

(12) 发明专利申请

(10) 申请公布号 CN 101939750 A

(43) 申请公布日 2011.01.05

(21) 申请号 200980105007.7

(74) 专利代理机构 上海专利商标事务所有限公司 31100

(22) 申请日 2009.01.09

代理人 蔡悦 钱静芳

(30) 优先权数据

12/028, 297 2008.02.08 US

(51) Int. Cl.

G06F 21/00 (2006.01)

(85) PCT申请进入国家阶段日

G06F 21/22 (2006.01)

2010.08.09

(86) PCT申请的申请数据

PCT/US2009/030555 2009.01.09

(87) PCT申请的公布数据

W02009/099706 EN 2009.08.13

(71) 申请人 微软公司

地址 美国华盛顿州

(72) 发明人 F·K·贝萨尼亞 A·米肖

N·C·舍曼 H·山本 Y·塞斯

S·賴特

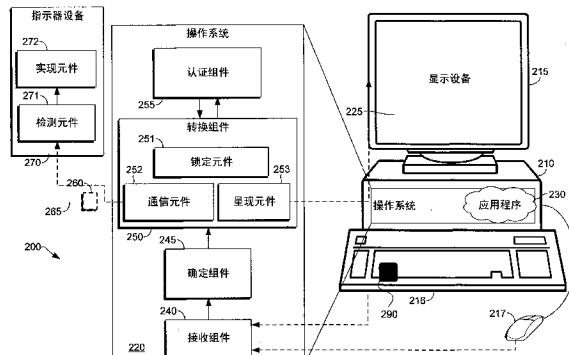
权利要求书 3 页 说明书 11 页 附图 5 页

(54) 发明名称

表示安全模式的用户指示器

(57) 摘要

提供了用于警告用户操作系统已进入安全模式的计算机可读介质、计算机化方法和计算机系统。最初，在驻留于默认模式的操作系统处接收输入。通常，该默认模式允许在操作系统上运行的应用程序访问输入。如果输入被标识为对执行受保护操作的调用，则操作系统从该默认模式转换到安全模式。通常，该安全模式限制应用程序截取输入。到安全模式的转换经由指示器设备自动传达给用户。通常，自动传达包括通过安全路径将来自操作系统的消息提供给指示器设备，该消息触发指示器设备生成用户可感知输出。因此，操作系统对指示器设备的操作施加独占控制。



1. 一种或多种其上包含计算机可执行指令的计算机可读介质,所述指令在被执行时执行一种用于警告用户操作系统已进入安全模式的方法,所述方法包括:

在驻留于默认模式的操作系统处接收(305)一个或多个输入,所述默认模式允许在所述操作系统上运行的应用程序访问所述一个或多个输入;

将所述一个或多个输入标识(310)为对执行受保护操作的调用;

从所述默认模式转换(315)到所述安全模式,所述安全模式限制在所述操作系统上运行的应用程序截取所述一个或多个输入;以及

自动将到所述安全模式的转换的指示传递(320)给指示器设备,其中所述指示器设备被配置成产生警告以便将到所述安全模式的转换通知给所述用户。

2. 如权利要求1所述的一种或多种计算机可读介质,其特征在于,在驻留于默认模式的操作系统处接收一个或多个输入包括检测执行所述受保护操作的用户发起指令。

3. 如权利要求2所述的一种或多种计算机可读介质,其特征在于,所述用户发起指令通过致动物理按钮来发起。

4. 如权利要求1所述的一种或多种计算机可读介质,其特征在于,所述指示器设备由所述操作系统独占控制。

5. 如权利要求1所述的一种或多种计算机可读介质,其特征在于,还包括:

在驻留于所述安全模式的操作系统处接收一种或多种形式的登录凭证;

认证所述一种或多种形式的登录凭证;以及

从所述安全模式转换到所述默认模式。

6. 如权利要求5所述的一种或多种计算机可读介质,其特征在于,还包括与从所述安全模式转换到所述默认模式相关联地,自动将到所述默认模式的转换的指示传递给所述指示器设备,其中所述指示器设备被配置成驰豫所述警告,由此将到所述默认模式的转换通知给所述用户。

7. 如权利要求1所述的一种或多种计算机可读介质,其特征在于,限制在所述操作系统上运行的应用程序截取所述一个或多个输入包括:

建立获取对所述一个或多个输入的访问权的安全等级;以及

询问在所述操作系统上运行的应用程序以标识所述应用程序中满足所述安全等级的安全程序。

8. 如权利要求1所述的一种或多种计算机可读介质,其特征在于,自动将到所述安全模式的转换传递给所述指示器设备包括向所述指示器设备传递消息,其中所述消息包括具有根据在安装所述指示器设备时提取的属性来配置的使用定义的协议。

9. 如权利要求1所述的一种或多种计算机可读介质,其特征在于,将所述一个或多个输入标识为对执行受保护操作的调用包括检测来自外围设备的安全警告序列(SAS)事件。

10. 一种用于提供操作系统的环境状态的用户可感知指示的计算机化方法,所述方法包括:

跟踪(305)由所述操作系统主存的应用程序的操作,其中所述操作系统的环境状态是默认模式;

确定(310)所述应用程序的受跟踪操作是否触发所述环境状态从所述默认模式到安全模式的转换,其中在所述安全模式中,所述应用程序被禁止读取由用户发起的对所述操

作系统的输入；

如果触发了所述环境状态的转换，则通过向由所述操作系统独占控制的指示器设备传递信号来向所述用户警告（355）所述转换，其中所述指示器设备被配置成通过提供所述用户可感知指示来警告所述用户；以及

如果受跟踪操作未能触发所述环境状态的转换，则将所述操作系统维持（360）于所述默认模式，由此免除向所述指示器设备传递所述信号。

11. 如权利要求 10 所述的方法，其特征在于，所述指示器设备被配置成在所述操作系统处于所述默认模式时驻留在无源状态中，并且调整到通过提供所述用户可感知指示来表示所述操作系统处于所述安全模式的通知状态。

12. 如权利要求 10 所述的方法，其特征在于，还包括在接收到满足所述应用程序的认证过程的安全凭证后将所述环境状态转换到所述默认模式。

13. 如权利要求 12 所述的方法，其特征在于，还包括在将所述环境状态转换到所述默认模式后，将驻留于所述通知状态的指示器设备调整到表示所述操作系统处于所述默认模式的无源状态。

14. 一种用于根据用户发起输入来独占控制位于至少一个人类接口设备（HID）中的指示器设备的计算机系统，所述系统包括：

具有驻留在其上的操作系统（220）的计算设备（210），其中所述操作系统被配置成确定所述用户发起输入是否调用所述操作系统的环境状态的改变，其中所述环境状态的改变包括默认模式和安全模式之间的转换；以及

第一 HID（290），所述第一 HID 具有设置在其上的由所述操作系统独占控制的第一指示器设备（270），其中所述第一指示器设备被配置成接收所述用户发起输入调用所述操作系统的环境状态的改变的指示并且生成用户可感知输出。

15. 如权利要求 14 所述的系统，其特征在于，所述第一指示器设备包括发光二极管（LED）、显示器指示器、发光设备、扬声器或触觉反馈设备中的至少一个。

16. 如权利要求 14 所述的系统，其特征在于，所述第一指示器设备还被配置成：

通过受保护路径从所述操作系统接收消息；

解释所述消息以确定所述指示是否调用所述环境状态的改变；以及

基于对所述消息的解释来控制所述用户可感知输出的生成。

17. 如权利要求 16 所述的系统，其特征在于，还包括第二 HID，所述第二 HID 具有由所述操作系统独占控制的第二指示器设备，其中所述第二指示器设备被配置成在接收到所述用户发起输入调用所述操作系统的环境状态的改变的指示后生成用户可感知输出，以使得由所述第二指示器设备生成的用户可感知输出与由所述第一指示器设备生成的用户可感知输出相对应。

18. 如权利要求 14 所述的系统，其特征在于，所述第一 HID 被配置成将所述用户发起输入提供给所述操作系统。

19. 如权利要求 14 所述的系统，其特征在于，调用所述操作系统的环境状态的改变包括在所述操作系统的一个或多个模式之间转换，其中所述第一指示器设备还被配置成生成各自对应于所述一个或多个模式中的相应模式的一个或多个不同的用户可感知输出，并且其中所述一个或多个模式包括所述安全模式。

20. 如权利要求 14 所述的系统，其特征在于，还包括可操作地耦合到所述操作系统的显示设备，其中所述显示设备包括用户界面 (UI) 显示，所述 UI 显示被配置成在接收到所述用户发起输入调用所述操作系统的环境状态从所述默认模式到所述安全模式的改变的指示后呈现安全登录屏幕。

表示安全模式的用户指示器

[0001] 背景

[0002] 目前,操作系统提供帮助向用户提供对安全桌面的访问权的各种实用程序。一旦处在安全桌面中,用户就被提示输入特权信息,诸如登录标识、口令或其他形式的认证(例如,指纹、虹膜扫描、脸部/语音识别信息等)。如果通过认证,则操作系统利用该特权信息来获取对安全网站的访问权,授予管理权限(例如,允许用户安装第三方软件),登录到计算会话,以及执行通常对不知道特权信息的用户禁止的其他操作。通常,在操作系统上运行的恶意应用程序试图在用户的特权信息在安全桌面处输入时记录该特权信息。在记录该特权信息后,这些应用程序可以获取对受保护信息的未授权访问权或权限。通常,应用程序通过呈现看上去与在安全桌面中呈现的显示区域相似的显示区域,由此提示毫无戒备的用户提供特权信息来执行对特权信息的记录或“探测”。因为这些应用程序可显示合法显示区域的许多样式的表示,所以用户不太可能将伪造的安全桌面与有效安全桌面区分开来。因此,无法检测出伪造的安全桌面可导致用户将特权信息让与赞助该应用程序的实体,该实体可出于欺诈目的(例如,身份盗取、访问机密文件等)利用该信息。

[0003] 概述

[0004] 提供本概述是为了以简化的形式介绍将在以下详细描述中进一步描述的一些概念。本概述不旨在标识所要求保护的主题的关键特征或必要特征,也不旨在用于帮助确定所要求保护的主题的范围。

[0005] 本发明的各实施例提供用于警告用户操作系统已进入安全模式的计算机化方法、计算机系统和其上包含用于警告用户操作系统已进入安全模式的计算机可执行指令的计算机可读介质。具体而言,与操作系统的环境状态从默认模式到安全模式的转换相关联地,该转换的指示被自动传递给指示器设备。因此,指示器设备生成通知用户计算设备处于安全模式的用户可感知输出。由此,用户能够在没有未获授权应用程序盗取信息的威胁的情况下快速识别输入特权信息是安全的。

[0006] 因此,在一方面,本发明的各实施例提供其上包含计算机可执行指令的一种或多种计算机可读介质,这些指令在被执行时执行一种用于警告用户操作系统已进入安全模式的方法。一般而言,操作系统负责向用户提供已进入安全模式的警告,而应用程序无法复制该安全模式。最初,在驻留于默认模式的操作系统处接收输入。通常,该默认模式允许在操作系统上运行的应用程序访问输入。这些输入被标识为对执行受保护操作的调用。在将输入标识为对执行受保护操作的调用后,操作系统从默认模式转换到安全模式。通常,该安全模式限制在操作系统上运行的应用程序截取输入。到安全模式的转换的指示被自动传递给指示器设备。一般而言,指示器设备被配置成产生警告以便将到安全模式的转换通知给用户。当操作系统驻留于安全模式时,可以在操作系统处接收登录凭证。在认证登录凭证后,操作系统可从安全模式转换到默认模式。到默认模式的转换的指示被自动传递给指示器设备。一般而言,指示器设备被配置成驰豫警告,由此将到默认模式的转换通知给用户。

[0007] 在另一方面,提供了一种用于根据用户发起输入来控制位于至少一个人类接口设备(HID)中的指示器设备的计算机化方法。最初,该系统包括计算设备、第一HID和显示设

备。计算设备可具有驻留在其上的操作系统。通常,该操作系统被配置成确定用户发起输入是否调用操作系统的环境状态的改变。在一个实施例中,环境状态的改变包括默认模式与安全模式之间的转换。第一 HID 可具有设置在其上的由操作系统独占控制的第一指示器设备。在各实施例中,第一指示器设备可以是发光二极管(LED)、显示器指示器、发光设备、扬声器、盲人用点字法反馈或其他可达性输入设备,或触觉反馈设备。通常,该第一指示器设备可接收用户发起输入调用操作系统的环境状态的改变的指示。在接收到该指示后,第一指示设备可生成用户可感知输出。具体而言,生成用户可感知输出包括通过受保护路径从操作系统接收消息;解释该消息以确定该指示是否调用环境状态的改变;以及基于对该消息的解释来控制用户可感知输出的生成。显示设备可操作地耦合到操作系统。通常,显示设备包括用户界面(UI)显示,该显示在接收到用户发起输入调用操作系统的环境状态从默认模式到安全模式的改变的指示后呈现安全登录屏幕。在各实施例中,在操作系统上运行的应用程序可具有在 UI 显示处复制该安全登录屏幕的能力;然而,该应用程序无法指示第一指示设备生成用户可感知输出。因此,该用户可感知输出准确地警告用户操作系统的环境状态被设为安全模式。

[0008] 在又一方面,本发明的各实施例涉及一种用于提供操作系统的环境状态的用户可感知指示的计算机化方法。一般而言,该方法包括以下步骤:跟踪由操作系统主存的应用程序的操作;以及确定受跟踪的应用程序操作是否触发环境状态从默认模式到安全模式的转换。如果触发环境状态的转换,则通过向由操作系统独占控制的指示器设备传递信号来向用户警告该转换。通常,指示器设备被配置成通过提供用户可感知指示来警告用户。然而,如果受跟踪操作未能触发环境状态的转换,则将操作系统维持于默认模式,由此免除向指示器设备传递信号。

[0009] 附图简述

[0010] 下面将参考附图详细描述本发明,其中:

[0011] 图 1 是适用于实现本发明的各实施例的示例性计算环境的框图;

[0012] 图 2 是适用于实现本发明的各实施例的示例性系统体系结构的示意图;

[0013] 图 3 是示出了根据本发明一实施例的用于警告用户操作系统已进入安全模式的总体方法的流程图;

[0014] 图 4 是示出根据本发明的各实施例的用于在无源状态和通知状态之间转换指示器设备的各阶段的渐进式屏幕显示;以及

[0015] 图 5 是根据本发明一实施例的提供安全登录屏幕的示例性 UI 显示的图示。

[0016] 详细描述

[0017] 此处用具体细节描述本发明以满足法定要求。然而,该描述本身并非旨在限制本专利的范围。相反,发明人设想所要求保护的主题还可结合其他当前或未来技术按照其他方式来具体化,以包括不同的步骤或类似于本文中所描述的步骤的步骤组合。此外,尽管术语“步骤”和 / 或“框”可在此处用于指示所采用的不同元素或方法,但除非而且仅当明确描述了各个步骤的顺序时,该术语不应被解释为意味着此处公开的各个步骤之中或之间的任何特定顺序。

[0018] 本发明的各实施例涉及用于警告用户操作系统已进入安全模式的计算机可读介质、计算机化方法和计算机系统。最初,在驻留于默认模式的操作系统处接收输入。通常,

该默认模式允许在操作系统上运行的应用程序访问输入。如果输入被标识为对执行受保护操作的调用，则操作系统从该默认模式转换到安全模式。通常，该安全模式限制应用程序截取输入。到安全模式的转换经由指示器设备自动传达给用户。通常，自动传达包括通过安全路径将来自操作系统的消息提供给指示器设备，该消息触发指示器设备生成用户可感知的输出。换言之，操作系统对指示器设备的操作施加独占控制。因此，向用户保证操作系统当前正排除恶意应用程序盗取可在处于安全模式时输入的特权信息。

[0019] 一般而言，本发明的各实施例涉及向用户警告操作系统的环境状态的改变。在一示例性实施例中，自动向指示器设备提供信号以通知用户操作系统的环境状态已从默认模式转换到安全模式。一般而言，默认模式允许主存（例如，同时运行）在操作系统上的应用程序读取用户提供给操作系统的输入（例如，经由输入设备，如下文中更全面地讨论的）。在一种情况下，应用程序在安装时在操作系统中建立“挂钩”（hook）。这些挂钩允许应用程序监听键击，或提供给操作系统的任何其他用户发起输入。因为应用程序可在默认模式中监听键击，所以应用程序可存储键击，仿真键击，在键击之间注入附加输入，或修改键击。通常，这些与键击或任何其他用户发起输入相关的操作由应用程序用来执行普通处理功能。然而，当处于默认模式时，无意地安装在操作系统上的恶意应用程序可建立挂钩并获取类似的对键击或任何其他用户发起输入的访问权。另外，当处于默认模式时，恶意应用程序可在 UI 显示处呈现有效安全登录屏幕的表示以提示用户在其中提供特权信息。

[0020] 为了安全地提供特权信息，用户或应用程序应当将操作系统的环境状态从默认模式改为受保护桌面模式。在一种情况下，在将用户发起输入标识为对执行受保护功能的调用时影响从默认模式到受保护桌面模式的转换。如此处所使用的，短语“对执行受保护功能的调用”不旨在是限制性的，而是涵盖调用操作系统来向用户请求特权信息的所有输入。如上所述，特权信息至少包括个人信息、口令、登录标识、社会保险号、银行账号、信用卡号、电子邮件地址、用户凭证等。在一种情况下，调用操作系统向用户请求特权信息的输入是在 web 浏览器应用程序处登录到银行账户中的请求。这种情况将在以下参考图 4 更全面地描述。在另一种情况下，调用操作系统向用户请求特权信息的输入是打开需要管理权限来访问的应用程序（例如，基于许可证发放）或文件夹（例如，文件系统格式化、受保护系统配置等）的命令。具体而言，具有与其绑定的管理权限的应用程序可包括用户访问控制（UAC）条件。在操作中，在接收到操纵这种类型的应用程序的请求后，由该应用程序呈现请求满足 UAC 条件的信息的安全登录屏幕。通常，这些安全登录屏幕简单地弹出在普通计算的上下文中呈现的窗口。因此，恶意应用程序很容易复制这些请求满足访问控制 UAC 条件的信息的安全登录屏幕。另外，在一示例性实施例中，与将操作系统的环境状态从默认模式改为受保护桌面模式相关联地，向指示器设备发送信号以警告用户该受保护桌面模式已建立，并且提交特权信息是安全的。

[0021] 在各实施例中，该安全模式限制主存在操作系统上的应用程序监听或截取用户发起输入。一般而言，安全模式是由操作系统提供的阻塞应用程序监听键击或其他输入的保护性外壳。在一种情况下，阻塞通过使已由安装在操作系统上的应用程序建立的挂钩“脱钩”来执行。因此，由应用程序用来访问用户发起输入的链路被切断。即，在安全模式中，应用程序被禁止监听诸如特权信息等由用户提供的输入。偶尔，应用程序可获取对在处于安全模式时提供的输入的访问权。然而，获取访问权通常涉及操作系统建立具有非常高阈值

的安全等级并询问主存在该操作系统上的应用程序以标识满足所建立安全等级的安全程序。在另一实施例中，从存储在操作系统上的访问控制列表中标识安全程序。可向这些安全程序提供对出于各种原因的用户发起输入的访问权。但在安全模式中，操作系统能够确定哪些应用程序被认为是安全程序，由此过滤掉恶意程序。

[0022] 一旦处于安全模式，操作系统就基本上锁定呈现在显示设备上的 UI 显示。为了解锁该 UI 显示，应向呈现在该 UI 显示上的输入区域（例如，如参考图 5 更全面地讨论的安全登录屏幕）提供若干预期输入之一。在一种情况下，预期输入包括满足由操作系统执行的认证过程的正确登录凭证、应用程序需要的登录凭证，或其组合。在接受用户提供的登录凭证后，操作系统的环境状态授予用户对受保护应用程序或文件的访问，并回复到默认状态。如果在预定义数量的尝试后用户提供的登录凭证无法满足认证过程，则操作系统将退出安全模式而不授予用户对受保护应用程序或文件的访问权。在另一种情况下，预期输入可以是表示用户不再打算提供特权信息的退出命令。另外，在一示例性实施例中，与将操作系统的环境状态从受保护桌面模式改为默认模式相关联地，向指示器设备发送信号以警告用户默认模式已建立，并且提交特权信息是不安全的。

[0023] 尽管已描述了操作系统的环境状态的两种不同模式，但本领域的普通技术人员应理解和明白，可以使用其他模式（例如，休眠模式、低电量模式、高处理模式等）来触发到 HID 的信号，并且本发明不限于所示和所述模式。由此，本发明的各实施例考虑映射到特定信号的各种模式，这些信号在被传递给 HID 时调用 HID 生成指示各种模式中的哪一种模式当前是活动的单独的、或共同的用户感知输出。此外，本发明的各实施例考虑应用由操作系统独占控制的指示器设备的结构来在操作系统检测到对由操作系统、应用程序或其他软件执行的任何功能的改变时在 HID 处提供警告。

[0024] 一般而言，指示器设备被设置在输入设备或可操作地耦合到操作系统的任何其他设备中或其表面上。在一示例性实施例中，指示器设备是位于 HID 处的 LED。在操作中，LED 将经由 HID 从操作系统接收指示操作系统的环境状态是安全模式的信号。该信号用于直接或间接控制 LED 的功能。在特定情况下，控制 LED 的功能包括指示 LED 生成用户可感知输出（例如，发光）或停止生成用户可感知输出。通常，信号由 HID 预处理。

[0025] 如此处所使用的，首字母缩写词“HID”不旨在是限制性的并且可涵盖与用户交互的任何类型的计算机设备。交互可包括从用户处接收输入，向用户传递输出或其组合。仅仅作为示例，HID 可包括以下设备中的一个或多个：键盘（例如，膝上型计算机的内部键盘、台式计算机的外部键盘）、鼠标、跟踪球、操纵杆、数字图像记录器 / 播放器、盲人用点字法指示器、图形输入板、游戏手柄、计算机、LCD 显示器、以及监视器。在一个实施例中，HID 向操作系统提供包含帮助操作系统为该特定 HID 格式化信号或消息的数据的自描述包。因此，操作系统可以按所识别 HID 的专用格式来格式化到该 HID 的信号，由此提升 HID 和 LED 或成对 LED 的功能。在另一实施例中，操作系统可操作地耦合到在向 HID 发送信号之前处理信号的驱动程序。在一种情况下，处理包括生成供传递给 HID 的消息，其中该消息包括具有根据 HID 或指示器设备的安装属性来配置的使用定义的协议。如上所述，HID 的安装属性可作为自描述包中的数据传递给操作系统。在另一种情况下，处理包括将安全和认证值构建到信号中以使得操作系统对 HID 或指示器设备施加唯一控制。

[0026] 在又一种情况下，处理包括用定义特定安全等级的协议（例如，USB 协议）来传递

信号,由此在 HID 和操作系统之间建立安全路径。因此,在这种情况下,执行操作系统和 HID 之间的允许该操作系统对 HID 施加独占控制的握手操作。作为示例,独占控制包括其中只有操作系统可以操纵 HID,操作系统和授权源能够操纵 HID,或者各种源能够操纵 HID 但操作系统在提供信号时获得最高优先级的情况。因此,由操作系统发送的通信可以从基本电子输出变化到格式化信号,到附加优先级的加密消息。在一实施例中,消息的格式化取决于 HID 和 / 或指示器设备的配置,尤其是在 HID 设置有用于解释消息并实现嵌入在其中的指令的逻辑的情况下。

[0027] 在一示例性实施例中,处理信号和传递信号的步骤在识别出操作系统的环境状态是安全模式时自动执行。然而,这些步骤可以独立地、串行地或并行地执行。另外,这些步骤可以在预定义延迟后执行。在其他实施例中,上述步骤可以在识别出操作系统的环境状态、另一模式或默认模式时执行。因此,本发明的各实施例考虑控制 HID 以便在转换到各种规定模式(例如,用户感兴趣的模式)之一时生成用户可感知输出,其中该用户可感知输出对于各种模式中的每一种可以分别不同。

[0028] 在描述了本发明的各实施例的概览以及其中表征的一些窗口状态之后,下面将描述适于实现本发明的示例性操作环境。

[0029] 一般参考附图,并首先具体参考图 1,示出了用于实现本发明的各实施例的示例性操作环境,并将其概括地指定为计算设备 100。计算设备 100 只是合适的计算环境的一个示例,并且不旨在对本发明的使用范围或功能提出任何限制。也不应该将计算设备 100 解释为对所示出的任一组件或其组合有任何依赖性或要求。

[0030] 可以在计算机代码或机器可使用指令(包括由计算机或诸如个人数据助理或其他手持式设备之类的其他机器执行的诸如程序组件之类的计算机可执行指令)的一般上下文中来描述。一般而言,包括例程、程序、对象、组件、数据结构等的程序组件指的是执行特定任务或实现特定提取数据类型的代码。本发明的各实施例可以在各种系统配置中实施,这些系统配置包括手持式设备、消费电子产品、通用计算机、专用计算设备等等。本发明也可以在其中任务由通过通信网络链接的远程处理设备执行的分布式计算环境中实施。

[0031] 继续参考图 1,计算设备 100 包括直接或间接耦合以下设备的总线 110 :存储器 112、一个或多个处理器 114、一个或多个呈现组件 116、输入 / 输出(I/O)端口 118、I/O 组件 120、和说明性电源 122。总线 110 可以是一条或多条总线(诸如地址总线、数据总线、或其组合)。虽然为了清楚起见利用线条示出了图 1 的各框,但是实际上,各组件的轮廓并不是那样清楚,并且比喻性地来说,线条更精确地将是灰色的和模糊的。例如,可以将诸如显示设备等的呈现组件认为是 I/O 组件。而且,处理器具有存储器。发明人关于此点认识到这是本领域的特性,并重申,图 1 的图示只是例示可以结合本发明的一个或多个实施例来使用的示例性计算设备。诸如“工作站”、“服务器”、“膝上型计算机”、“手持式设备”等分类之间没有区别,它们全部都被认为是在图 1 的范围之内的并且被称为“计算机”或“计算设备”。

[0032] 计算设备 100 通常包括各种计算机可读介质。作为示例而非限制,计算机可读介质可以包括随机存取存储器(RAM);只读存储器(ROM);电可擦可编程序只读存储器(EEPROM);闪存或其他存储技术;CDROM、数字多功能盘(DVD)或其他光学或全息介质;磁带盒、磁带、磁盘存储或其他磁存储设备,载波或可以用来编码所需要的信息并可以被计算设

备 100 访问的任何其他介质。

[0033] 存储器 112 包括易失性和 / 或非易失性存储器形式的计算机存储介质。存储器可以是可移动的,不可移动的,或两者的组合。示例性硬件设备包括固态存储器、硬盘驱动器、光盘驱动器等。计算设备 100 包括从诸如存储器 112 或 I/O 组件 120 等各种实体读取数据的一个或多个处理器。呈现组件 116 向用户或其他设备呈现数据指示。示例性呈现组件包括显示设备、扬声器、打印组件、振动组件等等。I/O 端口 118 允许计算设备 100 逻辑上耦合至包括 I/O 组件 120 的其他设备,其中某些设备可以是内置的。说明性组件包括话筒、操纵杆、游戏手柄、圆盘式卫星天线、扫描仪、无线设备等等。

[0034] 现在转向图 2,示出了根据本发明的一实施例的适用于实现本发明的各实施例的示例性系统体系结构 200 的示意图。本领域技术人员将了解和明白,图 2 所示出的示例性系统体系结构 200 只是一个合适的计算环境的示例,而非旨在对本发明的使用范围或功能提出任何限制。该示例性系统体系结构 200 也不应被解释成对于此处所示出的任一组件或其组合有任何依赖或要求。此外,操作系统 220 内的支持示例性系统体系结构 200 的逻辑也可以作为独立的产品、作为软件程序包的一部分、或其任何组合来提供。

[0035] 示例性系统体系结构 200 包括计算设备 210,该计算设备用于通过在被独占控制的指示器设备处提供警告来警告用户操作系统的环境状态已发生改变。计算设备 210 可以采取各种计算设备的形式。仅仅作为示例,计算设备 210 可以是个人计算设备(例如,图 1 的计算设备 100)、手持式设备(例如,个人数字助理)、膝上型计算机、消费电子产品、各种服务器等等。另外,计算设备可以包括两个或更多个被配置成在它们之间共享信息的电子设备。

[0036] 用于控制指示器设备向用户警告安全模式的计算设备的各实施例现在将参考各附图来描述。附图及相关联的描述是为了示出本发明的各实施例而提供的,而不是为了限制本发明的范围。本说明书中对“实施例”的引用旨在指示结合该实施例描述的特定特征、结构或特性被包括在本发明的至少一个实施例中。此外,出现在说明书中各个地方的短语“在一实施例中”不必全都指的是同一实施例。在全部附图中,重用附图标记来指示所引用的元素之间的对应关系。

[0037] 在各实施例中,计算设备 210 包括显示设备 215、输入设备 216、217 和 219、以及其上安装操作系统 220 的硬件。计算设备 210 被配置成在显示设备 215 上呈现 UI 显示 225。可操作地耦合到计算设备 210 的显示设备 215 可被配置成能够向诸如监视器、电子显示面板、触摸屏等等之类的用户呈现信息的任何呈现组件。在一个示例性实施例中,UI 显示 225 被配置成呈现有效安全登录屏幕(未示出)和 / 或呈现如应用程序 230 所需的内容,其中显示区域(参见图 5)通常用于发布应用程序 230 所生成的内容。在另一示例性实施例中,UI 显示 225 能够产生如由无意地主存在操作系统 220 上的恶意应用程序提供的伪造的安全登录屏幕。

[0038] 提供输入设备 216、217 和 290 以提供影响操作系统 210 的环境状态是默认模式还是安全模式等的输入。说明性设备包括键盘(如附图标记 216 所示)、鼠标(如附图标记 217 所示)、操纵杆、登录按钮(如附图标记 290 所示)、话筒、图 1 的 I/O 组件 120、或能够接收用户输入并将该输入的指示传送到计算设备 210 的任何其他组件。仅仅作为示例,输入设备 216 和 217 控制通常在 UI 显示 225 处呈现的登录凭证或其他特权信息的输入。在另一

示例中,输入设备 216 提供执行受保护操作的用户发起指令。具体而言,可以提示输入设备 216 提供用于在接收到用户输入时执行受保护操作(例如,登录到受保护网站,如上所述)的指令。用户输入可以是热键、键击序列、登录键组合(例如,Ctrl+Alt+Delete)、或向操作系统 220 指示已发起对该操作系统的环境状态的改变的任何其他安全警告序列(SAS)。

[0039] 另外,输入设备 290 可以是专用于登录到计算会话中或在操作系统 220 内触发安全事件的物理按钮。在一个实施例中,物理按钮是只对操作系统 220 触发无法解释或以其他方式篡改的安全信号的物理登录按钮。在接收到安全信号后,操作系统 220 可执行各种功能,包括发起登录序列。通常,安全信号被直接传递给操作系统 220 以使其对于其他组件和 / 或应用程序是透明的。仅仅作为示例,用户发起的对物理登录按钮的致动将生成通常与 Ctrl-Alt-Delete 命令类似的命令。在另一实施例中,物理按钮控制计算设备 210 的通电功能和 / 或调用初始安全登录屏幕的登录功能。而且,物理按钮可被重新编程为提供指示操作系统 220 执行各种功能或安全事件的用户发起输入。在一种情况下,对物理按钮进行重新编程包括将该按钮设置成请求操作系统 220 执行允许后续用户登录到操作系统 220 上的当前会话中的“快速用户切换”。尽管上文中描述了各种功能,但应理解和明白,输入设备 290 的物理按钮实施例可生成发送到操作系统的激活相关领域内已知的任何事件或计算会话的安全信号。此外,尽管被描绘为设置在输入设备 216 上的按钮,但输入设备 290 可被配置为接受单个用户致动作为完整输入的任何设备,并且可被配置成驻留在电子设备(例如,显示设备 215、计算设备 210、输入设备 217、膝上型计算机等)上。因此,输入设备 290 通过用单个移动或点击来触发安全模式来提供对安全操作系统 220 的快速且方便的访问。

[0040] 操作系统(OS)220 一般是指管理计算设备 210 的资源共享并向程序员提供用于访问这些资源的界面的软件。在操作中,操作系统 220 解释系统数据,并检测用户输入(例如,通过输入设备 216、217 和 290),并通过执行诸如以下进程来响应:在驻留于默认模式的操作系统 220 处理一个或多个输入(例如,利用接收组件 240);将该一个或多个输入标识为对执行受保护操作的调用(例如,利用确定组件 245);在默认模式、安全模式、以及任何其他可用模式之间转换(例如,利用转换组件 250);以及自动将到安全模式的转换的指示传递给指示器设备 270(利用通信元件 252),其中指示器设备 270 可通过其中的实现元件 272 来产生警告。在各实施例中,操作系统用于执行以下逻辑步骤:在驻留于安全模式的操作系统 220 处接收一个或多个登录凭证(例如,利用接收组件 240);认证该一个或多个登录凭证(例如,利用认证组件 255);从安全模式转换到默认模式(例如,利用转换组件 250);以及自动将到默认模式的转换的指示传递给指示器设备 270(例如,利用通信元件 252),其中指示器设备 270 可发出警报,由此将到默认模式的转换通知给用户。

[0041] 在一示例性实施例中,操作系统 220 包括接收组件 240、确定组件 245、转换组件 250、和认证组件 255。另外,操作系统 220 可主存应用程序 230、或在其上同时运行的多个应用程序。而且,操作系统 220 可经由安全路径 265 操作地耦合到指示器设备 270,并且耦合到显示设备 215,由此影响在 UI 显示 225 处呈现的内容。

[0042] 操作系统组件 220 的此操作系统结构只是可以在计算设备 210 上运行的合适结构的一个示例,而非旨在对本发明的使用范围或功能提出任何限制。所示操作系统 220 也不应被解释成对于所示组件 240、245、250 和 255 中的任一组件或其组合有任何依赖或要

求。在某些实施例中，组件 240、245、250 和 255 中的一个或多个可以作为独立应用程序来实现。在其他实施例中，组件 240、245、250 和 255 中的一个或多个可以直接集成到计算设备 210 的显示设备 215、应用程序 230、或其组合中。仅仅作为示例，转换组件 220 中的呈现组件 253 可以与显示设备 215 相关联地主存。本领域技术人员将理解，图 2 中所示出的组件 240、245、250 和 255 在本质上和数量上是示例性的，且不应该被解释为是限制性的。

[0043] 在本发明的各实施例的范围内，可以使用任意数量的组件以实现所需功能。虽然为了清楚起见利用线条示出了图 2 的各组件，但是实际上，各组件的轮廓并不是那样清楚，并且比喻性地来说，线条更精确地将是灰色的和模糊的。此外，虽然图 2 的某些组件和设备被描述成各单独的框，但是该描绘在本质上和数量上是示例性的，不应该解释为限制（例如，虽然只示出了一个显示设备 215，但是，可以有更多的显示设备可操作地耦合到计算设备 210，从而协作地运转以呈现 UI 显示 225）。

[0044] 在各实施例中，接收组件 240 被配置成接收并处理来自输入设备 216、217 和 290 的输入和 / 或来自输入设备 217 的受跟踪移动。应理解和明白，来自各种其他输入设备（例如，触摸屏面板）的其他输入可由接收组件 240 接收和解释；因此，本发明的范围不限于此处所描述的输入和输入设备。另外，输入可以在不具有用户交互或具有有限用户交互的情况下从应用程序（例如，应用程序 230）接收。如上文中更全面地讨论的，由应用程序提供的输入可例如根据该应用程序的 UAC 条件来触发操作系统 220 的环境状态的改变。因此，接收组件 240 能够接收并解释源自用户发起输入事件、由应用程序创建的内部自动化输入、或可操作地耦合到操作系统的任何其他设备的各种输入。

[0045] 在一示例性实施例中，这些输入可包括对执行受保护操作的调用。对输入中是否存在该调用的确定由确定组件 245 来进行。最初，确定组件 245 从接收组件 240 接收经处理的输入。分析该输入以标识调用是否存在于输入中。例如，确定组件 245 确定诸如应用程序 230 的受跟踪操作等输入是否将触发操作系统 220 的环境状态的转换。如果是，则确定组件 245 从输入中提取调用并将该调用传递给转换组件 250。如果否，则确定组件 245 尝试标识输入的内容并将这些内容分发到操作系统 220 中的适当位置。例如，如果输入包括关于安全凭证的信息（例如，经扫描的指纹文件），则确定组件 245 将该输入传递给认证组件 255。

[0046] 一般而言，转换组件 250 接收由接收组件 240 从输入中提取的调用并将该调用中的指令与操作系统 220 的当前环境状态进行比较。即，如果调用中的指令将操作系统 220 定向到不是当前模式的模式，则触发转换过程。否则，维持当前模式。仅仅作为示例，如果当前环境状态是默认模式并且调用中的指令（例如，来自登录按钮 290 的登录请求）指示意图改为安全模式，则触发环境状态的转换。因此，通过经由受保护路径 265 向指示器设备 270 传递信号 260 来警告指示器设备 270。如果调用中的指令未指示意图转换到安全模式，则输入无法触发环境状态的改变。因此，操作系统 220 被维持于默认模式，由此免除向指示器设备 270 传递信号。

[0047] 在一示例性实施例中，转换组件 250 包括锁定元件 251、通信元件 252 和呈现元件 253。在标识到触发转换后，锁定元件 251 调整操作系统 220 的配置设置以便与调用中所标识的模式相对应。例如，如果标识安全模式，则锁定组件 251 根据该安全模式来设置成配置设置。即，在一个实施例中，锁定元件 251 锁定可操作地耦合到操作系统 220 的 UI 显示 225

以防其呈现应用程序 230 所提供的内容。而且，锁定元件 251 可限制应用程序 230 监听由输入设备 216、217 和 290 提供的输入。在另一种情况下，如果标识默认模式，则锁定组件 251 根据该默认模式来设置配置设置。即，锁定组件为主存在操作系统 220 上的应用程序的普通操作开放操作系统 220。尽管以上讨论了两种示例模式，但本发明的各实施例构想在锁定元件 251 处接受各种模式并根据所接受的每一种模式来调整操作系统 220 的配置设置。

[0048] 如上所述，在各实施例中，呈现元件 253 被配置成根据操作系统 220 的当前环境状态来在显示设备 215 的 UI 显示 225 上呈现内容。例如，如果在转换组件 250 处触发到安全模式的转换，则呈现元件 253 可指示 UI 显示 225 呈现安全登录屏幕并限制应用程序 230 在 UI 显示 225 上呈现内容。在另一种情况下，如果默认模式是当前环境状态，则呈现元件 253 不限制应用程序 230 在 UI 显示 225 上呈现内容。

[0049] 在一示例性实施例中，通信元件 252 向指示器设备 270 传递指示当前环境状态的信号 265。在一种情况下，该信号在触发转换组件 250 处的转换时提供。在其他情况下，信号 260 由通信元件 252 连续地、在预定义时刻周期性地、按增量式间隔、或使用相关实践领域内已知的任何其他转换方案来提供。信号 260 还可采取任何数量的形式，如上文中更全面地讨论的。另外，通信元件 252 通过受保护路径 265 提供信号。受保护路径可被具体化为操作系统 220 的通信元件 252 和指示器设备 270 之间的任何可操作耦合。

[0050] 受保护路径 265 可以是有线的或是无线的。本发明的范围内的受保护路径 265 的具体有线实施例的示例包括 USB 连接和电缆连接。本发明的范围内的受保护路径 265 的具体无线实施例的示例包括近程无线网络和射频技术。应该理解和明白，“近程无线网络”的指定不旨在限制，且应该被广泛地解释以至少包括以下技术：协商无线外围 (NWP) 设备；近程无线空气干扰网络（例如，无线个人区域网 (wPAN)、无线局域网 (wLAN)、无线广域网 (wWAN)、蓝牙等）；无线对等通信（例如，超宽带）；以及支持设备之间的数据的无线通信的任何协议。另外，熟悉本发明领域的人员将会认识到，近程无线网络可通过不同于所示具体实施例的各种数据传输方法（例如，电缆连接、卫星传输、电信网络等）来实现。因此，应强调受保护路径 265 的各实施例不受所述示例的限制，而是涵盖各种各样的通信方法。

[0051] 一般而言，认证组件 255 用于确认响应于 UI 显示 225 上的有效安全登录屏幕而提交的用户凭证。确认可包括执行与应用程序 230 或用户正试图访问的文件相关的认证过程。在一种特定情况下，该认证过程将接收到的凭证与预期安全凭证进行比较以确定是否存在匹配。通常，如果存在匹配，则认证组件 255 授权用户继续调用安全登录屏幕的工作流。在一示例性实施例中，安全登录屏幕在触发到安全模式的转换时调用。而且，在确定满足预期安全凭证后，认证组件 255 向转换组件 250 提供从受保护桌面模式转换到默认模式的指示。同样，如上所述，失败条件或超时准则可导致向转换组件 250 发送从受保护桌面模式转换到默认模式的指示。

[0052] 指示器设备 270 通常被配置成在接收到来自操作系统 220 的信号 265 时向用户提供警告。如上所述，指示设备 270 可提供基于操作系统 220 的环境状态的一种或多种类型的用户感知输出。例如，如果指示器设备 270 是 USB 鼠标（例如，HID）中的 LED，则到受保护桌面模式的转换的指示将由信号 260 传递给鼠标，该指示将促使 LED 发光。在上述示例中，由信号 260 传递给鼠标的到默认模式的转换的指示将促使 LED 关闭。在另一种情况下，如果指示器设备 270 是扬声器，则由信号 260 传递给扬声器的到受保护桌面模式的转换

的指示将促使扬声器广播连续或间断的声音。在这种情况下，声音提供供视觉受损用户检测操作系统 220 正在呈现有效登录屏幕的可靠方法。然而，为了准确地识别受保护模式已被激活，用户应将发出声音的扬声器标识为指示器设备 270，而不是推论 (corollary) 扬声器。在上述示例中，由信号 260 传递给扬声器的到默认模式的转换的指示将促使扬声器关闭或产生不同的声音。

[0053] 在可将 HID 用作指示器设备 270 的其他实施例中，检测元件 271 和实现元件 272 可被包括在指示器设备中。如以上参考组件 240、245、250 和 255 所讨论的，元件 271 和 272 只是出于示例性目的而单独表达的，并且实际上可被具体化为一个或多个元件。检测元件 271 被配置成从操作系统 220 接收信号 260 或消息。在一种情况下，检测元件 271 被配置成解释信号 260 以确定是否在用户感知输出中调用改变。作为示例，指示与所指示的前一模式相似的模式的信号 260 将不调用改变。实现元件 272 通常被配置成根据对信号 260 的解释来控制用户感知输出的类型和持续时间。例如，模式可以映射到 LED 的不同的照度级或灯泡闪烁频率。利用对信号 260 的解释，实现元件 272 调用适当的或所映射的输出发生（例如，与当前模式相关联）。

[0054] 现在转向图 3，示出了例示根据本发明的一实施例的用于警告用户操作系统已进入安全模式的总体方法 300 的流程图。最初，在操作系统（例如，图 2 的操作系统 220）处接收一个或多个输入，如框 305 所示。可将这些输入标识为对执行受保护操作的调用，如框 310 所示。如果被标识为调用，则操作系统从默认模式转换到安全模式，如框 315 所示。如框 320 所示，将该转换的指示传递给指示器设备（例如，图 2 的指示器设备 270）。在具体实施例中，通过经由安全路径信令指示器设备来执行通信，如框 325 所示。因此，促使生成用户可感知输出，如框 330 所示。

[0055] 如框 335 所示，接收一个或多个登录凭证。对登录凭证执行认证过程（参见框 340），并且如果这些凭证是有效的，或使操作系统退出安全模式，则触发到默认模式的转换（参见框 345）。如框 350 所示，将该转换的指示传递给指示器设备。在具体实施例中，通过经由安全路径信令指示器设备来执行通信，如框 355 所示。因此，促使停止生成用户可感知输出，如框 360 所示。

[0056] 参考图 4，示出了例示根据本发明的各实施例的用于在无源状态和通知状态之间转换指示器设备的各阶段的渐进式屏幕显示 400。最初，操作系统处于默认模式。由此，UI 显示处于正常状况 410，由此允许应用程序在其上呈现内容 415 并监听用户发起输入。而且，HID 450 可操作地耦合到操作系统（例如，经由提供对指示器设备 460 的独占控制的受保护路径）。HID 450 接收操作系统正驻留在默认模式中的信号或某指示，并因此在指示器设备 460 处调用无源状态。该无源状态使指示器设备 460 警告用户操作系统不处于安全模式并制止提供特权信息。

[0057] 在触发到安全模式的转换后，该 UI 显示被切换到锁定状况 420。在该锁定状况 420 中，UI 显示提供安全登录屏幕 430 并且操作系统限制应用程序监听用户所提供的输入。而且，HID 450 接收操作系统处于安全模式的指示（例如，经由图 2 的信号 260），并调用指示器设备 460 将状态改为通知状态。在该通知状态中，指示器设备 460 警告用户提供特权信息作为安全凭证 435 以满足安全登录屏幕 430 是安全的。在满足在安全登录屏幕 430 的后台操作的认证过程后，操作系统回复到默认模式。因此，将该转换通知给 HID 450，并调用指

示器设备 460 来提供对应于该默认模式的适当的用户感知输出（如果有的话）。

[0058] 尽管示出了一个指示器设备 460，但本发明的各实施例构想指示器设备的各种组合。在一种情况下，可以提供控制或容纳由操作系统独占控制的第二指示器设备的第二 HID。通常，该第二指示器设备被配置成在接收到输入已触发操作系统的环境状态的改变的指示后生成用户可感知输出。具体而言，第二指示器设备所生成的用户可感知输出可以与指示器设备 460 所生成的用户可感知输出相对应。

[0059] 现在转向图 5，示出了根据本发明的一实施例的提供安全登录屏幕 540 的示例性 UI 显示 510 的图示。最初，在默认模式中，应用程序被允许在 UI 显示 510 上呈现内容 515。与转换到安全模式相关联地，呈现安全登录屏幕 540。在所描绘的情况下，提供供用户输入包括个人 ID 550 和口令 560 的安全凭证的登录输入区域 530。因为指示器设备正警告用户操作系统正阻塞恶意应用程序，所以他或她可以在没有身份盗取威胁的情况下安心地输入特权信息。在认证安全凭证后，访问如图所示的银行网站的 web 浏览器允许用户继续访问适当的账户。因此，指示器设备可靠地通知用户何时提供和不提供特权信息。

[0060] 参考各具体实施例描述了本发明，各具体实施例在所有方面都旨在是说明性的而非限制性的。不偏离本发明范围的情况下，各替换实施例对于本发明所属领域的技术人员将变得显而易见。

[0061] 从前面的描述可以看出，本发明很好地适用于实现上文所阐述的所有目的和目标，并且具有对于该系统和方法是显而易见且固有的其他优点。可以理解，某些特征和子组合是有用的，并且可以在不参考其他特征和子组合的情况下使用。这由权利要求所构想的，并在权利要求的范围内。

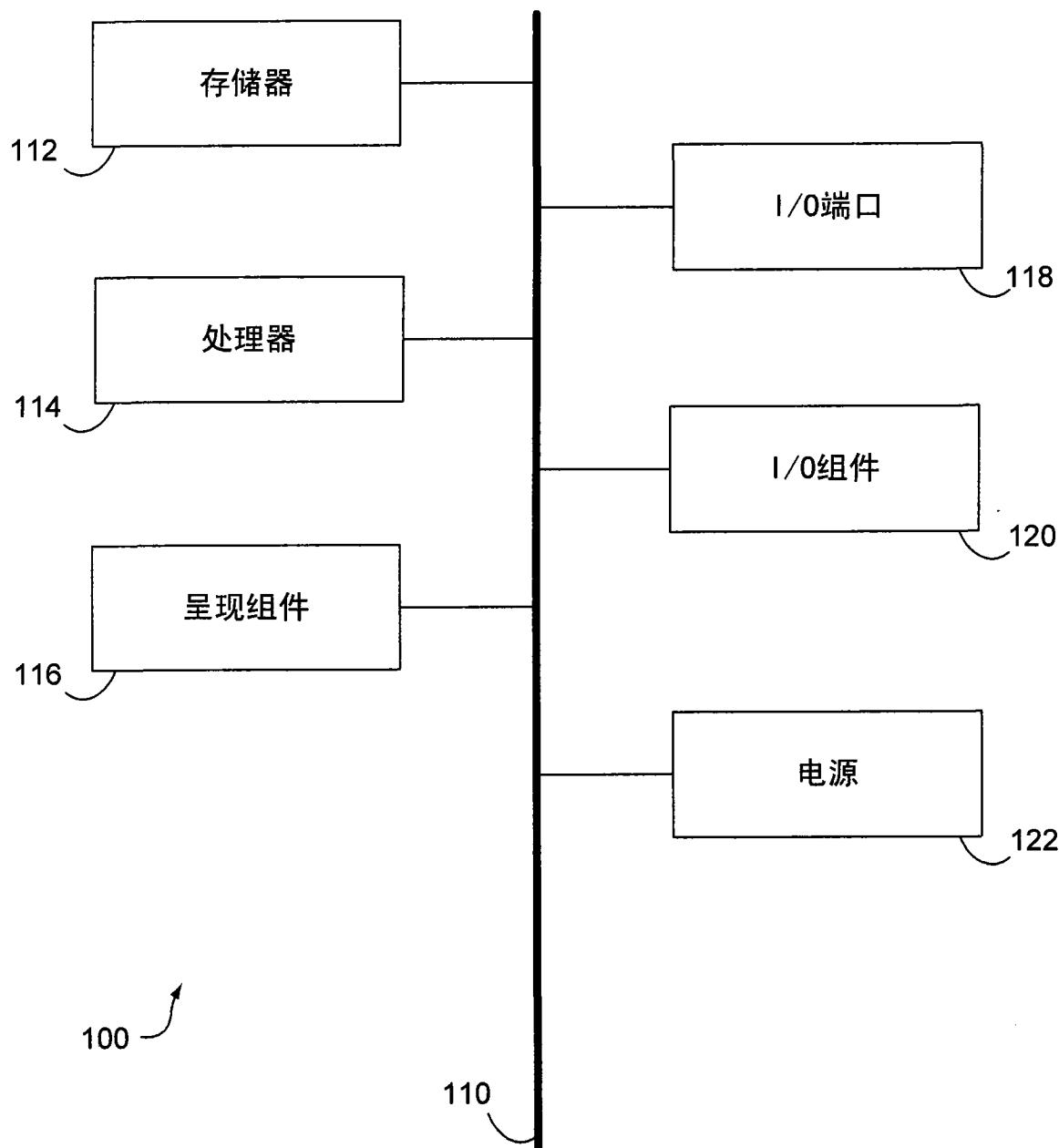


图 1

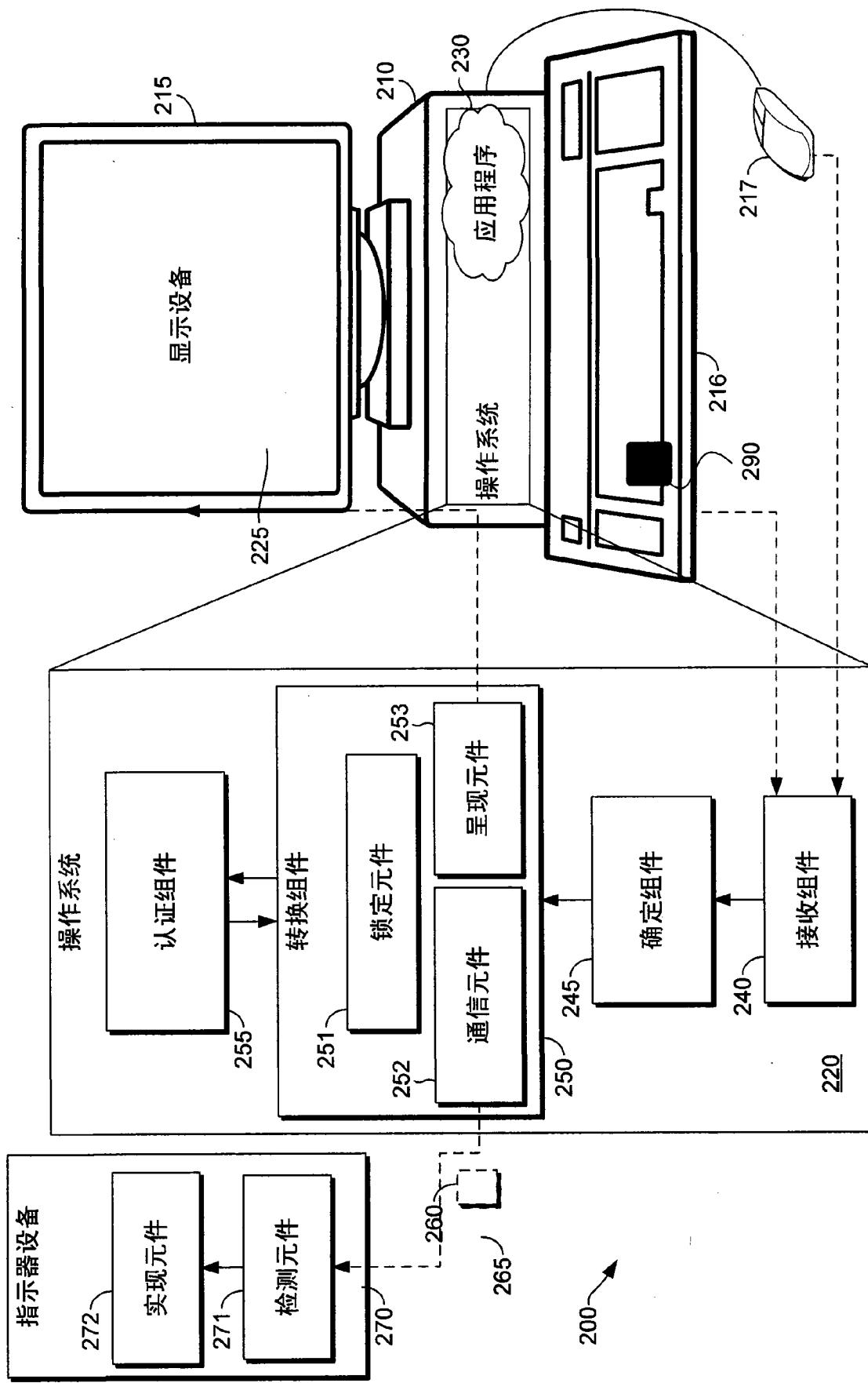


图 2

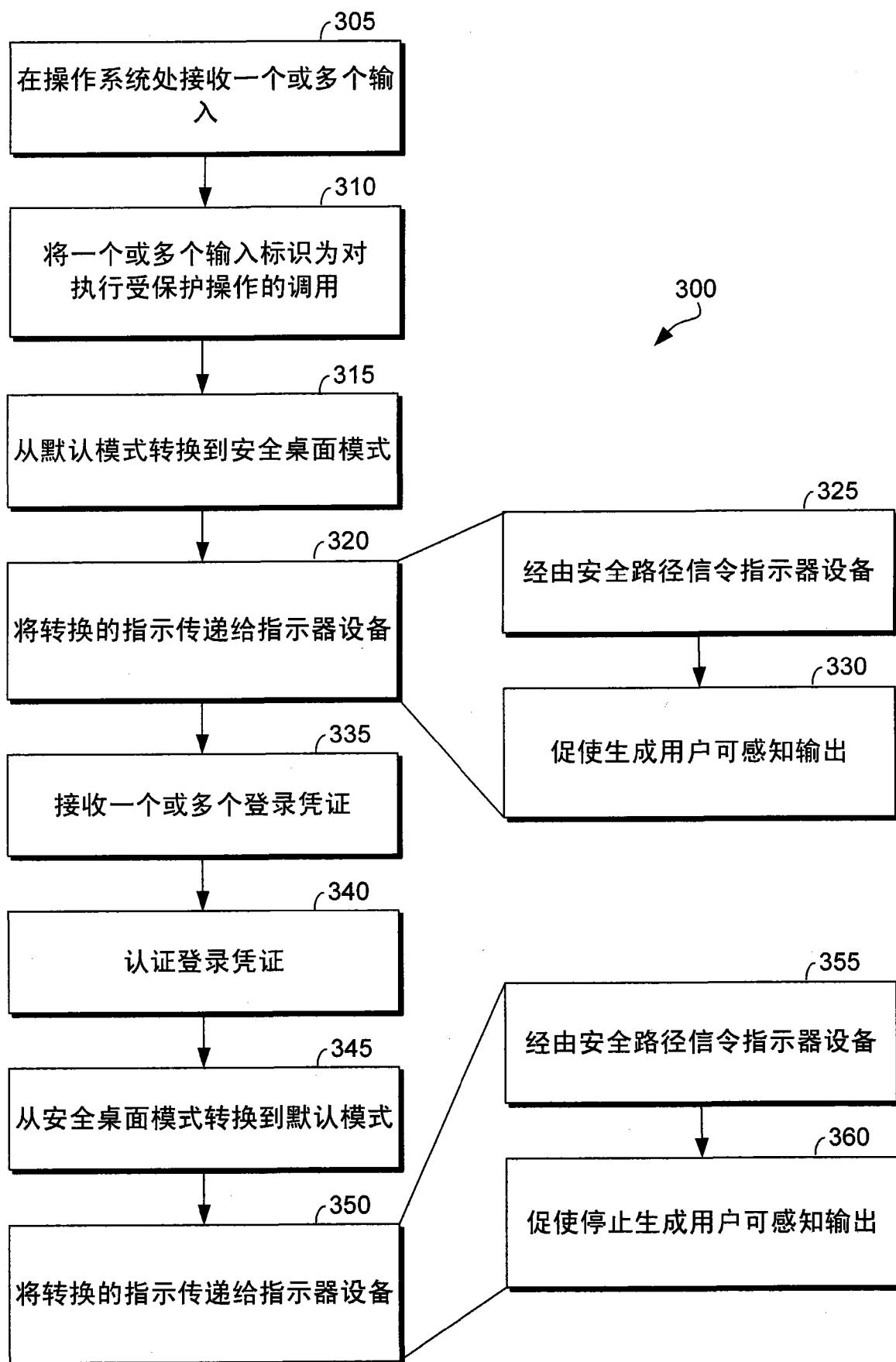


图 3

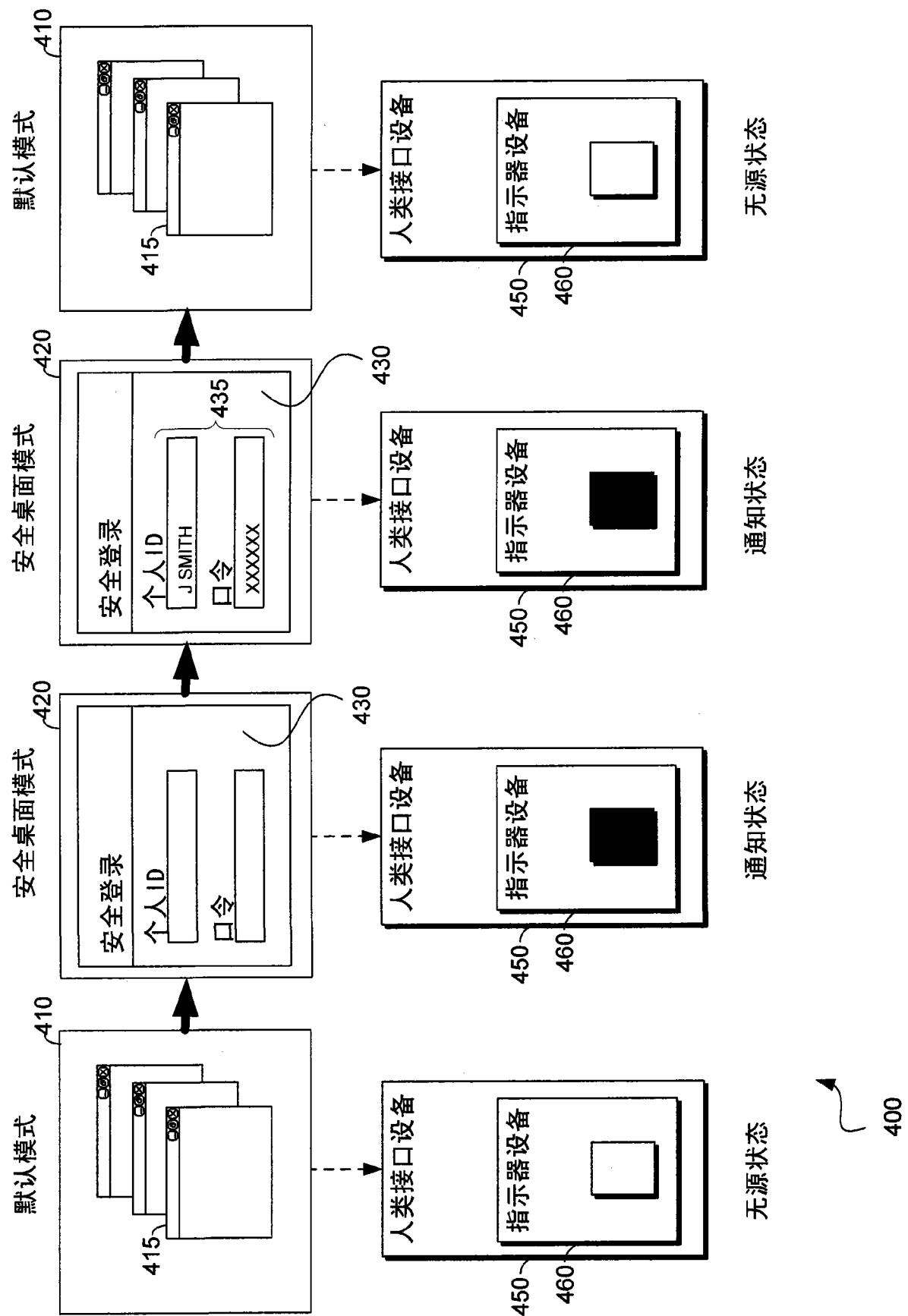


图 4

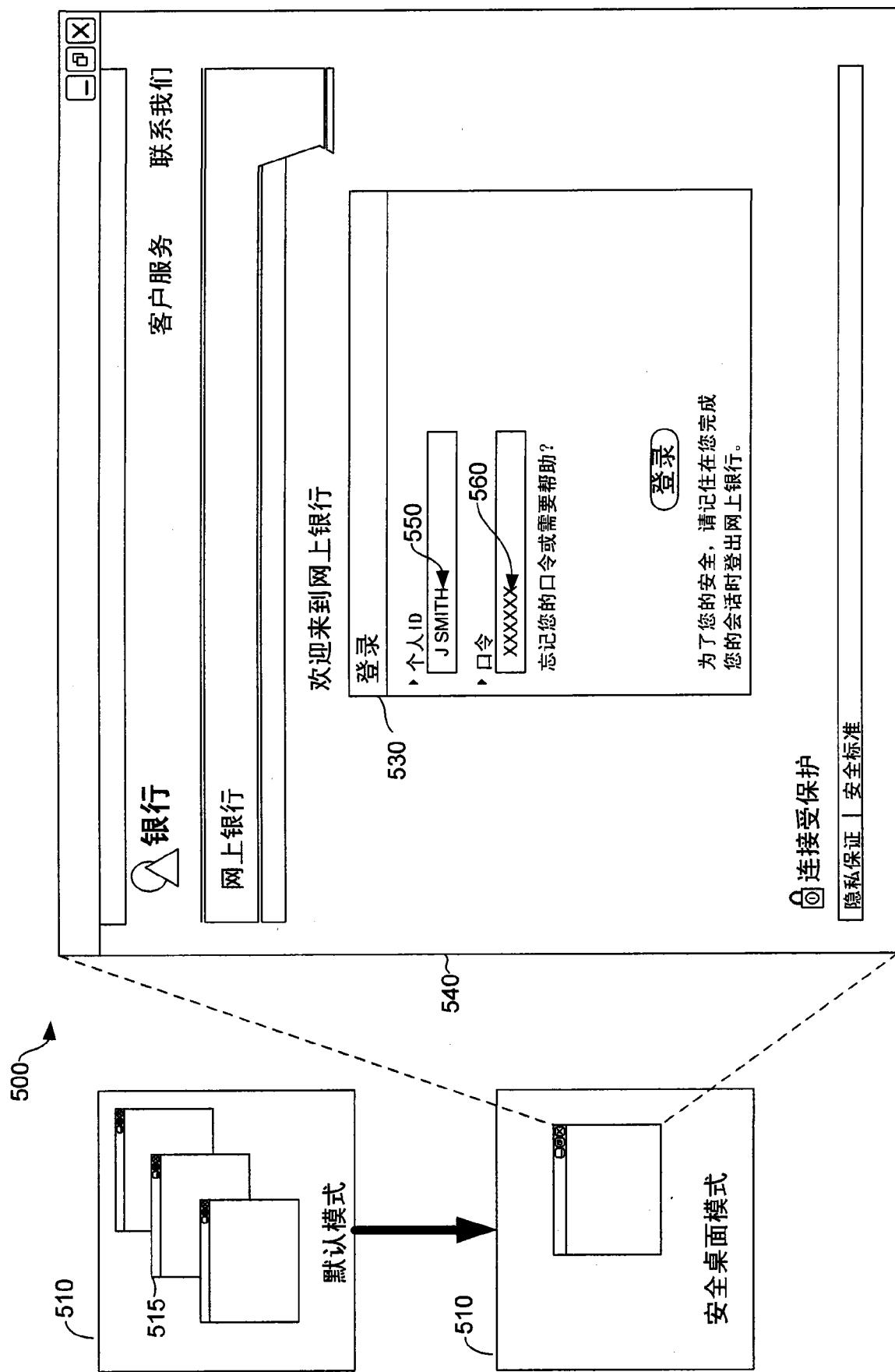


图 5