(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 1849773 B
(45)授权公告日 2011.10.05

(21)申请号 200480001391.3

(22)申请日 2004.07.29

(30)优先权数据
10/826,139 2004.04.15 US

(85)PCT申请进入国家阶段日
2005.05.26

(86)PCT申请的申请数据
PCT/US2004/024343 2004.07.29

(87)PCT申请的公布数据
WO2005/109736 EN 2005.11.17

(73)专利权人 微软公司
地址 美国华盛顿州

(72)发明人 A·塞尔泽 R·S·迪里克森
R·托库米 R·A·佛朗哥

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 顾嘉运

(51)Int.Cl.
H04L 9/00(2006.01)

(56)对比文件
EP 0844767 A1,1998.05.27,(说明书第3页第45行-第6页第58行,附图1-7).
US 6356937 B1,2002.03.12,全文.
US 2002/0149601 A1,2002.10.17,全文.
WO 03/049403 A2,2003.12.06,全文.

审查员 郭风顺

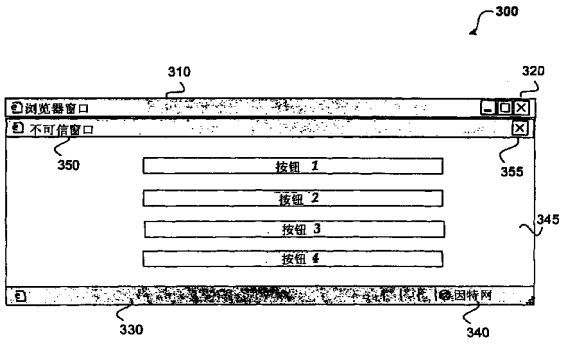
权利要求书 2 页 说明书 5 页 附图 6 页

(54)发明名称

用浏览器窗口显示安全元素

(57)摘要

本发明提供了一种方法和系统,用于提供针对通过以用户可信任和知道窗口的来源的方式显示浏览器窗口来抑制恶意活动的安全元素。在窗口上显示附加信息和装饰,以帮助确保终端用户不被迷惑或误导(“欺骗”)成相信窗口源自可信来源。当作出打开浏览器窗口的调用时,默认地显示状态栏。状态栏向用户提供了附加信息,如安全区域,以帮助用户确定内容的来源。安全区域向用户通知了内容所起源的位置。这一附加信息帮助确保用户具有关于是否要信任来源的必要信息。



CN 1849773 B

1. 一种用于提供浏览器窗口的安全特征的方法，其特征在于，包括：

接收打开窗口的调用；

确定与所述窗口相关联的安全级别，其中所述安全级别是从至少一个不可信安全级别和至少一个可信安全级别中选出；

当所述安全级别指示所述窗口内的内容来自不可信来源时，与一安全元素一起显示所述窗口，用户察看该安全元素，以确定所述窗口内的内容来自所述不可信来源；

检查与所述打开窗口调用相关联的属性；

调整所述调用中的至少一个属性，以便所述安全元素显示为不可信安全元素；以及

发送经修改的调用以打开窗口；

其中所述安全元素是一安全区域，该安全区域将所述内容所起源的位置通知给用户。

2. 如权利要求 1 所述的方法，其特征在于，确定与所述窗口相关联的安全级别还包括当用户正在因特网区域和受限区域的至少一个中导航时，确定所述安全级别为不可信级别。

3. 如权利要求 1 所述的方法，其特征在于，所述安全元素是状态栏。

4. 如权利要求 3 所述的方法，其特征在于，一区域显示在所述状态栏内。

5. 如权利要求 3 所述的方法，其特征在于，所述安全元素还包括标题栏。

6. 一种用于提供浏览器窗口的安全特征的方法，其特征在于，所述方法包括：

接收打开窗口的调用，其中，所述调用包括与所述窗口的属性相关联的参数；

对所述参数进行语法分析，以查找与一安全元素相关联的至少一个参数，当所述安全元素与所述窗口一起显示时，它向用户指示所述窗口内的内容来自不可信来源；

调整所述至少一个查找到的参数，使得所述安全元素在所述窗口被打开时显示；

确定与所述窗口相关联的安全级别；以及

当所述安全级别指示所述窗口内的内容来自不可信来源时，调整所述至少一个查找到的参数；

其中所述安全元素是一安全区域，该安全区域将所述内容所起源的位置通知给用户。

7. 如权利要求 6 所述的方法，其特征在于，所述安全级别选自至少一个不可信安全级别和至少一个可信安全级别。

8. 如权利要求 6 所述的方法，其特征在于，确定与所述窗口相关联的安全级别还包括当用户正在因特网区域和受限区域的至少一个中导航时，确定所述安全级别为不可信级别。

9. 如权利要求 8 所述的方法，其特征在于，所述安全元素是状态栏。

10. 如权利要求 9 所述的方法，其特征在于，一区域显示在所述状态栏内。

11. 如权利要求 9 所述的方法，其特征在于，所述安全元素还包括标题。

12. 一种用于提供浏览器窗口的安全特征的设备，其特征在于，包括：

用于接收打开窗口的调用的装置，其中，所述调用包括与所述窗口的属性相关联的参数；

用于对所述参数进行语法分析的装置，以查找与一安全元素相关联的至少一个参数，当所述安全元素与所述窗口一起显示时，它向用户指示所述窗口内的内容来自不可信来源；

用于调整所述至少一个查找到的参数的装置，使得所述安全元素在所述窗口被打开时显示；

用于确定与所述窗口相关联的安全级别的装置；以及

当所述安全级别指示所述窗口内的内容来自不可信来源时，用于调整所述至少一个查找到的参数的装置；

其中所述安全元素是一安全区域，该安全区域将所述内容所起源的位置通知给用户。

13. 如权利要求 12 所述的设备，其特征在于，所述安全级别选自至少一个不可信安全级别和至少一个可信安全级别。

14. 如权利要求 13 所述的设备，其特征在于，用于确定与所述窗口相关联的安全级别的装置还包括当用户正在因特网区域和受限区域的至少一个中导航时，用于确定所述安全级别为不可信级别的装置。

15. 如权利要求 12 所述的设备，其特征在于，一区域显示在所述状态栏内。

16. 如权利要求 12 所述的设备，其特征在于，还包括用于显示标题栏的装置。

用浏览器窗口显示安全元素

背景技术

[0001] 在访问因特网站点时保持计算机的安全性可能是困难的。每天都会有新的方法，它们误导用户选择他们相信能够执行安全任务的行动，然而实际上执行该任务却是恶意的。例如，浏览器窗口可以被恶意地绘制以模仿对话框或与可信来源相关联的窗口。看见该窗口的用户可能被误导成相信他们正在关闭该窗口，而实际上他们被重定向到另一站点或下载恶意文件。

发明内容

[0002] 本发明针对提供一种方法和系统，用于提供通过以用户可以信任并知道窗口来源的方式显示浏览器窗口来抑制恶意活动的安全元素。

[0003] 依照本发明的一个方面，该安全元素包括显示在窗口上的附加信息和装饰，以帮助确保当来源实际上是非可信来源时用户不被迷惑或误导（“欺骗”）成相信该窗口来自一可信来源。

[0004] 依照本发明的另一方面，当作出打开浏览器窗口的调用时，该安全元素是默认地显示的状态栏。该状态栏可以向用户提供附加信息，如安全区域，以帮助用户确定内容的来源。该安全区域将内容所起源的位置通知给用户。

[0005] 依照本发明的又一方面，用户在其中导航的安全区域用于确定要用浏览器窗口显示的安全元素。例如，当来源是非可信来源时，总是显示安全元素。当来源可信时，可能显示或不显示该安全元素。

附图说明

[0006] 图 1 示出了可在本发明的示例性实施例中使用的示例性计算装置。

[0007] 图 2 显示了示出用户可以访问的不同区域的示例性窗口。

[0008] 图 3 示出了在可信浏览器窗口内显示的不可信内容。

[0009] 图 4 示出了用于提高浏览器窗口的安全性的过程。

[0010] 图 5 示出了用于确定安全性设置的过程；以及

[0011] 图 6 示出了依照本发明的各方面用于调整与安全元素相关联的窗口参数的过程流。

具体实施方式

[0012] 一般而言，本发明针对提供一种方法和系统，用于提供通过以用户能够信任和知道窗口来源的方式显示窗口来抑制恶意活动的安全特征。包括附加信息和装饰的安全元素被显示在窗口上，以帮助确保终端用户不被迷惑或误导（“欺骗”）成相信该窗口源自可信来源。例如，用户能够在视觉上将从诸如操作系统等可信来源生成的窗口与具有从诸如外部网站等非可信来源生成的内容的窗口区分开来。

[0013] 依照一个实施例，当打开浏览器窗口时，默认地显示一状态栏。该状态栏向用户提

供了附加信息，如安全区域，以帮助用户确定内容的来源。该安全区域将内容所起源的位置通知给用户。例如，该安全区域可以指示内容源自因特网。该附加信息帮助确保用户具有关于是否要信任该来源的必要信息。

[0014] 说明性操作环境

[0015] 参考图 1，用于实现本发明的一个示例性系统包括诸如计算装置 100 的计算装置。在十分基本的配置中，计算装置 100 通常包括至少一个处理单元 102 和系统存储器 104。根据计算装置的确切配置和类型，系统存储器 104 可以是易失性（如 RAM）、非易失性（如 ROM、闪存等）或两者的某一组合。系统存储器 104 通常包括操作系统 105、一个或多个应用程序 106，并且可包括程序数据 107。在一个实施例中，应用程序 106 可包括窗口安全程序 120。一般而言，窗口安全程序 120 配置成确保窗口是用用户确定窗口中的内容的来源所必需的视觉提示和信息来打开的。这一基本配置在图 1 中由虚线 108 内的组件示出。

[0016] 计算装置 100 可具有另外的特征或功能。例如，计算装置 100 也可包括另外的数据存储设备（可移动和 / 或不可移动），如磁盘、光盘或磁带。这类另外的存储在图 1 中由可移动存储 109 和不可移动存储 110 示出。计算机存储介质可包括以用于储存如计算机可读指令、数据结构、程序模块或其它数据等信息的任一方法和技术实现的易失性和非易失性、可移动和不可移动介质。系统存储器 104、可移动存储 109 和不可移动存储 110 都是计算机存储介质的示例。计算机存储介质包括但不限于，RAM、ROM、EEPROM、闪存或其它存储器技术、CD-ROM、数字多功能盘 (DVD) 或其它光存储、磁盒、磁带、磁盘存储或其它磁存储设备、或可以用来储存期望的信息并可由计算装置 100 访问的任一其它介质。任一这类计算机存储介质可以是装置 100 的一部分。计算装置 100 也可具有（多个）输入设备 112，如键盘、鼠标、输入笔、语音输入设备、触摸输入设备等等。也可包括（多个）输出设备 114，如显示器、扬声器、打印机等等。

[0017] 计算装置 100 也包含允许装置如通过网络与其它计算装置 118 进行通信的通信连接 116。通信连接 116 是通信介质的一个示例。通信介质通常可以诸如载波或其它传输机制等已调制数据信号中的计算机可读指令、数据结构、程序模块或其它数据实施，并包括任一信息传送介质。术语“已调制数据信号”指以对信号中的信息进行编码的方式设置或改变其一个或多个特征的信号。作为示例而非局限，通信介质包括有线介质，如有线网络或直接连线连接，以及无线介质，如声学、RF、红外和其它无线介质。本发明使用的术语计算机可读介质包括存储介质和通信介质。

[0018] 包括安全元素的说明性窗口

[0019] 图 2 依照本发明的各方面示出了一个示例性窗口，它示出了用户可以访问的不同区域。安全区域用于帮助提供关于用户可能遇到的各种类型的内容的适当的安全级别。可以实现许多不同的安全区域，他们具有与其相关联的不同的可信赖程度。依照本发明的一个实施例，有五个安全区域，包括本地机器区域 (205)、可信站点区域 (230)、本地内联网区域 (240)、因特网区域 (250) 和受限区域 (260)。不同的区域具有与其相关联的不同安全级别。依照本发明的一个实施例，诸如状态栏 220 等安全元素总是与窗口一起显示。

[0020] 当前区域 (225、235、245、255 和 265) 在状态栏 220 的右侧底部显示。用户可以通过参考该区域来容易地评估与内容 215 相关联的风险。无论用户何时导航到一个不同的区域，该区域便被显示在状态栏内。

[0021] 依照本发明的一个实施例，有与每一区域相关联的默认安全设置。然而，这些安全设置可被改变和配置成基于组织及其用户所需的设置。

[0022] 例如，组织可为浏览器处理显示内容、下载程序和文件的方式指定设置，取决于内容或文件所来自的区域。例如，组织可以确信在其企业内联网内下载的任何内容都是安全的。因此，对于诸如本地机器区域 (225) 或本地内联网区域 (245) 等某些区域的安全设置可以被设为允许用很少或不用提示来下载的低级别。然而，对于诸如来自因特网区域或受限区域的内容等非可信来源的安全设置可能要严格得多。例如，可以向用户显示指示与内容相关联的风险的更多信息。

[0023] 由窗口 205 示出的本地机器区域是用于用户本地计算机上存在的内容的区域。用户计算机上找到的内容，除可能从不可信来源高速缓存在本地系统上的内容之外，都可以用高信任级别来处理。例如，浏览器可高速缓存从因特网获得的来自不可信来源的内容。一般而言，已经在本地计算机上的任何文件被假定为非常安全的，因此，向它们分配最小的安全设置。依照一个实施例，当导航的区域是本地机器区域时，安全元素可以被关闭。

[0024] 网站可以从可信站点区域 (235) 和受限站点区域 (265) 中添加或删除。可信站点区域 (235) 和受限站点区域 (265) 包含比因特网区域或本地内联网区域更可信或更不可信的站点。

[0025] 可信站点区域 (235) 指的是被认为不会有害的站点。例如，相信用户可以安全地下载或运行来自包含在“可信站点区域”中的站点的文件，而不用担心数据的可信赖性。该区域供高度可信的站点使用，例如可信商业伙伴的站点。依照一个实施例，当导航的区域是可信站点区域时，安全元素可以被关闭。

[0026] 受限站点区域 (265) 用于不可信的站点，并且被分配以高安全级别。当用户在受限站点时，向窗口 260 提供足够的信息，使得用户知道该内容来自不可信来源。依照一个实施例，当用户正在受限站点区内导航时，总是显示状态栏 (220) 和标题栏 (210)。

[0027] 本地内联网区域 (245) 通常包含不需要代理服务器的任何地址，如由系统管理员所定义的。这通常包括由网络路径 (如，\\computername\foldername) 指定的站点和本地内联网站点 (通常其地址不包含句点，如 http ://internal)。本地内联网区域 245 一般是可信的，因为内联网上的信息来自用户的公司。例如，由于用户公司内联网上的站点是可信的，因此组织通常希望用户能够运行来自该位置的所有类型的活动内容。依照本发明的一个实施例，当用户在本地内联网区域 (245) 中操作时，标题栏 (210) 和状态栏 (220) 可以被关闭。

[0028] 因特网区域 (255) 由不包括在用户的计算机上、公司的本地内联网上的网站或不被分配给可信站点区域或受限站点区域的站点构成。位于因特网上的站点一般不那么可信。因此，向因特网区域应用更高的安全级别。这一更高的安全级别帮助用户运行活动内容并将代码下载到其计算机。当用户导航到因特网区域 (255) 时，窗口 250 将具有用户知道内容来自何处所需的足够信息。例如，依照一个实施例，窗口 250 包括标题栏 (210) 和状态栏 (220)，其中在状态栏 (220) 中指示了因特网区域 (255)。

[0029] 图 3 示出了依照本发明的各方面在可信浏览器窗口中显示的不可信内容。

[0030] 可信浏览器窗口 300 包括标题栏 310、状态栏 330、区域信息 340 和不可信内容 345。不可信内容 345 包括标题栏 350，它具有关闭按钮 355，旨在欺骗用户相信当他们在关

闭按钮 335 上点击时窗口 310 将会关闭。依照本发明的一个实施例，在不可信区域内的任何窗口与状态栏 (330) 一起显示。在最可信的区域中，浏览器状态栏 (330) 和标题栏 (310) 可以被关闭。依照另一实施例，安全元素可以从不被关闭。

[0031] 内容 345 被绘制为示例性广告窗口。内容 345 被绘制，以试图误导用户点击内容 345 内的关闭按钮 355，而非点击关闭按钮 320。点击关闭按钮 355 对用户可以是恶意的。例如，当用户点击虚构的关闭按钮 355 而非如浏览器所做的那样关闭窗口时，用户可能被导航到另一窗口，或者更坏的情况是，病毒可能被下载到用户的计算机上。强迫对于不可信内容显示状态栏 (330) 有助于向用户提供区分内容源自何处的必要信息。如可以参考图 3 所见到的，内容 345 清楚地位于具有状态栏 (330) 的可信浏览器窗口内，它清楚地通知用户，该窗口来自因特网来源 (340)。

[0032] 状态栏 330 默认地被显示，以帮助将由诸如计算机操作系统等可信来源生成的窗口与由不可信来源生成的内容区分开来。

[0033] 通过在浏览器窗口 330 上显示附加信息和装饰，以帮助确保最终用户不被内容 345 迷惑或误导，可以抑制恶意活动。依照本发明的一个实施例，附加信息和装饰是使内容 345 看似为在网页窗口内的视觉提示。在本示例中，例如，如果不显示状态栏 330，可能导致用户相信内容 345 是由操作系统而非外部来源创建的窗口。

[0034] 当打开具有标题栏的浏览器窗口时，默认地显示状态栏，以确保状态栏中的信息对用户是可见的。安全区域 (340) 被显示在状态栏 330 内，以向用户通知，例如他们是在因特网上还是在本地内联网上。

[0035] 图 4 示出了依照本发明的各方面用于提高浏览器窗口的安全性的过程。在开始框之后，过程流到框 410，其中接收打开新窗口的调用。该打开窗口的调用一般具有定义窗口特征的相关联的窗口设置。这些设置一般包括诸如高度、宽度、位置、滚动条信息、标题栏、状态栏相关信息等信息。

[0036] 移至框 420，确定与安全区域相关联的安全设置。一般而言，安全设置涉及用户当前正在导航的区域（见图 5 和相关讨论）。安全设置可用于确定是否显示安全元素。

[0037] 转移到框 430，可基于安全设置修改窗口设置。一般而言，修改参数，使得窗口设置被配置成使在窗口上有足够的信息和装饰，以使用户能够识别不可信内容（见图 6 和相关讨论）。例如，显示状态栏。

[0038] 流到框 440，显示窗口。依照一个实施例，显示其上具有标题栏和状态栏的窗口，使得内容可以与网页窗口清楚地区别开来。

[0039] 图 5 示出了依照本发明的各方面用于确定安全性设置的过程。在开始框之后，过程流到框 510，其中确定安全区域。依照一个实施例，安全区域可以是五个区域之一，包括本地机器区域、可信站点区域、本地内联网区域、因特网区域和受限区域。

[0040] 移至判别框 520，判断区域是否可信。可信区域是被认为总是具有可信内容的区域。换言之，从可信区域接收的内容不是恶意的。当区域不可信时，过程流到框 530，其中被请求打开的窗口将包括供用户确定内容的位置是来自不可信来源所需的装饰和信息。依照一个实施例，对于包含来自不可信区域的内容的任何窗口，显示标题栏和状态栏。当区域可信时，过程流到结束块，处理结束。依照另一实施例，即使区域可信，窗口也包括供用户确定内容的位置是来自不可信来源所需的装饰和信息。处理然后步进到结束框，并返回以处理

其它行动。

[0041] 图 6 示出了依照本发明的各方面用于调整与安全元素相关联的窗口参数的过程流。在开始框之后，过程流到框 610，获取窗口参数。如上所述，窗口参数可以涉及与窗口相关联的任何属性，如：宽度、高度、滚动条、颜色、标题栏（开 / 关）、状态栏（开 / 关）等等。

[0042] 转移到框 620，对窗口参数进行语法分析以查找涉及状态栏的属性。依照一个实施例，也查找标题栏属性。

[0043] 流到框 630，将状态栏属性设置为开。这帮助确保即使窗口参数被设置成不显示状态栏时也将显示状态。

[0044] 过程然后可以流到操作框 640，其中标题栏也被打开。其它属性或信息也可以被打开并显示，以帮助确保窗口包含用户用于确定窗口内的内容不是窗口本身的足够装饰和信息。例如，可以在窗口周围放置特殊的边界。该过程然后流到结束框，并返回以处理其它行动。

[0045] 上述说明书、示例和数据提供了本发明的组成部分的制造和使用的完整描述。由于可以在不脱离本发明的精神和范围的情况下作出本发明的许多实施例，因此本发明驻留在所附权利要求书之中。

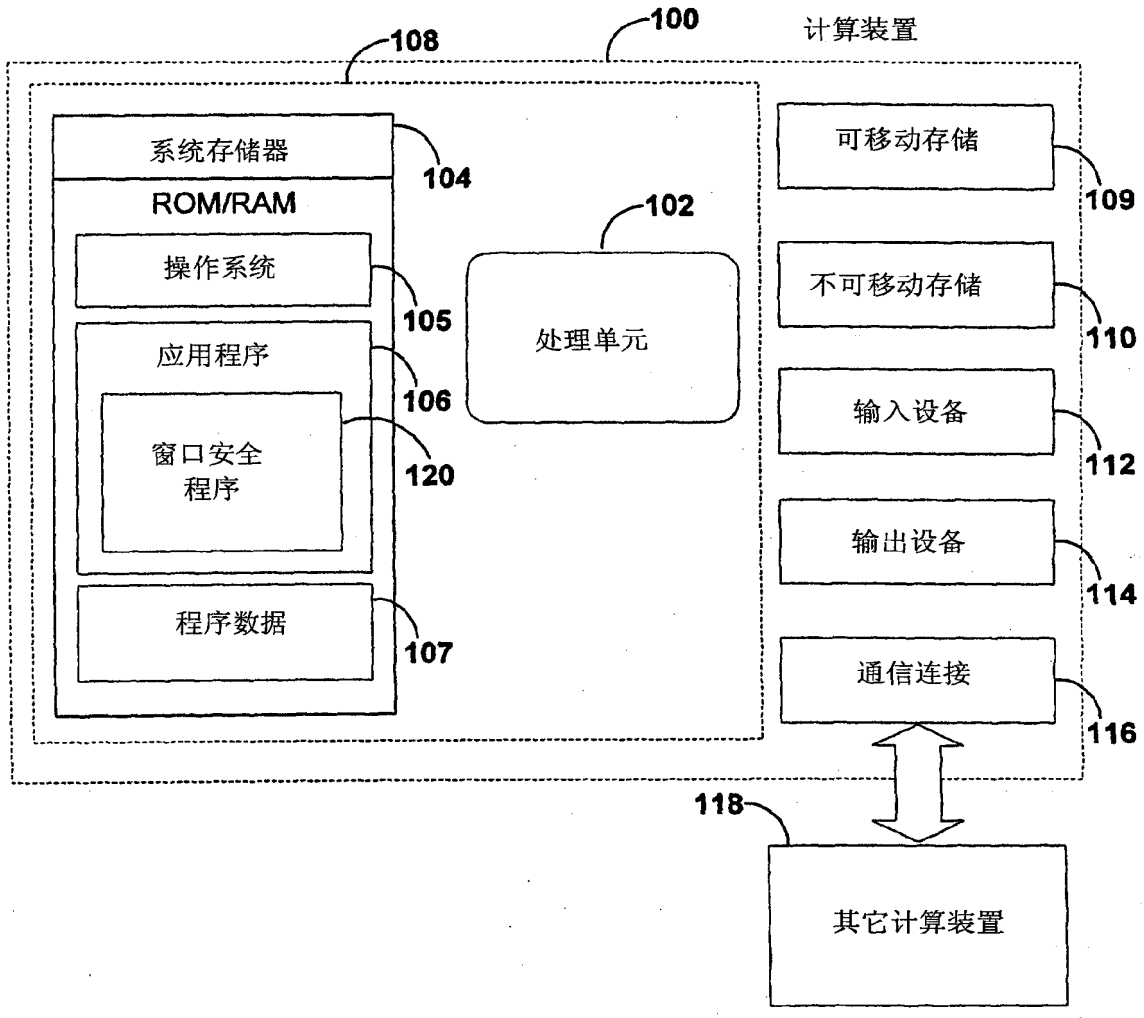

100
计算装置
108
系统存储器
104
ROM/RAM
操作系统
105
应用程序
106
窗口安全
程序
120
程序数据
107
102
处理单元
可移动存储
109
不可移动存储
110
输入设备
112
输出设备
114
通信连接
116
118
其它计算装置

图 1

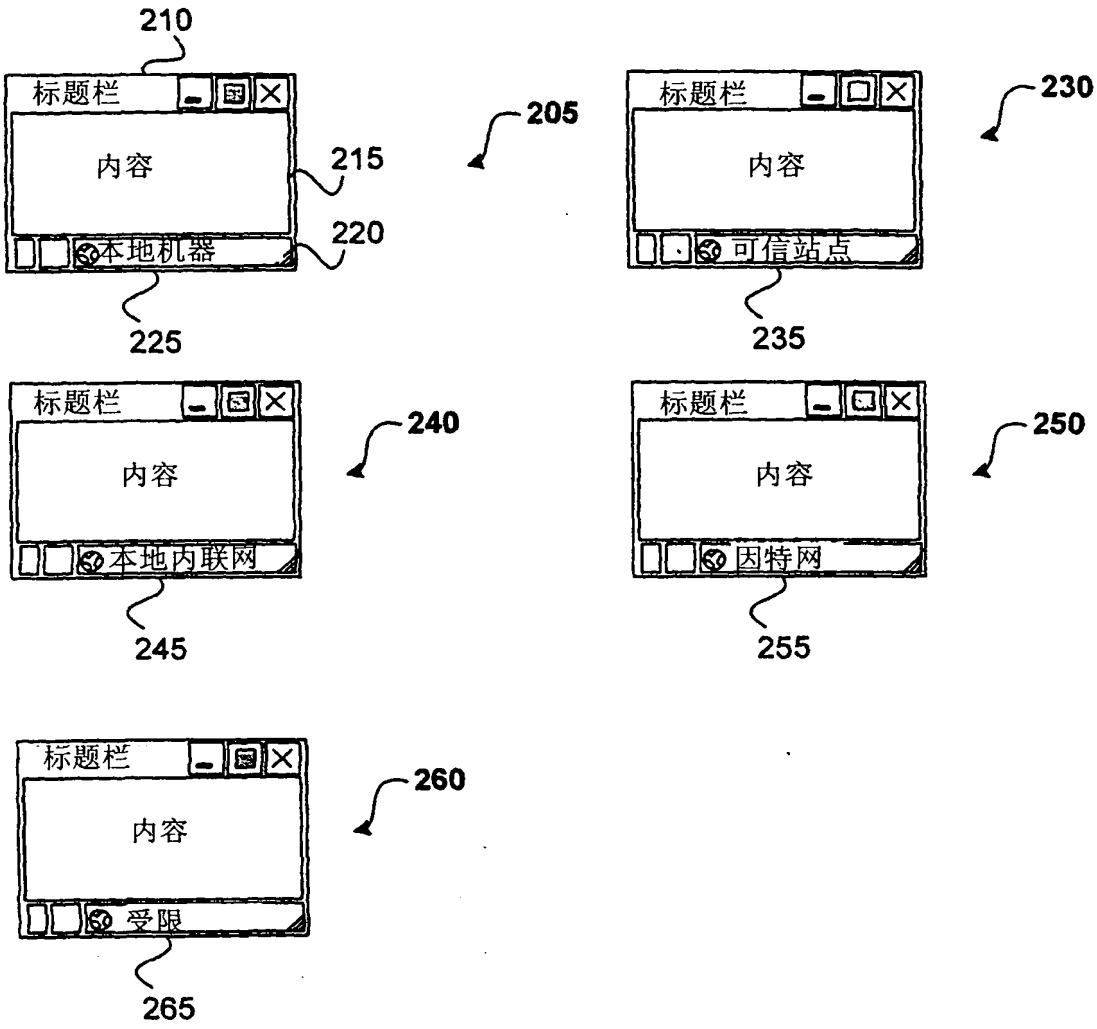

210
标题栏
内容
215
205
220
本地机器
225
标题栏
内容
230
可信站点
235
标题栏
内容
240
本地内联网
245
标题栏
内容
250
因特网
255
标题栏
内容
260
受限
265

图 2

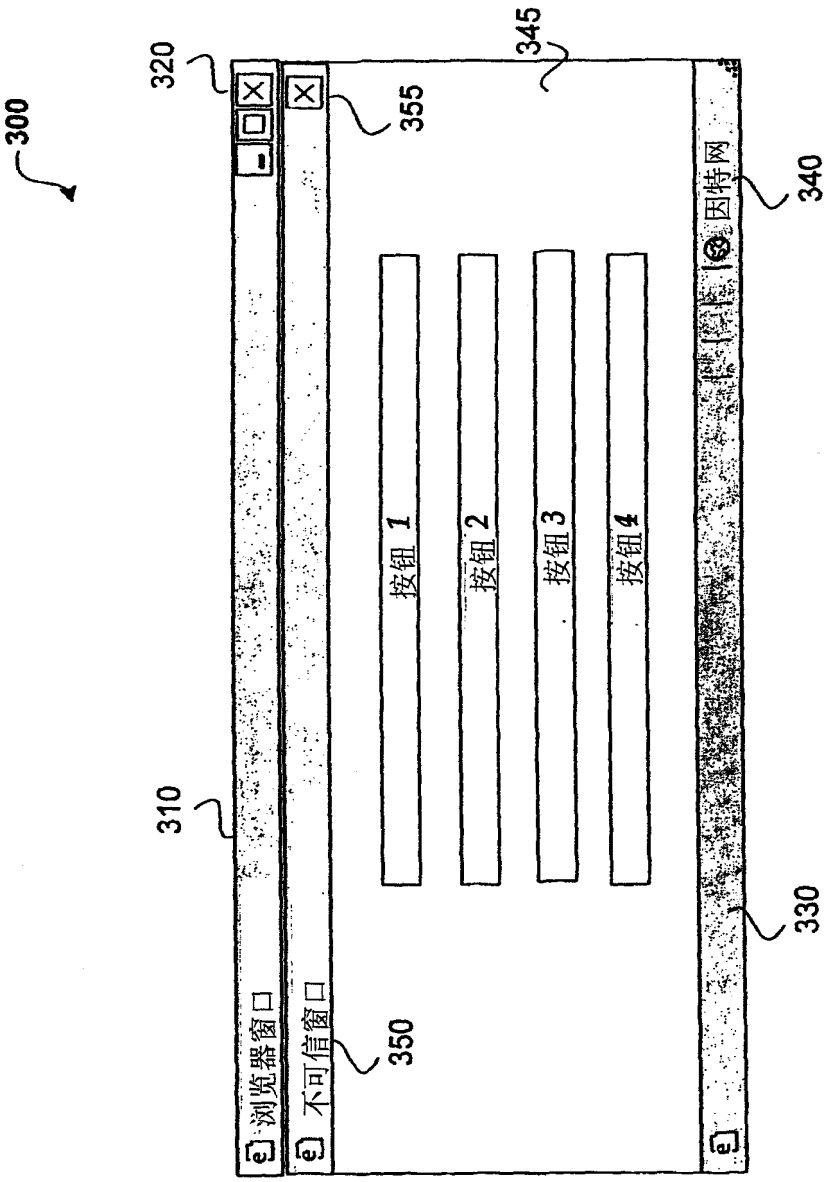


图 3

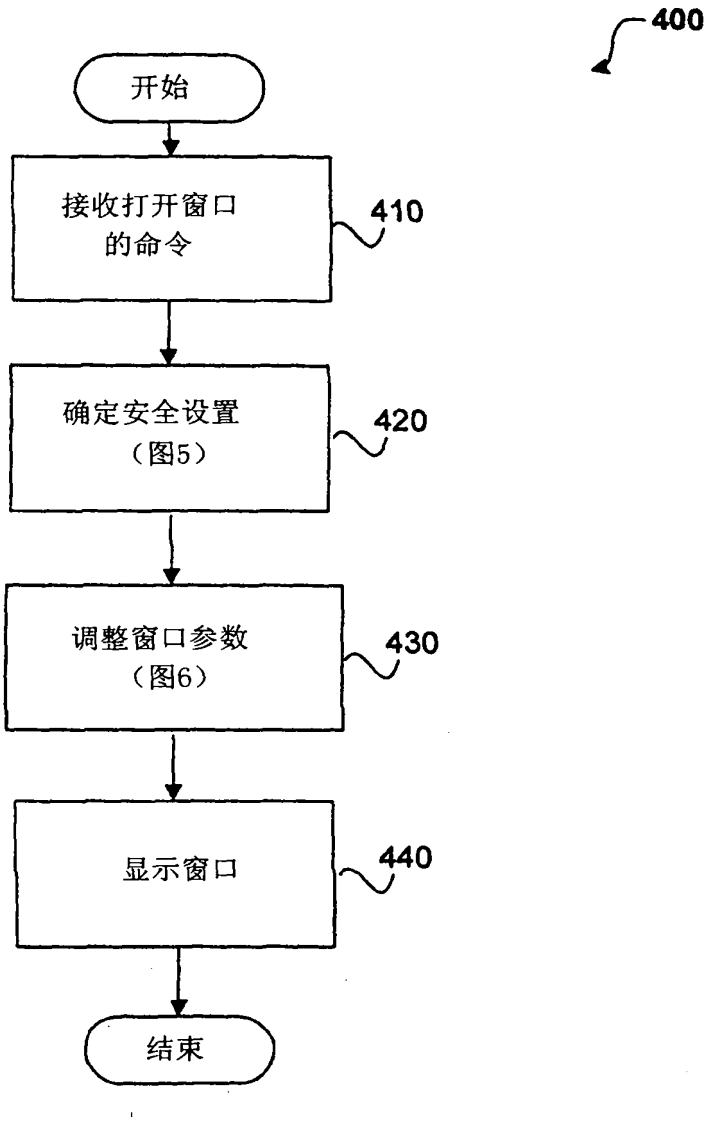


图 4

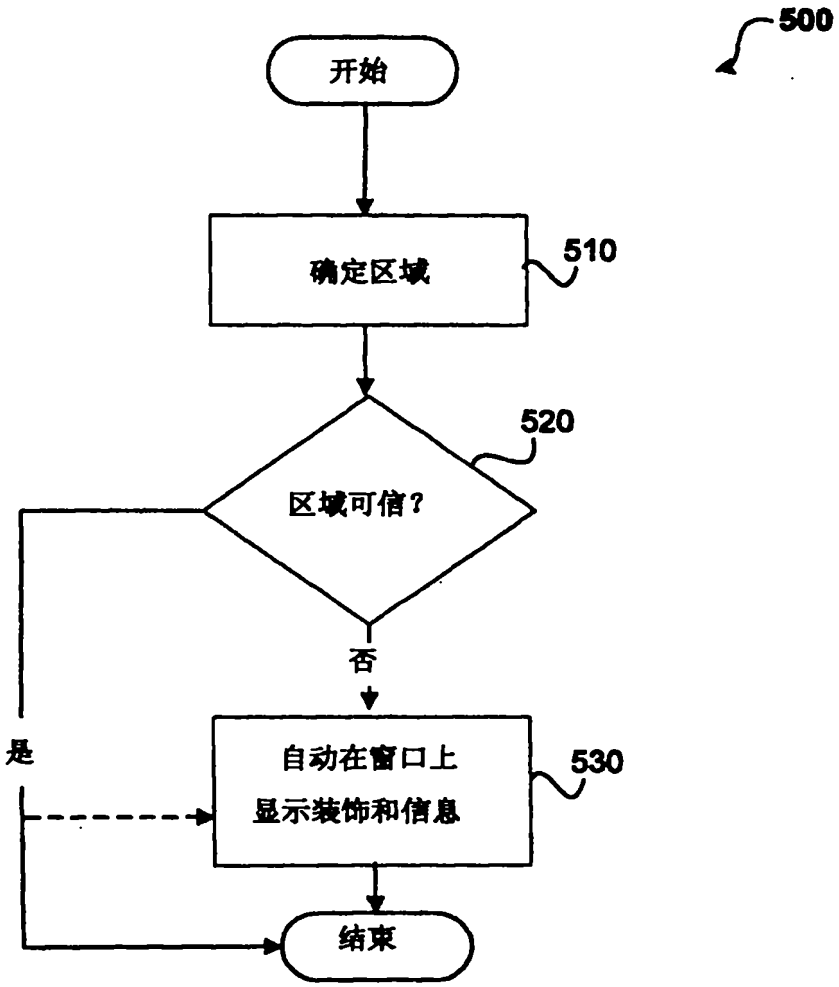


图 5

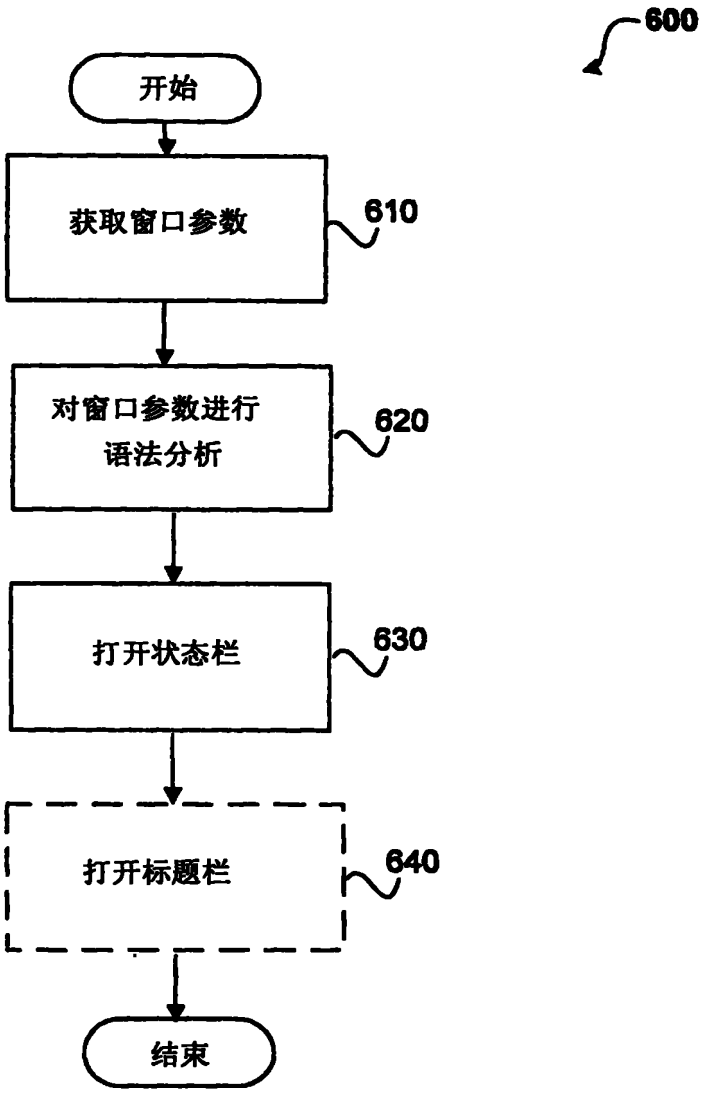


图 6