(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101002180 B
(45)授权公告日 2012.09.05

(21)申请号 200480043806.3
(22)申请日 2004.11.10
(30)优先权数据
60/592,141 2004.07.30 US
(85)PCT申请进入国家阶段日
2007.02.14
(86)PCT申请的申请数据
PCT/CA2004/001943 2004.11.10
(87)PCT申请的公布数据
WO2006/010239 EN 2006.02.02
(73)专利权人 捷讯研究有限公司
地址 加拿大安大略省
(72)发明人 梅拉妮·巴克 约翰·霍奇森
(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 王玮
(51)Int.Cl.
G06F 12/14(2006.01)
(56)对比文件
US 20030159059 A1,2003.08.21, 全文.
CN 1278082 A,2000.12.27, 说明书第2页第29-30行,第3页第15-20,23-26行,第3页第31行至第4页第1行,第4页第15-24行,第5页第17-18行,第7页第6-8行、附图1-2.
US 6151678 A,2000.11.21, 说明书第4栏第52-58行,第5栏第8-10行、附图5.
审查员 史雅云

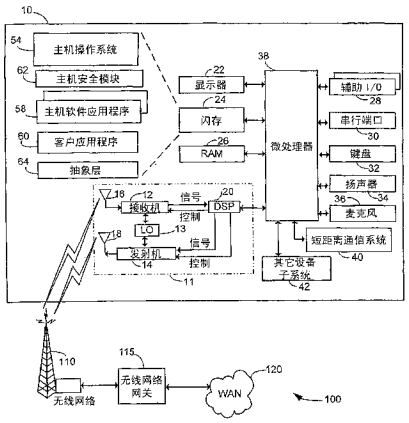
权利要求书 2 页 说明书 9 页 附图 4 页

(54)发明名称

用于协调客户和主机安全模块的方法和系统

(57)摘要

一种系统和方法,用于对移动电子设备上的客户安全模块和主机安全模块的操作进行协调。所述模块使用应用程序编程接口,通过平台抽象层来彼此进行通信,以协调所述模块的行为。具体地,客户安全模块指示主机安全模块何时对设备进行锁定和解锁,而且主机安全模块向客户安全模块警告用户尝试对设备进行锁定或解锁。



CN 101002180 B

1. 一种用于协调客户安全模块和主机安全模块的方法，其中两个模块均驻留在移动电子设备上，所述方法包括步骤：

检测锁定事件；

由客户安全模块实现第一锁定操作；

从客户安全模块向主机安全模块发送锁定命令；以及

响应于所述锁定命令，在主机安全模块处启动锁定操作。

2. 根据权利要求 1 所述的方法，其中所述检测锁定事件步骤包括向客户安全模块警告所述锁定事件，而且所述实现步骤包括由客户安全模块实现客户锁定。

3. 根据权利要求 2 所述的方法，其中所述向客户安全模块警告锁定事件包括：调用应用程序编程接口，用于向客户安全模块警告所述锁定事件。

4. 根据权利要求 1 所述的方法，其中所述发送步骤包括通过平台抽象层发送锁定命令。

5. 根据权利要求 1 所述的方法，其中所述发送步骤包括：调用应用程序编程接口，用于指示主机安全模块执行第二锁定。

6. 根据权利要求 1 所述的方法，其中所述启动锁定操作步骤包括启动安全屏幕。

7. 根据权利要求 1 所述的方法，其中所述启动锁定操作步骤包括锁定小键盘。

8. 根据权利要求 1 所述的方法，其中所述实现第一锁定操作步骤包括防止用户访问存储在设备上的数据。

9. 一种用于协调客户安全模块和主机安全模块的方法，其中两个模块均驻留在移动电子设备上，所述方法包括步骤：

接收用户安全输入；

验证接收到的所述用户安全输入；

如果所述用户安全输入有效，由客户安全模块执行第一解锁操作；

从客户安全模块向主机安全模块发送解锁命令；以及

响应于所述解锁命令，在主机安全模块处启动第二解锁操作。

10. 根据权利要求 9 所述的方法，其中所述验证步骤由客户安全模块执行。

11. 根据权利要求 9 所述的方法，其中所述发送步骤包括通过平台抽象层发送解锁命令。

12. 根据权利要求 11 所述的方法，其中所述平台抽象层包括多个应用程序编程接口，而且所述发送解锁命令步骤包括调用所述应用程序编程接口之一。

13. 根据权利要求 9 所述的方法，其中所述执行第一解锁操作步骤包括允许用户访问存储在设备上的数据。

14. 根据权利要求 9 所述的方法，其中所述启动第二解锁操作步骤包括允许用户访问主机端应用程序。

15. 根据权利要求 9 所述的方法，还包括步骤：检测输入事件，并响应于所述输入事件，显示用于接收所述用户安全输入的对话框。

16. 根据权利要求 15 所述的方法，其中所述检测输入事件步骤包括向客户安全模块警告输入事件，而且所述显示用于接收所述用户安全输入的对话框的步骤由所述客户安全模块执行。

17. 一种移动电子设备，包括：

主机操作系统；

主机安全模块，其中主机操作系统和主机安全模块驻留在所述设备的主机端上；

客户应用程序，所述客户应用程序包括客户安全模块，其中所述客户应用程序驻留在所述设备的客户端上；以及

抽象接口层，设置在客户端和主机端之间，所述抽象接口层包括多个应用程序编程接口，用于在客户安全模块与主机安全模块之间交换通信，

其中所述客户安全模块包括：用于响应于锁定事件而实现客户端锁定操作、以及调用所述应用程序编程接口之一以指示所述主机安全模块实现主机端锁定操作的组件。

18. 根据权利要求 17 所述的移动电子设备，其中所述主机安全模块包括：用于响应于来自所述客户安全模块的所述调用而执行主机锁定操作的组件。

19. 根据权利要求 17 所述的移动电子设备，其中所述应用程序编程接口包括：用于请求对口令进行验证的应用程序编程接口。

20. 一种移动电子设备，包括：

主机操作系统；

主机安全模块，其中主机操作系统和主机安全模块驻留在所述设备的主机端上；

客户应用程序，所述客户应用程序包括客户安全模块，其中所述客户应用程序驻留在所述设备的客户端上；以及

抽象接口层，设置在客户端和主机端之间，所述抽象接口层包括多个应用程序编程接口，用于在客户安全模块与主机安全模块之间交换通信，其中所述客户安全模块包括：用于响应于有效口令而对设备的客户端进行解锁、以及调用所述应用程序编程接口之一以指示所述主机安全模块对设备的主机端进行解锁的组件。

21. 根据权利要求 20 所述的移动电子设备，其中所述主机安全模块包括：用于响应于来自所述客户安全模块的所述调用而执行主机解锁操作的组件。

22. 根据权利要求 20 所述的移动电子设备，其中所述应用程序编程接口包括：用于请求对口令进行验证的应用程序编程接口。

23. 根据权利要求 20 所述的移动电子设备，其中所述主机安全模块包括用于在设备启动时进行操作的解锁组件，其中所述解锁组件接收输入口令并调用所述应用程序编程接口，以请求对所述输入口令进行验证。

用于协调客户和主机安全模块的方法和系统

[0001] 本申请要求2004年7月30日递交的美国临时专利申请序列号no.60/592,141的优先权,将其内容在此引入作为参考。

技术领域

[0002] 本申请涉及第三方主机设备上操作的客户应用程序,具体涉及对客户安全模块和主机安全模块的操作进行协调。

背景技术

[0003] 通常期望把提供特殊功能的成功的客户应用程序附加到第三方设备,该设备涉及相关但不同的功能。例如,在典型地提供语音呼叫能力和文本消息收发能力的移动电话中,合并其它方提供的、使移动电话能够用于无线数据通信的客户应用程序是有利的。在一个示例中,客户应用程序能够使用移动电话进行电子邮件通信。

[0004] 将已有的客户应用程序置于具有其自有架构和操作平台的移动电话上,将可能导致在客户应用程序中的特殊模块与在移动电话主机系统中操作的特定模块之间产生冲突。例如,客户应用程序可以包括用于实现客户安全策略组的安全模块。移动电话可以以其自有的主机安全模块实现其安全特征。由移动电话的主机安全模块所实现的安全特征可能不同于客户安全模块所实现的安全策略,或与客户安全模块所实现的安全策略产生冲突。因此,需要确保客户安全模块和主机安全模块对其安全行为做出协调,从而保持足够的数据安全级别。

发明内容

[0005] 本申请描述了一种系统和方法,用于对客户安全模块和主机安全模块的操作进行协调。所述模块使用应用程序编程接口,通过平台抽 象层来彼此进行通信,以协调所述模块的行为。特别地,客户安全模块指示主机安全模块何时对设备进行解锁,而且主机安全模块警告客户安全模块尝试对设备进行锁定或解锁。

[0006] 一方面,本申请提供了一种用于协调客户安全模块和主机安全模块的方法,其中两个模块均驻留在移动电子设备上。所述方法包括步骤:检测锁定事件;由客户安全模块和主机安全模块中的一个实现第一锁定操作;从客户安全模块和主机安全模块中的所述一个向客户安全模块和主机安全模块中的另一个发送锁定命令;以及响应于锁定命令,在客户安全模块和主机安全模块中的所述另一个处启动锁定操作。

[0007] 另一方面,本申请提供了一种用于协调客户安全模块和主机安全模块的方法,其中两个模块均驻留在移动电子设备上。所述方法包括步骤:接收用户安全输入;验证接收到的用户安全输入;由客户安全模块和主机安全模块中的一个执行第一解锁操作;从客户安全模块和主机安全模块中的所述一个向客户安全模块和主机安全模块中的另一个发送解锁命令;以及响应于解锁命令,在客户安全模块和主机安全模块中的所述另一个处启动第二解锁操作。

[0008] 另一方面，本申请提供了一种移动电子设备。所述设备包括主机操作系统和主机安全模块，其中主机操作系统和主机安全模块驻留在所述设备的主机端上。所述设备还包括客户应用程序，所述客户应用程序包括客户安全模块，其中所述客户应用程序驻留在所述设备的客户端上。在客户端和主机端之间设置抽象接口层，所述抽象接口层包括多个应用程序编程接口，用于在客户安全模块与主机安全模块之间交换通信。

[0009] 根据下文的详细描述和示出了一个或多个实施例的附图，本申请的其它方面和特征对于本领域的普通技术人员是显而易见的。

附图说明

[0010] 参考附图，仅作为示例对实施例进行描述，其中：

[0011] 图 1 是移动电子设备和通信系统的框图；

[0012] 图 2 示意地示出了如图 1 中所示设备的移动电子设备的系统软件 架构；

[0013] 图 3 以流程图的形式示出了一种用于对客户安全模块和主机安全模块进行协调的方法；以及

[0014] 图 4 以流程图的形式示出了一种用于在启动时对移动设备进行解锁的方法。

[0015] 在所有的附图中，相似的附图标记表示相似的元件和特征。

具体实施方式

[0016] 首先参考图 1，这是其中可以应用本申请的示例实施例的通信系统 100 和移动电子设备 10 的框图。通信系统 100 包括移动电子设备 10（图 1 中仅示出了一个）、用于与移动电子设备 10 进行通信的无线网络 110、以及用于将无线网络 110 与广域网 (WAN) 120 相接口的无线网络网关 115。

[0017] 在图 1 中的实施例中，移动电子设备 10 是手持双向移动通信设备 10，至少具有数据通信能力，可能还具有语音通信能力。在示例实施例中，该设备能够与因特网上的其它计算机系统进行通信。在多个实施例中，移动电子设备 10 包括数据通信设备、配置用于数据和语音通信的多模通信设备、移动电话、移动通信设备、能够进行无线通信的 PDA、单向或双向寻呼机、与计算机系统一同工作的无线 modem、以及任意类型的移动无线通信设备。在当前所描述的实施例中，每一个移动电子设备 10 都配置用于在无线网络 110 中工作。然而应当理解的是，本申请决不限于这些示例的设备类型，而是可以在其它设备中实现。示例实施例还可以应用于启用非无线功能的设备。

[0018] 设备 10 包括通信子系统 11，通信子系统 11 包括接收机 12、发射机 14、相关组件（例如一个或多个优选地为嵌入式或内置的天线元件 16 和 18）以及处理模块（例如数字信号处理器 (DSP) 20）。在某些实施例中，所述通信子系统包括本地振荡器 (LO) 13，而且在某些实施例中，所述通信子系统和微处理器 38 共用振荡器。对于通信领域的技术人员来说显而易见的是，通信子系统 11 的具体设计将会依赖于所述设备工作时意欲处于的通信网络。

[0019] 将天线 16 通过无线通信网络 110 接收到的信号输入接收机 12，接收机 12 可以执行普通的接收机功能，例如信号放大、下变频、滤波、信道选择等，而且在某些实施例中，还可以执行模拟至数字转换。以类似的方式，DSP 20 对将要发射的信号进行处理，例如包括调制和编码，并将其输入发射机 14 以便执行数字至模拟转换、上变频、滤波、放大，并通过

天线 18 在通信网络 110 上传输。

[0020] 设备 10 包括用于控制所述设备的整体操作的微处理器 38。微处理器 38 与通信子系统 11 进行交互，而且还与其它的设备子系统进行交互，例如显示器 22、闪存 24、随机存取存储器 (RAM)26、辅助输入 / 输出 (I/O) 子系统 28（例如可以包括拇指轮）、串行端口 30、键盘或小键盘 32、扬声器 34、麦克风 36、短距离通信子系统 40 以及通常由 42 所指定的任意的其它设备子系统。

[0021] 图 1 中所示的某些子系统执行与通信有关的功能，而其它子系统可以提供“驻留”或设备上功能。特别地，例如键盘 32 和显示器 22 的某些子系统可以同时用于与通信有关的功能（例如输入文本消息，用于在通信网络上发送）和设备驻留功能（例如计算器或任务列表）。

[0022] 在一个示例实施例中，微处理器 38 所使用的主机操作系统软件 54 和多种主机软件应用程序 58 被存储在例如闪存 24 的持久性存储器或类似存储元件中。主机软件应用程序 58 可以包括广泛的应用程序，包括文本消息收发应用程序、铃声应用程序、联系应用程序和 / 或游戏应用程序。本领域的技术人员可以认识到，可以将主机操作系统 54、特定的主机应用程序 58 或其部分临时加载到例如 RAM 26 的易失性存储器中。可以设想的是，还可以把接收到的通信信号存储在 RAM 26 中。

[0023] 除了其操作系统功能之外，微处理器 38 能够在所述设备上执行主机软件应用程序 58。通常在制造期间，将用于控制基本设备操作的、预定一组主机应用程序 58（例如至少包括语音通信应用程序）安装在设备 10 上。还可以通过网络 110、辅助 I/O 子系统 28、串行端口 30、短距离通信子系统 40 或任意其它适合的子系统 42，将其它应用程序加载到设备 10 上，而且由用户将这些应用程序安装到 RAM 26 或非易失性存储器中，以便由微处理器 38 执行。这种应用程序安装的灵活性增加了 设备的功能，而且可以提供增强的设备上功能、与通信有关的功能或两者都有。例如，安全的通信应用程序使得能够使用设备 10 来执行电子商务功能和其它类似的金融交易。

[0024] 在通信模式下，通信子系统 11 对接收到的信号（例如语音呼叫、文本消息或下载的网页）进行处理，然后将其输入微处理器 38，微处理器 38 对接收到的信号做进一步的处理，从而输出到扬声器 34 或显示器 22，或可选择地输出到辅助 I/O 设备 28。例如，设备 10 的用户还可以使用键盘 32 和显示器 22 以及可能的辅助 I/O 设备 28，编撰例如文本消息的数据项。然后，可以通过通信子系统 11 在通信网络上发送这样编撰的项。

[0025] 图 1 中的串行端口 30 通常实现在期望与用户的桌面计算机（未示出）同步的个人数字助理 (PDA) 类型的通信设备中，但串口 30 是可选的设备组件。这个串口 30 使用户能够通过外部设备或软件应用程序而不是通过无线通信网络来设置首选项，而且通过向设备 10 提供信息或软件下载（包括用户接口信息），扩展了设备的能力。

[0026] 短距离通信子系统 40 是另外一种可以在设备 10 与不同的系统或设备之间提供通信的组件，其中这些设备不需要是相似的设备。例如，子系统 40 可以包括红外设备以及相关的电路和组件或是蓝牙 ™ 通信模块，从而与相似能力的系统和设备进行通信。

[0027] 在示例实施例中，无线移动网络 110 是无线分组数据网络（例如 Mobitex™ 或 DataTAC™），提供了对移动电子设备 10 的无线覆盖，尽管它可以是任意其它类型的无线网络。无线移动网络 110 还可以是例如 GSM（全球移动通信系统）和 GPRS（通用分组无线业

务）的语音和数据网络、CDMA（码分多址）或例如 EDGE（增强型数据服务）或 UMTS（通用移动通信系统）的各种其它的第三代网络。

[0028] 设备 10 包括主机安全模块 62。主机安全模块 62 可以是驻留在设备 10 上的主机软件应用程序 58 之一。主机安全模块 62 按照设备 10 的安全策略而实施安全措施。例如，主机安全模块 62 可以监测设备的空闲时间，而且在超过空闲阈值时间时显示安全屏幕（即屏保）。在某些实施例中，主机安全模块 62 可以允许用户锁定键盘或小键盘 32。本领域的普通技术人员可以认识到主机安全模块 62 可以实施的其它安全或锁定特征。本领域的普通技术人员可以认识到，主机安全模块 62 虽然在图 1 中被描述为独立的实体，但是它可以分布在多个实体上。例如，主机安全模块 62 可以包括用于监测空闲时间的模块、用于显示安全屏幕以阻止设备访问的模块以及用于锁定小键盘的模块。在各种实施例中，这些或其它的模块可以是独立的模块、可以实现在主机操作系统 54 中或可以实现在一个或多个主机软件应用程序 58 中。可以理解的是，这里对主机安全模块的论述意欲包括所有这些变化和选择。

[0029] 除了驻留在设备 10 上的主机应用程序 58 之外，设备 10 还包括客户应用程序 60。例如，客户应用程序 60 可以是无线数据通信应用程序。例如，无线数据通信应用程序能够接收和发送电子消息。在一个实施例中，无线数据通信应用程序可以提供与远程电子消息收发服务器同步且协同工作的电子消息收发（即电子邮件），其中远程电子消息收发服务器在远程位置处与 WAN 120 相连。无线数据通信应用程序所提供的电子消息收发功能可以包括：编撰消息、保存消息和显示消息。其它功能或特征可以包括：通讯列表或目录、日历应用程序、任务列表应用程序、网络浏览器和其它模块或应用程序。客户应用程序 60 是齐全 (self-contained) 的单独实体，它被设计成工作在特定的“本地 (native)”设备上，这将在下文详细描述。

[0030] 客户应用程序 60 典型地由移动电子设备 10 的其余部分之外的单独实体创建和开发。典型地，客户应用程序 60 还与最初开发时有关的本地环境或设备相关。因此，客户应用程序 60 包括与客户应用程序 60 在其本地设备上的操作有关的功能和特征，但是封装成设计用于在第三方设备的第三方平台上运行的单独软件实体。为了使客户应用程序 60 能够与主机操作系统 54 和 / 或主机安全模块 62 以及其它主机应用程序 58 进行交互并交换消息和事件，设备 10 还可以包括抽象层 64。抽象层 64 包含或定义了一组应用程序编程接口 (API)，客户应用程序 60 或主机操作系统 54 和 / 或主机安全模块 62 和 / 或主机应用程序 58 可以使用这些 API，来在设备 10 的主机端与客户应用程序 60 之间交换指令、消息或事件。

[0031] 尽管图 1 所示的这组 API 包含在抽象层 64 中，本领域的普通技术人员可以理解，组成抽象层 64 的 API 不需要集中于并包含在单个库或文件中。可以理解的是，本文中的术语“应用程序编程接口”意欲包括范围广泛的、采用多种形式的进程间通信。例如在一个实施例中，API 可以包括由进程所调用的定义函数。在别的实施例中，API 可以包括从一个进程向另一个进程传递消息。本领域的普通技术人员可以理解用于进程间通信的可能接口的范围。这里对“调用”API 的引用并不意欲将操作范围限制于调用定义函数，而是意欲包括所有可能的接口形式。

[0032] 现在参考图 2，图 2 示意地示出了如图 1 所示设备 10 的移动电子设备的系统软件

架构 150。如图 2 所示，客户应用程序 60、主机安全模块 62 和主机应用程序 58 工作在主机操作系统 54 层之上。

[0033] 客户应用程序 60 包括客户操作系统层 70。在某些定义下，本质上可以不把客户操作系统层 70 看作“操作系统”，而是看作 I/O 管理层或平台。客户操作系统层 70 管理客户应用程序 60 的某些基本功能，包括文件结构和 I/O。客户操作系统层 70 提供了独立的平台，在该平台上能够运行客户专有的应用程序。

[0034] 在客户操作系统层 70 之上，客户应用程序 60 可以包括 Java 层 72 或 Java 虚拟机，包括客户安全模块 74 的多个客户模块 76 工作在层 72 中。客户安全模块 74 管理客户应用程序 60 的安全特征。例如，客户安全模块 74 可以实现口令封锁功能，借助该功能，如果没有输入有效的口令，那么用户将不能访问客户应用程序 60 及有关数据。在另一实施例中，客户安全模块 74 可以实现“小键盘”锁定系统，该系统要求特定的击键序列或按键组合以便对小键盘或键盘进行解锁。客户安全模块 74 可以包括用于接收用户口令的用户接口。

[0035] 系统软件架构 150 还包括平台抽象层 64。平台抽象层 64 在概念上可以分为主机端平台抽象层 64a 和客户端平台抽象层 64b。平台抽象层 64 能够在客户应用程序 60 与主机操作系统 54 和 / 或主机安全模块 62 和 / 或主机应用程序 58 之间实现消息和事件的往复通信。可以通过使用一个或多个 API 来实现平台抽象层 64。平台抽象层 64 允许客户应用程序 60 与主机操作系统 54、主机应用程序 58 和主机安全模块 62 无关地工作在 平台。

[0036] 客户安全模块 74 典型地实现一组安全特征，以保护用户数据和与客户应用程序 60 有关的其它数据。在其本地环境中，客户安全模块 74 可以关于客户应用程序 60 而维持特定等级的安全，该安全通常与主机安全模块 62 所提供的与设备 10 相关的安全不同。主机安全模块 62 可以实现的安全特征不足以达到客户应用程序 60 所需要的安全等级。由于可以将一些用户数据或与客户应用程序 60 相关的其它数据镜像或复制到设备 10 的主机端上的存储器中，因而需要安全模块 62、74 之间的一些协调，从而确保针对该数据的足够安全的保护。特别地，客户安全模块 74 和主机安全模块 62 对它们的行为进行协调，以便按照相同的安全策略对设备进行锁定和解锁。

[0037] 可以理解的是，在锁定情况下，尽管用户不能访问应用程序 60、58，设备 10 的特定功能可以继续工作。例如，在客户应用程序 60 包括无线数据通信应用程序的情况下，无线数据通信应用程序可以持续与无线网络进行通信，来接收和 / 或交换数据。

[0038] 现在参考图 3，图 3 以流程图的形式示出了一种方法 200，用于对移动设备上分离的安全模块的操作进行协调。方法 200 所基于的设备具有客户应用程序，其中客户应用程序具有实现口令保护特征的客户安全模块。所述设备还具有实现屏幕保护模式的主机安全模块。可以理解的是，所述安全模块可以实现其它的或额外的安全特征。例如，主机安全模块可以实现小键盘锁定特征。

[0039] 方法 200 开始时假定设备处于未锁定状态。在步骤 202，设备确定用户或远程管理员是否已经发起了客户锁定。客户安全模块可以允许用户例如从菜单中选择“锁定设备”操作。如果设备（或更具体地是客户应用程序）接收到用于执行客户锁定的客户指令或远程管理员指令，那么方法 200 前进到步骤 208。如果没有接收到指令，那么方法 200 前进到步骤 204，在步骤 204，设备确定 (access) 其是否已经接收到主机锁定指令。

[0040] 主机操作系统可以识别构成主机锁定指令的各种事件。例如，如果设备空闲了设

置的时间段，则会触发主机锁定。本领域的普通技术 人员可以理解，空闲超时可能需要由主机操作系统而不是客户应用程序来进行监测，这是因为客户应用程序可能不会一直处于设备的前台 (foreground)。其它应用程序可以控制设备处理器。因此，客户应用程序也许不能在所有情况下监测空闲超时。因此，空闲超时可以由主机操作系统来确定。空闲超时可以是步骤 204 的主机锁定指令事件。可以存在被定义为主机锁定指令的其它事件。例如，特殊的用户按键组合可以触发主机锁定。如果在步骤 204 中没有检测到主机锁定指令，那么方法 200 继续等待客户或主机锁定事件。

[0041] 如果在步骤 204 处接收到主机锁定指令，那么在步骤 206 处，将锁定事件的出现通信给客户应用程序。具体地，主机操作系统通过平台抽象层与客户应用程序进行通信。换句话说，主机操作系统调用 API，该 API 设计用于向客户应用程序警告接收到主机锁定事件。一旦调用了这个 API，那么方法 200 前进到步骤 208。

[0042] 在步骤 208，客户应用程序启动客户安全模块。公认的需要启动客户安全模块的时刻是 :在步骤 202 中用户选择了客户锁定，或是在步骤 206 中作为主机操作系统调用 API 的结果而接收到通知。一旦启动了客户安全模块，那么在步骤 210 中，客户安全模块实现客户锁定。在步骤 212，客户安全模块将消息向下中继到主机操作系统或主机安全模块，以指示它们执行其自有的锁定操作。步骤 212 包括调用 API 以触发主机操作系统实现主机锁定，或是运行主机安全模块以实现主机锁定。因此，在步骤 210 中锁定客户应用程序后，控制权返回设备的主机端以执行主机锁定。在步骤 214，实现主机锁定。在一个实施例中，主机锁定包括显示安全屏幕，即屏保。在其它实施例中，主机锁定包括实现键盘或小键盘封锁，作为安全屏幕的替代或附加。一旦主机安全模块实现了主机锁定，则在用户执行一组动作以对设备进行解锁（下文描述）之前，拒绝用户访问主机应用程序。典型地，在用户执行特定的动作以开始对设备进行解锁之前，安全屏幕保持处于前台，从而防止用户在没有满足安全要求的前提下访问任意的主机应用程序。

[0043] 在步骤 214 之后，设备处于锁定状态。在客户端或主机端上检测到锁定事件后，通过首先实现客户锁定以避免访问客户应用程序，然后 激励主机锁定以避免访问任意的主机应用程序，从而将设备置于锁定状态。

[0044] 在某些情况下，客户应用程序可要求比主机设备的安全更高的安全。因此，客户应用程序可以具有更具鲁棒性的安全措施。然而，在主机操作系统上运行客户应用程序可能会暴露客户应用程序的特定区域，例如存储在存储器中的用户专有数据。在某些情况下，尽管存在客户安全措施，也能够对信息或操作进行访问。因此，方法 200 的剩余步骤确保了用户在没有首先满足客户解锁过程的前提下不能解除主机锁定。

[0045] 当处于锁定状态时，在步骤 216 处，设备显示安全屏幕，而且主机操作系统或主机安全模块等待击键输入。在某些实施例中，当设备处于锁定状态时，主机安全模块实现小键盘或键盘锁定。可能需要特殊的按键序列对键盘进行解锁，例如在预定的时间长度内按下散列‘#’键或按下按键组合。在主机安全模块实现了小键盘锁定的实施例中，在步骤 216 处，主机安全系统对主机操作系统所检测的接收到的击键是否满足小键盘解锁要求进行评价。如果所检测的击键不满足要求，则忽略该击键且设备继续等待适当的击键或按键序列。如果所检测的击键是适当的按键序列，那么主机安全模块对小键盘进行解锁并且方法 200 前进到步骤 218。

[0046] 在步骤218，主机安全模块（在某些实施例中是主机操作系统）向客户应用程序警告接收到击键。具体地，主机安全模块调用适当的API以向客户安全模块通知接收到击键。在一个实施例中，主机安全应用程序没有实现小键盘锁定，API将接收到的击键传递给客户安全模块，从而客户安全模块可以使用接收到的击键作为用户输入口令的第一个字符。客户安全模块或主机安全模块所调用的API可评价接收到的击键是否是有意义的口令字符。例如，客户安全模块将会忽略例如向下箭头的方向键输入，或者客户安全模块将会显示菜单或选项列表；而将文本字符的输入当作口令的第一个字符。当主机安全模块（或主机操作系统）调用API以向客户安全模块警告接收到击键时，控制权传给客户安全模块。

[0047] 客户安全模块把用户口令输入屏幕显示在设备的显示器的前台，并等待用户口令输入。在步骤220，在某些实施例中，客户安全模块可以确定用户是否已经选择取消口令输入操作（即决定维持设备锁定）。客户安全模块的某些实施例可以将特殊的按键组合或击键识别为“取消”命令。如果在经过预定的持续时间后还没有输入口令，那么客户安全模块还会超时。例如，如果客户安全模块在两分钟内没有接收到击键，那么可以认为超时。在取消或超时时，在步骤222处，客户安全模块可以将控制权交还给主机安全模块，于是主机安全模块重建其安全特征，例如小键盘锁定和显示屏保。客户安全模块可以通过调用锁定命令API，将控制权传递给主机安全模块，如同步骤212中的调用一样。因此在步骤220处，设备回到锁定状态并等待输入击键。

[0048] 如果用户没有指示取消或没有超时，那么在步骤224处，客户安全模块对用户输入的口令进行评价。如果口令无效，那么在步骤226处，客户安全模块应用其口令重试策略以确定用户是否有资格重试口令输入。该策略可以建立最大尝试次数。如步骤228所示，在某些实施例中，当达到最大尝试次数后，通过删除存储在设备上的用户数据的“删除(kill)设备”操作来禁用该设备。这一步还可包括调用“删除”API，以使主机操作系统或主机安全模块从系统中删除或擦去特定的用户数据。除了响应于最大口令尝试次数的“删除操作”之外还可以采取其它动作，或是采取其它动作来替代“删除操作”。

[0049] 如果口令有效，那么方法200前进到步骤230，在步骤230，客户安全模块对设备的客户端进行解锁。在步骤232，客户安全模块利用指令把控制权传递给主机安全模块，来对设备进行解锁。客户安全模块可以通过调用主机解锁API来传递控制权，以向主机安全模块警告成功输入了用于对设备进行解锁的口令。在对设备的客户端进行解锁后，客户安全模块也可以关闭。在步骤234，主机安全模块执行对设备的主机端进行解锁所需的操作，例如关闭或最小化屏保或其它动作。然后在步骤236，主机安全模块可关闭。

[0050] 在步骤236之后，设备处于解锁状态，方法200返回到步骤202以等待其它锁定操作的启动。

[0051] 本领域的普通技术人员可以理解，方法200可以包括其它步骤或动作，以容纳具有不同特征的设备或安全模块。例如，安全模块可以允许用户在设备被锁定时做出E911紧急呼叫。因此，在步骤220附近，客户安全模块可以检测E911紧急呼叫的用户选择。这可以是在客户口令输入界面屏幕上呈现给用户的可选择的菜单动作项。当用户选择E911紧急呼叫时，客户安全模块可以调用E911 API以指示主机操作系统或其它的主机应用程序做出紧急呼叫，即使设备处于锁定状态。

[0052] 可以理解的是，例如客户管理员的用户或其它实体可以选择改变空闲超时值或其

它有关的配置值或选项。如果改变了超时值，例如用户通过客户应用程序所呈现的菜单选项做出改变，由于该值由主机操作系统监测，那么客户应用程序调用空闲超时改变 API，以指示主机操作系统更新空闲超时值。当前的空闲超时值可以由客户应用程序在设备启动时通过相同或相似 API 的调用传递给主机操作系统。

[0053] 根据上文所述，本领域的普通技术人员可以理解方法 200 的其它变体。

[0054] 在一个实施例中，启动时的解锁操作可能不同于图 3 所示的方法 200 所描述的解锁操作。当对移动设备加电时，移动设备可以以锁定状态加电。在某些实施例中，启动或加电过程所需要的时间长度可能难以接受。特别地，Java 虚拟机进行加载以及客户安全模块启动所需的时间长度可能难以接受。在 JVM 和客户安全模块启动之前，用户不能输入口令以启用设备。结果是，在客户应用程序被加载且可以使用之前，用户不能使用移动设备，甚至不能使用例如移动电话的主机应用程序。

[0055] 典型地，客户安全模块通过调用验证函数来执行口令验证。口令信息存储在设备的持久性存储器中，而且验证函数设计用于将用户输入的信息和存储的口令信息进行比较。验证函数不依赖于可访问的客户安全模块的初始化。因此，在一个实施例中，平台抽象层中设置有用于使主机端调用验证函数的 API。

[0056] 为了解决启动时的延迟，在一个实施例中，主机包括主机启动模块，主机启动模块实质上反映在请求解锁口令中客户安全模块的对话。因此，在启动时，主机启动模块显示用户输入对话屏幕，以提示用户 输入有效口令。一旦用户输入口令，主机通过平台抽象层调用客户端验证函数，并将输入的口令传递给该函数。验证函数确定口令是否有效，并将答案返回到主机启动模块。如果口令有效，那么主机启动模块通知主机安全模块，并对主机端进行解锁。在某些实施例中，客户端在启动时没有被锁定，所以一旦主机端被解锁，那么所有的设备应用程序都可以使用。在另一实施例中，客户端在启动时被锁定，所以验证函数或主机启动模块将会向客户安全模块通知已经输入了有效口令，从而一旦客户应用程序被初始化，那么客户端也被解锁。可以理解的是，主机启动模块可以包括主机安全模块的一部分。主机安全模块可以配置成：假定由主机端来处理口令输入，所以在这种情况下在启动时取消其口令对话屏幕。

[0057] 现在参考图 4，图 4 以流程图的形式示出了一种方法 300，用于在启动时对移动设备进行解锁。方法 300 在步骤 302 处开始，启动设备或对设备加电。在本实施例中，设备加电时主机被锁定，这意味着用户不能访问主机或客户应用程序。

[0058] 在启动时，主机运行可以包括一部分主机安全模块的主机启动模块，显示口令对话框，以请求用户口令输入，如步骤 304 处所示。设备在该状态下等待用户输入。在一个实施例中，设备可以具有取消选项，或可以在等待用户输入时超时，如步骤 306 所示。如果如此，那么在重新显示口令对话框以请求输入用户口令之前，在步骤 308 处，主机安全模块可以显示安全屏幕，并且在步骤 310 处等待击键。

[0059] 如果接收到口令，那么在步骤 312 处，设备对口令是否是有效口令做出评价。具体地，主机启动模块（或主机安全模块）通过经由平台抽象层提供的 API 来调用验证函数，并传递接收到的口令。返回用于指示输入口令是否有效的结果。如果口令无效，那么在步骤 314 处，主机启动模块确定是否应当允许用户再次尝试。如上所述，可能存在所允许的预定最大尝试次数。如果超过了最大次数，那么在步骤 316 处，可以实施特定的“删除设备”操

作。

[0060] 如果口令有效，那么在步骤318处对设备的主机端进行解锁。如上所述，在多个实施例中，客户端不会在启动时被锁定，这意味着仅需 要对主机端进行解锁。如果客户端在启动时被锁定，那么方法300包括其它步骤（未示出），在该步骤中主机启动模块（或主机安全模块）调用客户解锁API以指示客户安全模块对设备的客户端进行解锁。

[0061] 上文所述的本发明的实施例仅是示例性的。在不背离由所附权利要求限定的本申请的范围的前提下，本领域的技术人员可以对具体实施例进行改变、修改和变更。

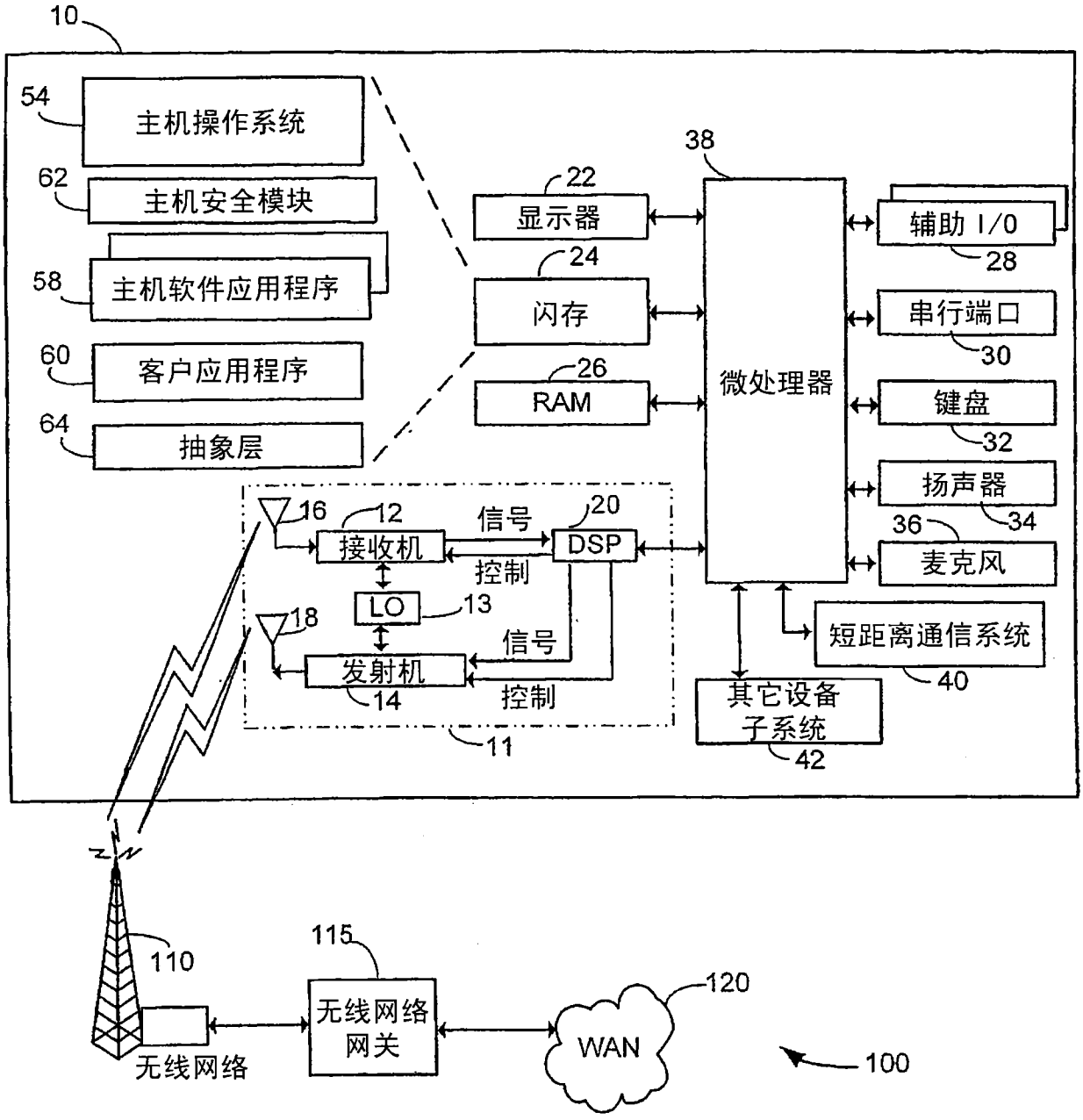

10
54
主机操作系统
62
主机安全模块
58
主机软件应用程序
60
客户应用程序
64
抽象层
22
显示器
24
闪存
26
RAM
38
微处理器
辅助 I/O
28
串行端口
30
键盘
32
扬声器
34
36
麦克风
短距离通信系统
40
其它设备
子系统
42
16
12
接收机
信号
20
DSP
控制
LO
13
18
信号
发射机
14
控制
11
110
115
无线网络
网关
120
WAN
100
无线网络

图 1

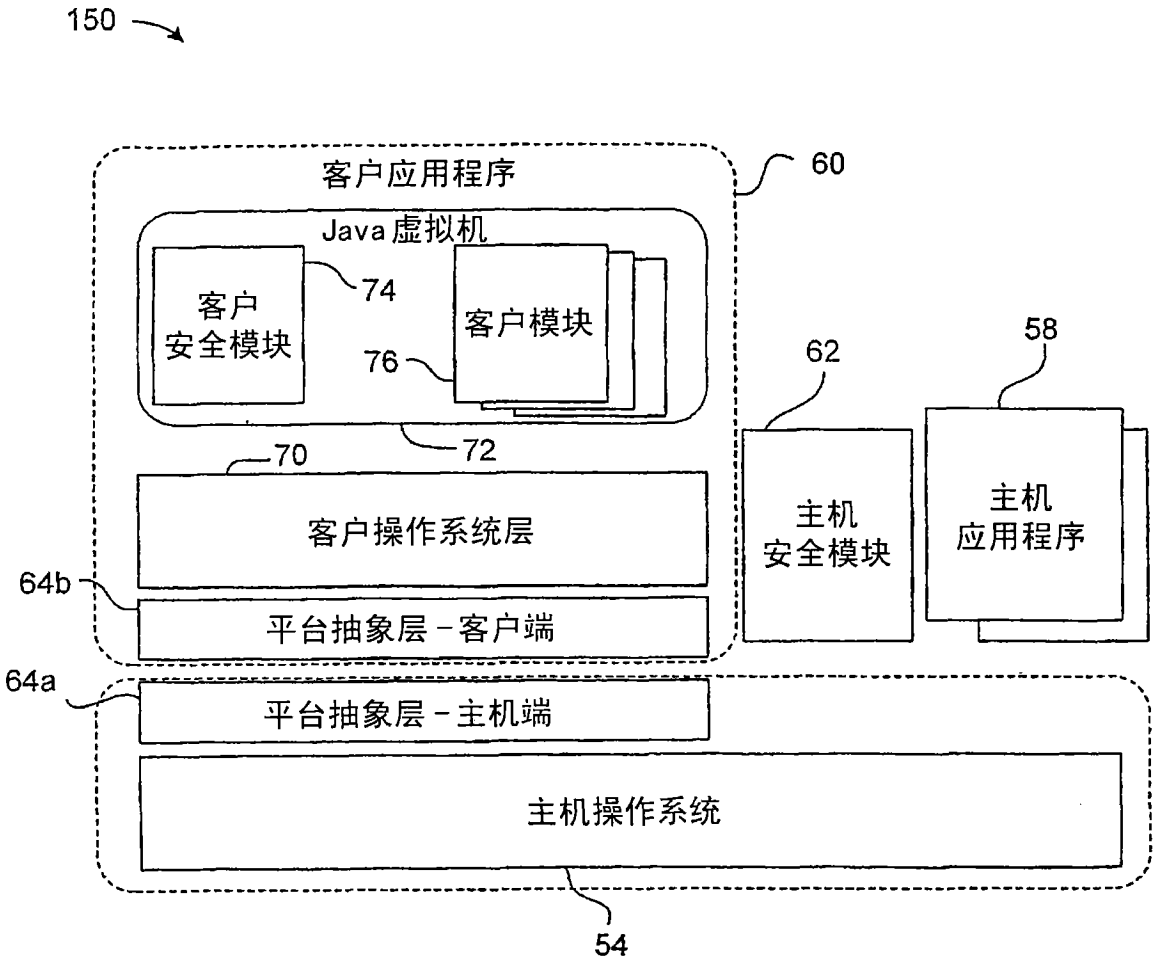

150
客户应用程序
60
Java 虚拟机
客户
安全模块
74
客户模块
76
72
70
客户操作系统层
64b
平台抽象层 - 客户端
64a
平台抽象层 - 主机端
主机操作系统
54
62
主机
安全模块
58
主机
应用程序

图 2

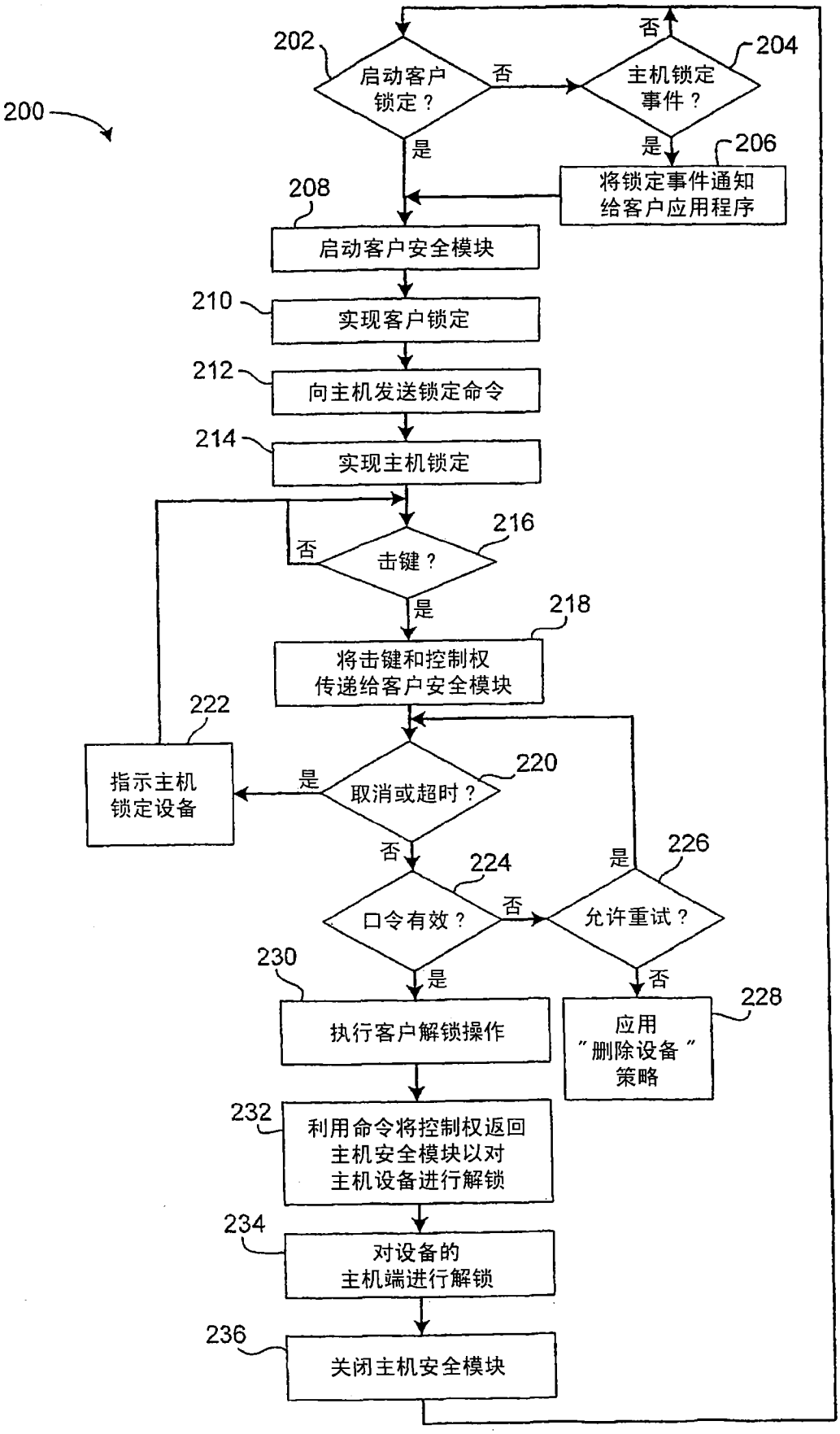

200
202
启动客户锁定？
否
是
204
主机锁定事件？
否
是
206
将锁定事件通知给客户应用程序
208
启动客户安全模块
210
实现客户锁定
212
向主机发送锁定命令
214
实现主机锁定
216
击键？
否
是
218
将击键和控制权传递给客户安全模块
220
取消或超时？
是
否
222
指示主机锁定设备
224
口令有效？
否
是
226
允许重试？
是
否
228
应用"删除设备"策略
230
执行客户解锁操作
232
利用命令将控制权返回主机安全模块以对主机设备进行解锁
234
对设备的主机端进行解锁
236
关闭主机安全模块

图 3

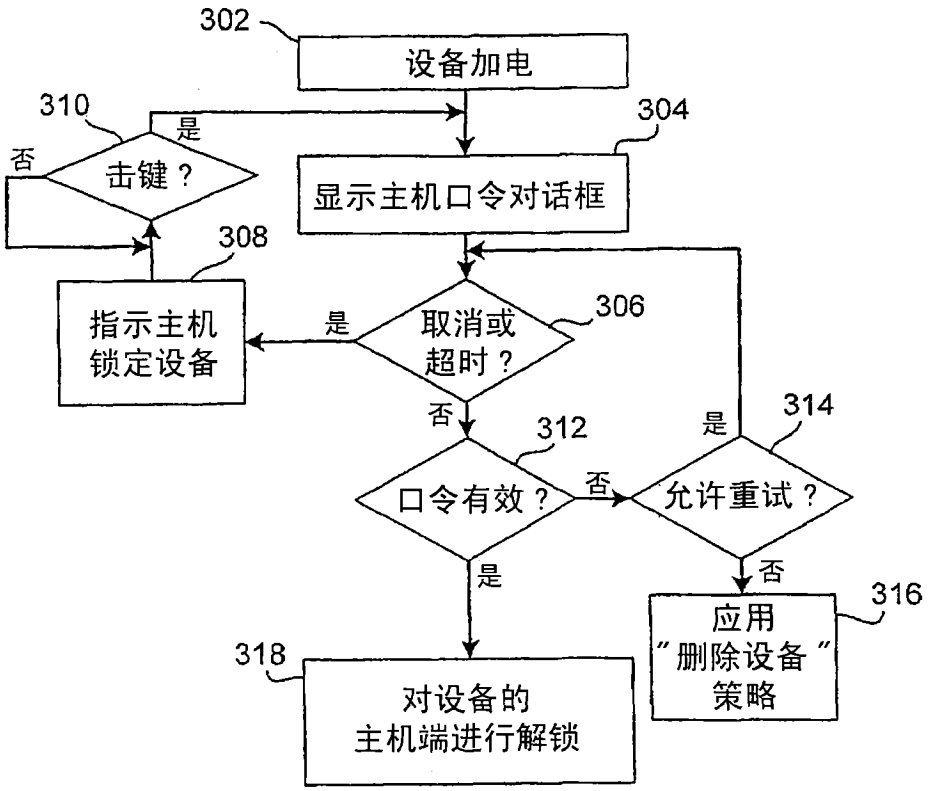

302
设备加电
304
显示主机口令对话框
306
取消或超时？
是
否
308
指示主机锁定设备
310
击键？
是
否
312
口令有效？
是
否
314
允许重试？
是
否
316
应用"删除设备"策略
318
对设备的主机端进行解锁

图 4