(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 104981814 A
(43)申请公布日 2015.10.14

(21)申请号 201380073058.2
(22)申请日 2013.03.15
(85)PCT国际申请进入国家阶段日
2015.08.14
(86)PCT国际申请的申请数据
PCT/CN2013/072732 2013.03.15
(87)PCT国际申请的公布数据
WO2014/139162 EN 2014.09.18
(71)申请人 英特尔公司
地址 美国加利福尼亚州
(72)发明人 G. 董 姚颉文 V. J. 齐默
M. A. 罗思曼
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 张凌苗 胡莉莉
(51)Int.Cl.
G06F 21/57(2013.01)
G06F 21/71(2013.01)

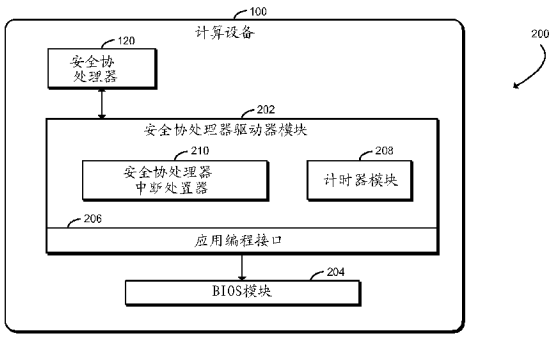
权利要求书3页 说明书9页 附图4页

(54)发明名称

安全协处理器引导性能

(57)摘要

用于改进计算设备上的平台初始化的技术包括使用计算设备的基本输入/输出系统(BIOS)开始计算设备的平台的初始化。当从BIOS模块接收到安全处理器命令时,安全协处理器驱动器模块将安全协处理器命令添加到命令列表。计算设备建立平台的初始化的周期性中断以关于针对之前提交的安全协处理器命令的响应的可用性查询安全协处理器,将由安全协处理器驱动器模块接收的任何响应转发给BIOS模块,并且将命令列表中的下一安全协处理器命令提交至安全协处理器。



CN 104981814 A

1. 一种用于改进平台初始化的计算设备，该计算设备包括：

执行提交至其的安全协处理器命令的安全协处理器；

开始计算设备的平台的初始化的基本输入/输出系统模块；

响应于从基本输入/输出系统模块接收到安全协处理器命令而将安全协处理器命令添加到命令列表的安全协处理器驱动器模块；以及

建立平台的初始化的周期性中断的计时器模块，

其中安全协处理器驱动器模块还响应于周期性中断的出现而(i)关于针对之前提交的安全协处理器命令的安全协处理器响应的可用性查询安全协处理器，并且(ii)响应于接收到可用的安全协处理器响应而将可用的安全协处理器响应转发给基本输入/输出系统模块。

2. 权利要求 1 的计算设备，其中安全协处理器驱动器模块还响应于接收到可用的安全协处理器响应而将命令列表中的下一安全协处理器命令提交至安全协处理器。

3. 权利要求 1 的计算设备，其中安全协处理器包括可信平台模块。

4. 权利要求 1 的计算设备，其中安全协处理器包括可管理性引擎。

5. 权利要求 1 的计算设备，其中安全协处理器包括会聚安全引擎。

6. 权利要求 1 的计算设备，其中安全协处理器包括带外处理器。

7. 权利要求 1 的计算设备，其中基本输入/输出模块还响应于从周期性中断的返回而继续平台的初始化。

8. 权利要求 1 的计算设备，其中计时器模块还响应于不涉及安全协处理器命令的初始化过程的完成而不继续初始化的周期性中断。

9. 权利要求 8 的计算设备，其中安全协处理器驱动器模块还响应于不涉及安全协处理器命令的初始化过程的完成而(i)将命令列表中所剩余的每一个安全协处理器命令提交至安全协处理器，并且(ii)对于剩余安全协处理器命令中的每一个，响应于接收到针对剩余安全协处理器命令中的一个的可用的安全协处理器响应而将可用的安全协处理器响应转发给基本输入/输出系统模块。

10. 权利要求 9 的计算设备，其中基本输入/输出系统模块还响应于初始化过程的完成而引导计算设备的操作系统。

11. 权利要求 1 的计算设备，其中命令列表遵循先进先出系统。

12. 权利要求 1 的计算设备，其中命令列表遵循后进先出系统。

13. 一种用于改进计算设备的平台初始化的方法，该方法包括：

使用计算设备的基本输入/输出系统开始计算设备的平台的初始化；

利用计算设备的安全协处理器驱动器并且从基本输入/输出系统接收要由计算设备的安全协处理器执行的安全协处理器命令；

响应于接收到安全协处理器命令而利用安全协处理器驱动器将安全协处理器命令添加到命令列表；以及

利用计算设备周期性地中断平台的初始化以(i)关于针对之前提交的安全协处理器命令的安全协处理器响应的可用性查询安全协处理器，并且(ii)响应于接收到可用的安全协处理器响应而将可用的安全协处理器响应转发给基本输入/输出系统模块。

14. 权利要求 13 的方法，其中中断平台的初始化包括响应于接收到可用的安全协处理

器响应而将命令列表中的下一安全协处理器命令提交至安全协处理器。

15. 权利要求 13 的方法，其中接收安全协处理器命令包括利用计算设备的可信平台模块驱动器并且从基本输入 / 输出系统接收要由计算设备的可信平台模块执行的可信平台模块命令 ；

其中将安全协处理器命令添加到命令列表包括响应于接收到可信平台模块命令而利用可信平台模块驱动器将可信平台模块命令添加到命令列表 ；并且

其中中断平台的初始化包括利用计算设备周期性地中断平台的初始化以（i）关于针对之前提交的可信平台模块命令的可信平台模块响应的可用性查询可信平台模块，并且（ii）响应于接收到可用的可信平台模块响应而将可用的可信平台模块响应转发给基本输入 / 输出系统模块。

16. 权利要求 15 的方法，其中中断平台的初始化包括响应于接收到可用的可信平台模块响应而将命令列表中的下一可信平台模块命令提交至可信平台模块。

17. 权利要求 13 的方法，还包括响应于从周期性中断的返回而在计算设备上继续平台的初始化。

18. 权利要求 13 的方法，还包括响应于完成不涉及安全协处理器命令的初始化过程而在计算设备上不继续初始化的周期性中断。

19. 权利要求 18 的方法，还包括 ：

利用计算设备并且响应于完成不涉及安全协处理器命令的初始化过程而将命令列表中所剩余的每一个安全协处理器命令提交至安全协处理器 ；以及

对于剩余安全协处理器命令中的每一个，利用计算设备并且响应于接收到针对剩余安全协处理器命令中的一个的可用的安全协处理器响应而将可用的安全协处理器响应转发给基本输入 / 输出系统。

20. 权利要求 19 的方法，还包括响应于完成初始化过程而在计算设备上引导计算设备的操作系统。

21. 权利要求 13 的方法，其中将命令列表中的下一安全协处理器命令提交至安全协处理器包括基于先进先出和后进先出之一将命令列表中的下一安全协处理器命令提交至安全协处理器。

22. 包括存储在其上的多个指令的一个或多个机器可读存储介质，所述指令响应于被执行而导致计算设备执行权利要求 13-21 中任一项的方法。

23. 一种用于改进平台初始化的计算设备，该计算设备包括 ：

用于使用计算设备的基本输入 / 输出系统开始计算设备的平台的初始化的装置 ；

用于利用计算设备的安全协处理器驱动器并且从基本输入 / 输出系统接收要由计算设备的安全协处理器执行的安全协处理器命令的装置 ；

用于响应于接收到安全协处理器命令而利用安全协处理器驱动器将安全协处理器命令添加到命令列表的装置 ；以及

用于周期性地中断平台的初始化以进行以下的装置 ：（i）关于针对之前提交的安全协处理器命令的安全协处理器响应的可用性查询安全协处理器，并且（ii）响应于接收到可用的安全协处理器响应而将可用的安全协处理器响应转发给基本输入 / 输出系统模块。

24. 权利要求 23 的计算设备，其中用于中断平台的初始化的装置包括用于响应于接收

到可用的安全协处理器响应而将命令列表中的下一安全协处理器命令提交至安全协处理器的装置。

25. 权利要求 23 的计算设备，还包括：

用于响应于从周期性中断的返回而继续平台的初始化的装置；

用于响应于完成不涉及安全协处理器命令的初始化过程而不继续初始化的周期性中断的装置；

用于响应于完成不涉及安全协处理器命令的初始化过程而将命令列表中所剩余的每一个安全协处理器命令提交至安全协处理器的装置；以及

用于针对剩余安全协处理器命令中的每一个，响应于接收到针对剩余安全协处理器命令中的一个的可用的安全协处理器响应而将可用的安全协处理器响应转发给基本输入 / 输出系统的装置。

安全协处理器引导性能

背景技术

[0001] 可信平台模块(TPM)和其他安全协处理器通常用于增强计算设备的安全性。这样的安全协处理器典型地执行各种加密功能并且常常用于断言平台的完整性。此外,因为安全协处理器通常能够执行加密过程,因而在一些情况下它们被用于从计算设备的主处理器卸载那些加密过程。

[0002] 在当今社会中,对于消费者享用各种计算设备而言,速度是基本的。例如,市场上已经出现超极本,其相比于标准笔记本计算机主要关注于增加的引导速度。另外,用于操作系统和计算机平台的一些标准通过例如要求计算设备在仅仅几秒内完成统一可扩展固件接口(UEFI)基本输入/输出系统(BIOS)加电自检(POST)而要求制造商关注引导速度。那些标准确保计算设备快速引导并且存在与服务器重启相关联的最小故障时间。另外,与引导典型 TPM 相关联的时延是明显的,这与那些标准是相反的。

附图说明

[0003] 通过示例的方式并且不作为限制而在随附各图中图示了本文所描述的概念。出于说明的简单性和清楚性,图中所图示的元件未必按照比例绘制。在认为适当的情况下,已经在各图当中重复参考标记以指示对应或类似的元件。

[0004] 图 1 是用于改进平台初始化的计算设备的至少一个实施例的简化框图;

图 2 是图 1 的计算设备的环境的至少一个实施例的简化框图;

图 3 和 4 是用于改进图 1 的计算设备上的平台初始化的方法的至少一个实施例的简化流程图;

图 5 是用于图 1 的计算设备的引导流的简化流程图;以及

图 6 是用于传统系统的引导流的简化流程图。

具体实施方式

[0005] 尽管本公开的概念容许各种修改和可替换形式,但是已经在图中通过示例的方式示出并且将在本文中详细描述其具体实施例。然而,应当理解的是,不意图将本公开的概念限于所公开的特定形式,而是相反,意图涵盖与本公开和随附权利要求相一致的所有修改、等同物和可替换物。

[0006] 在说明书中提及“一个实施例”、“实施例”、“说明性实施例”等指示所描述的实施例可以包括特定特征、结构或特性,但是每一个实施例可以或者可以不必包括该特定特征、结构或特性。而且,这样的短语未必是指相同实施例。此外,当结合实施例描述特定特征、结构或特性时,应当指出的是,结合不管是否明确描述的其他实施例实现这样的特征、结构或特性在本领域技术人员的认知内。

[0007] 在一些情形中,所公开的实施例可以在硬件、固件、软件或其任何组合中实现。所公开的实施例还可以实现为由暂时或非暂时机器可读(例如计算机可读)存储介质承载或者存储于其上的指令,所述指令可以由一个或多个处理器读取和执行。机器可读存储介质

可以体现为用于以机器可读的形式存储或传送信息的任何存储设备、机构或其他物理结构(例如易失性或非易失性存储器、介质盘或其他介质设备)。

[0008] 在图中,可以以具体布置和/或顺序示出一些结构或方法特征。然而,应当了解到,可以不要求这样的具体布置和/或顺序。相反地,在一些实施例中,这样的特征可以以与说明性图中所示出的不同方式和/或顺序进行布置。此外,结构或方法特征包括在特定图中并不意在暗示着在所有实施例中都要求这样的特征,并且在一些实施例中可以不包括这样的特征或者这样的特征可以与其他特征组合。

[0009] 现在参照图1,在说明性实施例中,用于改进的平台初始化的计算设备100被配置成在等待来自安全协处理器的响应的同时允许计算设备100的BIOS继续针对计算设备100的其他组件的初始化过程。如下文详细讨论的,这消除了与等待来自安全协处理器针对发送到安全协处理器的每一个安全协处理器命令的响应相关联的大量时延。

[0010] 计算设备100可以体现为能够改进平台初始化并且执行本文所描述的功能的任何类型的计算设备。例如,计算设备100可以体现为蜂窝电话、智能电话、平板计算机、膝上型计算机、个人数字助理、移动因特网设备、台式计算机、服务器和/或任何其他计算/通信设备。如图1中所示,说明性计算设备100包括处理器110、输入/输出("I/O")子系统112、存储器114、数据存储装置116、一个或多个外围设备118和安全协处理器120。当然,在其他实施例中,计算设备100可以包括其他或附加组件,诸如在典型计算设备中通常找到的那些(例如各种输入/输出设备、通信电路等)。此外,在一些实施例中,一个或多个说明性组件可以合并到另一组件中或者以其他方式形成另一组件的部分。例如,在一些实施例中,存储器114或其部分可以合并到处理器110中。

[0011] 处理器110可以体现为能够执行本文所描述的功能的任何类型的处理器。例如,处理器可以体现为(多个)单核或多核处理器、数字信号处理器、微控制器、或其他处理器或处理/控制电路。类似地,存储器114可以体现为能够执行本文所描述的功能的任何类型的易失性或非易失性存储器或数据存储装置。在操作中,存储器114可以存储在计算设备100的操作期间所使用的各种数据和软件,诸如操作系统、应用、程序、库和驱动程序。存储器114经由I/O子系统112通信耦合到处理器110,I/O子系统112可以体现为促进与处理器110、存储器114和计算设备100的其他组件的输入/输出操作的电路和/或组件。例如,I/O子系统112可以体现为或者以其他方式包括存储器控制器中心、输入/输出控制中心、固件设备、通信链路(即点对点链路、总线链路、电线、线缆、光导、印刷电路板迹线等)和/或促进输入/输出操作的其他组件和子系统。在一些实施例中,I/O子系统112可以形成片上系统(SoC)的部分并且连同处理器110、存储器114和计算设备100的其他组件一起合并在单个集成电路芯片上。

[0012] 数据存储装置116可以体现为被配置用于数据的短期或长期存储的一个或多个任何类型的设备,诸如例如存储器设备和电路、存储器卡、硬盘驱动器、固态驱动器或其他数据存储设备。计算设备100的外围设备118可以包括任何数目的附加外围或接口设备。包括在外围设备118中的特定设备可以例如取决于计算设备100的类型和/或意图用途。

[0013] 安全协处理器120可以体现为能够执行本文所描述的功能的(多个)任何硬件组件或电路。在一些实施例中,安全协处理器120能够建立可信执行环境。例如,安全协处理器120可以体现为可信平台模块(TPM)、可管理性引擎(ME)、会聚安全引擎(CSE)或其他带外

处理器。在一些实施例中，安全协处理器 120 体现为被配置成相对于处理器 110 独立地且以带外方式操作的带外处理器。

[0014] 现在参照图 2，在使用时，计算设备 100 建立用于改进平台初始化的环境 200。在说明性实施例中，环境 200 包括安全协处理器驱动器模块 202 和基本输入 / 输出系统（BIOS）模块 204。此外，安全协处理器驱动器模块 202 还包括应用编程接口 206、计时器模块 208 和安全协处理器中断处置器 210。安全协处理器驱动器模块 202、BIOS 模块 204、应用编程接口 206、计时器模块 208 和安全协处理器中断处置器 210 中的每一个可以体现为硬件、软件、固件或其组合。

[0015] 安全协处理器驱动器模块 202 管理安全协处理器 120 与计算设备 100 的其他组件之间的通信。例如，如下文详细讨论的，安全协处理器驱动器模块 202 可以将安全协处理器命令传送给安全协处理器 120 以供执行或其他处理。与等待安全协处理器做出响应（这典型地导致明显时延）相反，在一些实施例中，安全协处理器驱动器模块 202 查询或以其他方式轮询安全协处理器 120 的状态以确定安全协处理器 120 的响应是否准备就绪，并且如果没有，则恢复其他初始化，如下文更详细讨论的。

[0016] BIOS 模块 204 可以开始计算设备 100 的平台的初始化。这样，在一些实施例中，BIOS 模块 204 初始化和 / 或测试计算设备 100 的各种组件（例如输入 / 输出设备）。此外，BIOS 模块 204 可以使用安全协处理器驱动器模块 202 的应用编程接口（API）206 与安全协处理器驱动器模块 202 通信和交互。在一些实施例中，BIOS 模块 204 不直接与安全协处理器 120 通信，而是替代地将安全协处理器驱动器模块 202 用作中介。因而，当 BIOS 模块 204 想要发送安全协处理器命令时，BIOS 模块 204 将该命令发送给安全协处理器驱动器模块 202 而不是直接发送给安全协处理器 120。如下文所讨论的，安全协处理器 120 将该安全协处理器命令添加到命令列表。类似地，当安全协处理器驱动器模块 202 接收到来自安全协处理器 120 的响应时，响应继而可以转发给 BIOS 模块 204。当然，在一些实施例中，某些安全协处理器命令可能不会引起来自安全协处理器 120 的响应和 / 或可能不需要通过安全协处理器驱动器模块 202 转发给 BIOS 模块 204。

[0017] 计时器模块 208 被配置成建立计算设备 100 的平台的初始化的周期性中断。例如，在一些实施例中，计时器模块 208 可以包括或以其他方式利用高精度事件计时器（HPET）或其他硬件计时器。在一个实施例中，由计时器模块 208 建立的周期性中断是实时中断，其每当计算设备 100 的时钟达到某值时发生。当然，在其他实施例中，计时器模块 208 可以建立非周期性或具有改变的周期（例如周期的集合）的中断。例如，中断可以在一个 BIOS 阶段期间比另一 BIOS 阶段期间更不频繁地发生（即周期可以取决于 BIOS 阶段）。当中断发生时，安全协处理器中断处置器 210 被调用，并且将控制转移到安全协处理器中断处置器 210（例如从 BIOS 模块 204）。如下文详细讨论的，安全协处理器中断处置器 210 检查安全协处理器 120 的状态（即确定针对之前提交的安全协处理器命令的响应是否准备就绪），并且如果其准备就绪则从安全协处理器 120 得到响应。

[0018] 如果命令列表中存在任何安全协处理器命令，则安全协处理器中断处置器 210 将列表中的下一命令发送给安全协处理器 120 以进行处理，并且控制从安全协处理器中断处置器 210 返回。当然，如上文所讨论的，响应可以转发给 BIOS 模块 204。在一些实施例中，命令列表是队列化以供传输给安全协处理器 120 的安全协处理器命令的列表。例如，在安

全协处理器 120 是 TPM 的实施例中，命令列表是要队列化以执行的从 BIOS 模块 204 发送给安全协处理器驱动器模块 202（或者在这样的实施例中为 TPM 驱动器模块）的 TPM 命令的列表。在一些实施例中，一旦安全协处理器命令已经发送给安全协处理器 120 以执行，则将其从命令列表移除。应当了解到，命令列表中的安全协处理器命令的执行顺序可以取决于实施例而变化。例如，在一个实施例中，可以实现先进先出（FIFO）策略。在另一实施例中，可以使用后进先出（LIFO）策略。在又一实施例中，可以使用更复杂的策略来确定安全协处理器命令的执行优先级。命令列表可以作为任何适合的数据结构存储在计算设备 100 上。

[0019] 现在参照图 3 和 4，在使用时，计算设备 100 可以执行用于例如通过以下来改进平台初始化的方法 300 ：在等待来自安全协处理器 120 的针对发送给安全协处理器 120 的每一个安全协处理器命令的响应的同时允许 BIOS 模块 204 继续针对计算设备 100 的其他组件的初始化过程。说明性方法 300 以图 3 的框 302 开始，其中计算设备 100 确定计算设备 100 是否加电。一旦计算设备 100 已经加电，则计算设备 100 在框 304 中初始化安全协处理器中断处置器 210。在这样做时，在框 306 中，计算设备 100 初始化计时器。也就是说，如上文所讨论的那样建立平台的初始化的周期性中断。此外，在框 308 中，计算设备 100 初始化安全协处理器命令列表（例如建立适当的数据结构）。

[0020] 在框 310 中，计算设备 100 开始平台初始化。例如，计算设备 100 可以开始初始化和 / 或测试计算设备 100 的各种组件（例如各种输入 / 输出组件）。在框 312 中，计算设备 100 确定安全协处理器驱动器模块 202 是否已经从 BIOS 模块 204 接收到安全协处理器命令以传输给安全协处理器 120。如果是，则在框 314 中计算设备 100 将安全协处理器命令添加到安全协处理器命令列表并且继续平台初始化。在框 316 中，计算设备 100 确定是否已经触发安全协处理器中断（例如周期性中断）。如果在框 312 中计算设备 100 确定尚未从 BIOS 模块 204 接收到安全协处理器命令，则方法 300 直接前进到框 316。如果已经触发安全协处理器中断，则在框 318 中计算设备 100 检查安全协处理器 120 的状态。例如，计算设备 100 确定针对之前提交的安全协处理器命令的响应是否可用于从安全协处理器 120 传输给安全协处理器驱动器模块 202。此外，如果在框 316 中计算设备 100 确定尚未触发安全协处理器中断，则方法 300 前进到框 330，其中计算设备 100 确定非安全协处理器平台初始化是否完成，如下文更详细讨论的。换言之，在一些实施例中，计算设备 100 的安全协处理器中断处置器 210 仅响应于安全协处理器中断的出现而执行在方法 300 的框 318-328 中所描述的功能。

[0021] 在框 318 中检查安全协处理器 120 的状态之后，方法 300 前进到框 320（参见图 4）。如果在框 320 中计算设备 100 确定来自安全协处理器 120 的响应可用，则在框 322 中计算设备 100 的安全协处理器驱动器模块 202 从安全协处理器 120 接收安全协处理器响应。然而，如果计算设备 100 确定响应没有准备就绪，则方法 300 前进到框 330。在框 324 中，安全协处理器驱动器模块 202 将所接收的响应转发给 BIOS 模块 204。在一些实施例中，安全协处理器驱动器模块 202 信号传送事件以通知 BIOS 模块 204 安全协处理器响应可用。在这样的实施例中，如果 BIOS 模块 204 需要响应，则 BIOS 模块 204 能够经由事件回叫过程获取安全协处理器响应。

[0022] 在框 326 中，计算设备 100 确定安全协处理器命令列表是否为空。也就是说，计算设备 100 确定是否存在等待由安全协处理器 120 执行的任何安全协处理器命令。如果命令

列表为空，则方法 300 前进到框 330。然而，如果命令列表不为空，则在框 328 中安全协处理器驱动器模块 202 将下一安全协处理器命令发送给安全协处理器 120 以执行。如上文所讨论的，命令列表中的安全协处理器命令的执行优先级可以取决于所实现的特定策略而变化。在框 330 中，计算设备 100 确定非安全协处理器平台初始化是否完成。换言之，计算设备 100 确定安全协处理器命令(即安全协处理器命令列表中的命令)是否为被留下执行以便完成平台初始化的仅有命令。当然，在一些实施例中，可以存在要由 BIOS 模块 204 执行的附加命令，其依赖于来自安全协处理器 120 的对安全协处理器命令的响应。在这样的实施例中，计算设备 100 可以确定例如安全协处理器命令是否为能够当前执行的仅有命令。

[0023] 如果非安全协处理器平台初始化完成，则在框 332 中计算设备 100 停止计时器。也就是说，计算设备 100 停止中断平台初始化。在框 334 中，计算设备 100 确定安全协处理器命令列表是否为空。应当了解到，如果非安全协处理器平台初始化完成并且命令列表中没有剩余用于执行的安全协处理器命令，则平台初始化完成并且计算设备 100 的操作系统现在可以引导。因此，在框 338 中，计算设备 100 引导操作系统。当然，在一些实施例中，计算设备 100 可以包括多于一个操作系统。这样，可以引导默认操作系统，可以为计算设备 100 的用户给出选择用于引导的操作系统的选项，或者可以实现某种其他引导策略。

[0024] 如果在框 334 中计算设备 100 确定安全协处理器命令列表不为空，则在框 336 中计算设备 100 执行剩余安全协处理器命令。例如，安全协处理器驱动器模块 202 可以遵循传统方案：将命令列表中所剩余的每一个安全协处理器命令依次地传输给安全协处理器 120 以供执行，在发送下一个命令之前等待针对每一个所传输的命令的响应，并且将响应转发给 BIOS 模块 204 以完成初始化。如上文所讨论的，在一些实施例中，一个或多个非安全协处理器命令可以依赖于针对安全协处理器命令的响应以便执行。在这样的实施例中，如果非安全协处理器命令变得由 BIOS 模块 204 可执行(例如由于来自安全协处理器 120 的响应)，则方法 300 可以返回到框 330，其中计算设备 100 确定非安全协处理器平台初始化是否完成。计算设备 100 还可以重新启用与安全协处理器中断相关联的计时器。换言之，在这样的实施例中，计算设备 100 可以恢复以下过程：在等待来自安全协处理器 120 的对安全协处理器命令的响应的同时准许平台的非安全协处理器初始化。返回到框 330，如果计算设备 100 确定非安全协处理器初始化未完成，则方法 300 返回到图 3 的框 312，其中计算设备确定是否已经通过安全协处理器驱动器模块 202 从 BIOS 模块 204 接收到安全协处理器命令。

[0025] 现在参照图 5 和 6，在图 5 中说明性地示出计算设备 100 实现用于改进的平台初始化的方法 300 的引导流 502，而在图 6 中示出计算设备 100 实现用于平台初始化的传统方法的引导流 602。如图 5 中所示，当实现如本文所描述的针对计算设备 100 的平台初始化时，引导流 502 通常是连续的。如上文所讨论的，当 BIOS 模块 204 在初始化平台时遇到安全协处理器命令 504 时，命令 504 被传输给安全协处理器驱动器模块 202 以由安全协处理器 120 执行。命令 504 被添加到等待执行的命令 504 的命令列表，并且 BIOS 模块 204 继续与安全协处理器 120 无关的平台初始化。当所建立的安全协处理器中断被触发(例如通过给定时间段的过期)时，安全协处理器中断处置器 210 确定安全协处理器 120 是否具有针对之前提交的命令 504 的准备就绪的响应，并且如果是，则接收响应，将响应转发给 BIOS 模块 204，并且将命令列表中的下一命令 504 发送给安全协处理器 120 以供执行。这样，存在与初始化安全协处理器 120 相关联的最小或以其他方式减小的时延。然而，如图 6 中说明性示出的，

初始化安全协处理器120的传统方法涉及与等待来自安全协处理器120的针对每一个所提交的命令604响应相关联的大量时间延迟。特别地，当BIOS模块204遇到安全协处理器命令604时，命令604被传输给安全协处理器120。BIOS模块204在继续平台初始化之前必须等待来自安全协处理器120的针对所提交的命令604的响应。因为安全协处理器120的初始化典型地涉及执行若干(例如二十个或更多)安全协处理器命令604，所以时延在实现传统平台初始化时是明显的。例如，在TPM的情况下，“TpmSelfTest”命令必须在PEI（预先可扩展固件接口初始化)BIOS阶段期间发送给TPM，这花费大量时间从TPM接收响应。

[0026] 示例

下面提供本文所公开的设备、系统和方法的说明性示例。设备、系统和方法的实施例可以包括以下所描述的示例中的任何一个或多个以及其任何组合。

[0027] 示例1包括用于改进平台初始化的计算设备，该计算设备包括执行提交至其的安全协处理器命令的安全协处理器；开始计算设备的平台的初始化的基本输入/输出系统模块；响应于从基本输入/输出系统模块接收到安全协处理器命令而将安全协处理器命令添加到命令列表的安全协处理器驱动器模块；以及建立平台的初始化的周期性中断的计时器模块，其中安全协处理器驱动器模块还响应于周期性中断的出现而(i)关于针对之前提交的安全协处理器命令的安全协处理器响应的可用性查询安全协处理器，并且(ii)响应于接收到可用的安全协处理器响应而将可用的安全协处理器响应转发给基本输入/输出系统模块。

[0028] 示例2包括示例1的主题，并且其中安全协处理器驱动器模块还响应于接收到可用的安全协处理器响应而将命令列表中的下一安全协处理器命令提交至安全协处理器。

[0029] 示例3包括示例1和2中任一个的主题，并且其中安全协处理器包括可信平台模块。

[0030] 示例4包括示例1-3中任一个的主题，并且其中安全协处理器包括可管理性引擎。

[0031] 示例5包括示例1-4中任一个的主题，并且其中安全协处理器包括会聚安全引擎。

[0032] 示例6包括示例1-5中任一个的主题，并且其中安全协处理器包括带外处理器。

[0033] 示例7包括示例1-6中任一个的主题，并且其中基本输入/输出模块还响应于从周期性中断的返回而继续平台的初始化。

[0034] 示例8包括示例1-7中任一个的主题，并且其中计时器模块还响应于不涉及安全协处理器命令的初始化过程的完成而不继续初始化的周期性中断。

[0035] 示例9包括示例1-8中任一个的主题，并且其中安全协处理器驱动器模块还响应于不涉及安全协处理器命令的初始化过程的完成而(i)将命令列表中所剩余的每一个安全协处理器命令提交至安全协处理器，并且(ii)对于剩余安全协处理器命令中的每一个，响应于接收到针对剩余安全协处理器命令中的一个的可用的安全协处理器响应而将可用的安全协处理器响应转发给基本输入/输出系统模块。

[0036] 示例10包括示例1-9中任一个的主题，并且其中基本输入/输出系统模块还响应于初始化过程的完成而引导计算设备的操作系统。

[0037] 示例11包括示例1-10中任一个的主题，并且其中命令列表遵循先进先出系统。

[0038] 示例12包括示例1-11中任一个的主题，并且其中命令列表遵循后进先出系统。

[0039] 示例13包括用于改进计算设备的平台初始化的方法，该方法包括使用计算设备

的基本输入/输出系统开始计算设备的平台的初始化;利用计算设备的安全协处理器驱动器并且从基本输入/输出系统接收要由计算设备的安全协处理器执行的安全协处理器命令;响应于接收到安全协处理器命令而利用安全协处理器驱动器将安全协处理器命令添加到命令列表;以及利用计算设备周期性地中断平台的初始化以(i)关于针对之前提交的安全协处理器命令的安全协处理器响应的可用性查询安全协处理器,并且(ii)响应于接收到可用的安全协处理器响应而将可用的安全协处理器响应转发给基本输入/输出系统模块。

[0040] 示例14包括示例13的主题,并且其中中断平台的初始化包括响应于接收到可用的安全协处理器响应而将命令列表中的下一安全协处理器命令提交至安全协处理器。

[0041] 示例15包括示例13和14中任一个的主题,并且其中接收安全协处理器命令包括利用计算设备的可信平台模块驱动器并且从基本输入/输出系统接收要由计算设备的可信平台模块执行的可信平台模块命令;其中将安全协处理器命令添加到命令列表包括响应于接收到可信平台模块命令而利用可信平台模块驱动器将可信平台模块命令添加到命令列表;并且其中中断平台的初始化包括利用计算设备周期性地中断平台的初始化以(i)关于针对之前提交的可信平台模块命令的可信平台模块响应的可用性查询可信平台模块,并且(ii)响应于接收到可用的可信平台模块响应而将可用的可信平台模块响应转发给基本输入/输出系统模块。

[0042] 示例16包括示例13-15中任一个的主题,并且其中中断平台的初始化包括响应于接收到可用的可信平台模块响应而将命令列表中的下一可信平台模块命令提交至可信平台模块。

[0043] 示例17包括示例13-16中任一个的主题,并且其中接收安全协处理器命令包括利用计算设备的可管理性引擎驱动器并且从基本输入/输出系统接收要由计算设备的可管理性引擎执行的可管理性引擎命令;其中将安全协处理器命令添加到命令列表包括响应于接收到可管理性引擎命令而利用可管理性引擎驱动器将可管理性引擎命令添加到命令列表;并且其中中断平台的初始化包括利用计算设备周期性地中断平台的初始化以(i)关于针对之前提交的可管理性引擎命令的可管理性引擎响应的可用性查询可管理性引擎,并且(ii)响应于接收到可用的可管理性引擎响应而将可用的可管理性引擎响应转发给基本输入/输出系统模块。

[0044] 示例18包括示例13-17中任一个的主题,并且其中接收安全协处理器命令包括利用计算设备的会聚安全引擎驱动器并且从基本输入/输出系统接收要由计算设备的会聚安全引擎执行的会聚安全引擎命令;其中将安全协处理器命令添加到命令列表包括响应于接收到会聚安全引擎命令而利用会聚安全引擎驱动器将会聚安全引擎命令添加到命令列表;并且其中中断平台的初始化包括利用计算设备周期性地中断平台的初始化以(i)关于针对之前提交的会聚安全引擎命令的会聚安全引擎响应的可用性查询会聚安全引擎,并且(ii)响应于接收到可用的会聚安全引擎响应而将可用的会聚安全引擎响应转发给基本输入/输出系统模块。

[0045] 示例19包括示例13-18中任一个的主题,并且还包括响应于从周期性中断的返回而在计算设备上继续平台的初始化。

[0046] 示例20包括示例13-19中任一个的主题,并且还包括响应于完成不涉及安全协处理器命令的初始化过程而在计算设备上不继续初始化的周期性中断。

[0047] 示例 21 包括示例 13-20 中任一个的主题，并且还包括利用计算设备并且响应于完成不涉及安全协处理器命令的初始化过程而将命令列表中所剩余的每一个安全协处理器命令提交至安全协处理器；并且对于剩余安全协处理器命令中的每一个，利用计算设备并且响应于接收到针对剩余安全协处理器命令中的一个的可用的安全协处理器响应而将可用的安全协处理器响应转发给基本输入 / 输出系统。

[0048] 示例 22 包括示例 13-21 中任一个的主题，并且还包括响应于完成初始化过程而在计算设备上引导计算设备的操作系统。

[0049] 示例 23 包括示例 13-22 中任一个的主题，并且其中将命令列表中的下一安全协处理器命令提交至安全协处理器包括基于先进先出将命令列表中的下一安全协处理器命令提交至安全协处理器。

[0050] 示例 24 包括示例 13-23 中任一个的主题，并且其中将命令列表中的下一安全协处理器命令提交至安全协处理器包括基于后进先出将命令列表中的下一安全协处理器命令提交至安全协处理器。

[0051] 示例 25 包括计算设备，其包括：处理器；以及具有存储在其中的多个指令的存储器，所述指令在由处理器执行时使计算设备执行示例 13-24 中任一个的方法。

[0052] 示例 26 包括一个或多个机器可读存储介质，其包括存储在其上的多个指令，所述指令响应于被执行而导致计算设备执行示例 13-24 中任一个的方法。

[0053] 示例 27 包括用于改进平台初始化的计算设备，该计算设备包括用于使用计算设备的基本输入 / 输出系统开始计算设备的平台的初始化的装置；用于利用计算设备的安全协处理器驱动器并且从基本输入 / 输出系统接收要由计算设备的安全协处理器执行的安全协处理器命令的装置；用于响应于接收到安全协处理器命令而利用安全协处理器驱动器将安全协处理器命令添加到命令列表的装置；以及用于周期性地中断平台的初始化以进行以下的装置：(i) 关于针对之前提交的安全协处理器命令的安全协处理器响应的可用性查询安全协处理器，并且 (ii) 响应于接收到可用的安全协处理器响应而将可用的安全协处理器响应转发给基本输入 / 输出系统模块。

[0054] 示例 28 包括示例 27 的主题，并且其中用于中断平台的初始化的装置包括用于响应于接收到可用的安全协处理器响应而将命令列表中的下一安全协处理器命令提交至安全协处理器的装置。

[0055] 示例 29 包括示例 27 和 28 中任一个的主题，并且其中用于接收安全协处理器命令的装置包括用于利用计算设备的可信平台模块驱动器并且从基本输入 / 输出系统接收要由计算设备的可信平台模块执行的可信平台模块命令的装置；其中用于将安全协处理器命令添加到命令列表的装置包括用于响应于接收到可信平台模块命令而利用可信平台模块驱动器将可信平台模块命令添加到命令列表的装置；并且其中用于中断平台的初始化的装置包括用于周期性地中断平台的初始化以进行以下的装置：(i) 关于针对之前提交的可信平台模块命令的可信平台模块响应的可用性查询可信平台模块，并且 (ii) 响应于接收到可用的可信平台模块响应而将可用的可信平台模块响应转发给基本输入 / 输出系统模块。

[0056] 示例 30 包括示例 27-29 中任一个的主题，并且其中用于中断平台的初始化的装置包括用于响应于接收到可用的可信平台模块响应而将命令列表中的下一可信平台模块命令提交至可信平台模块的装置。

[0057] 示例 31 包括示例 27-30 中任一个的主题，并且其中用于接收安全协处理器命令的装置包括用于利用计算设备的可管理性引擎驱动器并且从基本输入 / 输出系统接收要由计算设备的可管理性引擎执行的可管理性引擎命令的装置；其中用于将安全协处理器命令添加到命令列表的装置包括用于响应于接收到可管理性引擎命令而利用可管理性引擎驱动器将可管理性引擎命令添加到命令列表的装置；并且其中用于中断平台的初始化的装置包括用于周期性地中断平台的初始化以进行以下的装置：(i) 关于针对之前提交的可管理性引擎命令的可管理性引擎响应的可用性查询可管理性引擎，并且 (ii) 响应于接收到可用的可管理性引擎响应而将可用的可管理性引擎响应转发给基本输入 / 输出系统模块。

[0058] 示例 32 包括示例 27-31 中任一个的主题，并且其中用于接收安全协处理器命令的装置包括用于利用计算设备的会聚安全引擎驱动器并且从基本输入 / 输出系统接收要由计算设备的会聚安全引擎执行的会聚安全引擎命令的装置；其中用于将安全协处理器命令添加到命令列表的装置包括用于响应于接收到会聚安全引擎命令而利用会聚安全引擎驱动器将会聚安全引擎命令添加到命令列表的装置；并且其中用于中断平台的初始化的装置包括用于周期性地中断平台的初始化以进行以下的装置：(i) 关于针对之前提交的会聚安全引擎命令的会聚安全引擎响应的可用性查询会聚安全引擎，并且 (ii) 响应于接收到可用的会聚安全引擎响应而将可用的会聚安全引擎响应转发给基本输入 / 输出系统模块。

[0059] 示例 33 包括示例 27-32 中任一个的主题，并且还包括用于响应于从周期性中断的返回而继续平台的初始化的装置。

[0060] 示例 34 包括示例 27-33 中任一个的主题，并且还包括用于响应于完成不涉及安全协处理器命令的初始化过程而不继续初始化的周期性中断的装置。

[0061] 示例 35 包括示例 27-34 中任一个的主题，并且还包括用于响应于完成不涉及安全协处理器命令的初始化过程而将命令列表中所剩余的每一个安全协处理器命令提交至安全协处理器的装置；以及用于针对剩余安全协处理器命令中的每一个，响应于接收到针对剩余安全协处理器命令中的一个的可用的安全协处理器响应而将可用的安全协处理器响应转发给基本输入 / 输出系统的装置。

[0062] 示例 36 包括示例 27-35 中任一个的主题，并且还包括用于响应于完成初始化过程而引导计算设备的操作系统的装置。

[0063] 示例 37 包括示例 27-36 中任一个的主题，并且其中用于将命令列表中的下一安全协处理器命令提交至安全协处理器的装置包括用于基于先进先出将命令列表中的下一安全协处理器命令提交至安全协处理器的装置。

[0064] 示例 38 包括示例 27-37 中任一个的主题，并且其中用于将命令列表中的下一安全协处理器命令提交至安全协处理器的装置包括用于基于后进先出将命令列表中的下一安全协处理器命令提交至安全协处理器的装置。

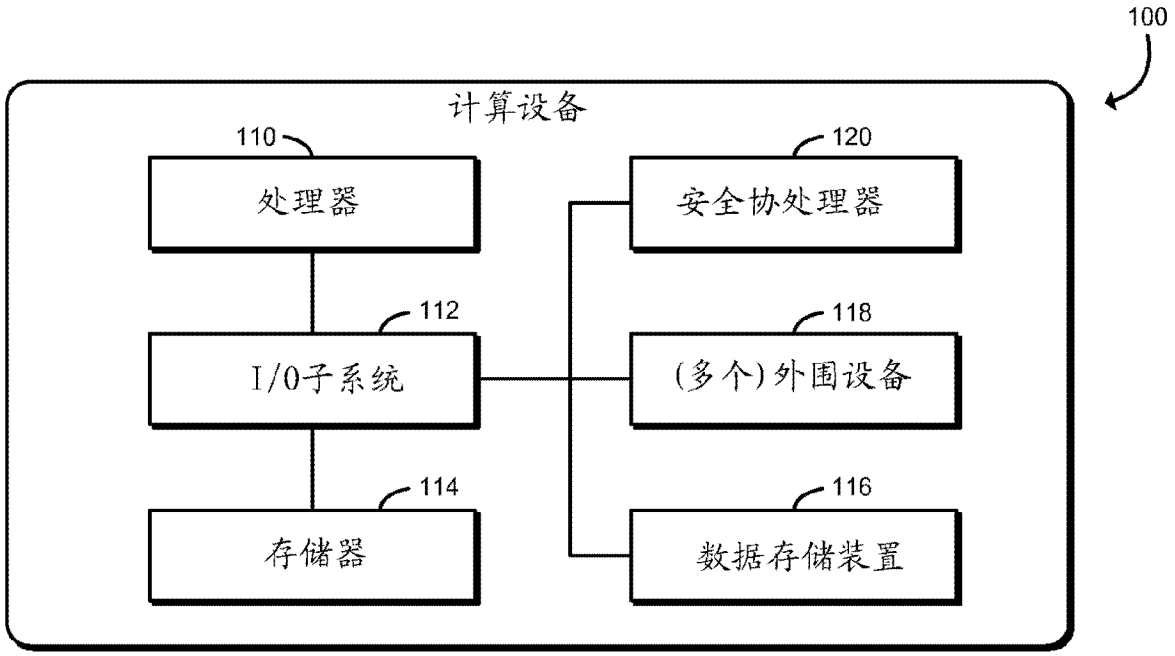

100
计算设备
110
处理器
120
安全协处理器
112
I/O子系统
118
(多个)外围设备
114
存储器
116
数据存储装置

图 1

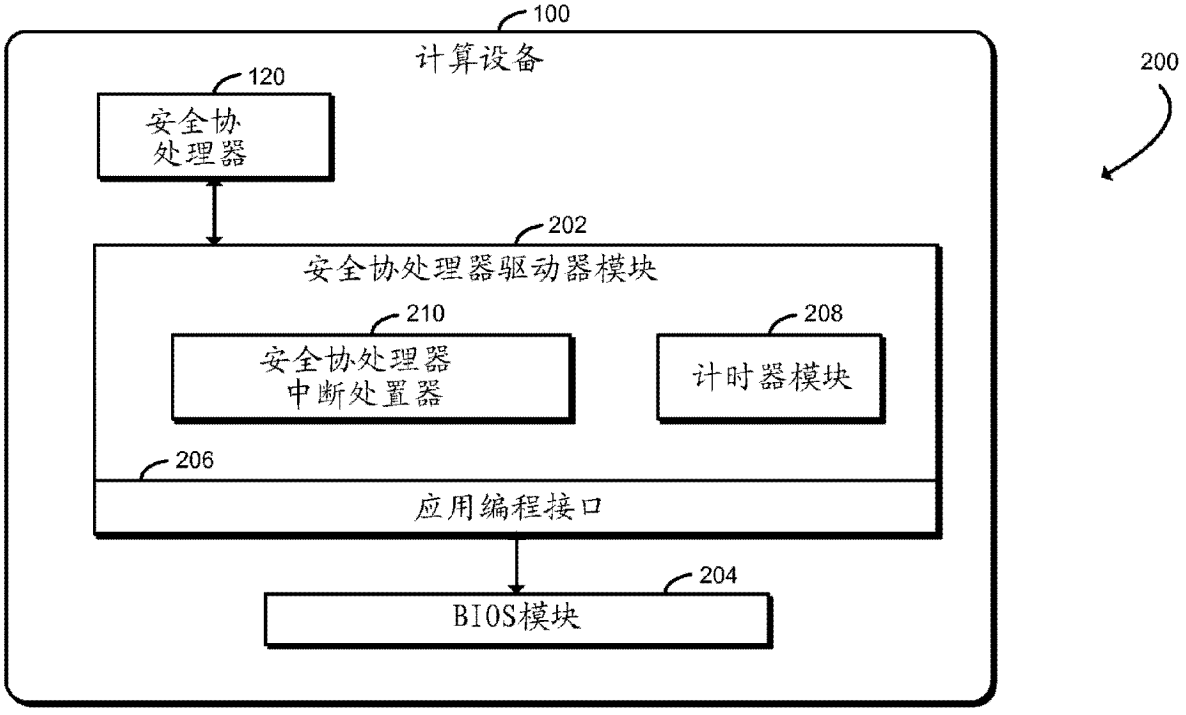

100
计算设备
200
120
安全协
处理器
202
安全协处理器驱动器模块
210
安全协处理器
中断处置器
208
计时器模块
206
应用编程接口
204
BIOS模块

图 2

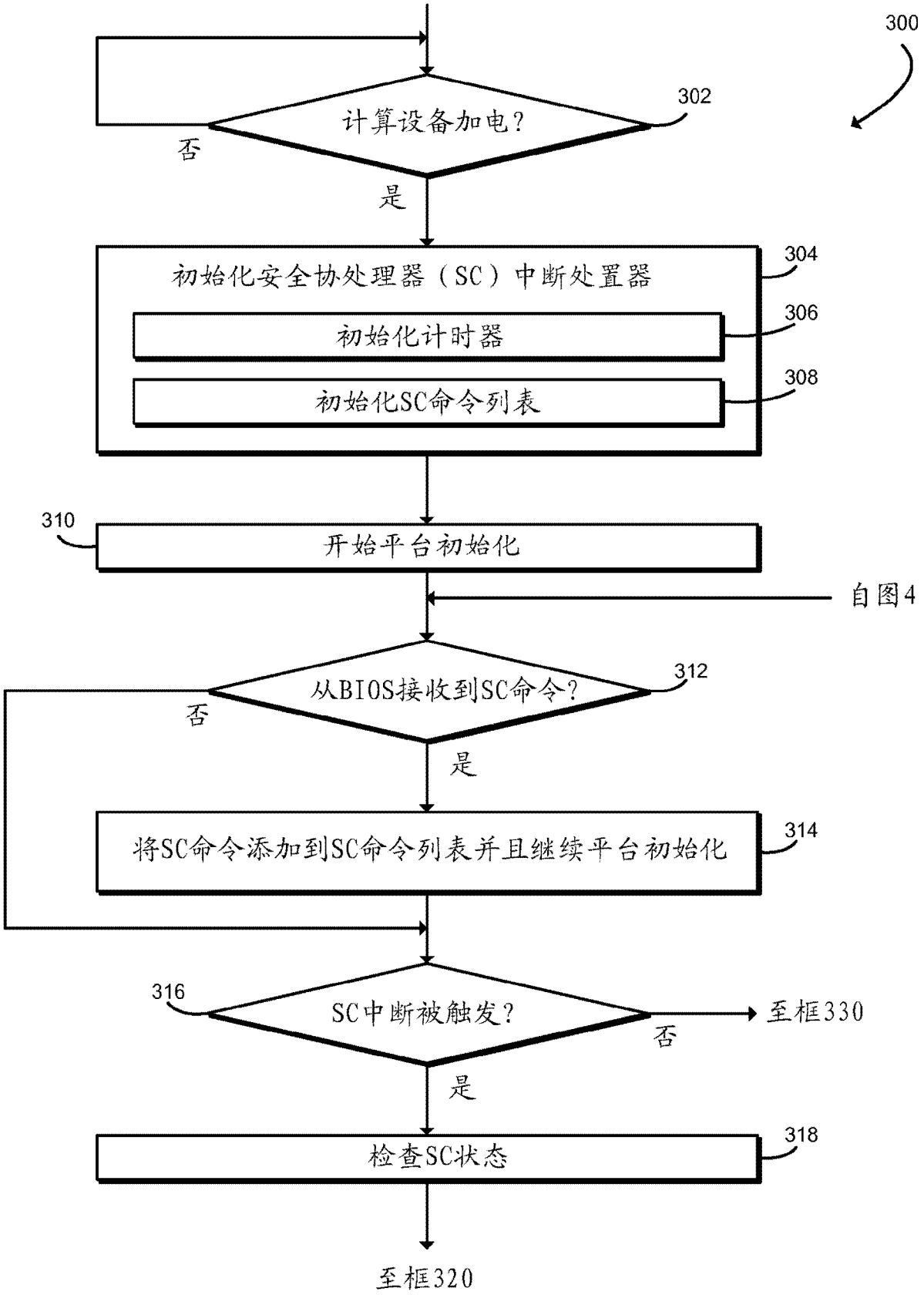

300
计算设备加电？
302
否
是
初始化安全协处理器（SC）中断处置器
304
初始化计时器
306
初始化SC命令列表
308
310
开始平台初始化
自图4
从BIOS接收到SC命令？
312
否
是
将SC命令添加到SC命令列表并且继续平台初始化
314
316
SC中断被触发？
至框330
否
是
检查SC状态
318
至框320

图 3

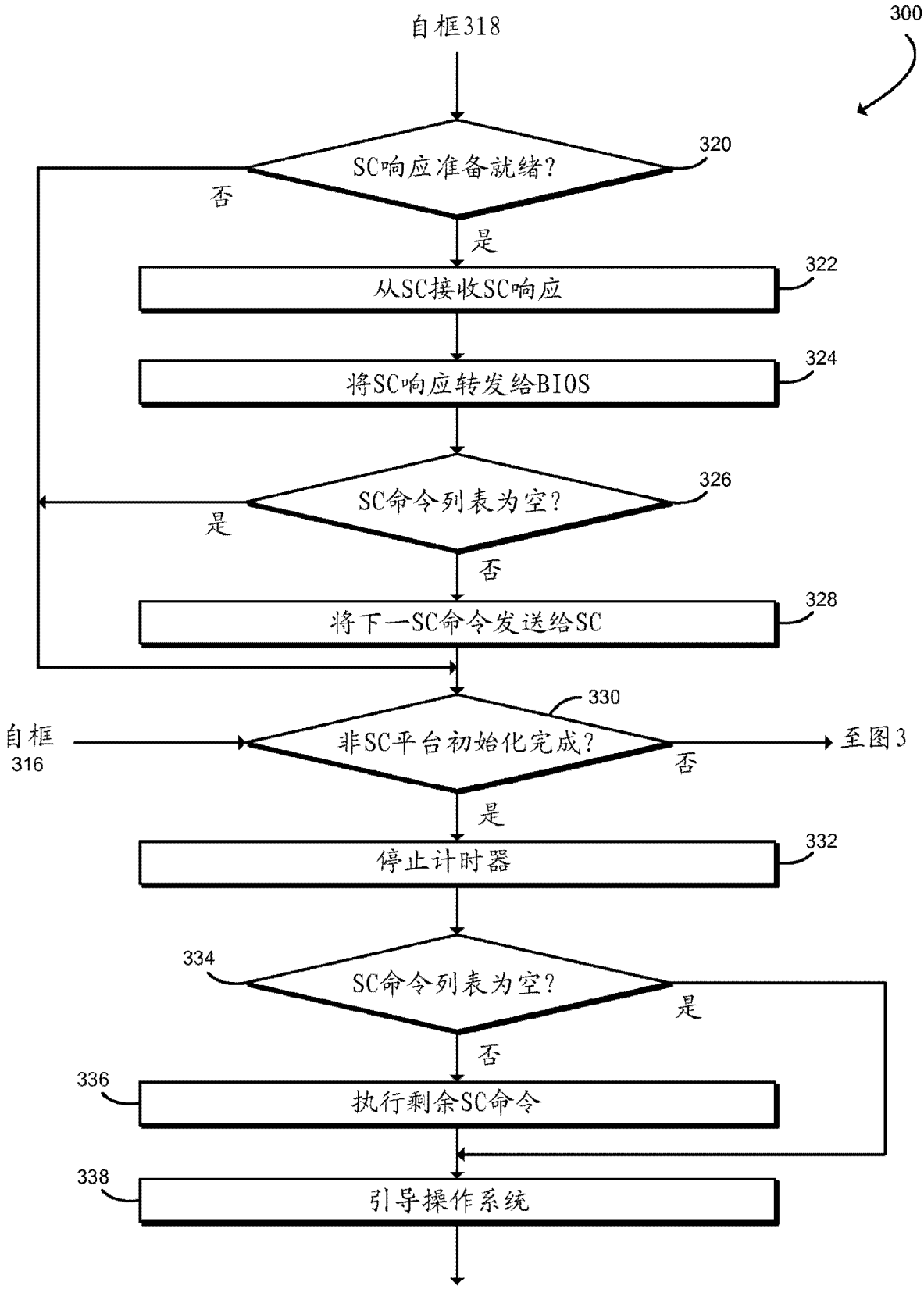

300
自框318
SC响应准备就绪?
320
否
是
从SC接收SC响应
322
将SC响应转发给BIOS
324
SC命令列表为空?
326
是
否
将下一SC命令发送给SC
328
自框
316
非SC平台初始化完成?
330
至图3
否
是
停止计时器
332
SC命令列表为空?
334
是
否
执行剩余SC命令
336
引导操作系统
338

图 4

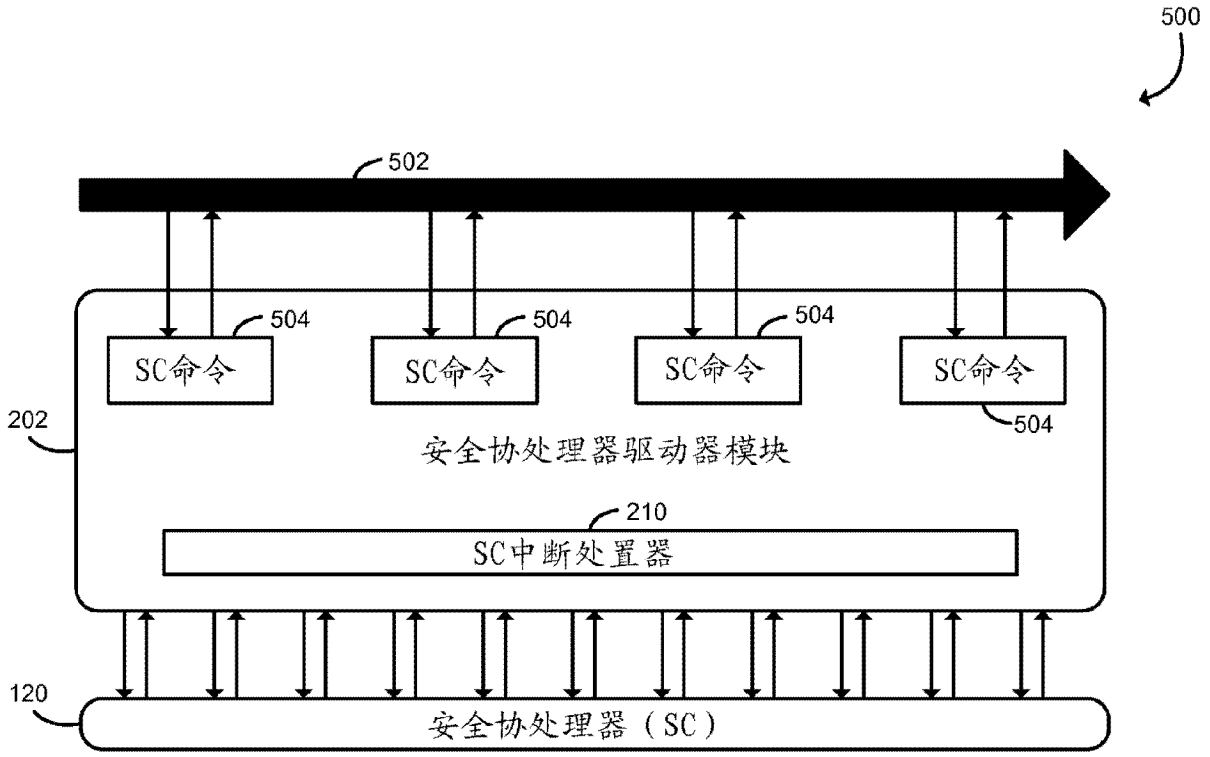

500
502
504
SC命令
SC命令
SC命令
SC命令
504
202
安全协处理器驱动器模块
210
SC中断处置器
120
安全协处理器（SC）

图 5

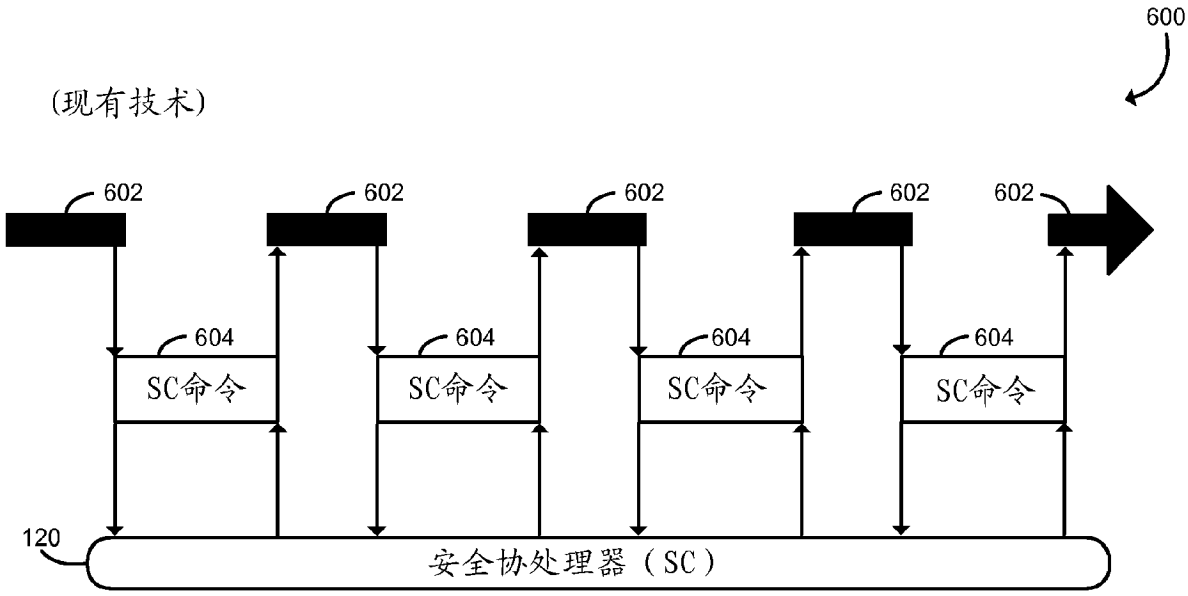

600
(现有技术)
602
602
602
602
602
604
SC命令
604
SC命令
604
SC命令
604
SC命令
120
安全协处理器（SC）

图 6