(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 102184373 A
(43)申请公布日 2011.09.14

(21)申请号 201110140909.3

(22)申请日 2011.05.30

(71)申请人 南京大学
地址 210093 江苏省南京市汉口路 22 号

(72)发明人 黄皓 钱振江

(74)专利代理机构 南京君陶专利商标代理有限公司 32215
代理人 沈根水

(51)Int.Cl.
G06F 21/22(2006.01)

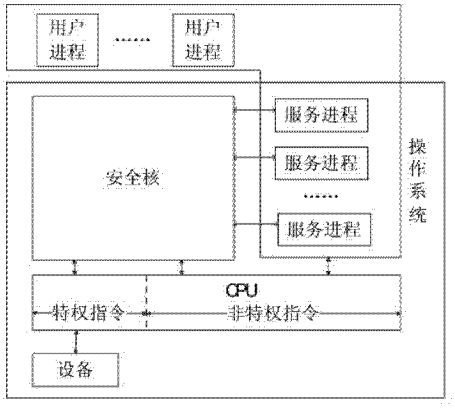
权利要求书 1 页 说明书 3 页 附图 1 页

(54)发明名称

基于保护模式与虚拟化机制实现操作系统安全核设计方法

(57)摘要

本发明是基于保护模式与虚拟化机制实现操作系统安全核设计方法，包括如下步骤：一、CPU保护模式提供了特权级0可以执行处理器的所有指令；非特权级1-N，只能执行处理器的部分指令；将操作系统划分成一个工作在特权级的安全核与工作在非特权级的若干个服务进程；二、安全核利用CPU保护模式，除安全核之外的进程只能做两件事：操纵自己的内存空间和向安全核发送消息。三、指定一个外存储区域存放安全核长久性数据，利用硬件虚拟化机制，保证只有安全核能访问这个区域，保障安全核的数据与代码的安全性。优点：安全核的数据与代码不会受到其它进程的破坏；资源访问都须在安全核的控制下进行；安全核非常小，便于进行形式化的描述与验证。



CN 102184373 A

1. 基于 CPU 的保护模式和虚拟化机制实现操作系统安全核的设计方法，其特征是该方法包括如下步骤：

一、CPU 保护模式提供了多个权限级 0-N，其中权限级 0 称为特权级，其它权限级 1-N 称为非特权级，硬件规定了特权级可以执行处理器的所有指令，硬件又规定非特权级只能执行处理器的部分指令，即规定了一些指令只能有特权级执行；利用 CPU 的保护模式将操作系统划分成一个工作在特权级的安全核与工作在非特权级的操作系统的服务进程两个部分；

二、安全核利用 CPU 保护模式，使得安全核之外的进程具有性质：1） 未经安全核许可不能访问其它进程的地址空间；2）只能通过向安全核发送消息来访问其它系统资源；

三、指定一个安全核专用的外存储区域存放安全核使用的各种长久性数据，利用硬件虚拟化控制机制，使得当执行一个访问安全核专用的外存储区域的 I/O 时自动陷入到安全核中，阻止任何安全核之外的程序访问安全核专用的外存储区域，保障安全核的数据的安全性。

2. 根据权利要求 1 所述的基于 CPU 的保护模式和虚拟化机制实现操作系统安全核的设计方法，其特征是安全核提供物理内存分配、消息传递与中断处理服务、进程调度，安全核的物理内存分配服务可以保证指定的两个进程内存空间是隔离的，使一个进程无法直接破坏另一个进程。

3. 根据权利要求 2 所述的基于 CPU 的保护模式和虚拟化机制实现操作系统安全核的设计方法，其特征是安全核提供息传递与中断处理服务，一个进程通过向安全核发送消息来访问除了自身内存地址之外的系统资源，安全核按照策略进行控制，安全核将消息转发给操作系统的相应的服务进程，由服务进程进行资源访问方面的信息管理工作，安全核只做策略控制，保持简洁性；一个进程通过向安全核发送消息来与另一个进程进行通信。

4. 根据权利要求 1 所述的基于 CPU 的保护模式和虚拟化机制实现操作系统安全核的设计方法，其特征是安全核进程调度服务确保进程调度过程中一个进程的上下文不会受到其它进程的破坏，确保的进程的静态完整性。

5. 根据权利要求 1 所述的基于 CPU 的保护模式和虚拟化机制实现操作系统安全核的设计方法，其特征是安全核控制所依赖的策略信息存放在一个安全核专用的外存储区域，一个专用的硬盘或者一个专用的硬盘分区，安全核利用虚拟化机制，设置处理器硬件，使得任何访问这个专用的外存储区域的指令都会跳转到安全核中，有安全核判断是否合法，阻止任何对安全核的专用的外存储区域的破坏行为。

基于保护模式与虚拟化机制实现操作系统安全核设计方法

技术领域

[0001] 本发明涉及的是一种基于 CPU 的保护模式和虚拟化机制的实现操作系统安全核的设计方法，属于计算机应用技术领域。

技术背景

[0002] 操作系统为用户程序提供了基础服务，为用户程序屏蔽了硬件平台的差异，用户程序利用操作系统提供标准服务来完成自身的任务。操作系统还必须提供驱动程序为用户程序提供各种硬件的接入服务。操作系统为了能够接入不断涌现的新设备，必须能够安装第三方开发的设备驱动程序使其成为操作系统的一部分。现有的操作系统是一个庞大的软件系统，其中还包括第三方开发的驱动程序，操作系统工作时可以执行任何指令。

[0003] 操作系统及其庞大，各个模块相互依赖，相关数据结构被各个模块共享，现有的软件工程方法难以排除操作系统中存在的漏洞。操作系统的漏洞可能被攻击者利用来安插恶意的程序，达到各式各样的攻击目标。同样第三方开发的驱动程序也可能存在安全漏洞，它们的安全性更加难以控制。

[0004] 操作系统提供的服务功能分别有不同的模块提供，对用户行为的控制涉及到操作系统的各个模块，在庞大的操作系统中分离对用户行为的控制和对用户服务请求的响应有着一定的难度。

发明内容

[0005] 本发明提出的是一种基于 CPU 的保护模式和虚拟化机制的实现操作系统安全核的设计方法，旨在提供一个利用 CPU 保护模式的机制构造一个充分小的安全核，具有两条性质 :(1)安全核之外的任何进程无法破坏安全核 ;(2)任意进程对任何资源的访问都必须受到安全核的控制。

[0006] 本发明的技术解决方案 :该方法包括如下步骤 :

一、CPU 保护模式提供了多个权限级 0-N，其中权限级 0 称为特权级，其它权限级 1-N 称为非特权级，硬件规定了特权级可以执行处理器的所有指令，硬件又规定非特权级只能执行处理器的部分指令，即规定了一些指令只能有特权级执行 ;利用 CPU 的保护模式将操作系统划分成一个工作在特权级的安全核与工作在非特权级的操作系统的服务进程两个部分 ;

二、安全核利用 CPU 保护模式，使得安全核之外的进程具有性质 :1) 未经安全核许可不能访问其它进程的地址空间 ;2) 只能通过向安全核发送消息来访问其它系统资源 ;

三、指定一个安全核专用的外存储区域存放安全核使用的各种长久性数据，利用硬件虚拟化控制机制，使得当执行一个访问安全核专用的外存储区域的 I/O 时自动陷入到安全核中，阻止任何安全核之外的程序访问安全核专用的外存储区域，保障安全核的数据的安全性。

[0007] 安全核提供物理内存分配、消息传递与中断处理服务、进程调度，安全核的物理内

存分配服务确保一个进程与另一个进程间的内存空间是隔离的，使一个进程无法直接破坏另一个进程。

[0008] 安全核提供息传递与中断处理服务，一个进程通过向安全核发送消息来访问除了自身内存地址之外的资源，安全核按照策略进行控制，安全核将消息转发给操作系统的相应的服务进程，由服务进程进行资源访问方面的信息管理工作，安全核只做策略控制，保持简洁性；一个进程通过向安全核发送消息来与另一个进程进行通信。

[0009] 安全核进程调度服务确保进程调度过程中一个进程的上下文不会受到其它进程的破坏，确保的进程的静态完整性。

[0010] 利用虚拟化机制使得即使在安全核休眠期间，任何访问安全核的专用存储区域的行为都激活安全核，并且在安全核允许的情况下才能实现访问。

[0011] 由于将安全核设计成唯一的特权级的程序，安全核可以实现与其它进程的隔离，保证安全核代码的安全。由于安全核采用专用的外村粗区域，并且利用虚拟化机制进行实时监控，保证了安全核数据的安全。由于将安全核设计成了唯一的进程间的通信信道和访问设备的通道，所以任何进程访问系统资源的的行为都会受到安全核的控制。

[0012] 本发明的优点：安全核本身不会受到其它进程的破坏；任何进程的资源访问都必须在安全核的控制下进行；安全核由几个非常小的独立程序组成，可以进行形式化的描述与验证。

附图说明

[0013] 附图 1 是本发明的应用示例图。

具体实施方式

[0014] 对照附图 1，安全核的保护从内外两个方面进行。将安全核设计得充分的小，以便利用现有的软件工程的方法和形式化的方法可以验证安全的正确性，从内部保证安全核的安全性；利用 CPU 的硬件的保护模式的机制从外部保护安全核的安全性，安全核掌握了进程物理内存分配的权力，安全核在分配物理内存的时候确保安全核的内存空间与其它的任何进程的内存空间都是隔离的；另外安全核控制着进程的加载，这样安全核在非执行状态下其它的任何进程无法破坏安全核，在安全核恢复运行的过程中也可以准确地恢复原来的安全状态。

[0015] 同样因为安全核在分配物理内存的时候确保安全核的内存空间与其它的任何进程的内存空间都是隔离的，其它的任何的进程都无法直接访问资源，也无法直接与其它进程进行通信。唯一的机制就是请求安全核向操作系统的某个服务进程转发服务请求消息，因此任意进程的对资源的访问都会受到安全核的控制。

[0016] CPU 的保护模式使得拥有特权级的程序具有极强的控制能力，在非特权级上运行的程序只能遵循运行在特权级的程序者制定的策略运行，能否制定一个好的策略是操作系统能够安全的关键所在。建立一个运行在特权级的安全核，安全核实现物理内存分配、消息传递与中断处理、进程调度。操作系统的其它服务功能都放在若干个工作在非特权级的服务进程中完成。安全核利用物理内存分配的机制实现进程间内存地址隔离，利用进程调度的机制使得只有安全核工作在特权级，其它进程都工作在非特权级，这样，任何进程都无法

破坏安全核。其次在进程隔离的基础上，安全核再提供消息传递与中断处理服务，任何进程访问资源或与其它的进程通信都必须通过向安全核发送消息，安全核根据策略进行控制，安全核将通过控制的请求转发给相应服务进程，安全核只做实质性的控制，复杂的数据分析工作交给操作系统的几个服务进程来完成，这样安全核可以逻辑清晰，代码量小，一般的实现可以在 1 万行之下，便于进行形式化的设计和验证。

[0017] 本发明基于 CPU 的保护模式实现操作系统安全核提供物理内存分配的的服务、消息传递与中断服务、进程调度服务。一个运行在非特权机上的进程无法执行特权指令，特权指令的执行能力被安全核完全屏蔽，而在得到了安全核提供的上述 3 项服务之后，就可以完成任何用户进程可以完成的任务。

[0018] 安全核提供的 3 项服务都是被中断激发的 :物理内存的分配被软中断或异常激发、进程调度也是被软中断核异常激发、消息传递也是被软中断激发。

[0019] 安全核对物理内存分配服务请求的响应安全核维护一个页表，利用 CPU 的 MMU 模块功能将一个进程的线性地址映射到物理内存地址，利用 CPU 的保护模式机制使得任何其它进程访问这个页表。当该模块收到了内存分配的请求后，就从空闲的物理内存空间为请求者分配地址并响应修改页表。当该模块收到了内存去配的请求后，就修改响应的页表核空闲物理内存空间的数据结构。安全核的物理内存分配使得除了安全核之外任何进程只可以做两件事 :(1) 操纵自己的内存空间 ;(2) 向安全核发送消息。

[0020] 该物理内存分配方法旨在确保进程的内存空间的完全隔离。

[0021] 安全核对消息传递与中断处理服务请求的响应安全核实现了系统能够产生的各种中断的处理程序，安全核截获所有的系统中断。当一个进程需要发出资源请求时通过软中断向安全核发出请求消息，安全核的中断处理程序截获了中断，安全核首先检查资源请求的合法性，如果合法就会调用消息传递的函数，将消息写入相应的服务进程的消息队列上，由操作系统的服务进程提供资源访问服务。当一个进程需要向另一个进程发送消息时，通过软中断向安全核发出请求消息，安全核仍然首先检查通信请求的合法性，如果合法就会调用消息传递的函数，将消息写入目标进程的消息队列上。如果硬件中断发生，也被设置成由安全核来响应，由安全核来控制输入资源。 安全核对进程调度服务请求的响应安全核为每一个进程维护一组描述进程的数据块队列，队列中的数据块描述进程当前的上下文，以便正确恢复进程的执行。当安全核收到进程切换的请求时，则(1)将当前进程的描述数据块放在队尾，并且把当前进程的上下文写入响应的描述数据块 ;(2) 将队首的进程的描述数据块的上下文写入相应的寄存器等对象，使该进程运行。

[0022] 该进程调度方法旨在提供进程调度的功能外确保进程的安全切换。

[0023] 利用虚拟化机制保护安全核的专用的外存储区域 CPU 的虚拟化机制提供了将指定的特权指令设置成敏感指令，将安全核设置在根特权级(root-priority)，其它的任何特权级的进程在执行敏感指令时都会陷入到指定的安全核中，安全核根据当前状态判断该操作是否可以被允许，阻止一切可能影响安全核安全的操作。

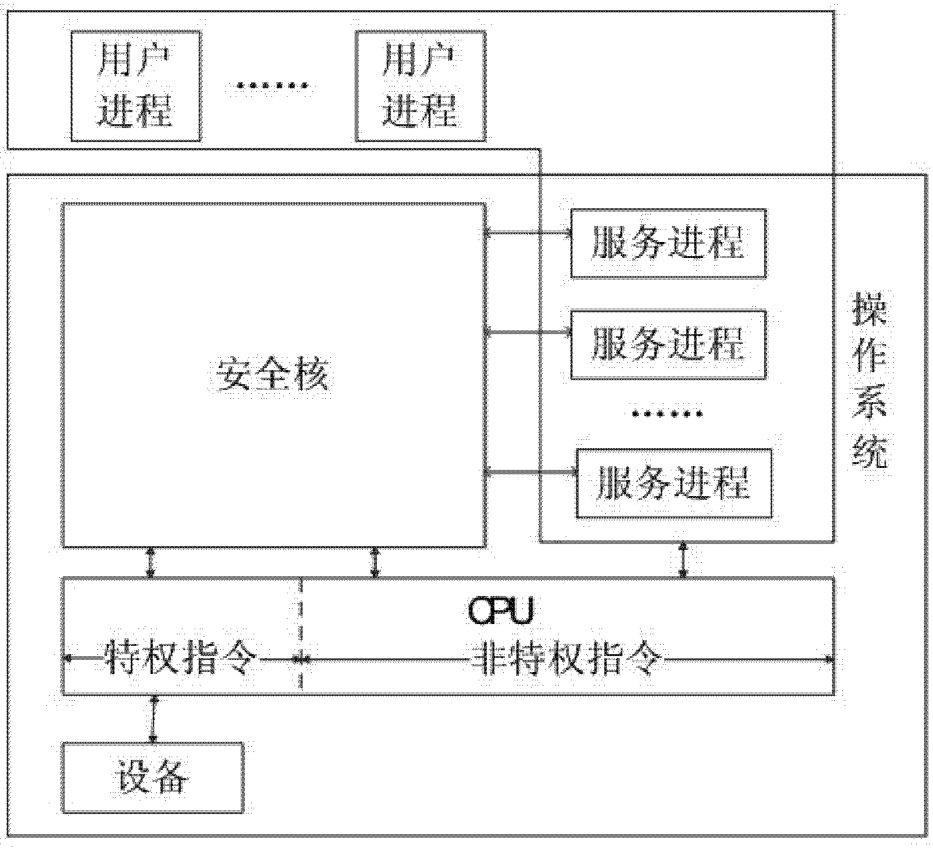


图 1