(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 101490691 B
(45)授权公告日 2013.04.17

(21)申请号 200780027306.4
(22)申请日 2007.08.03
(30)优先权数据
11/464,581 2006.08.15 US
(85)PCT申请进入国家阶段日
2009.01.19
(86)PCT申请的申请数据
PCT/EP2007/058088 2007.08.03
(87)PCT申请的公布数据
WO2008/019961 EN 2008.02.21
(73)专利权人 国际商业机器公司
地址 美国纽约
(72)发明人 G·J·博斯 G·陈
R·A·哈密尔顿二世 J·S·兰福德
(74)专利代理机构 北京市中咨律师事务所 11247
代理人 于静 李峥
(51)Int.Cl.
G06F 21/52(2013.01)
审查员 苏珊珊

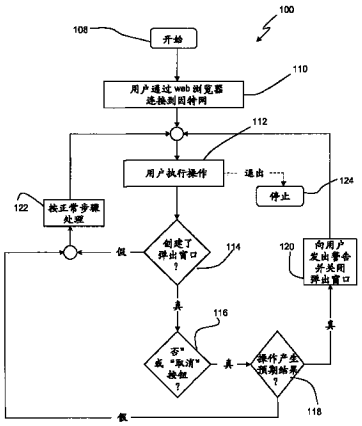
权利要求书 1 页 说明书 6 页 附图 5 页

(54)发明名称

检测欺骗命令按钮的方法和系统

(57)摘要

本发明是用于检测弹出窗口中的欺骗命令按钮的解决方案。所述解决方案跟踪所述弹出窗口的创建过程，检测所述弹出窗口中命令按钮的存在，检验所述弹出窗口中的每个命令按钮上所标记的值，以及确定选择所述弹出窗口上的命令按钮后所生成的后续操作。



CN 101490691 B

1. 一种用于检测欺骗命令按钮的方法，所述方法包括以下步骤：

跟踪弹出窗口的创建过程；

检测是否作为所述弹出窗口的一部分来创建命令按钮；

将所述命令按钮的赋值与“否”或“取消”按钮的值进行比较；

当比较结果为匹配时，确定在选择所述命令按钮时生成的后续操作；

对所生成的后续操作将关闭所述弹出窗口进行验证；以及

当选择所述命令按钮后的后续操作为关闭所述弹出窗口以外的其他操作时，警告用户所述弹出窗口可能导致潜在危险。

2. 根据权利要求 1 的方法，其中检测步骤包括执行后台源代码验证。

3. 根据权利要求 2 的方法，还包括以下步骤：未使用可以与关闭弹出窗口的“否”或“取消”按钮的值比较的值来创建命令按钮时，警告用户谨慎继续。

4. 一种用于检测欺骗命令按钮的系统，所述系统包括：

用于跟踪弹出窗口的创建过程的组件；

用于检测是否作为所述弹出窗口的一部分来创建命令按钮的组件；

用于将所述命令按钮的赋值与“否”或“取消”按钮的值进行比较的组件；

用于当比较结果为匹配时确定在选择所述命令按钮时生成的后续操作的组件；

用于对所生成的后续操作将关闭所述弹出窗口进行验证的组件；

用于当所述后续操作执行关闭所述弹出窗口以外的其他操作时，警告用户所述弹出窗口可能导致潜在危险的组件。

5. 根据权利要求 4 的系统，其中用于检测的组件执行后台源代码验证。

6. 根据权利要求 4 的系统，还包括用于未使用可以与关闭弹出窗口的“否”或“取消”按钮的值比较的值来创建命令按钮时，警告用户谨慎继续的组件。

7. 根据权利要求 4 的系统，还包括：

用于根据关闭窗口的 Web 浏览器应用程序接口 (API) 来验证所述弹出窗口的组件；

用于在检测到用户选择所述命令按钮之后所生成的后续操作无法与所述 Web 浏览器 API 通信时向用户发出警告的组件；以及

用于关闭所述弹出窗口的组件。

检测欺骗命令按钮的方法和系统

技术领域

[0001] 本发明一般地涉及避免因特网上广告的不良影响。具体地说，本发明涉及检测在联机会话期间由选择 Web 浏览器中弹出广告窗口上的命令按钮而可能触发的任何不良后续操作。更具体地说，本发明涉及阻止由关闭此类弹出窗口而触发的不良后续操作。

[0002] 背景技术

[0003] 在通常的因特网联机会话中，用户会遇到宣传所有可能的产品和服务种类的弹出窗口。这些广告通常作为独立的窗口在当前 Web 浏览器窗口的顶部“弹出”。有些弹出广告是无害的并且可以通过单击作为弹出窗口一部分提供的命令按钮而容易地关闭。但是，另外一些弹出窗口可能带有欺骗命令按钮。这些欺骗命令按钮可能触发隐藏的操作（如安装间谍软件、广告软件，窃取计算机周期，通过用户的计算机发送垃圾邮件）或其他不良应用。图 3 是似乎警告广告软件和间谍软件的弹出窗口的实例，但是该窗口本身可能具有无论选择“是”还是“否”按钮，都会安装恶意程序的欺骗按钮。尽管弹出广告可能具有由系统提供的无法进行欺骗的“取消”按钮，即窗口角落上的“X”按钮，但是此类由系统提供的按钮可能处于灰显、隐藏或禁用状态。某些用户可能不知道显式命令按钮和系统提供的“取消”按钮之间的区别。另外还有一些弹出窗口除了诸如“是”或“确认”按钮之类的肯定命令按钮以外，不提供任何关闭弹出窗口的命令按钮。图 4 是此类弹出窗口的实例。这限制了用户关闭弹出窗口的选择，其不可避免地触发用户未知的潜在不良后续操作。在尝试关闭此类恶意弹出窗口时，计算机用户面临着授权恶意操作的危险，计算机会将此恶意操作视为 由用户有意做出的操作。

[0004] 当前提供了避免恶意弹出窗口的方法，例如在用户明确给出下载程序的命令时扫描恶意程序代码，其中通过在下载程序代码之前与现有的程序集进行比较来执行扫描操作。另外还提供了一种通过将用户输入从错误的 Java 小程序转向主浏览器循环，并接收用户按键命令以关闭窗口来避开由该小程序生成的显示模型对话框的方法。此现有技术涉及使用 Java 编程语言创建的模型对话框。

[0005] 因此，需要克服相关技术中的至少一种上述缺点和 / 或限制。

发明内容

[0006] 本发明提供了一种用于检测弹出窗口中的欺骗命令按钮和 / 或预先警告用户在选择欺骗命令按钮以关闭弹出窗口时的潜在危害的方法、系统和计算机程序产品。

[0007] 本发明的第一方面提供了一种用于检测欺骗命令按钮的方法，所述方法包括下列步骤：跟踪弹出窗口创建过程；检测在所述弹出窗口中创建的命令按钮；检查所述命令按钮的赋值；以及确定在选择所述命令按钮时生成的后续操作。

[0008] 优选地，本发明提供了一种方法，其中所述检测步骤包括执行后台源代码验证。

[0009] 优选地，本发明提供了一种方法，所述方法还包括以下步骤：验证所生成的后续操作将关闭所述弹出窗口。

[0010] 优选地，本发明提供了一种方法，所述方法还包括以下步骤：当选择所述命令按钮

后的后续操作为关闭所述弹出窗口以外的其他操作时，警告用户所述弹出窗口可能导致潜在危险。

[0011] 优选地，本发明提供了一种方法，所述方法还包括以下步骤：当所述命令按钮的赋值限制用户选择时，警告用户谨慎继续。

[0012] 本发明的第二方面提供了一种用于检测欺骗命令按钮的方法，所述方法包括：根据关闭窗口的Web浏览器应用程序接口(API)来验证弹出窗 口的关闭操作以检测异常；以及在检测到用户选择所述命令按钮之后所生成的后续操作无法与所述Web浏览器API通信时向用户发出警告。

[0013] 优选地，本发明提供了一种方法，所述方法还包括以下步骤：在警告用户时关闭所述弹出窗口。

[0014] 本发明的第三方面提供了一种用于检测欺骗命令按钮的系统，所述系统包括：用于跟踪弹出窗口创建过程的组件；用于检测在所述弹出窗口中创建命令按钮的组件；用于检查所述命令按钮的赋值的组件；以及用于确定在选择所述命令按钮时生成的后续操作的组件。所述系统是可以作为插件、扩展、代理或任何可以与Web浏览器一起应用的装置而添加到现有计算机程序的计算机程序。

[0015] 优选地，本发明提供了一种系统，其中用于检测的组件执行后台源代码验证。

[0016] 优选地，本发明提供了一种系统，所述系统还包括用于验证所生成的后续操作将关闭所述弹出窗口的组件。

[0017] 优选地，本发明提供了一种系统，所述系统还包括用于当所述后续操作执行关闭所述弹出窗口以外的其他操作时，警告用户所述弹出窗口可能导致潜在危险的组件。

[0018] 优选地，本发明提供了一种系统，所述系统还包括用于当所述命令按钮的赋值限制用户选择时，警告用户谨慎继续的组件。

[0019] 优选地，本发明提供了一种系统，所述系统还包括：用于根据关闭窗口的Web浏览器应用程序接口(API)来验证所述弹出窗口的组件；用于在检测到用户选择所述命令按钮之后所生成的后续操作无法与所述Web浏览器API通信时向用户发出警告的组件；以及用于关闭所述弹出窗口的组件。

[0020] 本发明的第四方面提供了一种存储在机器可读介质中的用于检测欺骗命令按钮的计算机程序，所述计算机可读程序执行下列操作：跟踪弹出窗口创建过程；检测在所述弹出窗口中创建的命令按钮；检查所述命令按钮的赋值；以及确定在选择所述命令按钮时生成的后续操作。

[0021] 本发明的第五方面提供了一种部署用于检测欺骗命令按钮的应用的方法，所述方法包括：提供可执行下列操作的计算机基础结构：跟踪弹出窗口创建过程；检测在所述弹出窗口中创建的命令按钮；检查所述命令按钮的赋值；以及确定在选择所述命令按钮时生成的后续操作。

附图说明

[0022] 附图是示出本发明的典型实施例的示意表示，其并非旨在限制本发明的原理。在附图中，相同的标号表示各个图中的相同元素：

[0023] 图1是示出本发明的一个实施例的算法的流程图；

[0024] 图 2 是示出本发明的备选实施例的算法的流程图；

[0025] 图 3 是示出提供命令按钮以供用户选择以关闭弹出窗口的常见广告的示例弹出窗口；

[0026] 图 4 是示出限制关闭弹出窗口的用户选择的另一示例弹出窗口；

[0027] 图 5 是示出本发明的另一实施例的算法的流程图；

[0028] 图 6 示出了用于实现本发明的一个或多个实施例的示例性计算机系统。

具体实施方式

[0029] 已采用各种方法来防止恶意代码执行各种操作，但是仍需要提供一种方法来检测恶意代码并警告用户：如果用户发出关闭弹出窗口的命令，可能将恶意代码安装到计算机内。

[0030] 现在参考附图，图 1 示出了用于检测带有欺骗命令按钮的弹出窗口的算法 100 的过程流。欺骗按钮是单击按钮之后所产生的结果不会返回预期结果的按钮。欺骗命令按钮的外观与常见命令按钮的外观相同，通常在弹出窗口中成对出现（例如，图 3 中示出的“是”和“否”）。用户被诱导相信此类命令按钮提供了仅通过单击按钮便可发出所需命令的途径。但是，单击弹出窗口上的命令按钮可能触发其他操作。开始 108 之后，当通过 Web 浏览器连接到因特网 110 时，算法 100 处于备用状态。当用户在因特 网的联机会话期间执行操作 112 时，算法 100 跟踪打开窗口（例如 Java 中的“window.open”）的调用以判定 114 是否正在创建弹出窗口。算法 100 包括步骤 116 以通过执行后台页面源代码验证来检测是否作为弹出窗口的一部分来创建命令按钮。将命令按钮的值与“否”或“取消”按钮的值进行比较。当值匹配时，将执行进一步的检查 118 来判定单击命令按钮之后的后续操作是否只是“返回假 (False)”（例如，在不执行任何其他操作的情况下关闭窗口）。如果是，将在没有任何中断的情况下处理 122 后续操作。但是，如果后续操作不是“返回假”，将会警告用户注意欺骗命令按钮，并由系统自动关闭弹出窗口 120。这可防止用户单击欺骗按钮，从而最大程度上减小触发与单击欺骗按钮关联的恶意后续操作的风险。算法 100 然后被再次重置为备用以等待触发新弹出窗口创建的另一用户操作。如果判定 114 未创建弹出窗口，则算法 100 在 Web 浏览器如期望的那样处理用户命令 122 时返回备用模式。如果用户选择退出联机会话，则算法 100 将对命令进行注册并停止检测弹出窗口的创建 124。

[0031] 在图 2 中，除了图 1 内的算法 100 中列出的过程流之外，算法 200 还具有在逻辑步骤 116 之后的额外过程流 202 以解决弹出窗口未提供“取消”按钮的情况。这实质上意味着未使用可以与关闭弹出窗口的“否”或“取消”按钮的值比较的值来创建命令按钮。但是，弹出窗口可能包括限制用户选择的命令按钮，从而导致必须遵从并增加触发恶意或不希望出现的后续操作的风险。尽管未向用户提供选择以使用专门执行弹出窗口关闭操作的命令按钮来关闭弹出窗口，但是 Web 浏览器将通过类似如下的消息预先警告用户：“您正在浏览的弹出窗口不具有相应的取消功能，请谨慎继续”。但是，Web 浏览器将不采取额外操作来最大程度上减小处理用户发出的命令时的风险。备选地，将在不对用户进行警告的情况下处理命令。

[0032] 图 5 示出了本发明的另一实施例，其中提供了用于在过程流中根据关闭窗口的标准操作系统 (OS) 或 Web 浏览器应用程序接口 (API) 来验证关闭操作的算法 300。从步骤

116 或步骤 118 到步骤 122 的过程流还包括另一步骤 302，该步骤根据 API 的 OS 验证由命令按钮发出的关闭操作以 检测任何异常。当关闭弹出窗口的命令按钮未调用 Web 浏览器 API 时，则将此情况检测为异常。算法 300 然后向用户发送警告消息并自动关闭弹出窗口 120。该备选步骤 302 可以作为上述算法 100 或 200 的替代算法独立应用或者作为防止任何意外选择欺骗命令按钮的防护措施独立应用。作为防护措施，可以在逻辑步骤 122 之前立即实现此算法 300，以确保即使命令按钮似乎没有欺骗迹象，但是假如后续操作的行为未遵循预期的操作模式，则将对用户发出警告并且 Web 浏览器将立即关闭弹出窗口。

[0033] 因此，需要一种使得 Web 浏览器能够阻止弹出广告窗口中的按钮欺骗的方法。还需要一种能够添加到现有因特网 Web 浏览器程序中的可执行系统，以检测当用户选择作为弹出窗口的一部分提供的欺骗命令按钮时执行的恶意代码。进一步需要一种可以预先警告用户选择弹出窗口上的欺骗命令按钮之后可能的意外操作的可执行系统。

[0034] 图 6 示出了根据本发明的一个或多个实施例的用于检测弹出窗口中的欺骗命令按钮并当选择欺骗命令按钮时预先警告用户潜在危害的示例性系统 400。在此方面，系统 400 包括可以执行此处所述的用于检测欺骗命令按钮的各种过程的计算机基础结构 402。具体地说，计算机基础结构 402 被示为包括计算机系统 404，计算机系统 404 包括欺骗命令按钮检测系统 430，其使得计算机系统 404 能够通过执行本发明的过程步骤在创建弹出窗口时检测欺骗命令按钮的创建。

[0035] 所示的计算机系统 404 包括处理单元 408、存储器 410、至少一个输入 / 输出 (I/O) 接口 414 以及总线 412。进而，计算机系统 404 被示为与至少一个外部设备 416 和存储系统 418 通信。通常，处理单元 408 执行诸如欺骗命令按钮检测系统 430 之类的存储在存储器 410 和 / 或存储系统 418 中的计算机程序代码。在执行计算机程序代码时，处理单元 408 可以从存储器 410、存储系统 418 和 / 或 I/O 接口 414 读取数据和 / 或将数据写入上述元件。总线 412 提供计算机系统 404 中的各个组件之间的通信链路。至少一个外部设备 416 可以包括允许用户（未示出）与计算机系统 404 交互的任何设备（例如显示器 420）或允许计算机系统 404 与一个或多个其他计算机系 统通信的任何设备。

[0036] 在任何情况下，计算机系统 404 都可以包括能够执行由用户安装的计算机程序代码的任何通用计算制品（例如，个人计算机、服务器、手持设备等）。但是可以理解，计算机系统 404 和欺骗命令按钮检测系统 430 只是可以执行本发明的各个过程步骤的各种可能计算机系统的代表。在此方面，在其他实施例中，计算机系统 404 可以包括包含用于执行特定功能的硬件和 / 或计算机程序代码的任何专用计算制品、包括专用和通用硬件 / 软件的组合任何计算制品等。在每种情况下，都可以使用标准编程和工程技术分别创建程序代码和硬件。

[0037] 类似地，计算机基础结构 402 只是可用于实现本发明的各类计算机基础结构的示例。例如，在一个实施例中，计算机基础结构 402 包括通过诸如网络、共享存储器之类的任意类型的有线和 / 或无线通信链路通信以执行本发明的各个过程步骤的两个或更多计算机系统（例如，服务器群集）。当通信链路包括网络时，所述网络可以包括一个或多个网络类型（例如，因特网、广域网、局域网、虚拟专用网等）的任意组合。无论如何，计算机系统之间的通信都可以利用各种类型的传输技术的任意组合。

[0038] 如上所述，当用户选择弹出窗口 434 的命令按钮时，欺骗命令按钮检测系统 430 使

得计算机系统 404 能够执行返回“假”操作检查 432。所述弹出窗口在 Web 浏览器 440 内“弹出”。在此方面，欺骗命令按钮检测系统 430 被示为包括用于检测 Web 浏览器 440 上弹出窗口 434 的生成的弹出窗口创建检测系统 436，以及包括用于根据命令按钮的赋值，针对弹出窗口 434 中的每个命令按钮执行返回“假”操作检查 432 的命令按钮创建系统 438。上面讨论了这些系统中的每个系统的操作。可以理解，图 6 中示出的各种系统中的某些系统可以针对通过网络通信的一个或多个单独计算机系统 404 而单独实现、组合实现和 / 或存储在存储器中。进而可以理解，可以不实现某些系统和 / 或功能，或者可以将其他系统和 / 或功能包括为系统 400 的一部分。

[0039] 尽管在此示出和描述为用于检测弹出窗口中的命令按钮是否为欺骗按 钮的方法和系统，但是可以理解，本发明还提供了各种备选实施例。例如，在一个实施例中，本发明提供了一种包括计算机程序代码的计算机可读介质，所述计算机程序代码使得计算机基础结构能够确定在选择弹出窗口的命令按钮时触发的后续操作。在此方面，所述计算机可读介质包括诸如欺骗命令按钮检测系统 430 之类的实现本发明的各个过程步骤中每个步骤的程序代码。可以理解，术语“计算机可读介质”包括一个或多个任意类型的程序代码的物理实施例。具体地说，所述计算机可读介质包括包含在一个或多个便携存储制品（例如，光盘、磁盘、磁带等）、诸如存储器 410 和 / 或存储系统 418（例如，硬盘、只读存储器、随机存取存储器、高速缓冲存储器等）之类的一个或多个计算机系统数据存储部分上的程序代码，和 / 或包括为通过网络传输的数据信号（例如，在程序代码的有线 / 无线电子分发期间）的程序代码。

[0040] 在另一实施例中，本发明提供了一种在订阅、广告和 / 或收费的基础上执行本发明的过程步骤的商业方法。也就是说，服务提供商可以提供服务以判定弹出窗口是否带有当用户选择命令按钮时会触发恶意操作的欺骗命令按钮。在此情况下，服务器提供商可以为一个或多个客户创建、维护、支持诸如计算机基础结构 402 之类的执行本发明的过程步骤的计算机基础结构。作为回报，服务器提供商可以根据订阅和 / 或收费协议向客户（多个）收费，以及 / 或者服务器提供商可以通过向一个或多个第三方销售广告空间来收费。

[0041] 在另一实施例中，本发明提供了一种用于检测弹出窗口的欺骗命令按钮的方法。在这种情况下，可以获取（例如，创建、维护、提供等）诸如计算机基础结构 402 之类的计算机基础结构并且可以获取（例如，创建、购买、使用、修改等）一个或多个用于执行本发明的过程步骤的系统并将所述系统部署到计算机基础结构。在此方面，每个系统的部署可以包括下列一个或多个操作 :(1) 从计算机可读介质将程序代码安装在诸如计算机系统 404 之类的计算机系统中 ;(2) 将一个或多个计算机系统添加到计算机基础结构 ;以及 (3) 结合和 / 或修改计算机基础结构的一个或多个现有 系统以使得所述计算机基础结构能够执行本发明的过程步骤。

[0042] 如此处使用的，可以理解术语“程序代码”和“计算机程序代码”为同义词并表示一组指令的以任何语言、代码或符号表示的任何表达，所述指令旨在使具有信息处理功能的计算机系统直接执行特定功能，或者执行以下两者之一或全部后执行特定功能 :a) 转换为另一种语言、代码或符号 ;以及 b) 以不同的材料形式再现。在此方面，程序代码可以体现为一种或多种类型的程序产品，例如应用程序 / 软件程序、组件软件 / 功能库、操作系统、用于特定计算的基本 I/O 系统 / 驱动器和 / 或 I/O 设备等。

[0043] 尽管此处描述了本发明的优选实施例，但是上述描述只是示例性的。其并非旨在是穷举的或将本发明限于所公开的精确形式。显而易见，许多修改和变化都是可能的。相应领域中的技术人员可想到对此处描述的本发明的进一步修改，并且所有此类修改都被视为在所附权利要求限定的本发明的范围之内。

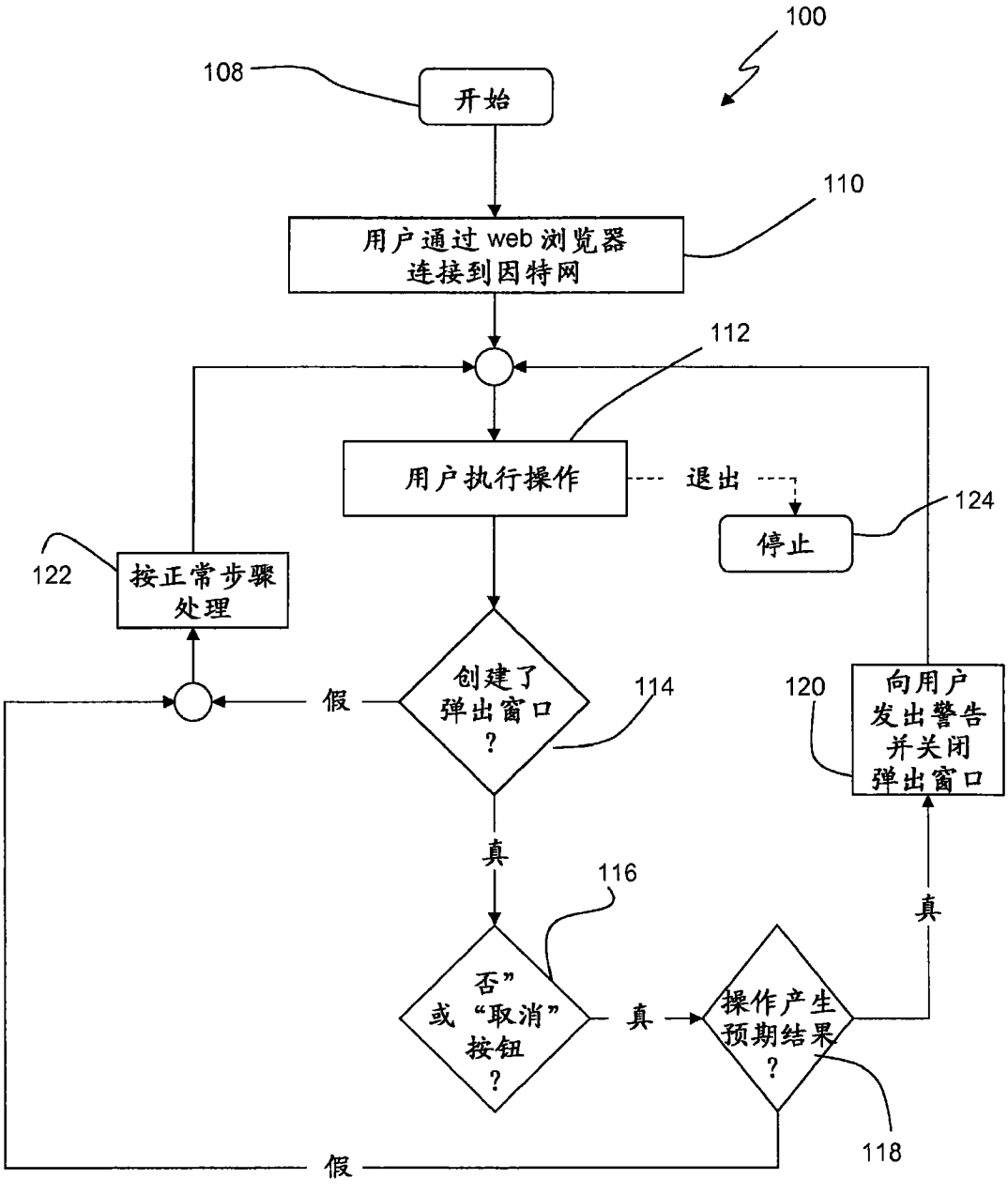

100
108
开始
110
用户通过 web 浏览器
连接到因特网
112
用户执行操作
退出
124
停止
122
按正常步骤
处理
假
创建了
弹出窗口
?
114
120
向用户
发出警告
并关闭
弹出窗口
真
116
真
否”
或“取消”
按钮
?
真
操作产生
预期结果
?
118
假

图 1

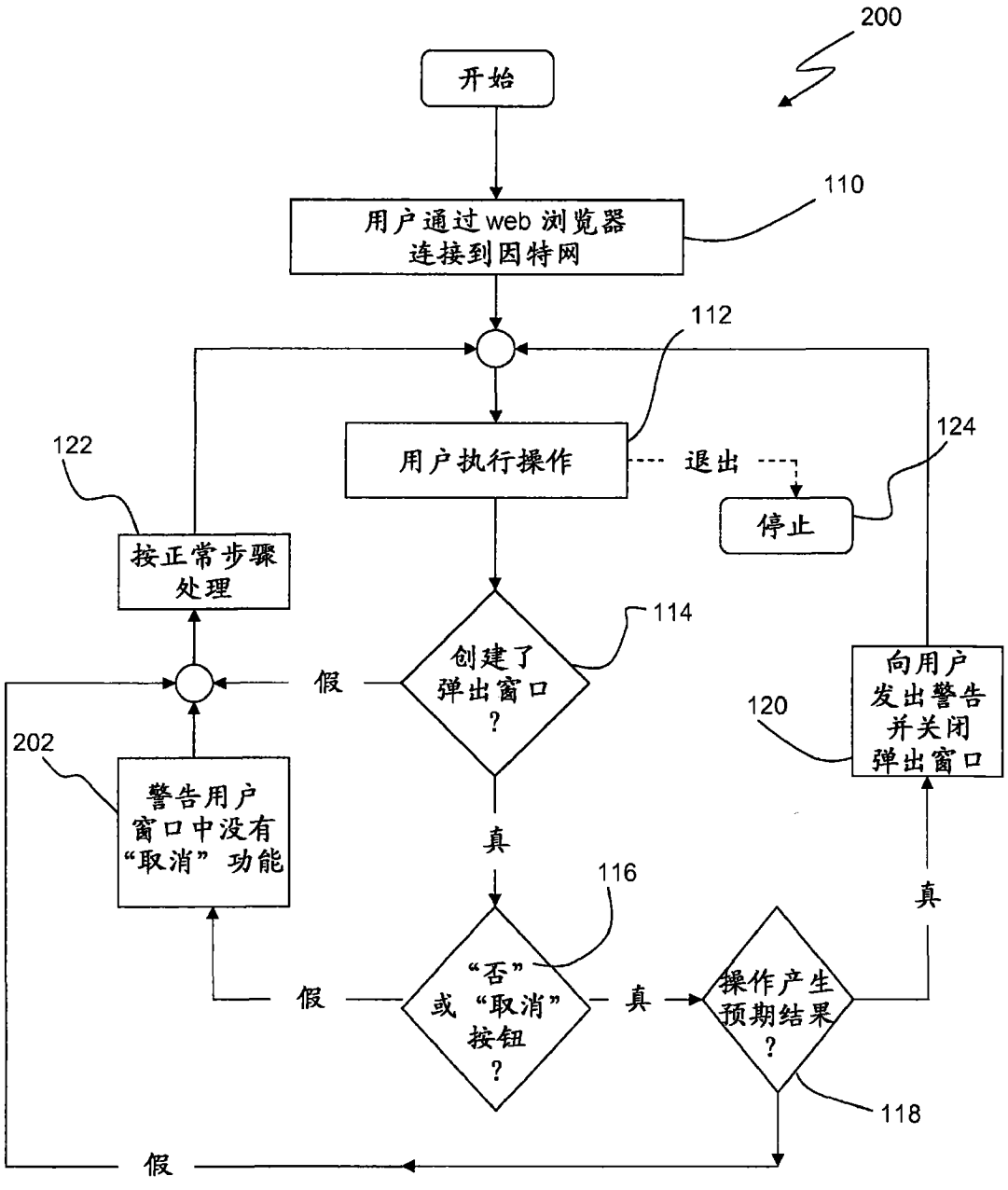

200
开始
110
用户通过web浏览器
连接到因特网
112
用户执行操作
退出
124
停止
122
按正常步骤
处理
114
创建了
弹出窗口
?
假
120
向用户
发出警告
并关闭
弹出窗口
202
警告用户
窗口中没有
“取消”功能
真
116
“否”
或“取消”
按钮
?
假
真
操作产生
预期结果
?
真
118
假

图 2

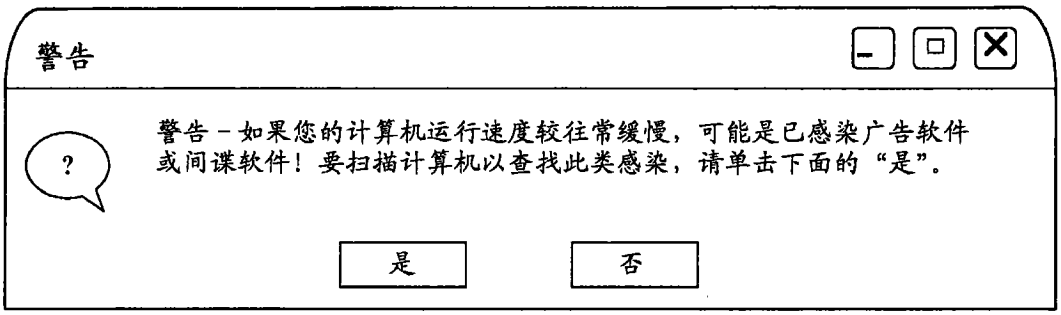

警告
?
警告－如果您的计算机运行速度较往常缓慢，可能是已感染广告软件或间谍软件！要扫描计算机以查找此类感染，请单击下面的“是”。
是
否

图 3

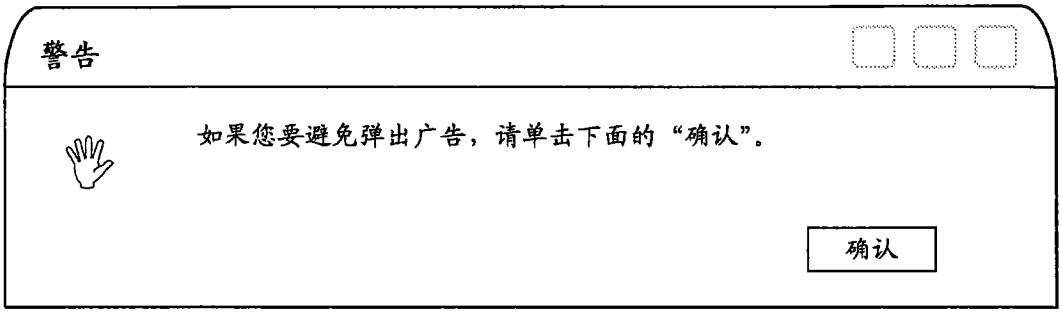

警告
如果您要避免弹出广告，请单击下面的“确认”。
确认

图 4

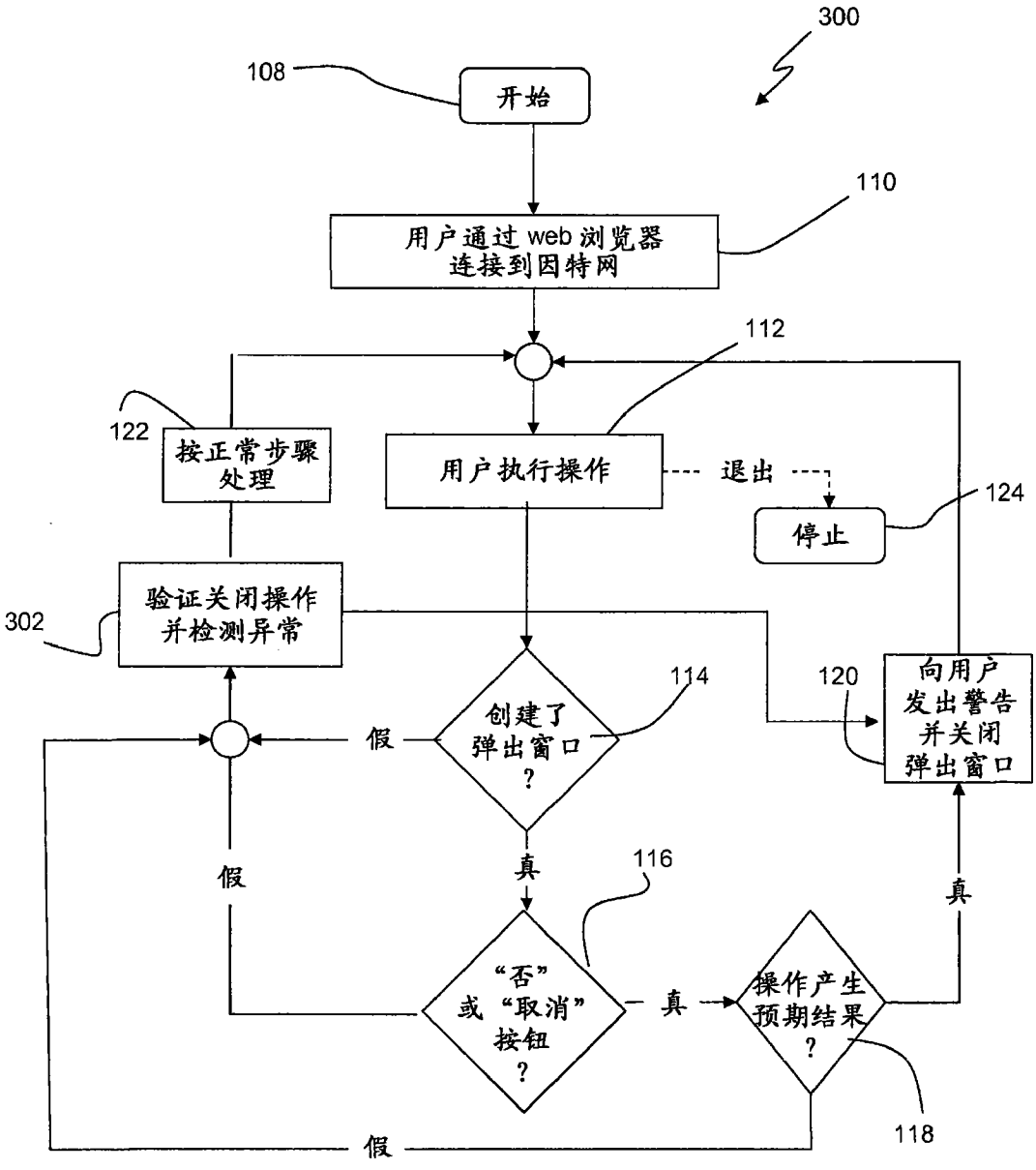

300
108
开始
110
用户通过 web 浏览器
连接到因特网
112
122
按正常步骤
处理
用户执行操作
退出
124
停止
验证关闭操作
并检测异常
302
114
创建了
弹出窗口
?
假
120
向用户
发出警告
并关闭
弹出窗口
真
116
假
真
“否”
或“取消”
按钮
?
真
操作产生
预期结果
?
118
假

图 5

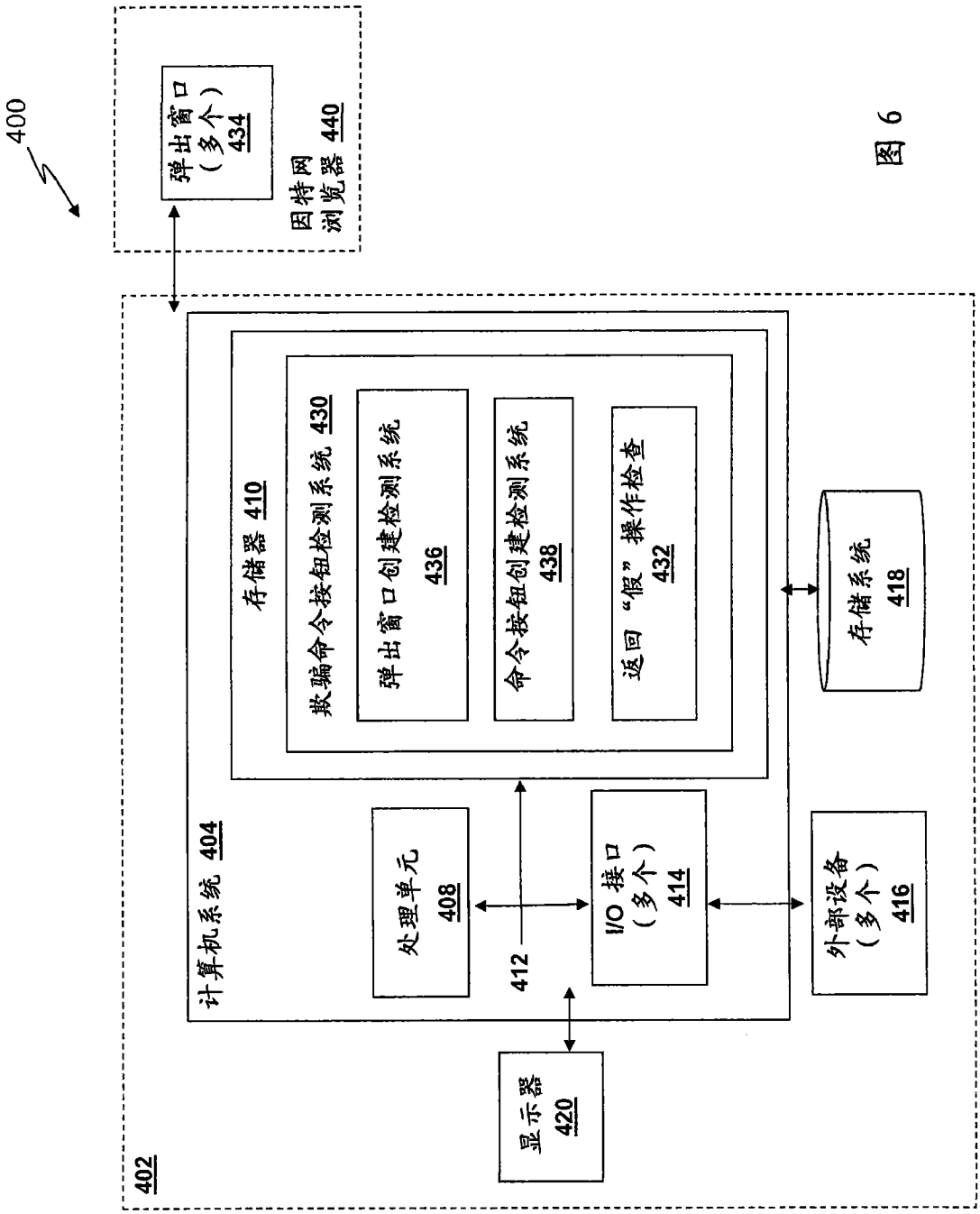

400
弹出窗口（多个）434
因特网浏览器 440
402
计算机系统 404
存储器 410
欺骗命令按钮检测系统 430
弹出窗口创建检测系统 436
命令按钮创建检测系统 438
返回“假”操作检查 432
处理单元 408
412
I/O 接口（多个）414
显示器 420
外部设备（多个）416
存储系统 418

图 6