



# [12] 发明专利申请公布说明书

[21] 申请号 200680028937.3

[43] 公开日 2008年8月6日

[11] 公开号 CN 101238471A

[22] 申请日 2006.7.27

[21] 申请号 200680028937.3

[30] 优先权

[32] 2005. 8. 9 [33] US [31] 11/200,662

[86] 国际申请 PCT/US2006/029609 2006.7.27

[87] 国际公布 WO2007/021513 英 2007.2.22

[85] 进入国家阶段日期 2008.2.4

[71] 申请人 英特尔公司

地址 美国加利福尼亚州

[72] 发明人 S·格罗布曼 D·格劳罗克

N·萨加尔 J·格鲁伯

[74] 专利代理机构 中国专利代理(香港)有限公司  
代理人 曾祥凌 王忠忠

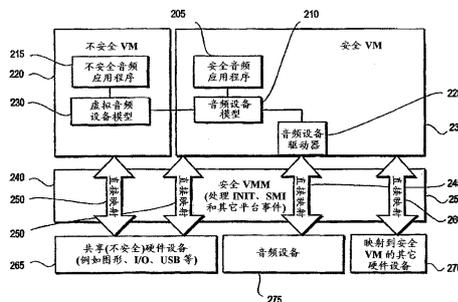
权利要求书 5 页 说明书 10 页 附图 4 页

## [54] 发明名称

安全音频程序的独占访问

## [57] 摘要

在平台上执行监控器，该监控器能够提供对平台的音频 I/O 设备的独占、安全访问，在平台上执行第一分区，通过将音频 I/O 设备从监控器直接映射到第一分区，来为在第一分区中执行的应用程序提供音频设备模型；以及向第一分区中以安全模式执行音频功能的程序提供对音频 I/O 设备的独占、安全访问。



1. 一种方法, 包括:

在平台上执行监控器, 所述监控器能够提供对所述平台的音频 I/O 设备的独占、安全访问;

在所述平台上执行第一分区;

通过将所述音频 I/O 设备从所述监控器直接映射到所述第一分区, 来为在所述第一分区中执行的应用程序提供所述第一分区中的音频设备模型; 以及

向在所述第一分区中以安全模式执行音频功能的程序提供对所述音频 I/O 设备的独占、安全访问。

2.

3. 如权利要求 1 所述的方法, 其特征在于, 还包括

在所述平台上执行第二分区; 以及

通过将所述音频设备模型从所述第一分区再映射到所述第二分区, 来在所述第二分区中提供虚拟音频设备模型;

以及

其中, 为在所述第一分区中执行的所述程序提供对所述音频 I/O 设备的独占访问的步骤还包括禁用所述虚拟音频设备模型。

4.

5. 如权利要求 2 所述的方法, 其特征在于, 禁用所述虚拟音频设备模型的步骤还包括为访问所述虚拟设备模型的应用程序提供空数据流。

6. 如权利要求 2 所述的方法, 其特征在于, 禁用所述虚拟音频设备模型的步骤还包括阻挡由应用程序对所述虚拟音频设备的访问。

7. 如权利要求 2 所述的方法, 其特征在于, 所述虚拟音频设备模型包括热可插拔设备的模型, 以及禁用所述虚拟音频设备模型的步骤还包括模拟所述虚拟音频设备模型的热拔事件。

8. 如权利要求 2 所述的方法, 其特征在于

所述第一分区包括在所述平台上执行的第一虚拟机;

所述第二分区包括在所述平台上执行的第二虚拟机;

所述监控器包括安全虚拟机监控器(SVMM); 以及

包含所述 SVMN 的代码和数据是从所述第一虚拟机不可访问的。

9. 如权利要求 6 所述的方法, 其特征在于, 提供对所述音频 I/O 设备的安全访问的步骤还包括: 所述 SVMM 禁止由在所述第二虚拟机中执行的程序对用于存储音频数据的存储位置进行直接存储器存取。

10. 如权利要求 2 所述的方法, 其特征在于, 还包括以下步骤:  
当没有应用程序在所述第一分区中以安全模式执行音频功能时, 向所述音频 I/O 设备提供到所述第一分区中的所述音频设备模型的输出数据以及到所述第二分区中的所述虚拟音频设备模型的输出数据这两者之和。

11. 如权利要求 1 所述的方法, 其特征在于, 还包括以下步骤:

监控在通信上耦合到所述平台的所有音频设备; 以及

如果所述第一分区中的所述程序正以安全模式执行, 则阻止在通信上耦合到所述平台的任何不安全音频设备的操作。

12. 一种系统, 包括:

平台, 包括处理器和存储器;

监控器, 驻留在所述存储器中并且可在所述平台上执行, 能够提供对所述平台的音频 I/O 设备的独占、安全访问;

第一分区, 可在所述平台上执行;

所述第一分区中的音频设备模型, 对在所述第一分区中执行的应用程序, 将所述音频 I/O 设备从所述监控器直接映射到所述第一分区;  
以及

所述监控器还向在所述第一分区中以安全模式执行音频功能的程序提供对所述音频 I/O 设备的独占、安全访问。

13. 如权利要求 10 所述的系统, 其特征在于, 还包括:

第二分区，能够在所述平台上执行，还包括从所述第一分区的音频设备模型再映射的虚拟音频设备模型；以及

所述监控器还至少部分地禁用所述虚拟音频设备模型。

14. 如权利要求 11 所述的系统，其特征在于，所述虚拟音频设备模型包括热可插拔设备的模型，以及所述监控器还模拟所述虚拟音频设备模型的热拔事件。

15. 如权利要求 11 所述的系统，其特征在于

所述第一分区包括在所述平台上执行的第一虚拟机；

所述第二分区包括在所述平台上执行的第二虚拟机；

所述监控器包括安全虚拟机监控器(SVMM)；以及

包含所述 SVMN 的代码和数据是从所述第一虚拟机不可访问的。

16. 如权利要求 13 所述的系统，其特征在于，所述 SVMM 还禁止由在所述第二虚拟机中执行的程序对用于存储音频数据的存储位置进行直接存储器存取。

17. 如权利要求 11 所述的系统，其特征在于，所述监控器还当没有应用程序在所述第一分区中以安全模式执行音频功能时，向所述音频 I/O 设备提供到所述第一分区中的所述音频设备模型的输出数据以及到所述第二分区中的所述虚拟音频设备模型的输出数据这两者之和。

18. 如权利要求 10 所述的系统，其特征在于，所述监控器还执行以下步骤：

监控在通信上耦合到所述平台的所有音频设备；以及

如果所述第一分区中的所述程序正以安全模式执行，则阻止在通信上耦合到所述平台的任何不安全音频设备的操作。

19. 一种机器可访问介质，其中存储了在由机器访问时使所述机器执行方法的数据，所述方法包括以下步骤：

在平台上执行监控器，所述监控器能够提供对所述平台的音频 I/O 设备的独占、安全访问；

在所述平台上执行第一分区；

通过将所述音频 I/O 设备从所述监控器直接映射到所述第一分区，来为在所述第一分区中执行的应用程序提供所述第一分区中的音频设备；以及

向在所述第一分区中以安全模式执行音频功能的程序提供对所述音频 I/O 设备的独占、安全访问。

20. 如权利要求 17 所述的机器可访问介质，其特征在于，所述方法还包括以下步骤：

在所述平台上执行第二分区；以及

通过将所述音频设备模型从所述第一分区再映射到所述第二分区，来在所述第二分区中提供虚拟音频设备模型；

以及

其中，为中所述第一分区中执行的所述程序提供对所述音频 I/O 设备的独占访问的步骤还包括禁用所述虚拟音频设备模型。

21. 如权利要求 18 所述的机器可访问介质，其特征在于，禁用所述虚拟音频设备模型的步骤还包括为访问所述虚拟设备模型的应用程序提供空数据流。

22. 如权利要求 18 所述的机器可访问介质，其特征在于，禁用所述虚拟音频设备模型的步骤还包括阻挡由应用程序对所述虚拟音频设备的访问。

23. 如权利要求 18 所述的机器可访问介质，其特征在于，所述虚拟音频设备模型包括热可插拔设备的模型，以及禁用所述虚拟音频设备模型的步骤还包括模拟所述虚拟音频设备模型的热拔事件。

24. 如权利要求 18 所述的机器可访问介质，其特征在于：

所述第一分区包括在所述平台上执行的第一虚拟机；

所述第二分区包括在所述平台上执行的第二虚拟机；

所述监控器包括安全虚拟机监控器(SVMM)；以及

包含所述 SVMN 的代码和数据是从所述第一虚拟机不可访问的。

25. 如权利要求 22 所述的机器可访问介质, 其特征在于, 提供对所述音频 I/O 设备的安全访问的步骤还包括: 所述 SVM 禁止由在所述第二虚拟机中执行的程序对用于存储音频数据的存储位置进行直接存储器存取。

26. 如权利要求 18 所述的机器可访问介质, 其特征在于, 还包括: 当没有应用程序在所述第一分区中以安全模式执行音频功能时, 向所述音频 I/O 设备提供到所述第一分区中的所述音频设备模型的输出以及到所述第二分区中的所述虚拟音频设备模型的输出这两者之和。

27. 如权利要求 17 所述的机器可访问介质, 其特征在于, 还包括: 监测在通信上耦合到所述平台的所有音频设备; 以及

如果所述第一分区中的所述程序正以安全模式执行, 则阻止在通信上耦合到所述平台的任何不安全音频设备的操作。

## 安全音频程序的独占访问

### 背景技术

使用诸如 Intel® Pentium 4 处理器等处理器的基于处理器的系统可能是个人计算机、服务器计算机、工作站、个人桌面助理(PDA)、游戏系统、机顶盒或者智能移动电话等。这种系统(或者在本文中称作平台)可包括一个或多个音频输入和输出设备。这些设备例如可包括: 板载音频卡或声卡, 连接到诸如 PCI Express™总线等系统总线; 外部设备, 通过诸如通用串行总线(USB)连接到系统; 乃至通过数据网络远程连接的设备, 采用可能通过网络电缆或无线的无线电或红外链路的网络连接将系统的音频输入数据和输出数据导向该数据网络。这种设备例如可提供通过一个或多个模拟或数字输出声道、以各种格式诸如线路电平模拟音频、SP/DIF 数字音频、如 Dolby Digital®比特流等数字比特流编码环绕声以及已知的许多其它格式来输出由在平台上执行的程序所产生或处理的声音的能力。类似地, 作为备选或附加的方案, 设备可提供模拟或数字格式的音频输入能力, 从而允许例如来自扩音器、线路电平模拟音频源或者具有各种格式的编码音频流的数字比特流的输入。这种音频输入数据然后可由系统的程序来接收、处理、分析和存储, 以便执行各种功能。

在一个实例中, 基于处理器的系统的这类音频能力允许将平台用于通过采用网络电话(VOIP)的网络的语音通信。通过在因特网或其它网络上发送语音数据之前对它进行加密, 诸如 Skype 和 PGPhone 之类的应用解决与通过 VOIP 所进行的通话的安全性和保密性相关的问题。但是, 以未加密格式对语音或其它通信进行编码的数据一般在它被接收或者被发送到的平台上仍然是可用的。其原因在于, 在输入语音或消息音频时的初始阶段以及在输出语音或消息音频时的最终阶段, 一

般需要由音频设备对未加密数字音频数据的缓冲器进行直接存储器存取。这可能允许平台上的恶意进程访问未加密的音频数据。通过在缓冲音频之前在硬件中对其进行加密,有可能避免这个问题,但是这类解决方案需要安装新的音频硬件。此外,即使音频数据无论何时都以数字形式进行加密,但是,如果模拟音频从平台设备输出到周围环境或者从周围环境输入平台设备,那么恶意进程可静静地利用处于输入模式的平台音频设备、如扩音器,以记录来自周围环境的音频数据(如果该记录是可能的)。

### 附图说明

图 1 是一个实施例中的虚拟环境的高级框图。

图 2 是一个实施例中的主要组件的高级框图。

图 3 表示一个实施例中的组合虚拟和实际适配器的输出数据。

图 4 是一个实施例的操作的高级流程图。

### 具体实施方式

一些实施例可包括虚拟化系统。虚拟化是一种技术,它使具有通过硬件和软件或者在一些情况下仅通过软件对虚拟化的支持的基于处理器的主机能够提供主机的抽象,使得主机的基础硬件表现为一个或多个独立操作的虚拟机。因此,各虚拟机可用作独立平台。通常,虚拟化技术用于使多个客户(guest)操作系统和/或其它客户软件(guest software)共存,并且明显同时且明显独立地在多个虚拟机上执行,然而实际是在物理上于相同硬件平台上执行。虚拟机可模仿主机的硬件或者提供完全不同的硬件抽象。

虚拟化系统为虚拟机中运行的客户软件提供一组资源(例如,处理器、存储器、IO 设备),并且可将物理主机的一部分或全部组件映射到虚拟机中,或者创建全虚拟组件。因此,虚拟化系统可以说是向客户软件提供虚拟裸机接口。在一些实施例中,虚拟化系统可包括控制主

机的虚拟机监控器(VMM)。VMM为在虚拟机(VM)中运行的客户软件提供一组资源,例如处理器、存储器和IO设备。VMM可将物理主机的部分或全部组件映射到虚拟机中,并且可创建以VMM中的软件模拟的完全虚拟组件,它们包含在虚拟机中(例如虚拟IO设备)。VMM采用硬件虚拟化体系结构中的工具来向虚拟机提供服务以及提供对执行于主机上的多个虚拟机以及它们之间的保护。一般来说,VMM运行的存储空间是由VMM提供服务的虚拟机的任何一个不可访问的主物理存储器的一部分。

图1图解说明了虚拟机环境100的一个实施例。在这个实施例中,基于处理器的平台116可执行VMM112。VMM虽然通常以软件实现,但可模拟虚拟裸机接口并将其输出到较高层软件。这种较高层软件可包括标准OS、实时OS,或者可能是具有有限操作系统功能性的分离(strip down)环境,以及在一些实施例中可能不包括标准OS中通常可用的OS工具。作为备选的方案,例如,VMM112可在另一个VMM之中或者采用VMM的服务来运行。在一些实施例中,VMM可通过例如硬件、软件、固件或者通过各种技术的结合来实现。

平台硬件116可能是个人计算机(PC)、大型计算机、诸如个人数字助理(PDA)或“智能”移动电话等的手持设备、便携计算机、机顶盒或其它基于处理器的系统。平台硬件116包括至少一个处理器118和存储器120。处理器118可能是能够运行程序的任何类型的处理器,例如微处理器、数字信号处理器、微控制器等。在实施例中,处理器可包括用于执行的微码、可编程逻辑或硬编码逻辑。虽然图1仅示出一个这样的处理器118,但是,在一实施例中,系统中可能存在一个或多个处理器。另外,处理器118可包括多个核心,支持多个线程等。在各个实施例中,存储器120可包括硬盘、软盘、随机存取存储器(RAM)、只读存储器(ROM)、闪速存储器、上述设备的任何组合、或者处理器118可读的其它任何类型的机器介质。存储器120可存储用于进行程序执行和其它方法实施例的指令和/或数据。

VMM 112 为客户软件提供一个或多个虚拟机的抽象,它可向各种客户提供相同或不同的抽象。图 1 示出两个虚拟机 102 和 114。在各虚拟机上运行的客户软件,如客户软件 101 和 111 可包括诸如客户 OS 104 或 106 等客户 OS 以及各种客户软件应用程序 108 和 110。客户软件 101 和 111 可访问虚拟机中的物理资源(例如处理器寄存器、存储器和 I/O 设备),客户软件 101 和 111 正在虚拟机中运行并执行其它功能。例如,根据虚拟机 102 和 114 中提供的处理器和平台的体系结构,客户软件 101 和 111 预期有权访问所有寄存器、高速缓存、结构、I/O 设备、存储器等。

在一个实施例中,处理器 118 根据虚拟机控制结构(VMCS)124 中存储的数据来控制虚拟机 102 和 114 的操作。VMCS 124 是一种结构,可包含客户软件 101 和 111 的状态、VMM 112 的状态、表明 VMM 112 希望如何控制客户软件 101 和 111 的操作的运行控制信息、控制 VMM 112 与虚拟机之间的转变的信息等。处理器 118 从 VMCS 124 中读取信息,以便确定虚拟机的执行环境并限制其行为。在一个实施例中,VMCS 124 存储在存储器 120 中。在一些实施例中,多个 VMCS 结构用来支持多个虚拟机。

可由客户软件(例如 101,包括客户 OS 104 和应用程序 108)访问的资源可分类为“特许”或者“非特许”。对于特许资源,VMM 112 有助于实现客户软件所需的功能性,同时保持对这些特许资源的最终控制。此外,各客户软件 101 和 111 预期将处理诸如异常(例如页面出错、一般保护出错等)、中断(例如硬件中断、软件中断)以及平台事件(例如初始化(INIT)和系统管理中断(SMI))之类的各种平台事件。这些平台事件的一部分是“特许的”,因为它们必须由 VMM 112 来处理,以便确保虚拟机 102 和 114 的正确操作,以及用于对客户软件以及客户软件之间的保护。客户操作系统以及客户应用程序均可尝试访问特许资源,并且均可引起或遇到特许事件。特许平台事件以及对特许资源的访问尝试在本文中统称为“特许事件”或“虚拟化事件”。

图 2 示出一个实施例中的系统的高级视图。图中所示的平台具有对于独占访问可能或者可能不安全的诸如一般、共享硬件设备 265 等一组硬件设备，例如图形或显示设备、诸如键盘、打印机等输入和输出设备以及诸如 USB 总线等总线上的其它设备。它还可能具有可由安全 VMM (SVMM) 240 确保安全的一组设备，如音频 I/O 设备 275 以及可能的其它设备 270。在这个实施例中，通过监测对设备的访问以及在发生对设备缓冲器的直接存储器存取(DMA)或者对设备的其它访问时在支持虚拟化的硬件中建立中断，然后根据所尝试访问的来源处理中断，VMM 可保障对设备的访问。因此，例如，如果安全 VM 235 和另一个(不安全) VM 220 在 SVMM 240 的监控下正在平台上执行，则在进程正执行于不安全 VM 220 时，SVMM 可禁止该进程对音频设备 275 的任何访问。此外，在这个实施例中，SVMM 代码和数据驻留在执行于主机上的 VM 不可访问的主机的物理存储器的一部分中。这可通过诸如存储器分区或存储器再映射等技术来实现。

在所示实施例中，通过由 SVMM 240 向安全 VM 235 提供的对音频硬件 275 的直接映射，平台的音频设备的设备驱动器 225 仅在安全 VM 235 中才是可用的。在安全 VM 235 中执行的进程 205 则经由安全 VM 235 中的音频设备模型 210 来访问音频硬件。但是，虽然音频数据也对执行于另一个不安全 VM 的进程 215 可用，但它仅经由作为安全 VM 中的“实际”音频设备模型 210 的映射的虚拟音频设备模型 230 才可用于那个进程。因此，安全 VM 205 中的应用程序可禁用虚拟设备音频模型 230。

类似地，其它硬件设备 270 可独占地映射 260 到安全 VMM 235。另一方面，不安全设备可直接映射 250 到不安全 VM 220 和安全 VM 235，并且对它们的访问可保持不受限制。

可参照两种情况来理解安全音频实施例的操作。第一种情况是当不安全音频应用程序、如图 2 中的应用程序 215 在安全音频应用程序 205 可能也在将音频设备用于输出的同时试图对音频设备 275 进行只

输出访问时的实施例的操作。由于一般来说，问题在于恶意进程可能在偷听安全或私人通话，因此，在该实施例中，甚至对于不安全程序，一般也自由地允许对音频进行只输出访问。因此，在这种情况下，音频设备模型 210 和虚拟音频设备模型 230 的输出通过求和或类似方法进行结合，并通过一个或多个音频设备 275 以组合方式输出。

第二种情况是当不安全 VM 中的程序、即不安全音频应用程序 215 试图访问其音频接口、即虚拟音频设备模型以便输入时的实施例的操作。如果安全 VM 或安全音频应用程序 205 中的程序正经由音频设备模型 210 以安全模式访问平台的音频设备，则它可能通过阻挡、掩蔽或模拟虚拟音频设备的断开连接，来阻挡从不安全 VM 对一个或多个音频设备 275 的访问。这一般在安全音频应用程序正产生音频输出数据时的情况下或者在它处于音频输入模式时的情况下进行，因为不安全 VM 中的恶意进程可能能够偷听安全音频应用程序的输出或者正输入到安全应用程序的环境声音、如扬声器的语音。

经由 SVM 可用的其它安全平台特征可包括防止系统存储器或者它的若干部分受到绕过处理器的直接存取的能力，以及对系统存储器的区域设置读、写或执行限制的能力。

图 3 示出当不安全音频应用程序试图对音频设备进行只输出访问时的实施例的操作。该图是平台的音频输出数据的图表，绘制出相对于时间 360 的幅度 310。该图示出在平台的音频输出上得到的输出波形 330。通过将访问安全 VM 中的音频设备模型的安全 VM 中的应用程序的音频输出 350 与访问不安全 VM 中的虚拟设备模型的不安全 VM 中的应用程序的音频输出 340 相加，来得到波形 330。

图 4 在高层次上示出当不安全音频应用程序在 420 试图对音频设备进行输入访问时的实施例的操作。如果安全 VM 中的任何程序以输入模式连接到平台的音频设备，430，或者以输出模式连接到平台的音频设备，450，则 SVM 可捕获(trap)该访问。虚拟音频设备模型然后被禁用，440。否则，可向不安全分区中的程序提供对音频设备的访问，

460。

440 中的动作可通过各种方式来进行。首先，虚拟设备可能只设置在一种模式中，在其中，它在安全程序实际上连接到平台音频时向所连接的不安全程序发送空数据。其次，可通过适度地处理不安全 VM 的访问程序中可能发生的任何所得误差来阻挡虚拟设备。一个备选方法是将虚拟音频设备建模为可热插拔(hot-pluggable)设备。访问可热插拔设备的应用程序一般设计成适度地处理它的断开连接。因此，在这种情况下进行 440 中的动作时，虚拟设备模型模拟设备的热拔(hot-unplug)事件，从而使平台音频设备对不安全虚拟机中的应用程序不可用。

在一些实施例中，平台可能具有与其连接的不安全以及安全的音频设备。在这类情况下，监控器知道各设备的状态。当安全设备由音频应用程序以安全模式访问时，在这类情况下，监控器禁用连接到平台的所有不安全音频设备。因此，例如，如果除了诸如声卡之类的安全音频设备之外还有诸如 webcam、MP3 播放器或者任何类型的数字记录器之类的不安全音频设备连接到 USB 总线，则 SVM 可禁用 USB 总线或者总线上的属于不安全音频设备的特定设备。如前所述，这可通过阻挡、空流动(null streaming)或掩蔽或者通过模拟断开连接事件来进行。

可对以上所述实施例进行许多变更。一种更简单的方案，其中不要求全虚拟化的原始监控器(monitor)和分区方案足以实现安全音频应用程序与其它音频应用程序的分隔的类型。分区可通过操作系统或诸如 BIOS 之类的其它系统或者作为监控器进行操作的其它低级固件或软件来实现。因此，一般来说，在一些实施例中，安全音频应用程序可能只是在不同的分区中执行，而没有专用于它的独立虚拟机。提供对音频 I/O 设备的访问的许多方法是本领域已知的。许多不同类型的设备驱动器以及驱动器的接口可用于安全和不安全分区中所使用的两种音频模型。这两种模型可能相同或者可能不相同。此外，禁用和启

用不安全分区中的音频访问的机制可能有所不同。诸如提供空数据流、阻挡和模拟热拔之类的机制只是解释性的，而许多其它实施例也是可行的。禁用和启用的控制可驻留在监控器中或者驻留在安全分区或 VM 中或者驻留在它们两者中。在其它实施例中，可能存在由安全分区独占访问的其它设备，而在另外的实施例中则不存在。

为了便于说明，以上描述中阐述了大量具体细节，以便透彻地理解所述实施例，但是，本领域的技术人员会理解，即使没有这些具体细节也可实施其它许多实施例。

以上详细说明了某些部分根据对基于处理器的系统中的数据位的操作的算法和符号表示来提供。这些算法描述和表示是本领域的技术人员用来向本领域的其它技术人员最有效地传达其工作主旨的方式。操作是要求物理量的物理处理的那些操作。这些数量可采取能够被存储、传递、组合、比较以及以其它方式处理的电、磁或其它物理信号的形式。主要为了一般使用的原因，将这些信号称作位、值、元素、符号、字符、项、编号等，已经证明有时非常便利。

但是应当记住，所有这些及类似的项均与适当的物理量相关联，并且只是应用于这些量上的便捷标签。除非明确说明，否则从描述中清楚地知道，诸如“执行”或“处理”或“计算”或者“确定”等术语可表示基于处理器的系统或类似电子计算设备的动作和过程，其中所述基于处理器的系统或类似电子计算设备处理表示为基于处理器的系统的存储设备或者其它这种信息存储、传送或显示设备中的物理量的数据，并将其转换为以类似方式表示的的其它数据。

在实施例的描述中，参照了附图。附图中，相同的标号在若干视图中描述基本上相同的组件。可采用其它实施例，并且可进行结构、逻辑和电气变更。此外，要理解，各种实施例虽然有所不同，但不一定相互排斥。例如，在一个实施例中描述的特定功能、结构或特性可包含在其它实施例中。

此外，在处理器中实现的一个实施例的设计可能经过从创建到模

拟直到制造的各种阶段。表示设计的数据可通过多种方式来表示设计。首先，如在模拟中可用的那样，硬件可采用硬件描述语言或者其它功能描述语言来表示。另外，采用逻辑和/或晶体管门电路(gate)的电路级模型可在设计过程的某些阶段产生。此外，在某个阶段，大部分设计达到表示硬件模型中的各种设备的物理设置的数据级。在采用传统半导体制造技术的情况下，表示硬件模型的数据可能是指定用于生产集成电路的掩模的不同掩模层上的各种特征存在或不存在的数据库。在设计中的任何表示中，数据可存储在任何形式的机器可读介质中。经调制或者以其它方式产生以便传送这种信息的光或电波、存储器或者磁或光存储设备、如磁盘或光盘可能是机器可读介质。这些介质的任一种可“携带”或“表明”设计或软件信息。在传送表明或者携带代码或设计的电载波以便执行电信号的复制、缓冲或重传时，制作新的副本。因此，通信提供商或网络提供商可制作构成或表示实施例的产品(载波)的副本。

实施例可作为程序产品来提供，它可包括其中存储了数据的机器可读介质，这些数据在由机器访问时可使机器执行根据所要求的主题的过程。机器可读介质可包括但不限于软盘、光盘、DVD-ROM 盘、DVD-RAM 盘、DVD-RW 盘、DVD+RW 盘、CD-R 盘、CD-RW 盘、CD-ROM 盘以及磁光盘、ROM、RAM、EPROM、EEPROM、磁卡或光卡、闪速存储器或者适合于存储电子指令的其它类型的媒体/机器可读介质。此外，实施例还可作为程序产品下载，其中程序可通过载波或其它传播介质中包含的数据信号、经由通信链路(例如调制解调器或网络连接)从远程数据源传送到请求设备。

以最基本的形式对许多方法进行了描述，但可以在不背离要求其权益的主题的基本范围的前提下对方法的任何一个添加或删除步骤，或者对所述消息的任何一个添加或减少信息。本领域的技术人员非常清楚，可进行其它许多修改和改变。具体实施例不是用于限制所要求的主题，而是用于对它进行说明。所要求的主题的范围不是由以上提

---

供的具体实例来确定，而是仅由以下权利要求书来确定。

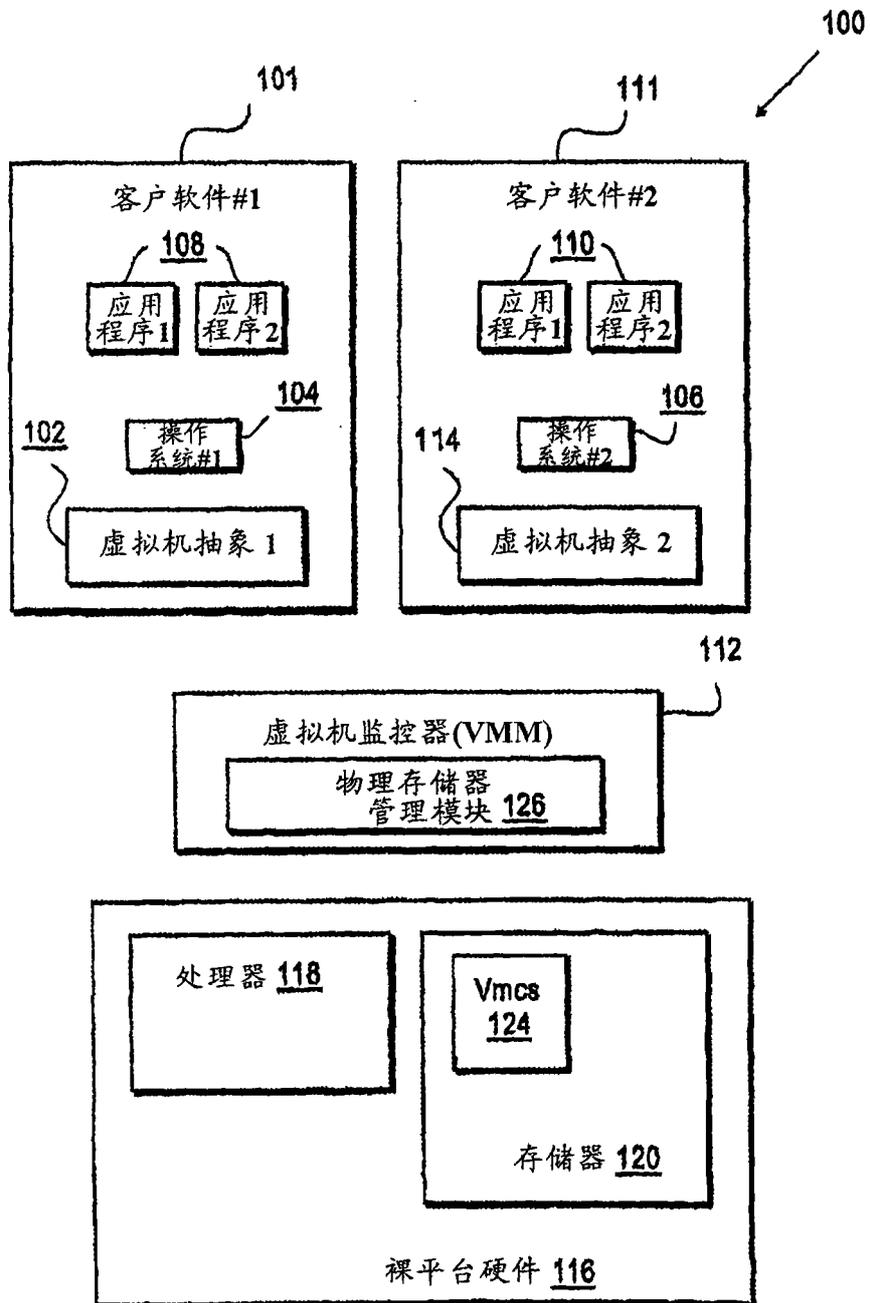


图 1

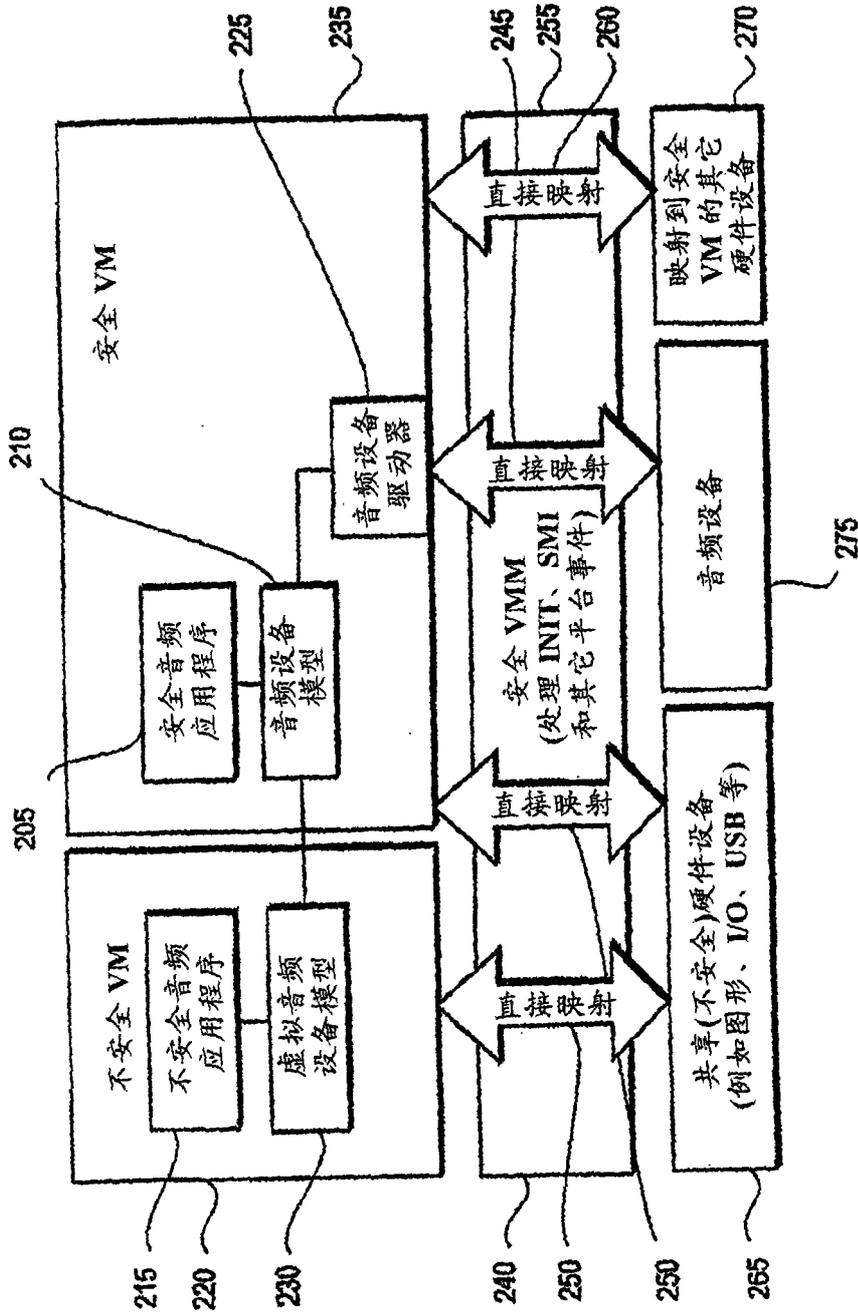


图 2

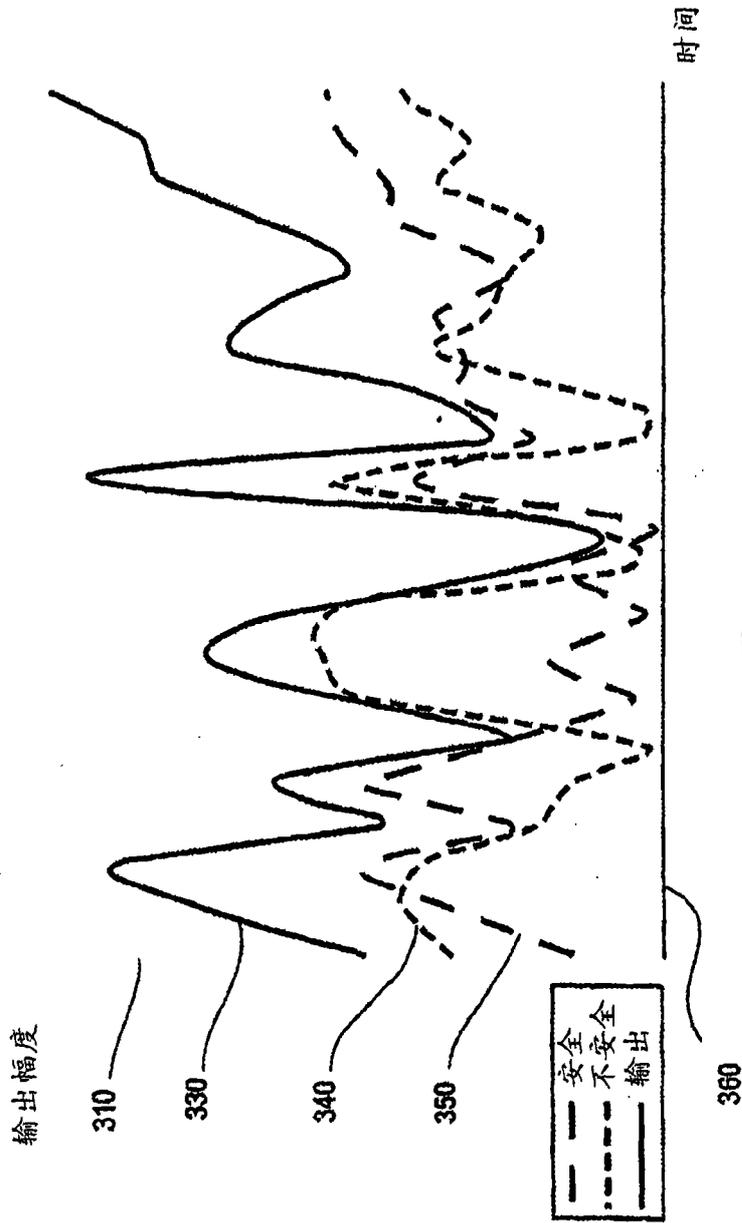


图 3

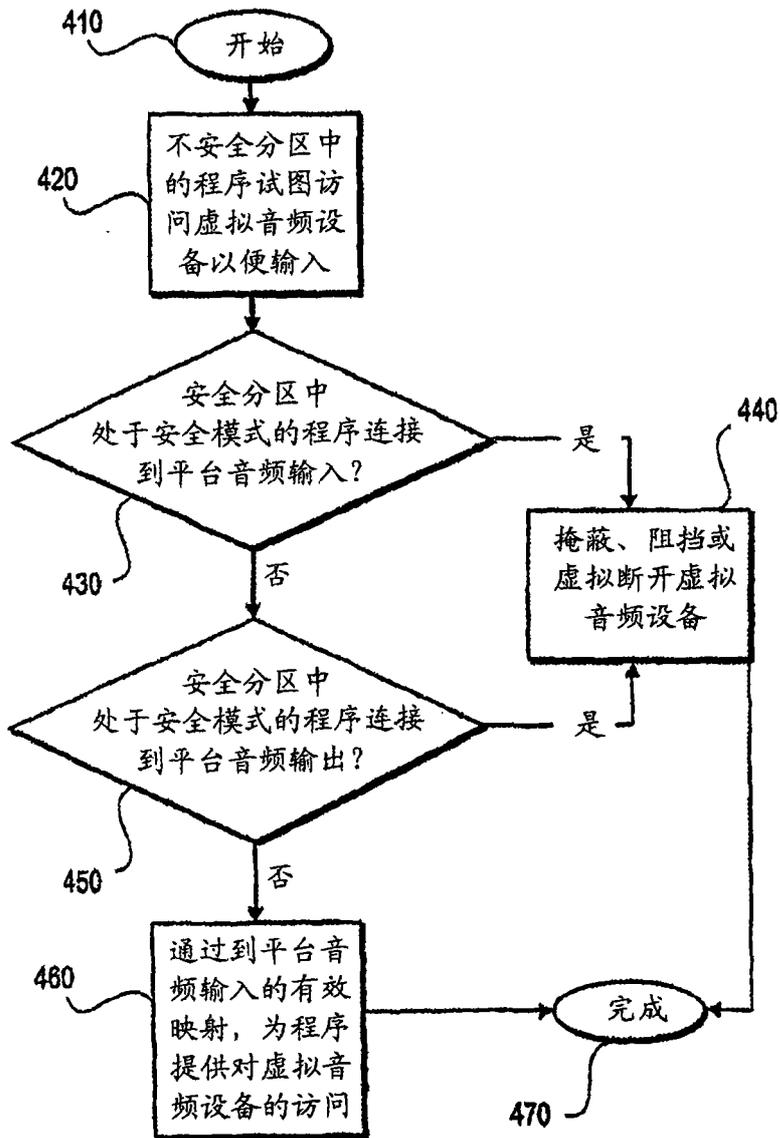


图 4