[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 15/18 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200580040764.2

[43] 公开日 2008 年 1 月 30 日

[11] 公开号 CN 101116070A

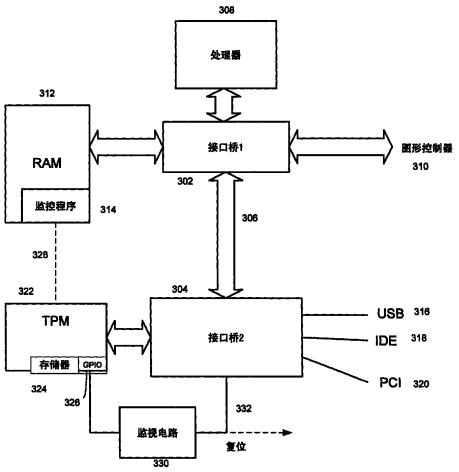
[22] 申请日 2005.12.20
[21] 申请号 200580040764.2
[30] 优先权
[32] 2004.12.23 [33] US [31] 11/021,021
[86] 国际申请 PCT/US2005/046091 2005.12.20
[87] 国际公布 WO2006/071630 英 2006.7.6
[85] 进入国家阶段日期 2007.5.28
[71] 申请人 微软公司
地址 美国华盛顿州
[72] 发明人 A·法兰克 P·英格兰
[74] 专利代理机构 上海专利商标事务所有限公司
代理人 顾嘉运
权利要求书 2 页 说明书 11 页 附图 7 页

[54] 发明名称

使用监控程序将 TPM 总是锁定为“开”的系统和方法

[57] 摘要

一种可通过包括用于验证已知监控程序的可信环境来保护免受攻击的计算机。该监控程序可用于确定计算机的状态是否遵循一组条件。这些条件可与使用条款有关，诸如可供按使用付费的信用、或计算机正运行诸如病毒保护等某些软件、或未附加未经授权的外设、或提供了所需令牌。该监控程序可直接或通过可信环境向监视电路发送信号。当未在给定超时期限内接收到该信号时，该监视电路干扰计算机的使用。



1．一种实现用于强制监控程序的操作的可信计算基础的计算机，所述计算机包括：

执行所述监视程序的处理器；

耦合至所述处理器以便确保所述监控程序的执行的可信环境，所述可信环境适用于从所述监控程序接收消息；

耦合至所述可信环境的监视电路，所述监视电路在一期限之后干扰所述计算机，除非所述可信环境在所述期限内接收到所述消息。

2．如权利要求 1 所述的计算机，其特征在于，所述可信环境密码地标识所述监控程序。

3．如权利要求 2 所述的计算机，其特征在于，所述可信环境还包括通用输入/输出端口，且所述监控程序在被密码地标识之后可访问所述通用输入/输出端口。

4．如权利要求 1 所述的计算机，其特征在于，所述监视电路还包括用于确定所述期限的计时器，且其中所述监视电路接收已签署的重启信号以便当所述已签署重启信号被验证时重启所述计时器。

5．如权利要求 1 所述的计算机，其特征在于，所述可信环境经由专用通信线路耦合至所述监视电路。

6．如权利要求 1 所述的计算机，其特征在于，所述监视电路当干扰所述计算机时使所述计算机重新引导。

7．如权利要求 6 所述的计算机，其特征在于，使所述计算机重新引导的信号承载于一导体上，所述导体适用于抗篡改。

8．如权利要求 1 所述的计算机，其特征在于，所述监控程序结合发送消息至少一次验证令牌。

9．如权利要求 9 所述的计算机，其特征在于，所述令牌包括供所述监控程序用于确定所述监控程序是否是当前版本的版本号。

10．一种激励计算机中的已知操作状态的方法，包括：

执行一已知监控程序；

从所述已知监控程序向一监视电路发送信号；以及

响应于所述信号防止所述监视电路干扰所述计算机的操作。

11．如权利要求 10 所述的方法，其特征在于，还包括验证所述已知监控程序的真实性。

12．如权利要求 10 所述的方法，其特征在于，所述从监控程序发送信号还包括，在向所述监视电路发送所述信号之前从所述监控程序向一可信环境发送所述信号。

13．如权利要求 10 所述的方法，其特征在于，还包括：

签署所述信号，且所述监视器验证所述信号的真实性。

14．如权利要求 10 所述的方法，其特征在于，还包括：

当未在预定时间内接收到所述信号时，干扰所述计算机的操作。

15．一种供计算机中使用的监视电路，包括：

用于确定时间期限的计时器；

用于接收重启所述计时器的信号的输入；以及

用于当在所述时间期限中未接收到所述信号时干扰所述计算机的操作的输出。

16．如权利要求 15 所述的监视电路，其特征在于，还包括密码能力，其中所述信号被数字签署，且所述密码电路确定所述信号的真实性。

17．如权利要求 15 所述的监视电路，其特征在于，所述输入被耦合至一可信环境。

18．如权利要求 17 所述的监视电路，其特征在于，所述可信环境控制至所述监视电路的所述信号。

19．如权利要求 15 所述的监视电路，其特征在于，所述输出被耦合至复位电路和总线驱动器电路之一。

20．如权利要求 15 所述的监视电路，其特征在于，所述监视电路以限制对所述计时器、所述输入和所述输出之一的访问的方式被设置在所述计算机中。

使用监控程序将 TPM 总是锁定为“开”的系统和方法

背景

供诸如个人计算机等计算设备中使用的可信平台模块（TPM）是已知的。TPM 的目的在于提供计算机身份和与交易、应用程序和媒体的许可、保护用户数据以及特殊功能有关的安全服务。

可信平台模块可在市场上出售，例如一 TPM 出自 STM microelectronics，即 ST19WP18 模块。TPM 存储密钥，然后使用那些密钥来认证应用程序、BIOS 信息、或身份。然而，对 TPM 的使用是自愿的，且根据目前和预期的标准和实现，它不能用于在计算设备上强加条件。某些商业模型假定计算机超出计算机所有者/供应商的直接控制之外，例如按使用付费（pay-per-use）商业模型。在这样的情况中，TPM 服务有可能被规避，且如果发生规避，则可能对商业带来不期望的负面影响。

概述

一种可信平台模块（TPM）可用于认证在计算设备上强制条件的监控程序。注入或写入 TPM 的所有者密钥可用于要求由所有者批准的监控程序是可操作的。进而，所批准的监控程序能够经由监控程序的经认证的状态来访问 TPM 的资源。TPM 的这一安全资源可以是例如通用输入/输出（GPIO）端口。简单的监视计时器可被配制成以定时的间隔对计算机复位，除非该监视计时器该在间隔期内由使用 GPIO 接收到的信号重启。

通过以这种方式配置计算机，TPM 可用于帮助确保已知监控程序正在运行，且监视计时器可用于帮助确保监控程序或 TPM 中的任何一个未被禁用或篡改。

附图简述

图 1 是互联多个计算资源的网络的框图；

图 2 是表示根据本发明的实施例的计算机的简化、代表性的框图；

图 3 是示出图 2 的计算机内的功能层的分层表示的简化、代表性的框图；

图 4 是图 2 的计算机的计算机体系结构的简化、代表性的框图；

图 5 是图 2 的计算机的替换计算机体系结构的简化、代表性的框图；

图 6 是 TPM 的简化、代表性的框图；以及

图 7 是示出使用监控程序锁定 TPM 的方法的流程图。

详细描述

尽管以下文字阐明了各种不同实施例的详细描述，但应理解，该描述的合法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，而不是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现实的。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，它们仍落入本发明的范围之内。

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”或类似语句在本发明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，除非权利要求元素通过叙述单词“指的是”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 35 U.S.C. § 112 第 6 段的应用来解释。

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而生成这样的软件指令和程序。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。

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 可经由以太网连接 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，大型机34可使用另一通信链路36被连接至网络10。

图2示出计算机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）局部总线和外围部件互连（PCI）总线（也被称为Mezzanine总线）。

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、RF、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。

系统存储器130包括易失性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中元件之间传递信息的基本例程，它通常存储在ROM 131中。RAM 132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1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。

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1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。

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 1 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。阴极射线管 191 或其它类型的显示设备也经由诸如视频接口 190 的接口连接至系统总线 121。除监视器以外，计算机也可以包括其它外围输出设备，诸如扬声器 197 和打印机 196，它们可以通过输出外围接口 190 连接。

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 1 中只示出存储器存储设备 181。图 1 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。

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 LAN 171。当在 WAN 网络环境中使用时，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 WAN 173 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 1 示出了远程应用程序 185 驻留在存储器设备 181 上。

通信连接 170、172 允许设备与其它设备通信。通信连接 170、172 是通信介质的示例。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、RF、红外线和其它无线介质。计算机可读介质可包括存储介质和通信介质两者。

将在以下更详细描述的可信平台模块 125 或其它可信环境可存储数据以及密钥，并验证可执行代码和数据。可信平台模块规范在章节 4.5.2.1 中有陈述：“作为系统初始化的一部分，将进行对平台组件和配置的测量。进行测量将不会检测出不安全的配置，也不会采取措施来阻止初始化过程的继续。这种责任归于诸如操作系统等合适的基准监控程序。”。因为 TPM 未被定义为强制工具，因此以下所述的进一步增强对常见的 TPM 进行了补充。

监视电路 126 可被配置成测量时间期限，且当时间期满时触发干扰计算机 110 的操作的信号 127。干扰可以是使计算机 110 重新引导的系统复位。干扰可中断系统总线 121 或外围总线上的数据。为防止监视器 126 干扰计算机 110 的操作，可能要求通信连接 128 上的信号对时间期限复位并再次启动定时过程。如图 2 中所示，监视计时器复位信号可承载于通信连接 128 上。如将在以下更详细描述的，TPM 125 可响应于来自监控程序的信号来启动监视计时器的复位。以下所述的步骤可用于帮助确保存在特定的、所需的监控程序且该程序通过使用 TPM 125 和监视电路 126 的组合正在操作中。

讨论并描述了图 3，它是示出诸如图 2 的代表性计算机内的功能层的分层表示的简化的框图。可信平台模块 202 可以是驻留在基本输入/输出结构（BIOS）204 下方的硬件。TPM 202 可用作计算机和更高层操作，诸如 BIOS 204 的资源。BIOS 可激活监控程序 206。监控程序驻留在监控程序层 210 处，在操作系统 208 下方。监控程序 206 可访问并使用 TPM 202 的资源以实现与更高层实体的操作相关联的策略。操作系统 208 支持计算机 110 的主要功能，且可以负责（在初始程序引导过程移交控制之后）通信、用户输入/输出、磁盘和其它存储器访问、应用程序启动

等。操作系统也可直接访问和使用 TPM 202。如图所示，第一和第二应用程序 212、214 可在操作系统 208 上运行。在某些情况中，监控程序可强制与操作系统 208 和应用程序 212、214 有关的策略。例如，在应用程序 214 可从磁盘 216 启动之前，由线 218 所示，操作系统可检查许可状态以确定应用程序 214 是否满足启动的给定准则。启动的准则以及随后使用监控程序函数对应用程序的计量在于 2004 年 12 月 8 日提交的代理案卷号为 30835/40476 的美国专利申请“Method for Pay-As-You-Go Computer and Dynamic Differential Pricing”中有更详细讨论。简要地，例如在按使用付费或预付情形中，监控程序 206 可用于测量和计量应用程序、实用程序和计算机资源。

简要地参考图 6，将更详细地描述 TPM 202。TPM 202 可具有包括易失性和非易失性存储器两者的内部存储器 502，其中至少一部分没有遭受篡改或未经授权的写操作的危险。存储器可为配置 TPM 202 起见并为建立对外部实体的信任，存储供确认声称与所有者有联系的实体使用的所有者密钥 504。存储器可也包括平台配置寄存器（PCR）506 等。PCR 506 可用于存储与监控程序 206 相关联的散列或其它强（strong）标识符。TPM 202 还可包括时钟 508 和密码服务 510。这两者均可在如将在以下更详细描述的认证和授权过程中使用。TPM 202 还可包括总线 512，它有时被称为单引脚总线或通用输入/输出（GPIO）。在一个实施例中，GPIO 512 可被耦合至如在别处所描述的监视电路。

TPM 202 也可被耦合至通用总线 514 用于计算机内的数据通信，例如运行监控程序 206 的进程。使用总线 514，或在某些情况中的另一机制 516，TPM 202 能够测量监控程序。对监控程序的测量可包括检查监控程序的密码散列，即检查由监控程序所占用的存储器范围的散列。PCR 可用于存储测量数据 506。所有者密钥 504 可例如通过要求所有者密钥 504 来确认的监控程序的数字签署的散列来与监控程序 506 的散列建立联系。所有者密钥 504 可在制造时或稍后例如递送给顾客时被写入或注入到 TPM 202 内。所有者密钥 504 然后用于认证监控程序 206。

在一个示例性实施例中，监控程序 206 由引导序列中它之前的可信模块，例如由 BIOS 测量。监控程序度量，诸如由 BIOS 204 计算出的散列，可经由总线 514 被存储在 TPM PCR 506 中。当 TPM 202 确认该度量（散列）时，TPM 202 然后可允许访问分配给监控程序 206 并存储在 TPM 202 中的监视程序 206 的唯一密钥和/或其它机密。TPM 202 将向任何监控程序分配与监控程序的度量所匹配的任何度量相对应的密钥和机密。

可使用所有者密钥 504 和相应的监控程序度量 506，即已知监控程序 206 的散列来对 TPM 编程。所有者密钥被用于对监控程序度量 506 编程或更新，使得仅拥有所有者密钥 504 的实体可为已知监控程序 206 设置 PCR 寄存器 506。标准的 TPM 202 具有仅针对给定度量 506 验证的监控程序 206 可控制 GPIO 512 的特征。当 GPIO 512 以防篡改的方式连接至监视电路 126 时，可完成信任链。即，仅经验证的监控程序 206 可控制 GPIO 512，且仅 GPIO 512 可用于重启监视电路 126。从而，尽管监控程序 206 可被替换或更改，但仅由所有者密钥 506 设置的 PCR 506 验证的监控程序 206 可用于重启监视电路 126 的计时器。因此，仅经授权的监控程序可用于防止监视器例如通过对计算机 110 复位来干扰计算机 110。监视电路 126 的计时器可被置为被选来允许还原经破坏或篡改的计算机 110，但足够短来防止大量有用的工作在计算机 110 上完成的期限。例如，监视器可被置为除非由经确认的监控程序 206 重启，否则每隔 10-20 分钟即干扰计算机 110。

所有者密钥 504 和监控程序度量 506 可在安全制造环境中被编程，或可使用对所有者密钥 504 编程的实体所知的传输密钥来现场编程。一旦所有者密钥 504 已知，编程实体，例如服务供应商可设置监控程序的度量，它将确定哪一监控程序能访问 GPIO 总线。可能需要所有者密钥 504 来对所有者密钥重新编程。对所得密钥的使用可便于密钥分发、定标（scaling）以及针对万一本地所有者密钥 504 被泄漏时可能遭受的广泛损失的保护。密钥管理技术在数据安全领域中是已知的。

图 4 是与计算机 110 相同或类似的计算机 300 的代表性体系结构的框图。该计算机可具有第一和第二接口桥 302、304。接口桥 302、304 可由高速总线 306 连接。第一接口桥 302 可连接至处理器 308、图形控制器 310 和存储器 312。存储器 312 可主存监控程序 314、以及其它通用存储器使用。

第二接口桥 304 可连接至外围总线和组件，例如通用串行总线（USB）316、集成驱动器电子设备（IDE）318、或外围部件互连（PCI）320，用于连接磁盘驱动器、打印机、扫描仪等。第二接口桥也可连接至 TPM 322。如上所述，TPM 322 可具有用于密钥和散列数据的安全存储器 324、以及通用输入/输出（GPIO）326。TPM 322 可由连接 328 物理上或逻辑上耦合至监控程序。如上所述，BIOS 204 可测量监控程序 206，并在 TPM 322 中存储度量，这向监控程序 314 分配对应于所提供的度量的密钥和机密。监控程序 314 从而被给予对使用这些密钥和机密锁定的资源和数据的访问权。为向监视电路 330 发送信号，连接 328 也可由监控程序使用来控制 GPIO 326。该信号可使监视器复位。当监视电路 330 在由监视电路 330 中

的设定所规定的时间期限内未接收到该信号时，可经由连接 332 发送复位或其它干扰信号。为了防止篡改，GPIO 326 与监视电路 330 之间的连接可例如通过在电路板层之间密封或布线以防止对监视电路 330 的手动重启来保护。可类似地针对篡改保护计算机复位信号连接 332，或监视电路 330 与主处理器计算机复位点（未示出）之间的复位信号连接 332 的至少一部分。

图 5 是图 2 的计算机的替换体系结构的代表性框图。与图 4 的描述相比，同样标号的组件是相同的。监视电路 330 被移至第二接口桥 304 内，示出监视电路 330 可如何组合到另一电路内以改进抗篡改能力的代表性图示。监视电路 330 与第二接口桥芯片 304 的集成尽管本身是适当的，但仅是说明性的。由于第二接口桥 304 是计算机体系结构的一个主要组件，因此所需级别的干扰可从第二接口桥 304 之内实现。从而，可能不需要从监视电路外部到第二接口桥 304 的连接，诸如连接 332。

在该替换体系结构中，GPIO 326 可能未被用于向监视电路 330 发送复位信号。相反，可经由直接从监控程序 314 到监视电路 330 的逻辑连接 334 发送消息。

因为在两个实体（314、330）之间可能不存在足够的信任级别，因此消息可使用 TPM 322 中所保存的密钥来签署。例如，这些密钥可在第一引导（例如，在生产线上，为可信度起见）期间与监控程序 314 相关联。密钥可被任意分配，或如上所述密钥可从主密钥和诸如根证书、序列号或制造序号等已知数据中导出。监视计时器 330 可被配置成仅与例如在装配线上的计算机 110 的第一引导期间使用这些密钥在签署的消息有关。此外，监控程序将这些密钥锁入 TPM 332 内，使得仅同样测量的监控程序 314 可访问这些密钥。该体系结构的变型是监控程序依赖于 TPM 332 来向其分配对其度量而言唯一且相应的这些密钥。

在正常操作期间，监控程序 314 可请求 TPM 322 代其对要发送给监视计时器 330 的消息进行签署。TPM 332 使用对应于监控程序 314 的密钥（按照在每一引导期间由 BIOS 存储到 TPM 322 内的其度量）来签署消息。监控程序 314 可经由例如连接 328 的逻辑连接从 TPM 322 接收已签署消息，然后经由逻辑连接 334 将其提供给监视电路 330。

当监视电路 330 接收到该消息时，监视电路 330 可使用密钥（在制造期间设置）以认证该消息。或者，它可使用逻辑连接 336 请求使用 TPM 322 中的密钥或密码来验证。如果另一监控程序正在运行，则它会不同地测量，得到由 TPM 分配的不同的密钥和机密。从而，替换监控程序将不能够正确签署该消息，以使它将由

监视电路 330 认证。因此，监视电路 330 将启动制裁（sanction），诸如当计算机 110 的定时间隔期满之后激发其复位。对已签署或加密消息的使用可减少对逻辑连接 328 和 334 的攻击的几率。

讨论并描述了图 7，它是示出使用监控程序将可信平台模块（TPM）总是锁定为“开”的方法的流程图。典型的 TPM，例如 TPM 125 可任选地由用户启用。如下所述，该方法将帮助确保 TPM 125 仍被启用，并且由企业所有者选择的监控程序 206 将被执行，但是冒了诸如禁用计算机 110 等制裁的风险。

在开始 402 处以通电开始，计算机 110 可通过正常的引导机制启动各种硬件组件。这也适用于 TPM 322。引导序列可遵循可信计算平台联盟（TCPA）方法。用于测量的核心信任根（CRTM）测量 BIOS 133 并将其度量存储到 TPM 322 内（403）。然后，CRTM 加载并执行 BIOS 133。（CRTM 理想上可被存储在计算机 110 中非常难以攻击的可信位置中。）

BIOS 133 可按照常规方式执行，从而启动并列举各种计算机组件，只有一个例外——它可在加载并执行每一软件模块之前对其进行测量。而且，它可将这些度量存储到 TPM 322 内。具体地，它可测量监控程序 314 并将监控程序度量存储到 TPM 322 内（405）。

TPM 322 将密钥和机密唯一且相应地分配给监控程序度量。要点在于，TPM 322 始终如一地分配对应于给定度量的唯一密钥和机密（408）。因此，监控程序 314 可用的密码是唯一、一致且相应的。结果是，任何监控程序可锁定资源，使其仅对该特定的监控程序独占地可用。例如，这允许通过仅关于与真实监控程序 314 相关联的度量对连接至监视电路 330 的 GPIO 326 编程而将真实的监控程序 314 链接至监视电路 330。GPIO 326 则仅对与真实监控程序 314 相同地测量的监控程序可用。

不考虑所加载的监控程序真实与否，引导序列加载并执行监控程序（410）。正常的引导过程可继续（411），并假定成功的引导，之后是计算机 110 的正常操作（412）。

一旦监控程序 314 在 410 处被加载并执行之后，它启动其循环（413-419）。首先，监控程序 314 经由 TPM GPIO 326 向监视电路 330 发送消息（413）。该消息可用信号通知 TPM 322 使用 GPIO 326 来发信号通知监视电路 330 重启其计时器（未示出）。

当向 TPM 322 发送消息之后，监控程序返回其测试状态 414。监控程序可测

试计算机 110 的状态是否遵循当前策略。当前策略可涉及已知程序、实用程序或外设的特定的存在与否。测试也可与计量或其它按使用付费度量有关。例如，测试可检查可供消费的可用供应包与特定的应用程序操作之间的关系。在另一实施例中，测试可与诸如日历月等特定时间期限期间的操作有关。

当测试 414 失败时，可跟随否分支（416），在那里监控程序根据策略行动。动作可以仅是发送给操作系统的警告代码或呈现给用户的警告消息。动作可以是对操作系统和用户施加的某些制裁，例如限制或消除计算机的某一功能。这可应用于硬件和/或软件功能。例如，可减慢计算机、可禁用某些软件、或可禁用某些设备，例如网络摄像头。更严厉的制裁可以是限制 OS 可用的 RAM 的量，或减少操作系统可用的指令集体系结构。在一个示例性实施例中，当找到不遵循条件时监控程序 314 可用的一个行动过程可以是不采取措施来重启监视电路 330 的计时器而令监视电路 330 施加制裁。

当测试成功时，可跟随是分支（414）。在任一情况中，执行在返回到步骤 413 之前等待一间隔（419）。等待间隔避免了因反复运行监视程序 314 而耗尽计算机的资源。显然，该等待间隔 419 应是监视计时器计数期限的某一部分。可用部分的确定可以是计算机正常操作将延迟循环执行完成的可能性。然后循环返回至上述步骤 413。重复循环的周期可被置为小于监视电路超时期限的任何时间，否则将出现不期望的干扰。

当 TPM 322 接收到消息（420）时，TPM 322 根据监控程序度量行动。如果度量被认为是非真实失败（420），则将采用否分支至框 422，在那里不采取任何动作，即不发送到监视电路 330 的信号。TPM 322 不需要任何其它动作，因为监视电路 330 将干扰计算机 110，除非采取步骤来停止。可任选地，TPM 322 在 422 处可生成用于日志记录的出错、生成警告/出错代码、通知操作系统以及可向用户显示消息。

当 TPM 322 验证监控程序度量真实时，可激活 GPIO 326 来用信号通知监视电路 330 重启其计时器（424）。如上所述，重启监视电路计时器防止监视电路 330 启动干扰动作，诸如对计算机 110 的复位。监视电路 330 然后可将计时器复位为其初始值（426）。计时器然后可计数（428）并测试预定时间是否期满（430）。计时器期限是可设定的。计时器实现是已知的，且计时器是数到给定数字、减至 0、数到设定时钟时间、还是其它机制均是设计选择。

如果计时器未期满，则可从 430 采用返回到 428 的否分支，这将对计时器进

行另一次计数。当时间期满时，可从 430 采用是分支，监视器可通过干扰计算机（432）来实施制裁。干扰可以是系统复位、引起重新引导或对外设的禁用等。监视电路计时器递减计数至干扰432的期限可能足以允许用户纠正计算机110上的不遵循条件，但应足够频繁以限制计算机 110 上的可靠或有用活动。

从 432 到 426 的链接可以是概念上的。如果通过对整个计算机复位来实现干扰，则该链接是没有实际意义的。在更微小干扰的情况中，例如减缓计算机，该链接用于重启递减计数并可导致更严重的禁用干扰，例如引起复位。

可见可通过以上方法实现与按使用付费来供应计算机相关联的企业所有者或其它承保人的两个目的。首先，如果 TPM 322 因为用户选择不使用 TPM 322 或对计算机进行黑客攻击以禁用 TPM 322 而被禁用，则将不会生成至监视电路 330 的消息，且计算机 110 将被干扰。

类似地，如果 TPM 322 被启用并是可操作的，但监视程序被更改或替换，可能更改或忽略有效策略（例如，使用策略），则 TPM 将不会承兑监视程序的请求。实际上，经更改的监控程序度量不同于真实监控程序的度量。因此，当监控程序度量被存储到 TPM 322 内时，它将分配对该经更改的监控程序的相应且唯一的一组密钥和机密，这组密钥和机密不同于 GPIO 326 操作所需的那些。结果，从经更改的监控程序到 TPM 以向 GPIO 326 发送信号的任何消息将不会被承兑。从而，监视电路 330 将不会接收到重启信号，并且计算机 110 将被干扰。

在这两种情况中，TPM 322 必须被启用，且真实监控程序 314 必须就位且是可操作的以使计算机 110 正确操作。

可构想以上方法和装置的其它使用。例如，引导过程的一部分可要求经授权用户提供凭证。如果未提供正确的凭证，则引导过程可能不能加载真实的监控程序，这将最终导致对计算机 110 的禁用。

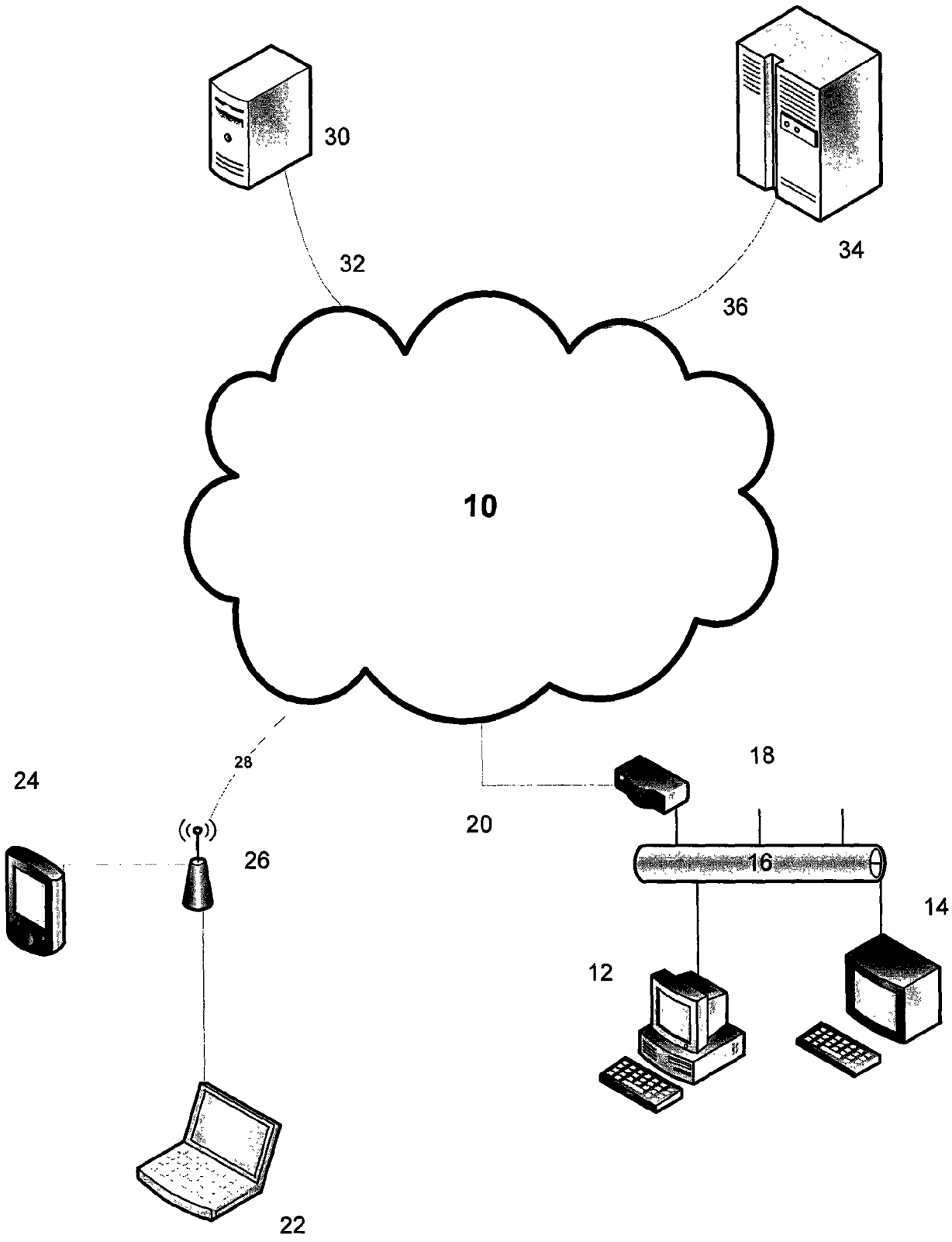


图 1

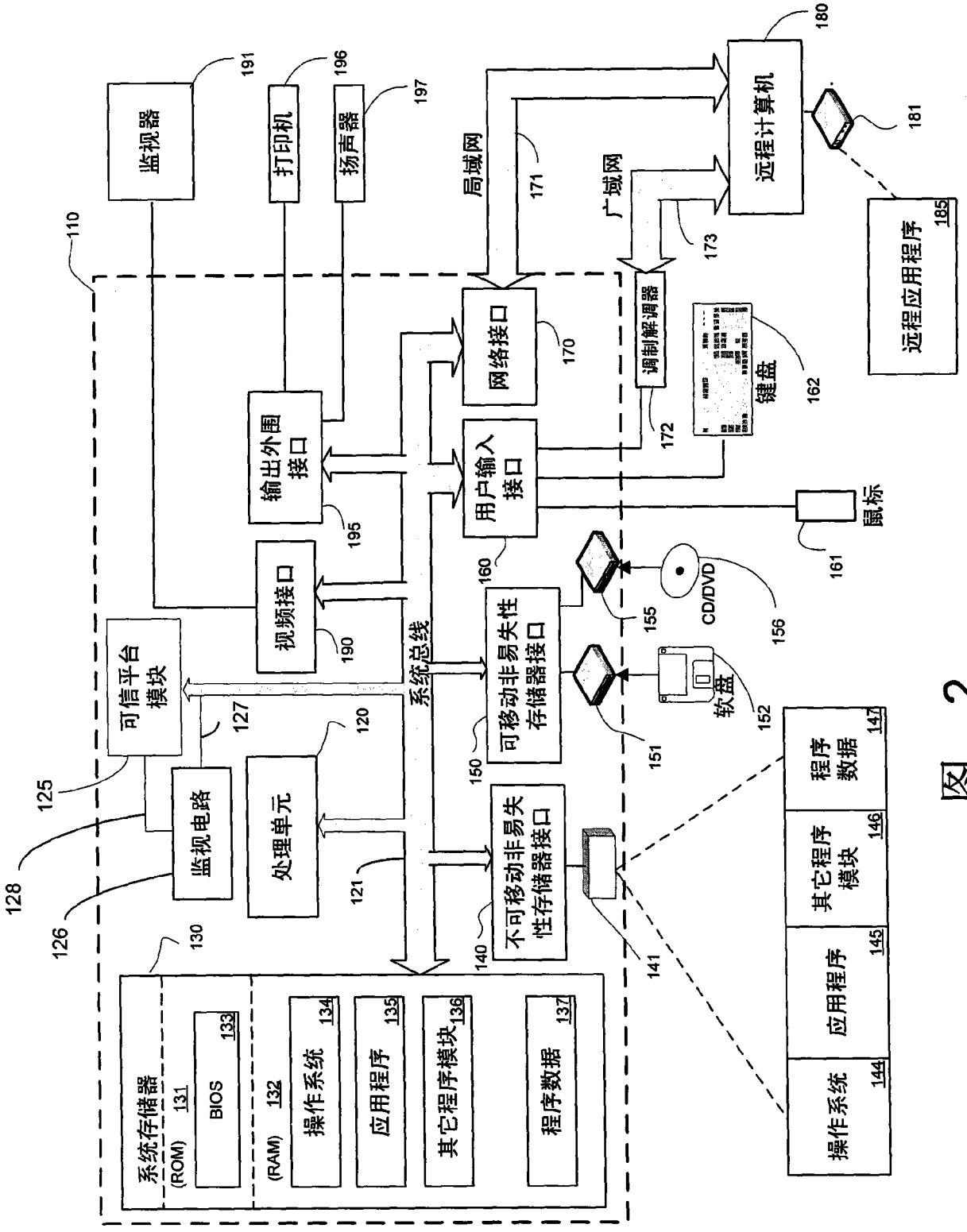

监视器
191
打印机
196
扬声器
197
局域网
171
广域网
173
远程计算机
180
181
远程应用程序
185
110
网络接口
170
调制解调器
172
键盘
162
输出外围接口
195
用户输入接口
160
鼠标
161
视频接口
190
系统总线
可信平台模块
125
127
处理单元
120
121
可移动非易失性存储器接口
150
155
CD/DVD
156
软盘
152
151
不可移动非易失性存储器接口
140
141
监视电路
128
126
130
系统存储器
(ROM) 131
BIOS 133
(RAM) 132
操作系统 134
应用程序 135
其它程序模块 136
程序数据 137
操作系统 144
应用程序 145
其它程序模块 146
程序数据 147

图 2

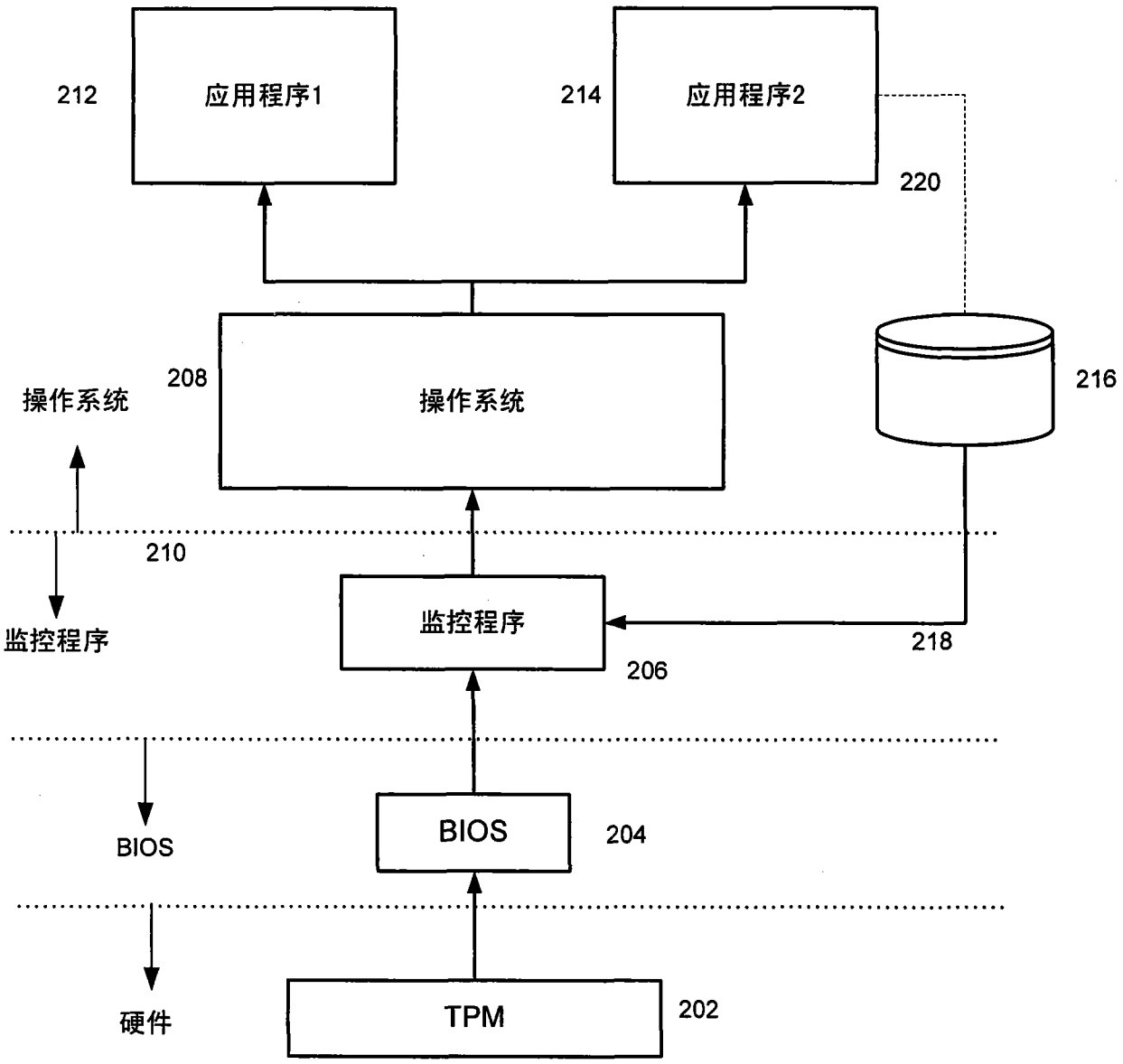

212
应用程序1
214
应用程序2
220
208
操作系统
操作系统
216
210
监控程序
监控程序
218
206
BIOS
BIOS
204
硬件
TPM
202

图 3

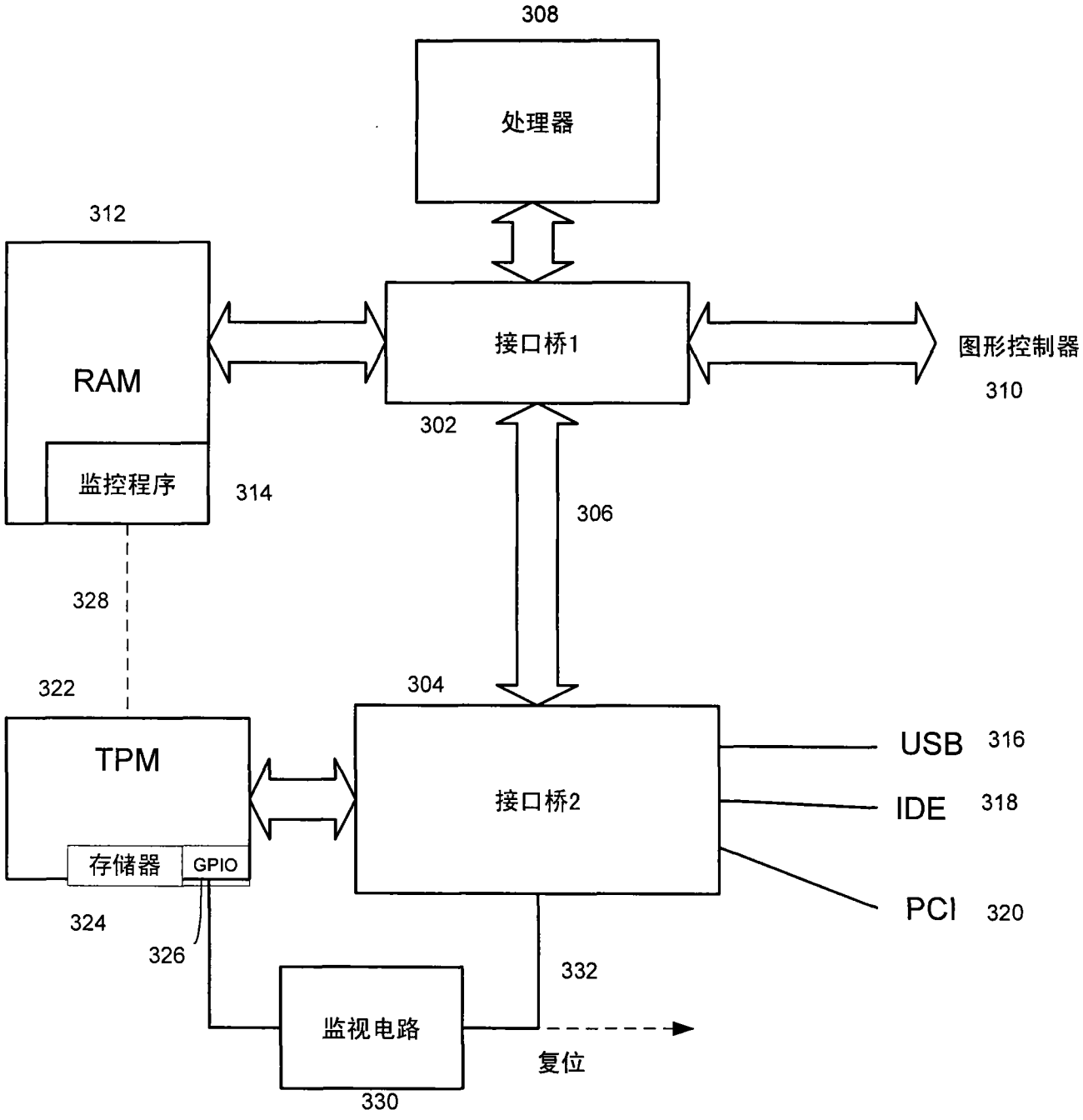

308
处理器
312
RAM
监控程序
314
接口桥1
302
图形控制器
310
306
328
322
304
TPM
存储器
GPIO
324
326
接口桥2
USB
316
IDE
318
PCI
320
332
监视电路
330
复位

图 4

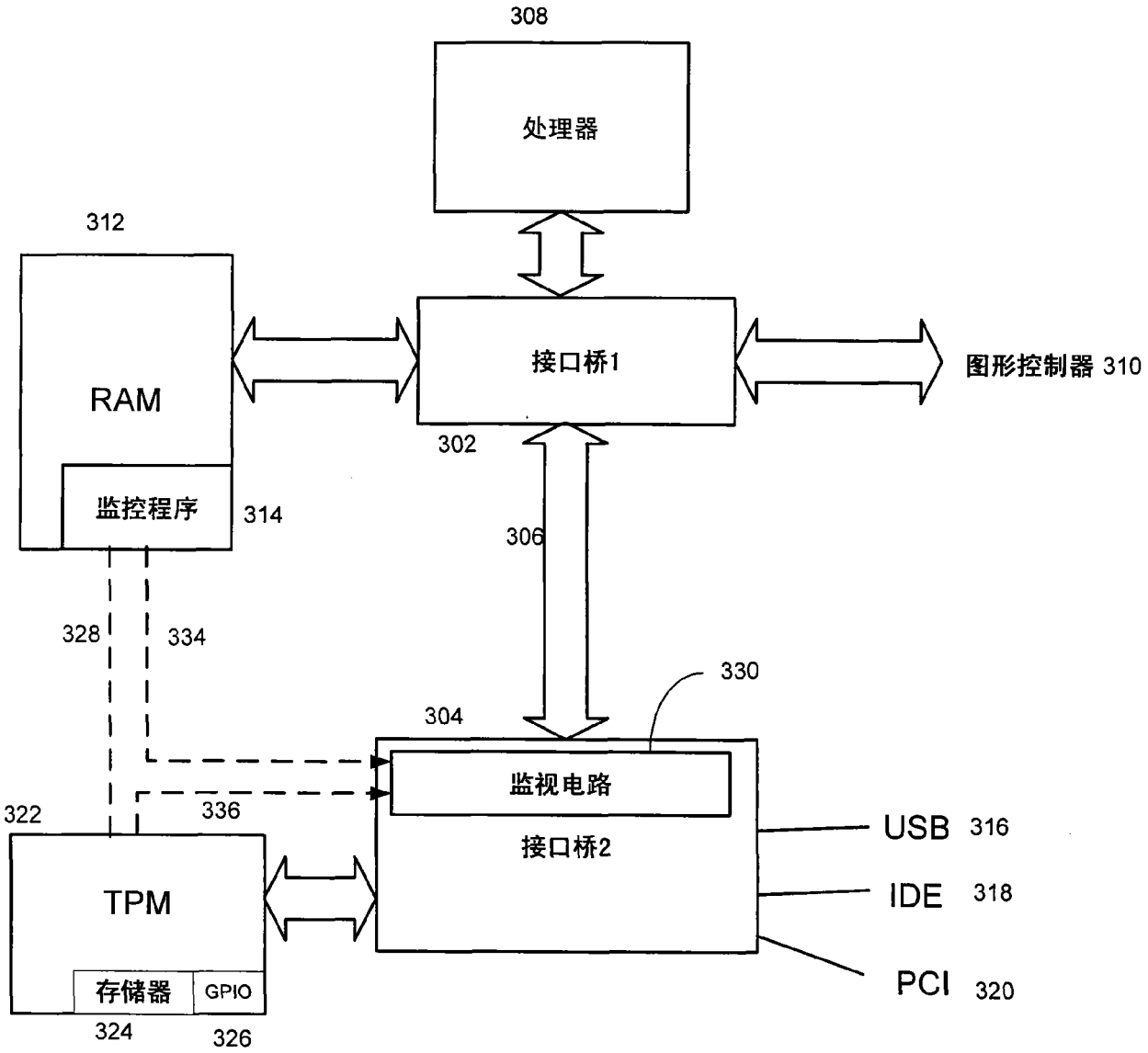

308
处理器
312
RAM
监控程序
314
接口桥1
图形控制器 310
302
306
328
334
330
304
监视电路
322
336
TPM
存储器
GPIO
324
326
接口桥2
USB 316
IDE 318
PCI 320

图 5

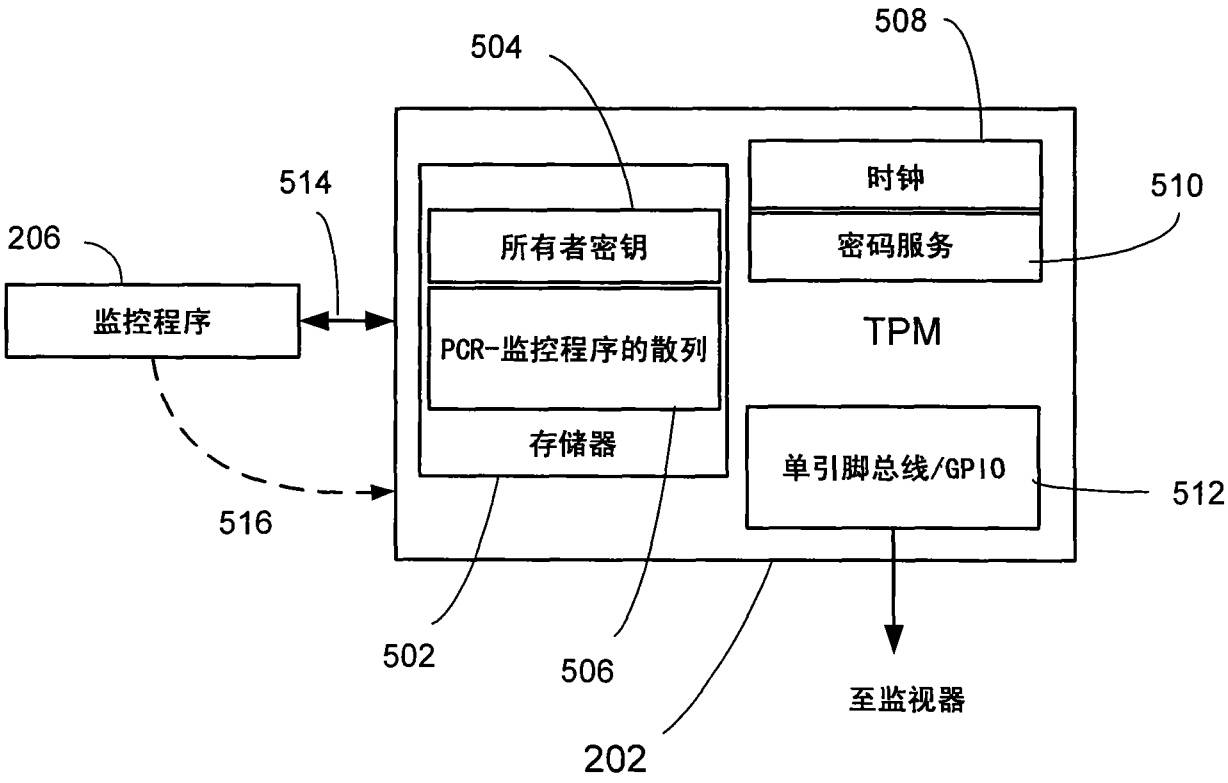

508
504
514
510
206
时钟
所有者密钥
密码服务
监控程序
PCR-监控程序的散列
TPM
存储器
单引脚总线/GPIO
512
516
502
506
至监视器
202

图 6

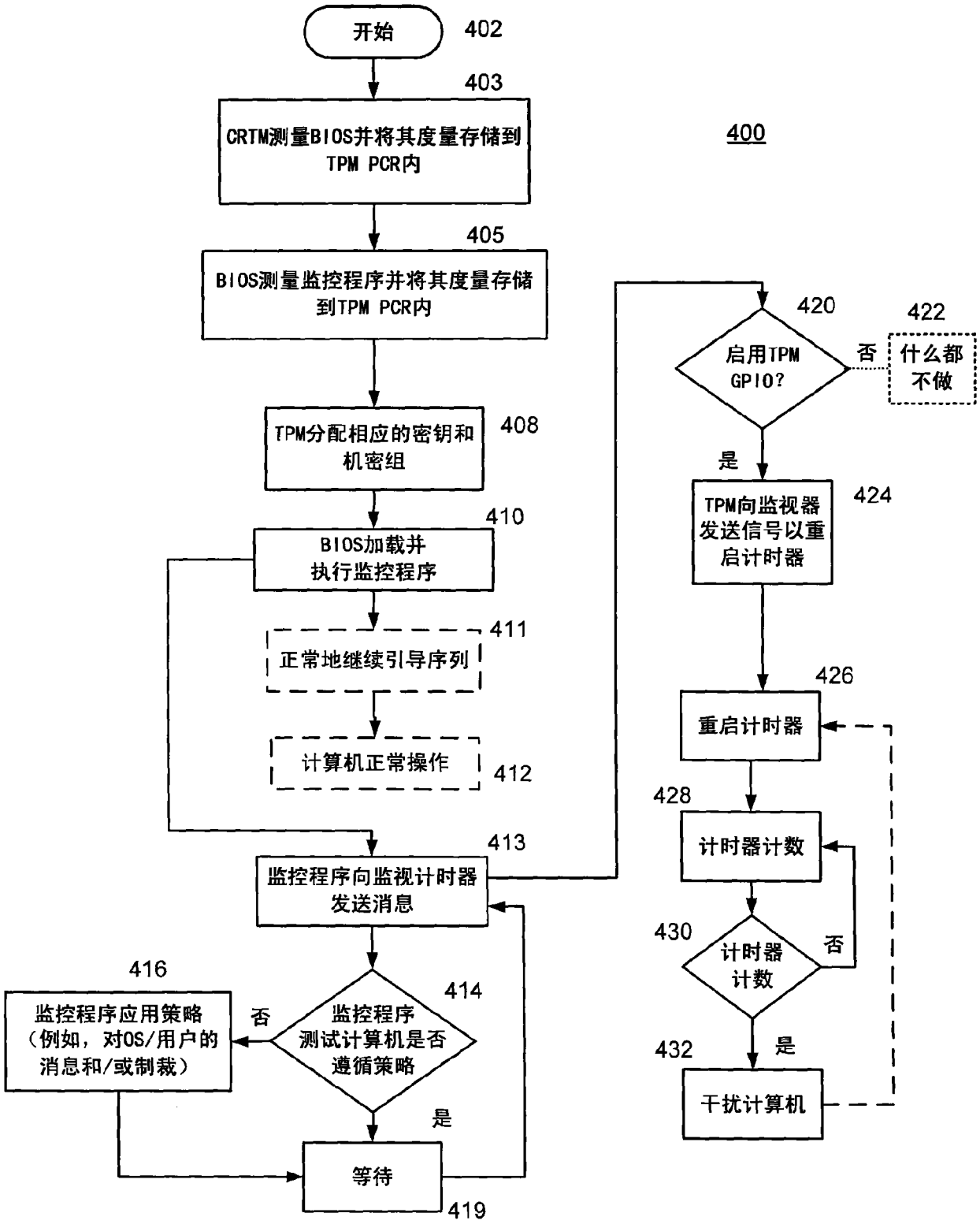

开始
402
403
CRTM测量BIOS并将其度量存储到TPM PCR内
400
405
BIOS测量监控程序并将其度量存储到TPM PCR内
TPM分配相应的密钥和机密组
408
410
BIOS加载并执行监控程序
411
正常地继续引导序列
计算机正常操作
412
413
监控程序向监视计时器发送消息
414
监控程序测试计算机是否遵循策略
否
416
监控程序应用策略（例如，对OS/用户的消息和/或制裁）
是
等待
419
420
启用TPM GPIO?
否
422
什么都不做
是
TPM向监视器发送信号以重启计时器
424
426
重启计时器
428
计时器计数
430
计时器计数
否
是
432
干扰计算机

图 7