(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102609638 A
(43)申请公布日 2012.07.25

(21)申请号 201110435671.7

(22)申请日 2011.12.22

(71)申请人 中国航天科工集团第二研究院七〇六所
地址 100854 北京市海淀区永定路51号

(72)发明人 曾颖明 王斌 王宏涛 王晓程 姚金利 陈志浩 马书磊 赵政耀 李红

(74)专利代理机构 北京思海天达知识产权代理有限公司 11203
代理人 张慧

(51)Int.Cl.
G06F 21/00(2006.01)
G06F 9/455(2006.01)

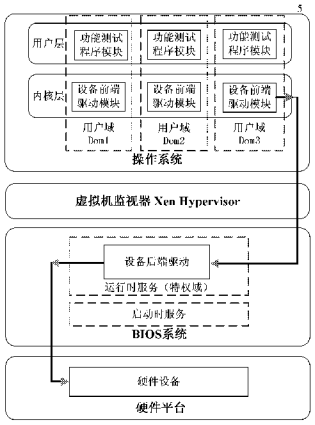
权利要求书 1 页 说明书 3 页 附图 1 页

(54)发明名称

基于UEFI运行时服务的Xen虚拟机架构及其实现方法

(57)摘要

一种基于UEFI运行时服务的Xen虚拟机架构及其实现方法。包括硬件平台、BIOS系统、虚拟机监视器和操作系统，其中UEFI BIOS包括UEFI启动时服务和UEFI运行时服务，特权域作为UEFI运行时服务的一部分，在操作系统运行阶段与设备前端驱动通信；虚拟机监视器位于系统硬件平台与虚拟计算域操作系统软件之间，负责监控下层硬件，操作系统包括内核层的设备前端驱动和用户层的功能测试程序。Xen常规的块设备驱动程序分成前端驱动和后端驱动两部分。由于特权域不存储在硬盘中，而是作为UEFI运行时服务存储在Flash芯片中，解决了目前Xen虚拟机架构存在的安全防护级别不高的问题。同时实现了Xen特权域精简化。



CN 102609638 A

1. 一种基于 UEFI 运行时服务的 Xen 虚拟机架构，包括硬件平台、BIOS 系统、虚拟机监视器和操作系统，其特征在于：UEFI BIOS 包括 UEFI 启动时服务和 UEFI 运行时服务，特权域作为 UEFI 运行时服务的一部分，它包括设备后端驱动，在操作系统运行阶段与设备前端驱动通信；虚拟机监视器位于系统硬件平台与虚拟计算域操作系统软件之间，负责监控下层硬件，并将硬件抽象成可管理调度的实体供上层计算域使用，还为上层计算域提供有效的隔离机制；操作系统包括内核层的设备前端驱动和用户层的功能测试程序；

Xen 常规的块设备驱动程序分成前端驱动和后端驱动两部分，当前端设备驱动程序在接到来自虚拟域操作系统的读写请求后通过事件通道和共享内存向后端设备提出服务请求；后端是运行在特权域中的 UEFI 设备驱动程序，负责接收和完成前端转发的 I/O 请求。

2. 一种基于 UEFI 运行时服务的 Xen 虚拟机架构的实现方法，其特征在于：包括以下步骤：

2.1、运行在用户域中的功能测试程序发送 I/O 读写请求给设备前端驱动；

2.2、设备前端驱动在收到 I/O 读写请求后，将 I/O 读写请求发送给 XenHypervisor；

2.3、Xen Hypervisor 通过事件通道和共享内存将 I/O 读写请求发送给设备后端驱动；

2.4、运行在特权域中的设备后端驱动在收到 I/O 读写请求后，通过其中的原生设备驱动将 I/O 读写请求发送给硬件设备；

2.5、硬件设备进行处理后，将数据返回给设备后端驱动；

2.6、设备后端驱动将获取到的数据发送给 Xen Hypervisor；

2.7、Xen Hypervisor 通过事件通道和共享内存将获取到的数据返回给设备前端驱动；

2.8、设备前端驱动将获取到的数据返回给功能测试程序。

基于 UEFI 运行时服务的 Xen 虚拟机架构及其实现方法

技术领域

[0001] 本发明涉及一种新的 Xen 虚拟机架构，特别是涉及一种基于新一代 UEFI 架构及其实现方法。

背景技术

[0002] Xen 虚拟机架构为一个事实上的开源虚拟化解决方案标准，它具有开源特性、接近于原生系统的性能、永不停机的动态移植功能，以及对原生操作系统的支持等特点。“统一可扩展固件接口 (UEFI)”是一个描述平台固件与操作系统及其它应用软件之间接口的新一代 BIOS 技术标准。UEFI 主要由一系列包含平台相关信息的系统表和供操作系统引导程序、操作系统调用的启动服务和运行时服务构成。这些部件联合起来为一个操作系统的启动与预启动程序的执行提供了一个标准环境。当操作系统启动后，启动服务将全部被卸载，而运行时服务仍滞留在系统内存中，以供上层操作系统调用。

[0003] 在最新的 Xen 虚拟机架构中，其采用的是分离设备驱动模式。该模式在每个用户域中建立前端设备驱动，在特权域中建立后端设备驱动。所有的用户域操作系统像使用普通设备一样向前端设备发送请求，而前端设备通过 I/O 请求描述符和设备通道将这些请求以及用户域的身份信息发送到处于特权域中的后端设备。后端驱动会检查该请求的有效性，进行虚拟设备地址到物理设备地址的变换。但这种架构存在问题是一旦特权域被攻破，后端驱动易被破坏或篡改，将导致所有的虚拟域都将失去保护机制，无法防止重要数据文件和机密信息的泄漏、窃取。另外，在特权域中实现与前端驱动通信的后端设备驱动会导致特权域系统复杂化，也不符合 Xen 特权域精简化的设计初衷。

发明内容

[0004] 本发明的目的在于提供一种新的 Xen 虚拟机架构及其实现方法，解决目前 Xen 虚拟机架构安全防护级别不高，特权域系统不够安全的问题。其中，特权域不存储在硬盘中，而是作为 UEFI 运行时服务存储在 Flash 芯片中。

[0005] 本发明一种基于 UEFI 运行时服务的 Xen 虚拟机架构，是采用以下技术手段实现的：

[0006] 一种基于 UEFI 运行时服务的 Xen 虚拟机架构，包括硬件平台、BIOS 系统、虚拟机监视器 (Xen hypervisor) 和操作系统，其中 UEFI BIOS 包括 UEFI 启动时服务和 UEFI 运行时服务，特权域作为 UEFI 运行时服务的一部分，它包括设备后端驱动，在操作系统运行阶段与设备前端驱动通信；虚拟机监视器位于系统硬件平台与虚拟计算域操作系统软件之间，负责监控下层硬件，并将硬件抽象成可管理调度的实体供上层计算域使用，还为上层计算域提供有效的隔离机制；操作系统包括内核层的设备前端驱动和用户层的功能测试程序。

[0007] Xen 常规的块设备驱动程序分成前端驱动和后端驱动两部分。当前端设备驱动程序在接到来自虚拟域操作系统的读写请求后可以通过事件通道和共享内存向后端设备提出服务请求。后端是运行在特权域中的 UEFI 设备驱动程序，负责接收前端转发的 I/O 请求，

并且通过真正的设备驱动访问物理设备，或使用软件形式处理，完成 I/O 请求。

[0008] 本发明一种基于 UEFI 运行时服务的 Xen 虚拟机架构的实现方法是采用以下技术手段实现的。

[0009] 运行在用户域中的功能测试程序发送 I/O 读写请求给设备前端驱动；

[0010] 设备前端驱动在收到 I/O 读写请求后，将 I/O 读写请求发送给 Xen Hypervisor；

[0011] Xen Hypervisor 通过事件通道和共享内存将 I/O 读写请求发送给设备后端驱动；

[0012] 运行在特权域中的设备后端驱动在收到 I/O 读写请求后，通过其中的原生设备驱动将 I/O 读写请求发送给硬件设备；

[0013] 硬件设备进行处理后，将数据返回给设备后端驱动；

[0014] 设备后端驱动将获取到的数据发送给 Xen Hypervisor；

[0015] Xen Hypervisor 通过事件通道和共享内存将获取到的数据返回给设备前端驱动；

[0016] 设备前端驱动将获取到的数据返回给功能测试程序。

[0017] 本发明基于 UEFI 运行时服务的 Xen 虚拟机架构及其实现方法，与现有技术相比，具有以下明显的优势和有益效果。

[0018] 本发明基于 UEFI 运行时服务的 Xen 虚拟机架构及其实现方法，由于特权域不存储在硬盘中，而是作为 UEFI 运行时服务存储在 Flash 芯片中，解决了目前 Xen 虚拟机架构存在的安全防护级别不高的问题。同时实现了 Xen 特权域精简化。

附图说明

[0019] 图 1 为本发明 Xen 虚拟机架构的结构示意图；

[0020] 图 2 为本发明 Xen 虚拟机架构实现方法的示意图。

具体实施方式

[0021] 以下结合说明书附图，对本发明的具体实施例加以说明。

[0022] 请参阅图 1 所示，为本发明 Xen 虚拟机架构的结构示意图。从图中可以看出，Xen 虚拟机架构由操作系统、虚拟机监视器、BIOS 系统和硬件平台组成。其中，

[0023] 功能测试程序模块，位于用户域（操作系统）层，属于用户态程序，用于对硬件设备进行各项测试。

[0024] 设备前端驱动模块，位于用户域（操作系统）层，属于内核态程序，用于与设备后端驱动通信，与传统原生设备驱动不同，其不能直接访问硬件设备。

[0025] Xen Hypervisor：位于虚拟层，用于为用户域与特权域间的通信提供事件通道和共享内存等机制。

[0026] 设备后端驱动：位于特权域 (UEFI BIOS) 层，属于 UEFI 运行时服务程序，用于与设备前端驱动通信以及与硬件设备通信。它提供平台访问硬件设备的唯一接口，其在包括传统原生设备驱动部分的同时，还负责与设备前端驱动进行通信。

[0027] 硬件设备：位于硬件平台层，如 PCI 网卡、SAS 卡等硬件设备。

[0028] 请参阅图 2 所示，本发明 Xen 虚拟机架构实现方法的示意图。具体步骤如图所述。

[0029] 运行在用户域中的功能测试程序发送 I/O 读写请求给设备前端驱动。

[0030] 设备前端驱动在收到 I/O 读写请求后，将 I/O 读写请求发送给 Xen Hypervisor。

[0031] Xen Hypervisor 通过事件通道和共享内存将 I/O 读写请求发送给设备后端驱动。

[0032] 运行在特权域中的设备后端驱动在收到 I/O 读写请求后，通过其中的原生设备驱动将 I/O 读写请求发送给硬件设备。

[0033] 硬件设备进行处理后，将数据返回给设备后端驱动。

[0034] 设备后端驱动将获取到的数据发送给 Xen Hypervisor。

[0035] Xen Hypervisor 通过事件通道和共享内存将获取到的数据返回给设备前端驱动。

[0036] 设备前端驱动将获取到的数据返回给功能测试程序。

[0037] 最后应说明的是：以上实施例仅用以说明本发明而并非限制本发明所描述的技术方案；因此，尽管本说明书参照上述的各个实施例对本发明已进行了详细的说明，但是，本领域的普通技术人员应当理解，仍然可以对本发明进行修改或等同替换；而一切不脱离发明的精神和范围的技术方案及其改进，其均应涵盖在本发明的权利要求范围当中。

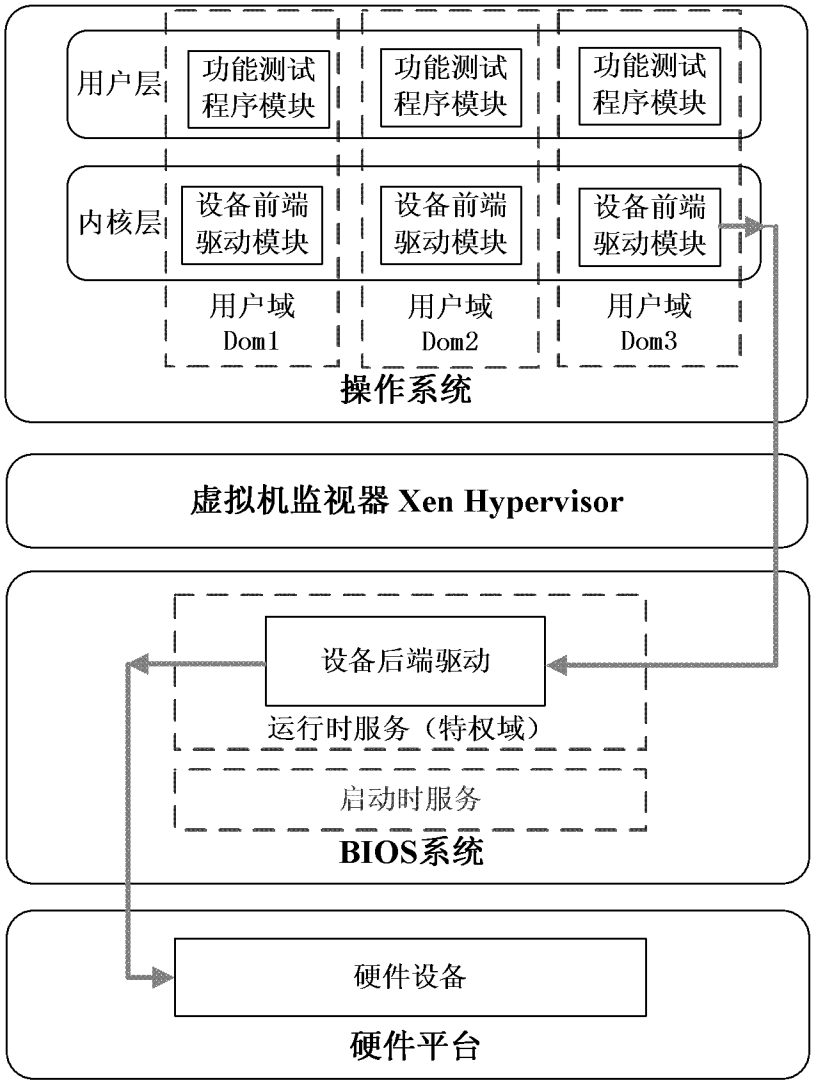

用户层
功能测试程序模块
功能测试程序模块
功能测试程序模块
内核层
设备前端驱动模块
设备前端驱动模块
设备前端驱动模块
用户域 Dom1
用户域 Dom2
用户域 Dom3
操作系统
虚拟机监视器 Xen Hypervisor
设备后端驱动
运行时服务（特权域）
启动时服务
BIOS系统
硬件设备
硬件平台

图 1

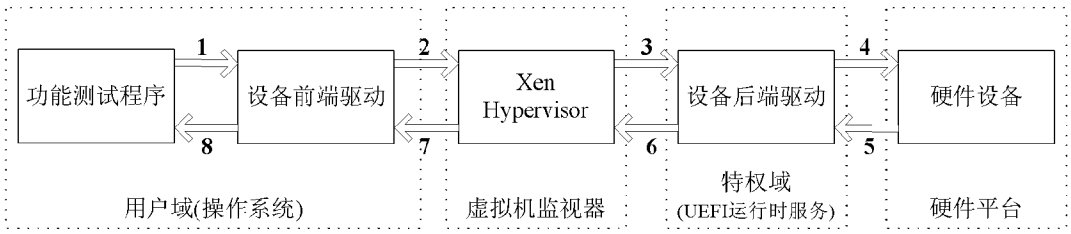

功能测试程序
设备前端驱动
Xen Hypervisor
设备后端驱动
硬件设备
1
2
3
4
5
6
7
8
用户域(操作系统)
虚拟机监视器
特权域 (UEFI运行时服务)
硬件平台

图 2