(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 102934121 A
(43)申请公布日 2013.02.13

(21)申请号 201080067405.7
(22)申请日 2010.04.13
(85)PCT申请进入国家阶段日
2012.12.13
(86)PCT申请的申请数据
PCT/US2010/030944 2010.04.13
(87)PCT申请的公布数据
WO2011/129815 EN 2011.10.20
(71)申请人 惠普发展公司,有限责任合伙企业
地址 美国德克萨斯州
(72)发明人 L. 王 V. 阿利 J. 蒙香
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 段俊峰 王洪斌
(51)Int.Cl.
G06F 21/44(2013.01)
G06F 21/57(2013.01)

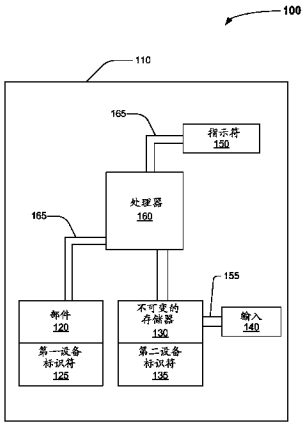
权利要求书 2 页 说明书 8 页 附图 4 页

(54)发明名称

安全系统和方法

(57)摘要

提供了安全方法。该方法可包括将置于部件(120)内的第一设备标识符(125)与置于不可变的存储器(130)内的第二设备标识符(135)相比较。该部件和该不可变的存储器可以至少部分地被置于电子设备(110)内。该方法可包括如果该第一设备标识符与该第二设备标识符相对应,则正常启动该电子设备。该方法可以进一步包括如果该第一设备标识符未能与该第二设备标识符相对应,则提供至少一个指示符(150)。还提供了安全系统。



CN 102934121 A

1. 一种安全方法，包括：

将置于部件（120）内的第一设备标识符（125）与置于不可改变的存储器（130）内的第二设备标识符（135）相比较；

其中该部件和该不可变的存储器至少部分地被置于电子设备（110）内；

如果该第一设备标识符与该第二设备标识符相对应，则正常启动该电子设备；以及

如果该第一设备标识符未能与该第二设备标识符相对应，则提供至少一个指示符（150）。

2. 权利要求 1 的方法，进一步包括：

如果该第一设备标识符（125）未能与该第二设备标识符（135）相对应，则在提供该至少一个指示符（150）之后，正常地启动该电子设备（110）。

3. 权利要求 1 的方法，进一步包括：

如果该第一设备标识符（125）未能与该第二设备标识符（135）相对应，则在提供该至少一个指示符（150）之后，禁止该电子设备（110）功能性的至少一部分；以及

启动该电子设备。

4. 权利要求 1 的方法，进一步包括：

在将该第一设备标识符与该第二设备标识符相比较之前通过将至少一个输入（140）提供到该电子设备，来激活安全测试模式。

5. 权利要求 1、2、3 或 4 的方法，其中该至少一个指示符（150）包括显示视觉信号。

6. 权利要求 1、2、3 或 4 的方法，其中该至少一个指示符（150）包括使可听信号发声。

7. 权利要求 4 的方法，其中将该至少一个输入（140）提供到该设备包括激活置于该电子设备的表面上的至少一个手动输入设备。

8. 权利要求 1、2、3 或 4 的方法，其中该至少一个指示符（150）包括生成射频信号。

9. 权利要求 1、2、3 或 4 的方法，其中该部件（120）从由以下组成的部件的组中选择：平台特定模块、时间特定模块、以及地理特定模块；以及

其中该不可变的存储器（130）包括基本输入 / 输出系统（"BIOS"）。

10. 权利要求 9 的方法，其中该平台特定模块包括可信平台模块（"TPM"）。

11. 权利要求 9 的方法，其中该地理特定模块包括可信密码模块（"TCM"）。

12. 一种系统（100），包括：

部件（120），包括第一设备标识符（125）；

不可变的存储器（130），包括第二设备标识符（135）；以及

算法，其当由该系统（100）执行时，将该第一设备标识符与该第二设备标识符相比较；以及

如果该第一设备标识符的至少一部分与该第二设备标识符的至少一部分相对应，则允许正常启动该系统（100）；以及

如果该第一设备标识符未能与该第二设备标识符相对应，则提供至少一个指示符（150）。

13. 权利要求 12 的系统，其中该不可变的存储器（130）和处理器（160）包括基本输入 / 输出系统（"BIOS"）。

14. 权利要求 12 或 13 的系统，其中该部件（120）从由以下组成的部件的组中选择：平

台特定模块、时间特定模块、以及地理特定模块。

15. 权利要求 14 的系统，其中该平台特定模块包括可信平台模块（"TPM"）。

16. 权利要求 14 的系统，其中该地理特定模块包括可信密码模块（"TCM"）。

17. 权利要求 12 的系统，其中该至少一个指示符（150）从由以下组成的指示符的组中选择：视觉信号、可听信号、和射频信号。

18. 权利要求 12 的系统，进一步包括至少一个输入（140），其被配置成发起由该处理器（160）执行该算法。

19. 权利要求 12、13 或 14 的系统，其中该部件（120）、不可变的存储器（130）和该处理器（160）至少部分地被置于电子设备（110）内；以及

其中该电子设备从由以下组成的电子设备的组中选择：膝上型计算机、便携式计算机、上网本计算机、板式计算机、个人数字助理、蜂窝式通信设备、以及手持游戏设备。

安全系统和方法

背景技术

[0001] 随着日益移动的世界范围的民众，计算设备频繁地在地球表面上被运输。当穿过安全检查点(例如在许多世界机场中发现的安全检查点)时，计算设备可能受到″加电″测试，以确定该设备实际上是计算设备，并且确定该计算设备是否包含合法的硬件、固件或软件。虽然这样的测试对检测伪造计算设备可以是有效的，但是它们经常不能够检测包含在该计算设备中的硬件、固件或软件是否已经被损害、改变或伪造。当计算设备内的一个或多个安全设备已经被损害、改变或移除时，该问题变得尤其尖锐。

附图说明

[0002] 一个或多个公开的实施例的优点可以在阅读以下详细描述时和参照附图时变得显而易见，其中：

图 1 是描绘了根据在此描述的一个或多个实施例的说明性安全系统的示意图；

图 2 是描绘了根据在此描述的一个或多个实施例的另一个说明性安全系统的示意图；

图 3 是描绘了根据在此描述的一个或多个实施例的说明性安全方法的流程图；以及

图 4 是描绘了根据在此描述的一个或多个实施例的另一个说明性安全方法的流程图。

具体实施方式

[0003] 随着置于日益移动的世界人口中的过多的便携式电子设备(诸如膝上型和便携式计算机)，便携式电子设备本身和包含在其中的数据的安全由于由这样的设备和它们包含的数据所带来的潜在安全威胁而已经受到增加的细查。虽然变化的测试方法已经被开发和采用，以检测伪造的、改变的或以其它方式损害的电子设备，但检测便携式电子设备是否已经被损害的简单的测试系统或方法将给安全人员提供检测和暂停这样的设备的运输的能力。为实现该任务，在此提供了在检测伪造的、改变的或以其它方式损害的电子设备时有用的安全系统。另外，在此还提供了在检测伪造的、改变的或以其它方式损害的电子设备时有用的安全方法。

[0004] 提供了安全方法。该方法可以包括将置于部件内的第一设备标识符与置于不可变的存储器内的第二设备标识符相比较。该部件和该不可变的存储器可以至少部分地被置于电子设备内。该方法可包括如果该第一设备标识符与该第二设备标识符相对应，则正常启动该电子设备。该方法可以进一步包括如果该第一设备标识符未能与该第二设备标识符相对应，则提供至少一个标记。

[0005] 还提供了安全系统。该系统可包括具有第一设备标识符的部件和具有第二设备标识符的不可变的存储器。该系统可以进一步包括算法，该算法当被系统执行时，可以将该第一安全设备标识符与第二安全设备标识符相比较。如果该第一设备标识符的至少一部分与该第二设备标识符的至少一部分相对应，则该系统可以正常启动。如果该第一设备标识符未能与该第二设备标识符相对应，则该系统可以提供至少一个指示符。

[0006] 现在参考图 1，提供了示例安全系统 100。该系统 100 可以包括电子设备 110，该

电子设备 110 具有至少部分地置于其内的部件 120、不可变的存储器 130、输入 140、指示符 150 和处理器 160。第一设备标识符 125 可以被至少部分地置于该部件 120 内。第二设备标识符 135 可以至少部分地置于该不可变的存储器 130 内。该电子设备 110 可以包括具有置于其中的列出的元件的至少一部分的任何设备。这样的电子设备可以包括但不限于：膝上型计算机、便携式计算机、上网本计算机、板式（slate）计算机、平板计算机、个人数字助理、蜂窝式通信设备、或手持游戏设备。

[0007] 部件 120 可以包括适合于提供、生成或存储唯一的第一设备标识符 125 的任何设备。在一些实施例中，该部件 120 可以包括不可分开地附着到该电子设备 110 的一个或多个设备，例如该部件 120 可包括一个或多个表面安装设备，例如直接焊接到至少部分地置于该电子设备 110 内的电路板的一个或多个设备。在一些实施例中，该部件 120 可以被不可分开地或以其它方式永久地附着到该电子设备 110 从而使得移除该部件 120 致使该电子设备不可操作。在其它实施例中，该部件 120 可以包括可分开地附着到该电子设备 110 的一个或多个设备，例如一个或多个插座安装设备。

[0008] 在一些实施例中，该部件 120 可以包括非易失性存储设备，诸如忆阻器、只读存储器（ROM）或闪存。该部件 120 可以包括一个或多个平台特定模块、一个或多个时间特定模块、一个或多个地理特定模块、或其任意组合。在一些实施例中，该部件 120 可以包括可信平台模块（"TPM"）、可信密码模块（"TCM"），或类似的安全设备。 在至少一些实施例中，该部件 120 可以通过一个或多个管道 165 被通信耦合到不可变的存储器 130 或处理器 160。

[0009] 如在此所使用的，术语＂耦合＂或＂耦合的＂或被称为在被＂耦合的＂状态中的部件可以指代任何形式的直接的、间接的、光学的或无线的电连接。在一个或多个实施例中，该电连接可以包括但不限于链接两个或更多个设备的任何导电连接或磁感应连接。该连接可以是导电的，例如使用诸如铜线或铝线、印刷电路板上的导电带等等的一个或多个导体来连接两个或更多个部件。该连接可以是磁感应的，例如通过使电流经过感应地耦合到次级线圈的初级线圈来从变压器次级线圈激发电流的流动。该连接可以是电磁的，例如通过控制电流经由独立的继电器线圈流过继电器触点，使得电流经过该继电器线圈可以磁性地打开和关闭该继电器触点。

[0010] 在部件 120 包括诸如 TPM 的平台特定模块的情况下，该 TPM 可包括符合由可信计算组所发布的最新近的 TPM 规范的任意数量的设备、系统或系统和设备的组合。在一些实施例中，哈希密钥摘要可以被置于该 TPM 的一部分内，以指示该电子设备 110 的＂制造时＂或＂初始配置时＂的硬件和软件配置。在一些实施例中，唯一的 RSA（加密密钥）可以在生产该电子设备 110 的时候被布置、存储或以其它方式嵌入在该 TPM 内。这样，在该部件 120 合并了 TPM 的情况下，采取一个或多个哈希密钥串、加密密钥、或其它类似的标识符的形式的第一设备标识符 125 可以不仅被用来唯一地区分特定的电子设备 110，而且在一些情况中还被用来唯一地区分该电子设备 110 的硬件、固件、和软件配置。

[0011] 在部件 120 包括诸如 TCM 的平台特定模块的情况下，该 TCM 可包括适合于提供至少一个加密密钥的任意数量的设备、系统或系统和设备的组合。在一些实施例中，唯一的私有密钥可以在生产该电子设备 110 的时候被置于该 TCM 的一部分之内。在该部件合并了 TCM 的情况下，采取一个或多个加密密钥或其它类似的标识符的形式的第一设备标识符 125 可以被用来唯一地区分特定的电子设备 110。

[0012] 在该部件 120 包括地理特定模块的情况下，该部件 120 可以包括适合于全部或部分地基于该电子设备 110 的地理位置来提供第一设备标识符 125 的任意数量的设备、系统或系统和设备的组合。地理特定模块可以采用各种方法来确定该电子设备 110 的位置。在一个示例中，全球定位系统（" GPS "）接收器可以被结合到地理特定模块中，以使用一个或多个 GPS 信号来提供设备位置。在另一个示例中，该地理特定模块可以使用经由例如置于该电子设备内的网络接口卡（"NIC"）所检测的网际协议（"IP"）地址来确定该电子设备 110 的物理位置。在又一个示例中，该地理特定模块可以例如经由一个或多个全球移动通信系统（"GSM"）接收器或经由一个或多个码分多址（"CDMA"）接收器使用一个或多个蜂窝通信信号来确定该电子设备 110 的物理位置。因此，在至少一些实施例中，该电子设备 110 的物理位置可以提供该第一设备标识符 125 的至少一部分。

[0013] 在部件 120 包括时间特定模块的情况下，部件 120 可包括适合于全部或部分地基于一个或多个时间标记（例如实时时钟（"RTC"）、经过时间时钟（elapsed time clock，"ETC"）等等）来提供第一设备标识符 125 的任意数量的设备、系统或系统和设备的组合。各种方法可被用来确定该时间标记，例如，部件 120 可以包括在完成特定事件时被激活的 ETC，所述事件例如对该电子设备 110 或置于该设备 110 中的一个或多个固件或软件例程的初始激活。因此，在至少一些实施例中，与该电子设备 110 相关联的至少一个时间标记可以提供该第一设备标识符 125 的至少一部分。

[0014] 因此，可以看到的是，该第一唯一标识符 125 可以包括适合于唯一地识别该电子设备 110 的任何数据。在一些实施例中，该第一唯一标识符 125 可以包括适合于识别一个或多个系统参数（例如该电子设备 110 的硬件、软件或固件配置）的任何数据。在一些实施例中，该第一设备标识符 125 可以包括适合于确定一个或多个物理参数（例如与特定的电子设备 110 相关联的物理位置或经过的操作时间）的任何数据。在一些实施例中，该第一设备标识符 125 可以包括置于该部件 120 内的唯一标识数据、系统参数数据和物理参数数据的任意组合。

[0015] 该不可变的存储器 130 可以被至少部分地置于该电子设备 110 内。该不可变的存储器可以包括任何类型的永久的、非易失性存储设备（示例包括忆阻器、只读存储器（"ROM"）、闪存，等等）。该不可变的存储器 130 可以包括适合于永久地存储数据的任意数量的系统、设备、系统和设备的组合。在一些实施例中，该不可变的存储器 130 可以是专用非易失性存储器模块。在其它实施例中，该不可变的存储器 130 可以是更大的易失性或非易失性存储器模块的非易失性部分。例如，在一些实施例中，该不可变的存储器 130 可以是至少部分地置于基本输入输出系统（"BIOS"）存储器模块之内的非易失性存储器模块，该基本输入输出系统存储器模块置于该电子设备 110 之内。

[0016] 在一些实施例中，该不可变的存储器 130 可以执行一系列机器可读指令，该一系列机器可读指令将该第一设备标识符 125 的至少一部分与该第二设备标识符 135 的至少一部分相比较。在一些实施例中，该不可变的存储器 130 可以包括系统 BIOS，该系统 BIOS 能够执行加电自检（"POST"），之后执行一个或多个机器可读指令集，例如用于激活置于该电气设备 110 内的一个或多个子系统（诸如 GPS 接收器、NIC、ETC、或 RTC）的指令。如果该第一设备标识符 125 的至少一部分与该第二设备标识符 135 的至少一部分相对应，则该电子设备 110 可以被允许执行特定动作，例如执行与引导例程（boot routine）相关联的一系列

机器可读指令，以例行地启动该电子设备 110。如果该第一设备标识符 125 的至少一部分未能与该第二设备标识符 135 的至少一部分相对应，则可以由该电子设备提供至少一个指示符 150，以指示该失败的相关。例如，如果发生了该第一设备标识符 125 的至少一部分和该第二设备标识符 135 的至少一部分之间的失败的相关，则该电子设备可以点亮一系列预定的指示符 150、使独特的指示符 150 发声、或生成预定的 RF 信号指示符 150。

[0017] 该第二设备标识符 135 可以全部或部分地被布置、写入、存储、或以其它方式嵌入在该不可变的存储器 130 之内。该第二设备标识符 135 可以包括在识别一个或多个电子设备参数时有用的任何数据。在一些实施例中，第二设备标识符 135 可以包括置于该不可变的存储器 130 内的唯一标识数据结构，例如由该电子设备制造商写入到该不可变的存储器中的唯一标识串。在一些实施例中，第二设备标识符 135 可以包括指示该电子设备 110 的操作或功能性被允许或禁止的地理区域的数据结构。该地理区域可以是包含的（inclusive）或排他的（exclusive），例如，包含的数据结构可以指示该电子设备 110 被授权成仅在美国内操作，或替代地，排他的数据结构可指示该电子设备 110 被授权成在除了美国以外的任何区域中操作。在一些实施例中，该第二设备标识符 135 可以包括指示电子设备 110 被允许操作的时间限制的数据，例如指示该电子设备 110 被授权成仅操作 500 小时的数据串。

[0018] 输入 140 可包括适合于将输入信号提供到该电子设备 110 的任意数量的系统、设备或系统和设备的任意组合。在其最基本的形式，该输入 140 可以如置于该电子设备 110 上的开关（例如 " 电源 " 或 " 测试 " 开关）一样简单。在一些实施例中，该输入 140 可以包括适合于将可变输入（例如键盘或鼠标输入）提供到电子设备 110 的一个或多个设备。在至少一些实施例中，该输入 140 可以通过一个或多个管道 155 被通信耦合到不可变的存储器 130 或处理器。

[0019] 在一些实施例中，用户可以例如通过按下置于该电子设备 110 上的电源按钮来激活输入 140。响应于用户激活该电源按钮输入 150，该电子设备 110 可以开始自引导指令（" 引导 "）序列。在其它实施例中，用户可以例如通过压下置于该电子设备 110 的表面上的 " 测试 " 按钮来激活该输入 140。响应于该用户激活该测试按钮输入 150，该电子设备 110 可以进入安全测试模式，并开始执行一个或多个测试序列。在一些实施例中，该引导或测试序列可以由该电子设备 110 不可见地执行（即在不提供外部指示给用户的情况下被执行）。

[0020] 该指示符 150 可以包括适合于提供任何可有形或无形地检测的指示的任意数量的系统、设备或系统和设备的任意组合。在一些实施例中，该指示符 150 可以包括任何可有形地检测的事件，例如可通过使用视力、听力、触觉、嗅觉或味觉的人感觉中的一个或多个检测的事件。在一些实施例中，该指示符 150 可以包括任何不可有形地检测的事件，例如不可通过使用人感觉中的一个或多个检测的事件，例如射频（"RF"）信号。在一些实施例中，指示符 150 的操作可以提供例如在正常引导或测试序列期间该电子设备 110 是否正常运行的指示。在一些实施例中，该指示符 150 可以置于该电子设备 110 之上或附近，例如置于该电子设备 110 的表面上的一个或多个被点亮的设备或可听到的扬声器。在一些实施例中，该指示符 150 可以被部分地或完全地置于该电子设备 110 之内，例如置于该电子设备 11 之内的射频发射器。

[0021] 在至少一些实施例中，该指示符 150 可以通过一个或多个管道 165 被通信耦合到处理器 160、部件 120、不可变的存储器 130 或其任意组合。

[0022] 该处理器 160 可以包括适合于执行机器可读指令集的任意数量的系统、设备、或系统和设备的任意组合。在一些实施例中，该处理器 160 可以包括专用于执行机器可读指令集的系统或设备，例如置于计算设备内的中央处理单元（"CPU"）。在一些实施例中，该处理器 160 可以包括置于电子设备内的一个或多个共享的系统或设备，例如置于计算设备内的一个或多个协同处理器。

[0023] 在一些实施例中，该处理器 160 可以执行一系列机器可读指令，该一系列机器可读指令将该第一设备标识符 125 的至少一部分与该第二设备标识符 135 的至少一部分相比较。如果该第一设备标识符 125 的至少一部分与该第二设备标识符 135 的至少一部分相对应，则该电子设备 110 可以被允许执行特定动作，例如执行与引导例程相关联的一系列机器可读指令，以例行地启动该电子设备 110。如果该第一设备标识符 125 的至少一部分未能与该第二设备标识符 135 的至少一部分相对应，则可以由该电子设备提供至少一个指示符 150，以指示该失败的相关。例如，如果发生了该第一设备标识符 125 的至少一部分和该第二设备标识符 135 的至少一部分之间的失败的相关，则该电子设备可以点亮一系列预定的指示符 150、使独特的指示符 150 发声、或生成预定的 RF 信号指示符 150。

[0024] 该第一设备标识符 125 和第二设备标识符 135 之间的相关或关系可以包括设备标识数据、设备配置数据、设备地理数据、设备时间数据或其组合中的一个或多个部分。在一些实施例中，该第一设备标识符 125 可以包括由设备制造商嵌入在部件 120 中的唯一装备标识符，而该第二设备标识符 135 可以包括嵌入在置于该电子设备 110 之内的不可变的存储器 130 的一部分中的等同的唯一设备标识符。在这样的实施例中，将该第一设备标识符 125 与第二设备标识符 135 相比较提供了该原始部件 120 是否已经被替换为代替物的指示。例如，将置于计算设备之内的可信平台模块 120 中的该第一设备标识符 125 与置于该系统 BIOS 的不可变部分 130 中的第二设备标识符 135 相比较可以提供该原始 TPM 120 是否已经被替换或该电子设备 110 的原始软件、固件、或硬件配置是否已经被改变的指示。

[0025] 在一些实施例中，该第一唯一标识符 125 可以包括全部或部分地从该电子设备 110 的物理位置（例如从置于该电子设备 110 之内的 GPS 接收器、蜂窝接收器、或 NIC 适配器）得出的标识符。该第二唯一标识符 135 可以全部或部分地包括该电子设备 110 的操作被允许或禁止的地理区的列表。例如，可以使用置于平板计算设备 110 之内的 GPS 接收器来得到该第一唯一标识符 125。 在这样的实施例中，该第一唯一标识符可以指示该计算设备 110 的物理位置为在麻省的波士顿之内。置于系统 BIOS 的不可变部分 130 中的该第二唯一标识符 135 可以指定麻省的状态为用于该电子设备 110 的使用的允许的区域。如在这个示例中，当该第一设备标识符（例如麻省的波士顿）全部或部分地与该第二设备标识符（例如，在麻省之内）相对应，则该处理器 160 可以允许该电子设备的正常操作。另一方面，如果该第一设备标识符 125 指示了缅因的班戈的物理位置，则该第一设备标识符（例如缅因的班戈）和该第二设备标识符（例如，麻省之内）将不对应，并且作为响应该处理器 160 可以提供至少一个指示符 150。

[0026] 在一些实施例中，该第一唯一标识符 125 可以包括全部或部分地从与该电子设备 110 相关联的一个或多个时间参数得到的标识符，所述时间参数例如使用置于该电子设备 110 之内的实时时钟（"RTC"）或经过时间时钟所收集的数据。该第二唯一标识符 135 可以全部或部分地包括时间范围或基于时间的范围，在该范围上，该电子设备 110 的操作被允

许或替代地被禁止。例如，可以通过使用从置于便携式计算设备 110 之内的经过时间时钟所收集的数据来得到该第一唯一标识符 125。在这样的实施例中，该第一唯一标识符可以指示该便携式计算设备 110 已经操作的经过时间。置于系统 BIOS 的不可变部分 130 中的该第二唯一标识符 135 可以指定该便携式计算设备 110 被授权操作的时间量。在这种情况中，该第一设备标识符 125（经过时间）和该第二设备标识符 135（授权时间）可以被比较，并且如果该经过时间小于该授权时间，可以允许该便携式计算设备 110 的正常操作。另一方面，如果该第一设备标识符 125（经过时间）大于该第二设备标识符（授权时间），则该第一和第二设备标识符将不对应，并且作为响应该处理器 160 可以提供至少一个指示符 150。

[0027] 现在参照图 2，提供计算设备 200 作为示例电子设备 110。在一些实施例中，该计算设备 200 可以包括部件 120，诸如合并了固件 210 和密码逻辑 220 的可信平台模块（"TPM"）。第一设备标识符 125 可以被完全或部分地布置、存储、或以其它方式嵌入在该 TPM 120 之内。该计算设备 200 还可以包括至少部分地置于该系统 BIOS 230 之内的不可变的存储器 130。第二设备标识符 135 可以全部或部分地置于该系统 BIOS 230 的不可变的存储器 130 内。

[0028] 该计算设备 200 还可以包括合并了南桥 240、北桥 250、存储器模块 255、和中央处理单元（"CPU"）260 的处理器 160。在一些实施例中，该处理器 160 的南桥 240 部分可以被通信地耦合到一个或多个指示符 150，例如一个或多个视觉指示符 270、一个或多个音频指示符 275、或其任意组合。在一些实施例中，该处理器 160 的南桥 240 部分可以被通信地耦合到一个或多个指示符 150，例如一个或多个 RF 指示符 285、一个或多个蓝牙指示符 280、或其任意组合。在一些实施例中，该处理器 160 的南桥 240 部分可以通过一个或多个管道 165 被通信地耦合到该不可变的存储器 130（例如该系统 BIOS 230）和该部件 120（例如 TPM 210，220）。

[0029] 该计算设备 200 还可以包括一个或多个视频输出 290。在至少一些实施例中，该一个或多个视频输出 290 可以通过一个或多个管道被通信地耦合到该处理器 160 的北桥 250 部分。在一些实施例中，该计算设备 200 还可以包括作为输入设备 140 而运行的电源按钮 295。该电源按钮 295 可以通过一个或多个管道被通信地耦合到该系统 bios 230。在一些实施例中，该计算设备 200 还可以包括可以作为输入设备 140 而运行的测试按钮 295。该测试按钮 295 可以通过一个或多个管道被通信地耦合到该系统 bios 230、该南桥 240、该北桥 250、或其任意组合。

[0030] 将部件 120 至少部分地集成到 TPM 中以及将不可变的存储器 130 至少部分地集成到系统 BIOS 230 中提供了该第一设备标识符 125 和第二设备标识符 135 的物理布置的仅一个示例。该第一设备标识符 125、第二设备标识符 135 或该第一和第二设备标识符两者被布置、存储或嵌入在该电子设备 100 内或计算设备 200 内的替代位置中的其它实施例是可能的。

[0031] 参考图 3，提供了示例安全方法 300。该方法可以包括在 310 将第一设备标识符 125 与第二设备标识符 135 相比较。在一些实施例中，该第一设备标识符 125 可以是预定的数据结构，例如在那里由设备制造商将该第一设备标识符 125 存储在或其它方式嵌入在该部件 120 中。在一些实施例中，该第一设备标识符 125 可以全部或部分地是通过使用一个或多个变量所形成的数据序列，该一个或多个变量例如网络接口卡（"NIC"）或 GPS 接收器

的输出(即,物理位置数据),或来自诸如实时时钟或经过时间时钟的定时设备的输出(即,时间数据)。该第二设备标识符 135 可以包括由该设备制造商布置、存储、或以其它方式嵌入在不可变的存储器 130 中的一个或多个数据结构。

[0032] 在标识数据形成该第一设备标识符 125 的至少一部分的情况下,在 310 的该比较可以包括将从该部件 120 获得的该第一设备标识符 125 的至少一部分与从该不可变的存储器 130 获得的第二设备标识符 135 相比较。在位置信息(例如从 NIC 或 GPS 提供的数据)形成该第一设备标识符 135 的至少一部分的情况下,在 310 的该比较可以包括将该第一设备标识符 125 的至少一部分与置于该不可变的存储器 130 内的可允许的或禁止的位置数据相比较。在时间信息(例如全部或部分地从 RTC 或 ETC 提供的数据)形成该第一设备标识符 135 的至少一部分的情况下,在 310 的该比较可以包括将该第一设备标识符 125 的至少一部分与置于该不可变的存储器 130 内的时间数据相比较。

[0033] 如果在 320 该第一设备标识符 125 的至少一部分与该第二设备标识符 135 的至少一部分相对应,则在 330 该设备 100 可正常启动。如果在 320 该第一设备标识符 125 的至少一部分未能与该第二设备标识符 135 的至少一部分相对应,则在 340 该设备 100 可提供至少一个指示符 150。在 330 正常启动该设备 100 可以包括将该设备 100 置于用户可以在没有一个或多个软件、固件或硬件限制的存在的情况下与该设备自由地交互的状态中。在 340 提供至少一个指示符 150 可以包括提供一个或多个指示符,其包括一个或多个视觉指示符、一个或多个可听指示符、一个或多个射频指示符等等。

[0034] 参考图 4,提供了另一个示例安全方法 400。在一些实施例中,在 310 的对该第一设备标识符 125 和该第二设备标识符 135 的比较可以由该电子设备的用户所提供的动作来发起。例如,在 410,该用户可将至少一个输入提供到该电子设备。在一些实施例中,该输入 140 可以包括激活用于该电子设备 110 的电源开关。在一些实施例中,该输入 140 可以包括例如通过激活置于在该设备 100 之中、之上或附近的输入 140 来激活安全测试模式。

[0035] 如果该第一设备标识符 125 和第二设备标识符 135 未能对应,则在提供至少一个指示符(在 340)之后,可以禁止该电子设备功能性的至少一部分(在 420)。这样的禁止可能影响该电子设备的功能性、速度或其它相似参数。例如,被运输到未被标识为由该第二设备标识符 135 可允许的操作区域的区域的具有基于地理的第一设备标识符 125 的设备,可以被完全禁止运行。在另一个示例中,具有超过嵌入在该第二设备标识符 135 中的预定阈值的基于时间的第一设备标识符 125 的设备可以例如通过减小该处理器 160 的时钟速度来禁止或影响该电子设备 110 的性能。

[0036] 将图 4 中所描述的方法 400 应用到参照图 2 详细描述的计算设备 200,可以进一步描述示例性安全过程方法 400。用户可以通过按下置于该计算设备 200 的表面上的开 / 关按钮 295 来开始执行该方法 400(在 410)。在进行加电自检("POST")之后,该 BIOS 230 可以启用必要的系统设备,例如机载 NIC、GPS 接收器、RTC 或 ETC,以执行该安全方法。在不使用系统设备的情况下,例如,当预加载的标识数据被用作该第一设备标识符 125 时,该 BIOS 230 可以在不启用该计算设备 200 上的任何附加系统资源的情况下继续进行。取决于该电子设备 200 的配置,该第一设备标识符 125 可以被预加载到置于该设备之内的 TPM 210 中,或通过使用诸如系统 NIC、GPS、ETC 或 RTC 的一个或多个系统资源来全部或部分地生成。

[0037] 在完成 POST 之后,该 BIOS 230 可以(在 310)将置于该不可变的存储器 130 中的

第二设备标识符 135 与该第一设备标识符 125 相比较。如果该第一设备标识符 125 与该第二设备标识符 135 全部或部分地相对应(在 320),则该 BIOS 230 可以允许该计算设备 200 的正常引导序列(在 330)。如果该第一设备标识符 125 的至少一部分未能与该第二设备标识符 135 的至少一部分全部或部分地相对应(在 320),则该 BIOS 230 可以提供至少一个指示符 150,包括点亮一个或多个视觉指示符 270,使一个或多个可听指示符 275 发声,或使用 RF 指示符 280 来提供一个或多个 RF 信号(在 340)。

[0038] 在提供该至少一个指示符之后,计算设备 200 功能性的至少一部分可以被禁止(在 420)。在一些实施例中,该计算设备 200 的整个功能性可以被禁止,例如如果该第一设备标识符 125 的至少一部分未能与该第二设备标识符 135 的至少一部分相对应,则可以暂停该引导序列。在一些实施例中,计算设备 200 的性能可能被损害、影响或妨碍,从而对该计算设备 200 的一个或多个特征产生影响。例如,在该第一设备标识符 125 全部或部分地基于 ETC 的情况下,如果用户在该 ETC 已经超过由该第二设备标识符 135 所施加的时间限制之后引导该电子设备 200,则一个或多个软件或固件例程可以被禁止(在 420)。在禁止该计算设备功能性的至少一部分之后,该 BIOS 230 然后可以允许该引导序列的继续(在 430)。

[0039] 尽管为了方便、讨论和可读性进行了顺序描述,但在图 3 和 4 中所描绘的动作、步骤或序列中的至少一些能以不同次序和 / 或并行地被执行。另外,一个或多个特定实施例可以仅执行图 3 和 4 中所描述的有限数量的动作、步骤或序列。另外,可以通过使用第二处理器来执行一个或多个动作、步骤或序列,该第二处理器邻近或远离执行图 3 和 4 中所描述的一个或多个动作、步骤、或序列中的全部或一部分的该第一处理器被布置。

[0040] 已经使用一组数字上限和一组数字下限来描述某些实施例和特征。应当理解的是,从任何下限到任何上限的范围是被想到的,除非另有指示。某些下限、上限和范围出现在以下的一个或多个权利要求中。全部数值是 " 大约 " 或 " 近似 " 该指示的值,并且考虑由本领域普通技术人员所预期的实验误差和变化。

[0041] 虽然前述内容针对本发明的实施例,但本发明的其它和进一步实施例可以在不背离其基本范围的情况下被想出,并且其范围由随后的权利要求书所确定。

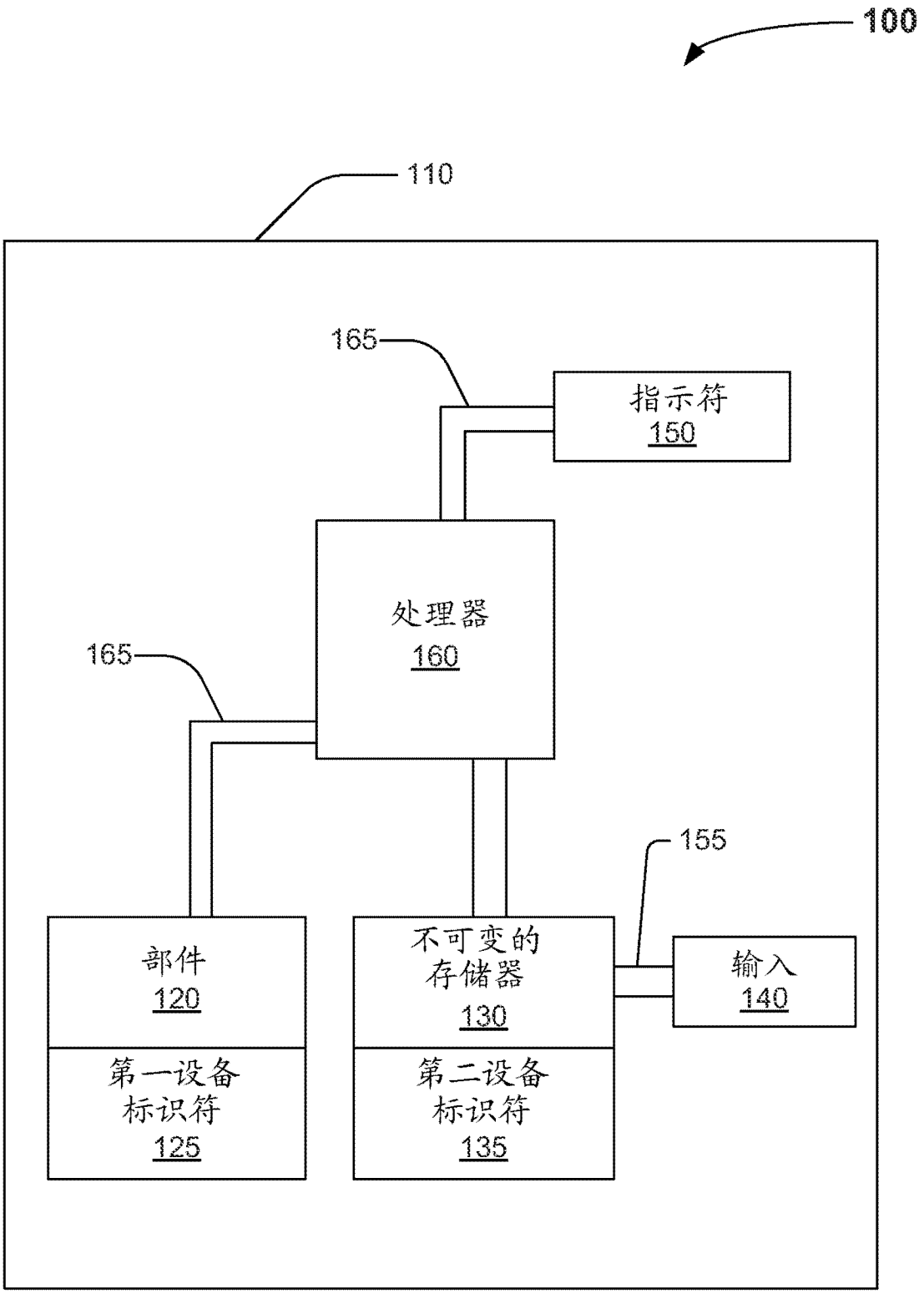

100
110
165
指示符
150
处理器
160
165
155
部件
120
第一设备
标识符
125
不可变的
存储器
130
第二设备
标识符
135
输入
140

图 1

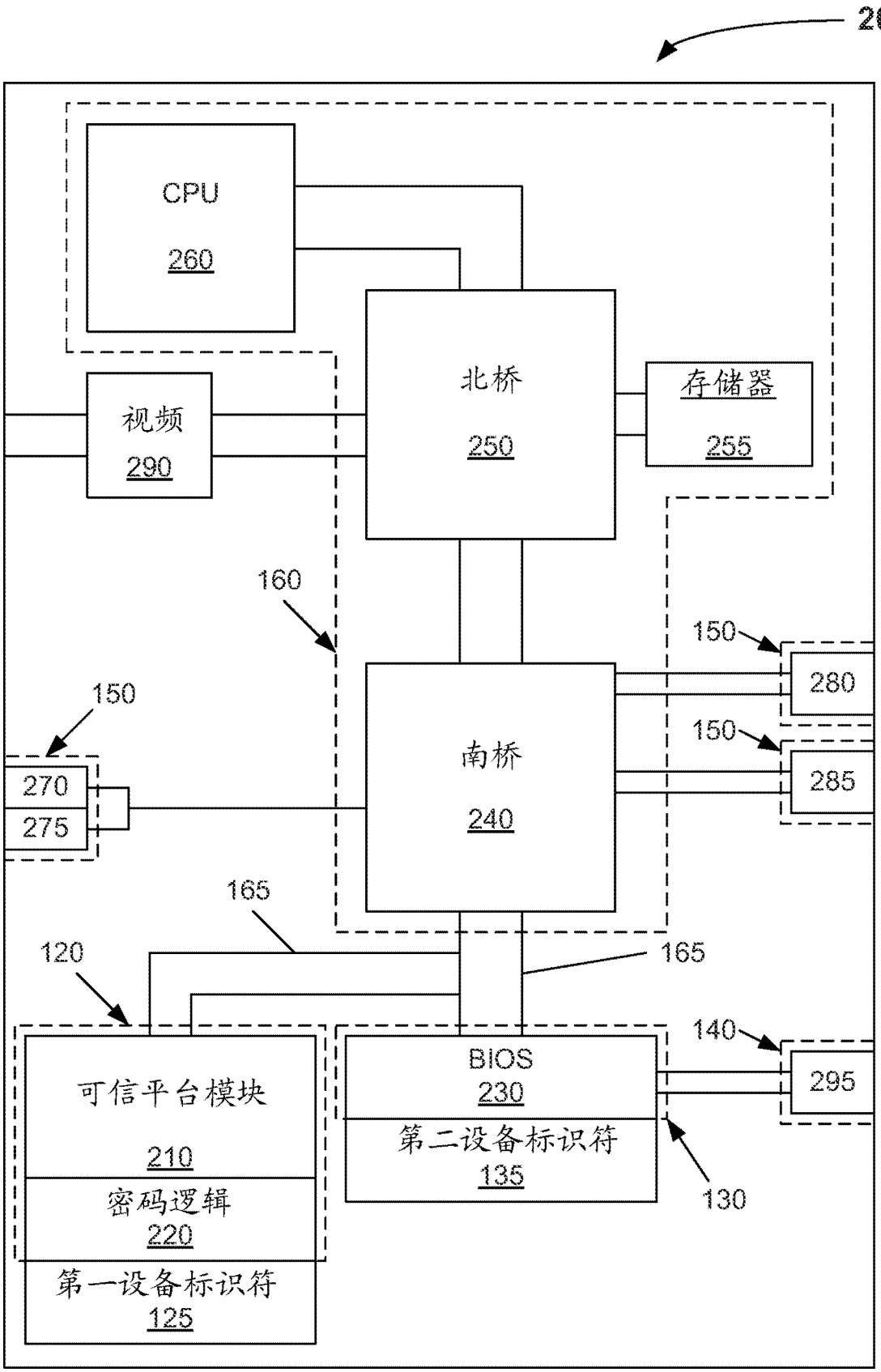

200
CPU
260
北桥
250
存储器
255
视频
290
160
150
280
150
285
150
270
275
南桥
240
165
165
120
140
295
BIOS
230
第二设备标识符
135
130
可信平台模块
210
密码逻辑
220
第一设备标识符
125

图 2

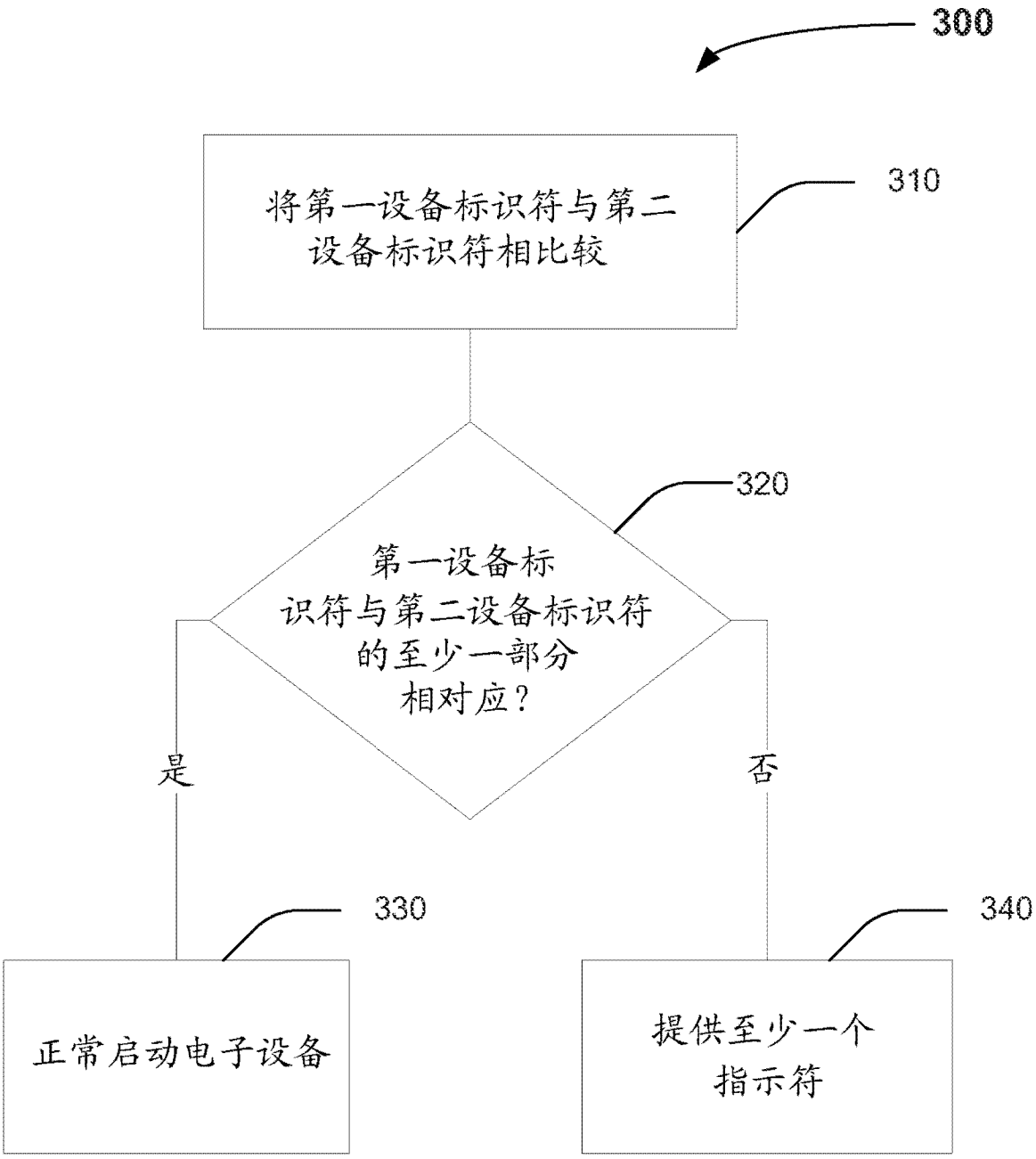

300
将第一设备标识符与第二设备标识符相比较
310
第一设备标识符与第二设备标识符的至少一部分相对应？
320
是
否
330
340
正常启动电子设备
提供至少一个指示符

图 3

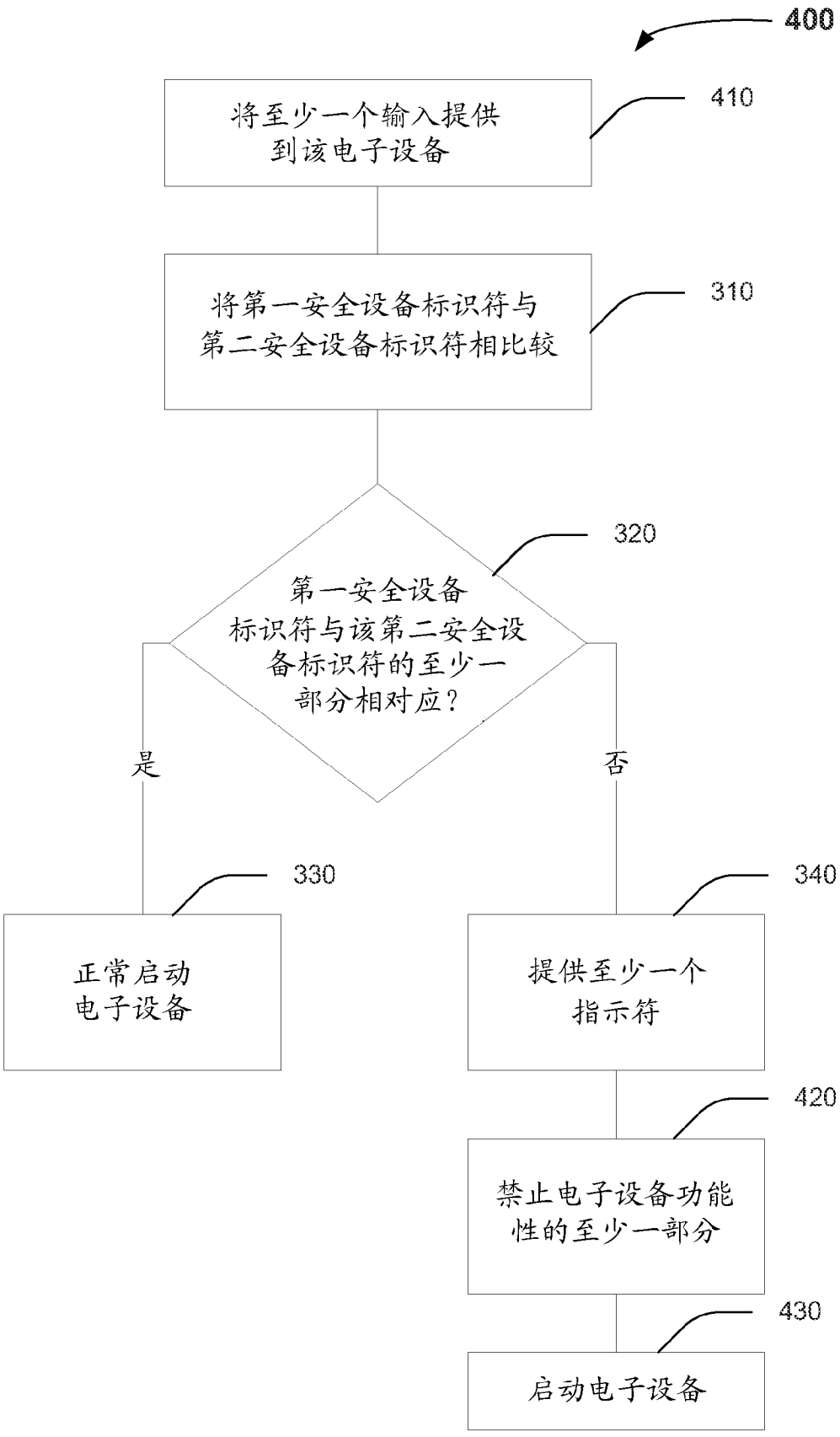

400
将至少一个输入提供到该电子设备
410
将第一安全设备标识符与第二安全设备标识符相比较
310
第一安全设备标识符与该第二安全设备标识符的至少一部分相对应？
320
是
否
330
正常启动电子设备
340
提供至少一个指示符
420
禁止电子设备功能性的至少一部分
430
启动电子设备

图 4