通过所述域切换器将所述电子设备的当前硬件域由所述第二硬件域切换至所述第一硬件域;通过目标监控器启动所述目标机密虚拟机;其中,所述目标监控器为所述多个第二监控器中的与所述目标机密虚拟机对应的监控器。

[0006] 在一实施方式中,所述通过所述域切换器将所述电子设备的当前硬件域由所述第二硬件域切换至所述第一硬件域,包括:向所述域切换器发送第一硬件域切换指令;其中,所述第一硬件域切换指令用于指示将所述当前硬件域由所述第二硬件域切换至所述第一硬件域;通过所述域切换器对所述第二硬件域的上下文进行存储,以及对所述第一硬件域的上下文进行调用,完成所述第一硬件域切换指令。

[0007] 在一实施方式中,在所述通过目标监控器启动所述目标机密虚拟机之后,所述调用方法还包括:响应于所述目标监控器发送的对目标设备的数据传输指令,基于所述数据传输指令查询第二硬件域切换表,确定所述目标设备对应的第三硬件域;其中,所述数据传输指令通过所述目标监控器基于所述目标机密虚拟机对所述目标设备的数据传输请求生成;所述第二硬件域切换表包括各机密虚拟机对应的硬件域分别与各设备对应的硬件域之间的切换关系;通过所述域切换器将所述目标机密虚拟机的当前硬件域由所述第一硬件域

切换至所述第三硬件域;通过所述目标监控器对所述目标设备执行与所述数据传输指令对应的操作,并向所述目标机密虚拟机反馈与所述数据传输指令对应的操作结果。

[0008] 在一实施方式中,在所述通过目标监控器启动所述目标机密虚拟机之后,所述调用方法还包括:通过所述目标监控器运行于用户态,执行所述目标机密虚拟机对应的操作;其中,所述目标机密虚拟机对应的操作包括异常退出处理、超级调用中的至少一项。

[0009] 在一实施方式中,在所述通过目标监控器启动所述目标机密虚拟机之后,所述调用方法还包括:响应于所述目标监控器发送的对所述普通虚拟机的第二调用指令,基于所述第二调用指令查询所述第一硬件域切换表,确定所述第二硬件域;通过所述域切换器将所述电子设备的当前硬件域由所述第一硬件域切换至所述第二硬件域;通过所述第一监控器启动所述普通虚拟机。

[0010] 在一实施方式中,所述第一调用指令包括所述第一硬件域与所述第二硬件域的切换关系的第一索引信息;在所述基于所述第一调用指令查询第一硬件域切换表,确定所述目标机密虚拟机对应的第一硬件域之前,所述调用方法还包括:响应于所述目标机密虚拟机的创建信息,通过所述电子设备的安全监控器生成所述第一硬件域与所述第二硬件域的切换关系,及所述第一索引信息;通过所述安全监控器将所述第一硬件域与所述第二硬件域的切换关系,以及所述第一索引信息,更新至所述第一硬件域切换表。

[0011] 本申请实施例还提供了一种机密虚拟机的调用装置,所述调用装置应用于电子设备,所述电子设备包括普通虚拟机对应的第一监控器,域切换器,以及与多个机密虚拟机一一对应的多个第二监控器;所述电子设备通过所述第一监控器与云服务提供商通信;所述调用装置包括查询模块、切换模块及调用模块;所述查询模块用于响应于所述第一监控器发送的对目标机密虚拟机的第一调用指令,基于所述第一调用指令查询第一硬件域切换表,确定所述目标机密虚拟机对应的第一硬件域;其中,所述第一硬件域切换表包括所述普通虚拟机对应的第二硬件域分别与各机密虚拟机对应的硬件域的切换关系;所述切换模块用于通过所述域切换器将所述电子设备的当前硬件域由所述第二硬件域切换至所述第一硬件域;所述启动模块用于通过目标监控器启动所述目标机密虚拟机;其中,所述目标监控器为所述多个第二监控器中的与所述目标机密虚拟机对应的监控器。

[0012] 本申请实施例还提供了一种电子设备,所述电子设备包括存储器和处理器,所述存储器存储有计算机程序,所述处理器执行所述计算机程序时实现上述机密虚拟机的调用方法。

[0013] 本申请实施例还提供了一种计算机可读存储介质,所述计算机可读存储介质存储有计算机程序,所述计算机程序被处理器执行时实现上述机密虚拟机的调用方法。

[0014] 本申请还提供了一种计算机程序产品,所述计算机程序产品被存储在存储介质中,所述计算机程序产品被至少一个处理器执行时实现上述机密虚拟机的调用方法。

[0015] 本申请提供的一种机密虚拟机的调用方法及其相关产品,在电子设备通过普通虚拟机对应的第一监控器与云服务提供商通信的基础上,通过响应于第一监控器发送的对目标机密虚拟机的第一调用指令,基于第一调用指令查询第一硬件域切换表,确定目标机密虚拟机对应的第一硬件域,并通过域切换器将电子设备的当前硬件域由普通虚拟机对应的第二硬件域切换至第一硬件域,以及通过目标监控器启动目标机密虚拟机,使机密虚拟机脱离云服务提供商的控制,可从根本上消除机密虚拟机的攻击原语,能够提高机密虚拟机

的防攻击效果。

附图说明

[0016] 图1是本申请实施例提供的机密虚拟机的调用方法的流程示意图;

[0017] 图2是本申请实施例提供的机密虚拟机的调用方法的另一流程示意图;

[0018] 图3是本申请实施例提供的机密虚拟机的调用方法的另一流程示意图;

[0019] 图4是本申请实施例提供的电子设备的软件架构示意图;

[0020] 图5是本申请实施例提供的电子设备的硬件架构示意图;

[0021] 图6是本申请实施例提供的机密虚拟机的调用装置的结构示意图;

[0022] 图7是本申请实施例提供的电子设备的结构示意图。

具体实施方式

[0023] 下面将结合本申请实施例中的附图,对本申请实施例中的技术方案进行清楚地描述,显然,所描述的实施例是本申请一部分实施例,而不是全部的实施例。基于本申请中的实施例,本领域普通技术人员获得的所有其他实施例,都属于本申请保护的范围。

[0024] 本申请的说明书和权利要求书中的术语“第一”、“第二”等是用于区别类似的对象,而不用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换,以便本申请的实施例能够以除了在这里图示或描述的那些以外的顺序实施,且“第一”、“第二”等所区分的对象通常为一类,并不限定对象的个数,例如第一对象可以是一个,也可以是多个。此外,说明书以及权利要求中“和/或”表示所连接对象的至少其中之一,字符“/”,一般表示前后关联对象是一种“或”的关系。

[0025] 本申请实施例提供的机密虚拟机的调用方法可应用于电子设备。其中,电子设备可以是终端或服务器。在一些实施例中,终端可以是智能手机、平板电脑、笔记本电脑、台式计算机等;服务器可以配置成独立的物理服务器,也可以配置成多个物理服务器构成的服务器集群或者分布式系统,还可以配置成提供云服务、云数据库、云计算、云函数、云存储、网络服务、云通信、中间件服务、域名服务、安全服务、CDN以及大数据和人工智能平台等基础云计算服务的云服务器。进一步,本申请实施例提供的机密虚拟机的调用方法可以应用于电子设备的软件中,软件可以是实现机密虚拟机的调用方法的应用等,但并不局限于以上形式。

[0026] 下面结合附图,通过具体的实施例对本申请实施例提供的机密虚拟机的调用方法进行详细地说明。

[0027] 本申请实施例提供的一种机密虚拟机的调用方法,应用于电子设备,电子设备包括普通虚拟机对应的第一监控器,域切换器,以及与多个机密虚拟机一一对应的多个第二监控器;电子设备通过第一监控器与云服务提供商通信。请参见图1,本申请实施例提供的机密虚拟机的调用方法可以包括:

[0028] 步骤S101:响应于第一监控器发送的对目标机密虚拟机的第一调用指令,基于第一调用指令查询第一硬件域切换表,确定目标机密虚拟机对应的第一硬件域;其中,第一硬件域切换表包括普通虚拟机对应的第二硬件域分别与各机密虚拟机对应的硬件域的切换关系;

[0029] 可选地,第一调用指令可以为第一监控器运行过程中,根据自身对目标机密虚拟机的调用需求生成的调用指令;也可以为基于用户通过普通虚拟机输入的调用目标机密虚拟机的请求生成的调用指令。

[0030] 可选地,第一调用指令可以包括普通虚拟机与目标机密虚拟机的身份信息。实际实现时,在接收到第一监控器发送的对目标机密虚拟机的第一调用指令的情况下,可以基于普通虚拟机与目标机密虚拟机的身份信息,查询第一硬件域切换表,得到与普通虚拟机和目标机密虚拟机的身份信息匹配的第一切换关系,并将第一切换关系中的机密虚拟机对应的硬件域确定为第一硬件域。

[0031] 可选地,第一调用指令还可以包括目标机密虚拟机对应的第一硬件域与普通虚拟机对应的第二硬件域的切换关系的第一索引信息;第一索引信息可以为一个数字或一个符号,在第一索引信息为一个数字的情况下,第一索引信息可以为用于标识第一硬件域与第二硬件域的切换关系的身份识别(Identification,ID)号。实际实现时,在接收到第一监控器发送的对目标机密虚拟机的第一调用指令的情况下,可以基于第一调用指令中的第一索引信息查询第一硬件域切换表,得到与第一索引信息匹配的第一表项,进一步可以将第一表项中的除普通虚拟机对应的第二硬件域之外的硬件域,确定为目标机密虚拟机对应的第一硬件域。

[0032] 步骤S102:通过域切换器将电子设备的当前硬件域由第二硬件域切换至第一硬件域;

[0033] 本申请实施例提供的机密虚拟机的调用方法可以支持两种管理模式:第一监控器对普通虚拟机进行管理的普通模式,以及第二监控器对机密虚拟机进行管理的机密模式;域切换器可以作为普通模式与机密模式的中转站,可以理解为普通模式与机密模式的接口,通过域切换器进行硬件域的切换,实现普通模式与机密模式的转换。

[0034] 实际实现时,可以通过域切换器直接将电子设备的当前硬件域由第二硬件域切换至第一硬件域,实现普通模式到机密模式的切换;也可以通过域切换器进行第一硬件域与第二硬件域的上下文切换,将电子设备的当前硬件域由第二硬件域切换至第一硬件域,实现普通模式到机密模式的切换,具体实现可参见下述相关描述,此处不作描述。本申请实施例不对通过域切换器将电子设备的当前硬件域由第二硬件域切换至第一硬件域的具体实现方式进行限定。

[0035] 步骤S103:通过目标监控器启动目标机密虚拟机;其中,目标监控器为多个第二监控器中的与目标机密虚拟机对应的监控器。

[0036] 实际实现时,在将电子设备的当前硬件域切换至第一硬件域的情况下,目标监控器可以基于第一硬件域,自动执行启动目标机密虚拟机的操作。

[0037] 本申请实施例在电子设备通过第一监控器与云服务提供商通信的基础上,通过响应于第一监控器发送的对目标机密虚拟机的第一调用指令,基于第一调用指令查询第一硬件域切换表,确定目标机密虚拟机对应的第一硬件域,并通过域切换器将电子设备的当前硬件域由普通虚拟机对应的第二硬件域切换至第一硬件域,以及通过目标监控器启动目标机密虚拟机,使机密虚拟机脱离云服务提供商的控制,可从根本上消除机密虚拟机的攻击原语,能够提高机密虚拟机的防攻击效果。

[0038] 在一实施方式中,上述步骤S102:通过域切换器将电子设备的当前硬件域由第二

硬件域切换至第一硬件域,包括:

[0039] 向域切换器发送第一硬件域切换指令;其中,第一硬件域切换指令用于指示将当前硬件域由第二硬件域切换至第一硬件域;

[0040] 通过域切换器对第二硬件域的上下文进行存储,以及对第一硬件域的上下文进行调用,完成第一硬件域切换指令。

[0041] 实际实现时,可以向域切换器发送将当前硬件域由第二硬件域切换至第一硬件域的硬件域切换指令,域切换器在接收到该硬件域切换指令的情况下,可以通过对第二硬件域的上下文进行存储,并对第一硬件域的上下文进行调用,来完成第一硬件域的切换指令。

[0042] 本申请实施例通过向域切换器发送第一硬件域切换指令,以及通过域切换器对第二硬件域的上下文进行存储,以及对第一硬件域的上下文进行调用,完成第一硬件域切换指令,使得硬件域切换无需经过最高权限的安全监控器,能够在保证硬件域切换的安全性的基础上,提高硬件域切换的效率,降低了实现硬件域切换功能的设计复杂性。

[0043] 在一实施方式中,在上述步骤S101中的基于第一调用指令查询第一硬件域切换表,确定目标机密虚拟机对应的第一硬件域之前,本申请实施例提供的机密虚拟机的调用方法还包括:

[0044] 响应于目标机密虚拟机的创建信息,通过电子设备的安全监控器生成第一硬件域与第二硬件域的切换关系,及第一索引信息;

[0045] 通过安全监控器将第一硬件域与第二硬件域的切换关系,以及第一索引信息,更新至第一硬件域切换表。

[0046] 实际实现时,在目标机密虚拟机创建完成的情况下,可以将目标机密虚拟机对应的第一硬件域发送至安全监控器,安全监控器可以基于第一硬件域及预先存储的普通虚拟机对应的第二硬件域,生成第一硬件域与第二硬件域的切换关系,以及用于标识该切换关系的第一索引信息。进一步,安全监控器可以将该切换关系及第一索引信息更新至第一硬件域切换表中,以便普通虚拟机对应的第一监控器,或目标机密虚拟机对应的目标监控器基于更新后的第一硬件域切换表中的切换关系与第一索引信息,进行第一硬件域与第二硬件域的切换。

[0047] 本申请实施例通过响应于目标机密虚拟机的创建信息,通过电子设备的安全监控器生成第一硬件域与第二硬件域的切换关系,及第一索引信息,以及通过安全监控器将第一硬件域与第二硬件域的切换关系,以及第一索引信息,更新至第一硬件域切换表,能够提高利用第一硬件域切换表进行第一硬件域与第二硬件域切换的效率与准确性。

[0048] 请参见图2,在上述步骤S103中的通过目标监控器启动目标机密虚拟机之后,本申请实施例提供的机密虚拟机的调用方法还可以包括:

[0049] 步骤S201:响应于目标监控器发送的对目标设备的数据传输指令,基于数据传输指令查询第二硬件域切换表,确定目标设备对应的第三硬件域;其中,数据传输指令通过目标监控器基于目标机密虚拟机对目标设备的数据传输请求生成;第二硬件域切换表包括各机密虚拟机对应的硬件域分别与各设备对应的硬件域之间的切换关系;

[0050] 步骤S202:通过域切换器将目标机密虚拟机的当前硬件域由第一硬件域切换至第三硬件域;

[0051] 步骤S203:通过目标监控器对目标设备执行与数据传输指令对应的操作,并向目

标机密虚拟机反馈与数据传输指令对应的操作结果。

[0052] 实际实现时,在目标机密虚拟机的运行过程中,可以根据自身需要向目标监控器发送对目标设备的数据传输请求,目标监控器可以响应于目标机密虚拟机对目标设备的数据传输请求,生成目标设备的数据传输指令。可选地,数据传输需求可以为数据读取需求和数据写入需求中的任一项;相应地,数据传输指令可以为数据读取指令和数据写入指令中的任一项。

[0053] 可选地,针对每个机密虚拟机,上述第二硬件域切换表包括机密虚拟机对应的硬件域分别与各设备对应的硬件域之间的切换关系。

[0054] 可选地,数据传输指令可以包括目标机密虚拟机与目标设备的身份信息。实际实现时,在接收到目标监控器发送的对目标设备的数据传输指令的情况下,可以基于目标机密虚拟机与目标设备的身份信息,查询第二硬件域切换表,得到与目标机密虚拟机与目标设备的身份信息匹配的第二切换关系,并将第二切换关系中的设备对应的硬件域确定为目标设备对应的第三硬件域。

[0055] 可选地,数据传输指令还可以包括目标机密虚拟机对应的第一硬件域与目标设备对应的第三硬件域的切换关系的第二索引信息;第二索引信息可以为一个数字或一个符号,在第二索引信息为一个数字的情况下,第二索引信息可以为用于标识第一硬件域与第三硬件域的切换关系的身份识别(Identification,ID)号。实际实现时,在接收到目标监控器发送的对目标设备的数据传输指令的情况下,可以基于数据传输指令中的第二索引信息查询第二硬件域切换表,得到与第二索引信息匹配的第二表项,进一步可以将第二表项中的除目标机密虚拟机对应的第一硬件域之外的硬件域,确定为目标设备对应的第三硬件域。

[0056] 域切换器还可以作为目标机密虚拟机与目标设备的中转站,可以理解为目标机密虚拟机与目标设备的数据传输接口,通过域切换器进行硬件域的切换,才能实现目标机密虚拟机与目标设备的数据传输。

[0057] 实际实现时,可以通过域切换器将目标机密虚拟机的当前硬件域由第一硬件域切换至第三硬件域,以及通过目标监控器对目标设备执行与数据传输指令对应的操作,实现目标机密虚拟机与目标设备的数据传输;也可以通过域切换器对目标机密虚拟机对应的第一硬件域的上下文进行存储,以及对目标设备对应的第三硬件域的上下文进行调用,将目标机密虚拟机的当前硬件域由第一硬件域切换至第三硬件域,以及通过目标监控器对目标设备执行与数据传输指令对应的操作,实现目标机密虚拟机与目标设备的数据传输。本申请实施例不对通过域切换器将目标机密虚拟机的当前硬件域由第一硬件域切换至第三硬件域的具体实现方式进行限定。

[0058] 进一步,在目标机密虚拟机对应的硬件域切换至目标设备对应的第三硬件域的情况下,目标监控器可以对目标设备执行与数据传输指令对应的操作,生成与数据传输指令对应的操作结果,并将与数据传输指令对应的操作结果,向目标机密虚拟机进行反馈。可选地,与数据传输指令对应的操作可以为数据读取操作及数据写入操作中的任一项。

[0059] 本申请实施例通过响应于目标监控器发送的对目标设备的数据传输指令,基于数据传输指令查询第二硬件域切换表,确定目标设备对应的第三硬件域,并通过域切换器将目标机密虚拟机的当前硬件域由第一硬件域切换至第三硬件域,以及通过目标监控器对目

标设备执行与数据传输指令对应的操作,并向目标机密虚拟机反馈与数据传输指令对应的操作结果,能够提高机密虚拟机与设备进行数据传输的效率与安全性;另外,在多个机密虚拟机与多个第二监控器一一对应的基础上,每个机密虚拟机通过不同的第二监控器进行管理,可以避免在多个机密虚拟机与同一设备进行数据传输过程中,因某个机密虚拟机崩溃,影响其他机密虚拟机与该设备的数据传输的问题。

[0060] 在一实施方式中,在上述基于数据传输指令查询第二硬件域切换表,确定目标设备对应的第三硬件域之前,本申请实施例提供的机密虚拟机的调用方法还包括:

[0061] 响应于目标机密虚拟机的创建信息,通过电子设备的安全监控器生成第一硬件域分别与各设备对应的硬件域的切换关系,及第一硬件域分别与各设备对应的硬件域的切换关系的索引信息;

[0062] 通过安全监控器将第一硬件域分别与各设备对应的硬件域的切换关系,以及第一硬件域分别与各设备对应的硬件域的切换关系的索引信息,更新至第二硬件域切换表。

[0063] 实际实现时,在目标机密虚拟机创建完成的情况下,可以将目标机密虚拟机对应的第一硬件域发送至安全监控器,安全监控器可以基于第一硬件域及预先存储的各设备对应的硬件域,生成第一硬件域分别与各设备对应的硬件域的切换关系,以及分别用于标识第一硬件域与各设备对应的硬件域的切换关系的索引信息。进一步,安全监控器可以将第一硬件域分别与各设备对应的硬件域的切换关系及其索引信息,更新至第二硬件域切换表中,以便目标机密虚拟机对应的目标监控器基于更新后的第二硬件域切换表中的切换关系及其索引信息,进行第一硬件域与各设备对应的硬件域的切换。

[0064] 本申请实施例通过响应于目标机密虚拟机的创建信息,通过电子设备的安全监控器生成第一硬件域与各设备对应的硬件域的切换关系及其索引信息,以及通过安全监控器将第一硬件域与各设备对应的硬件域的切换关系及其索引信息,更新至第二硬件域切换表,能够提高利用第二硬件域切换表进行目标机密虚拟机对应的第一硬件域与各设备对应的硬件域的切换效率与切换准确性。

[0065] 在一实施方式中,在上述步骤S103中的通过目标监控器启动目标机密虚拟机之后,本申请实施例提供的机密虚拟机的调用方法还包括:

[0066] 通过目标监控器运行于用户态,执行目标机密虚拟机对应的操作;其中,目标机密虚拟机对应的操作包括异常退出处理、超级调用中的至少一项。

[0067] 实际实现时,为了防止目标监控器陷入到内核态,目标监控器可以使用用户态虚拟化委托的硬件拓展,将机密虚拟机对应的操作置于用户态,从而可以将目标监控器的能力控制在用户态的权限中。

[0068] 本申请实施例在通过目标监控器启动目标机密虚拟机之后,通过目标监控器运行于用户态,执行目标机密虚拟机对应的异常退出处理、超级调用等操作,可将目标监控器的能力控制在用户态的权限中,从而能够提升目标监控器对目标机密虚拟机进行管理的安全性与灵活性。

[0069] 请参见图3,在上述步骤S103中的通过目标监控器启动目标机密虚拟机之后,本申请实施例提供的机密虚拟机的调用方法还可以包括:

[0070] 步骤S301:响应于目标监控器发送的对普通虚拟机的第二调用指令,基于第二调用指令查询第一硬件域切换表,确定第二硬件域;

[0071] 步骤S302:通过域切换器将电子设备的当前硬件域由第一硬件域切换至第二硬件域;

[0072] 步骤S303:通过第一监控器启动普通虚拟机。

[0073] 可选地,第二调用指令可以为目标监控器运行过程中,根据自身对普通虚拟机的调用需求生成的调用指令;也可以为基于用户通过目标机密虚拟机输入的调用普通虚拟机的请求生成的调用指令。

[0074] 可选地,第二调用指令可以包括普通虚拟机与目标机密虚拟机的身份信息。实际实现时,在接收到目标监控器发送的对普通虚拟机的第二调用指令的情况下,可以基于普通虚拟机与目标机密虚拟机的身份信息,查询第一硬件域切换表,得到与普通虚拟机和目标机密虚拟机的身份信息匹配的第一切换关系,并将第一切换关系中的普通虚拟机对应的硬件域确定为第二硬件域。

[0075] 可选地,第二调用指令还可以包括目标机密虚拟机对应的第一硬件域与普通虚拟机对应的第二硬件域的切换关系的第一索引信息。实际实现时,在接收到目标监控器发送的对普通虚拟机的第二调用指令的情况下,可以基于第二调用指令中的第一索引信息查询第一硬件域切换表,得到与第一索引信息匹配的第一表项,进一步可以将第一表项中的除目标机密虚拟机对应的第一硬件域之外的硬件域,确定为普通虚拟机对应的第二硬件域。

[0076] 实际实现时,可以通过域切换器直接将电子设备的当前硬件域由第一硬件域切换至第二硬件域,实现机密模式到普通模式的切换;也可以通过域切换器对第一硬件域的上下文进行存储,并对第二硬件域的上下文进行调用,将电子设备的当前硬件域由第二硬件域切换至第一硬件域,实现机密模式到普通模式的切换。本申请实施例不对通过域切换器将电子设备的当前硬件域由第二硬件域切换至第一硬件域的具体实现方式进行限定。

[0077] 实际实现时,在将电子设备的当前硬件域切换至第二硬件域的情况下,第一监控器可以基于第二硬件域,自动执行启动普通虚拟机的操作。

[0078] 本申请实施例通过响应于目标监控器发送的对普通虚拟机的第二调用指令,基于第二调用指令查询第一硬件域切换表,确定第二硬件域,并通过域切换器将电子设备的当前硬件域由第一硬件域切换至第二硬件域,以及通过第一监控器启动普通虚拟机,能够提高运行于机密模式下的目标监控器对运行于普通模式下的普通虚拟机的调用效率与调用安全性。

[0079] 请参见图4,在一具体实施例中,本申请实施例提供的电子设备的软件架构可以包括:普通虚拟机、管理普通虚拟机的Hypervisor(相当于普通虚拟机对应的第一监控器,其与云服务提供商通信,是不可信的)、安全跳板(相当于域切换器)、机密虚拟机、管理机密虚拟机的Per-VM Monitor(相当于机密虚拟机对应的第二监控器)及设备Enclave。在一些实施例中,该软件架构可以称为UNIVISOR框架。

[0080] 可选地,普通虚拟机及不可信的Hypervisor运行时隶属于普通模式;安全跳板、机密虚拟机、Per-VM Monitor及设备Enclave运行时隶属于机密模式。在普通模式中,Hypervisor可以管理vCPU调度和内存分配等任务。当创建一个机密虚拟机时,Hypervisor会分配对应的资源并请求安全监视器进行安全检查;在机密模式中,其特权模式还是与普通模式的保持一致,但每个机密虚拟机由一个单独的Per-VM Monitor进行管理,Per-VM Monitor会管理机密虚拟机的大部分请求。

[0081] 其中,Per-VM Monitor:该软件模块可以将虚拟化相关的模拟操作从Hypervisor中解耦出来。在UNIVISOR框架中,每个机密虚拟机都会有一个单独的Per-VM Monitor处理对应的VMEXIT和Hypercall请求,这样诸如二阶段页表异常、Virt I/O和中断等处理就不用陷入到Hypervisor中,而是在Per-VM Monitor中进行处理。为了防止陷入到内核态,Per-VM Monitor使用用户态虚拟化委托的硬件拓展,将机密虚拟机VMEXIT和Hypercall处理置于用户态,从而将Per-VM Monitor的能力控制在一个用户态的权限中。

[0082] 安全跳板:该软件模块可以将硬件域切换的功能从电子设备的安全监视器中解耦出来,简化普通模式和机密模式之间的接口。在UNIVISOR框架中,安全跳板可以作为普通模式和机密模式的中转站。当普通模式使用第一硬件域切换表提供的机密指令进行世界切换时,可以先进入到安全跳板模块中,进行上下文切换,并根据第一硬件域切换表中的信息进行硬件资源访问权限的切换。在完成这些操作后,才会进入到机密虚拟机内部。安全跳板模块通过硬件域切换表,绕过了最高权限的安全监管者,简化了实现机密模式和普通模式切换的软件设计。

[0083] 设备Enclave:该软件模块可以将数据输入/输出(I/O)功能从Hypervisor中解耦出来。在UNIVISOR框架中,设备Enclave可以是一系列I/O Enclave的总称。每一类的I/O设备请求会将对应的设备驱动放置到一个独立的I/O Enclave中。每当机密虚拟机想进行I/O操作的情况下,可以先通过安全跳板将机密虚拟机对应的硬件域切换至I/O Enclave对应的硬件域,再通过Per-VM Monitor对Enclave进行具体的I/O操作,最后将I/O操作结果通过Per-VM Monitor反馈给机密虚拟机。

[0084] 本申请实施例通过上述UNIVISOR框架,可以将针对机密虚拟机的攻击原语从Hypervisor中解耦开来,使得Hypervisor无法直接在VMEXIT、Hypercall发生时,对机密虚拟机发起攻击,并简化了Hypervisor和机密虚拟机相互切换的接口设计,可以增加切换安全性和性能,另外,使得Hypervisor无法直接通过中断,攻击机密虚拟机。

[0085] 为了提供上述UNIVISOR框架中隔离Hypervisor的独特硬件原语,本申请实施例对传统虚拟化硬件的功能进行了拓展,可以在保证安全性的同时保证较小的功能拓展开销。

[0086] 请参见图5,在另一具体实施例中,本申请实施例提供的电子设备的硬件架构包括:访问控制单元、主处理器、权限检查器、页表遍历器及机密中断控制器;其中,主处理器包括新模式的控制状态(Control Status Register,CSR)寄存器,页表遍历器具有权限检查功能。

[0087] 可选地,本申请实施例在传统虚拟化硬件的功能的基础上进行了如下拓展:

[0088] 1)CSR寄存器可以用来支持机密模式;可选地,在原有虚拟化相关的CSR基础上,对CSR寄存器的功能进行了如下拓展:第一,UNIVISOR拓展额外的机密模式,并且提供对于机密模式内部的资源访问限制;可选地,可以通过提供不同的机密虚拟机号,并且将机密虚拟机号和Cache、TLB等资源相绑定,最后提供硬件域切换表相关安全性检查实现。第二,UNIVISOR实现虚拟化用户态委托,将所有的虚拟化相关功能限制在用户态,限制特权管理只能由安全跳板实现。

[0089] 2)设计硬件域切换表实现安全地址空间切换。为了实现不同软件组件的隔离,本申请实施例通过硬件域切换表实现地址空间切换过程中的安全检查和控制流的安全写换。可选地,硬件域切换表会在处理器内部中实现一个存储模块,记录不同硬件域之间的切换

规则,包括目标地址空间、目标ID、目标地址等。一旦硬件指令触发,就会自动进行硬件上的权限检查,可以先跳转到安全跳板,再由安全跳板使能在硬件域切换表中的配置,进入到机密虚拟机所在的硬件域中。

[0090] 3)设计机密中断控制器实现安全中断。因为普通时间的中断控制器在Hypervisor的控制下,很难不使用Hypervisor的中断管理并且同时保证中断安全。为此,本申请实施例设计了机密模式下的独立中断控制器,该中断控制器为不同机密虚拟机提供了独立中断上下文,每个机密虚拟机对应的Per-VM Monitor都可以独立配置自己中断信息。这样配置后,不同硬件域之间的中断就可以互不影响,从而Hypervisor就无法影响机密虚拟机的中断功能。

[0091] 本申请实施例设计了一种最小特权系统的UNIVISOR框架,UNIVISOR提供了基础的攻击原语消除方案,可以防止攻击者继续利用基本攻击原语提出新的具体攻击;UNIVISOR还通过软硬件结合的方式实现了对于性能的优化,可以在极低的开销下保证安全性,并且硬件的修改不引入额外的兼容性问题。具体地,通过解耦可信计算基软件,构建基于每个机密虚拟机的管理程序切片,可以剥离虚拟机监控者程序的攻击原理;通过引入机密模式,将管理程序功能从不可信的虚拟机监管者管理程序中解耦,并将其委托给可信的用户态管理监控器,可以保护隔离机密虚拟机内部的敏感数据和代码,能够避免机密虚拟机依赖不可信的Hypervisor去管理TLB、Cache和中断等,一旦Hypervisor被攻陷,攻击者就可以将这些资源管理的权利转化为发起攻击的能力,来获取机密虚拟机内部的机密信息或者破坏其完整性的问题;另外,通过引入硬件域切换表,可以解决引入用户态管理者监控器世界切换开销过大的问题,并且将机密域切换功能从安全监视器中解耦,能够避免机密虚拟化和传统硬件虚拟化不兼容的问题:因机密虚拟化出现的时间比硬件虚拟化晚,并且试图将一些安全功能从Hypervisor中解耦出来,给Hypervisor和机密虚拟机的通信增加了复杂性,这种复杂性也引入了一定安全问题,同时也有一些功能很难从Hypervisor中解耦出来;此外,设计了一种新的中断控制器,将中断路由控制从不可信的管理程序中解耦,并允许用户态管理监控器管理中断,剥离了虚拟机监控者程序的中断注入原语,能够避免因没有可信的安全中断控制器及可信的I/O设备,很难在系统正常运行时,同时保证中断安全和I/O高效的问题。

[0092] 本申请实施例还提供一种机密虚拟机的调用装置600,调用装置600应用于电子设备,电子设备包括普通虚拟机对应的第一监控器,域切换器,以及与多个机密虚拟机一一对应的多个第二监控器;电子设备通过所述第一监控器与云服务提供商通信。请参见图6,本申请实施例提供的调用装置600可以包括查询模块601、切换模块602及调用模块603。

[0093] 其中,查询模块601用于响应于第一监控器发送的对目标机密虚拟机的第一调用指令,基于第一调用指令查询第一硬件域切换表,确定目标机密虚拟机对应的第一硬件域;其中,第一硬件域切换表包括普通虚拟机对应的第二硬件域分别与各机密虚拟机对应的硬件域的切换关系;

[0094] 切换模块602用于通过域切换器将电子设备的当前硬件域由第二硬件域切换至第一硬件域;

[0095] 启动模块603用于通过目标监控器启动目标机密虚拟机;其中,目标监控器为多个第二监控器中的与目标机密虚拟机对应的监控器。

[0096] 本申请实施例提供的机密虚拟机的调用装置能够实现上述机密虚拟机的调用方法实施例的各个步骤,且能达到相同的技术效果,为避免重复,这里不再赘述。

[0097] 本申请实施例还提供一种电子设备,包括处理器和存储器,存储器上存储有可在处理器上运行的程序或指令,该程序或指令被处理器执行时实现上述机密虚拟机的调用方法实施例的各个步骤,且能达到相同的技术效果,为避免重复,这里不再赘述。

[0098] 图7为实现本申请实施例的电子设备的硬件结构示意图,该电子设备包括:

[0099] 处理器701,可以采用通用的中央处理器(Central Processing Unit,CPU)、微处理器、应用专用集成电路(Application Specific Integrated Circuit,ASIC)、或者一个或多个集成电路等方式实现,用于执行相关程序,以实现本申请实施例所提供的技术方案;

[0100] 存储器702,可以采用只读存储器(Read Only Memory,ROM)、静态存储设备、动态存储设备或者随机存取存储器(Random Access Memory,RAM)等形式实现。存储器702可以存储操作系统和其他应用程序,在通过软件或者固件来实现本说明书实施例所提供的技术方案时,相关的程序代码保存在存储器702中,并由处理器701来调用执行本申请实施例的机密虚拟机的调用方法;

[0101] 输入/输出接口703,用于实现信息输入及输出;

[0102] 通信接口704,用于实现本设备与其他设备的通信交互,可以通过有线方式(例如USB、网线等)实现通信,也可以通过无线方式(例如移动网络、WIFI、蓝牙等)实现通信;

[0103] 总线705,在设备的各个组件(例如处理器701、存储器702、输入/输出接口703和通信接口704)之间传输信息;

[0104] 其中处理器701、存储器702、输入/输出接口703和通信接口704通过总线705实现彼此之间在设备内部的通信连接。

[0105] 本申请实施例提供的电子设备能够实现上述机密虚拟机的调用方法实施例的各个步骤,且能达到相同的技术效果,为避免重复,这里不再赘述。

[0106] 本申请实施例还提供一种计算机可读存储介质,计算机可读存储介质上存储有程序或指令,该程序或指令被处理器执行时实现上述机密虚拟机的调用方法实施例的各个步骤,且能达到相同的技术效果,为避免重复,这里不再赘述。

[0107] 其中,处理器为上述实施例中所述的电子设备中的处理器。计算机可读存储介质,包括计算机可读存储介质,如计算机只读存储器ROM、随机存取存储器RAM、磁碟或者光盘等。

[0108] 本申请实施例另提供了一种芯片,芯片包括处理器和通信接口,通信接口和处理器耦合,处理器用于运行程序或指令,实现上述机密虚拟机的调用方法实施例的各个步骤,且能达到相同的技术效果,为避免重复,这里不再赘述。

[0109] 应理解,本申请实施例提到的芯片还可以称为系统级芯片、系统芯片、芯片系统或片上系统芯片等。

[0110] 本申请实施例提供一种计算机程序产品,该程序产品被存储在存储介质中,该程序产品被至少一个处理器执行以实现如上述机密虚拟机的调用方法实施例的各个步骤,且能达到相同的技术效果,为避免重复,这里不再赘述。

[0111] 需要说明的是,在本文中,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、物品或者装置不仅包括那些要素,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、物品或者装置所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不删除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。此外,需要指出的是,本申请实施方式中的方法和装置的范围不限按示出或讨论的顺序来执行功能,还可包括根据所涉及的功能按基本同时的方式或按相反的顺序来执行功能,例如,可以按不同于所描述的次序来执行所描述的方法,并且还可以添加、省去、或组合各种步骤。另外,参照某些示例所描述的特征可在其他示例中被组合。

[0112] 通过以上的实施方式的描述,本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现,当然也可以通过硬件,但很多情况下前者是更佳的实施方式。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可以以计算机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(如ROM/RAM、磁碟、光盘)中,包括若干指令用以使得一台终端(可以是手机,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的方法。

[0113] 上面结合附图对本申请的实施例进行了描述,但是本申请并不局限于上述的具体实施方式,上述的具体实施方式仅仅是示意性的,而不是限制性的,本领域的普通技术人员在本申请的启示下,在不脱离本申请宗旨和权利要求所保护的范围情况下,还可做出很多形式,均属于本申请的保护之内。

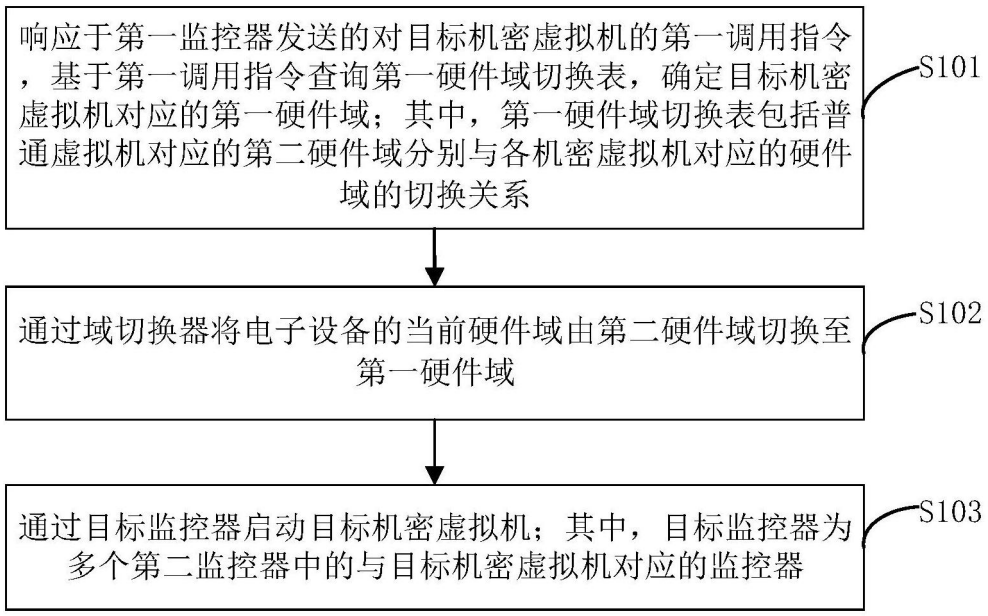

响应于第一监控器发送的对目标机密虚拟机的第一调用指令，基于第一调用指令查询第一硬件域切换表，确定目标机密虚拟机对应的第一硬件域；其中，第一硬件域切换表包括普通虚拟机对应的第二硬件域分别与各机密虚拟机对应的硬件域的切换关系
S101
通过域切换器将电子设备的当前硬件域由第二硬件域切换至第一硬件域
S102
通过目标监控器启动目标机密虚拟机；其中，目标监控器为多个第二监控器中的与目标机密虚拟机对应的监控器
S103

图1

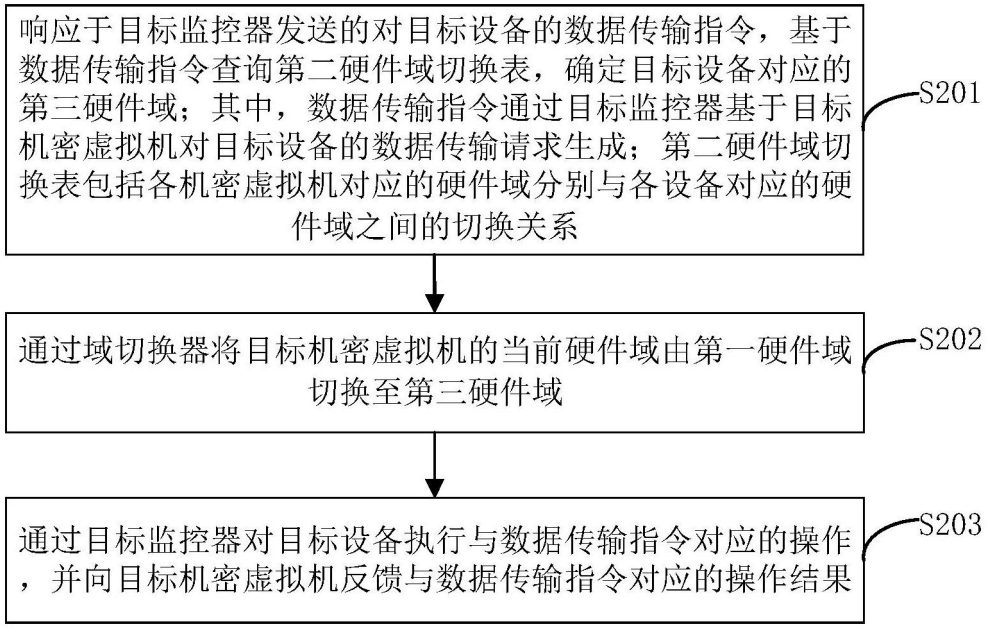

响应于目标监控器发送的对目标设备的数据传输指令，基于数据传输指令查询第二硬件域切换表，确定目标设备对应的第三硬件域；其中，数据传输指令通过目标监控器基于目标机密虚拟机对目标设备的数据传输请求生成；第二硬件域切换表包括各机密虚拟机对应的硬件域分别与各设备对应的硬件域之间的切换关系
S201
通过域切换器将目标机密虚拟机的当前硬件域由第一硬件域切换至第三硬件域
S202
通过目标监控器对目标设备执行与数据传输指令对应的操作，并向目标机密虚拟机反馈与数据传输指令对应的操作结果
S203

图2

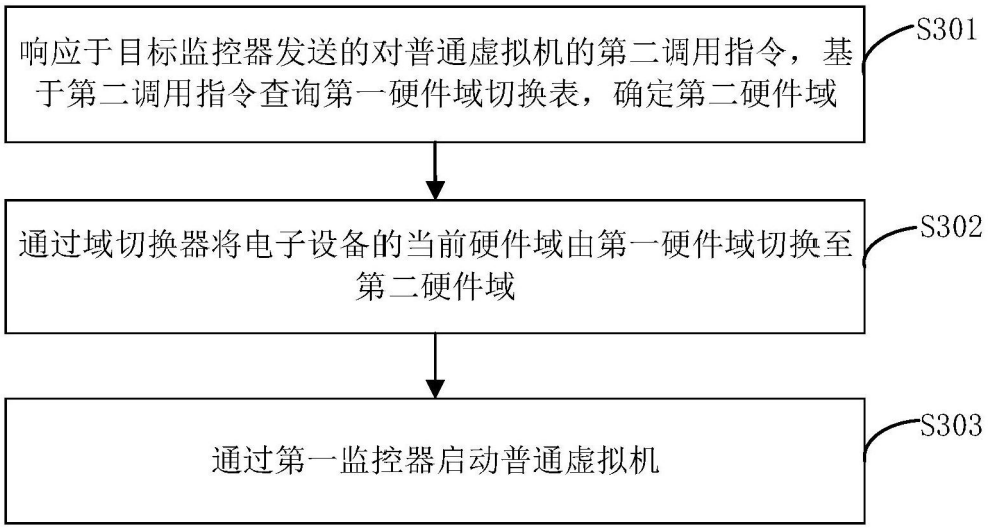

响应于目标监控器发送的对普通虚拟机的第二调用指令，基于第二调用指令查询第一硬件域切换表，确定第二硬件域
S301
通过域切换器将电子设备的当前硬件域由第一硬件域切换至第二硬件域
S302
通过第一监控器启动普通虚拟机
S303

图3

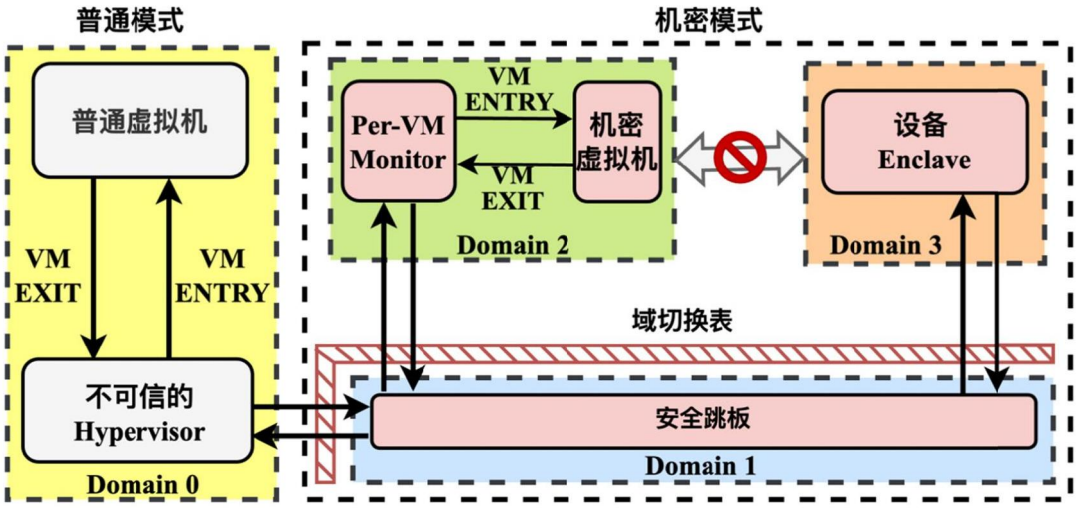

普通模式
机密模式
普通虚拟机
VM EXIT
VM ENTRY
不可信的 Hypervisor
Domain 0
VM ENTRY
Per-VM Monitor
机密虚拟机
VM EXIT
Domain 2
设备 Enclave
Domain 3
域切换表
安全跳板
Domain 1

图4

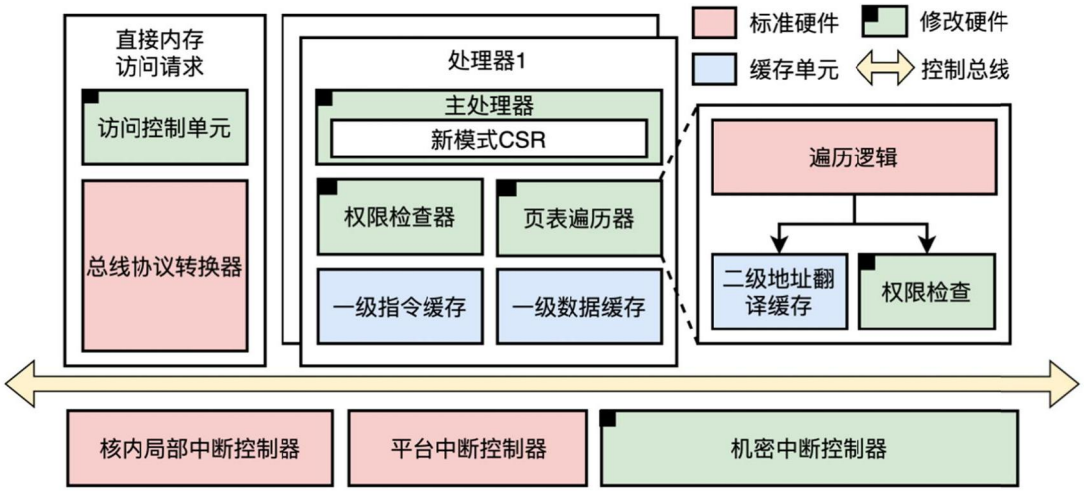

直接内存
访问请求
访问控制单元
总线协议转换器
处理器1
主处理器
新模式CSR
权限检查器
页表遍历器
一级指令缓存
一级数据缓存
标准硬件
修改硬件
缓存单元
控制总线
遍历逻辑
二级地址翻
译缓存
权限检查
核内局部中断控制器
平台中断控制器
机密中断控制器

图5

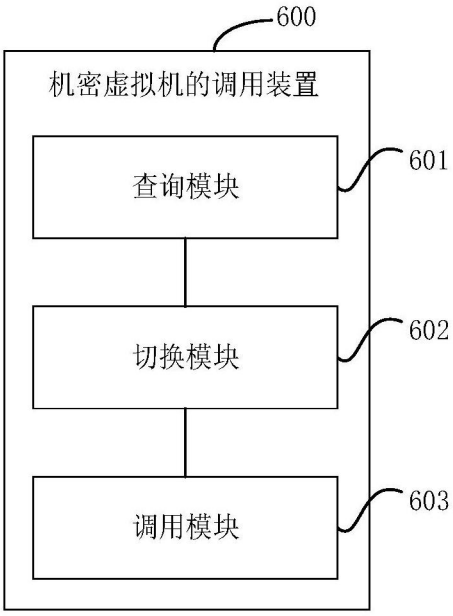

600
机密虚拟机的调用装置
查询模块
601
切换模块
602
调用模块
603

图6

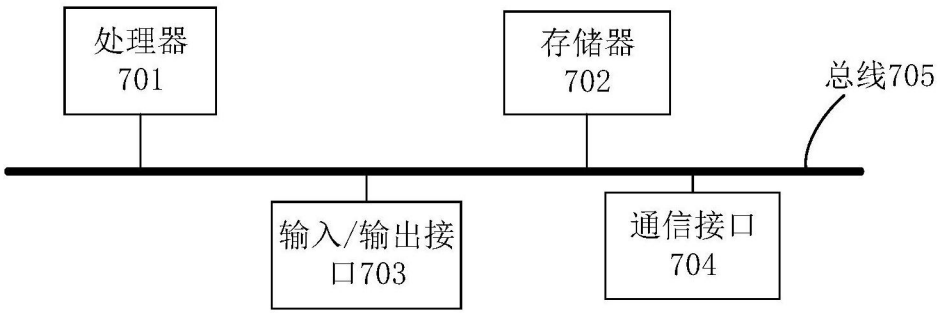

处理器
701
存储器
702
总线705
输入/输出接
口703
通信接口
704

图7