



(12)发明专利申请

(10)申请公布号 CN 105917346 A

(43)申请公布日 2016.08.31

(21)申请号 201580004434.1

(22)申请日 2015.01.16

(30)优先权数据

14/166,743 2014.01.28 US

(85)PCT国际申请进入国家阶段日

2016.07.13

(86)PCT国际申请的申请数据

PCT/US2015/011838 2015.01.16

(87)PCT国际申请的公布数据

W02015/116410 EN 2015.08.06

(71)申请人 高通股份有限公司

地址 美国加利福尼亚州

(72)发明人 M·L·米兰达 Q·Y·巴希尔

S·博拉普拉高达

(74)专利代理机构 北京律盟知识产权代理有限公司 11287

代理人 宋献涛

(51)Int.Cl.

G06F 21/51(2006.01)

G06F 21/57(2006.01)

G06F 21/44(2006.01)

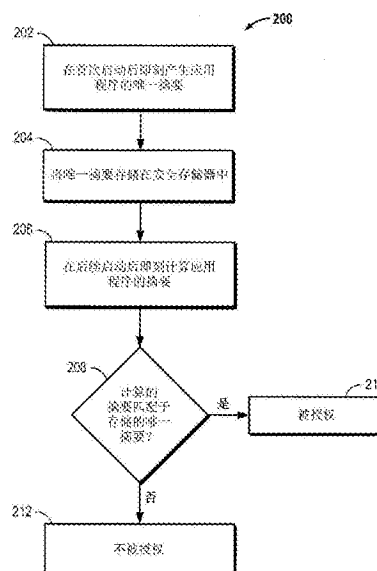
权利要求书2页 说明书6页 附图4页

(54)发明名称

授权应用程序供计算装置使用

(57)摘要

本发明揭示一种授权应用程序供使用的设备和方法。计算装置可利用应用程序且可包含安全存储器和处理器。所述处理器可：在首次启动后即刻产生所述应用程序的唯一摘要；将所述唯一摘要存储在所述安全存储器中；在后续启动后即刻计算所述应用程序的应用程序摘要；以及如果所述计算的应用程序摘要匹配于所述存储的唯一摘要，那么授权所述应用程序供使用。



1. 一种计算装置,其包括:
安全存储器;以及
处理器,其用以:
在首次启动后即刻产生应用程序的唯一摘要;
将所述唯一摘要存储在所述安全存储器中;
在后续启动后即刻计算所述应用程序的应用程序摘要;以及
如果所述计算的应用程序摘要匹配于所述存储的唯一摘要,那么授权所述应用程序供使用。
2. 根据权利要求1所述的计算装置,其中如果所述计算的应用程序摘要不匹配所述存储的唯一摘要,那么不授权所述应用程序供使用。
3. 根据权利要求1所述的计算装置,其中所述唯一摘要是在所述首次启动后即刻基于至少所述应用程序的散列函数而产生。
4. 根据权利要求3所述的计算装置,其中所述唯一摘要进一步基于与所述处理器相关联的序列号和所述应用程序的所述散列函数的串接而产生。
5. 根据权利要求4所述的计算装置,其中在后续启动后的所述计算的应用程序摘要是基于与所述处理器相关联的所述序列号和所述应用程序的所述散列函数的串接。
6. 一种授权应用程序供使用的方法,其包括:
在首次启动后即刻产生所述应用程序的唯一摘要;
将所述唯一摘要存储在安全存储器中;
在后续启动后即刻计算所述应用程序的应用程序摘要;以及
如果所述计算的应用程序摘要匹配于所述存储的唯一摘要,那么授权所述应用程序供使用。
7. 根据权利要求6所述的方法,其中如果所述计算的应用程序摘要不匹配所述存储的唯一摘要,那么不授权所述应用程序供使用。
8. 根据权利要求6所述的方法,其中所述唯一摘要是在所述首次启动后即刻基于至少所述应用程序的散列函数而产生。
9. 根据权利要求8所述的方法,其中所述唯一摘要进一步基于与处理器相关联的序列号和所述应用程序的所述散列函数的串接而产生。
10. 根据权利要求9所述的方法,其中在后续启动后的所述计算的应用程序摘要是基于与所述处理器相关联的所述序列号和所述应用程序的所述散列函数的串接。
11. 一种包含代码的非暂时性计算机可读媒体,所述代码在由处理器执行时致使所述处理器:
在首次启动后即刻产生应用程序的唯一摘要;
将所述唯一摘要存储在安全存储器中;
在后续启动后即刻计算所述应用程序的应用程序摘要;以及
如果所述计算的应用程序摘要匹配于所述存储的唯一摘要,那么授权所述应用程序供使用。
12. 根据权利要求11所述的计算机可读媒体,其中如果所述计算的应用程序摘要不匹配所述存储的唯一摘要,那么不授权所述应用程序供使用。

13. 根据权利要求11所述的计算机可读媒体,其中所述唯一摘要是在所述首次启动后即刻基于至少所述应用程序的散列函数而产生。

14. 根据权利要求13所述的计算机可读媒体,其中所述唯一摘要进一步基于与所述处理器相关联的序列号和所述应用程序的所述散列函数的串接而产生。

15. 根据权利要求14所述的计算机可读媒体,其中在后续启动后的所述计算的应用程序摘要是基于与所述处理器相关联的所述序列号和所述应用程序的所述散列函数的串接。

16. 一种计算装置,其包括:

用于在首次启动后即刻产生应用程序的唯一摘要的装置;

用于将所述唯一摘要存储在安全存储器中的装置;

用于在后续启动后即刻计算所述应用程序的应用程序摘要的装置;以及

如果所述计算的应用程序摘要匹配于所述存储的唯一摘要,那么授权所述应用程序供使用。

17. 根据权利要求16所述的计算装置,其中如果所述计算的应用程序摘要不匹配所述存储的唯一摘要,那么不授权所述应用程序供使用。

18. 根据权利要求16所述的计算装置,其中所述唯一摘要是在所述首次启动后即刻基于至少所述应用程序的散列函数而产生。

19. 根据权利要求18所述的计算装置,其中所述唯一摘要进一步基于与处理器相关联的序列号和所述应用程序的所述散列函数的串接而产生。

20. 根据权利要求19所述的计算装置,其中在后续启动后的所述计算的应用程序摘要是基于与所述处理器相关联的所述序列号和所述应用程序的所述散列函数的串接。

授权应用程序供计算装置使用

技术领域

[0001] 本发明涉及授权应用程序供计算装置使用的设备和方法。

背景技术

[0002] 通常,用于计算装置的应用程序绑定到所述计算装置且经验证以供使用。在当前实施方案中,当在启动后加载应用程序时,产生经签名的摘要和应用程序摘要以验证所述应用程序,这两者常常利用芯片的序列号。经签名的摘要是基于以存储在引导ROM或一次可编程存储器中的公共密钥解密的签名。应用程序摘要是由应用程序的散列函数结合所述序列号而产生。将经签名摘要与本地计算的散列摘要进行比较,且如果它们相同,那么应用程序通过验证。否则,应用程序未通过验证。

[0003] 不利的是,基于芯片供应商的唯一序列号的此静态签名已被发现是繁琐的。

发明内容

[0004] 本发明的方面可涉及授权应用程序供使用的设备和方法。计算装置可利用应用程序且可包含安全存储器和处理器。所述处理器可:在首次启动后即刻产生所述应用程序的唯一摘要;将所述唯一摘要存储在所述安全存储器中;在后续启动后即刻计算所述应用程序的应用程序摘要;以及如果所述计算的应用程序摘要匹配于所述存储的唯一摘要,那么授权所述应用程序供使用。

附图说明

[0005] 图1是可在其中实践本发明的方面的计算装置的图。

[0006] 图2是说明确定应用程序是否经授权供使用的过程的实例的流程图。

[0007] 图3是说明可用以实施授权或不授权应用程序供使用的过程的组件的框图。

[0008] 图4是与在确定计算的应用程序摘要以及授权或不授权应用程序供使用中利用的功能相关的过程的实例。

具体实施方式

[0009] 词语“示范性”或“实例”在本文中是指“充当实例、例子或说明”。本文中描述为“示范性”或描述为“实例”的任何方面或实施例不一定解释为比其它方面或实施例优选或有利。

[0010] 如本文所使用,术语“计算系统或装置”指代任何形式的可编程计算机装置,包括但不限于膝上型计算机和桌上型计算机、平板计算机、智能电话、电视机、家用电器、蜂窝式电话、个人电视装置、个人数据助理(PDA)、掌上型计算机、无线电子邮件接收器、具多媒体因特网功能的蜂窝式电话、全球定位系统(GPS)接收器、无线游戏控制器、交通工具(例如,汽车)内的接收器、交互式游戏装置、笔记本电脑、智能笔记本电脑、上网本、移动电视装置或任何数据处理设备。

[0011] 图1中说明可用以授权应用程序供使用的实例计算装置100,如下文将详细地描述。展示计算装置100包括可经由总线105电耦合(或适当时可以另外方式连通)的硬件元件。所述硬件元件可包含:一或多个处理器110,包含(不限于)一或多个通用处理器和/或一或多个专用处理器(例如数字信号处理芯片、图形加速处理器和/或类似物);一或多个输入装置115(例如,键盘、小键盘、触摸屏、鼠标等);以及一或多个输出装置120,其包含至少显示装置121,且可进一步包含(不限于)扬声器、打印机和/或类似物。此外,处理器110可在规则模式112和安全模式114中操作。

[0012] 计算装置100可进一步包含以下各项(和/或与以下各项通信):一或多个非暂时性存储装置125,所述非暂时性存储装置可包括(但不限于)本地及/或网络可存取的存储装置,和/或可包含(但不限于)磁盘驱动器、驱动阵列、光学存储装置、例如随机存取存储器(“RAM”)和/或只读存储器(“ROM”)等固态存储装置,其可为可编程的、可快闪更新的和/或其类似者。此类存储装置可经配置以实施任何适当数据存储装置,包含但不限于各种文件系统、数据库结构及/或其类似者。

[0013] 计算装置100还可包含通信子系统130,其可包含(不限于)模式、网卡(无线或有线)、红外通信装置、无线通信装置和/或芯片组(例如蓝牙装置、802.11装置、Wi-Fi装置、WiMax装置、蜂窝式通信装置等)和/或类似物。通信子系统130可准许与网络、其它计算机系统 and/或本文中所描述的任何其它装置交换数据。在许多实施例中,计算装置100将进一步包括非暂时性工作存储器135,其可包含RAM或ROM装置,如上文所描述。而且,计算装置100可包含安全存储器137以辅助授权应用程序供使用,如稍后将更详细描述。

[0014] 计算装置100还可包括展示为当前位于工作存储器135内的软件元件,其包含操作系统140、应用程序145、装置驱动器、可执行库和/或其它代码。在一个实施例中,应用程序可经设计以实施方法和/或配置系统以实施本发明的实施例,如本文中所描述。仅仅作为实例说明,相对于下文论述的方法描述的一或多个程序可实施为可由计算装置(和/或计算装置内的处理器)执行的代码和/或指令;在一方面中,根据本发明的实施例,随后此些代码和/或指令可用以配置和/或适配通用计算机(例如,计算装置)以根据所描述方法执行一或多个操作。

[0015] 这些指令及/或代码的集合可存储在非暂时性计算机可读存储媒体(例如上文所描述的存储装置125)上。在一些情况下,存储媒体可能并入到例如计算装置100等计算机系统内。在其它实施例中,存储媒体可能与计算机系统(例如,可装卸式媒体,例如压缩光盘)分开,及/或提供于安装包中,使得存储媒体可用以编程、配置及/或适配其上存储有指令/代码的通用计算机。这些指令可能呈可由计算机化计算装置100执行的可执行代码的形式,且/或可能呈源和/或可安装代码的形式,所述源和/或可安装代码在计算装置100上编译和/或安装于计算装置100上(例如,使用多种通常可用编译程序、安装程序、压缩/解压缩实用程序等中的任一者)后,接着呈可执行代码的形式。

[0016] 所属领域的技术人员将显而易见可根据特定要求作出大量变化。举例来说,还可能使用定制硬件,且/或可能将特定元件实施于硬件、软件(包含便携式软件,例如小程序等)或两者中。此外,可以采用到其它计算装置(例如,网络输入/输出装置)的连接。

[0017] 如先前描述,通过当前常规方法基于处理器的唯一序列号(例如,来自芯片供应商)在每次启动后的应用程序的静态签名已被发现为繁琐的。如将描述,本发明的实施例并

不需要基于用于启动的处理器序列号的签名。本发明的方面提供将应用程序动态绑定到计算装置而不需要签名的设备和方法。

[0018] 具体来说,本发明的方面可涉及授权应用程序供使用的设备和方法。在一个实施例中,如将更详细描述,计算装置100可包含安全存储器137和授权应用程序145供使用的处理器110。处理器110可在安全模式114中操作以执行包含以下各项的操作:在首次启动后即刻产生应用程序145的唯一摘要;将所述唯一摘要存储在安全存储器137中;在后续启动后即刻计算应用程序145的应用程序摘要;以及如果计算的应用程序摘要匹配于所存储的唯一摘要,那么授权所述应用程序供使用。以此方式,应用程序145可在首次启动时绑定到计算装置100。如将描述,通过基于应用程序的散列函数和处理器110的序列号计算应用程序的唯一摘要且将其保存到例如安全存储器137等安全存储区域中,应用程序145可在首次启动时动态绑定到计算装置100。

[0019] 额外参考图2,下文将描述实施本发明的实施例的方法过程200。在框202处,在安全模式114中操作的处理器110在应用程序的首次启动后即刻产生应用程序145的唯一摘要。接着,在框204处,如在安全模式114中操作的处理器110命令,将所述唯一摘要存储在安全存储器137中。在框206处,在后续启动后,在安全模式114中操作的处理器110即刻计算应用程序145的应用程序摘要。如果在框208处,在安全模式114中操作的处理器110确定计算的摘要匹配于存储在安全存储器137中的所存储的唯一摘要,那么授权应用程序145供使用(框210)。然而,如果计算的摘要不匹配存储在安全存储器137中的所存储的唯一摘要,那么不授权应用程序145供使用(框212)。

[0020] 额外参考图3,下文将描述说明可用以实施用于授权或不授权应用程序的过程的组件的框图。在此实例中,处理器110在安全模式114中操作以产生受信任区310以执行安全操作,包含安全启动加载器312和安全验证器320的安全操作。例如,在首次启动后,安全启动加载器312即刻产生正加载到计算装置上的应用程序145的唯一摘要。例如,这可由计算装置制造商完成以在其计算装置上加载经许可的应用程序供使用。安全启动加载器312可命令将针对第1启动的唯一摘要325作为所述应用程序的唯一摘要条目330存储在安全存储器137中。在应用程序145的后续启动(例如,由计算装置的购买者)后,验证器320可即刻计算应用程序145的应用程序摘要,且将其与安全存储器137中针对应用程序先前所存储的唯一摘要327进行比较。如果验证器320确定计算的应用程序摘要匹配于存储在安全存储器137中的应用程序的所存储的唯一摘要327,那么授权340应用程序145供计算装置使用。另一方面,如果验证器320确定计算的应用程序摘要不匹配存储在安全存储器137中的应用程序的所存储的唯一摘要327,那么不授权342应用程序145供计算装置使用。应了解,在安全模式114中操作的处理器110可实施先前描述的安全启动加载器312和验证器320的操作。

[0021] 下文将描述功能、操作和组件的各种示范性实施例。例如,针对首次启动的唯一摘要325可至少基于应用程序145的散列函数而产生。进一步,针对首次启动的唯一摘要325可进一步基于与处理器相关联的序列号325与应用程序的散列函数的串接。针对第1启动的此唯一摘要可作为所述应用程序的唯一摘要条目330存储在安全存储器137中。随后,在后续启动后,基于与处理器相关联的序列号325和应用程序145的散列函数的串接而确定计算的应用程序摘要。如先前描述,如果验证器320确定计算的应用程序摘要匹配于存储在安全存储器137中的应用程序的所存储的唯一摘要327,那么授权340应用程序145供计算装置使

用。另一方面,如果验证器320确定计算的应用程序摘要不匹配存储在安全存储器137中的应用程序的所存储的唯一摘要327,那么不授权342应用程序145供计算装置使用。

[0022] 在一个实施例中,所述散列函数可为安全散列算法。进一步,安全存储器137可包含受保护存储器块,例如重放受保护存储器块。然而应了解,可利用任何类型的安全或受保护类型的存储器或存储装置。

[0023] 额外参考图4,下文将描述涉及确定计算的应用程序摘要以及授权或不授权应用程序的过程400的实例。在一个实施例中,在过程400中可以看出,在后续启动中,通过安全散列算法410处理应用程序402和标头404的组合以产生计算的应用程序摘要415的第一迭代。接着,将计算的应用程序摘要415的第一迭代与同处理器相关联的序列号325串接(框420)以产生计算的应用程序摘要。在决策框430,验证器确定计算的应用程序摘要是否匹配于存储在安全存储器137中的应用程序的所存储的唯一摘要330,且如果是的话,授权450应用程序供计算装置使用。另一方面,如果在决策框430处,验证器确定计算的应用程序摘要不匹配存储在安全存储器137中的应用程序的所存储的唯一摘要327,那么不授权455应用程序145供计算装置使用。

[0024] 因此,如先前描述,在首次启动后,安全启动加载器312将首先验证应用程序145,且将应用程序的唯一摘要330存储在安全存储器137中。不需要签名过程(例如以处理器的序列号的签名)。此外,在后续启动时不需要签名过程用于验证。如先前描述,在后续启动中,安全启动加载器312可验证应用程序145。可计算借助散列算法的应用程序的摘要,且对照从首次启动时保存且存储在安全存储器137中的唯一摘要330进行比较。因此,不需要每一应用程序的签名。这显著改善应用程序的授权中的时间效率。

[0025] 应了解,先前描述的本发明的各方面可以结合由装置(例如,计算装置100)的处理器(例如,处理器110)执行指令而实施,如先前所描述。具体来说,装置的电路(包括但不限于处理器)可在执行根据本发明的实施例的方法或过程(例如,图2-4的过程和功能)的程序、例程或指令执行的控制下操作。举例来说,此类程序可以固件或软件(例如存储于存储器和/或其它位置中)实施且可由处理器和/或装置的其它电路实施。此外,应了解,术语处理器、微处理器、电路、控制器等是指能够执行逻辑、命令、指令、软件、固件、功能性等的任何类型的逻辑或电路。

[0026] 应了解,当装置为移动或无线装置时其可经由穿过无线网络的一或多个无线通信链路通信,所述无线通信链路基于或以其它方式支持任何合适的无线通信技术。例如,在一些方面中,无线装置及其它装置可与包含无线网络的网络相关联。在一些方面中,网络可包括身体区域网络或个域网(例如,超宽带网络)。在一些方面中,网络可包括局域网或广域网。无线装置可支持或以其它方式使用多种无线通信技术、协议或标准中的一或多个,例如,3G、LTE、高级LTE、4G、CDMA、TDMA、OFDM、OFDMA、WiMAX及WiFi。类似地,无线装置可以支持或以其它方式使用多种对应调制或多路复用方案中的一或多者。无线装置因此可以包含适当组件(例如,空中接口)以使用上文或其它无线通信技术建立一或多个无线通信链路及经由一或多个无线通信链路来通信。例如,装置可包括具有相关联的发射器和接收器组件(例如,发射器和接收器)的无线收发器,其可包含促进无线媒体上的通信的各种组件(例如,信号产生器及信号处理器)。众所周知,移动无线装置因此可以无线方式与其它移动装置、蜂窝电话、其它有线及无线计算机、因特网网站等通信。

[0027] 本文中的教示可以并入到多种设备(例如,装置)中(例如,在其内实施或由其执行)。例如,本文教示的一或多个方面可并入到以下各项中:电话(例如,蜂窝式电话)、个人数据助理(“PDA”)、平板计算机、移动计算机、膝上型计算机、娱乐装置(例如,音乐或视频装置)、头戴式耳机(例如,头戴受话器、耳机等)、医疗装置(例如,生物标识传感器、心率监视器、计步器、EKG装置等)、用户I/O装置、计算机、有线计算机、固定计算机、桌上型计算机、服务器、销售点装置、机顶盒或任何其它合适的装置。这些装置可具有不同的功率和数据要求。

[0028] 在一些方面中,无线装置可以包含用于通信系统的接入装置(例如Wi-Fi接入点)。此接入装置可提供(例如)经由有线或无线通信链路到另一网络(例如,广域网,例如因特网或蜂窝式网络)的连接性。因此,接入装置可以使得另一装置(例如Wi-Fi站)能够接入另一网络或某一其它功能性。

[0029] 所属领域的技术人员将了解,可使用多种不同技术和技艺中的任一者来表示信息和信号。举例来说,可以由电压、电流、电磁波、磁场或磁粒子、光场或光粒子或其任何组合来表示贯穿上文描述可能参考的数据、指令、命令、信息、信号、位、符号和码片。

[0030] 所属领域的技术人员将进一步了解,可以将结合本文中所揭示的实施例而描述的各种说明性逻辑块、模块、电路及算法步骤实施为电子硬件、计算机软件或两者的组合。为清楚说明硬件与软件的此可互换性,上文已大体上关于其功能性而描述了各种说明性组件、块、模块、电路和步骤。此功能性是实施为硬件还是软件取决于特定应用和施加于整个系统上的设计约束。所属领域的技术人员可针对每一特定应用以不同方式实施所描述的功能性,但此些实施决策不应被解释为会导致脱离本发明的范围。

[0031] 可使用经设计以执行本文所描述的功能的通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或其它可编程逻辑装置、离散门或晶体管逻辑、离散硬件组件或其任何组合来实施或执行结合本文中所揭示的实施例而描述的各种说明性逻辑块、模块及电路。通用处理器可为微处理器,但在替代方案中,处理器可为任何常规的理器、控制器、微控制器或状态机。处理器还可实施为计算装置的组合,例如,DSP与微处理器的组合、多个微处理器、结合DSP核心的一或多个微处理器,或任何其它此类配置。

[0032] 结合本文中所揭示的实施例而描述的方法或算法的步骤可直接体现于硬件、由处理器执行的软件模块或两者的组合中。软件模块可以驻留在RAM存储器、快闪存储器、ROM存储器、EPROM存储器、EEPROM存储器、寄存器、硬盘、可移动磁盘、CD-ROM,或所属领域中已知的任何其它形式的存储媒体中。示范性存储媒体耦合到处理器,使得处理器可以从存储媒体读取信息并且将信息写入到存储媒体。在替代例中,存储媒体可与处理器成一体式。处理器和存储媒体可驻留在ASIC中。ASIC可以驻留在用户终端中。在替代方案中,处理器和存储媒体可以作为离散组件驻留在用户终端中。

[0033] 在一或多个示范性实施例中,所描述的功能可以在硬件、软件、固件或其任何组合中实施。如果在软件中实施为计算机程序产品,那么可以将功能作为一或多个指令或代码存储在计算机可读媒体上或经由计算机可读媒体进行传输。计算机可读媒体包含计算机存储媒体及通信媒体两者,通信媒体包含促进将计算机程序从一处传送到另一处的任何媒体。存储媒体可为可由计算机存取的任何可用媒体。举例来说且非限制,此类计算机可读媒体可包括RAM、ROM、EEPROM、CD-ROM或其它光盘存储装置、磁盘存储装置或其它磁性存储装

置,或可用于携载或存储呈指令或数据结构的形式所要程序代码且可由计算机存取的任何其它媒体。又,任何连接被恰当地称为计算机可读媒体。例如,如果使用同轴电缆、光纤电缆、双绞线、数字订户线(DSL)或如红外线、无线电以及微波的无线技术从网站、服务器或其它远程源传输软件,那么同轴电缆、光纤电缆、双绞线、DSL或如红外线、无线电以及微波的无线技术包含于媒体的定义中。如本文中所使用,磁盘和光盘包含压缩光盘(CD)、激光光盘、光学光盘、数字多功能光盘(DVD)、软性磁盘和蓝光光盘,其中磁盘通常以磁性方式再生数据,而光盘利用激光以光学方式再生数据。上文的组合也应包含在计算机可读媒体的范围内。

[0034] 提供对所揭示的实施例的先前描述以使得所属领域的技术人员能够制作或使用本发明。所属领域的技术人员将容易地了解对这些实施例的各种修改,并且可在不脱离本发明的精神或范围的情况下将本文所定义的一般原理应用到其它实施例中。因此,本发明并不希望限于本文中所示的方面,而应被赋予与本文中所揭示的原理和新颖特征一致的最广范围。

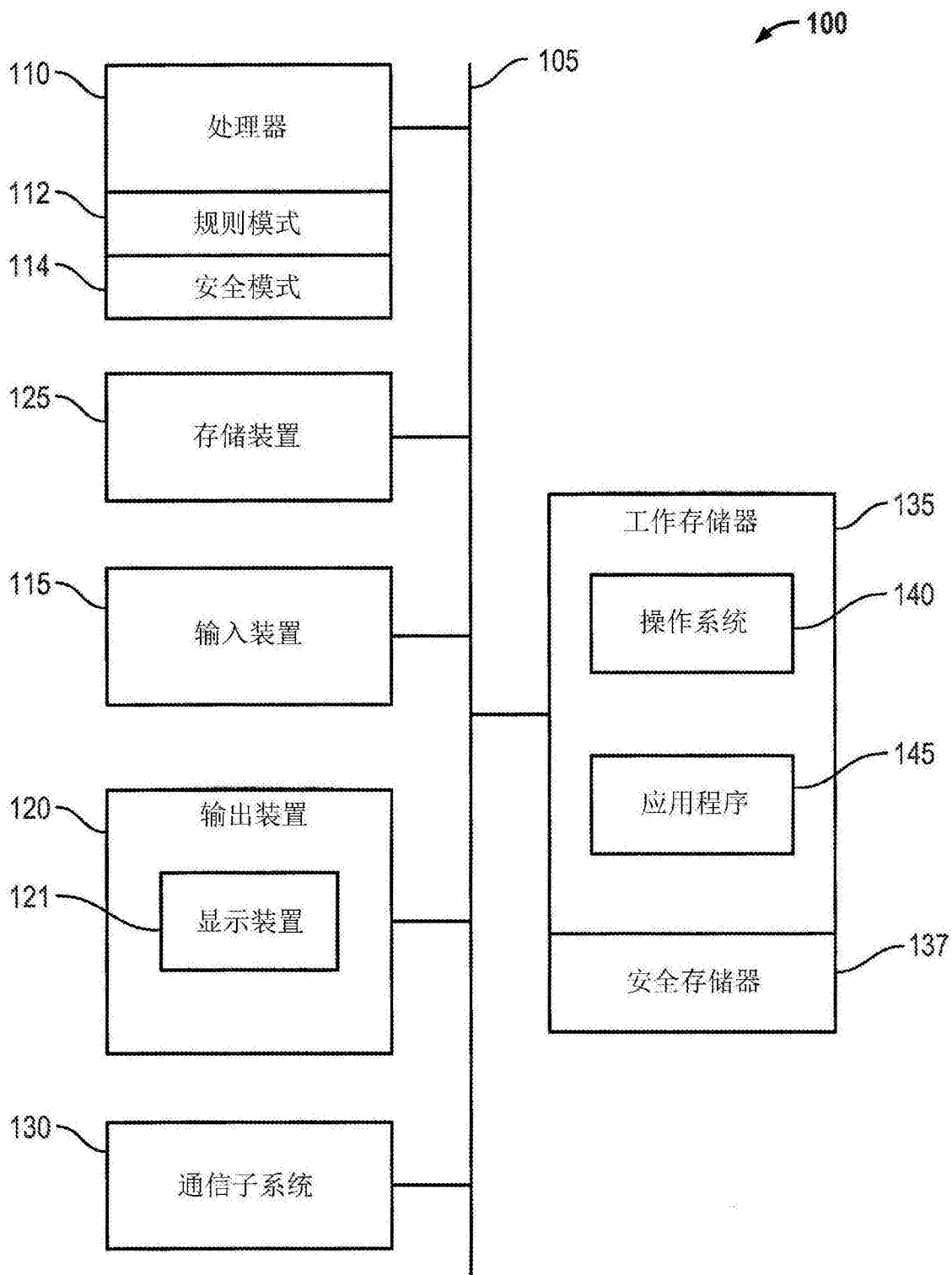


图1

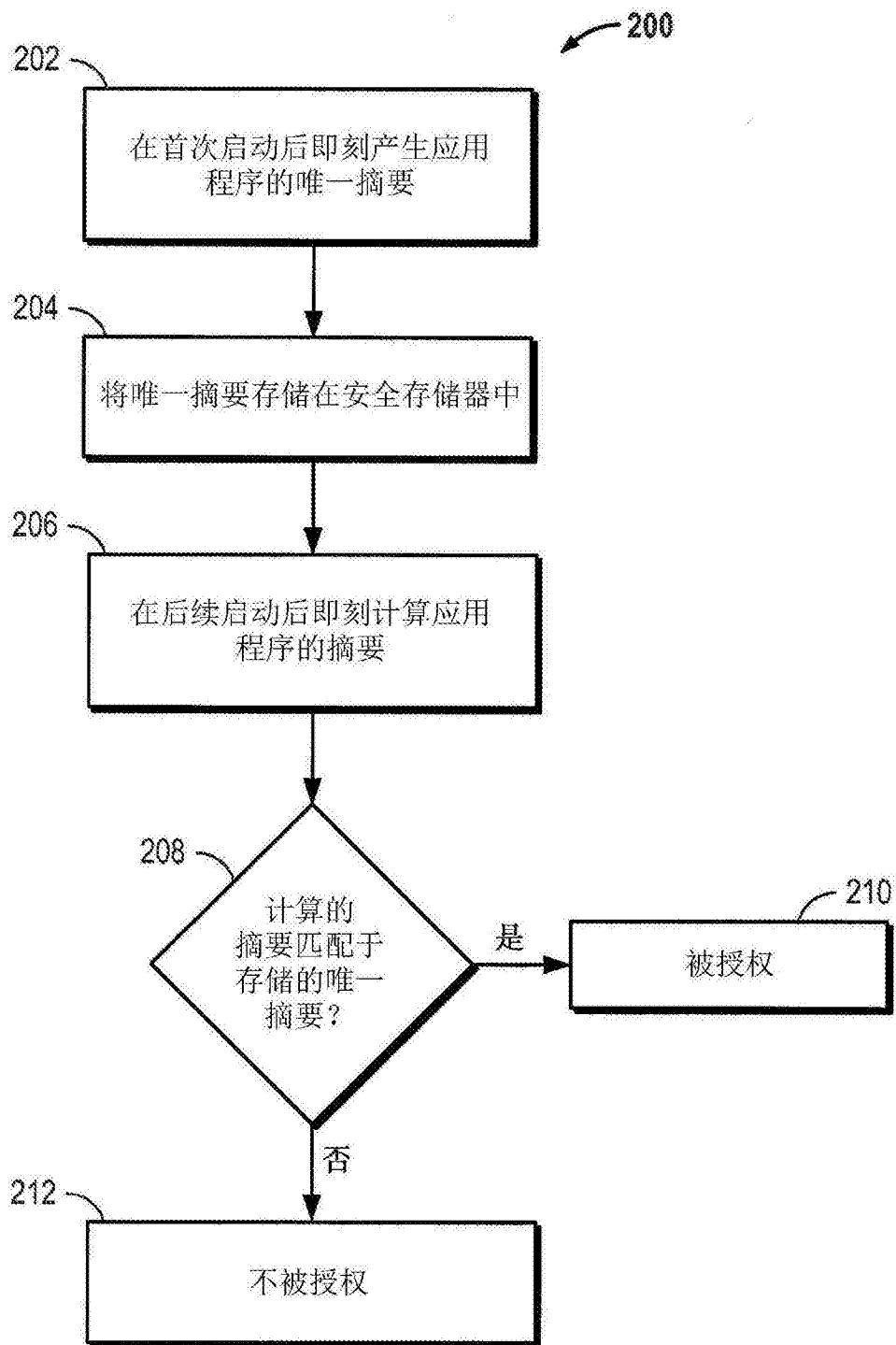


图2

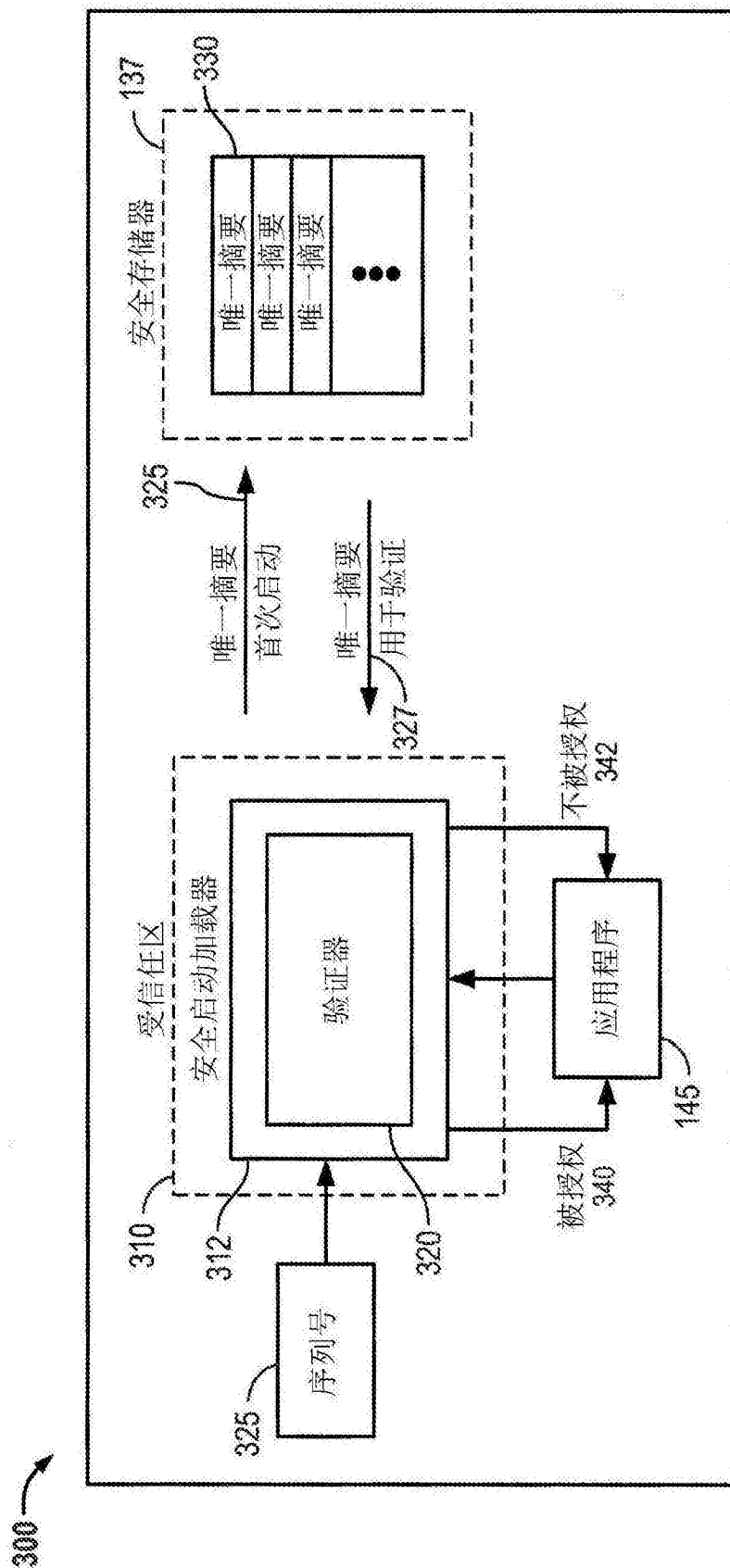


图3

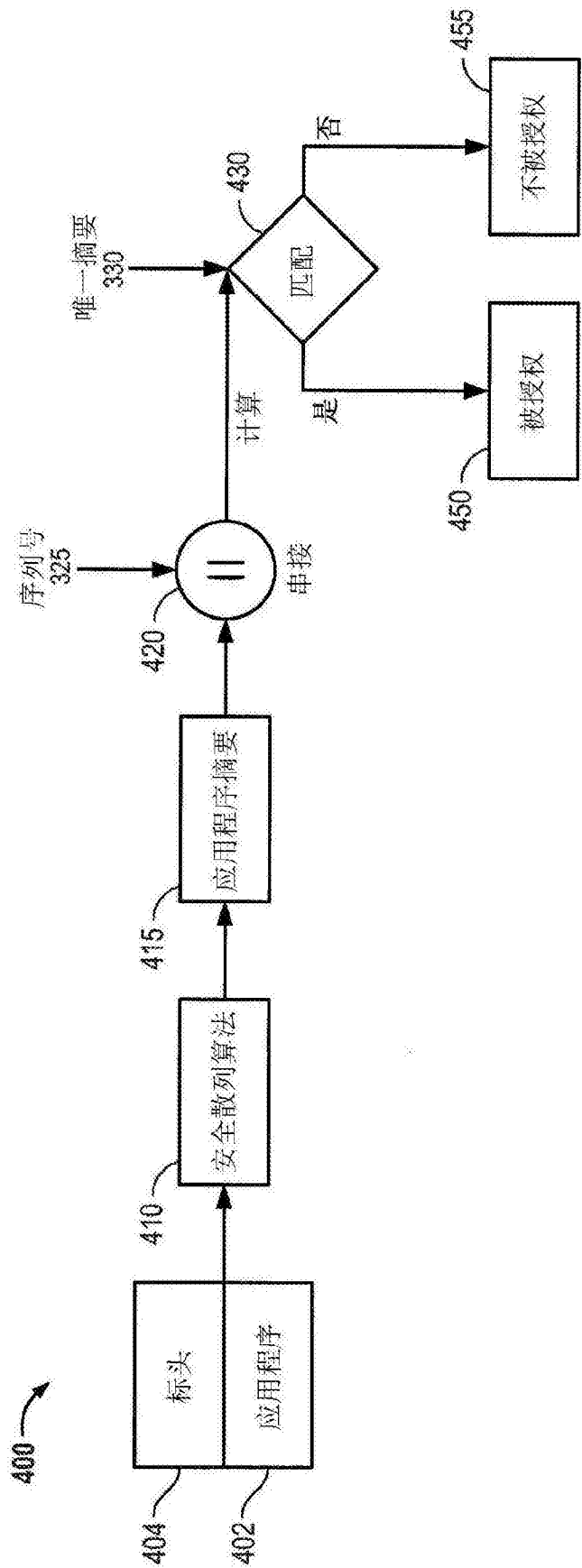


图4