



(12) 发明专利

(10) 授权公告号 CN 101142558 B

(45) 授权公告日 2011.03.16

(21) 申请号 200680006199.2

(22) 申请日 2006.03.08

(30) 优先权数据

11/074,500 2005.03.08 US

(85) PCT申请进入国家阶段日

2007.08.27

(86) PCT申请的申请数据

PCT/US2006/012811 2006.03.08

(87) PCT申请的公布数据

W02006/096890 EN 2006.09.14

(73) 专利权人 微软公司

地址 美国华盛顿州

(72) 发明人 A·弗兰克 W·J·维斯提恩

(74) 专利代理机构 上海专利商标事务所有限公

司 31100

代理人 顾嘉运

(51) Int. Cl.

G06F 11/30 (2006.01)

G06F 12/14 (2006.01)

(56) 对比文件

US 2002/0147782 A1, 2002.10.10, 说明书第 [0007] 段至 [0060] 段、附图 1 至 3.

US 2005/0033747 A1, 2005.02.10, 说明书第 [0037], [0062] 段.

US 5355161 A, 1994.10.11, 说明书第 10 栏第 35 至 40 行.

CN 1532700 A, 2004.09.29, 全文.

US 2005/0050355 A1, 2005.03.03, 全文.

审查员 刘长勇

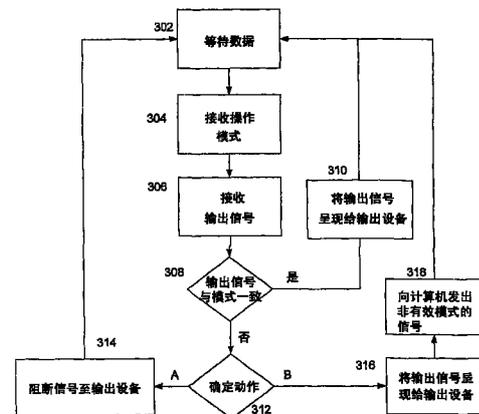
权利要求书 1 页 说明书 8 页 附图 4 页

(54) 发明名称

用于可信计量和停用的系统和方法

(57) 摘要

一种通过配置诸如图形处理单元等输出控制器来在将输出信号呈现给输出设备之前屏蔽输出信号而适于在不同的操作模式中使用的计算机。输出控制器中的安全环境验证输出信号的数字签名或散列来确定输出信号是否与当前操作模式兼容。因此,当计算机在受限功能模式中操作,诸如当所计量的使用时间期满时仅呈现授权的输出信号。该装置和方法也公开了用于确定计算机是否应从待机或非计量模式返回至活动或计量模式的类似的输出信号屏蔽。



1. 一种适用于在多个操作模式中操作的计算机,包括:

第一输出设备;

耦合至所述第一输出设备的第一输出控制器,包括:

第一隔离计算环境;以及

存储器,它存储对应于旨在呈现给所述第一输出设备的输出数据的位模式,其中所述第一隔离计算环境分析所述位模式来确定所述输出数据是否与所述计算机的当前操作模式一致;以及

主板,其中所述主板上设置有与所述第一隔离计算环境通信的第二隔离计算环境,用于将所述当前操作模式传达给所述第一隔离计算环境,并且当所述输出数据与所述计算机的当前操作模式不一致时,所述第一隔离计算环境指示所述第二隔离计算环境改变所述计算机的当前操作模式;以及

其中,所述第一隔离计算环境干预所述第一输出设备的正常操作,以阻止所述输出数据到达其相应的输出;

所述输出数据被检查以确定该输出数据是否与被授权在特定操作模式期间执行的程序相关联,以便能有效地将所述计算机仅限于被预定对充值或重新激活所述计算机有用的那些应用程序或实用程序的操作,或者对诊断和维护有用的那些应用程序或实用程序的操作。

2. 如权利要求 1 所述的计算机,其特征在于,所述第一输出控制器是显示控制器、声音控制器和触觉控制器中的至少一个。

3. 如权利要求 1 所述的计算机,其特征在于,所述第一隔离计算环境具有加密能力,并使用数字签名和散列码的至少其中之一来分析所述位模式。

4. 如权利要求 1 所述的计算机,其特征在于,当所述输出数据与所述计算机的当前操作模式不一致时,所述第一输出控制器进行更改或者阻断至所述第一输出设备的所述输出数据中的一项。

用于可信计量和停用的系统和方法

[0001] 背景

[0002] 用于个人计算机分发的即用即付或按使用付费商业模式建立在在在的基础上筹募资金以交换对计算机或其某些组件的有利使用的概念上。当按使用付费资金提供或预付时间期限即将期满时,向用户给予对帐户“充值”以确保不中断地使用计算机的机会。然而,当资金提供或使用时间期限在帐户被充值之前期满时发生状况。完全禁用计算机可能会阻止用户进行充值和还原操作。另一方面,理论上允许充值的允许用户对计算机的有限使用的制裁在有限使用允许满足用户的足够功能时可能鼓励不付费行为。

[0003] 此外,当系统被停用时,除允许重新激活以外,它也应允许维护,例如对磁盘驱动器整理碎片和对例如网络子系统的故障诊断。从而,需要在订阅使用期满之后阻止对计算机的有利使用,同时在订阅条款被满足时允许用于维护或重新激活计算机的进程。

[0004] 概述

[0005] 使用超出正常输出处理的信号分析的内部能力来配置诸如图形处理器或声卡等输出处理单元。信号分析处理能力用于分析被呈现来输出的输出数据。取决于计算机的操作模式,输出处理单元可确定输出数据是否与当前操作模式一致。安全处理能力阻止可能会使分析处理失败的篡改,并且还阻止向方案操作员提供与监视操作和制裁进程相关联的用于更新的安全结束点。

[0006] 根据本发明的一个方面,可使用图形处理单元(GPU)来过滤或分析所显示的图形,使得仅显示与对计算机充值或故障诊断相关联的授权图形图像。显示图形可被数字地签署或可具有允许 GPU 标识授权图形图像以便当在制裁下操作时使用的散列码。

[0007] 根据本发明的另一方面,可使用图形或声音处理单元来有助于确定计算机何时从事有利使用从而应被计量,或何时基本空闲且不应被计量。通过在与屏幕保护程序、维护实用程序、或其它空闲进程相关联的输出数据同诸如文字处理程序或 MP3 播放器等用户关联进程相关联的输出数据之间进行区分,输出处理单元可补充计算机中所支持的现有计量进程。

[0008] 附图简述

[0009] 图 1 是计算机网络的简化且代表性的框图;

[0010] 图 2 是计算机的简化且代表性的框图;

[0011] 图 3 是示出图 2 的计算机的 CPU/ 主板与图形处理单元之间的逻辑关系的简化且代表性的框图;以及

[0012] 图 4 是描述一种操作按使用付费或即用即付计算机的方法的流程图。

[0013] 各个实施例的详细描述

[0014] 尽管以下文字阐述了各个不同实施例的详细描述,但应理解,该描述的法律范围由本发明所附的权利要求书的文字来定义。该详细描述应被解释为仅是示例性的,且不描述每个可能的实施例,因为描述每个可能的实施例即使不是不可能也是不实际的。可使用当前的技术或在本专利的申请日之后开发的技术来实现众多替换实施例,它们仍落入权利要求书的范围之内。

[0015] 应理解,除非使用语句“如此处所使用的,术语‘__’此处定义为指的是……”或类似语句在本专利中显式地定义一术语,否则不旨在显式或隐式地超出该术语的普通或寻常意义而限制该术语的含义,且这样的术语不应被解释为限于基于本专利的任何部分中所作出的任何陈述(除权利要求书的语言以外)的范围。就本专利所附权利要求书中所述的任何术语在本专利中以与单数意义一致的方式引用而言,这仅是为了清楚起见以便不混淆读者,且这样的权利要求术语不旨在通过暗示等限于该单数意义。最后,除非权利要求元素是通过叙述单词“装置”和功能而未叙述任何结构来定义的,否则任何权利要求元素的范围不旨在基于对 35U. S. C. § 112 第 6 段的应用来解释。

[0016] 众多发明性功能和众多发明性原理最佳地使用软件程序或指令以及诸如专用 IC 等集成电路(IC)来实现。尽管可能要花费大量努力以及存在例如由可用时间、当前技术以及经济上的考虑而激发的众多设计选择,但期望本领域的普通技术人员在由此处公开的概念和原理指导时,将能容易地以最小的试验来生成这样的软件指令和程序以及 IC。从而,为了简明以及最小化模糊根据本发明的原理和概念的任何风险,如果有这样的软件和 IC 的进一步描述,它们也将被限于关于优选实施例的原理和概念的要素。

[0017] 众多现有技术的高价值计算机、个人数字助理、组织器等可能不适于在没有附加安全性的情况下在预付或按使用付费的商业模型中使用。如上所述,这些设备可能需要附加的功能和底层安全服务来满足按使用付费或即用即付商业模型的要求。例如,个人计算机可能会从提供的因特网服务中断开,但仍可用于文字处理、电子表格等。在例如因特网服务供应商或其它商业实体等服务供应商以对将来费用的预期来对个人计算机的成本承保时,该“无限制价值”产生了欺诈应用和偷窃的可能。类似地,当按使用付费或即用即付计算机未被授权来进行完全操作时,期望支持足够的功能来完成授权过程而不提供足够的功能来引诱用户在制裁模式下使用计算机。

[0018] 图 1 示出可用于实现动态软件供应系统的网络 10。网络 10 可以是因特网,虚拟专用网(VPN),或允许一台或多台计算机、通信设备、数据库等彼此通信连接的任何其它网络。网络 10 可经由以太网 16、路由器 18 以及陆线 20 连接至个人计算机 12 和计算机终端 14。另一方面,网络 10 可经由无线通信站 26 和无线链路 28 被无线连接至膝上型计算机 22 和个人数字助理 24。类似地,服务器 30 可使用通信链路 32 连接至网络 10,而大型机 34 可使用另一通信链路 36 连接至网络 10。

[0019] 图 2 示出可连接至网络 10 且可用于实现动态软件供应系统的一个或多个组件的计算机 110 形式的计算设备。计算机 110 的组件可包括,但不限于,处理单元 120、系统存储器 130 和将包括系统存储器在内的各种系统组件耦合至处理单元 120 的系统总线 121。系统总线 121 可以是若干类型的总线结构中的任一种,包括存储器总线或存储器控制器、外围总线和使用各种总线体系结构中的任一种的局部总线。作为示例,而非限制,这样的体系结构包括工业标准体系结构(ISA)总线、微通道体系结构(MCA)总线、扩展的 ISA(EISA)总线、视频电子技术标准协会(VESA)局部总线 and 外围部件互连(PCI)总线(也被称为 Mezzanine 总线)。

[0020] 隔离计算环境 125 可存储程序和数据并引起对其的执行。隔离计算环境 125 可被部署和配置成实施计算机 110 的用户与对计算机 110 有利害关系的服务供应商之间的协议条款。

[0021] 可使用一种以上的方式来实例化隔离计算环境 125。当由一个或多个离散组件实现时,隔离计算环境 125 可被设置在计算机的主板上。主板可以是适用于给定应用的任何电路互连和组件安装基础技术,且范围可从玻璃纤维材料至铸模环氧树脂、聚酯薄膜、陶瓷等。当隔离计算环境 125 被设置在主板上或主板中时,隔离计算环境 125 可使用环氧树脂来涂敷或被埋在互连层或组件之下。涂敷或掩埋隔离计算环境 125 可用于增加移除或篡改隔离计算环境 125 本身、至隔离计算环境 125 的相关联电源和接地连接、或至隔离计算环境 125 的数据和地址连接的难度。理想上,移除或去除隔离计算环境 125 会对主板和 / 或周围组件造成持久的损害,并致使计算机 110 不可操作。

[0022] 或者,隔离计算环境 125 可被包括在处理单元 120 中,从而提供对处理单元寄存器和数据总线(未示出)的更好访问。隔离计算环境 125 也可由外设主存或例如由操作系统使用软件来模拟。此外,它可薄如软件模块之间的常规边界。显然,隔离计算环境 125 抵抗攻击的能力受到主存环境强度的限制。

[0023] 计算机 110 通常包括各种计算机可读介质。计算机可读介质可以是能够被计算机 110 访问的任何可用介质,且包括易失性和非易失性介质、可移动和不可移动介质。作为示例,而非限制,计算机可读介质可以包括计算机存储介质和通信介质。计算机存储介质包括以任何方法或技术实现的用于存储诸如计算机可读指令、数据结构、程序模块或其它数据等信息的易失性和非易失性、可移动和不可移动介质。计算机存储介质包括,但不限于,RAM、ROM、EEPROM、闪存或其它存储器技术、CD-ROM、数字多功能盘(DVD)或其它光盘存储、磁带盒、磁带、磁盘存储或其它磁性存储设备、或能用于存储所需信息且可以由计算机 110 访问的任何其它介质。通信介质通常具体化为诸如载波或其它传输机制等已调制数据信号中的计算机可读指令、数据结构、程序模块或其它数据,且包含任何信息传递介质。术语“已调制数据信号”指的是这样一种信号,其一个或多个特征以在信号中编码信息的方式被设定或更改。作为示例,而非限制,通信介质包括有线介质,诸如有线网络或直接线连接,以及无线介质,诸如声学、射频、红外线和其它无线介质。上述中任一个的组合也应包括在计算机可读介质的范围之内。

[0024] 系统存储器 130 包括易失性和 / 或非易失性存储器形式的计算机存储介质,诸如只读存储器(ROM) 131 和随机存取存储器(RAM) 132。基本输入 / 输出系统 133(BIOS) 包含有助于诸如启动时在计算机 110 中的元件之间传递信息的基本例程,它通常存储在 ROM131 中。RAM132 通常包含处理单元 120 可以立即访问和 / 或目前正在操作的数据和 / 或程序模块。作为示例,而非限制,图 2 示出了操作系统 134、应用程序 135、其它程序模块 136 和程序数据 137。

[0025] 计算机 110 也可以包括其它可移动 / 不可移动、易失性 / 非易失性计算机存储介质。仅作为示例,图 2 示出了从不可移动、非易失性磁介质中读取或向其写入的硬盘驱动器 141,从可移动、非易失性磁盘 152 中读取或向其写入的磁盘驱动器 151,以及从诸如 CD ROM 或其它光学介质等可移动、非易失性光盘 156 中读取或向其写入的光盘驱动器 155。可以在示例性操作环境下使用的其它可移动 / 不可移动、易失性 / 非易失性计算机存储介质包括,但不限于,盒式磁带、闪存卡、数字多功能盘、数字录像带、固态 RAM、固态 ROM 等。硬盘驱动器 141 通常由诸如接口 140 等不可移动存储器接口连接至系统总线 121,磁盘驱动器 151 和光盘驱动器 155 通常由诸如接口 150 等可移动存储器接口连接至系统总线 121。

[0026] 以上描述和在图 2 中示出的驱动器及其相关联的计算机存储介质为计算机 110 提供了对计算机可读指令、数据结构、程序模块和其它数据的存储。例如,在图 2 中,硬盘驱动器 141 被示为存储操作系统 144、应用程序 145、其它程序模块 146 和程序数据 147。注意,这些组件可以与操作系统 134、应用程序 135、其它程序模块 136 和程序数据 137 相同或不同。操作系统 144、应用程序 145、其它程序模块 146 和程序数据 147 在这里被标注了不同的标号是为了说明至少它们是不同的副本。用户可以通过输入设备,诸如键盘 162 和定点设备 161(通常指鼠标、跟踪球或触摸垫)向计算机 20 输入命令和信息。其它输入设备(未示出)可以包括麦克风、操纵杆、游戏垫、圆盘式卫星天线、扫描仪等。这些和其它输入设备通常由耦合至系统总线的用户输入接口 160 连接至处理单元 120,但也可以由诸如并行端口、游戏端口或通用串行总线(USB)等其它接口或总线结构连接。监视器 191 或其它类型的显示设备也经由诸如图形处理单元 190 的接口连接至系统总线 121。除监视器以外,计算机也可以包括用于连接诸如打印机 196 和扬声器 197 等其它外围输出设备的输出外围接口 195。

[0027] 计算机 110 可使用至一台或多台远程计算机,诸如远程计算机 180 的逻辑连接在网络化环境下操作。远程计算机 180 可以是个人计算机、服务器、路由器、网络 PC、对等设备或其它常见网络节点,且通常包括以上相对于计算机 110 描述的许多或所有元件,尽管在图 2 中只示出存储器存储设备 181。图 2 中所示逻辑连接包括局域网(LAN)171 和广域网(WAN)173,但也可以包括其它网络。这样的连网环境在办公室、企业范围计算机网络、内联网和因特网中是常见的。

[0028] 当在 LAN 连网环境中使用时,计算机 110 通过网络接口或适配器 170 连接至 LAN171。当在 WAN 连网环境中使用时,计算机 110 通常包括调制解调器 172 或用于通过诸如因特网等 WAN173 建立通信的其它装置。调制解调器 172 可以是内置或外置的,它可以通过用户输入接口 160 或其它合适的机制连接至系统总线 121。在网络化环境中,相对于计算机 110 所描述的程序模块或其部分可以存储在远程存储器存储设备中。作为示例,而非限制,图 2 示出了远程应用程序 185 驻留在存储器设备 181 上。可以理解,所示网络连接是示例性的,可使用在计算机之间建立通信链路的其它手段。

[0029] 隔离计算环境可以是以上介绍的隔离计算环境 125 或与其类似。隔离计算环境 125 可包括存储器、逻辑电路和时钟或定时器,例如定时器可用于通过对实时间间隔计数来实现时钟。存储器可包括易失性和非易失性存储器。隔离计算环境还可包括数字签名验证电路。当需要对外部实体的单向验证,例如对服务器(未示出)的验证时,随机数生成器可以是数字签名验证电路的一部分。数字签名技术是公知的,并且散列、签名验证、对称和非对称算法及其相应的密钥将不在此处详细讨论。对隔离计算环境的详细描述在美国专利申请第 11/022,493 号中给出,该申请通过引用包含在此。从安全性角度来看,理想的隔离计算环境提供仅可经由所主存的应用程序或逻辑提供的良好定义的接口来访问的计算环境。具体地,任何其它一方,包括对手,仅可经由这些接口来与主存隔离计算环境的逻辑交互。

[0030] 图 3 示出显示输出控制器 192 与计算机 110 中后文中被称为 CPU/ 主板 124 的其它功能组件之间的逻辑关系的计算机 110 的示例性实施例。输出控制器 192 可以是图形处理单元 190、输出外围接口 195、或其它接口设备。代表性的输出设备 210 可以是任何相应的设备,诸如显示器/监视器、扬声器、打印机等。CPU/ 主板 124 上特别关注的是处理单元、

隔离计算环境 125、系统存储器 130、以及网络接口 170。

[0031] CPU/ 主板 124 可包括隔离计算环境 125 和保持输出控制器设备驱动程序 202 和输出存储器 204 的存储器。当输出控制器 192 是图形处理单元 190 时,输出存储器 204 可以是图像存储器缓冲区。输出控制器设备驱动程序 202 可以是使来自活动程序的一般显示指令适应于所安装的特定输出控制器 192 所期望的特定格式和协议的软件例程。不同品牌和型号的输出控制器 192 可能需要不同的协议和数据格式。从而,输出控制器设备驱动程序 202 可对每一品牌 / 型号的输出控制器有所不同。输出存储器 204 是对诸如显示图形等程序数据 137 的方便描述,尤其是可与任何数目的应用程序和实用程序 134、135、136 相关联的静态图像,但也可包括所生成的图形图像。

[0032] 图 3 中所述的输出控制器 192 可包括输出存储器 206,在图形处理单元的情况中,存储器可以是能够由图形处理单元处理器(未示出)写入同时由输出电路(未示出)读取的双端口存储器。输出控制器 192 可包括由输出控制器 192 支持并包含 在其中的隔离计算环境 208,如将在以下更详细描述。隔离计算环境 208 可包括安全存储器 210 来提供对密钥、证书、散列码等的可信存储。

[0033] 如上所述,可能存在两个隔离计算环境。第一个控制状态和使用度量,第二个关于输出信道支持第一个,且可被主存在输出控制器 192 中。在某些情况中,隔离计算环境的这两个实例可由同一硬件物理主存。

[0034] 输出控制器 192 可由如上所述的主系统总线 121 耦合至 CPU/ 主板 124。逻辑上,CPU/ 主板 124 的隔离计算环境 125 可通过系统总线 121 上的安全信道 212 被耦合至输出控制器 192 的隔离计算环境 208。对安全信道 212 的使用可允许两个隔离计算环境 125、208 彼此认证,然后在一个实施例使用本领域中已知的 Diffie-Hellman 密钥交换所生成的会话密钥来通信。对会话密钥的使用允许在相互认证的端点,如隔离计算环境 125、208 之间进行加密数据的高速通信。将在以下更详细地描述对安全通道通信的应用。

[0035] 在操作中,隔离计算环境 125 可用于确定计算机何时运行在完全操作模式或制裁模式中。如在以上引用的美国专利申请中所述的,值可被存储在隔离计算环境 125 中,并且随着计算机的使用而递增地消费。在一个替换实施例中,隔离计算环境可在特定的一段时间内,例如一个历月内监视使用。当时间期限的值被耗尽时,隔离计算环境 125 可向处理单元 120 发送信号以限制计算机的功能。这可包括减慢处理速度、限制可访问的存储器量等。隔离计算环境 125 也可干预来禁用连网能力。隔离计算环境 125 结合处理单元 120 可仅允许某些授权的程序执行。这些选项中某一些可能具有不期望的副作用,例如减缓处理器可引起存储器访问和外围接口的定时问题,或者禁用联网能力可限制用户对计算机 110 充值或重新启用的能力。

[0036] 实行制裁的另一替换是 CPU/ 主板 124 的隔离计算环境 125 建立与图形处理单元 190 的隔离计算环境 208 的通信。隔离计算环境 125 在认证步骤之后可向隔离计算环境 208 指示,计算机 110 正在制裁模式中操作。隔离计算环境 208 然后可干预输出控制器 192 的正常操作,例如阻止输出信号到达其相应的输出。

[0037] 当处于制裁模式操作中时,可在允许输出存储器 206 中的数据输出至例如监视器 191 之前检查该数据。或者,可在将表示图形图像的数据写入输出存储器 206 之前检查该数据。例如,可在将表示图形图像的数据写至输出存储器 206 之前检查该数据。当检查输出

数据时,可采用若干种方法。总体上,检查数据来确定它是否与被授权在特定操作模式,例如制裁模式操作或待机操作期间执行的程序相关联。使用图形控制器 191 作为示例,通过仅显示与制裁模式操作相关联的图形,可有效地将计算机 110 仅限于被预定对充值或重新激活计算机 110 有用的那些应用程序或实用程序的操作,或者对诊断和维护有用的那些应用程序或实用程序的操作。屏蔽输出图形可避免使用以上列出的其它制裁措施及其变型,它们通常是不期望或不可预测、具有副作用的。

[0038] 总而言之,输出控制器 192 可确认输出数据或媒体是否匹配执行模式。输出控制器 192 可仅当对计算机 110 的给定操作模式允许输出时才传输输出。输出数据或媒体可使用例如数字签名等已知机制来标识。限定(qualification)元数据可附加于输出数据或媒体,或被单独提供给输出控制器 190。限定元数据可由计算机供应商或服务供应商数字地签署。

[0039] 尽管输出控制器的主要选择可以是提供或阻断输出信号,但存在其它选择。例如,图形控制器 191 可按照某种方式使输出退化而非阻断图形输出。例如,当处于受限模式中时,可单色或添加噪声地呈现显示。类似地,声音控制器可对音频信号限制带宽。

[0040] 当输出控制器 192 是图形处理单元 190 时,可进行特别的考虑以适应用户与所显示的图像的可能的交互。为了允许定位文本和提示,并为了允许输入字符,由散列签名验证的所显示图像的区域可具有良好定义的排除区或“断口(cut-out)”。对断口的使用允许所显示图形的一部分具有有用交互所需的某一程度的可变性,并仍允许关于非断口区进行认证。为此,与所显示的图像相关联的经签署或认证的元数据被用于限定可对所显示的图像进行认证的存储器的范围。通过本质上指定图像的像素范围,可容纳为输入或其它非固定数据保留的区域同时保持限定输出信号的好处。输出信号的限定将在以下更详细描述。

[0041] 除图形处理单元 190 的情况以外,可考虑若干特定情况。为了减轻简单替换图形处理单元 190 的攻击,图形处理单元 190 可被“锚定”至计算机 110,即密码绑定至处理单元 120 或主板 124 的隔离计算环境 125(见相关申请 11/039,165,为所有目的通过引用该申请将其包含在此)。减轻“替换”攻击的另一方法是对输出图形的全部或部分加密。因此,使用不能够解密或具有错误密钥的替换处理单元进行的攻击将不会响应输出图形信号。

[0042] 减轻旁路输出控制器 192 攻击的另一方式是通过使计算机 ICE 125 在引导期间认证并枚举所有设备。这包括密钥交换等。结果,进行攻击的替换输出控制器 192 将不能被认证,从而不能对发送给输出控制器 192 的信号和数据解密。此外,可通过消除或破坏计算机 110 与输出控制器 192 的隔离计算环境 208 之间的通信来攻击该模型。可通过采用心跳形式的方案,并加密和/或数字签署(使用在制造和/或引导期间在两个隔离计算环境 125、208 之间交换的密钥)通信来减轻这些攻击。如果输出控制器 192 的隔离计算环境 208 怀疑通信受到攻击,则它可对隔离计算环境 125 一起应用严厉的限制。类似地,计算机隔离计算环境 125 可一并限制、制裁或停止计算机。

[0043] 对输出图形还要考虑的另一个区域是授权图形的窗口边界区域。为了减轻扩大或使用窗口边界的攻击,可使用在制裁模式中使用的固定窗口边界来对图形处理单元 190 编程。扩大该模型的灵活性,可将图形控制器 191 编程为允许足够窄且暗淡的边界,例如具有例如不宽于 3 像素的一致宽度,且具有一致的颜色。如此定义之后,攻击者使用边界可获取的功能非常有限。

[0044] 参考图 4, 讨论并描述了操作计算机的方法。计算机 110 的操作模式可涉及已经讨论的若干替换, 例如完全功能模式或制裁模式。当处于完全功能模式中时, 计算机 110 可提供对用户正常可用的所有服务和实用程序的访问, 而当处于制裁模式中时, 仅有受限的集合可用。或者, 计算机 110 可处于操作状态或待机状态中。在操作状态中可对计算机 110 进行计量, 例如对于预付时间限制的消费使用, 而在待机状态中, 计量可被挂起。在制裁模式中是否对计算机 110 进行计量是商业决策。在任何情况下, 无论是确定完全 / 制裁模式还是操作 / 待机状态, 方案提供者, 例如因特网服务供应商可对度量的准确性和作为度量结果采取的措施两者具有直接利益。

[0045] 如图 4 中所示, 输出控制器 192 可等待来自设备驱动程序 202 的数据 (302)。输出控制器 192 可接收指示计算机当前操作模式, 例如完全 / 制裁操作或操作 / 待机的信号 (304)。此时 CPU/ 主板 124 的隔离计算环境 125 可与输出控制器的隔离计算环境 208 建立安全通信信道 212。使用安全通信信道 212, 隔离计算环境 125 可传输模式信息以及必要时的更新的签名或散列信息。隔离计算环境 208 可能不能直接访问外部主机, 因此隔离计算环境 125 可以是用于与散列、证书、新 / 更新的可允许输出信号和新 / 更新的操作模式有关的主要更新模式。数据可由任何可信源提供, 例如输出控制器固件更新可来自制造商而不是服务供应商。当 304 处没有接收到指示新模式的任何信号时, 操作使用当前模式继续。输出设备 190 可接收包括预期输出的数据的输出信号 (306)。预期的输出可以是面向用户的, 诸如视觉、听觉或触觉的。数据也可预期用作非用户输出, 诸如打印机或传真机。使用来自框 304 的最后设置, 输出控制器 192 可确定输出信号何时与计算机 110 的操作模式一致。

[0046] 为了确定与操作模式的一致性, 输出控制器 192 可在将信号输出给适当的输出设备之前验证输出信号的数字签名。输出信号既可包括最终输出的数据又可包括指示输出信号的本质和输出信号的可兼容模式的标记。例如, 输出信号可以是付费屏幕, 也可包含与“断口”有关的标记, 且输出信号与制裁模式操作兼容。输出信号, 包括标记在内, 可被数字地签署。验证数字签名在本领域中是已知的, 简要地, 可使用已知、可信实体所拥有的秘密密钥对输出信号的适当部分的散列加密。隔离计算环境 208 然后可使用其自己的密钥对散列解密, 并将其与隔离计算环境 208 计算出的散列进行比较。该密钥可以导出对称密钥, 或可以是公钥技术密钥对, 这两者在本领域中均已知。

[0047] 用于确定输出信号何时与操作模式一致的类似替换使用输出信号的散列验证。在该实施例中, 已知输出信号的散列被预载到隔离计算环境 208 的安全存储器 210 中。当接收到输出信号 (306) 时, 隔离计算环境 208 计算指定数据范围的输出信号的散列。范围信息可伴随散列或输出信号, 因为结果 (得到的散列) 是已知的。当隔离计算环境 208 计算出的散列与预存的散列匹配时, 可使用查找表或类似方案来确定输出信号与当前模式的兼容性。

[0048] 经签署的数据与散列匹配均得到可为与当前操作模式的一致性而进行匹配的经验证的输出信号。经确认的输出信号可与相应模式匹配, 例如受限或待机模式。未确认输出信号在制裁模式中可能不被允许。从而, 未确认输出信号可被阻止呈现给输出设备。或者, 可向输出设备呈现替代信号, 例如指示原始输出被阻断并建议接下来的步骤的消息。在又一替换中, 可将输出信号的退化形式呈现给输出设备。当计算机 110 处于待机模式中, 即不被计量, 且接收了不能确认的输出信号时, 未确认输出信号可被呈现给适当的输出设备。

此外,信号可从隔离计算环境 208 发送到隔离计算环境 125,指示呈现了未确认的输出。隔离计算环境 125 然后可评估是否要返回至操作模式并重新启动计量。

[0049] 计算上可能难以标识潜在取得遵循执行模式的资格的窗口。一个选择是蛮力,即图形控制器 190 可采用某种试探法来定位预期窗口的开始处并自此执行测量过程。

[0050] 更有效的模型是使操作系统 134 向图形控制器 190 提供关于假定对执行模式合格的窗口 / 框架 / 窗口小部件的位置的暗示。只要图形控制器 190 使用该信息作为暗示,而不代替验证来使用它,即可维持安全模型。该暗示允许图形控制器 190 关注于具有潜在兴趣的区域。该模型取决于图形控制器 190 是可疑的合理假设,并仅允许限定的窗口 / 框架 / 窗口小部件呈现到屏幕。类似地,如果决定了计量决策,即仅当图形处理器 190 确定所显示的所有信息不需要计量时,它才向计算机 110 或计量电路(未示出)发出不要计量的信号。

[0051] 可通过允许在制裁模式中维持后台来优化用户体验。即,图形控制器 190 将不会接受新的未限定的窗口 / 框架 / 窗口小部件,但将允许之前所显示的转入制裁模式。

[0052] 尽管前述文字描述了本发明的各个不同实施例的详细描述,但应理解,本发明的范围由本发明所附权利要求书的文字定义。该详细描述应被解释为仅是示例性的,且不描述本发明的每个可能的实施例,因为描述每个可能的实施例即使不是不可能也是不实际的。可使用当前的技术或在本专利的申请日之后开发的技术来实现众多替换实施例,它们仍落入定义本发明的权利要求书的范围之内。

[0053] 因此,可对此处描述并示出的技术和结构进行各种修改和变化,而不背离本发明的精神和范围。从而,应理解,此处所述的方法和装置仅是说明性的,而不限定本发明的范围。

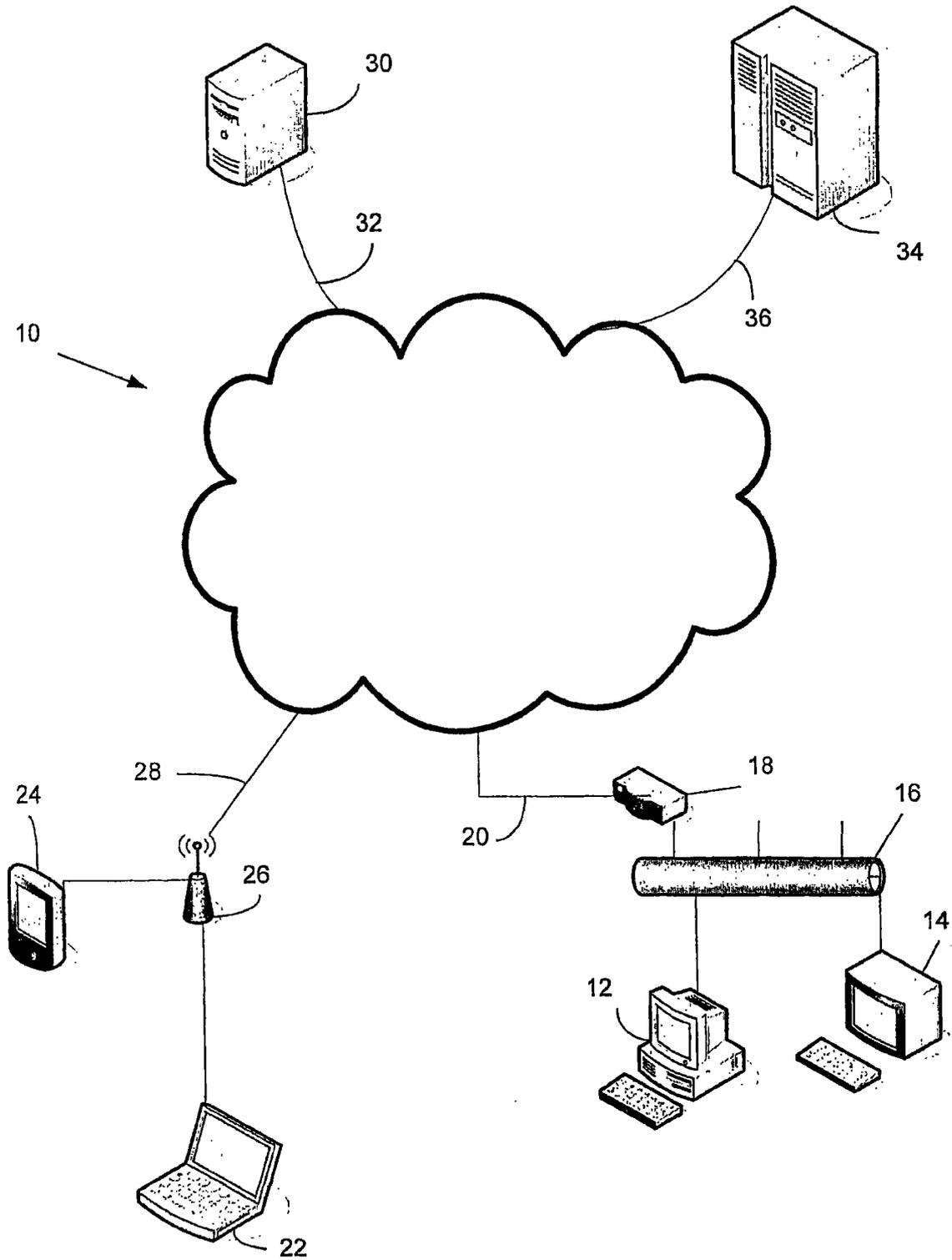


图 1

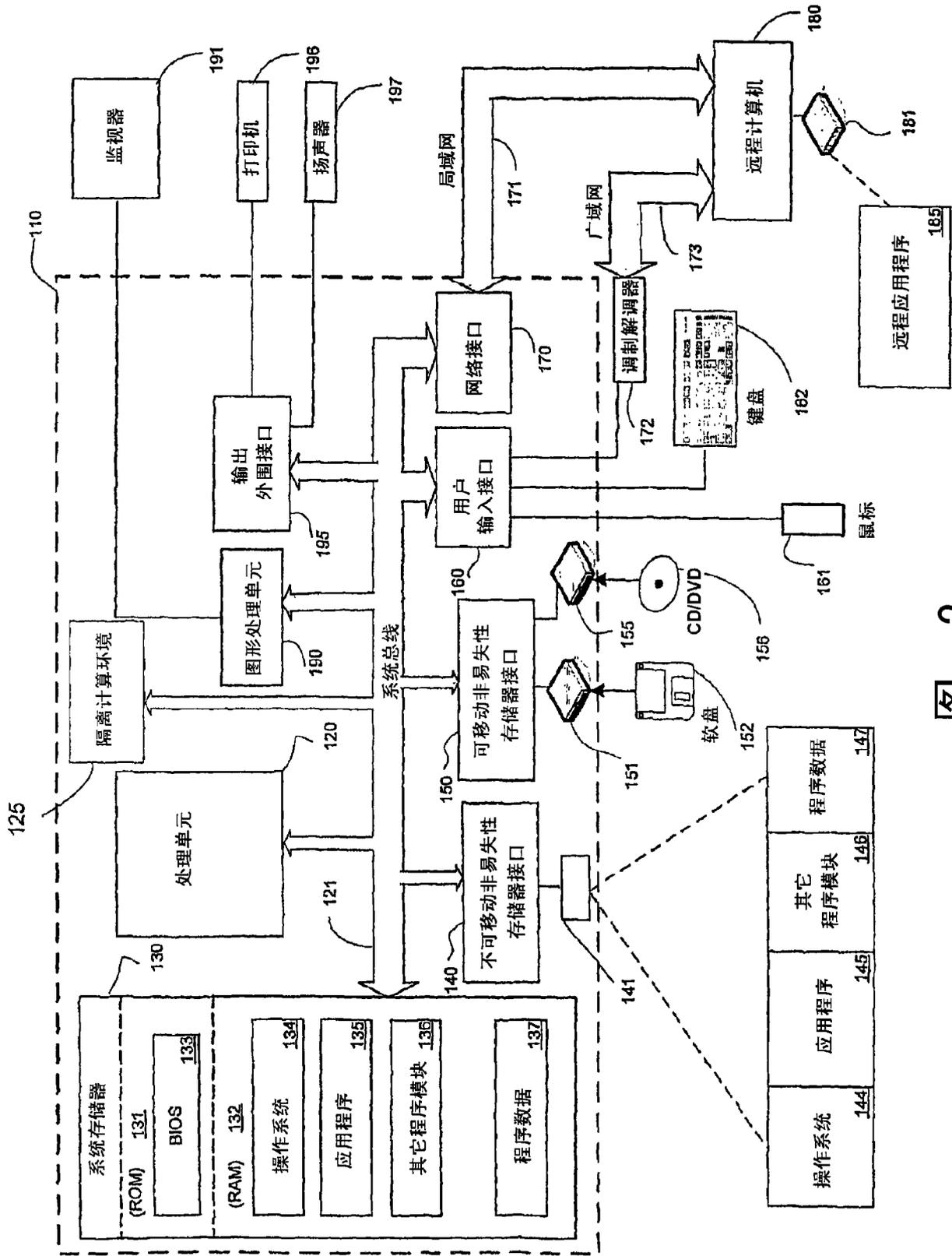


图 2

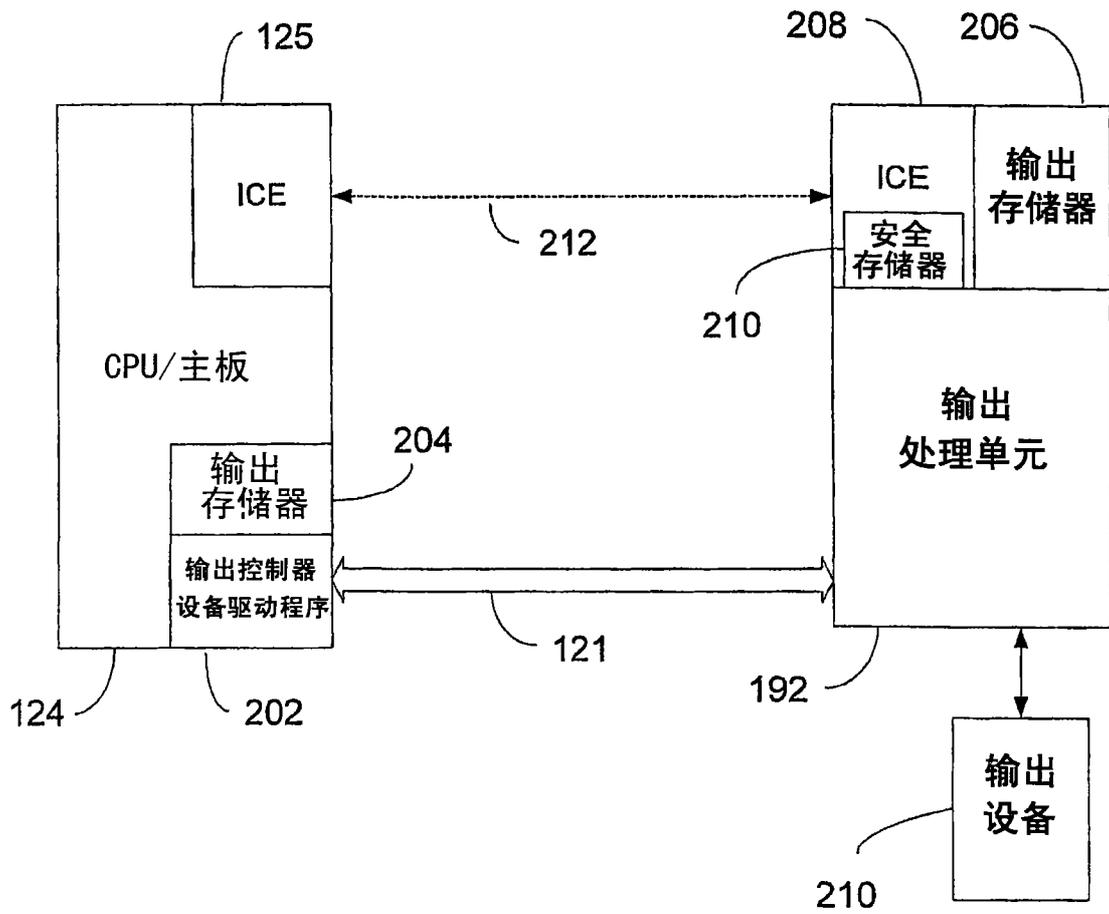


图 3

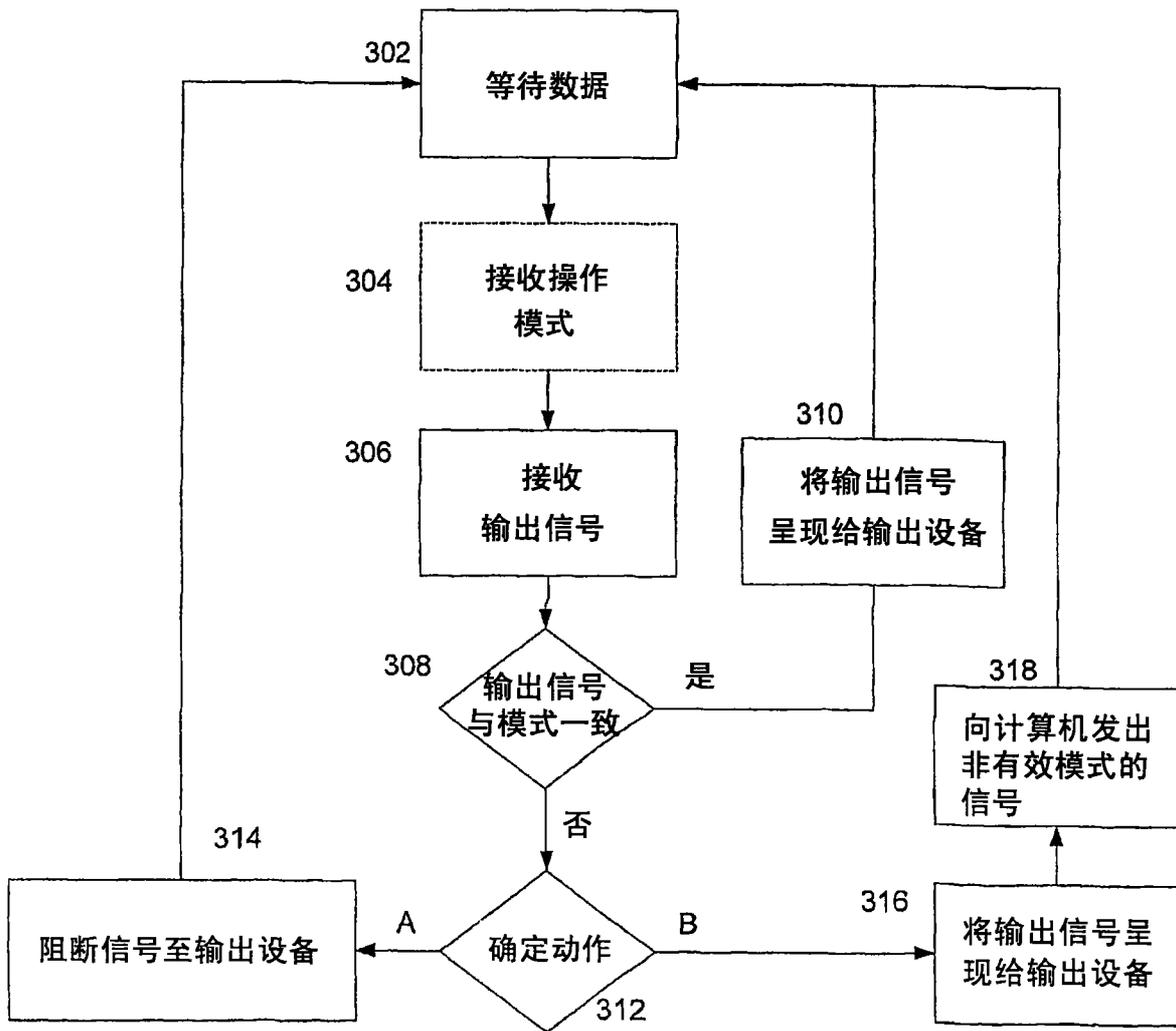


图 4