



(12) 发明专利申请

(10) 申请公布号 CN 112740209 A

(43) 申请公布日 2021. 04. 30

(21) 申请号 201980061881.9

(22) 申请日 2019.09.11

(30) 优先权数据

10-2018-0112989 2018.09.20 KR

(85) PCT国际申请进入国家阶段日

2021.03.19

(86) PCT国际申请的申请数据

PCT/KR2019/011774 2019.09.11

(87) PCT国际申请的公布数据

W02020/060101 KO 2020.03.26

(71) 申请人 三星电子株式会社

地址 韩国京畿道

(72) 发明人 李宅基 金钟洙 权恩荣 李达姆

赵大行

(74) 专利代理机构 北京市立方律师事务所

11330

代理人 谢玉斌

(51) Int.Cl.

G06F 21/56 (2006.01)

G06F 21/60 (2006.01)

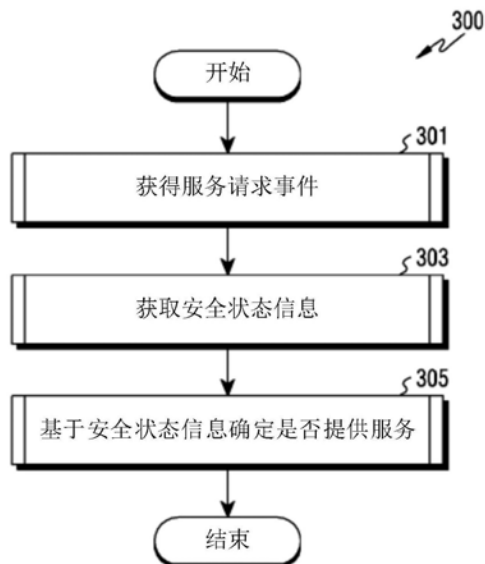
权利要求书2页 说明书22页 附图14页

(54) 发明名称

通过使用安全元件提供服务的电子装置及其操作方法

(57) 摘要

本发明的各个实施例涉及用于通过使用安全元件来提供服务的电子装置及其操作方法。所述电子装置包括：处理器，所述处理器用于获取所述电子装置的安全状态信息；以及安全元件，所述安全元件在所述处理器的控制下操作，从所述处理器接收所述电子装置的安全状态信息，并包括用于存储接收到的所述电子装置的安全状态信息的存储库，其中，所述安全元件感测安全相关服务请求命令，从所述存储库获取关于所述电子装置的安全状态信息，以及能够基于所获取的所述电子装置的安全状态信息是否满足指定条件来对感测到的安全相关服务请求命令进行处理或忽略。其他实施例也是可行的。



1. 一种电子装置,所述电子装置包括:
处理器,所述处理器用于获取所述电子装置的安全状态信息;以及
安全元件,所述安全元件在所述处理器的控制下运行,从所述处理器接收所述电子装置的安全状态信息,并包括用于存储接收到的所述电子装置的安全状态信息的存储库,
其中,所述安全元件获得安全相关服务请求命令,
从所述存储库获取所述电子装置的安全状态信息,以及
基于所获取的所述电子装置的安全状态信息是否满足指定条件来对感测到的安全相关服务请求命令进行处理或忽略。
2. 根据权利要求1所述的电子装置,其中,所述电子装置的安全状态信息包括以下至少一项:关于所述电子装置的rooting或non-rooting的信息、关于是否感测到恶意软件的信息、关于是否改变保修位的信息、关于是否仿冒访问规则执行器的信息、关于所述电子装置的系统区域的安全状态信息、或关于安装在所述电子装置中的应用的安全状态信息。
3. 根据权利要求1所述的电子装置,其中,所述安全状态信息指示了安全等级或安全问题的类型中的至少一项。
4. 根据权利要求1所述的电子装置,其中,所述指定条件是基于所述安全相关服务请求命令的类型来确定的。
5. 根据权利要求1所述的电子装置,其中,所述安全相关服务请求命令是从所述处理器或外部电子装置接收到的。
6. 根据权利要求1所述的电子装置,其中,所述安全元件响应于所获取的所述电子装置的安全状态信息满足所述指定条件,正常处理所获得的安全相关服务请求命令以执行与所述命令相对应的功能,并响应于所获取的所述电子装置的安全状态信息不满足所述指定条件,忽略感测到的安全相关服务请求命令。
7. 根据权利要求1所述的电子装置,其中,所述安全元件从所述处理器接收与所述安全相关服务请求命令相关的应用的安全状态信息,
从存储在所述存储库中的所述电子装置的安全状态信息获取与所述安全相关服务请求命令相关的应用的安全状态信息,以及
基于接收到的应用的安全状态信息和获取的所述应用的安全状态信息是否一致,处理或忽略感测到的安全相关服务请求命令。
8. 根据权利要求7所述的电子装置,其中,所述处理器在所述应用被安装在所述电子装置中的时间点,确定所述应用的安全状态信息,以及
控制将确定的所述应用的安全状态信息发送到所述安全元件,其中所述安全状态信息存储在所述安全元件的存储库中。
9. 根据权利要求1所述的电子装置,其中,所述安全元件确定所述电子装置的安全状态信息是否满足与仿冒访问规则执行器相关的条件,
当所述电子装置的安全状态信息不满足与仿冒访问规则执行器相关的所述条件时,识别与感测到的安全相关服务请求命令相对应的接口,
当所识别的接口是与仿冒访问规则执行器相对应的接口时,忽略感测到的安全相关服务请求命令,以及
当所识别的接口不是与仿冒访问规则执行器相对应的接口时,执行与感测到的安全相

关服务请求命令相对应的功能。

10. 根据权利要求9所述的电子装置,其中,所述安全元件向所述处理器或所述外部电子装置提供对所述安全相关服务请求的响应信号,并且

其中,所述响应信号包括以下各项中的至少一项:所述安全相关服务请求命令所请求的信息、指示所述安全相关服务请求命令所执行的功能的结果的信息、或指示是否许可安全相关服务的信息。

11. 一种电子装置的操作方法,所述方法包括:

处理器获取所述电子装置的安全状态信息;

在所述处理器的控制下运行的安全元件将所述电子装置的安全状态信息存储在所述安全元件内的存储库中;

所述安全元件感测安全相关服务请求命令;

所述安全元件获取存储在内部存储库中的所述电子装置的安全状态信息;以及

所述安全元件基于所获取的所述电子装置的安全状态信息是否满足指定条件来对感测到的安全相关服务请求命令进行处理或忽略。

12. 根据权利要求11所述的方法,其中,所述电子装置的安全状态信息包括以下至少一项:关于所述电子装置的rooting或non-rooting的信息、关于是否感测到恶意软件的信息、关于是否改变保修位的信息、关于是否仿冒访问规则执行器的信息、关于所述电子装置的系统区域的安全状态信息、或关于安装在所述电子装置中的应用的安全状态信息,

所述安全状态信息指示了安全等级或安全问题的类型中的至少一项,

所述指定条件是基于所述安全相关服务请求命令的类型来确定的,并且

所述安全相关服务请求命令是从所述处理器或外部电子装置接收到的。

13. 根据权利要求11所述的方法,其中,所述安全元件对感测到的安全相关服务请求命令进行处理或忽略包括:

所述安全元件响应于所获取的所述电子装置的安全状态信息满足所述指定条件,正常处理感测到的安全相关服务请求命令以执行与所述命令相对应的功能,以及

所述安全元件响应于所获取的所述电子装置的安全状态信息不满足所述指定条件,忽略感测到的安全相关服务请求命令。

14. 根据权利要求11所述的方法,所述方法还包括所述安全元件从所述处理器接收与所述安全相关服务请求命令相关的应用的安全状态信息,

其中,所述安全元件对感测到的安全相关服务请求命令进行处理或忽略包括:

所述安全元件从获取的安全状态信息识别与所述安全相关服务请求命令相关的应用的安全状态信息;以及

所述安全元件基于接收到的所述应用的安全状态信息和所识别的所述应用的安全状态信息是否一致来对感测到的安全相关服务请求命令进行处理或忽略。

15. 根据权利要求14所述的方法,所述方法还包括:

所述处理器在所述应用被安装在所述电子装置中的时间点,确定所述应用的安全状态信息;以及

所述处理器控制将所确定的所述应用的安全状态信息发送到所述安全元件,其中所述安全状态信息存储在所述安全元件的存储库中。

通过使用安全元件提供服务的电子装置及其操作方法

技术领域

[0001] 本公开的各种实施例涉及用于通过使用安全元件来提供服务的电子装置及其操作方法。

背景技术

[0002] 电子装置可以通过使用安全元件来提供各种安全相关服务。安全元件是用于生成、存储和/或管理对安全敏感的信息(例如,凭证)的硬件模块。安全元件存储诸如信用支付服务或交通卡之类的服务应用程序,并存储和/或管理与个人身份或凭证有关的证书(例如,身份证、居民登记证、驾驶执照、入学证、护照或电子标识(电子ID))。

[0003] 安全元件被设计为在其自己的安全元件芯片中具有独立的安全性,而与获得对该安全元件的访问权的另一元件(例如,卡外实体(OCE))的安全质量无关。例如,安全元件被设计为以硬件或软件方式感测各种非法攻击,并安全地保护存储在安全元件中的信息免受感测到的非法攻击。

发明内容

[0004] 技术问题

[0005] 安全元件被安装在诸如移动设备或IoT设备等需要安全性的电子装置中并从属于其使用。例如,当从电子装置的主处理器接收到有效命令时,安全元件在不受特定限制的情况下对与接收的命令相对应的功能进行处理。即,安全元件从属于主处理器操作,并且因此在不过滤的情况下处理从主处理器输入的所有有效命令。因此,当在电子装置中产生安全威胁时,电子装置中包括的安全元件在安全性方面容易受到攻击。例如,当获得电子装置的最高权限(rooted)或电子装置被仿冒时,电子装置中包括的安全元件的访问控制被禁用,因此与安全有关的信息可能受到非法攻击。

[0006] 因此,本公开的各种实施例涉及一种用于基于电子装置的安全状态通过安全元件提供安全服务的电子装置及其操作方法。

[0007] 问题的解决方案

[0008] 根据各种实施例,电子装置可以包括:处理器,所述处理器用于获取所述电子装置的安全状态信息;以及安全元件,所述安全元件在所述处理器的控制下运行,从所述处理器接收所述电子装置的安全状态信息,并包括用于存储接收到的所述电子装置的安全状态信息的存储库。所述安全元件可以感测安全相关服务请求命令,从所述存储库获取所述电子装置的安全状态信息,以及基于所获取的所述电子装置的安全状态信息是否满足指定条件来对感测到的安全相关服务请求命令进行处理或忽略。

[0009] 根据各种实施例,电子装置的操作方法可以包括:处理器获取所述电子装置的安全状态信息;在所述处理器的控制下运行的安全元件将所述电子装置的安全状态信息存储在所述安全元件内的存储库中;所述安全元件感测安全相关服务请求命令;所述安全元件获取存储在内部存储库中的所述电子装置的安全状态信息;以及所述安全元件基于所获取

的所述电子装置的安全状态信息是否满足指定条件来对感测到的安全相关服务请求命令进行处理或忽略。

[0010] 本发明的有益效果

[0011] 各种实施例可以基于电子装置中的电子装置的安全状态通过安全元件来确定是否提供服务,从而在电子装置的安全性易受攻击的状态下防止存储在安全元件中的安全相关信息受到非法攻击,并且提供更高质量的安全相关服务。

附图说明

[0012] 图1是根据各种实施例的在网络环境内的电子装置的框图。

[0013] 图2是示出根据各种实施例的在安全元件与其他组件之间的通信结构的框图。

[0014] 图3是根据各种实施例的基于电子装置中的电子装置的安全状态信息来提供安全相关服务的流程图。

[0015] 图4是根据各种实施例的在电子装置中存储电子装置的安全状态信息的流程图。

[0016] 图5是根据各种实施例的在电子装置中存储电子装置的安全状态信息的示例图。

[0017] 图6是根据各种实施例的基于电子装置中的电子装置的安全状态信息提供使用了应用的安全相关服务的流程图。

[0018] 图7是根据各种实施例的基于电子装置中的电子装置的安全状态信息提供使用了应用的安全相关服务的示例图。

[0019] 图8是根据各种实施例的基于电子装置中的电子装置的安全状态信息提供使用了应用的安全相关服务的信号流程图。

[0020] 图9是根据各种实施例的基于电子装置中的电子装置的安全状态信息通过无线接口提供服务的流程图。

[0021] 图10是根据各种实施例的基于电子装置中的电子装置的安全状态信息通过无线接口提供服务的示例图。

[0022] 图11是根据各种实施例的基于电子装置中的电子装置的安全状态信息来控制对使用通信接口的安全元件的访问的流程图。

[0023] 图12是根据各种实施例的基于电子装置中的电子装置的安全状态信息来控制对使用通信接口的安全元件的访问的示例图。

[0024] 图13是根据各种实施例的基于电子装置中的电子装置的安全状态信息来提供安全相关信息的流程图。

[0025] 图14是根据各种实施例的基于电子装置中的电子装置的安全状态信息来提供安全相关信息的示例图。

[0026] 图15是根据各种实施例的基于电子装置中的电子装置的安全状态信息来提供安全相关信息的信号流程图。

[0027] 最佳实施方式

[0028] 下面参考附图提及本文件的各种实施例。应当理解,实施例和其中使用的术语无意将其中阐述的技术限制为特定实施例形式,而是包括相应实施例的各种修改,等同形式和/或替代形式。关于附图的描述,相同的参考符号可以用于相同的组件。除非另有明确说明,否则单数形式的表达可以包括复数形式的表达。

[0029] 图1是示出根据各种实施例的网络环境100中的电子装置101的框图。参照图1,网络环境100中的电子装置101可经由第一网络198(例如,短程无线通信网络)与电子装置102进行通信,或者经由第二网络199(例如,远程无线通信网络)与电子装置104或服务器108进行通信。根据实施例,电子装置101可经由服务器108与电子装置104进行通信。根据实施例,电子装置101可包括处理器120、存储器130、输入装置150、声音输出装置155、显示装置160、音频模块170、传感器模块176、接口177、触觉模块179、相机模块180、电力管理模块188、电池189、通信模块190、用户识别模块(SIM) 196或天线模块197。在一些实施例中,可从电子装置101中省略所述部件中的至少一个(例如,显示装置160或相机模块180),或者可将一个或更多个其它部件添加到电子装置101中。在一些实施例中,可将所述部件中的一些部件实现为单个集成电路。例如,可将传感器模块176(例如,指纹传感器、虹膜传感器、或照度传感器)实现为嵌入在显示装置160(例如,显示器)中。

[0030] 处理器120可运行例如软件(例如,程序140)来控制电子装置101的与处理器120连接的至少一个其它部件(例如,硬件部件或软件部件),并可执行各种数据处理或计算。根据实施例,作为所述数据处理或计算的至少部分,处理器120可将从另一部件(例如,传感器模块176或通信模块190)接收到的命令或数据加载到易失性存储器132中,对存储在易失性存储器132中的命令或数据进行处理,并将结果数据存储在非易失性存储器134中。根据实施例,处理器120可包括主处理器121(例如,中央处理器(CPU)或应用处理器(AP))以及与主处理器121在操作上独立的或者相结合的辅助处理器123(例如,图形处理单元(GPU)、图像信号处理器(ISP)、传感器中枢处理器或通信处理器(CP))。另外地或者可选择地,辅助处理器123可被适配为比主处理器121耗电更少,或者被适配为具体用于指定的功能。可将辅助处理器123实现为与主处理器121分离,或者实现为主处理器121的部分。

[0031] 在主处理器121处于未激活(例如,睡眠)状态时,辅助处理器123可控制与电子装置101(而非主处理器121)的部件之中的至少一个部件(例如,显示装置160、传感器模块176或通信模块190)相关的功能或状态中的至少一些,或者在主处理器121处于激活状态(例如,运行应用)时,辅助处理器123可与主处理器121一起来控制与电子装置101的部件之中的至少一个部件(例如,显示装置160、传感器模块176或通信模块190)相关的功能或状态中的至少一些。根据实施例,可将辅助处理器123(例如,图像信号处理器或通信处理器)实现为在功能上与辅助处理器123相关的另一部件(例如,相机模块180或通信模块190)的部分。

[0032] 存储器130可存储由电子装置101的至少一个部件(例如,处理器120或传感器模块176)使用的各种数据。所述各种数据可包括例如软件(例如,程序140)以及针对与其相关的命令的输入数据或输出数据。存储器130可包括易失性存储器132或非易失性存储器134。

[0033] 可将程序140作为软件存储在存储器130中,并且程序140可包括例如操作系统(OS) 142、中间件144或应用146。

[0034] 输入装置150可从电子装置101的外部(例如,用户)接收将由电子装置101的其它部件(例如,处理器120)使用的命令或数据。输入装置150可包括例如麦克风、鼠标或键盘。

[0035] 声音输出装置155可将声音信号输出到电子装置101的外部。声音输出装置155可包括例如扬声器或接收器。扬声器可用于诸如播放多媒体或播放唱片的通用目的,接收器可用于呼入呼叫。根据实施例,可将接收器实现为与扬声器分离,或实现为扬声器的部分。

[0036] 显示装置160可向电子装置101的外部(例如,用户)视觉地提供信息。显示装置160

可包括例如显示器、全息装置或投影仪以及用于控制显示器、全息装置和投影仪中的相应一个的控制电路。根据实施例,显示装置160可包括被适配为感测触摸的触摸电路或被适配为测量由触摸引起的力的强度的传感器电路(例如,压力传感器)。

[0037] 音频模块170可将声音转换为电信号,反之亦可。根据实施例,音频模块170可经由输入装置150获得声音,或者经由声音输出装置155或与电子装置101直接(例如,有线地)连接或无线连接的外部电子装置(例如,电子装置102)的耳机输出声音。

[0038] 传感器模块176可感测电子装置101的操作状态(例如,功率或温度)或电子装置101外部的环境状态(例如,用户的状态),然后产生与感测到的状态相应的电信号或数据值。根据实施例,传感器模块176可包括例如手势传感器、陀螺仪传感器、大气压力传感器、磁性传感器、加速度传感器、握持传感器、接近传感器、颜色传感器、红外(IR)传感器、生物特征传感器、温度传感器、湿度传感器或照度传感器。

[0039] 接口177可支持将用来使电子装置101与外部电子装置(例如,电子装置102)直接(例如,有线地)或无线连接的一个或更多个特定协议。根据实施例,接口177可包括例如高清晰度多媒体接口(HDMI)、通用串行总线(USB)接口、安全数字(SD)卡接口或音频接口。

[0040] 连接端178可包括连接器,其中,电子装置101可经由所述连接器与外部电子装置(例如,电子装置102)物理连接。根据实施例,连接端178可包括例如HDMI连接器、USB连接器、SD卡连接器或音频连接器(例如,耳机连接器)。

[0041] 触觉模块179可将电信号转换为可被用户经由他的触觉或动觉识别的机械刺激(例如,振动或运动)或电刺激。根据实施例,触觉模块179可包括例如电机、压电元件或电刺激器。

[0042] 相机模块180可捕获静止图像或运动图像。根据实施例,相机模块180可包括一个或更多个透镜、图像传感器、图像信号处理器或闪光灯。

[0043] 电力管理模块188可管理对电子装置101的供电。根据实施例,可将电力管理模块188实现为例如电力管理集成电路(PMIC)的至少部分。

[0044] 电池189可对电子装置101的至少一个部件供电。根据实施例,电池189可包括例如不可再充电的原电池、可再充电的蓄电池、或燃料电池。

[0045] 通信模块190可支持在电子装置101与外部电子装置(例如,电子装置102、电子装置104或服务器108)之间建立直接(例如,有线)通信信道或无线通信信道,并经由建立的通信信道执行通信。通信模块190可包括能够与处理器120(例如,应用处理器(AP))独立操作的一个或更多个通信处理器,并支持直接(例如,有线)通信或无线通信。根据实施例,通信模块190可包括无线通信模块192(例如,蜂窝通信模块、短程无线通信模块或全球导航卫星系统(GNSS)通信模块)或有线通信模块194(例如,局域网(LAN)通信模块或电力线通信(PLC)模块)。这些通信模块中的相应一个可经由第一网络198(例如,短程通信网络,诸如蓝牙、无线保真(Wi-Fi)直连或红外数据协会(IrDA))或第二网络199(例如,远程通信网络,诸如蜂窝网络、互联网、或计算机网络(例如,LAN或广域网(WAN)))与外部电子装置进行通信。可将这些各种类型的通信模块实现为单个部件(例如,单个芯片),或可将这些各种类型的通信模块实现为彼此分离的多个部件(例如,多个芯片)。无线通信模块192可使用存储在用户识别模块196中的用户信息(例如,国际移动用户识别码(IMSI))识别并验证通信网络(诸如第一网络198或第二网络199)中的电子装置101。

[0046] 天线模块197可以向电子装置101的外部(例如,外部电子装置)发送信号或从电子装置101的外部(例如,外部电子装置)接收信号或电力。根据实施例,天线模块197可以由导体或导电图案形成,并且根据一些实施例,除了导体或导电图案之外,并且还可以包括其他组件(例如,RFIC)。根据实施例,天线模块197可以包括一个或多个天线,并且可以例如通过通信模块190(例如,无线通信模块192)从中选择适合于在通信网络(例如,第一网络198或第二网络199)中使用的通信方案的至少一个天线。然后可以经由所选的至少一个天线在通信模块190与外部电子装置之间发送或接收信号或电力。

[0047] 上述部件中的至少一些可经由外设间通信方案(例如,总线、通用输入输出(GPIO)、串行外设接口(SPI)或移动工业处理器接口(MIPI))相互连接并在它们之间通信地传送信号(例如,命令或数据)。

[0048] 根据实施例,可经由与第二网络199连接的服务器108在电子装置101和外部电子装置104之间发送或接收命令或数据。电子装置102和电子装置104中的每一个可以是与电子装置101相同类型的装置,或者是与电子装置101不同类型的装置。根据实施例,将在电子装置101运行的全部操作或一些操作可在外部电子装置102、外部电子装置104或服务器108中的一个或更多个运行。例如,如果电子装置101应该自动执行功能或服务或者应该响应于来自用户或另一装置的请求执行功能或服务,则电子装置101可请求所述一个或更多个外部电子装置执行所述功能或服务中的至少部分,而不是运行所述功能或服务,或者电子装置101除了运行所述功能或服务以外,还可请求所述一个或更多个外部电子装置执行所述功能或服务中的至少部分。接收到所述请求的所述一个或更多个外部电子装置可执行所述功能或服务中的所请求的所述至少部分,或者执行与所述请求相关的另外功能或另外服务,并将执行的结果传送到电子装置101。电子装置101可在对所述结果进行进一步处理的情况下或者在不对所述结果进行进一步处理的情况下将所述结果提供作为对所述请求的至少部分答复。为此,可使用例如云计算技术、分布式计算技术或客户机-服务器计算技术。

[0049] 安全元件172是用于提供、存储和/或管理对安全敏感的信息的模块。安全元件172例如可以存储和/或管理提供信用支付服务或交通卡服务的应用(或小程序),并且可以存储和/或管理信息和/或证书(例如,身份证、居民登记证、驾驶执照、入学证、护照)或与个人身份或证书有关的电子标识(电子ID)。安全元件172可以被实现为独立电路,并且可以包括单独的处理器。安全元件172包括单独的处理器,并且可以根据处理器120的控制进行操作。例如,安全元件172可以从属于处理器120进行操作。安全元件172可以由处理器120或无线通信模块190激活和/或停用。

[0050] 安全元件172可以包括内置在电子装置101的固定芯片中的嵌入式安全元件(eSE)。可以基于与电子装置101的操作系统不同的操作系统来驱动安全元件172。例如,安全元件172可以基于独立的操作系统来操作。根据实施例,安全元件172可以基于安全信道协议与处理器120和/或至少一个另一组件通信。根据实施例,安全元件172可以通过使用单个有线协议(SWP)、ISO或串行外围接口(SPI)来与处理器120和/或至少一个另一组件通信。根据实施例,安全元件172可以安装由服务提供商提供的小程序,并通过使用安装的小程序来提供安全相关服务。根据实施例,安全元件172可以包括用户识别模块196。例如,在所示的图1中,安全元件172和用户识别模块196被构造为单独的模块,但是安全元件和用户识别模块196可以根据设计方案被构造为一个模块。

[0051] 图2是示出根据各种实施例的在安全元件172与至少一个另一组件之间的通信结构的框图200。根据实施例,至少一个另一组件可以是包括在图1的电子装置101中的处理器120。

[0052] 参照图2,各种实施例的处理器120(例如,图1的处理器120)可以通过至少一个接口直接和/或间接地与安全元件172(例如,图1的安全元件172)连接。至少一个接口例如可以包括I2C、SWP、SPI或ISO中的至少一个。编号的接口是仅仅是一个示例,但是本公开的各种实施例将不限于这些。例如,处理器120可以通过除编号的接口之外的遵从其他通信协议的接口直接和/或间接地与安全元件172连接。根据实施例,处理器120可以通过使用单独的访问规则执行器(或访问规则执行模块)通过至少一个另一组件(例如,短程通信模块210(例如,图1的无线通信模块192))与安全元件172间接通信。根据实施例,处理器120可以通过使用访问权限观察器(或访问权限观察模块)直接与安全元件172通信。根据实施例,访问规则执行器可以是用于通过短程通信模块210管理对I2C接口的访问权限和/或对安全元件172的访问权限的软件模块。根据实施例,访问权限观察器可以是用于管理对SPI接口的访问权限和/或通过SPI接口对安全元件172的访问权限的软件模块。

[0053] 根据各种实施例,处理器120可以感测电子装置101的安全状态。根据实施例,处理器120可以获得以下中的至少一项:获得电子装置的最高权限(rooting)或未获得电子装置的最高权限(non-rooting)、是否感测到恶意软件、是否改变(破解)保修位、是否仿冒安全元件172的访问规则执行器、是否感测到电子装置101的系统区域的非法攻击、或者是否感测到对安装在电子装置101中的应用的非法攻击。处理器120可以通过使用本领域技术人员已知的安全状态感测技术来感测电子装置101的安全状态。例如,处理器120可以通过使用保修位来感测电子装置101的安全状态。例如,在启动电子装置101时,处理器120可以检查保修位以确定启动映像是否正常。响应于保修位的改变,处理器120可以确定启动映像是异常的,并且可以通过rooting状态来确定电子装置101的安全状态。这仅仅是一个示例,但是本公开的各种实施例的安全状态感测技术不限于此。例如,根据本公开的各种实施例,可以使用本领域技术人员已知的各种安全状态感测技术。

[0054] 根据各种实施例,处理器120可以将指示感测到的电子装置101的安全状态的安全状态信息提供给安全元件172。例如,电子装置101的安全状态信息可以包括以下信息中的至少一项:指示电子装置101的系统区域的安全状态的信息,或指示安装在电子装置中的应用的安全状态的信息。安全状态信息可以以指示安全等级(或安全质量)或指示安全问题的类型的形式构造。例如,安全等级可以预先被不同地定义为阶梯级的等级0到等级N,并且处理器120可以基于先前定义的安全等级来确定与当前感测到的电子装置101的安全状态相对应的安全等级。例如,“安全等级N”可以是其中安全等级是最高阶而电子装置101是安全的状态,而“安全等级0”可以被定义为其中安全等级是最低阶而电子装置101的安全状态非常弱的状态。“安全等级N-a”可以被定义为其中电子装置101被rooted并因此易受安全性影响的状态,“安全等级N-b”可以被定义为其中电子装置102已经被rooted并且安全元件172的访问规则执行器被仿冒并且因此在安全性方面容受攻击的状态。对于另一示例,电子装置101的安全状态信息可以被定义为指示rooting、仿冒访问规则执行器、感测恶意软件或破解保修位中的至少一个安全问题的状态。响应于获得电子装置101的rooting,处理器120可以提供指示“安全等级N-a”和“rooted”的安全状态信息,并且将提供的安全状态信息提

供给安全元件172。安全状态信息的定义可以由服务提供商和/或设计者确定和/或改变。

[0055] 根据各种实施例,处理器120可以在与实时、周期性时间点或指定事件发生时间点中的至少一个相对应的时间点处感测电子装置101的安全状态,并向安全元件172提供指示感测到的安全状态的安全状态信息。例如,处理器120可以在启动事件发生时间点、应用安装时间点、软件更新时间点、或安全相关服务请求发生时间点中的至少一个时间点处感测电子装置101的安全状态。根据实施例,处理器120可以在每个安全状态感测时间点处向安全元件172提供指示感测到的电子装置101的安全状态的信息。例如,响应于感测电子装置101的安全状态,处理器120可以激活安全元件172,并且将电子装置101的安全状态信息提供给激活的安全元件172。根据实施例,响应于感测到电子装置101的安全状态的改变,处理器120可以将指示改变后的电子装置101的安全状态的信息提供给安全元件172。例如,处理器120可以实时、在周期性时间点处、或指定事件发生时间点处感测电子装置101的安全状态,并且当在当前时间点处感测到的电子装置101的安全状态与在前一时间点处感测到的电子装置101的安全状态的至少一部分彼此不同时,处理器120可以激活安全元件172,并且向激活的安全元件172提供在当前时间点处感测到的电子装置101的安全状态。根据实施例,处理器120可以通过使用安全信道协议将安全状态信息提供给安全元件172。例如,处理器120可以通过可靠的主体将安全状态信息提供给安全元件172,并且可以防止安全状态信息由此被仿冒。

[0056] 根据各种实施例,处理器120可以基于用户输入来执行第一应用,并且得到正在被执行的第一应用请求使用安全元件172的安全相关服务。处理器120可以通过使用第一应用向安全元件172发送请求安全相关服务的命令。根据实施例,当发送请求安全相关服务的命令时,处理器120可以将第一应用的安全状态信息一起发送到安全元件172。根据实施例,处理器120可以在请求安全相关服务的同时将包括第一应用的安全状态信息的命令信号发送到安全元件172。第一应用的安全状态信息可以包括应用的完整性和/或可靠性验证所必需的信息(例如,应用哈希信息)。

[0057] 根据各种实施例,处理器120可以从安全元件172接收对请求安全相关服务的命令的响应信号。处理器120可以基于来自安全元件172的响应信号来提供安全相关服务,或通知用户无法提供安全相关服务。根据实施例,处理器120可以基于包括在响应信号中的至少一个信息来确定是否已经从安全元件172许可(或允许)安全相关服务。当响应信号中包括与请求安全相关服务的命令相对应的信息或指示对该安全相关服务的许可(或允许)的信息时,处理器120可以基于至少一个信息来提供安全相关服务。当在响应信号中包括指示不许可(或拒绝)安全相关服务的信息时,处理器120可以控制提供了指示不能提供安全相关服务的用户界面的显示装置160。指示不能提供安全相关服务的用户界面可以包括安全状态信息。例如,当从安全元件172接收到的响应信号中包括指示不许可(或拒绝)安全相关服务的信息和安全状态信息时,处理器120可以控制提供了指示不能提供安全相关服务的用户界面的显示装置160。根据实施例,响应于在指定时间内没有接收到请求安全相关服务的命令的响应信号,处理器120可以控制提供了指示不能提供安全相关服务的用户界面的显示装置160。例如,响应于在从向安全元件172发送请求安全相关服务的命令的时间点起的指定时间段内未从安全元件172接收到响应信号,处理器120可以控制提供了指示不能提供安全相关服务的用户界面的显示装置160。根据实施例,指示不能提供安全相关服务的用户

界面可以包括指示由于安全状态原因而无法提供安全相关服务的信息。

[0058] 根据各种实施例,安全元件172可以通过至少一个接口与处理器120或短程通信模块210通信。根据实施例,安全元件172可以由处理器120或短程通信模块210周期性地或在特定时间点处被激活或操作。

[0059] 根据各种实施例,安全元件172可以通过安全通道协议从处理器120接收安全状态信息,并将接收到的安全状态信息存储在安全元件172内的存储库中。例如,可以将安全状态信息存储在安全元件172内的不可变区域中。安全元件172可以在当前时间添加和存储从处理器120接收的安全状态信息,而无需删除在先前时间点处存储的安全状态信息。例如,安全元件172可以将当前时间点的安全状态信息和过去时间点的安全状态信息一起存储在不可变区域中。根据实施例,安全元件172可以存储安全状态信息的改变历史信息。

[0060] 根据各种实施例,响应于获得安全相关服务请求事件,安全元件172可以基于先前存储在安全元件172内的存储库中的安全状态信息来确定是否提供安全相关服务。安全元件172可以基于先前存储的安全状态信息来确定是否满足与所请求的安全相关服务相对应的指定条件。安全元件172可以在其中响应于满足指定条件而提供安全相关服务和响应于不满足指定条件而阻止安全相关服务而进行操作。

[0061] 根据实施例,安全元件172可以从处理器120接收请求安全相关服务的命令以及第一应用的安全状态信息。安全元件172可以基于安全相关服务请求命令来执行相关小程序。例如,安全相关服务请求命令可以包括提供安全相关服务请求命令的第一应用的信息(例如,标识信息),或者与第一应用相对应的第一小程序的信息(例如,标识信息)。安全元件172可以基于包括在安全相关服务请求命令中的信息来执行与第一应用相对应的第一小程序。响应于第一应用是支付应用,第一小程序可以是支付小程序。通过使用第一小程序,安全元件172可以从安全元件172内的存储库获取第一应用的先前存储的安全状态信息。第一应用的先前存储的安全状态信息可以是在将第一应用和与第一应用相对应的第一小程序存储在电子装置101中的时间点处从处理器120提供给安全元件172并且被存储在安全元件172内的存储库中的信息。安全元件172可以比较从处理器120接收到的第一应用的安全状态信息和从安全元件172内的存储库获取的第一应用的安全状态信息。当从处理器120接收到第一应用的安全状态信息和从安全元件172内的存储库获取的第一应用的安全状态信息彼此相同时,安全元件172可以通过使用第一小程序来处理请求安全相关服务的命令,从而控制为提供所请求的安全相关服务。当从处理器120接收到第一应用的安全状态信息和从安全元件172内的存储库获取的第一应用的安全状态信息彼此不同时,安全元件172可以确定提供安全相关服务是不可能的,并且控制为在第一小程序中不处理请求安全相关服务的命令。例如,安全元件172可以在没有正常处理处理器120已经使用第一应用发送的安全相关服务请求命令的情况下忽略(或丢弃)该安全相关服务请求命令。根据实施例,响应于出于恶意目的而篡改了第一应用或用类似的另一应用替换了第一应用,接收到的第一应用的安全状态信息和从安全元件172内的存储库获取的第一应用的安全状态信息可以彼此不同。

[0062] 根据实施例,安全元件172可以通过处理器120或短程通信模块(例如,图2的短程通信模块210)从外部电子装置接收请求安全相关服务的命令(或信号)。安全相关服务请求命令可以包括指示与安全相关服务请求命令相关的小程序的信息(例如,标识信息)。安全

元件172可以基于安全相关服务请求命令中包括的信息来执行作为相关小程序的第二小程序。第二小程序可以是交通卡小程序。安全元件172可以通过使用第二小程序来获取先前存储在安全元件172内的存储库中的安全状态信息。安全元件172可以通过使用第二小程序来确定先前存储的安全状态信息是否满足指定条件。例如,指定条件可以是指示在电子装置101中未安装恶意软件的条件。对于另一示例,指定条件可以是指示电子装置101没有rooted并且未安装恶意软件的条件。对于进一步的示例,指定条件可以包括安全等级0。这仅仅是一个示例,但是本公开的各种实施例不限于这些。响应于识别出先前存储的安全状态信息满足指定条件,安全元件172可以通过使用第二小程序来处理请求安全相关服务的命令,从而在提供所请求的安全相关服务的情况下进行控制。响应于识别出先前存储的安全状态信息不满足指定条件,安全元件172可以确定由于安全状态较弱所以不可能提供安全相关服务,并且控制为在第二小程序中不处理请求安全相关服务的命令。例如,安全元件172可以通过使用第二小程序来忽略(或丢弃)安全相关服务请求命令。

[0063] 根据实施例,安全元件172可以基于接收到安全状态信息和安全相关服务请求命令(或信号)的接口,来确定是否提供安全相关服务。例如,当与和至少一个另一组件(例如,处理器120或短程通信模块210)的接口有关的安全状态信息不满足指定条件时,安全元件172可以忽略从相应接口输入的安全相关服务请求命令,或阻止从相应接口接收信号。例如,当安全状态信息指示电子装置101已经被rooted并且管理通过短程通信模块210对安全元件172的访问权限的访问规则执行器已经被仿冒时,安全元件172可以确定由于作为与短程无线通信模块210的接口的SWP的安全性较弱,因此无法提供安全相关服务。当SWP的安全性较弱并且因此不可能提供安全相关服务时,安全元件172可以在没有从SWP接收到信号的情况下忽略从SWP或块接收到的安全相关服务请求命令。又例如,当与具有至少一个另一组件的接口有关的安全状态信息满足指定条件时,安全元件172可以正常处理从相应接口输入的安全相关服务请求命令,从而控制为提供所请求的安全相关服务。例如,当安全状态信息指示了电子装置101没有被rooted并且管理通过短程通信模块210对安全元件172的访问权限的访问规则执行器尚未被仿冒的状态时,安全元件172可以确定作为与短程无线通信模块210的接口的SWP的安全性没有问题,并正常处理从SWP接收到的安全相关服务请求命令。根据实施例,安全元件172的操作系统220可以识别在其中输入了(或接收了)安全相关服务请求命令的接口。安全元件172可以在每个输入了安全相关服务请求命令的时间点处识别存储在安全元件172内的存储库中的安全状态信息,并基于所识别的安全状态信息以及接收有安全相关服务请求命令(或信号)的接口来确定是否提供安全相关服务。

[0064] 根据实施例,安全元件172可以从处理器120接收请求安全相关服务的命令。当不存在与请求安全相关服务的命令相关的小程序时,安全元件172可以直接识别存储在内部存储库中的电子装置101的安全状态信息,并确定是否提供安全相关服务。例如,安全元件172可以基于安全相关服务请求命令来确定是否存在相关小程序。例如,安全相关服务请求命令可以包括提供有安全相关服务请求命令的第三应用的信息(例如,标识信息)。基于第三应用的信息,安全元件172可以确定与第三应用相对应的小程序是否存在。响应于第三应用是财务相关应用,安全元件172可以基于包括在安全相关服务请求命令中的应用信息,识别出与财务相关应用相对应的相关小程序不存在于安全元件172内。响应于不存在相关小程序,安全元件172可以通过操作系统直接识别存储在安全元件172内的存储库中的安全状

态信息,并基于所识别的安全状态信息确定是否提供安全相关服务。根据实施例,安全元件172可以基于指示存储在内部存储库中的过去的电子装置101的安全状态信息的安全历史信息 and 当前安全状态信息是否满足指定条件来确定是否提供安全相关服务。指定条件例如可以指示其中指示过去安全状态信息的安全历史信息 and 当前安全状态信息都具有安全等级0的条件。这仅仅是一个示例,但是本公开的各种实施例不限于此。当指示过去安全状态信息的安全历史信息 and 当前安全状态信息满足指定条件时,安全元件172可以处理安全相关服务请求命令,从而在提供了所请求的安全相关服务的情况下进行控制。例如,当指示过去安全状态信息的安全历史信息 and 当前安全状态信息满足指定条件时,安全元件172可以向处理器120提供包括安全相关请求命令所请求的安全相关信息(例如,证书信息)的响应信号。当指示过去安全状态信息的安全历史信息 and 当前安全状态信息不满足指定条件时,安全元件172可以确定该安全状态较弱并且因此安全相关服务请求是不可能的,并且忽略(或丢弃)安全相关服务请求命令,而不正常处理。

[0065] 根据实施例,安全元件172可以发送对请求安全相关服务的命令的响应信号。例如,安全元件172可以向处理器120提供指示所请求的安全相关服务被许可(或被允许)或未被许可(或被拒绝)的响应信号。根据实施例,响应于确定如果不能提供所请求的安全相关服务,则安全元件172可以向处理器120提供响应信号,该响应信号包括指示所请求的安全相关服务没有被许可的信息和安全状态信息。

[0066] 根据各种实施例,短程通信模块210可以通过短程无线网络从外部电子装置(例如,电子装置102)接收信号,并基于接收到的信号来控制安全元件172的活动状态。短程通信模块210可以确定从外部电子装置接收的信号是否是用于请求指定的安全相关服务的信号。当从外部电子装置接收到的信号是指定的安全相关服务请求信号时,短程通信模块210可以激活安全元件172,并将从外部电子装置接收到的信号转发到安全元件172。响应于从安全元件172提供的响应信号,短程通信模块210可以通过短程无线网络将提供的响应信号发送到外部电子装置。

[0067] 根据各种实施例,短程通信模块210可以从处理器120接收将被转发到安全元件172的信号,并且将接收到的信号转发到安全元件172。当安全元件172在从处理器120接收到将被转发到安全元件172的信号的时间点处于停用状态(或休眠)状态时,短程通信模块210可以在安全元件172被激活的情况下进行控制,然后将该信号从处理器120转发到激活的安全元件172。短程通信模块210可以将响应信号从安全元件172转发到处理器120。

[0068] 根据各种实施例,电子装置(例如,图1的电子装置101)可以包括用于获取电子装置101的安全状态信息的处理器(例如,图1的处理器120)和在处理器120的控制下操作的安全元件(例如,图1的安全元件172),该安全元件从处理器120接收电子装置101的安全状态信息,并包括用于存储接收到的电子装置的安全状态信息的存储库。安全元件172可以感测安全相关服务请求命令,从存储库获取电子装置的安全状态信息,并基于获取到的电子装置的安全状态信息是否满足指定条件来处理或忽略感测到的安全相关服务请求命令。

[0069] 根据各种实施例,电子装置101的安全状态信息可以包括以下至少一项:关于电子装置101是否rooting的信息、关于是否存在恶意软件的信息、关于是否改变保修位的信息、关于是否仿冒访问规则执行器的信息、关于电子装置的系统区域的安全状态信息、或关于电子装置中安装的应用的安全状态信息。

[0070] 根据各种实施例,安全状态信息可以指示安全等级或安全问题的类型中的至少一项。

[0071] 根据各种实施例,可以基于安全相关服务请求命令的类型来确定指定条件。

[0072] 根据各种实施例,可以从处理器120或外部电子装置(例如,图1的电子装置102)接收请求安全相关服务的命令。

[0073] 根据各种实施例,安全元件172可以响应于获取的电子装置101的安全状态信息满足指定条件而正常处理感测到的安全相关服务请求命令以执行与该命令相对应的功能,并且响应于获取的电子装置101的安全状态信息不满足指定条件而忽略感测到的安全相关服务请求命令。

[0074] 根据各种实施例,安全元件172可以从处理器120接收与安全相关服务请求命令有关的应用的安全状态信息,从存储在存储库中的电子装置101的安全状态信息获取与安全相关服务请求命令有关的应用的安全状态信息,并基于接收到的应用的安全状态信息和获取的应用的安全状态信息是否彼此一致来处理或忽略感测到的安全相关服务请求命令。

[0075] 根据各种实施例,处理器120可以在应用被安装在电子装置中的时间点确定应用的安全状态信息,并且进行控制以将确定的应用的安全状态信息发送到安全元件172,其中安全状态信息被存储在安全元件的存储库中。

[0076] 根据各种实施例,安全元件172可以确定电子装置10的安全状态信息是否满足与仿冒访问规则执行器有关的条件,并且当电子装置101的安全状态信息不满足与仿冒访问规则执行器有关的条件时识别与感测到的安全相关服务请求命令相对应的接口,并且当所识别的接口是仿冒的访问规则执行器所对应的接口时忽略感测到的安全相关服务请求命令,当所识别的接口不是仿冒的访问规则执行器所对应的接口时执行与感测到的安全相关服务请求命令相对应的功能。

[0077] 根据各种实施例,安全元件172可以将对安全相关服务请求命令的响应信号提供给处理器120或外部电子装置102。响应信号可以包括以下至少一种信息:安全相关请求命令所请求的信息、指示由安全相关服务请求命令所执行的功能的结果的信息、或指示是否允许安全相关服务的信息。

[0078] 图3是根据各种实施例的在电子装置中提供安全相关服务的流程图300。在下面的实施例中,各个操作也可以顺序执行,但是不必须按照顺序执行。例如,各个操作的顺序也可以改变,并且至少两个操作也可以并行执行。这里,电子装置可以是图1的电子装置101。

[0079] 参照图3,在操作301中,各种实施例的电子装置(例如,图1的安全元件172)可以获得安全相关服务请求事件。安全相关服务可以是使用存储在安全元件172中的信息或安装在安全元件172中的小程序的服务。例如,安全相关服务可以是安装在安全元件172中的使用支付小程序或交通卡小程序的服务。对于另一示例,安全相关服务可以是使用与存储在安全元件172中的用户状态或凭证有关的证书或服务。例如,当从处理器(例如,图2的处理器120)接收到使用支付应用的支付请求命令时,或者从外部电子装置(例如,图1的电子装置102)接收到交通费用支付请求命令时,安全元件172可以确定发生了安全相关服务请求事件。对于另一示例,当从用于至少一个另一组件(例如,图1的处理器120或图2的短程无线通信模块210)的接口(例如,SPI或SWP)接收到安全相关服务请求命令时,安全元件172可以确定发生了安全相关服务请求事件。对于另一示例,当从处理器120接收到使用

银行应用的用户认证请求命令时,安全元件172可以确定发生了安全相关服务请求事件。

[0080] 在操作303中,各种实施例的电子装置(例如,安全元件172)可以获取指示电子装置的安全状态的安全状态信息。根据实施例,安全元件172可以获取存储在安全元件172内的存储库中的安全状态信息。例如,安全状态信息可以包括指示电子装置101是否rooting、是否感测到恶意软件、是否破解保修位、是否仿冒安全元件172的访问规则执行器、电子装置101的系统区域上的安全状态信息、安装在电子装置101中的应用上的安全状态信息中的至少一个。安全状态信息可以以指示安全等级(或安全质量)或指示安全问题的类型的形式来构造。例如,安全等级可以预先被不同地定义为阶梯级的等级0到等级N。例如,“安全等级N”可以是其中安全等级最高而电子装置101是安全的状态;“安全等级0”可以被定义为其中电子装置101的安全状态非常弱而安全等级最低的状态。“安全等级N-a”可以被定义为电子装置101被rooted的状态,“安全等级N-b”可以被定义为其中电子装置102被rooted而安全元件172的访问规则执行器被仿冒的状态。对于另一示例,安全状态信息可以被定义为指示感测到rooting、访问规则执行器仿冒、恶意软件感测或保修位破解中的至少一个安全问题的状态。安全状态信息的定义可以由服务提供商和/或设计者确定和/或改变。根据实施例,存储在安全元件172内的存储库中的安全状态信息的安全状态(172)安全状态(172)信息可以包括当前时间点的安全状态信息和指示过去时间点的安全状态信息的安全历史信息。根据实施例,可以由处理器120实时、周期性时间点或指定事件发生时间点中的至少一个时间点处获取安全状态信息,并将其存储在安全元件172内的存储库中。

[0081] 在操作305中,各种实施例的电子装置(例如,安全元件172)可以基于安全状态信息来确定是否提供服务。安全元件172可以基于获取的安全状态信息是否满足指定条件来确定是否提供服务。根据实施例,响应于获取的安全状态信息不满足指定条件,安全元件172可以确定它是不可能提供所请求的安全相关服务的状态,并且在未提供所请求的安全相关服务的情况下进行操作。例如,安全元件172可以忽略或丢弃从至少一个另一组件输入的安全相关服务请求命令。根据实施例,响应于获取的安全状态信息满足指定条件,安全元件172可以确定它是可以提供所请求的安全相关服务的状态,并且操作其中提供所请求的安全相关服务。例如,安全元件172可以正常处理从至少一个另一组件输入的安全相关服务请求命令。根据实施例,可以基于感测到的安全相关服务请求事件(或命令)的类型来不同地确定指定条件。例如,当通过使用支付小程序的支付请求命令感测到安全相关服务请求事件时,指定条件可以包括其中存储在安全元件172内的存储库中的支付应用的安全信息(例如,哈希信息)与从处理器120接收到的支付应用的安全状态信息彼此一致的条件。对于另一示例,响应于通过使用交通卡小程序的交通费用支付命令感测到安全相关服务请求事件,指定条件可以包括指示“未rooted且未感测到恶意软件”的条件。对于进一步的示例,响应于通过SWP接口接收到安全相关服务请求命令并感测到安全相关服务请求事件,指定条件可以包括指示“未rooted并且访问规则执行器未被仿冒”的条件。对于另一示例,当从处理器120接收到使用银行应用提供的用户认证请求命令并且感测到安全相关服务请求事件时,指定条件可以包括指示当前安全等级和过去安全等级均为0的条件。上述示例是用于帮助理解本公开的示例,但是本公开不限于此。

[0082] 图4是根据各种实施例的在电子装置中提供电子装置的安全状态信息的流程图400。下面描述的图4的操作可以是图3的操作303的详细操作的至少一部分,并且也可以是

在执行图3的操作之前执行的操作。在下面的实施例中,各个操作也可以顺序执行,但是不必按照顺序执行。例如,各个操作的顺序也可以改变,并且至少两个操作也可以并行执行。这里,电子装置可以是图1的电子装置101。下面,将参考图5描述图4的至少部分操作。图5是根据各种实施例的将电子装置的安全状态信息存储在电子装置中的示例图。

[0083] 参照图4,在操作401中,各种实施例的电子装置(例如,图1的处理器120)可以感测电子装置的安全状态。处理器120可以在与实时、周期性时间点或指定事件发生时间点(例如,启动时间点、软件更新时间点、以及应用安装时间点)中的至少一个相对应的时间点处感测电子装置的安全状态。根据实施例,处理器120可以获得以下中的至少一项:电子装置是否rooting、是否感测到恶意软件、是否改变(破解)保修位、是否仿冒安全元件172的访问规则执行器、是否感测到对电子装置101的系统区域的非法攻击、或是否感测到对安装在电子装置101中的应用的非法攻击。处理器120可以通过使用本领域技术人员公知的技术(例如,保修位)来感测到电子装置的安全状态。例如,在启动电子装置101时,处理器120可以检查保修位以确定启动映像是否正常。响应于保修位发生改变,处理器120可以确定引导图像是异常的,并且将电子装置的安全状态确定为rooting状态。这仅仅是一个示例,但是本公开不限于此。

[0084] 根据各种实施例,在操作403中,电子装置(例如,处理器120)可以将指示获得的电子装置的安全状态的安全状态信息转发到安全元件(例如,图1的安全元件172)。处理器120可以提供指示电子装置的安全状态的安全状态信息。安全状态信息可以包括上述图3中说明的信息。例如,如图5所示,处理器120可以将指示电子装置101是否已经被rooted的安全状态信息510通过安全信道520转发到安全元件172。

[0085] 根据各种实施例,在操作405中,电子装置(例如,安全元件172)可以存储安全状态信息。响应于从处理器120接收到安全状态信息,安全元件172可以将接收到的安全状态信息存储在安全元件172内的存储库中。例如,安全元件172可以将电子装置的安全状态信息存储在安全元件172内的不可变区域中。根据实施例,安全元件172可以在当前时间点添加并存储从处理器120接收到的安全状态信息,而不会删除在先前时间点存储的安全状态信息。例如,安全元件172可以将当前时间点的安全状态信息和过去时间点的安全状态信息一起存储在不可变区域中。根据实施例,安全元件172可以存储安全状态信息的改变历史信息。例如,如图5所示,安全元件172可以在安全元件172内的存储库中存储指示电子装置101是否已经被rooted的安全状态信息530。

[0086] 图6是根据各种实施例的基于电子装置中的电子装置的安全状态信息提供使用了应用的安全相关服务的流程图600。下文描述的图6的操作可以是图3的操作301、303和305的详细操作的至少一部分。在下面的实施例中,各个操作也可以顺序执行,但是不必按照顺序执行。例如,各个操作的顺序也可以改变,并且至少两个操作也可以并行执行。这里,电子装置可以是图1的电子装置101。下面,将参考图7描述图6的至少部分操作。图7是根据各种实施例的基于电子装置中的电子装置的安全状态信息提供使用该应用的安全相关服务的示例图。

[0087] 参照图6,在操作601中,各个实施例的电子装置(例如,图1的处理器120)可以获得第一应用的安全相关服务请求。根据实施例,处理器120可以基于第一输入来执行第一应用,并且基于正在执行的第一应用的第二输入感测已请求安全相关服务。安全相关服务可

以包括在图3的操作301中描述的服务。例如,响应于通过支付应用感测到支付请求事件,处理器120可以感测发生了使用该支付应用的安全相关服务请求。例如,如图7所示,处理器120可以在执行支付应用710的状态下通过支付应用710感测支付请求事件。

[0088] 根据各种实施例,在操作603中,电子装置(例如,图1的处理器120)可以提供第一应用的安全状态信息和安全相关服务请求命令。根据实施例,响应于感测到第一应用的安全相关服务请求,处理器120可以提供当前正在执行的第一应用的安全状态信息,并通过使用第一应用来提供安全相关服务请求命令。第一应用的安全状态信息是第一应用的完整性和/或可靠性验证所必需的信息,并且例如可以包括哈希信息。根据实施例,处理器120可以将所提供的第二应用的安全状态信息和安全相关服务请求命令转发给安全元件172。例如,如图7所示,处理器120可以向安全元件172转发支付请求命令730和支付应用的安全状态信息732。

[0089] 根据各种实施例,在操作605中,电子装置(例如,图1的安全元件172)可以获取第一应用的先前存储的安全状态信息。根据实施例,响应于接收到安全相关服务请求命令,安全元件172可以基于安全相关服务请求命令执行第一小程序,并且可以通过使用执行的第一小程序获取先前存储在安全元件172内的存储库中的第一应用的安全状态信息。例如,如图7所示,响应于接收到支付请求命令730,安全元件172可以基于支付请求命令执行支付小程序720,并且通过使用支付小程序720识别和获取存储在安全元件172内的存储库中的支付应用的安全状态信息740。

[0090] 根据各种实施例,在操作607中,电子装置(例如,图1的安全元件172)可以比较第一应用的先前存储的安全状态信息和提供的第一应用的安全状态信息以确定是否一致。根据实施例,安全元件172可以将先前存储在安全元件172内的存储库中的第一应用的安全状态信息与通过使用第一小程序从处理器120接收到的第一应用的安全状态信息进行比较以确定两个安全状态信息是否彼此一致。

[0091] 根据各种实施例,在操作609中,响应于第一应用的先前存储的安全状态信息和提供的第一应用的安全状态信息彼此一致,电子装置(例如,图1的安全元件172)可以执行与安全相关服务请求命令相对应的功能。根据实施例,响应于第一应用的先前存储的安全状态信息和提供的第一应用的安全状态信息彼此一致,安全元件172可以确定已经验证过的第一应用的完整性和/或可靠性,并且通过使用第一小程序正常处理安全相关服务请求命令。例如,如图7所示,安全元件172可以通过使用支付小程序720来执行与支付请求命令相对应的支付功能。

[0092] 根据各种实施例,在操作611中,响应于第一应用的先前存储的安全状态信息和提供的第一应用的安全状态信息彼此不一致,电子装置(例如,图1的安全元件172)可以忽略安全相关服务请求命令。根据实施例,响应于第一应用的先前存储的安全状态信息和提供的第一应用的安全状态信息彼此不一致,安全元件172可以确定不存在第一应用的完整性和/或可靠性,并且控制其中不使用第一小程序处理安全相关服务请求命令。例如,安全元件172可以忽略或丢弃从处理器120接收到的支付请求命令。

[0093] 图8是根据各种实施例的基于电子装置中的电子装置的安全状态信息来提供使用了应用的安全相关服务的信号流程图800。以下描述的图8的操作可以是图6的操作的至少一部分。这里,电子装置可以是图1的电子装置101。

[0094] 参照图8,在操作810中,各种实施例的电子装置101的处理器(例如,图1的处理器120)可以感测使用第一应用的安全相关服务请求。根据实施例,电子装置101的处理器120可以基于针对正在执行的第一应用的用户输入来感测已请求安全相关服务。感测安全相关服务请求的操作可以包括在图6的操作601中描述的操作。下面,根据实施例,可以省略用虚线表示的操作。

[0095] 根据各种实施例,在操作812中,电子装置101的处理器120可以将第一应用的安全状态信息和安全相关服务请求命令发送到安全元件172。根据实施例,当感测到使用了第一应用的安全相关服务请求时,处理器120可以通过使用第一应用来提供安全相关服务请求命令,并提供第一应用的安全状态信息(例如,哈希信息)。处理器120可以将提供的安全相关服务请求命令和第一应用的安全状态信息发送到安全元件172。

[0096] 根据各种实施例,在操作814中,电子装置101的安全元件172可以获取第一应用的先前存储的安全状态信息。根据实施例,响应于接收到安全相关服务请求命令和第一应用的安全状态信息,安全元件172可以基于接收到的安全相关服务请求命令来执行第一小程序,并且可以通过使用执行的第一小程序来获取先前存储在安全元件172内的存储库中的第一应用的安全状态信息。

[0097] 根据各种实施例,在操作816中,电子装置101的安全元件172可以比较第一应用的先前存储的安全状态信息和接收到的第一应用的安全状态信息,以确定二者是否一致。根据实施例,安全元件172可以将先前存储在安全元件172内的存储库中的第一应用的安全状态信息与通过使用第一小程序从处理器120接收到的第一应用的安全状态信息进行比较以确定两个安全状态信息是否彼此一致。

[0098] 根据各种实施例,在操作818中,电子装置101的安全元件172可以基于第一应用的先前存储的安全状态信息与提供的第一应用的安全状态信息是否一致来执行安全相关服务请求命令相对应的功能或忽略安全相关服务请求命令。响应于第一应用的先前存储的安全状态信息和提供的第一应用的安全状态信息彼此一致,安全元件172可以执行安全相关服务请求命令相对应的功能。响应于第一应用的先前存储的安全状态信息和提供的第一应用的安全状态信息彼此不一致,安全元件172可以忽略安全相关服务请求命令。

[0099] 根据各种实施例,在操作820中,电子装置101的安全元件172可以将对安全相关服务请求的响应信号转发给处理器120。响应信号可以包括以下信息中的至少一个信息:安全相关服务请求命令所请求的信息、指示由安全相关服务请求命令所执行的功能的结果的信息、或指示是否许可(或允许)安全相关服务的信息。

[0100] 图9是根据各种实施例的基于电子装置中的电子装置的安全状态信息通过无线接口提供服务的流程图900。下面描述的图9的操作可以是图3的操作301、303和305的详细操作的至少一部分。在下面的实施例中,各个操作也可以顺序执行,但是不必须按照顺序执行。例如,各个操作的顺序也可以改变,并且至少两个操作也可以并行执行。这里,电子装置可以是图1的电子装置101。下面,将参考图10描述图9的至少部分操作。图10是根据各种实施例的基于电子装置中的电子装置的安全状态信息提供使用了应用的安全相关服务的示例图。

[0101] 参照图9,在操作901中,各种实施例的电子装置(例如,图1的安全元件172)可以从外部电子装置获得安全相关服务请求。根据实施例,安全元件172可以接收通过处理器120

或短程通信模块(例如,图2的210)从外部电子装置发送的安全相关服务请求命令(或信号)。例如,如图10所示,安全元件172可以通过处理器120或短程通信模块210从外部电子装置接收请求交通费用支付的信号。

[0102] 根据各种实施例,在操作903中,电子装置(例如,安全元件172)可以确定先前存储的安全状态信息是否满足指定条件。根据实施例,安全元件172可以通过使用与安全相关服务请求信号有关的小程序来识别先前存储的安全状态信息,并且确定先前存储的安全状态信息是否满足指定条件。安全相关服务请求信号可以包括指示与安全相关服务请求命令相关的小程序的信息(例如,标识信息)。安全元件172可以基于从外部电子装置接收到的安全相关服务请求信号中包括的信息来执行相关小程序。例如,如图10所示,响应于通过短程通信模块210从外部电子装置接收到请求交通费用支付的信号,安全元件172可以基于接收到的请求交通费用支付信号来执行交通卡小程序1020。响应于由“未感测到恶意软件”设置的指定条件,安全元件172可以通过使用交通卡小程序1020来识别先前存储在安全元件172内的存储库中的安全状态信息中的指示是否感测恶意软件的信息1030,以识别是否满足指定条件。该指定条件仅仅是一个示例,可以由设计者和/或服务提供商设置和更改。例如,指定条件可以包括安全等级、是否rooting、以及是否仿冒访问规则执行器中的至少一项的条件。

[0103] 根据各种实施例,在操作905中,响应于先前存储的安全状态信息满足指定条件,电子装置(例如,安全元件172)可以将与安全相关服务请求相对应的响应信号发送给外部电子装置。根据实施例,响应于识别出先前存储的安全状态信息满足指定条件,安全元件172可以确定安全状态较强,并且确定可以提供安全相关服务。安全元件172可以通过使用第二小程序来正常处理请求安全相关服务的命令,并且控制为安全相关服务请求命令的响应信号被发送到外部电子装置。例如,响应于指示未感测到恶意软件的安全状态信息,安全元件172可以确定满足指定条件,并且控制为通过使用交通卡小程序1020发送通过短程无线通信网络的交通费用支付响应信号。

[0104] 根据各种实施例,在操作907中,响应于先前存储的安全状态信息不满足指定条件,电子装置(例如,安全元件172)可以忽略安全相关服务请求。根据实施例,响应于识别出先前存储的安全状态信息不满足指定条件,安全元件172可以确定由于安全状态较弱的原因,不可能提供安全相关服务,并且控制为在第二小程序中不处理请求安全相关服务的命令。例如,响应于指示存在恶意软件的安全状态信息,安全元件172可以确定不满足指定条件,并且控制为使用交通卡小程序1020的通过短程无线通信网络的交通费用支付请求未被处理。例如,因为已经安装了用于监视和记录通过短程无线通信模块(例如,图2的短程无线通信模块210)发送和/或接收的分组的恶意软件,所以安全元件172可以控制为未使用交通卡小程序1020将交通费用支付请求的响应信号发送到外部电子装置。对于另一示例,由于已经安装了用于监视和记录通过短程无线通信模块210发送和/或接收的分组的恶意软件,所以安全元件172可以控制为使用交通卡小程序1020通过短程通信网络将拒绝支付请求的响应信号发送到外部电子装置。拒绝支付请求的响应信号可以包括指示拒绝支付请求的原因的信息。例如,拒绝支付请求的响应信号可以包括指示感测安全问题(例如,感测恶意软件)的错误代码。

[0105] 图11是根据各种实施例的基于电子装置中的电子装置的安全状态信息来控制对

使用通信接口的安全元件的访问的流程图1100。下文描述的图11的操作可以是图3的操作301、303和305的详细操作的至少一部分。在下面的实施例中，各个操作也可以顺序执行，但是不必按照顺序执行。例如，各个操作的顺序也可以改变，并且至少两个操作也可以并行执行。这里，电子装置可以是图1的电子装置101。下面，将参考图12描述图11的至少部分操作。图12是根据各种实施例的基于电子装置中的电子装置的安全状态信息控制使用通信接口的对安全元件的访问的示例图。

[0106] 参照图11，在操作1101中，各种实施例的电子装置（例如，图1的安全元件172）可以获得安全状态信息，该安全状态信息指示感测到对访问规则执行器的仿冒。根据实施例，安全元件172可以从先前存储在内部存储库中的安全状态信息中获取指示仿冒访问规则执行器的安全状态信息。例如，如图12所示，安全元件172的操作系统可以从先前存储的安全状态信息中获取指示仿冒与I2C和SWP接口相对应的访问规则执行器的信息1242。根据实施例，安全元件172可以从处理器120接收指示仿冒安全元件172的访问规则执行器的安全状态信息。访问规则执行器可以包括用于控制对安全元件172的访问的访问权限。

[0107] 根据各种实施例，在操作1103中，电子装置（例如，安全元件172）可以通过阻止接口来设置与仿冒的访问规则执行器相对应的接口。安全元件172可以识别与访问规则执行器仿冒相对应的接口，并通过阻止接口来设置所识别的接口。例如，如图12所示，安全元件172可以识别出与仿冒的访问规则执行器相对应的接口是SWP 1224、SPI 1222、或ISO 1232之中的SWP 1224，其是至少一个另一组件与安全元件172之间的接口，并通过阻止通信的阻止接口来设置SWP 1224。

[0108] 根据各种实施例，在操作1105中，电子装置（例如，安全元件172）可以确定是否感测到请求安全相关服务的命令。根据实施例，安全元件172的操作系统可以获得通过至少一个接口输入到安全元件172的安全相关服务请求命令。

[0109] 根据各种实施例，在操作1107中，电子装置（例如，安全元件172）可以确定用于获得命令的接口是否是阻止接口。根据实施例，响应于获得输入到安全元件172的安全相关服务请求命令，安全元件172的操作系统可以确定输入有安全相关服务请求命令的接口是否是阻止接口。例如，如图12所示，安全元件172可以确定是否已经通过设置为阻止接口的SWP 1224输入了获得的安全相关服务请求命令。

[0110] 根据各种实施例，在操作1109中，当用于获得命令的接口不是阻止接口时，电子装置（例如，安全元件172）可以正常处理获得的命令。根据实施例，当通过不是阻止接口的另一接口输入了安全相关服务请求命令时，安全元件172的操作系统可以正常处理输入的安全相关服务请求命令。例如，如图12所示，当通过SPI 1222或ISO 1232输入了安全相关服务请求命令时，安全元件172的操作系统可以正常处理输入的安全相关服务请求命令。

[0111] 根据各种实施例，在操作1111中，当用于获得命令的接口是阻止接口时，电子装置（例如，安全元件172）可以忽略获得的命令。根据实施例，当通过阻止接口输入安全相关服务请求命令时，安全元件172的操作系统可以不处理输入的安全相关服务请求命令而忽略该输入的安全相关服务请求命令。例如，如图12所示，当仿冒访问规则执行器1210时，未许可的应用可以通过使用仿冒的访问规则执行器来尝试访问安全元件172，因此安全元件172可以忽略通过SWP 1224输入的安全相关服务请求命令。

[0112] 图13是根据各种实施例的基于电子装置中的电子装置的安全状态信息来提供安

全相关信息的流程图1300。下文描述的图13的操作可以是图3的操作301、303和305的详细操作的至少一部分。在下面的实施例中，各个操作也可以顺序执行，但是不必按照顺序执行。例如，各个操作的顺序也可以改变，并且至少两个操作也可以并行执行。这里，电子装置可以是图1的电子装置101。下面，将参考图14来描述图13的至少部分操作。图14是根据各种实施例的基于电子装置中的电子装置的安全状态信息来提供安全相关信息的示例图。

[0113] 参照图13，在操作1301中，各种实施例的电子装置（例如，图1的处理器120）可以感测第三应用的安全相关服务请求。根据实施例，处理器120可以基于第一输入来执行第三应用，并且基于正在执行的第三应用的第二输入来感测已请求安全相关服务。安全相关服务可以包括在图3的操作301中描述的服务。例如，响应于通过财务相关应用获得了认证请求事件，处理器120可以感测发生了使用了财务相关应用的安全相关服务请求。例如，如图14所示，处理器120可以在执行了财务相关应用1410的状态下感测用户认证请求事件。

[0114] 根据各种实施例，在操作1303中，电子装置（例如，处理器120）可以提供安全相关服务请求命令。根据实施例，处理器120可以通过使用第三应用来提供安全相关服务请求命令。例如，处理器120可以通过使用财务相关应用来提供用户认证请求命令。根据实施例，安全相关服务请求命令可以包括财务相关应用的信息（例如，标识信息）。

[0115] 根据各种实施例，在操作1305中，电子装置（例如，安全元件172）可以获取先前存储的安全状态信息。根据实施例，响应于从处理器120接收到安全相关服务请求命令，安全元件172可以获取存储在安全元件172内的存储库中的安全状态信息。安全元件172可以基于安全相关服务请求命令确定不存在相关小程序。例如，安全相关服务请求命令可以基于安全相关服务请求命令中包括的信息来确定不存在与第三应用相对应的小程序。安全元件172可以通过使用操作系统来获取存储在安全元件172内的存储库中的安全状态信息。

[0116] 根据各种实施例，在操作1307中，电子装置（例如，安全元件172）可以确定先前存储的安全状态信息是否满足指定条件。根据实施例，安全元件172可以基于是否指示存储在内部存储库中的过去的电子装置101的安全状态信息的安全历史信息 and 当前安全状态信息是否满足指定条件来确定是否提供安全相关服务。例如，如图14所示，安全元件172可以从内部存储库获取当前的安全状态信息1422和安全历史信息1420，并确定获取的信息是否满足指定条件。指定条件例如可以指示其中指示过去安全状态信息的安全历史信息 and 当前安全状态信息都具有安全等级0的条件。这仅仅是一个示例，但是本公开的各种实施例不限于此。例如，指定条件可以是是否rooting和是否存在恶意软件的条件。安全元件172可以基于指定条件从安全元件172内的存储库获取安全状态信息，并且确定获取的安全状态信息是否满足指定条件。

[0117] 根据各种实施例，在操作1309中，响应于先前存储的安全状态信息满足指定条件，电子装置（例如，安全元件172）可以提供对安全相关服务请求的响应信号。根据实施例，响应于当前安全状态信息 and 安全历史信息满足指定条件，安全元件172可以处理安全相关服务请求命令，从而在提供所请求的安全相关服务的情况下进行控制。例如，安全元件172可以将包括由安全相关服务请求命令所请求的安全相关信息（例如，证书信息）的响应信号提供给处理器120。

[0118] 根据各种实施例，在操作1311中，响应于先前存储的安全状态信息不满足指定条件，电子装置（例如，安全元件172）可以忽略安全相关服务请求命令。根据实施例，响应于

当前安全状态信息和安全历史信息不满足指定条件,安全元件172可以忽略安全相关服务请求命令,从而控制为未提供所请求的安全相关服务。当指示过去安全状态信息的安全历史信息和当前安全状态信息不满足指定条件时,安全元件172可以向处理器120提供指示由于安全状态的原因而无法进行服务的响应信号。

[0119] 图15是根据各种实施例的基于电子装置中的电子装置的安全状态信息提供安全相关信息的信号流程图1500。下文描述的图15的操作可以是图13的操作的至少一部分。这里,电子装置可以是图1的电子装置101。下面,根据实施例,可以省略用虚线表示的操作。

[0120] 参照图15,在操作1510中,各种实施例的电子装置101的处理器(例如,图1的处理器120)可以获得使用了第三应用的安全相关服务请求。根据实施例,电子装置101的处理器120可以基于正在执行的第三应用的用户输入来感测已请求安全相关服务。感测安全相关服务请求的操作可以包括在图13的操作1301中描述的操作。

[0121] 根据各种实施例,在操作1512中,电子装置101的处理器120可以将安全相关服务请求命令发送到安全元件(例如,图1的安全元件172)。根据实施例,当感测到使用第三应用的安全相关服务请求时,处理器120可以通过使用第三应用来提供安全相关服务请求命令,并将提供的安全相关服务请求命令发送到安全元件172。

[0122] 根据各种实施例,在操作1514中,电子装置101的安全元件172可以获取先前存储的安全状态信息。根据实施例,响应于从处理器120接收到安全相关服务请求命令,安全元件172可以基于接收到的安全相关服务请求命令来确定不存在相关小程序。例如,安全相关服务请求命令可以基于安全相关服务请求命令中包括的信息来确定不存在与第三应用相对应的小程序。安全元件172可以通过使用操作系统来获取存储在安全元件172内的存储库中的安全状态信息。例如,安全元件172可以从内部存储库获取包括当前安全状态信息和安全历史信息的安全状态信息。

[0123] 根据各种实施例,在操作1516中,电子装置101的安全元件172可以确定先前存储的安全状态信息是否满足指定条件。根据实施例,安全元件172可以确定当前安全状态信息和安全历史信息是否满足指定条件。指定条件例如可以指示当前安全状态信息和安全历史信息都具有安全等级0的条件。这仅仅是一个示例,但是本公开的各种实施例不限于此。例如,指定条件可以是是否rooting和是否存在恶意软件的条件。安全元件172可以从安全元件172内的存储库中获取与指定条件有关的安全状态信息,并确定获取的安全状态信息是否满足指定条件。

[0124] 根据各种实施例,在操作1518中,基于在先前的存储的安全状态信息是否满足指定条件,电子装置101的安全元件172可以确定:提供安全相关服务或者忽略安全相关服务请求命令。响应于先前存储的安全状态信息满足指定条件,安全元件172可以正常处理安全相关服务请求命令,以允许提供所请求的安全相关服务。响应于先前存储的安全状态信息不满足指定条件,安全元件172可以忽略安全相关服务请求命令,以允许未提供所请求的安全相关服务。

[0125] 根据各种实施例,在操作1520中,电子装置101的安全元件172可以将对服务请求的响应信号转发给处理器120。该响应信号可以包括以下信息中的至少一项信息:安全相关服务请求命令所请求的信息、指示由安全相关服务请求命令所执行的功能的结果的信息、或指示许可(或允许)安全相关服务的信息。

[0126] 在上述各种实施例中,已经描述了电子装置101的安全元件172存储指示电子装置101的安全状态的安全状态信息,并且确定是否通过该安全状态信息提供安全相关服务。然而,根据各种实施例,电子装置101的安全元件172可以存储至少一个外部电子装置(例如,图1的电子装置102)的安全状态信息。例如,安全元件172可以存储以下至少一项:至少一个外部电子装置102的rooting或non-rooting、至少一个外部电子装置102的恶意软件存在或不存在、至少一个外部电子装置102的保修位的改变或不改变、对至少一个外部电子装置102的安全元件172的访问规则执行器的仿冒或不仿冒、至少一个外部电子装置102的系统的系统区域上的安全状态信息、或安装在至少一个外部电子装置102中的应用上的安全状态信息。电子装置101可以通过处理器120和/或通信模块190从至少一个外部电子装置接收安全相关服务请求命令(或信号),并基于存储在安全元件172内的存储库中的至少一个外部电子装置的安全状态信息确定是否通过安全元件172提供从至少一个外部电子装置请求的安全相关服务。例如,电子装置101的安全元件172可以基于先前存储在内部存储库中的至少一个外部电子装置的安全状态信息正常处理或忽略安全相关服务请求命令。

[0127] 根据各种实施例,电子装置(例如,图1的电子装置101)的操作方法可以包括:处理器(例如,图1的处理器120)获取电子装置的安全状态信息,在处理器120的控制下操作的安全元件将电子装置的安全状态信息存储在安全元件(例如,图1的安全元件172)内的存储库中,安全元件172感测安全相关服务请求命令,安全元件172获取存储在内部存储库中的电子装置的安全状态信息,安全元件172基于获取的电子装置的安全状态信息是否满足指定条件来处理或忽略感测到的安全相关服务请求命令。

[0128] 根据各种实施例,电子装置的安全状态信息可以包括以下至少一项:关于电子装置是否rooting的信息、关于是否感测到恶意软件的信息、关于是否改变保修位的信息、关于是否仿冒访问规则执行器的信息、关于电子装置的系统区域的安全状态信息、或关于安装在电子装置中的应用的安全状态信息。

[0129] 根据各种实施例,安全状态信息可以指示安全等级或安全问题的类型中的至少一项。

[0130] 根据各种实施例,可以基于安全相关服务请求命令的类型来确定指定条件。

[0131] 根据各种实施例,可以从处理器120或外部电子装置(例如,图1的电子装置102)接收请求安全相关服务的命令。

[0132] 根据各种实施例,安全元件172处理或忽略感测到的安全相关服务请求命令可以包括:当获取的电子装置的安全状态信息满足指定条件时安全元件172正常处理感测到的安全相关服务请求命令以执行与该命令相对应的功能,当获取的电子装置的安全状态信息不满足指定条件时安全元件172忽略感测到的安全相关服务请求命令。

[0133] 根据各种实施例,该方法可以进一步包括:安全元件172从处理器120接收与安全相关服务请求命令有关的的应用的安全状态信息。安全元件172处理或忽略感测到的安全相关服务请求命令可以包括:安全元件172从获取的安全状态信息中识别与安全相关服务请求命令有关的的应用的安全状态信息,以及安全元件172基于接收到的应用的安全状态信息和所识别的应用的安全状态信息是否彼此一致来处理或忽略感测到的安全相关服务请求命令。

[0134] 根据各种实施例,该方法可以进一步包括:处理器120在应用被安装在电子装置中

的时间点处确定应用的安全状态信息;以及处理器120控制以将确定的应用的安全状态信息发送到安全元件172,其中该安全状态信息存储在安全元件172的存储库中。

[0135] 根据各种实施例,安全元件172处理或忽略感测到的安全相关服务请求命令可以包括:安全元件172确定电子装置的安全状态信息是否满足与仿冒访问规则执行器相关的条件,并且当电子装置的安全状态信息不满足与仿冒访问规则执行器相关的条件时安全元件172识别与感测到的安全相关服务请求命令相对应的接口,当所识别的接口是与仿冒的访问规则执行器相对应的接口时安全元件172忽略感测到的安全相关服务请求命令,并且当所识别的接口不是与仿冒的访问规则执行器相对应的接口时安全元件172执行与感测到的安全性相对应的功能。

[0136] 根据各种实施例,该方法可以进一步包括安全元件172将对安全相关服务请求命令的响应信号提供给处理器120或外部电子装置102。响应信号可以包括以下至少一种信息:安全相关请求命令所请求的信息、指示由安全相关服务请求命令所执行的功能的结果的信息、或指示是否允许安全相关服务的信息。

[0137] 根据各种实施例的电子装置可以是各种类型的电子装置之一。电子装置可包括例如便携式通信装置(例如,智能电话)、计算机装置、便携式多媒体装置、便携式医疗装置、相机、可穿戴装置或家用电器。根据本公开的实施例,电子装置不限于上述那些电子装置。

[0138] 应该理解的是,本公开的各种实施例以及其中使用的术语并不意图将在此阐述的技术特征限制于具体实施例,而是包括针对相应实施例的各种改变、等同形式或替换形式。对于附图的描述,相同的参考标号可用来指代相同或相关的组件。将理解的是,与术语相应的单数形式的名词可包括一个或更多个事物,除非相关上下文另有明确指示。如这里所使用的,诸如“A或B”、“A和B中的至少一个”、“A或B中的至少一个”、“A、B或C”、“A、B和C中的至少一个”以及“A、B或C中的至少一个”的短语中的每一个短语可包括在与所述多个短语中的相应一个短语中一起列举出的项的所有可能组合。如这里所使用的,诸如“第1”和“第2”或者“第一”和“第二”的术语可用于将相应部件与另一部件进行简单区分,并且不在其它方面(例如,重要性或顺序)限制相应的组件。将理解的是,在使用了术语“可操作地”或“通信地”的情况下或者在不使用术语“可操作地”或“通信地”的情况下,如果一元件(例如,第一元件)被称为“与另一元件(例如,第二元件)结合”、“结合到另一元件(例如,第二元件)”、“与另一元件(例如,第二元件)连接”或“连接到另一元件(例如,第二元件)”,则意味着所述一元件可与所述另一元件直接(例如,有线地)连接、与所述另一元件无线连接、或经由第三元件与所述另一元件连接。

[0139] 如这里所使用的,术语“模块”可包括以硬件、软件或固件实现的单元,并可与其他术语(例如,“逻辑”、“逻辑块”、“部分”或“电路”)可互换地使用。模块可以是被适配为执行一个或更多个功能的单个集成部件或者是该单个集成部件的最小单元或部分。例如,根据实施例,可以以专用集成电路(ASIC)的形式来实现模块。

[0140] 可将在在此阐述的各种实施例实现为包括存储在存储介质(例如,内部存储器136或外部存储器138)中的可由机器(例如,电子装置101)读取的一个或更多个指令的软件(例如,程序140)。例如,在控制器的控制下,所述机器(例如,电子装置101)的处理器(例如,处理器120)可在不使用或无需使用一个或更多个其它部件的情况下调用存储在存储介质中的所述一个或更多个指令中的至少一个指令并运行所述至少一个指令。这使得所述机器能够

操作用于根据所调用的至少一个指令执行至少一个功能。所述一个或更多个指令可包括由编译器产生的代码或能够由解释器运行的代码。可以以非暂时性存储介质的形式来提供机器可读存储介质。其中,术语“非暂时性”仅意味着所述存储介质是有形装置,并且不包括信号(例如,电磁波),但是该术语并不在数据被半永久性地存储在存储介质中与数据被临时存储在存储介质中之间进行区分。

[0141] 根据实施例,可在计算机程序产品中包括和提供根据本公开的各种实施例的方法。计算机程序产品可作为产品在销售者与购买者之间进行交易。可以以机器可读存储介质(例如,紧凑盘只读存储器(CD-ROM))的形式来发布计算机程序产品,或者可经由应用商店(例如,Play Store™)在线发布(例如,下载或上传)计算机程序产品,或者可直接在两个用户装置(例如,智能电话)之间分发(例如,下载或上传)计算机程序产品。如果是在线发布的,则计算机程序产品中的至少部分可以是临时产生的,或者可将计算机程序产品中的至少部分至少临时存储在机器可读存储介质(诸如制造商的服务器、应用商店的服务器或转发服务器的存储器)中。

[0142] 根据各种实施例,上述部件中的每个组件(例如,模块或程序)可包括单个实体或多个实体。根据各种实施例,可省略上述组件中的一个或更多个部件,或者可添加一个或更多个其它组件。可选择地或者另外地,可将多个组件(例如,模块或程序)集成为单个组件。在这种情况下,根据各种实施例,该集成组件可仍旧按照与所述多个组件中的相应一个组件在集成之前执行一个或更多个功能相同或相似的方式,执行所述多个组件中的每一个组件的所述一个或更多个功能。根据各种实施例,由模块、程序或另一组件所执行的操作可顺序地、并行地、重复地或以启发式方式来执行,或者所述操作中的一个或更多个操作可按照不同的顺序来运行或被省略,或者可添加一个或更多个其它操作。

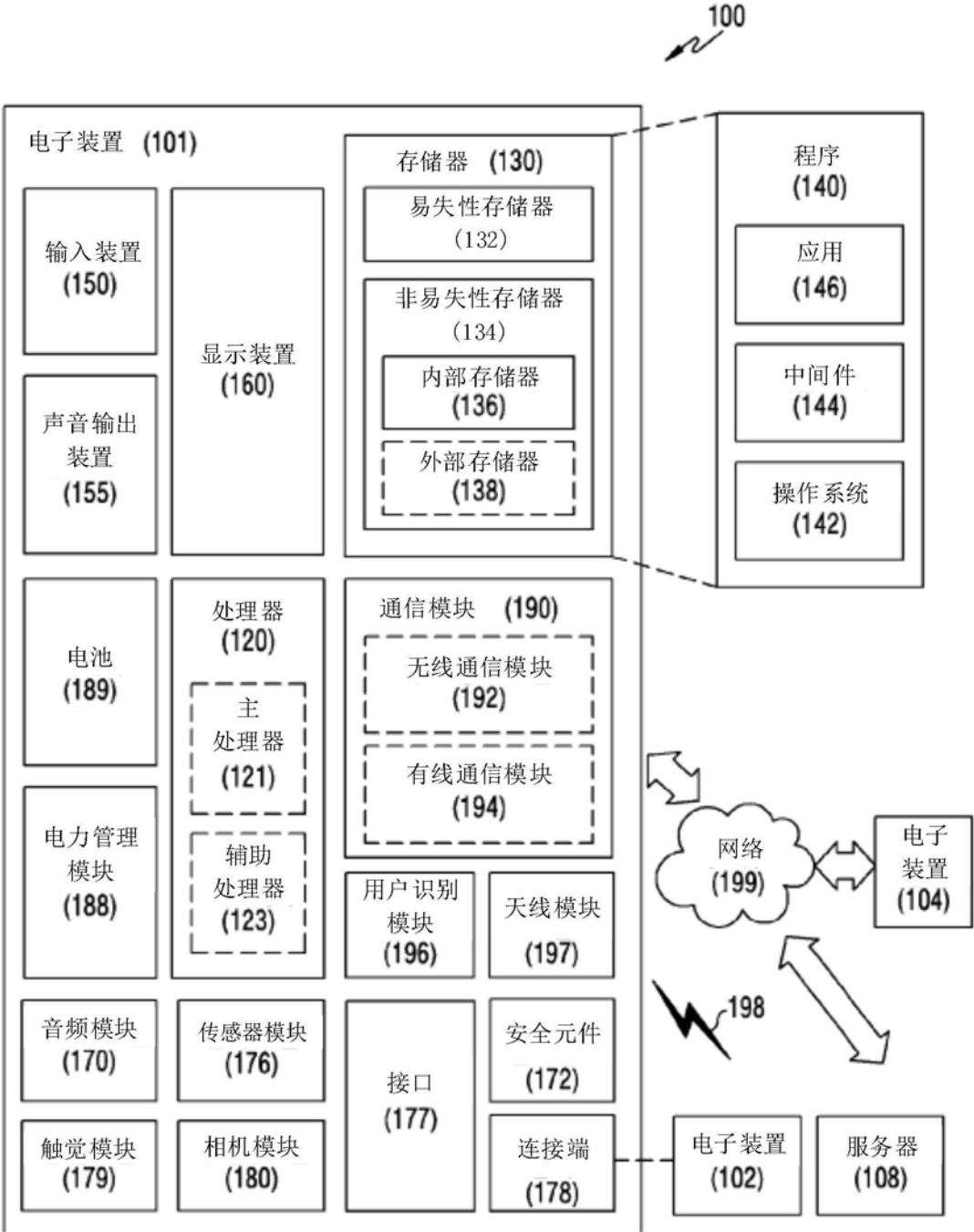


图1

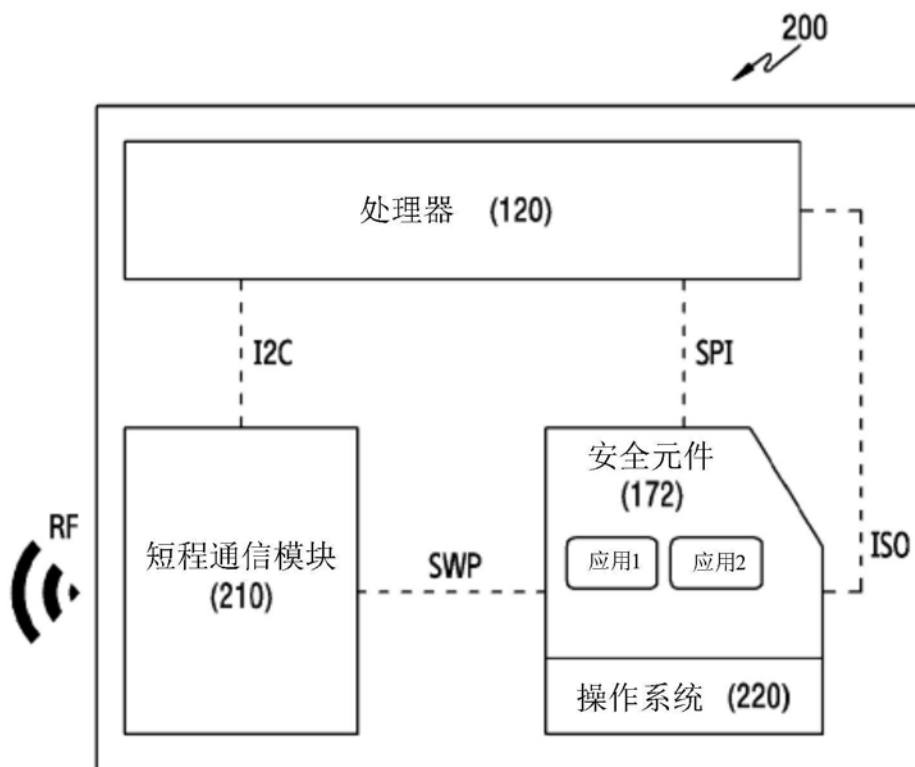


图2

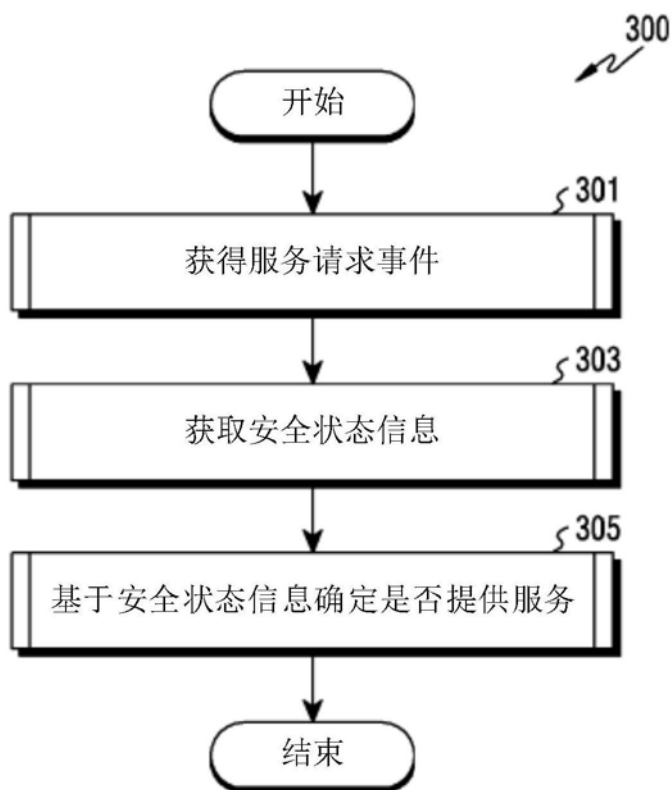


图3

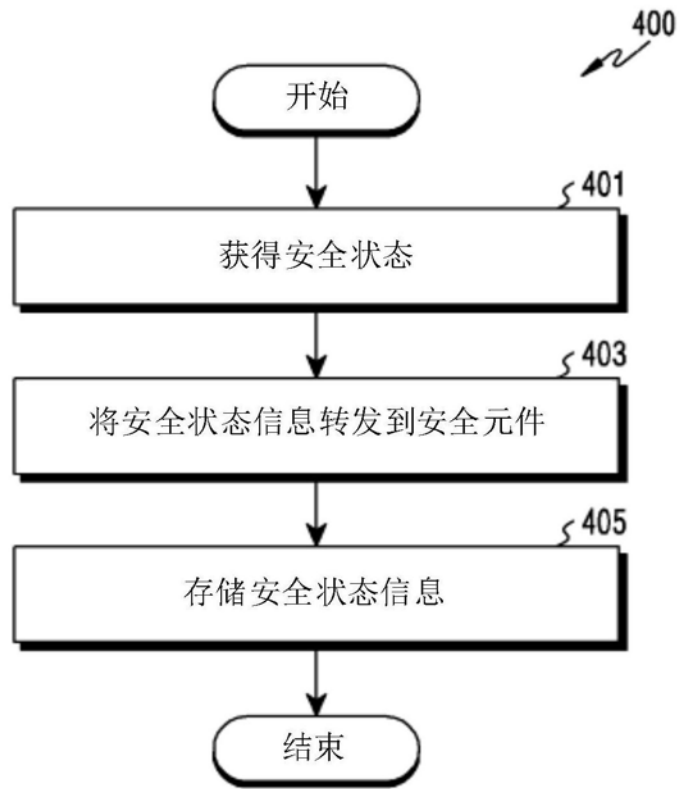


图4

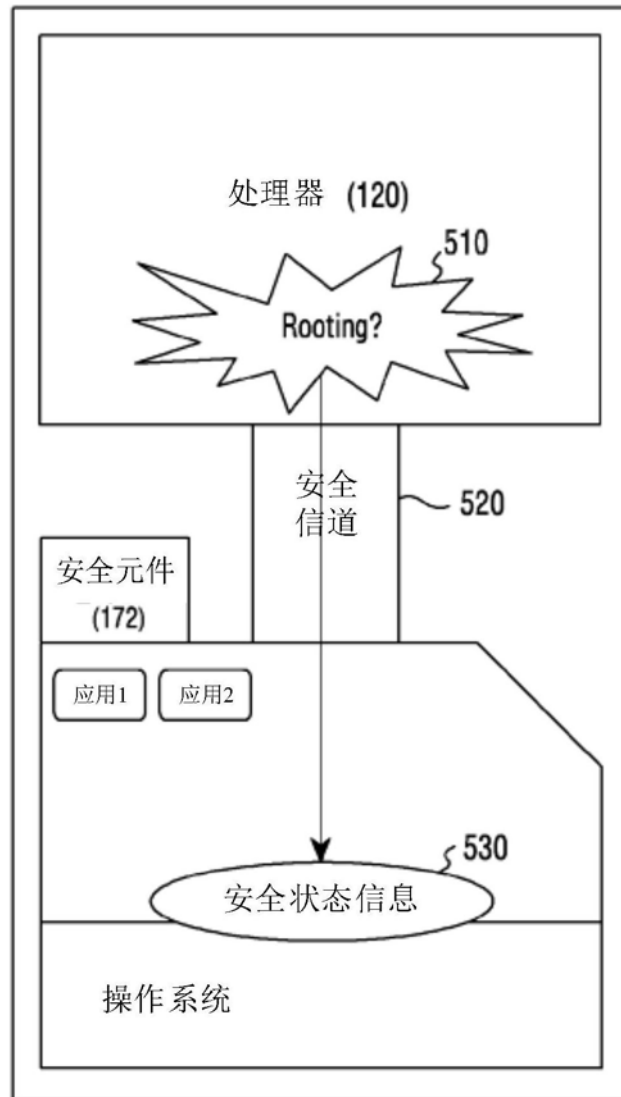


图5

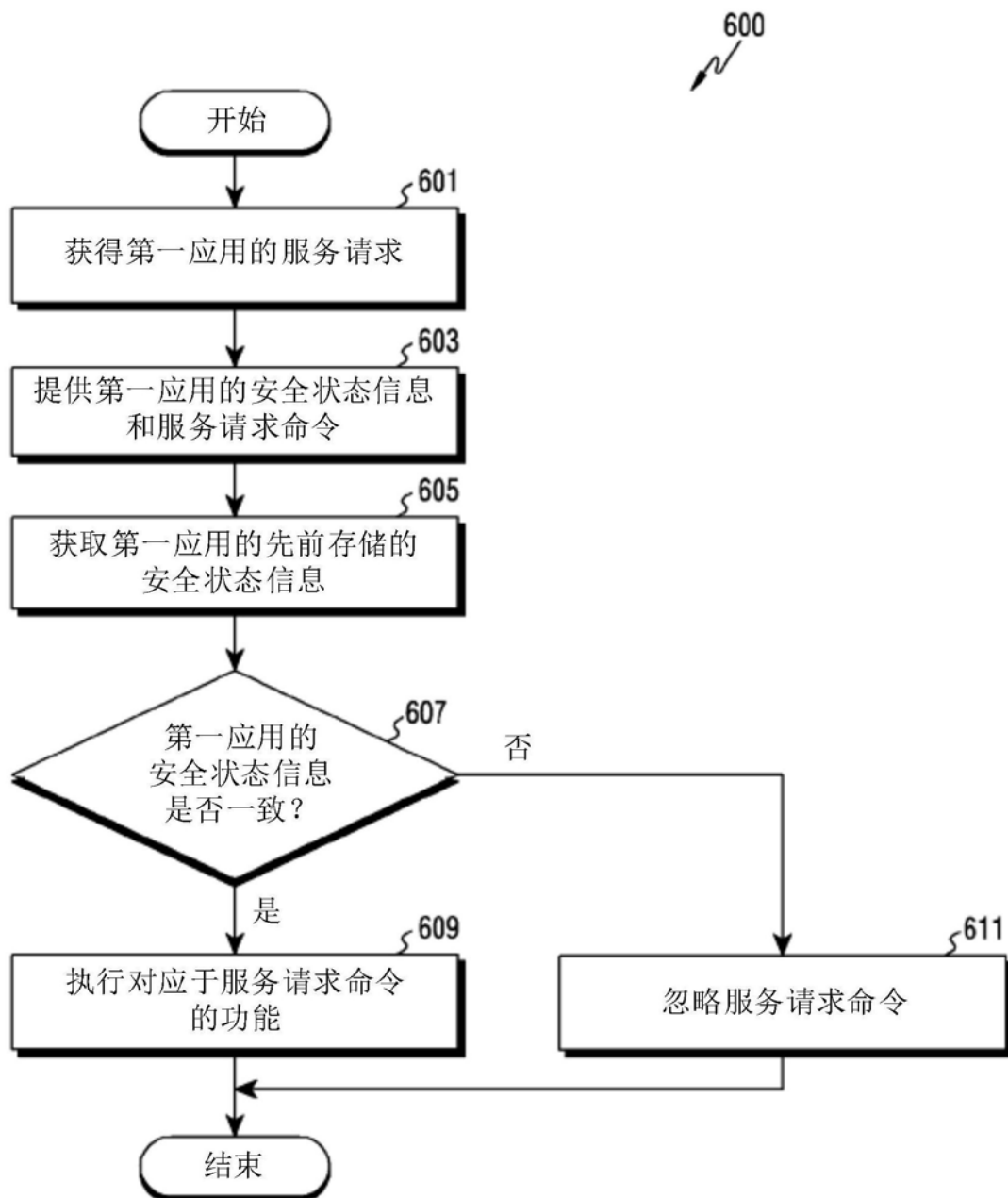


图6

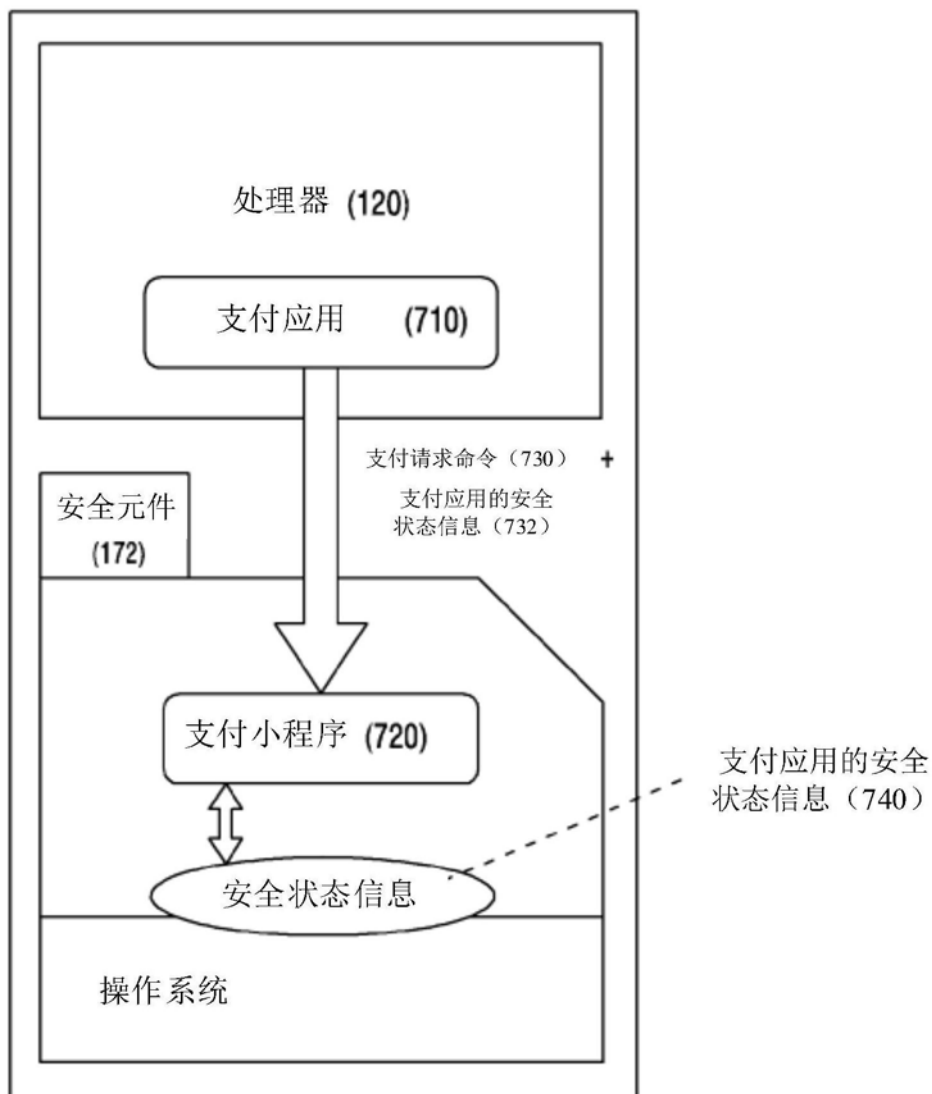


图7

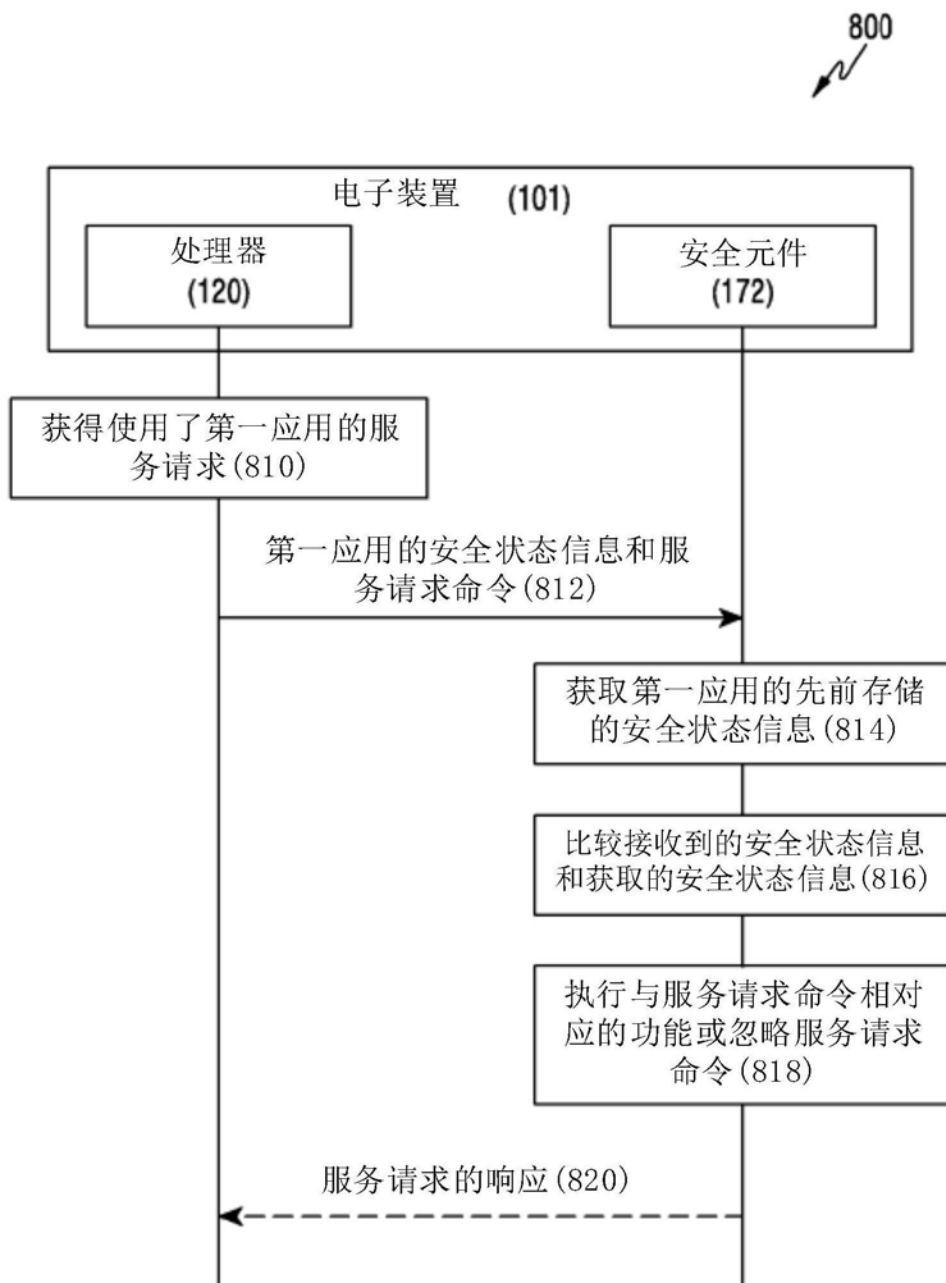


图8

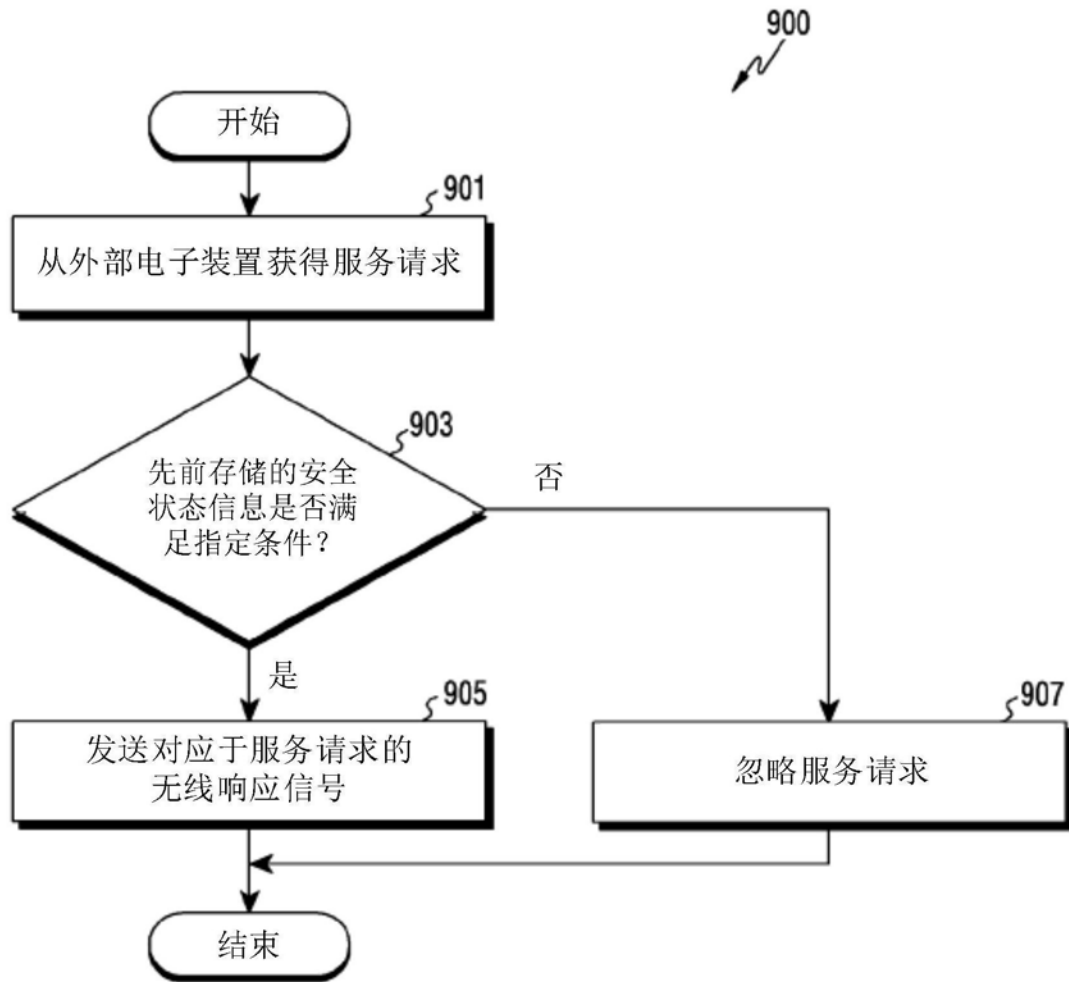


图9

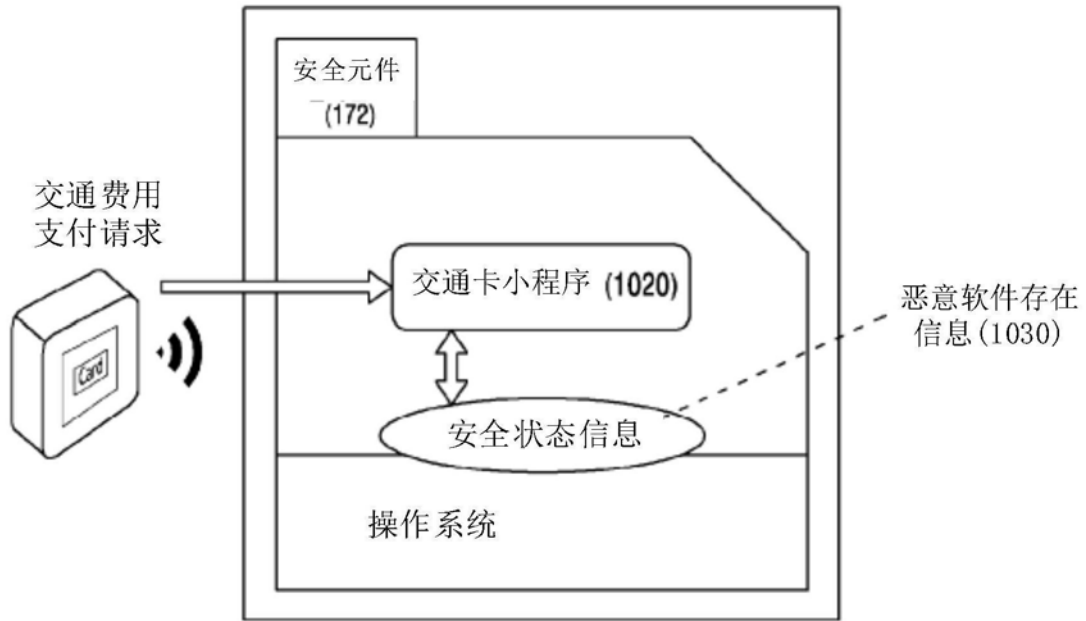


图10

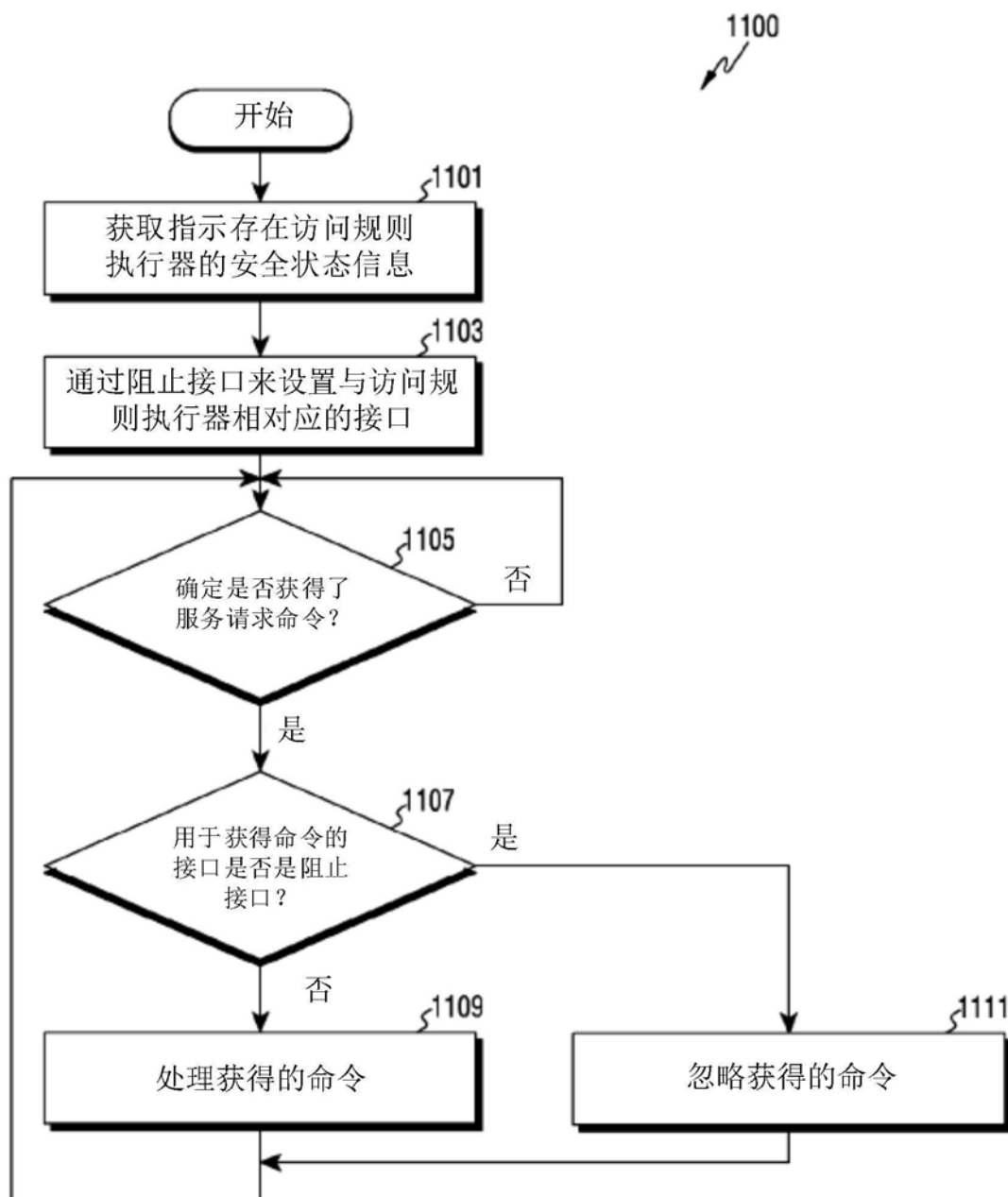


图11

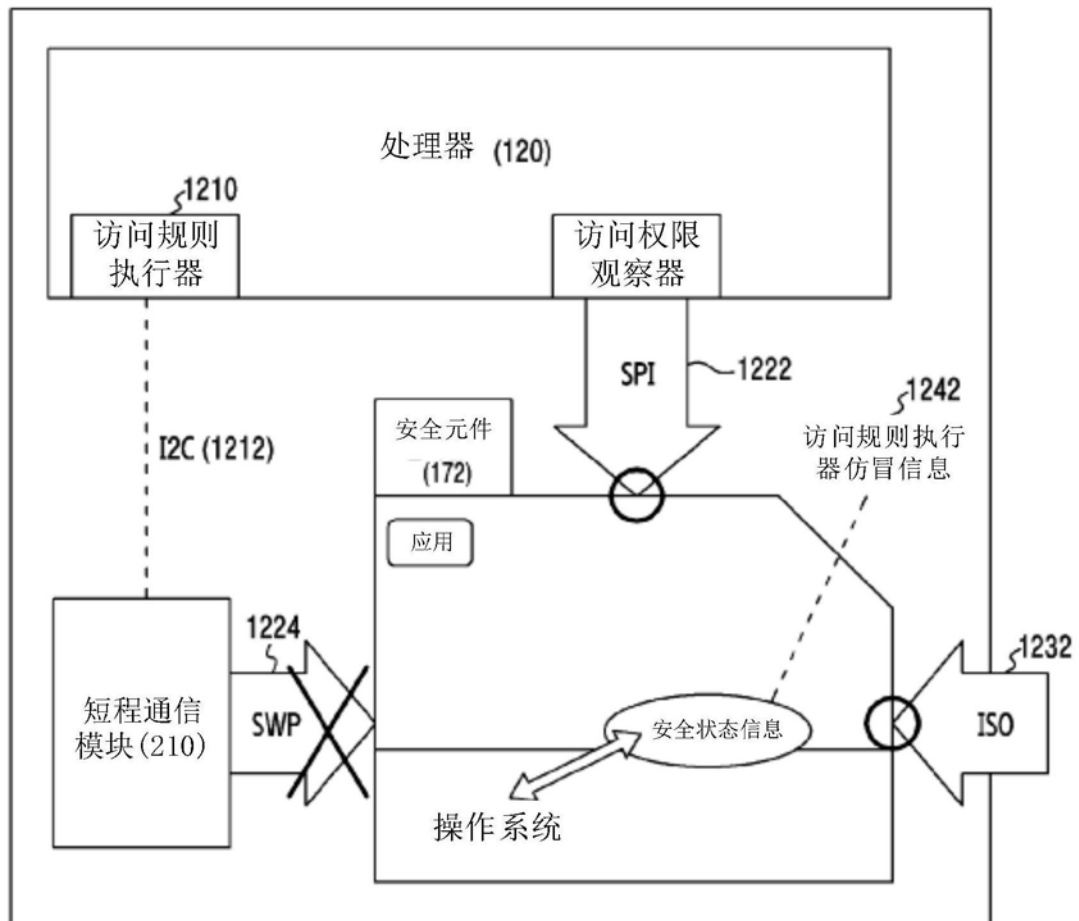


图12

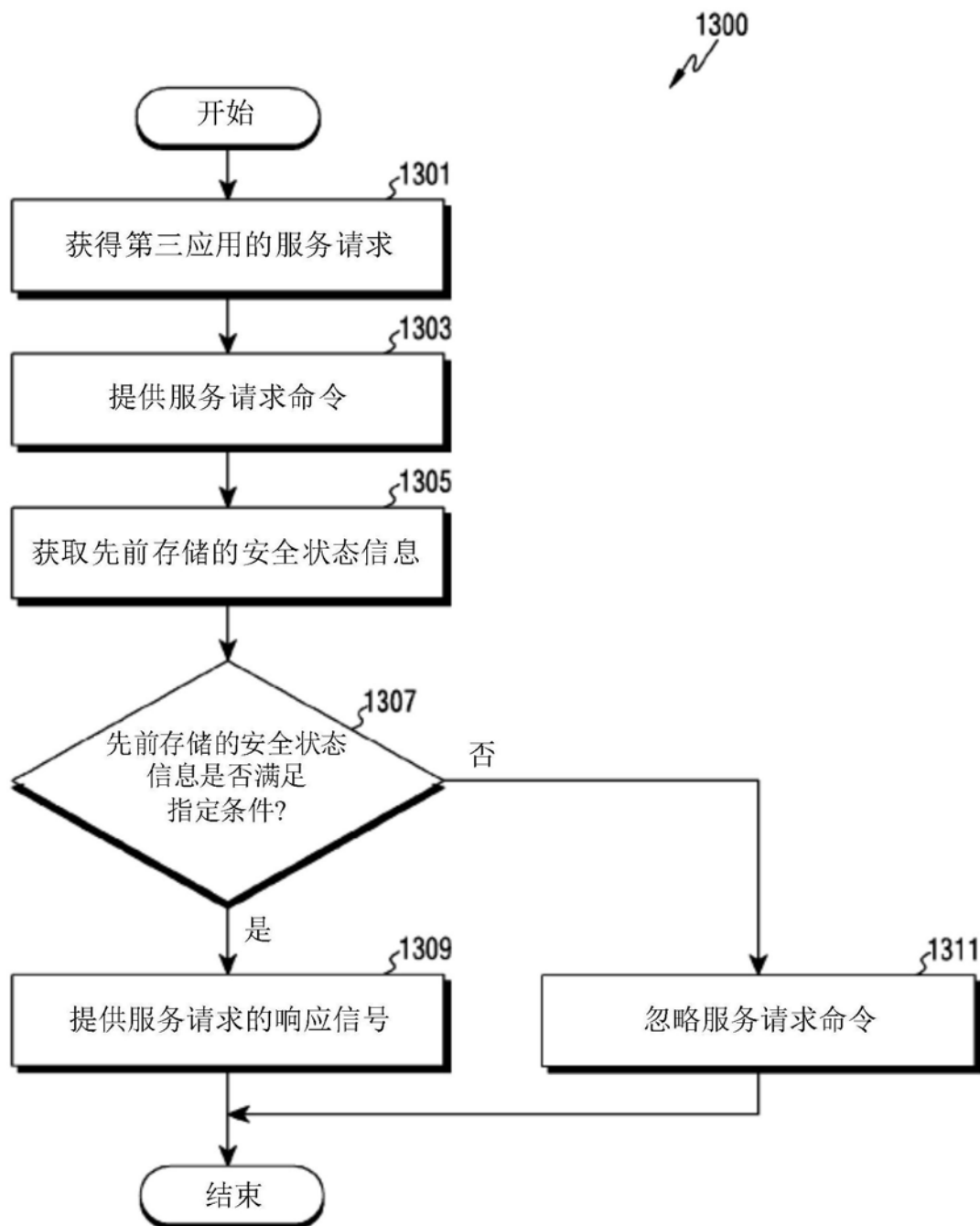


图13

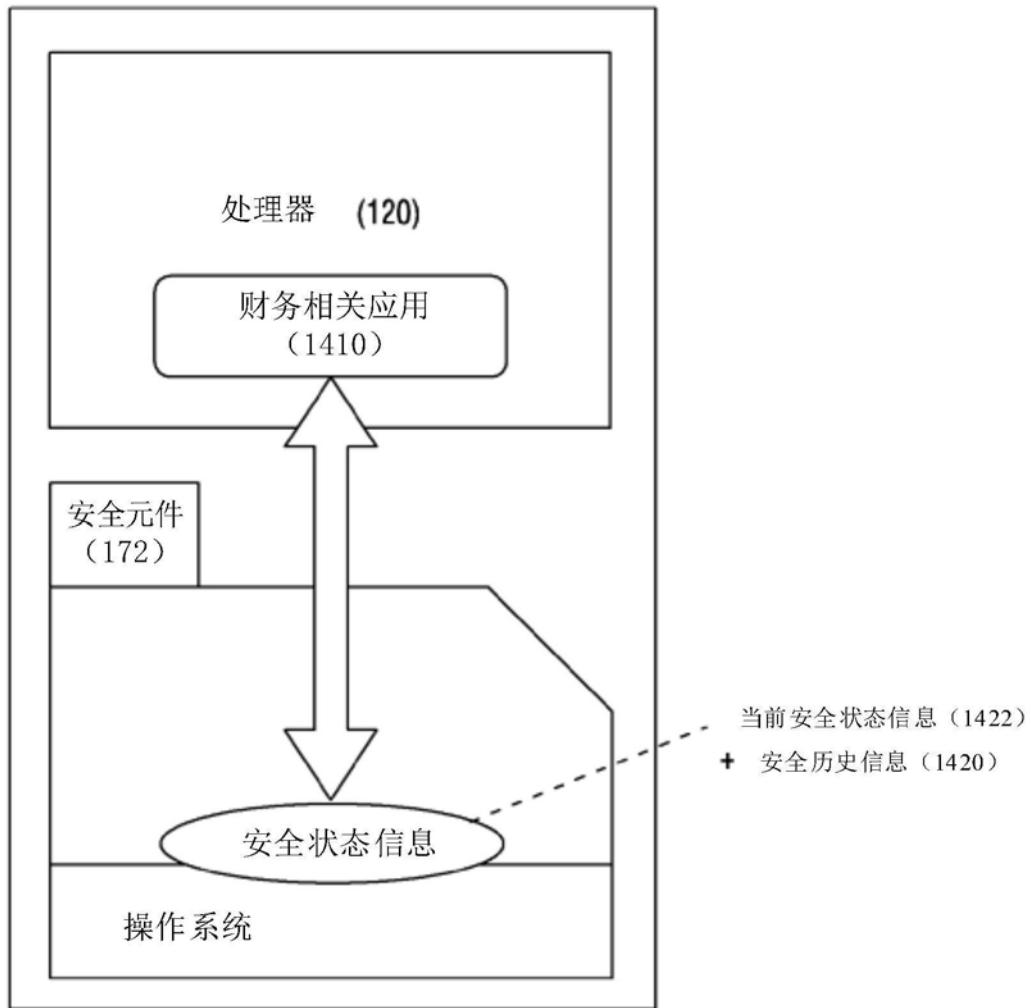


图14

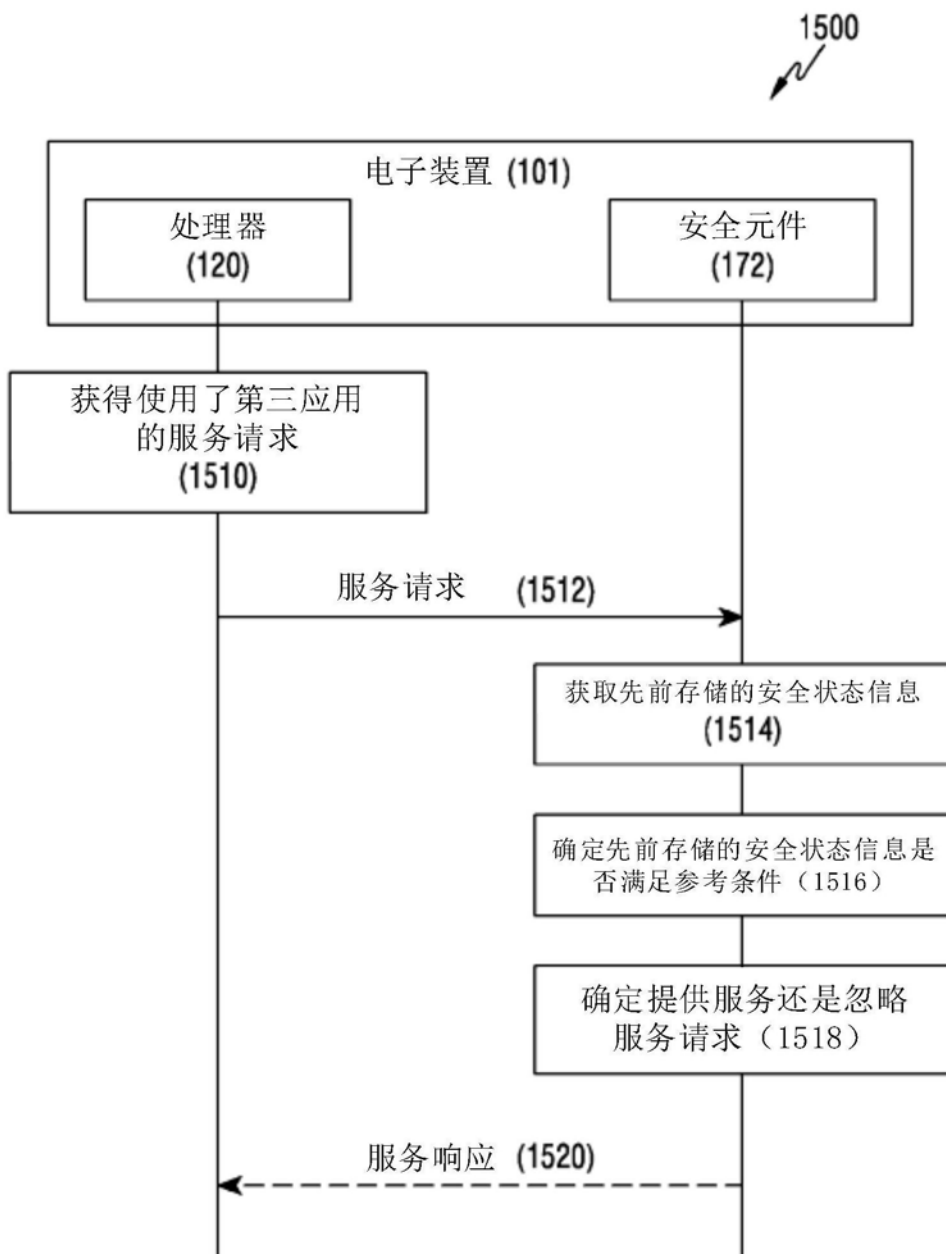


图15