(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2007 年1 月25 日 (25.01.2007)

PCT

(10) 国际公布号
WO 2007/009328 A1

(51) 国际专利分类号:
G06F 12/00 (2006.01)

(21) 国际申请号: PCT/CN2006/000497

(22) 国际申请日: 2006 年3 月24 日 (24.03.2006)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200510084208.7
2005 年7 月15 日 (15.07.2005) CN

(71) 申请人 (对除美国外的所有指定国): 联想 (北京) 有限公司(LENOVO (BEIJING) LIMITED) [CN/CN]; 中国北京市海淀区上地信息产业基地创业路6号, Beijing 100085 (CN)。

(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): 王晓丁(WANG, Wanding) [CN/CN]; 中国北京市海淀区上地信息产业基地创业路6号, Beijing 100085 (CN)。

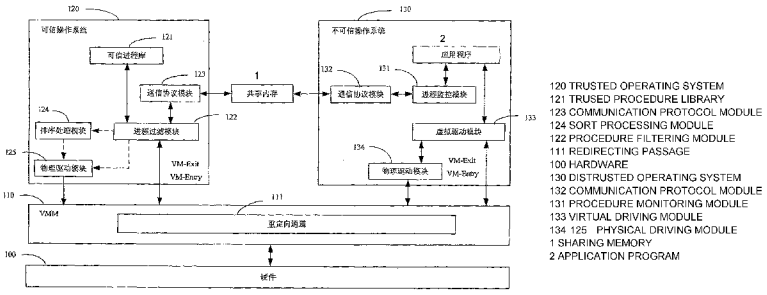
(74) 代理人: 中科专利商标代理有限责任公司(CHINA SCIENCE PATENT & TRADEMARK AGENT LTD.); 中国北京市海淀区王庄路1号清华同方科技大厦B座15层, Beijing 100083 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH,

[见续页]

(54) Title: A VIRTUAL MACHINE SYSTEM SUPPORTING TRUSTED COMPUTING AND A TRUSTED COMPUTING METHOD IMPLEMENTED ON IT

(54) 发明名称: 支持可信计算的虚拟机系统及在其上实现可信计算的方法



(57) Abstract: A virtual machine system supporting trusted computing includes a virtual machine monitor, a hardware and multiple operating systems (OSs). Said multiple OSs include at least a trusted OS, and at least a distrusted OS, a redirecting passage sets in the virtual machine monitor, the redirecting passage is adapted to redirecting an I/O instruction from the distrusted OS to the trusted OS. Wherein, the trusted OS checks the trusted degree of a procedure information of the distrusted OS, and sends to the hardware an FO instruction that corresponds to a trusted procedure information confirmed via the trusted degree check , transferred via the redirecting passage and came from the distrusted OS, performs an I/O operation by the hardware.

(57) 摘要:

一种支持可信计算的虚拟机系统具有虚拟机监视器、硬件以及多个操作系统。该多个操作系统中包括至少一个可信操作系统，以及至少一个不可信操作系统，该虚拟机监视器中设置有重定向通道，该重定向通道用于将来自不可信操作系统的 I/O 指令重定向到可信操作系统。其中，可信操作系统对来自不可信操作系统的进程信息进行可信度检查，并将经可信度检查确认为可信进程信息所对应的、经重定向通道传送的来自不可信操作系统的 I/O 指令发送给硬件，由硬件执行 I/O 操作。

WO 2007/009328 A1

GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW。

(84) 指定国（除另有指明，要求每一种可提供的地区保护）：ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告。

所引用双字母代码及其它缩写符号，请参考刊登在每期PCT公报期刊起始的“代码及缩写符号简要说明”。

支持可信计算的虚拟机系统及在其上实现可信计算的方法

技术领域

本发明涉及虚拟计算机系统和可信计算方法，特别是指一种支持可信计算的虚拟机系统和在该支持可信计算的虚拟机系统上实现可信计算的方法。

背景技术

在现有的计算机体系架构中，一般而言，所有类型的操作系统（Operating System, OS）都可以在一台计算机上运行，因此运行在操作系统上的软件进程原则上可以任意访问计算机上的硬件资源，比如：读取内存中的数据、修改硬盘上的数据等。这种完全开放式架构已经带来了大量的信息安全问题，包括众所周知的病毒和网络诈骗。因此，人们开始寻找一些改进的架构和技术，从根本上改善计算机的信息安全性。

一种典型的技术是开发防病毒软件，将其安装到计算机上，用于预防和清除计算机病毒。传统的防病毒软件是根据病毒的技术思路来编写的，能够识别并清除计算机病毒。但是，恶意的计算机使用人员不断根据计算机系统的漏洞编写出新的病毒，同时老的病毒也不断变种，这些新老病毒严重的破坏了计算机的使用。据不完全统计，现有计算机病毒数据库中所记录的病毒已经超过 7 万条，这使得防病毒软件疲于应付，同时也使防病毒软件越来越大，其在运行时使计算机系统资源大大浪费。实际上，人们在使用计算机过程中，可以使用的可信应用程序相对而言是很少的，能够达到 1000 种已经是非常可观了，但是这些少数的可信应用程序却要防范大量计算机病毒，并且这些计算机病毒还在不断增加，这成为计算机使用过程中迫切需要解决的重要问题。

因此，为了从根本上解决计算机安全使用的问题，人们提出了支持可信计算的计算机架构系统。该计算机架构系统的设计思想是：在计算机上运行应用软件之前，首先检查应用软件的可信度，在计算机操作系统确保该应用软件是可信安全的应用软件后，计算机操作系统才接受并在本机上运行该应用软件，否则拒绝该应用软件在本机上运行。

在可信计算组织（Trusted Computing Group, TCG）提出的一种可信计算架构中，要求在主板的 LPC 总线上增加一个可信平台模块（Trusted Platform Module, TPM）芯

片，该芯片用作检查计算机上其他软件模块可信度的基础，其首先检查 BIOS 的完整性是否被改变，然后检查主引导记录（Master Boot Record, MBR）的完整性是否被改变，接着检查操作系统内核（Operating System Kernel）的完整性是否被改变，最后检查上层应用软件的完整性是否改变。这种方法可以保证计算机始终运行在某种可信状态下，但是其在如何判断哪些新进程是可信进程方面没有提供简单可行的方法，并且由于需要修改操作系统的内核，因此无法在不对现有操作系统做大的改变的情况下实现这种可信计算架构。

微软公司的中国专利申请第 200410056423.1 号公开了其下一代操作系统中的 NGSCB（Next Generation Secure Computing Base）可信计算架构，该可信计算架构借助于可信平台模块和主板上的 CPU 和芯片组（Chipsets）隔离计算指令，将进程分为受保护进程和普通进程。对于受保护进程，其将在受保护的内存中运行，这样恶意程序就很难对这些受保护的进程进行破坏。这种架构适合于提高网络应用的安全性，特别是在用户使用 PC 做在线交易的时候。但是这种架构本质上是在同一个操作系统内核中构建可信计算的区域，因此就构架原理来说，操作系统本身的安全漏洞将会影响到可信计算区域的安全性，同时，该架构也需要修改操作系统内核，不容易升级及更新换代，不能适应计算机日新月异的发展，使新的程序往往得不到保护。

为了克服上述问题，人们考虑到采用虚拟机平台技术。

目前典型的虚拟机架构有英特尔的 VT-i 和 VT-x 技术，其中 VT-x 是应用于台式机和 X86 服务器平台上的虚拟化技术，而 VT-i 则是应用于安腾平台上的虚拟化技术。此外，还有 AMD 的 Pacifica 虚拟化技术。

如图 1 所示，在现有已经公开的虚拟机架构中，重点是实现对于硬件资源的虚拟化，从而在一台计算机上可以并行地运行多个操作系统，图上表示为操作系统 1 和操作系统 2，这里只是以两个操作系统为例，其数量不限于两个。由于这些操作系统相互之间不干扰，比如 OS1 能访问的内存是 OS2 所不能访问的，这样，这种架构也同时实现了多个操作系统之间的隔离。

在这种虚拟机架构中，通过在实际的硬件层面上增加一组专门给虚拟机监视器（Virtual Machine Monitor，VMM）使用的指令、虚拟计算资源、存储资源以及 I/O 资源，使得用户操作系统（Guest OS）不需要任何修改就可以运行在虚拟机架构上，这就提供了一个非常广的创新应用范围。其中，常用的用户操作系统可以包括

Windows98、Windows2000、WindowsXP、Linux、Unix、Mac 等。

然而，图 1 所示的虚拟机架构并未实现在某个用户操作系统中的进程访问硬件资源时对该进程的可信度检查，因此，恶意进程可以直接通过 I/O 指令访问硬件资源，甚至破坏硬件资源，例如，清楚硬盘上的数据等。

并且，从计算机芯片技术的发展趋势来看，不管是 Intel、AMD，还是其他芯片供应商，都把虚拟化当作未来计算机发展的重要趋势，也就是说，在这种趋势下，以后市场上出售的计算机几乎都会支持虚拟机架构。如何实现虚拟机平台技术架构上的可信计算成了业界研究的一个热点。

发明内容

本发明的目的之一在于提供一种支持可信计算的虚拟机系统，其能从根本上提升使用计算机的信息安全性，并且不增加额外的硬件成本。

本发明的另一目的在于提供一种实现可信计算的方法，其能从根本上提升使用计算机的信息安全性。

根据本发明的第一方面，提供一种支持可信计算的虚拟机系统，其具有虚拟机监视器、硬件以及多个操作系统。该多个操作系统中包括至少一可信操作系统、以及至少一不可信操作系统，该虚拟机监视器中设置有重定向通道，该重定向通道用于将来自不可信操作系统的 I/O 指令重定向到可信操作系统。其中，可信操作系统对来自不可信操作系统的进程信息进行可信度检查，并将经可信度检查确认为可信进程信息所对应的、经重定向通道传送的来自不可信操作系统的 I/O 指令发送给硬件，由硬件执行 I/O 操作。

根据本发明的第二方面，提供一种实现可信计算的方法，其包括如下步骤：

步骤一，不可信操作系统发出 I/O 指令和进程信息；

步骤二，虚拟机监视器截获该 I/O 指令，通过重定向通道将 I/O 指令重定向到可信操作系统；

步骤三，可信操作系统对接收到的进程信息进行可信度检查，并将经可信度检查确认为可信进程信息所对应的 I/O 指令发送给硬件，由硬件执行 I/O 操作。

与现有技术相比，本发明的有益效果是：由于本发明提供利用进程过滤模块和可信进程库对来自不可信操作系统的进程信息进行可信度检查，可以避免恶意进程访问

硬件资源，破坏硬件资源。并且，本发明在现有的硬件基础上即可实现，因此不需要花费额外的硬件成本，简单易行。

附图说明

图 1 为现有技术虚拟机架构的结构示意图；

图 2 为本发明支持可信计算的虚拟机系统的结构示意图；

图 3 为在图 2 所示的虚拟机系统上实现进程信息可信度检查以及执行 I/O 操作的流程图；

图 4 为图 2 中所示的共享内存的信息存储区域设计的示意图。

具体实施方式

下面结合附图详细描述本发明的支持可信计算的虚拟机系统和在该支持可信计算的虚拟机系统上实现可信计算的方法。

第 1 实施例

图 2 为本发明第 1 实施例支持可信计算的虚拟机系统的结构框图。其中，该支持可信计算的虚拟机系统包括硬件 100、虚拟机监视器 110 以及其上运行的多个操作系统。为了方便描述，这里仅仅以两个操作系统为例进行说明。在这两个操作系统中，一个操作系统为可信操作系统 120，另一个操作系统为不可信操作系统 130。不可信操作系统 130 为用户所控制，运行用户所需要执行的应用程序，可信操作系统 120 在该虚拟机系统的后台运行。在这个虚拟机系统中，始终具有可信操作系统 120，可以为一个，也可以为多个。对于不可信操作系统 130，其数量可以根据用户的需要而安装在这个虚拟机系统中。

硬件 100 为现有计算机系统的硬件，其具有处理器、内存、I/O 设备、PCI 设备以及其他设备。

虚拟机监视器 110 运行在上层的操作系统与底层的硬件之间，对所有的硬件系统资源的操作请求（如，I/O 指令等）进行监视，同时将所有对硬件资源的操作请求重定向到可信操作系统 120 中。虚拟机监视器 110 包括虚拟处理器、虚拟内存、虚拟 I/O 设备、虚拟 PCI 设备、以及其他虚拟设备。该虚拟机监视器 110 与现有的虚拟机监视器相比，增加了重定向通道 111，该重定向通道 111 可以将来自不可信操作系统 130

的 I/O 指令重定向到可信操作系统 120。

可信操作系统 120 中包括：可信进程库 121、进程过滤模块 122、通信协议模块 123、虚拟驱动模块 124 以及物理驱动模块 125。该可信进程库 121 中存储有现有的可信应用程序的进程信息，该进程信息用于判断来自不可信操作系统 130 的进程信息是否为可信进程信息。

该不可信操作系统 130 包括进程监控模块 131、通信协议模块 132、虚拟驱动模块 133 以及物理驱动模块 134。该不可信操作系统 130 上所运行的应用程序为新的未经过可信度检查的应用程序，这里将其假定为不可信程序。

以上的通信协议模块 124 和 132 所采用的通信协议可以是 TCP/IP 协议，因为在安装系统的时候，可以给可信操作系统和不可信操作系统分配独立的 IP 地址。

以上的通信协议模块 124 和 132 所采用的通信协议也可以是一种简化的通信协议。在这个简化的通信协议中，各个不可信操作系统之间以数字序号作为标记进行区分，虚拟机监视器 110 事先会在内存中为操作系统之间的通信划分出如图 4 所示的共享内存，该共享内存中设置有与各个不可信操作系统（用户操作系统）对应的内容，即用户操作系统编号、操作系统名称、操作系统类型、发送数据以及返回数据等信息。然后不同的操作系统的通信协议模块之间通过定期查询的机制去该共享内存区域中读取对方发送过来的信息。

具体而言，当不可信操作系统需要给可信操作系统传递参数或者数据时，通信协议模块将这些参数或者数据存储到“发送数据”区域中，可信操作系统中的通信模块定期检查该“发送数据”区域中是否有新的发送数据，进而读取该发送数据。当可信操作系统的进程过滤模块需要将可信度检查结果反馈给不可信操作系统时，其通信协议模块将该结果存储在“返回数据”区域，同样的，不可信操作系统的通信协议模块也会定期检查该“返回数据”区域中是否有新的返回数据，进而读取该返回数据。

在本发明的虚拟机系统中，当不可信操作系统 130 执行应用程序时，由于假定这些应用程序为不可信程序，其进程也为不可信进程。为了保证虚拟机系统不受到恶意进程的破坏，因此，在不可信进程通过 I/O 指令访问硬件 100 之前，需要利用可信操作系统 120 对来自不可信操作系统 130 的进程信息进行可信度检查。只有在该进程信息经可信操作系统 120 确认为是可信的进程信息时，硬件 100 才执行与该确认为可信进程的不可信进程对应的 I/O 指令，完成 I/O 操作。从而，可以防止恶意进程破坏硬

件 100。

在现有的虚拟机系统中，虚拟机监视器的处理器具有两组计算指令：一组是 Root 指令，包含有 VM-Entry 指令，虚拟机监视器使用该 VM-Entry 指令来将控制权将给指定操作系统；另一组是 Non-Root 指令，包含有 VM-Exit 指令，操作系统使用该 VM-Exit 指令来将控制权交回给虚拟机监视器。同时，虚拟机系统也为每个操作系统定义了对应的虚拟机控制（Virtual-Machine Control Structure，VMCS）数据结构，VMCS 用于保存和恢复该操作系统的状态。虚拟机监视器为每个 VMCS 在内存中分配空间，并且通知处理器当前需要处理的 VMCS 的起始地址。当虚拟机监视器 110 需要把控制权交给某个操作系统时，其调用 VM-Entry 指令（该指令中包含有与该操作系统的 VMCS 对应的信息），处理器就会从该操作系统对应的 VMCS 中恢复该操作系统的状态；当该操作系统需要访问硬件资源时，就由其中的虚拟驱动模块调用 VM-Exit 指令，处理器就会把该操作系统的状态保存在 VMCS 中，同时虚拟驱动模块将控制权交还给虚拟机监视器。

为了便于进一步理解本发明第 1 实施例的支持可信计算的虚拟机系统，请一并参考图 2 和图 3，其中，图 3 为该虚拟机系统中执行的 I/O 操作可信度检查的流程图。

首先，在不可信操作系统 130 中，当应用程序进程开始执行的时候，一方面，应用程序进程发出硬件访问请求，此时，虚拟驱动模块 133 在收到该硬件访问请求后将硬件访问请求传递给物理驱动模块 134，然后，物理驱动模块 134 将该硬件访问请求转换为 I/O 指令发送给虚拟机监视器 110。同时，虚拟驱动模块 133 调用 VM-Exit 指令，从而将控制权交给虚拟机监视器 110，处理器将该不可信操作系统 130 的状态保存在该不可信操作系统 130 所对应的 VMCS 中。

另一方面，进程监控模块 131 截获应用程序进程的进程信息，通过通信协议模块 132 将该进程信息传送到共享内存（未标示）。如图 4 所示，该共享内存中设置有与不可信操作系统 130 对应的内容，即用户操作系统编号、操作系统名称、操作系统类型、发送数据以及返回数据等信息。该进程信息存储在共享内存中与不可信操作系统对应的“发送数据”区域中。

其次，在虚拟机监视器 110 中，当虚拟机监视器 110 截获到该 I/O 指令后，其通过调用 VM-Entry 指令将控制权交给可信操作系统 120，从而从 VMCS 中恢复可信操作系统 120 的状态。并且，该虚拟机监视器 110 通过重定向通道 111，将该 I/O 指令

发送给可信操作系统 120 的进程控制模块 122。然后，进程过滤模块 122 从该 I/O 指令中提取出进程导引（Guid），根据该进程导引通过通信协议模块 123 从共享内存中的“发送数据”区域获得不可信操作系统 130 所存储的进程信息。

接下来，进程过滤模块 122 根据存储在可信进程库 121 中的可信应用程序进程信息，判断该进程信息是否为可信进程信息。

（1）如果该进程信息为可信进程信息，则，进程过滤模块 122 将 I/O 指令发送到物理驱动模块 125，物理驱动模块 125 通过虚拟机监视器 110 将该 I/O 指令传送给硬件 100，由硬件 100 执行 I/O 操作。在存在多个不可信操作系统时，当来自各个不可信操作系统的 I/O 指令都需要执行时，该可信操作系统 120 需要增加一个排序机制，例如图 2 中的排序处理模块 124，来对各个 I/O 指令进行排序处理，然后依次发送给物理驱动模块 125。当然，在只有一个不可信操作系统时，也可以通过该排序处理模块 124 发送给物理驱动模块 125。

最后，由硬件 100 依次执行这些 I/O 指令。

（2）如果该进程信息被判断为不可信的进程信息，则，进程过滤模块 122 将该进程信息被判断为不可信进程信息的信息通过通信协议模块 123 存储到共享内存中与不可信操作系统 130 所对应的“返回数据”区域。然后，不可信操作系统 130 通过通信协议模块 132 获得存储在共享内存的“返回数据”区域中的信息，进而取消该 I/O 操作。

第 2 实施例

以上介绍的是在一台虚拟机系统上实现可信操作系统 120 对来自不可信操作系统 130 的进程信息进行可信度检查和执行 I/O 操作的情况，由于通用的计算机通常具备和 LAN 或者 WAN 进行通信的接口，本发明的虚拟机系统也可以实现对来自内部或者外部网络的不可信操作系统的进程信息的可信度检查，以及在确认该进程信息为可信进程信息后执行 I/O 操作。

也就是说，本发明的虚拟机系统可以作为一个网络计算机系统，包括本机和网络计算机。其中，本机为图 2 所示的虚拟机结构，其上可以根据本机用户的需要安装不可信操作系统，也可以不安装不可信操作系统。网络计算机对于本机来说为不可信的计算机，其所安装的操作系统为不可信操作系统，这些不可信操作系统的相关信息同本机上的不可信操作系统一样，可以存储在虚拟机监视器所划分的共享内存中。该不

可信操作系统与可信操作系统以及虚拟机监视器之间的通信（包括进程信息的发送接收、I/O 指令的发送、以及 VM-Entry 和 VM-Exit 指令的传送）可以通过现有的通信协议，例如 TCP/IP 协议，来实现。对于本领域的普通技术人员而言，在本发明第 1 实施例的基础上很容易实现上述的架构。

本发明可以应用在商用和消费计算机上，从根本上提升计算机的抗攻击能力。例如：当本发明的技术方案应用于网吧安全管理时，一方面可以杜绝木马程序对网吧电脑上的硬盘保护功能的破解，另一方面可以杜绝木马程序对用户的游戏帐号和密码的盗用，极大地减少用户的经济损失。当本发明的技术方案应用于消费计算机时，可以由生产厂家在互联网上维护一个进程验证服务器，由客服人员不断地去更新完善可信进程库，从而帮助广大消费用户抵御黑客和病毒的攻击。

在未来的多网融合的时代，智能手机这类移动设备、数字电视机这类家电设备会变得很普及，用户会越来越多地通过手机或者是数字电视机进行网上交易等关键应用，从而给用户带来更多的信息安全风险，因此通过应用本发明的技术方案，能从根本上保护用户的关键应用不被不可信的病毒、木马破坏。

上述具体实施方式仅为详细说明本发明的技术方案，并不是对本发明的限制，本领域的技术人员在不脱离本发明技术方案的主旨的情况下所作的变化者在本发明的保护范围内。

权 利 要 求

1. 一种支持可信计算的虚拟机系统，具有虚拟机监视器（110）、硬件（100）以及多个操作系统，其特征在于：

该多个操作系统中包括至少一可信操作系统（120）、以及至少一不可信操作系统（130）；以及

该虚拟机监视器（110）中设置有重定向通道（111），该重定向通道（111）用于将来自不可信操作系统（130）的 I/O 指令重定向到可信操作系统（120），

其中，可信操作系统（120）对来自不可信操作系统（130）的进程信息进行可信度检查，并将经可信度检查确认为可信进程信息所对应的、经重定向通道（111）传送的来自不可信操作系统（130）的 I/O 指令发送给硬件（100），由硬件（100）执行 I/O 操作。

2. 如权利要求 1 所述的虚拟机系统，其特征在于：

不可信操作系统（130）包括进程监控模块（131）、通信协议模块（132）、虚拟驱动模块（133）和物理驱动模块（134），其中，

进程监控模块（131），用于在不可信操作系统（130）运行应用程序时，截获应用程序的进程信息，并将其通过通信协议模块（132）发送给可信操作系统（120）；

虚拟驱动模块（133），用于获取来自应用程序的硬件访问请求，并通过物理驱动模块（134）将该请求转换为 I/O 指令发送给虚拟机监视器（110），

以及，

该可信操作系统（120）包括可信进程库（121）、进程过滤模块（122）、通信协议模块（123）和物理驱动模块（125），其中，

过程过滤模块（122），用于根据可信进程库（121）中存储的可信进程判断通信协议模块（123）接收的进程信息是否为可信进程，

当该进程信息为可信进程时，通过物理驱动模块（125）将 I/O 指令发送给硬件（100），由硬件（100）执行 I/O 操作，

当该进程信息为不可信进程时，通过通信协议模块（123）将该进程信息为不可信进程的信息发送给不可信操作系统（130），由不可信操作系统（130）取消该 I/O 指

令。

3. 如权利要求 1 或者 2 所述的虚拟机系统，其特征在于，该可信操作系统（120）进一步包括排序处理模块（124），在来自一个或者多个不可信操作系统的 I/O 指令被执行之前，该排序处理模块（124）用于对 I/O 指令进行排序。

4. 如权利要求 3 所述的虚拟机系统，其特征在于，该不可信操作系统（130）为网络计算机上的操作系统，其与可信操作系统（120）之间通过 TCP/IP 协议进行通信。

5. 如权利要求 3 所述的虚拟机系统，其特征在于，不可信操作系统（130）和可信操作系统（120）之间通过设置共享内存进行通信。

6. 一种在权利要求 1 所述的虚拟机系统上实现可信计算的方法，包括如下步骤：

步骤一，不可信操作系统（130）发出 I/O 指令和进程信息；

步骤二，虚拟机监视器（110）截获该 I/O 指令，通过重定向通道（111）将 I/O 指令重定向到可信操作系统（120）；

步骤三，可信操作系统（120）对接收到的进程信息进行可信度检查，并将经可信度检查确认为可信进程信息所对应的 I/O 指令发送给硬件（100），由硬件（100）执行 I/O 操作。

7. 如权利要求 6 所述的方法，其特征在于进一步包括：

步骤四，当该进程信息为不可信进程时，将该进程信息为不可信进程的信息发送给不可信操作系统（130），由不可信操作系统（130）取消该 I/O 指令。

8. 如权利要求 7 所述的方法，其特征在于：

步骤一中包括：

进程监控步骤，在不可信操作系统（130）运行应用程序时，截获应用程序的进程信息，并将其发送给可信操作系统（120）；以及

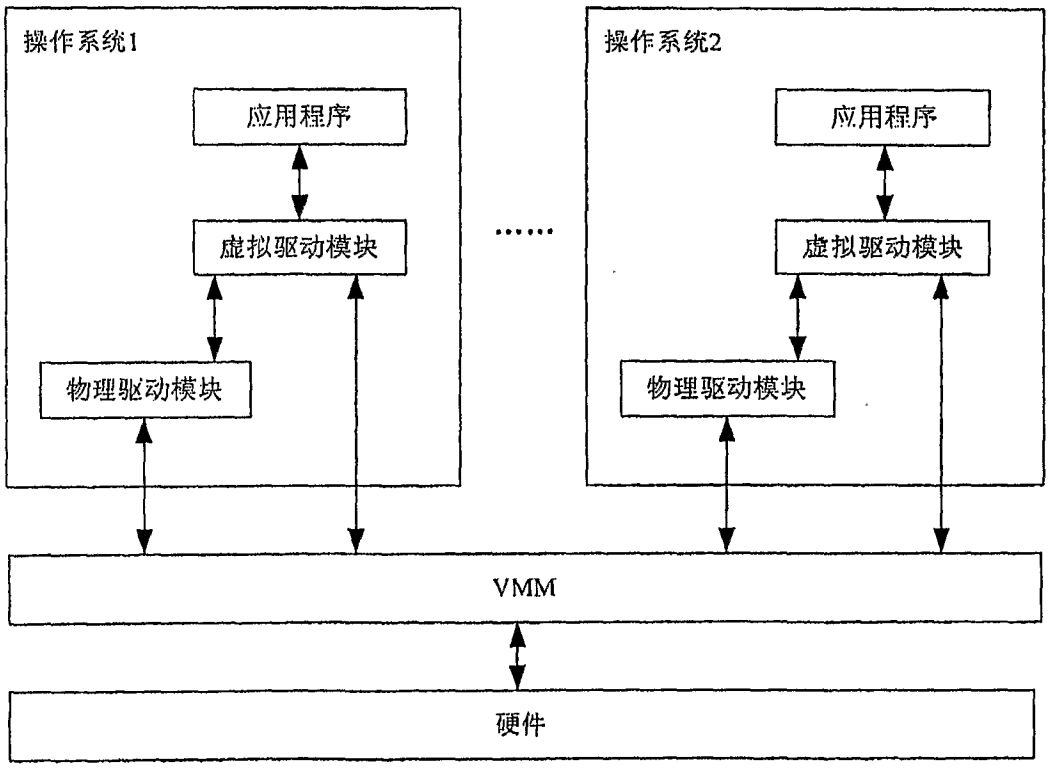
硬件访问请求获取步骤，用于获取来自应用程序的硬件访问请求，并将该硬件访问请求转换为 I/O 指令发送给虚拟机监视器（110）。

9. 如权利要求 6－8 中任何一项所述的方法，其特征在于，

步骤三中进一步包括排序处理步骤，在来自一个或者多个不可信操作系统的 I/O 指令被执行之前，对 I/O 指令进行排序。

10. 如权利要求 9 所述的方法，其特征在于，该不可信操作系统（130）与可信操作系统（120）之间通过 TCP/IP 协议或者共享内存的方式进行通信。

图 1



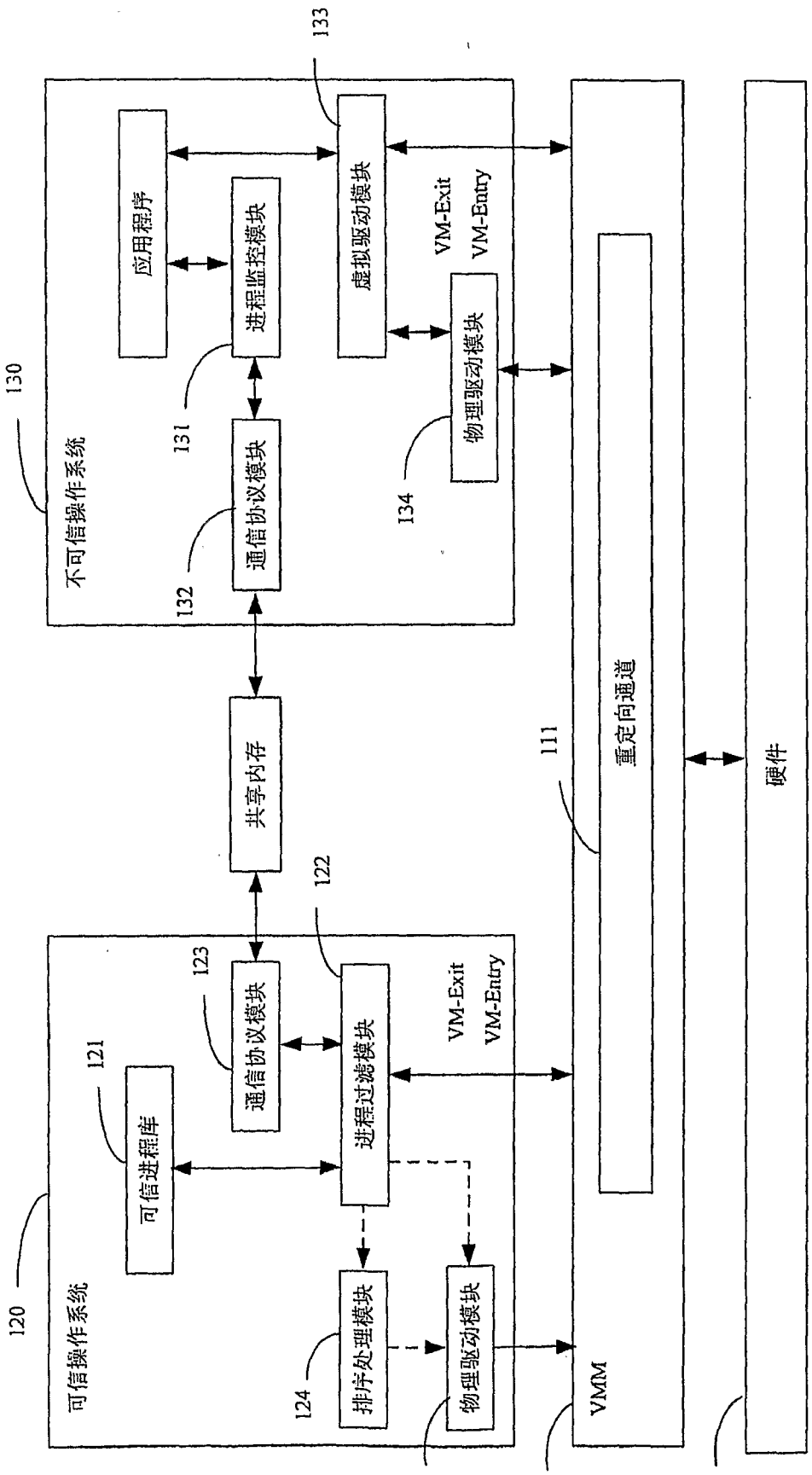

130
不可信操作系统
应用程序
进程监控模块
131
通信协议模块
132
133
虚拟驱动模块
VM-Exit
VM-Entry
物理驱动模块
134
共享内存
120
可信操作系统
可信进程库
121
通信协议模块
123
进程过滤模块
122
VM-Exit
VM-Entry
排序处理模块
124
物理驱动模块
111
重定向通道
VMM
硬件

图 2

图 3

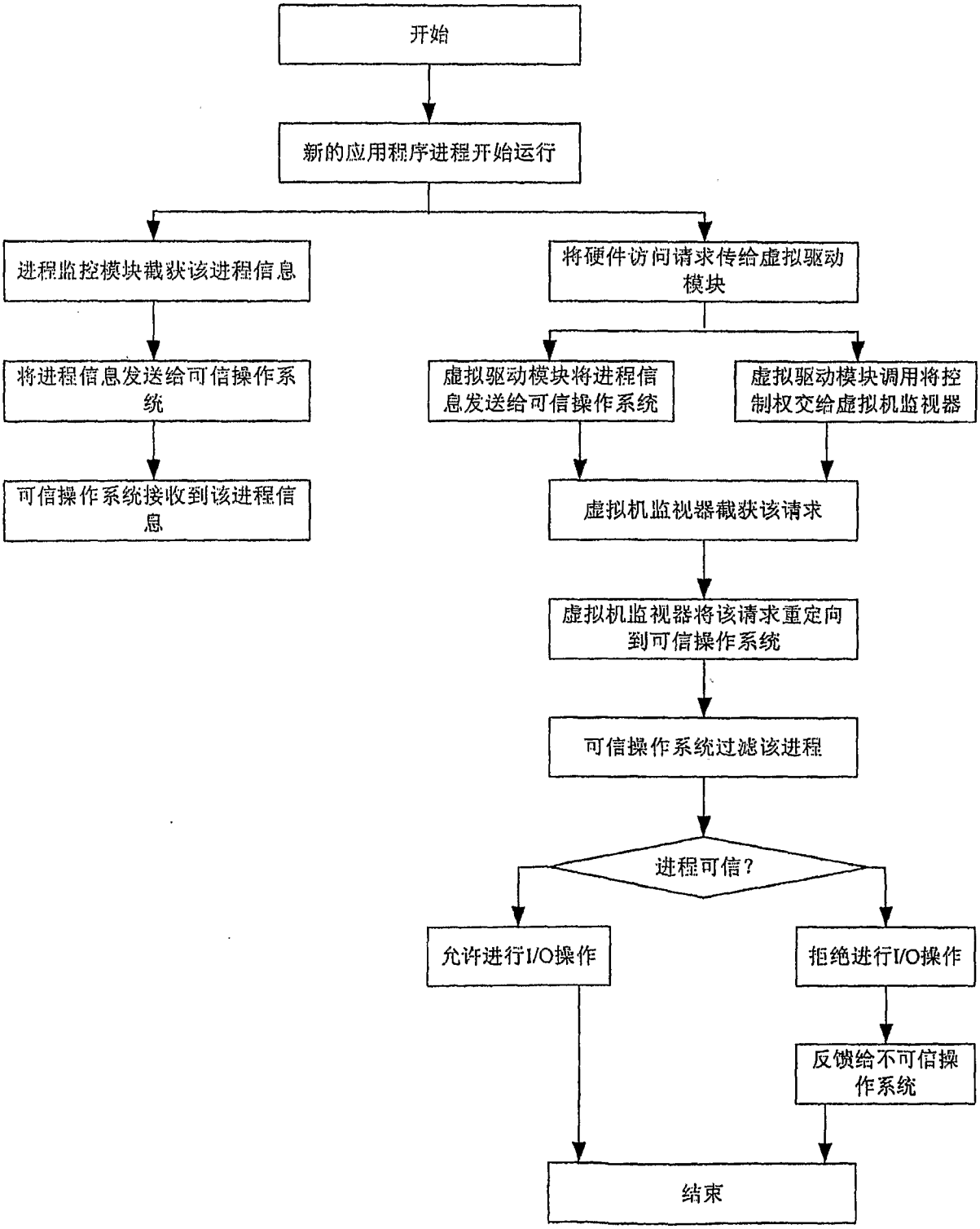
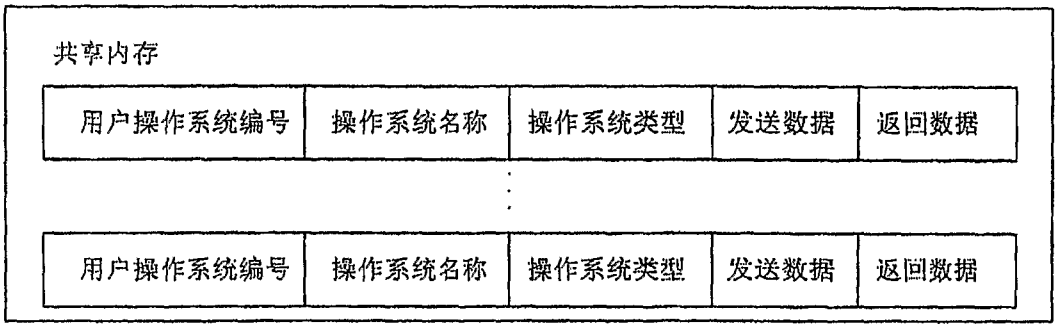

开始
新的应用程序进程开始运行
进程监控模块截获该进程信息
将进程信息发送给可信操作系统
可信操作系统接收到该进程信息
将硬件访问请求传给虚拟驱动模块
虚拟驱动模块将进程信息发送给可信操作系统
虚拟驱动模块调用将控制权交给虚拟机监视器
虚拟机监视器截获该请求
虚拟机监视器将该请求重定向到可信操作系统
可信操作系统过滤该进程
进程可信?
允许进行I/O操作
拒绝进行I/O操作
反馈给不可信操作系统
结束

图 4


共享内存
用户操作系统编号
操作系统名称
操作系统类型
发送数据
返回数据
用户操作系统编号
操作系统名称
操作系统类型
发送数据
返回数据

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2006/000497

A. CLASSIFICATION OF SUBJECT MATTER

G06F 12/00（2006.01）i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F12 （2006.01）i
G06F9 （2006.01）i
G06F11（2006.01）i

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPODOC WPI CNPAT PAJ CNKI
virtual trust+ untrust+ OS perating w system program application procedure proceeding programme

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO03104981A2（INTEL CORPOATION）18.Dec 2003（18.12.2003）page 4 line 2 to page14 line	1，6-8
A		2-5，9，10
A	US20020194496A1（Jonathan Griffin et al）19.Dec 2002（19.12.2002）the whole document	1-10
A	GB2382419A （Hewlett-packard Company）28.May 2003（28.05.2003）the whole document	1-10

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13.Jun 2006（13.06.2006）	19 OCT 2006 (19.10.2006)
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer Li Qiong Telephone No. 86-10-62084932

Form PCT/ISA /210 (second sheet) (April 2005)

更正页

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2006/000497

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
WO03104981A2	18.Dec 2003 (18.12.2003)	US2003229794A	11.Dec 2003 (11.12.2003)
		AU2003231237A	22.Dec 2003 (22.12.2003)
		EP1512074A	09.Mar 2005 (09.03.2005)
		RU2004139086A	10.Jul 2005 (10.07.2005)
		CN1675623A	28.Sep 2005 (28.09.2005)
		JP2005529401T	29.Sep 2005 (29.09.2005)
		US2006015869A	19.Jan 2006 (19.01.2006)
US20020194496A1	19.Dec 2002 (19.12.2002)	GB2376764B	29.Dec 2004 (29.12.2004)
		EP1271282A	02.Jan 2003 (02.01.2003)
GB2382419A	28.May 2003 (28.05.2003)	DE10254621A	12.Jun 2003 (12.06.2003)
		US2003226031A	04.Dec 2003 (04.12.2004)
		US2005223221A	06.Oct 2005 (06.10.2005)

国际检索报告

国际申请号
PCT/CN2006/000497

A. 主题的分类

G06F 12/00（2006.01）i

按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F12（2006.01）i

G06F9（2006.01）i

G06F11（2006.01）i

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

WPI EPODOC CNPAT PAJ CNKI

虚拟　可信　操作系统　进程　过程

C. 相关文件

类　型*	引用文件，必要时，指明相关段落	相关的权利要求
X	WO03104981A2（英特尔公司）18.12 月 2003（18.12.2003）第 4 页第 2 行至第 14 页第 32 行	1，6-8
A		2-5，9，10
A	US20020194496A1（Jonathan Griffin 等）19.12 月 2002（19.12.2002）全文	1-10
A	GB2382419A （Hewlett-packard Company）28.5 月 2003（28.05.2003）全文	1-10

☐ 其余文件在 C 栏的续页中列出。　　☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
13.6 月 2006（13.06.2006）	19 OCT 2006
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号：　(86-10)62019451	受权官员 李琼 电话号码：(86-10)62084932

PCT/ISA/210 表(第 2 页) (2005 年 4 月)

更正页

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2006/000497

检索报告中引用的专利文件	公布日期	同族专利	公布日期
WO03104981A2	18.12 月 2003（18.12.2003）	US2003229794A	11.12 月 2003（11.12.2003）
		AU2003231237A	22.12 月 2003（22.12.2003）
		EP1512074A	09.3 月 2005（09.03.2005）
		RU2004139086A	10.7 月 2005（10.07.2005）
		CN1675623A	28.9 月 2005（28.09.2005）
		JP2005529401T	29.9 月 2005（29.09.2005）
		US2006015869A	19.1 月 2006（19.01.2006）
US20020194496A1	19.12 月 2002（19.12.2002）	GB2376764B	29.12 月 2004（29.12.2004）
		EP1271282A	02.1 月 2003（02.01.2003）
GB2382419A	28.5 月 2003（28.05.2003）	DE10254621A	12.6 月 2003（12.06.2003）
		US2003226031A	04.12 月 2003（04.12.2004）
		US2005223221A	06.10 月 2005（06.10.2005）