[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/00 (2006.01)
G06F 11/30 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200610001482.8

[43] 公开日 2007 年 7 月 25 日

[11] 公开号 CN 101004767A

[22] 申请日 2006.1.19
[21] 申请号 200610001482.8
[71] 申请人 联想（北京）有限公司
地址 100085 北京市海淀区上地信息产业基地创业路 6 号
[72] 发明人 王晓丁

[74] 专利代理机构 北京银龙知识产权代理有限公司
代理人 郝庆芬

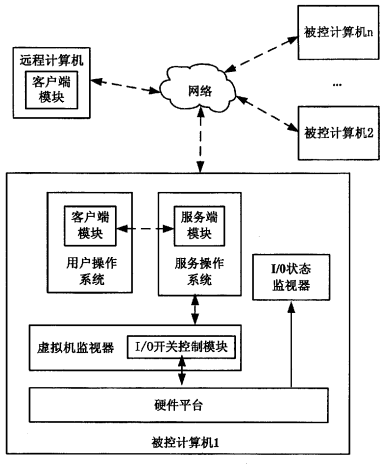
权利要求书 2 页 说明书 9 页 附图 5 页

[54] 发明名称

计算机系统及其 I/O 端口访问控制方法

[57] 摘要

本发明提供了一种计算机系统及其 I/O 端口访问控制方法，所述计算机系统包括：至少一个用户操作系统，服务操作系统，虚拟机监视器和硬件平台，其中用户操作系统包括客户端模块，用于同服务操作系统中的服务端模块进行交互并接收输入的 I/O 端口访问控制参数信息；服务操作系统包括服务端模块，用于同所述客户端模块进行交互并执行控制参数的设置；虚拟机监视器包括 I/O 开关控制模块，用于根据 I/O 端口控制参数决定是否允许执行来自用户操作系统的 I/O 指令。 所述计算机系统还包括用于显示 I/O 端口的状态的 I/O 状态监视器。 本发明的计算机系统可动态设置 I/O 端口访问参数且不能被未经授权的用户改动，用户还可直观地看到端口的禁用情况。



1. 一种计算机系统包括至少一个用户操作系统，服务操作系统，虚拟机监视器和硬件平台，其特征在于：

用户操作系统包括客户端模块，用于同服务操作系统中的服务端模块进行交互，并接收输入的I/O端口访问控制参数信息；

服务操作系统包括服务端模块，用于同所述客户端模块进行交互，并执行I/O端口访问控制参数的设置修改；

虚拟机监视器包括I/O开关控制模块，用于根据I/O端口控制参数决定是否允许执行来自用户操作系统的I/O指令。

2. 根据权利要求1所述的计算机系统，其特征在于还包括I/O状态监视器，用于根据I/O端口控制参数直观显示I/O端口的状态。

3. 根据权利要求1或2所述的计算机系统，其特征在于，所述服务操作系统为用户不可见的嵌入式操作系统。

4. 根据权利要求1或2所述的计算机系统，其中，所述计算机系统包括用于存储I/O端口控制参数信息的非易失性可重写介质区域和预定内存区域。

5. 根据权利要求1或2所示的计算机系统，其特征在于，还包括通过网络与之连接的远程计算机，所述远程计算机中包括具有网络功能的客户端模块，所述服务操作系统所包含的服务端模块也具有网络功能，远程计算机中的客户端模块通过网络与服务操作系统中包含服务端模块进行交互。

6. 根据权利要求5所述的计算机系统，其特征在于，所述服务操作系统为用户不可见的嵌入式操作系统。

7. 根据权利要求5所述的计算机系统，其中，在计算机系统的非易失性可重写介质中和内存预定区域中均保存有I/O端口控制参数信息。

8. 根据权利要求5所述的计算机系统，其中服务端模块是Web server，客户端模块是常用浏览器。

9. 根据权利要求5所述的计算机系统，其中服务端模块和客户端模块是SNMP server。

10. 一种I/O端口访问控制的方法，所述方法包括以下步骤:

步骤一，用户操作系统发出 I/O 操作请求；

步骤二，虚拟机监视器截获来自用户操作系统的 I/O 指令；

步骤三，从系统预定的内存区域获取预先设置的 I/O 端口访问控制参数，根据参数设置判断是否禁用端口；

步骤四，如果参数设置为禁用，则禁止执行改 I/O 指令，否则，允许执行该 I/O 指令。

11. 根据权利要求 10 所述的方法，其中所述步骤四还包括：将 I/O 端口访问控制参数信息发送给 I/O 状态监视器。

12. 根据权利要求 10 或 11 所述的方法，其中所述步骤三中预先设置的 I/O 端口访问控制参数的设置，包括以下步骤：

步骤一，客户端模块向服务操作系统中的服务端模块发出访问请求；

步骤二，服务端模块响应客户端模块的请求并将 I/O 端口访问控制参数信息传送给客户端模块；

步骤三，客户端模块接收到 I/O 端口访问控制参数信息直观显示，并接收管理员对参数信息的设置；

步骤四，客户端模块将设置后的 I/O 端口访问控制参数信息传送给服务端模块，根据这些参数信息更新 I/O 端口访问控制参数的设置。

计算机系统及其I/O端口访问控制方法

技术领域

本发明涉及计算机系统，特别是涉及一种计算机系统及其 I/O 端口访问控制方法。

背景技术

随着计算机技术和网络技术的发展，现代企业的办公自动化水平逐步提高，企业对于计算机和网络的依赖性也日益增强，而信息安全问题也成为企业所面临的不可避免的重大问题，其中机密数据泄漏问题是众多高新技术企业异常关心的问题，这是因为机密数据外泄将给企业造成不可估量的损失。因此，为避免机密数据外泄，很多企业都采取了一些措施。大多数企业都将存储有机密数据的计算机与外部网隔离，并使用企业内部网和专用网以防范外部人员对于本单位数据的非法存取，而对于拷贝方式的机密数据泄露，许多单位都采取限制员工使用软驱、光驱、USB 端口进行数据拷贝等一些措施。另外，还一有些单位为了避免机密数据通过拷贝形式外泄，甚至将软驱读写器、光驱等从物理装置上拆除，并封上 USB 端口，或者委托一些厂商在主机上设置一个外加锁的 USB 控制开关，只允许管理员拨动开关。这些方法的使用虽然也起到了避免数据通过拷贝方式外泄的作用，但是方式不太灵活。

为了避免通过软驱、光驱和 USB 等方式拷贝机密文件而造成机密泄露，目前也出现了一种机密信息管理系统，该系统主要是对原始文档进行集中管理，并将其转换为不允许修改的特有格式，使员工通过嵌入在 IE 中的阅读器进行浏览，使这些文件成为只能在内部网上浏览而不能对其进行修改的电子文件，并且对所有用户设置特定权限，不同权限的用户的访问权限也不同，例如级别高的用户可以打印，级别低的只能阅读，为防止二次传播，还采用机器绑定的方式，只允许内部网中的特定机器才能访问网页中的电子文件。这种方式对于拷贝方式的机密文件泄露，的确起到了很好的作用，然而，对于许多研发企业单位，或者企业单位内部的研发部门，即通常在开发者的计

算机中保存有许多机密数据、机密文件、程序设计文件等资料的情况下，就无法使用这种机密信息管理系统来防止数据拷贝方式的机密泄露。

除此之外，还有一种防止拷贝方式的机密泄露的方法，这种方式是在用户操作系统中安装一个内核级别的软件，通过这个内核级别的软件对 I/O 端口进行开关控制，但是，这种做法无法防止用户进入操作系统的安全模式自行将该内核级别的软件删除。

现有的一些做法要么有些极端，方式非常不灵活，无法实现计算机系统管理员根据需要动态地设置 I/O 端口的访问权限，或者根据需要临时允许用户使用这些端口，要么不能防止用户自己移除 I/O 端口的开关控制功能，此外，还不能让用户直观地了解端口的禁用情况，即哪些端口允许使用，哪些端口禁止使用。

发明内容

为此，本发明的一个目的就是提供一种计算机系统以及对该系统的 I/O 端口访问进行控制的方法，使得能够动态设置 I/O 端口访问权限，不能被未经授权的用户更改。

本发明的另一目的在于，提供一种计算机系统以及对该系统的 I/O 端口访问进行控制的方法，使得用户能够直观地看到 I/O 端口的禁用情况。

为此本发明提供了一种计算机系统，包括至少一个用户操作系统，服务操作系统，虚拟机监视器和硬件平台，其特征在于：

用户操作系统包括客户端模块，用于同服务操作系统中的服务端模块进行交互，并接收输入的 I/O 端口访问控制参数信息；

服务操作系统包括服务端模块，用于同所述客户端模块进行交互，并执行 I/O 端口访问控制参数的设置修改；

虚拟机监视器包括 I/O 开关控制模块，用于根据 I/O 端口控制参数决定是否允许执行来自用户操作系统的 I/O 指令。

本发明的计算机系统，其特征在于还包括 I/O 状态监视器，用于根据 I/O 端口访问控制参数直观显示 I/O 端口的状态。

本发明的计算机系统，其特征在于，所述服务操作系统为用户不可见的嵌入式操作系统。

本发明的计算机系统，其中，所述计算机系统包括用于存储 I/O 端口控制参数信息的非易失性可重写介质区域和预定内存区域。

本发明的计算机系统，其特征在于，还包括通过网络与之连接的远程计算机，所述远程计算机中包括具有网络功能的客户端模块，所述服务操作系统所包含的服务端模块也具有网络功能，远程计算机中的客户端模块通过网络与服务操作系统中包含服务端模块进行交互。

本发明的计算机系统，其特征在于，所述服务操作系统为用户不可见的嵌入式操作系统。

本发明的计算机系统，其中，在计算机系统的非易失性可重写介质中和内存预定区域中均保存有 I/O 端口控制参数信息。

本发明的计算机系统，其中服务端模块是 Web server，客户端模块是常用浏览器。

本发明的计算机系统，其中服务端模块和客户端模块是 SNMP server。

本发明还提供了一种在本发明的计算机系统中实现 I/O 端口访问控制的方法，所述方法包括以下步骤:

步骤一，用户操作系统发出 I/O 操作请求；

步骤二，虚拟机监视器截获来自用户操作系统的 I/O 指令；

步骤三，从系统预定的内存区域获取预先设置的 I/O 端口访问控制参数，根据参数设置判断是否禁用端口；

步骤四，如果参数设置为禁用，则禁止执行改 I/O 指令，否则，允许执行该 I/O 指令。

本发明的 I/O 端口访问控制的方法，其中所述步骤四还包括：将 I/O 端口访问控制参数信息发送给 I/O 状态监视器。

本发明的 I/O 端口访问控制的方法，其中所述步骤三中预先设置的 I/O 端口访问控制参数的设置，包括以下步骤：

步骤一，客户端模块向服务操作系统中的服务端模块发出访问请求；

步骤二，服务端模块响应客户端模块的请求并将 I/O 端口访问控制参数信息传送给客户端模块；

步骤三，客户端模块接收到 I/O 端口访问控制参数信息直观显示，并

接收管理员对参数信息的设置；

步骤四，客户端模块将设置后的 I/O 端口访问控制参数信息传送给服务端模块，根据这些参数信息更新 I/O 端口访问控制参数的设置。

本发明的计算机系统和 I/O 端口访问控制方法，不但实现了灵活的 I/O 端口的访问控制，还防止了用户自行删除对 I/O 端口的访问控制功能，并且使得用户可以直观的看到端口禁用情况。

附图说明

下面将参考附图结合实施例对本发明进行详细的描述，其中：

图 1 为本发明的计算机系统的结构示意图；

图 2 为本发明的 I/O 端口访问控制方法的流程图；

图 3 为利用客户端模块进行参数设置的流程图；

图 4 为本发明的计算机系统中的 I/O 端口访问控制参数的数据结构图；

图 5 为可以在本发明中应用的涉及 I/O 端口访问控制参数设置部分的 html 页面的结构示意图；

图 6 为包含在本发明计算机系统的被控制计算机中的 I/O 状态监视器的结构示意图；

图 7 为图 6 所示的 I/O 状态监视器的状态指示面板的示意图。

具体实施方式

图 1 示出了本发明的计算机系统的结构示意图，所示出的被控计算机包括服务操作系统（SOS）、用户操作系统（COS）、虚拟机监视器（VMM）、I/O 状态监视器以及硬件平台。其中，用户操作系统是最终用户使用的操作系统，诸如 widows XP；服务操作系统是为用户操作系统提供各种服务的操作系统；虚拟机监视器是直接运行在硬件之上的最高一级的“特权层”，具有系统资源控制权，用于控制系统硬件资源（处理器、内存、其它设备等）分配的软件层，所述用户操作系统和服务操作系统运行在该虚拟机监视器上；I/O 状态监视器用于显示当前的 I/O 端口的禁用情况；其中，所述硬件平台支持虚拟计算指令。

上述用户操作系统包含有客户端模块，用于同服务操作系统中的服务端模块进行交互以实现 I/O 端口访问控制参数的访问，系统管理员可以通过该

客户端模块从服务操作系统中的服务端模块获取参数设置信息，以便查看被控计算机的 I/O 端口访问控制参数的设置情况，还可通过客户端模块对参数设置进行更改，客户端模块将更改后的 I/O 端口访问控制参数信息发送给服务操作系统中的服务端模块。

在上述服务操作系统中包含有服务端模块，用于同客户端模块进行交互并执行 I/O 端口访问控制参数的设置，服务端模块接收客户模块的 I/O 端口访问控制参数请求、获取参数设置信息并发送给客户端模块，接收来自客户端模块的参数设置的更改信息，并根据所接收的更改信息对 I/O 端口访问控制参数进行更新。

在上述虚拟机监视器（VMM）中运行有 I/O 开关控制模块，用于根据 I/O 端口访问控制参数，决定是否允许执行来自用户操作系统的 I/O 指令，同时将发送控制信号给 I/O 状态监视器，以显示当前的 I/O 端口的禁用情况。

图 1 示出的计算机系统中，各个被控计算机通过网络连接在一起。优选地，由系统管理员使用远程计算机通过网络对被控计算机进行集中控制。因此，优选服务操作系统中的服务端模块具有网络功能，并且远程计算机中包括的客户端模块也具有网络功能以同远程计算机中的服务端模块进行交互。应当指出的是，图 1 示出的被控计算机可以通过用户操作系统中的客户端模块对 I/O 访问控制参数进行设置，因此一个被控计算机也可构成本发明的一个的计算机系统。

为安全起见，在本发明的计算机系统中，客户端模块对服务操作系统的访问可以采用一些限制措施，使得只有管理员才能够更改设置，诸如通过身份验证等方式。

下面将参考图 2 介绍在本发明的计算机系统中，进行 I/O 端口访问控制的方法步骤。

图 2 示出了本发明的 I/O 端口访问控制方法的流程图。首先，用户操作系统发出 I/O 端口访问请求。具体地，在用户操作系统中，用户操作或者应用程序触发 I/O 端口访问请求，该访问请求被转换为函数调用之后提交给用户操作系统内核，在用户操作系统内核中的硬件驱动程序将该函数调用转换为 I/O 端口访问控制器能够识别的 I/O 指令，然后通过 CPU 提交给 I/O 端口

访问控制器去执行。

接着，虚拟机监视器截获来自服务操作系统的 I/O 的指令。由于在本发明中采用了虚拟化技术，因此在本发明硬件平台上，CPU 支持两类指令，一类是专门供虚拟机监视器使用 ROOT 指令，另一类是专门供运行在虚拟机监视器上操作系统使用的 NON-ROOT 指令，因此，当 CPU 接到来自用户操作系统的 I/O 指令时，就将控制权交给虚拟机监视器，例如，调用 VM-ENTRY 命令，使得从 NON-ROOT 模式切换成 ROOT 模式，并把 I/O 指令交由虚拟机监视器处理，这样虚拟机监视器就截获了来自用户操作系统的 I/O 指令。

然后，虚拟机监视器中的 I/O 开关控制模块根据所截获的这些 I/O 指令的类型，从存储 I/O 端口访问控制参数的预定内存区域中获取参数设置信息，并根据获取的参数信息判断是禁止这些 I/O 指令执行，还是允许执行该指令。需要注意的是，由于虚拟监视器主要负责为操作系统进行资源分配和管理，而并不能基于自身的需求从诸如硬盘上直接取得 I/O 端口访问控制参数设置信息，因此需要在预定的内存区域中保存一份 I/O 端口访问控制参数信息，以使虚拟机监视器能够获取参数设置信息，例如，可以在系统启动时由服务操作系统将存储在诸如硬盘中的 I/O 端口访问控制参数拷贝到预定的内存区域中，并且参数更改之后也需要更新该预定内存区域中的参数设置。

如果允许执行，那么 CPU 将这些 I/O 指令提交给 I/O 端口访问控制器执行，同时发送控制信号给 I/O 状态监视器使其直观显示 I/O 端口状态，完成操作后，CPU 将操作权交给用户操作系统，例如调用 VM-EXIT 命令，使得从 ROOT 模式切换成 NON-ROOT 模式，用户操作系统的硬件驱动程序得到 I/O 请求的结果后，将请求结果返回给用户操作系统；否则，禁止 I/O 指令的执行，并发送控制信号给 I/O 状态监视器使其直观地显示 I/O 端口状态，之后，将操作权交给用户操作系统，例如，CPU 调用 VM－EXIT 命令，从 ROOT 模式切换成 NON-ROOT 模式，用户操作系统的硬件驱动程序得到 I/O 请求的结果后，将请求结果返回给用户操作系统。当然，也可以设置成当参数设置发生变化的情况下才发送控制信号修改指示状态。服务操作系统优选没有显示功能的嵌入式操作系统。

在图 2 所述的方法中，位于虚拟机监视器中的 I/O 开关控制模块是根据

预先设置的I/O端口访问控制参数，来决定是否允许CPU将来自用户操作系统的I/O指令交给I/O端口访问控制器执行。下面，将参考图3，描述在本发明的计算机系中，通过客户端模块对I/O端口访问控制参数进行设置的过程。

图3示出了通过客户端模块进行参数设置的流程图。首先，管理员通过客户端模块向服务操作系统中的服务端模块发送访问请求。接着，服务操作系统中的服务端模块获取存储在系统非易失性可重写介质（诸如硬盘、EEPROM、FLASH等）中的I/O端口访问控制参数设置信息，将这些信息发送给客户端模块。然后，客户端模块接收到参数信息后进行显示，管理员根据需求对 I/O 端口访问控制参数设置进行更改。接着，客户端模块将更改后的参数信息发送给服务端模块。服务端模块接收到更改后的参数设置信息后，使用这些设置后的信息更新参数设置，包括修改存储在非易失性可重写介质中（诸如硬盘、EEPROM、FLASH等）的I/O端口访问控制参数设置信息，同时更新存储在预定内存区域的I/O端口访问控制参数。

当客户端模块运行在用户操作系统中时，在这种情况下，客户端模块可以通过虚拟机监视器提供的共享内存与服务端模块进行数据传输，数据格式可以基于I/O端口开关控制参数设置的需求进行约定。

此外，还可以通过网络执行该参数设置过程。这时客户端模块可以运行在用户操作系统中，也可以运行在远程计算机中。在计算机网络中，管理员可以在远程计算中通过客户端模块对I/O端口开关控制参数进行设置。这时，服务端模块和客户端模块都需具有网络功能。下面介绍通过计算机网络设置I/O访问控制参数的过程。首先，远程计算机中的客户端模块可以通过使用服务端模块的IP地址向服务端模块发送访问请求；接着位于服务操作系统中处于等待访问请求状态的服务端模块将 I/O 端口访问控制参数信息通过网络传送至远程计算机中的客户端模块；管理员通过客户端模块，可以查看现有I/O端口访问控制参数，并根据需要对 I/O 端口访问控制参数进行设置。设置后的 I/O 端口访问控制参数由远程计算机中的客户端模块通过网络传送至被控计算机中的服务端模块。然后服务端模块使用修改后的参数信息，更新参数设置，包括更新存储在预定内存区域中的参数设置信息。

本发明中，用于提供网络功能的服务端模块可以以Web Server方式实现，

这样客户端模块就可以直接使用操作系统中已有的网络浏览器软件与其通信，最终实现控制参数设置功能。此外，还可以采用其它方式实现，诸如服务端模块以 SNMP Server 实现，远程计算机上的客户端模块可以使用 SNMP Server，而两者之间通过 SNMP 协议进行通信。此外，需要注意的是，对于被控计算机中的服务操作系统进行访问需要进行权限控制，诸如可以在服务端模块处设置身份认证来实现对参数设置权的控制。

在本发明中，I/O 端口访问控制参数的数据结构的可以如图 4 设计，主要包括 I/O 控制器序号，I/O 控制器名称和开关状态三个字段，可以分别由“0”和“1”表示允许和禁用状态，也可以使用其它方式表示，诸如“1”表示允许而 “0”表示禁用，或者分别用“Y”和“N”表示。

图 5 示出了在使用网络设置参数的情况下，可以在本发明中应用的涉及 I/O 端口访问控制参数设置部分的 html 页面的结构示意图。该页面的显示结果与图 4 所示的参数设置对应，其中开关状态为“1”的软驱和 USB 处于禁用状态，而开关状态为“0”的其它 I/O 端口处于允许使用状态。

本发明的计算机系统的被控计算机中所包含的 I/O 状态监视器，主要用于显示 I/O 端口的状态，使用户直观了解计算机中的 I/O 端口禁用情况，其结构如图 6 所示，主要包括连接线接头、单片机控制芯片和状态指示单元组成。连接线接头用于同被控计算机主机连接，连接方式可以是串口、并口、USB 口多种方式；单片机控制芯片用于根据来自主机的信号控制状态指示单元的动态显示；状态指示单元用于根据来自单片机控制芯片的控制信号显示当前 I/O 端口禁用情况，简单的状态指示单元包括指示灯，诸如发光二极管，通过指示灯的状态来指示 I/O 端口禁用情况。当然，在仅使用单个指示元件的情况下，也可以省略单片机控制芯片。

图 7 为图 6 所示的 I/O 状态监视器的状态指示面板的示意图。每个指示灯表示一个相应的 I/O 端口状态。实现 I/O 端口状态监视功能还需要在 I/O 端口访问控制过程中，在获得状态信息之后发送控制信号给 I/O 监视器以进行直观显示 I/O 端口的状态。

本发明所提供的计算机系统及其 I/O 端口访问控制方法，通过虚拟机监视器中的 I/O 开关控制模块，实现了 I/O 端口访问的控制，通过客户端模块以

及服务操作系统中的服务端模块使得管理人员可以灵活地设置 I/O 端口访问控制参数，并且有效地防止了未经授权用户将与该功能相关的模块或者信息删除。此外，本发明还可以直观地显示 I/O 端口禁用情况，使得最终用户可以清楚地了解当前哪些端口可以使用，哪些端口禁止使用。

以上描述通过实施例的方式介绍了本发明，但本发明并不仅限于所描述的实施例。应当注意的是，在并不偏离本发明的精神和范围的情况下，还存在许多可替代的方式和变型，诸如 I/O 状态监视器也可以采用软件形式显示在用户操作系统中，供最终用户查看。

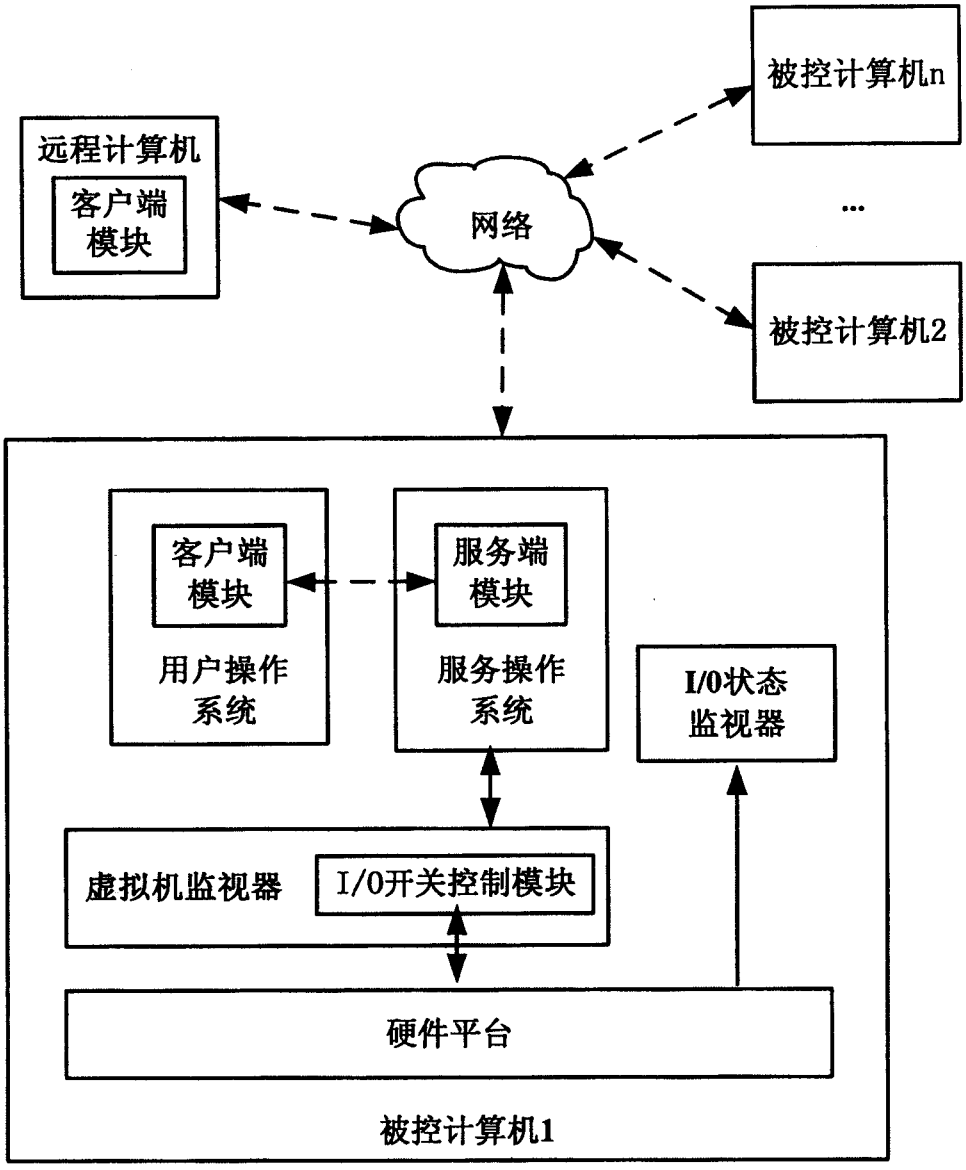

被控计算机n
远程计算机
客户端模块
网络
...
被控计算机2
客户端模块
服务端模块
用户操作系统
服务操作系统
I/O状态监视器
虚拟机监视器
I/O开关控制模块
硬件平台
被控计算机1

图 1

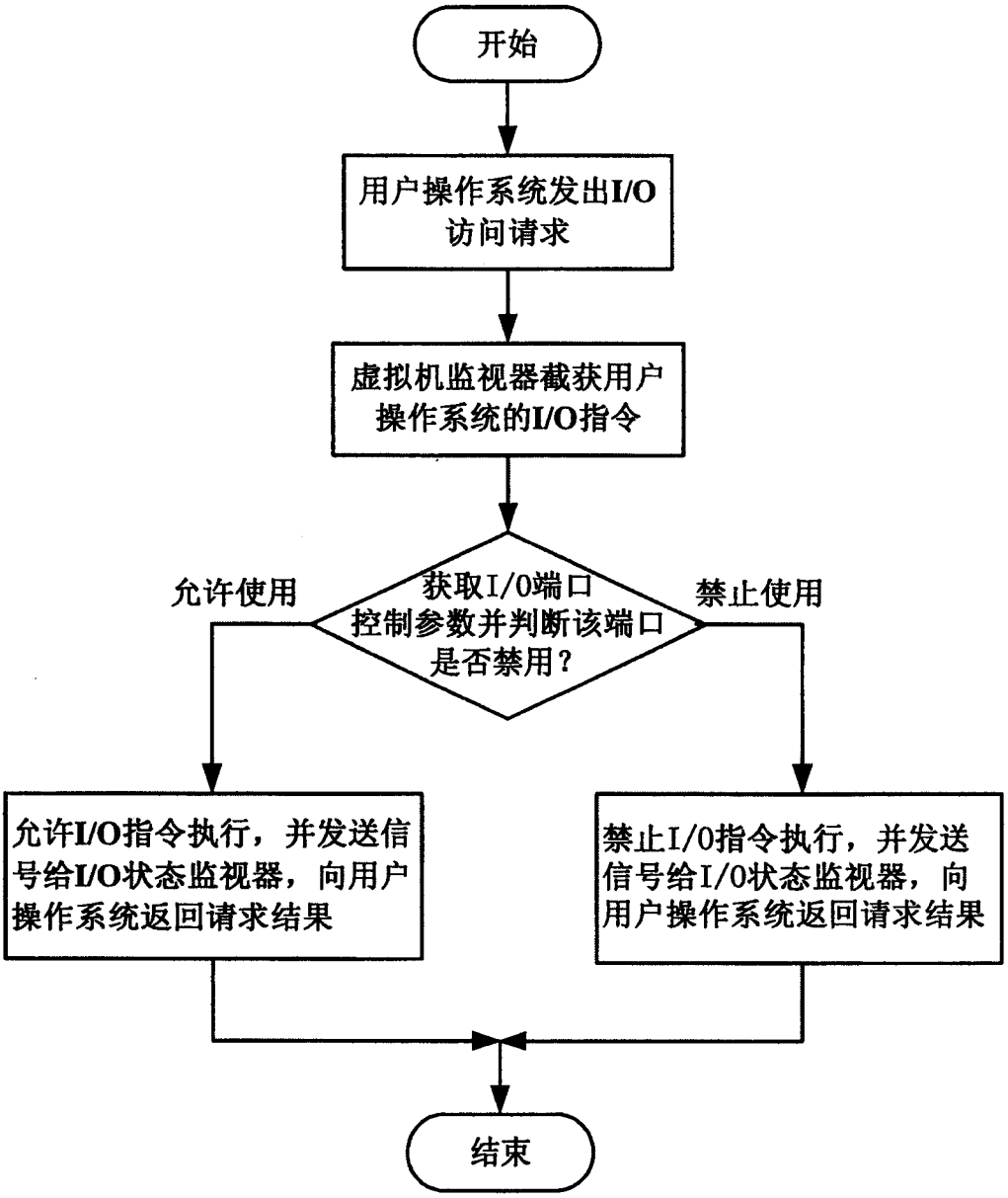

开始
用户操作系统发出I/O访问请求
虚拟机监视器截获用户操作系统的I/O指令
获取I/O端口控制参数并判断该端口是否禁用？
允许使用
禁止使用
允许I/O指令执行，并发送信号给I/O状态监视器，向用户操作系统返回请求结果
禁止I/O指令执行，并发送信号给I/O状态监视器，向用户操作系统返回请求结果
结束

图 2

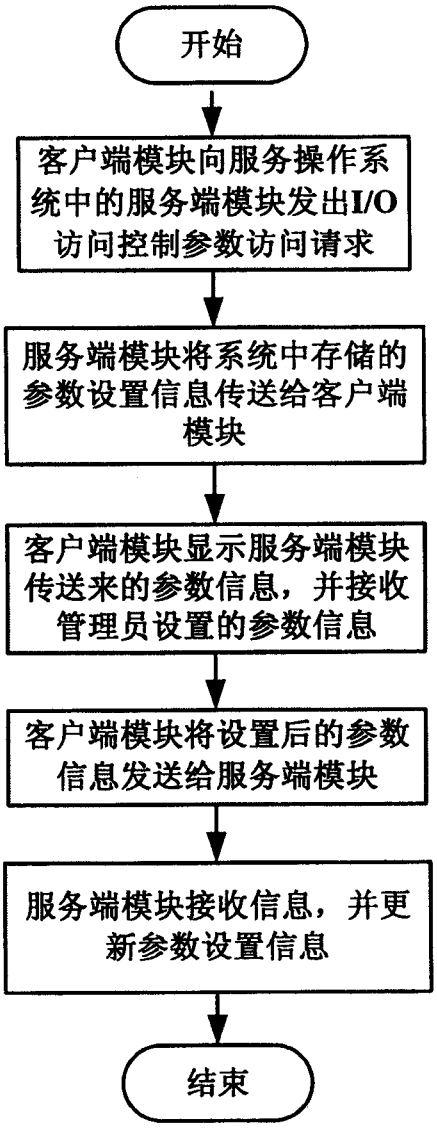

开始
客户端模块向服务操作系统中的服务端模块发出I/O访问控制参数访问请求
服务端模块将系统中存储的参数设置信息传送给客户端模块
客户端模块显示服务端模块传送来的参数信息，并接收管理员设置的参数信息
客户端模块将设置后的参数信息发送给服务端模块
服务端模块接收信息，并更新参数设置信息
结束

图 3

I/O控制器序号	I/O控制器名称	开关状态
1	软驱	1
2	光驱	0
3	USB	1
4	串口	0
5	并口	0

图 4

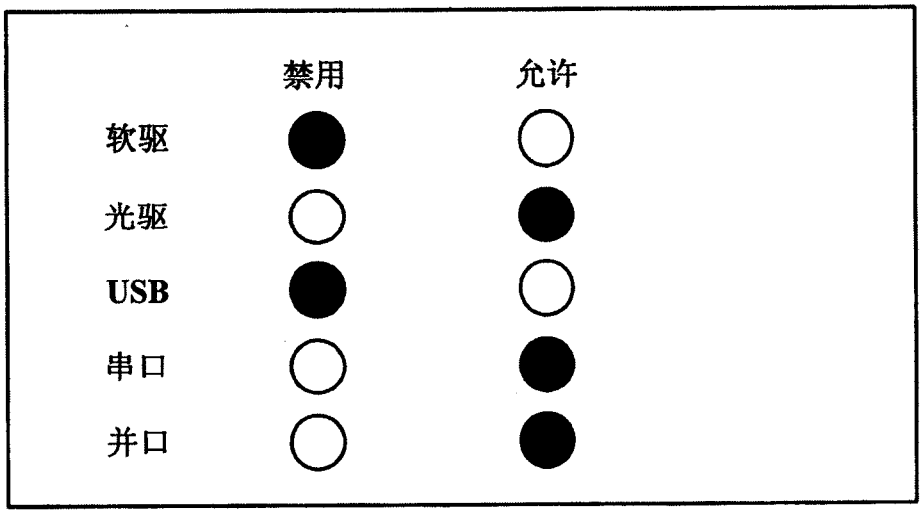


图 5

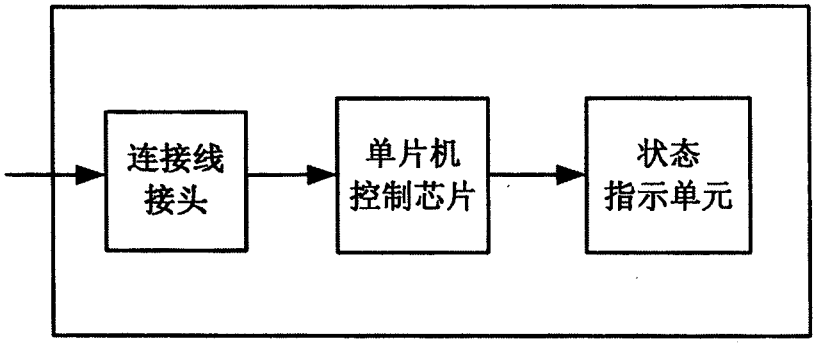


图 6

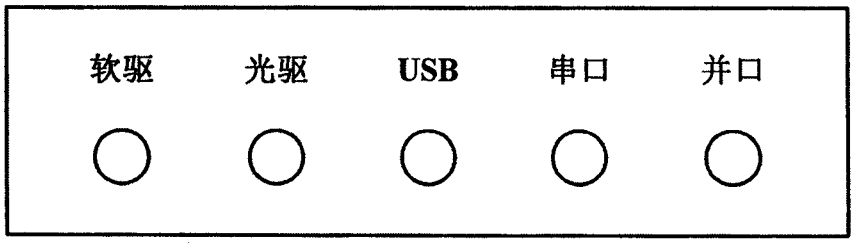


图 7