(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 101373441 B
(45)授权公告日 2012.04.18

(21)申请号 200810200121.5
(22)申请日 2008.09.19
(73)专利权人 苏州壹世通科技有限公司
地址 215021 江苏省苏州工业园区金鸡湖大道 1355 号国际科技园 A0406
(72)发明人 舒曼·拉菲扎德 保罗·威尔曼 林贻基 胡英
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 陈亮
(51)Int.Cl.
G06F 9/455(2006.01)
G06F 21/00(2006.01)

(56)对比文件
CN 1585927 A,2005.02.23, 全文.
US 2005/0204357 A1,2005.09.15, 全文.

审查员 顾静

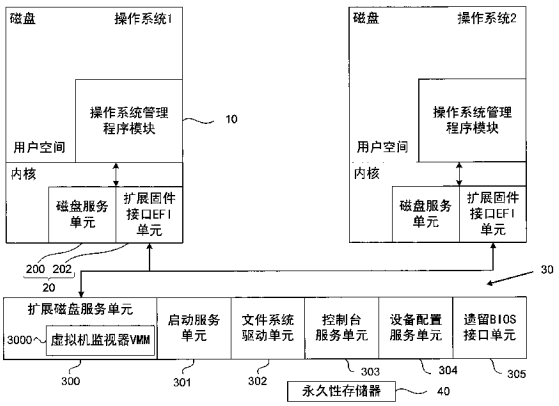
权利要求书 1 页 说明书 4 页 附图 1 页

(54)发明名称

一种基于固件的虚拟化平台系统

(57)摘要

本发明公开了一种基于固件的虚拟化平台系统，保护平台的程序数据和持久性元数据，防止本地操作系统的破坏。其技术方案为：系统包括：操作系统管理程序模块；闪存虚拟操作系统驱动程序模块，该模块包括：扩展固件接口 EFI 单元，与 VMM 通讯和请求 VMM 服务；扩展固件接口模块，安装于固件 EFI 中，负责运行期操作系统实例发出的验证请求及系统管理的控制协议的实现，包括：扩展磁盘服务单元，动态分区及创建删除虚拟机，内含用于隔离各个操作系统实例的 VMM；被保护变量存储区域，用于存储 VMM 中的可读写持久性数据，以使其只能被该扩展固件接口模块访问；永久性存储器，存储只读的 VMM 程序数据，以避免对其恶意更改。本发明应用于计算机领域。



CN 101373441 B

1. 一种基于固件的虚拟化平台系统，将虚拟机监视器 VMM 中的持久性数据放置在一个永久性存储器中，并利用该永久性存储器的固件从操作系统启动时就隐藏该永久性存储器，该虚拟化平台系统包括：

操作系统管理程序模块，安装于每个操作系统实例的用户空间内，为在操作系统环境下执行虚拟化任务和资源管理提供方便，允许用户通过虚拟机监视器 VMM 给予的认证设置任务的优先级，在多个运行期操作系统之间管理和分配物理资源，创造或销毁操作系统实例；

闪存虚拟操作系统驱动程序模块，安装于每个操作系统实例的内核中，由操作系统管理程序模块调用，与操作系统实例进行交互，该模块包括：

磁盘服务单元，在虚拟机监视器 VMM 许可下格式化和分配磁盘资源；

扩展固件接口 EFI 单元，与该虚拟机监视器 VMM 进行通讯和请求 VMM 服务，VMM 服务包括分配物理资源、构建或销毁操作系统实例和修改已有操作系统实例的状态；

扩展固件接口模块，安装于固件 EFI 中，负责运行期的操作系统实例发出的验证请求以及系统管理的控制协议的实现，该模块进一步包括：

扩展磁盘服务单元，用于进行动态分区以及创建删除虚拟机，内含用于隔离各个操作系统实例的虚拟机监视器 VMM，用于进行系统的虚拟化以及分区指引；

被保护变量存储区域，存储 VMM 中的可读写持久性数据，用于确定当前运行的操作系统实例所分配的资源，运行期操作系统没有直接访问被保护变量存储区域的权限，其中的持久性数据只能通过该扩展固件接口模块访问；

永久性存储器，存储只读的虚拟机监视器 VMM 程序数据，以避免对 VMM 程序数据的恶意更改。

2. 根据权利要求 1 所述的基于固件的虚拟化平台系统，其特征在于，该永久性存储器是外部即插即用存储器。

3. 根据权利要求 1 所述的基于固件的虚拟化平台系统，其特征在于，该永久性存储器是闪存阵列存储器。

一种基于固件的虚拟化平台系统

技术领域

[0001] 本发明涉及一种计算机平台，尤其涉及一种与虚拟机监视器 VMM 相关的基于固件的虚拟化平台系统。

背景技术

[0002] 操作系统的虚拟化是一项为了在一台物理计算机上安装多个操作系统的已有的技术。近年来，数据中心的建造者已经开始使用虚拟化作为改善服务器性能和其可利用性的一种手段。这就在工业领域和学术研究领域引起了对虚拟化新的兴趣。不仅如此，虚拟化技术在消费市场也同样有机会产生更大的影响。软件开发商往往依赖多个操作系统实例来测试新的软件。PC 厂商使用虚拟化的一些技术提供一个可靠的还原点，以便用于操作系统出故障时或感染病毒时。新兴市场的客户使用虚拟化来维护本土语言版本和英语版本的不同操作系统。

[0003] 现有虚拟化架构在 RAM 中存储临时元数据，并在二级存储器（通常是一个磁盘）上存储持久性元数据。临时元数据通过操作系统使用传统的虚拟内存技术来防止篡改。对于具有虚拟化能力的现代处理器，CPU 的硬件存储器管理单元甚至可以防止有特权的操作系统代码对虚拟内存的未经授权的访问。

[0004] 然而，在用户的虚拟化架构中，持久性程序数据和元数据经常得不到保障，这是因为这些架构通常通过配置并行的操作系统来获得磁盘的直接访问。直接访问磁盘为并行的虚拟操作系统提供了最佳的性能，但它无法防止未经授权的或伪造的磁盘访问。从客户的角度来看，为了得到最佳的性能，可以牺牲一定的安全性，即容忍未经授权的磁盘访问破坏系统中的另一个操作系统的风险。但是，不能容忍整个系统不可启动或者 VMM 完全无法使用。

[0005] 通常情况下，当操作系统拥有直接磁盘权限时，无法防止操作系统存取磁盘的任何部分，因此有可能损害 VMM 的持久性数据。这包括描述硬件资源的静态分区配置的元数据和每个虚拟操作系统环境的定义。持久性数据还包括 VMM 的可执行程序。因此，一个未经授权的磁盘区域的写入操作会带来灾难性的后果，包括配置数据的销毁，或者一个系统分区规则的破坏，两者都会使整个系统陷入无法恢复、无法启动的状态。

[0006] 在服务器和用户部署中，系统的虚拟机监视器 VMM 软件保持其不可侵犯性是至关重要的。但是如上所述，目前的虚拟化架构将重要的 VMM 数据存储在磁盘上，它可以被计算机中任一操作系统访问。由于用户的虚拟环境不稳定、经常感染病毒、实验性代码故障和传统操作系统的破坏性行为，一般的操作系统中的整个虚拟化架构很容易受到侵害，并且难以挽救。

发明内容

[0007] 本发明的目的在于解决上述问题，提供了一种基于固件的虚拟化平台系统，保护平台的程序数据和持久性元数据，防止本地操作系统的破坏。

[0008] 本发明的技术方案为：本发明揭示了一种基于固件的虚拟化平台系统，将虚拟机监视器 VMM 中的持久性数据放置在一个永久性存储器中，并利用该永久性存储器的固件从操作系统启动时就隐藏该永久性存储器，该虚拟化平台系统包括：

[0009] 操作系统管理程序模块，安装于每个操作系统实例的用户空间内，为在操作系统环境下执行虚拟化任务和资源管理提供方便，允许用户通过虚拟机监视器 VMM 给予的认证设置任务的优先级，在多个运行期操作系统之间管理和分配物理资源，创造或销毁操作系统实例；

[0010] 闪存虚拟操作系统驱动程序模块，安装于每个操作系统实例的内核中，由操作系统管理程序模块调用，与操作系统实例进行交互，该模块包括：

[0011] 磁盘服务单元，在虚拟机监视器 VMM 许可下格式化和分配磁盘资源；

[0012] 扩展固件接口 EFI 单元，与该虚拟机监视器 VMM 进行通讯和请求 VMM 服务，VMM 服务包括分配物理资源、构建或销毁操作系统实例和修改已有操作系统实例的状态；

[0013] 扩展固件接口模块，安装于固件 EFI 中，负责运行期的操作系统实例发出的验证请求以及系统管理的控制协议的实现，该模块进一步包括：

[0014] 扩展磁盘服务单元，用于进行动态分区以及创建删除虚拟机，内含用于隔离各个操作系统实例的虚拟机监视器 VMM，用于进行系统的虚拟化以及分区指引；

[0015] 被保护变量存储区域，存储 VMM 中的可读写持久性数据，用于确定当前运行的操作系统实例所分配的资源，运行期操作系统没有直接访问被保护变量存储区域的权限，其中持久性数据只能通过该扩展固件接口模块访问；

[0016] 永久性存储器，存储只读的虚拟机监视器 VMM 程序数据，以避免对 VMM 程序数据的恶意更改。

[0017] 上述的基于固件的虚拟化平台系统，其中，该永久性存储器是外部即插即用存储器。

[0018] 上述的基于固件的虚拟化平台系统，其中，该永久性存储器是闪存阵列存储器。

[0019] 本发明对比现有技术有如下的有益效果：在现有的虚拟化解决方案中，运行期操作系统有权直接访问磁盘资源，现有的虚拟化结构无法防止操作系统的故障和恶意篡改对数据的破坏，因而无法提供对虚拟化平台的程序数据和持久性元数据（比如配置信息）的保护。本发明利用 EFI 建立一个可扩展的模块，该模块可分配系统资源给普通的单个或多个操作系统。该模块还可以支持将只读的 VMM 程序数据存储在一个已配置好的外部的只读的即插即用存储设备中，少量的可读写持久性虚拟元数据（通常是 64KB 或更少）能够存储到 EFI 平台上的只能够被 EFI 模块访问的被保护变量区域中。这样，本发明就能模块化地将持久性元数据和平台程序数据放到操作系统无法写入的地方，既允许一个认证用户在运行期或启动时控制和分配资源，同时又能防止未授权用户或操作系统的故障损坏虚拟机平台的重要数据。

附图说明

[0020] 图 1 是本发明的基于固件的虚拟化平台系统的较佳实施例的原理图。

具体实施方式

[0021] 下面结合附图和实施例对本发明作进一步的描述。

[0022] 图 1 示出了本发明的基于固件的虚拟化平台系统的较佳实施例的原理。请参见图 1，基于固件的虚拟化平台系统的实施例包括操作系统管理程序模块 10、闪存虚拟操作系统驱动程序模块 20、扩展固件接口模块 30 以及永久性存储器 40。

[0023] 操作系统管理程序模块 (OS Manager)10 安装在每个操作系统实例的用户空间内，为在普通操作系统环境下执行虚拟化任务和资源管理提供了方便。操作系统管理程序模块 10 允许用户通过底层虚拟机监视器 (VMM)3000 给予的适当认证，设置任务的优先级，在多个运行期操作系统实例之间管理和分配物理资源（如 I/O 和内存），创造或销毁操作系统的实例。对于新建一个操作系统实例，操作系统管理程序中的一个关键功能是磁盘资源管理。磁盘资源管理包括 ：用户空间的操作系统管理程序使用户能够创建新的虚拟磁盘分区来放置新的操作系统实例 ；格式化现有分区的文件系统 ；将虚拟分区分配给一个或多个操作系统实例。以这种方式，操作系统管理程序使用户能够灵活地控制其存储资源，这是建立操作系统虚拟机和多个操作系统实例之间的数据共享的基础（就像用户在多个操作系统实例之间共享应用程序或数据时情况一样）。

[0024] 闪存虚拟操作系统驱动程序 (Flash VOS Driver) 模块 20 安装于每个操作系统实例的内核 (Kernel) 中，由操作系统管理程序模块 10 调用，与操作系统实例进行交互。闪存虚拟操作系统驱动程序模块 20 包括磁盘服务单元 200 和扩展固件接口 EFI 单元 202，其中磁盘服务单元 200 在虚拟机监视器 VMM 3000 许可下格式化和分配磁盘资源，而扩展固件接口 EFI 单元 202 与虚拟机监视器 VMM 3000 进行通讯和请求 VMM 服务，VMM 服务包括分配物理资源、构建或销毁操作系统实例和修改已有操作系统实例的状态（比如挂起或者恢复）。

[0025] 扩展固件接口模块 (Flash VOS EFI)30 安装于固件 EFI 中，是在传统的 EFI 组件，例如传统的启动服务 (Boot Services) 单元 301、文件系统驱动 (File-system Drivers) 单元 302、控制台服务 (Console Services) 单元 303、设备配置服务 (Device Configure Services) 单元 304、遗留 BIOS 接口 (Legacy BIOS Interface) 单元 305，旁边的另一个模块，负责运行期的操作系统所发出的验证请求以及系统管理的控制协议的实现。扩展固件接口模块 30 包括扩展磁盘服务单元 300 和被保护变量存储区域（未图示），扩展磁盘服务单元 300 用于进行动态分区以及创建、删除虚拟机，可进行系统的虚拟化以及分区指引，内含用于隔离各个操作系统实例的虚拟机监视器 VMM 3000。被保护变量存储区域用于存储 VMM 中的可读写持久性数据，用于确定给当前运行的哪些操作系统实例分配什么资源，持久性数据存储在被保护变量存储区域中可使其只能被扩展固件接口模块 30 访问，避免元数据被恶意更改。这个扩展接口固件模块 30 也包含一个启动时的操作系统管理器，允许用户执行和用户空间操作系统管理程序模块 10 相同的功能，只是这个操作系统管理器在 EFI 启动控制台而已。启动时的操作系统管理器在系统没有任何操作系统时通过配置一个新的系统来设立操作系统环境。一旦建立了至少一个操作系统，用户既可以使用运行期用户空间操作系统管理程序模块 10，也可以使用启动时基于 EFI 的操作系统管理器。

[0026] 永久性存储器 40 存储只读的虚拟机监视器 VMM 程序数据，以避免对 VMM 程序数据的恶意更改。这个永久性存储器 40 可以是外部即插即用存储器，也可以是闪存阵列存储器。VMM 程序数据存储在这个永久性存储器 40 中并使其只读。

[0027] 上述实施例是提供给本领域普通技术人员来实现或使用本发明的，本领域普通技

术人员可在不脱离本发明的发明思想的情况下，对上述实施例做出种种修改或变化，因而本发明的保护范围并不被上述实施例所限，而应该是符合权利要求书提到的创新性特征的最大范围。

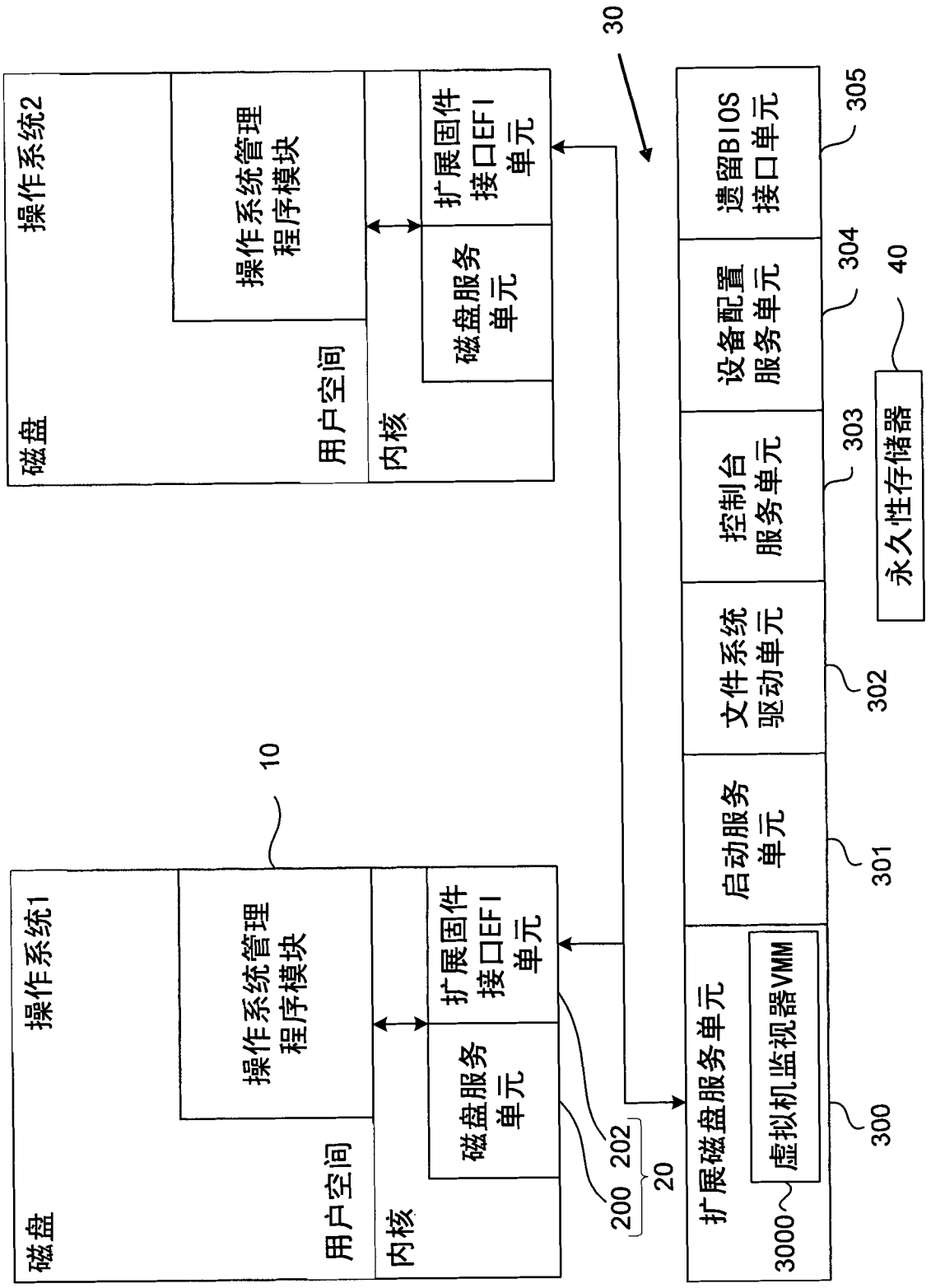

磁盘
操作系统1
操作系统管理程序模块
用户空间
内核
磁盘服务单元
扩展固件接口EFI单元
10
200
202
20
30
扩展磁盘服务单元
虚拟机监视器VMM
3000
300
启动服务单元
301
文件系统驱动单元
302
控制台服务单元
303
设备配置服务单元
304
遗留BIOS接口单元
305
永久性存储器
40
磁盘
操作系统2
操作系统管理程序模块
用户空间
内核
磁盘服务单元
扩展固件接口EFI单元

图 1