(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108140088 A
(43)申请公布日 2018.06.08

(21)申请号 201680058739.5

(22)申请日 2016.11.28

(30)优先权数据
15/173,778 2016.06.06 US

(85)PCT国际申请进入国家阶段日
2018.04.08

(86)PCT国际申请的申请数据
PCT/US2016/063862 2016.11.28

(87)PCT国际申请的公布数据
WO2017/213688 EN 2017.12.14

(71)申请人 谷歌有限责任公司
地址 美国加利福尼亚州

(72)发明人 H.M.戈登 M.S.布雷斯西 小威廉.M.哈尔平

(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 邵亚丽

(51)Int.Cl.
G06F 21/55(2006.01)
G06F 21/56(2006.01)

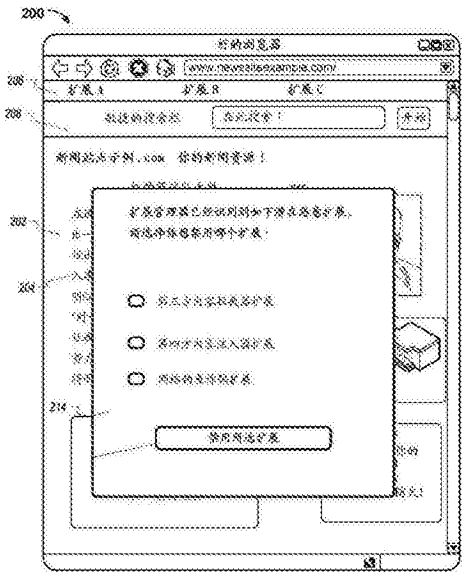
权利要求书2页 说明书15页 附图5页

(54)发明名称

禁用恶意浏览器扩展

(57)摘要

扩展管理器可以识别安装在计算设备上的浏览器扩展被配置为修改浏览器应用程序的操作。扩展管理器可以基于浏览器扩展修改在浏览器应用程序内呈现的内容的方式确定浏览器扩展是恶意浏览器扩展。响应于确定浏览器扩展是恶意浏览器扩展，所述扩展管理器可以禁用浏览器扩展，并且然后启动从计算设备卸载扩展管理器的卸载过程。



CN 108140088 A

1.一种方法,包括:

通过扩展管理器识别安装在计算设备上的浏览器扩展被配置为修改浏览器应用程序的操作;

基于所述浏览器扩展修改在所述浏览器应用程序内呈现的内容的方式,由所述扩展管理器确定所述浏览器扩展是恶意浏览器扩展;

响应于确定所述浏览器扩展是恶意浏览器扩展,由所述扩展管理器在所述浏览器应用程序内禁用所述浏览器扩展,其中,禁用所述浏览器扩展防止所述浏览器扩展修改所述浏览器应用程序内呈现的内容;

在完成禁用所述浏览器扩展时,由所述扩展管理器启动从所述计算设备卸载所述扩展管理器的卸载过程。

2.根据权利要求1所述的方法,还包括:

在所述计算设备处呈现的用户界面内提供将所述浏览器扩展识别为恶意浏览器扩展的文本或图形信息的视觉显示;以及

响应于将所述浏览器扩展识别为恶意浏览器扩展的所述文本或图形信息的显示,接收请求禁用所述浏览器扩展的用户输入;

其中,响应于通过在所述计算设备处呈现的所述用户界面接收请求禁用所述浏览器扩展的用户输入,执行由所述扩展管理器禁用所述浏览器扩展。

3.根据前述权利要求中任一项所述的方法,其中,禁用所述浏览器扩展包括卸载所述浏览器扩展。

4.根据前述权利要求中任一项所述的方法,其中,确定所述浏览器扩展是恶意浏览器扩展包括:

由所述扩展管理器访问存储设备,所述存储设备存储先前已被识别为修改所述浏览器应用程序内呈现的内容的浏览器扩展的一系列恶意浏览器扩展;以及

确定所述浏览器扩展包括在存储在所述存储设备中的所述一系列恶意浏览器扩展中。

5.根据前述权利要求中任一项所述的方法,其中,确定所述浏览器扩展是恶意浏览器扩展包括:

确定所述浏览器扩展将未授权内容插入到从给定网络位置获得的并显示在所述浏览器应用程序内的主要内容的显示中,其中,所述未授权内容从不同于所述主要内容的所述给定网络位置的网络位置获得。

6.根据前述权利要求中任一项所述的方法,其中,确定所述浏览器扩展是恶意浏览器扩展包括:

确定所述浏览器扩展阻止显示由所述计算设备获得的授权内容,用于由所述浏览器应用程序显示,其中,所述授权内容是包括在通过所述浏览器应用程序请求的给定网页中的主要内容或通过执行所述给定网页的代码由所述浏览器应用程序请求的第三方内容中的一个。

7.根据前述权利要求中任一项所述的方法,其中,确定所述浏览器扩展是恶意浏览器扩展包括:

确定所述浏览器扩展是第四方搜索栏扩展,其将搜索栏显示为所述浏览器应用程序的所述显示的一部分。

8.根据前述权利要求中任一项所述的方法，其中，确定所述浏览器扩展是恶意浏览器扩展包括：

确定所述浏览器扩展独立于来自所述用户的请求或者通过执行包括在由所述用户请求的用于此种通信的给定网页中的代码与外部服务器通信。

9.一种计算设备，包括：

存储器，其用于存储数据和指令；和

一个或多个处理器，其执行存储在所述存储器上的指令，其中，所述指令使所述一个或多个处理器执行被配置为执行根据前述权利要求中任一项所述方法的扩展管理器。

10.一种用计算机程序编码的计算机存储介质，所述程序包括在由数据处理装置执行时使所述数据处理装置执行包括根据权利要求1至8中任一项所述的方法的操作的指令。

禁用恶意浏览器扩展

技术领域

[0001] 本文档总体涉及自动识别和禁用恶意且不需要的计算扩展。

背景技术

[0002] 互联网促进了跨全球的用户之间的信息交流和交易。计算系统使用网络浏览器向用户呈现内容。用户可能有意或无意地在计算机上安装软件，并且该软件可以改变由浏览器呈现的信息的呈现或以其他方式改变浏览器的操作或改变浏览器与安装在其上的计算机或远程计算系统的交互。改变浏览器的操作的软件可以被称为安装在浏览器上的“浏览器扩展(browser extension)”。

发明内容

[0003] 本文档描述了用于自动识别和禁用恶意或其他不想要或不期望的浏览器扩展(统称为恶意扩展)的技术、方法、系统和其他机制。通常，安装在计算设备上的浏览器扩展管理器可以使用一种或多种用于识别恶意浏览器扩展的技术来将安装在计算设备的浏览器上的一个或多个浏览器扩展识别为恶意浏览器扩展，如下所讨论的。扩展管理器(例如，通过停用、卸载或限制对所识别的恶意浏览器扩展的访问)可以自动禁用所识别的恶意浏览器扩展。在完成对恶意浏览器扩展的禁用之后，扩展管理器可以自动从计算设备上卸载本身。

[0004] 通常，本说明书中描述的主题的一个创新方面可以用一种方法实现，该方法包括通过扩展管理器识别安装在计算设备上的浏览器扩展被配置为修改浏览器应用程序的操作；基于浏览器扩展修改在浏览器应用程序内呈现的内容的方式确定浏览器扩展是恶意浏览器扩展；响应于确定浏览器扩展是恶意浏览器扩展而禁用浏览器扩展，其中禁用浏览器扩展防止浏览器扩展修改浏览器应用程序内呈现的内容；以及在完成禁用浏览器扩展之后启动从计算设备卸载扩展管理器的卸载过程。

[0005] 这些和其他实施例中每个可以可选地包括以下特征中的一个或更多个。扩展管理器可以被进一步配置为在呈现在计算设备处的用户界面内提供将浏览器扩展识别为恶意浏览器扩展的文本或图形信息的视觉显示。计算设备可以包括用于接收用户输入的用户输入设备，该用户输入请求响应于将浏览器扩展识别为恶意浏览器扩展的文本或图形信息的显示而禁用浏览器扩展。响应于通过用户输入设备接收请求浏览器扩展被禁用的用户输入，扩展管理器可以禁用该浏览器扩展。禁用浏览器扩展可以包括卸载浏览器扩展。

[0006] 确定浏览器扩展是恶意浏览器扩展可以包括访问存储设备，该存储设备存储先前已被识别为修改浏览器应用程序内呈现的内容的浏览器扩展的一系列恶意浏览器扩展；以及确定浏览器扩展包括在存储在存储设备中的一系列恶意浏览器扩展中。确定浏览器扩展是恶意浏览器扩展可以包括确定浏览器扩展将未授权内容插入到从给定网络位置获得的并显示在浏览器应用程序内的主要内容的显示中，其中未授权内容从不同于主要内容的给定网络位置的网络位置获得。确定浏览器扩展是恶意浏览器扩展可以包括确定浏览器扩展阻止显示由计算设备获得的授权内容，用于由浏览器应用程序显示，其中授权内容是包括

在通过浏览器应用程序请求的给定网页中的主要内容或第三方内容中的一个，第三方内容通过执行给定网页的代码由浏览器应用程序请求。确定浏览器扩展是恶意浏览器扩展可以包括确定浏览器扩展是第四方搜索栏扩展，其将搜索栏显示为浏览器应用程序的显示的一部分。确定浏览器扩展是恶意浏览器扩展可以包括确定浏览器扩展独立于来自用户的请求或者通过执行包括在由用户请求的用于此种通信的给定网页中的代码与外部服务器通信。

[0007] 应理解，可以以任何便利的形式来实现各方面。例如，各方面可以通过适当的计算机程序来实现，该计算机程序可以被携带在可以是有形载体介质(例如磁盘)或无形载体介质(例如通信信号)的适当载体介质上。各方面也可以使用合适的装置来实现，该装置可以采取运行被布置为实现本发明的计算机程序的可编程计算机的形式。各方面可以被组合，以使得在一个方面的背景下描述的特征可以在另一个方面中实现。

[0008] 在某些情况下，具体实现方式可以实现以下优点中的一个或多个。恶意浏览器扩展可以在较少或没有用户输入的情况下由非复杂用户来容易识别和移除。通过自动识别和移除限制对所需内容的访问、注入不想要的内容或降低系统性能的恶意浏览器扩展，可以改进用户网页浏览体验。通过移除可能潜在访问敏感信息(例如，浏览历史记录、财务信息)并向外部计算系统提供敏感信息的恶意浏览器扩展来保护隐私。计算资源可以由于自动卸载扩展管理器而被留存。因此，实现方式可以解决与有效移除恶意浏览器扩展相关联的问题。

[0009] 在附图和下面的描述中阐述了一个或多个实现方式的细节。其他特征、目的和优点将从说明书和附图以及权利要求中显而易见。

附图说明

[0010] 图1是可以用于实现本文档中描述的系统和方法的系统的概念图。

[0011] 图2示出了显示在包含主要内容、第三方内容和不想要的第四方内容的浏览器中的示例网页。

[0012] 图3示出了在图2的示例网页上显示的示例扩展管理器对话框。

[0013] 图4是用于识别和禁用恶意浏览器扩展的示例过程的流程图。

[0014] 图5是示例计算机系统的框图。

[0015] 各附图中相同的附图标记指示相同的元件。

具体实施方式

[0016] 本文档总体上描述了用于识别和禁用恶意浏览器扩展的系统和方法。恶意浏览器扩展是以不期望的方式改变网络浏览器的性能的浏览器扩展。例如，内容拦截器型恶意浏览器扩展可以拦截或以其他方式限制对用户希望查看的期望内容的访问。例如，内容拦截器型恶意浏览器扩展可以防止浏览器加载由网页请求的额外的第三方内容(例如，视频、音频内容、图像等)连同网页的主要内容一起显示。作为另一个示例，内容注入器型恶意浏览器扩展响应于执行由用户请求的网页中的代码，可以注入由第四方内容提供者提供的还没有被请求的不需要的内容。作为又一个示例，钓鱼型恶意浏览器扩展可以尝试引诱用户输入可以用来窃取用户的身份或者通过向用户的信用卡进行未授权的支付而从用户窃取用户的身份的敏感的或个人的信息(例如，信用卡信息)。

[0017] 浏览器扩展管理器可以安装在用户的设备上并使用各种技术来自动识别恶意浏览器扩展、禁用恶意浏览器扩展，并且然后自动从用户的计算设备上卸载本身。例如，扩展管理器可以通过将用于浏览器扩展的信息与包含在先前已识别的恶意浏览器扩展的数据库中的信息进行比较来识别安装在计算设备上的浏览器中的浏览器扩展是恶意浏览器扩展。然后，扩展管理器可以通过停用恶意浏览器扩展、卸载恶意浏览器扩展或限制浏览器扩展改变浏览器的动作来禁用恶意浏览器扩展。在一些实现方式中，扩展管理器向用户提供一系列所识别的潜在的恶意浏览器扩展，并且允许用户选择将被禁用的恶意浏览器扩展。在一些实现方式中，在扩展管理器已识别出所有所识别的恶意浏览器扩展之后，扩展管理器自动从用户的计算设备卸载本身。在一些实现方式中，扩展管理器可以是安装在运行在用户的计算设备上的浏览器上的浏览器扩展。

[0018] 图1示出了在其中内容被分发给用户设备106的示例环境100的框图。示例环境100包括网络102，诸如局域网(LAN)、广域网(WAN)、因特网、或其组合。网络102连接网站104、用户设备106和内容项提供者104。.示例环境100可以包括许多用户设备106和提供各种主要内容108的许多发布者104(即，内容项提供者)。

[0019] 资源发布者104可以提供用于在用户设备106上呈现的资源。例如，发布者104a可以包括可以通过网络102可以提供给用户设备106的资源的数据库。在一些实现方式中，由资源发布者104发布的资源可以采取包含文本、图片、图形、嵌入式视频、嵌入式音频和其他媒介的网页的形式。由资源发布者104发布的资源还可以采取流式音频、流式视频、发送到移动设备的文本消息更新或其他数字媒体的形式。在一些实现方式中，资源发布者104中每个可以是控制、管理和/或拥有一个或多个网站的集合的实体。网站是一个或多个与域名相关联的且由一个或多个服务器托管的资源。示例网站是以超文本标记语言(HTML)格式化的网页集合，其可以包含文本、图像、多媒体内容和编程元素(例如脚本)。每个网站都可以由发布者维护，发布者是控制、管理和/或拥有网站的实体。

[0020] 示例环境100可以包括控制到用户设备106的第三方内容项112的分发的第三方内容提供者110。例如，第三方内容提供者110可以是提供用于在用户设备106处呈现的视频内容的视频服务器的集合。第三方内容提供者110可以向用户设备提供第三方内容项112(例如，广告、图像、视频、音频或其他内容)用于与已由发布者104发布的资源(主要内容108)并排显示。由第三方内容提供者110(其不同于发布者)提供的第三方内容项112可以与由发布者104提供的资源合并，用于通过用户设备106在用户设备106处或其他地方显示。例如，发布者104a可以提供包含关于落基山脉的文章的网页，该网页被配置为当由客户端设备106a加载时请求并接收来自第三方内容提供者110的落基山脉的图像并且将图像并入包括所提供的网页的显示器。

[0021] 客户端设备106是能够通过网络102请求并接收资源的电子设备。示例用户设备106包括个人计算机(例如，用户设备106a和106b)、移动通信设备(例如客户端设备106c)以及可以通过网络102发送和接收数据的其他设备。客户端设备106通常包括诸如网络浏览器等的用户应用程序，以促进通过网络102发送和接收数据。例如，客户端设备106a包括安装在客户端设备106a上的浏览器126，用于促进通过网络102发送和接收数据并且将从资源发布者108和第三方内容提供者110接收的主要内容108和第三方内容112分别呈现给客户端设备106a的用户。

[0022] 客户端设备106可以提交请求来自发布者的资源的资源请求。例如，客户端设备106b可以通过网络102向发布者108b发送对主要内容108b(例如，关于最新名人新闻的文章)的请求。进而，表示所请求的主要内容108b的数据可以被提供给客户端设备106b以通过客户端设备106b呈现。所请求的主要内容108b可以是例如网站的主页、来自社交网络的网页、视频剪辑或文字处理文档。表示所请求的主要内容项108b的数据可以包括使主要内容108b在客户端设备106b处呈现的数据。

[0023] 主要内容108还可以包括一个或多个标签或指示符，所述标签或指示符在被执行时使得客户端设备106b生成对第三方内容(例如，视频内容、音频内容、图像、动画图形、文本内容、广告或其他由第三方提供的内容等)的请求并且将该请求传输到诸如第三方内容提供者110的一个或多个内容项分发网络。例如，由发布者104a提供给客户端设备106b的网页包括引起两个图像和视频与有待产生的网页一起显示的请求的标签。客户端设备106b可以向第三方内容提供者110发送对两个图像和与网页指定的参数匹配的视频的请求。响应于该请求，第三方内容提供者110可以通过网络102将所请求的图像和视频提供给客户端设备106b用于连同网页的内容(例如，在网页的主要内容旁边的网页的空白处、或者沿着网页的顶部或底部)一同显示在客户端设备106b上。

[0024] 在一些实现方式中，被包括在已提供给用户设备106的资源中的标签可以包括指定内容项时隙的数据。内容项时隙是资源的一部分(例如，网页的一部分)或用户显示的一部分(例如，另一个窗口的呈现位置或网页的一个位置中)，其中可以呈现诸如视频、音频或图像内容等的内容项。例如，内容项时隙可以指定内容项的空间位置，该空间位置是在用户设备处初始呈现资源之后可见的资源的一部分的下方、上方或附近的指定距离(例如，2厘米或指定数量的像素)。在一些实现方式中，当用户设备106呈现资源时，执行与该资源中的时隙相关联的代码启动对内容项的请求以填充时隙。内容项请求随后被发送到提供用于内容项时隙的内容项的内容项分发系统(例如，第三方内容提供者110)。

[0025] 如上所讨论的，诸如网页(和第三方内容项)的资源由在计算设备上操作的浏览器呈现。例如，运行在客户端设备106a上的浏览器126可以响应于在由浏览器126执行的包括在主要内容中的代码时从客户端设备106a发送到第三方内容提供者110的对第三方内容的请求而呈现从发布者104接收到的主要内容108以及从第三方内容提供者110接收到的第三方内容112。例如，浏览器126呈现在客户端设备106a处接收的网页以显示网页的主要内容。该网页还包括使浏览器126请求一个或多个第三方内容项112(诸如视频或图像)用于连同网页的主要内容一起显示在内容项时隙中的代码。

[0026] 浏览器126还可以包括作为附加项安装到浏览器126上的一个或多个扩展130。扩展130可以例如由为浏览器126提供软件的软件提供者提供，或者由已经设计扩展130与浏览器126一起操作的第三方软件提供者提供。扩展130可以改变浏览器126的执行。例如，浏览器130a可以为浏览器126的主屏幕设置专用背景图像而浏览器130b向浏览器126添加侧栏，该侧栏显示客户端设备106a的用户已经表示感兴趣的运动队的当前运动分数。在一些情况下，客户端设备106a的用户可以在线搜索浏览器扩展并将浏览器扩展安装在客户端设备106a上，以使得浏览器扩展改变浏览器126的某些功能。

[0027] 不幸地，在实践中，并非所有浏览器扩展为浏览器126的操作添加有用的或有益的功能。或者在一些情况下，浏览器扩展可以提供某些期望的功能，同时还执行不想要的或不

期望的功能。例如，恶意软件供应者114也可以连接到网络102并且可以向用户设备106提供恶意软件116。如果恶意软件116安装在用户设备106中的一个(诸如客户端设备106a)上，则它可以以用户想不到的不期望的或不利的方式改变浏览器126和/或客户端设备106a的性能。在一些情况下，恶意软件供应者114可以指出特定块的软件具有某些功能，但是实际上，软件可以在安装后执行其他不想要的功能或者期望和不期望的功能的混合。恶意软件116可以采取与客户端设备106a上的浏览器126分开操作的浏览器扩展或软件的形式。

[0028] 恶意软件116(包括恶意浏览器扩展)可以采取若干种形式。例如，内容拦截器型恶意软件116可以拦截或以其他方式限制对用户希望查看的期望内容的访问。例如，内容拦截器型意浏览器扩展响应于执行包括在由浏览器126呈现的网页中的代码可以防止浏览器加载由浏览器126请求的来自第三方内容供应者110的第三方内容112(例如，视频、音频内容、图像等)。一些内容拦截器型恶意软件116可以防止用户完全访问某些网站或网站的某些部分。另外，这种内容拦截器型恶意软件116可以防止用户查看补充显示在浏览器126中的网页的主要内容的信息或者用户可能希望查看的其他信息(例如与包含在网页中的文章相关的文章的预览图)。在一些情况下，内容拦截器型恶意软件116可以响应于执行网页中的代码而用包括在网页中的未由代码指示的其他内容代替所请求的内容。

[0029] 作为另一示例，内容注入器型恶意软件116响应于由用户请求的网页中的代码的执行可以注入由第四方内容提供者提供的还未被请求的不想要的内容。例如，客户端设备106a的用户将网页的URL输入到浏览器126中。浏览器126使客户端设备106a请求来自发布者104b的包含主要内容的网页。发布者104b将包含主要内容108b的网页从主要内容108的存储器提供给客户端设备106a。浏览器126呈现网页以显示主要内容并且额外执行包括在网页中的代码以从第三方内容提供者110产生对一个或多个第三方内容项112的请求。浏览器126显示接收自第三方内容提供者110的第三方内容112以及网页的主要内容。另外，在这个示例中，浏览器扩展130a是内容注入器型恶意浏览器扩展。例如，浏览器扩展130a先前从恶意软件提供者114在客户端设备106a处被接收并且安装在浏览器126中。

[0030] 浏览器扩展130a(在该示例中，其是内容注入器型恶意浏览器扩展)可以改变浏览器126的操作，以使得浏览器126响应于执行包括在从发布者104a接收到的网页中代码显示未请求的额外的第四方内容。例如，恶意浏览器扩展130a可以检测到浏览器126已经接收到网页并且呈现网页的主要内容用于显示在客户端设备106a的显示屏幕上。然后，恶意浏览器扩展130a可以生成对第四方内容(例如，不想要的内容)的请求，并且使客户端设备106a将该请求输送至第四方内容供应者118。恶意浏览器扩展130a独立于包括在由浏览器126呈现的网页中的任何代码生成该请求。响应于接收到该请求，第四方内容供应者118可以从不想要的内容项120的存储器中提供一个或多个第四方内容项。然后，第四方内容供应者118将不想要的第四方内容提供给客户端设备106a。恶意浏览器扩展130a然后使浏览器126显示接收自第四方内容供应者118的不想要的第四方内容以及由浏览器126呈现的网页的一些内容或全部内容。

[0031] 在一些情况下，如由网页中的代码所指示的，浏览器扩展130a可以使浏览器126在由网页指定的内容项时隙中显示不想要的第四方内容120，代替从第三方内容提供者110请求的第三方内容项112。在一些情况下，浏览器扩展130a可以使浏览器126在其他位置中显示不想要的第四方内容120，所述其他位置可以部分地或完全地拦截网页的主要内容或从

第三方内容提供者110接收的一个或多个第三方内容项112。从第四方内容提供者118接收的不想要的第四方内容120和从第三方内容提供者110接收的第三方内容112之间的一个区别在于浏览器126响应于执行包括在从发布者104接收的网页中的代码而生成对第三方内容112的请求，而相反，恶意浏览器扩展130a独立于包括在网页中的代码生成对不想要的第四方内容120的请求，并且使客户端设备106a向第四方内容供应者118输送请求。在一些情况下，浏览器扩展130a可以响应于对包括在网页中的额外内容的请求的直接指示扫描网页以识别包括在网页中的信息，以使得请求切向相关的不想要的第四方内容120而不请求第四方内容120。

[0032] 在一些情况下，不想要的第四方内容项120例如可以尝试诱导用户选择第四方内容项120以将用户还没有请求的或者可以将额外的恶意软件安装在客户端设备106a上的浏览器126引导到的网络位置(例如，URL)。作为另一示例，不想要的第四方内容120可以显示与用户请求的网页的主要内容无关或不相关的信息。另外，在请求不想要的第四方内容120并使浏览器126呈现不想要的第四方内容120时由恶意浏览器扩展130a执行的动作可以霸占计算资源，诸如客户端设备106a的活动内存或处理容量，从而总体上降低客户端设备106a的性能。因此，移除恶意浏览器扩展的结果是改善了客户端设备的性能。

[0033] 作为恶意软件116的又一个示例，钓鱼型恶意软件116可以尝试引诱用户输入可以用来例如窃取用户的身份或者通过向用户的信用卡进行未授权的支付而从用户窃取用户的身份的敏感的或个人的信息(例如，信用卡信息)。

[0034] 恶意软件116的另一个示例是浏览器扩展，其可以尝试访问存储在客户端设备106上的信息并将该信息传输到与恶意软件相关联的远程服务器。例如，恶意浏览器扩展130可以访问用户的浏览器历史并且在用户不知道或不允许的情况下将该信息提供给远程服务器。其他类型恶意浏览器扩展包括占用浏览器126的显示区域的一部分的浏览器扩展，从而混乱了与不想要的视觉信息的显示。示例包括模仿浏览器126的URL或搜索栏但将用户引导至搜索服务或用户打算联系的可能不是搜索服务的其他服务器的搜索条。恶意浏览器扩展130也可以访问客户端设备106的资源，以使客户端设备106充当“机器人程序”以在远程“主”计算系统的请求下执行动作。恶意浏览器扩展130(例如，通过在后台不断运行以扫描所加载的网页的内容来识别注入不想要的第四方内容的机会，或通过参与与远程服务器的不想要的或未授权的通信)也可以过度利用计算机资源，这会降低客户端设备106的整体性能。

[0035] 继续图1中所示的示例，示例环境100包括安装在客户端设备106a上的扩展管理器132。扩展管理器132可以监视安装在客户端设备106a上的浏览器扩展130的操作，并识别恶意浏览器扩展或潜在的一个或多个浏览器扩展的恶意活动。扩展管理器132然后可以禁用所识别的恶意或潜在恶意的浏览器扩展。扩展管理器132可以进一步被配置为在完成禁用恶意浏览器扩展之后自动从客户端设备106a卸载本身。在一些实现方式中，扩展管理器132不限于识别恶意或潜在恶意的浏览器扩展，而是总体上被配置为识别和禁用安装在用户设备106上的恶意或潜在恶意软件。

[0036] 为了安装扩展管理器132，客户端设备106a的用户可以例如访问远程服务器来下载和安装扩展管理器132。作为另一示例，用户可以安装来自物理存储设备(诸如CD-ROM或闪存“拇指”驱动器)的扩展管理器132。扩展管理器132可以作为浏览器126的扩展而被安

装。例如，浏览器扩展130b可以是扩展管理器。在一些实现方式中，扩展管理器132可以是安装在客户端设备106a上但不作为浏览器扩展安装的独立软件。

[0037] 扩展管理器132可以使用识别恶意或潜在恶意的浏览器扩展的一种或多种技术来。例如，扩展管理器132可以通过识别修改浏览器126的功能的某个方面的软件(包括通过识别修改浏览器126的显示功能或通信功能的浏览器扩展)来识别安装在客户端设备106a上的浏览器扩展。扩展管理器132还可以扫描客户端设备106a的程序注册表以识别安装在客户端设备106a上的浏览器扩展。扩展管理器132然后可以分析所识别的浏览器扩展的属性和/或功能，以确定所标识的浏览器扩展中的任意扩展是否是恶意的或潜在恶意的浏览器扩展。

[0038] 在一个示例过程中，扩展管理器132可以将用于所识别的浏览器扩展的识别信息(例如扩展ID)与存储在计算机存储器128中的先前所识别的恶意浏览器扩展134的数据库进行比较。扩展管理器132可以执行这种比较以确定所识别的浏览器扩展中的任何扩展是否包括在恶意浏览器扩展的数据库中。在图1示出的示例环境100中，恶意扩展数据库134存储在客户端设备106a的存储器128(例如，主动式存储器、固态存储器或硬盘存储器空间)中。在其他示例中，恶意扩展数据库134存储在远程位置处。例如，恶意扩展识别服务器可以通过网络102与客户端设备106a通信。扩展管理器132可以将用于安装在客户端设备106a上的浏览器扩展130的识别信息提供至可以访问恶意扩展数据库134的恶意扩展识别服务器，以确定浏览器扩展130中的任何扩展130是否是恶意浏览器扩展并将所识别的恶意浏览器扩展的指示返回给客户端设备106a用于扩展管理器132在禁用恶意浏览器扩展时使用。

[0039] 扩展130的可以用于确定扩展130中的任何扩展是否是恶意浏览器扩展的识别信息可以采取若干种形式。例如，扩展130的标题或名称可以用于用唯一识别扩展130。如果扩展130的标题或名称出现在恶意扩展数据库134中，则扩展130被识别为恶意的或潜在恶意的扩展。作为另一个示例，可以将与扩展130相关联的文件的文件名(例如，安装文件、可执行文件、数据文件或与扩展130相关联的其他文件的文件名)与恶意扩展数据库134中的文件名进行比较以确定扩展130是否是恶意扩展。作为另一个示例，用于扩展130的识别信息可以采取用作扩展130的标识符的唯一字符串的形式。

[0040] 在一些实现方式中，与扩展130通信的远程计算系统的识别特征可以用作扩展130的识别信息。例如，扩展管理器132可以确定特定扩展130与特定外部计算系统通信。这些外部计算系统可以通过例如IP地址、URL标识符或其他标识符被识别。扩展管理器132然后可以将这些与扩展130通信的外部计算系统的标识符与存储在恶意扩展数据库134中的值进行比较，以确定这些外部计算系统的任何标识符是否指示浏览器130是恶意浏览器130。例如，扩展管理器132可以确定浏览器扩展130b与第四方内容供应者118通信。扩展管理器132可以使用与第四方内容供应者118相关联的IP地址或URL识别第四方内容供应者118。扩展管理器132然后可以访问恶意扩展数据库134并将用于第四方内容供应者118的标识符(例如，浏览器扩展130b用来与第四方内容供应者118通信的IP地址或URL)与包括在恶意扩展数据库134中的信息进行比较。如果第四方内容供应者118的标识符包括在恶意扩展数据库134中，扩展管理器132可以确定浏览器扩展130b被认为是恶意浏览器扩展。

[0041] 浏览器扩展130的其他属性或功能还可以用于确定浏览器扩展130是否是恶意浏览器扩展。例如，访问客户端设备106a的特定通信端口的扩展130(使用恶意扩展数据库134

中的信息)可以被识别为恶意或潜在恶意的浏览器扩展。作为另一个示例,被确定为访问客户端设备106a的存储器的特定部分(例如,硬盘空间)的扩展130可以(使用恶意扩展数据库134中的信息)被识别为恶意或潜在恶意的浏览器扩展。例如,被确定为访问计算机存储器的受限部分的浏览器扩展130可被识别为恶意或潜在恶意的浏览器扩展。这些类型的恶意浏览器扩展可以由扩展管理器132识别及禁用。例如,扩展管理器132可以监视所使用的通信端口或由浏览器扩展所访问的存储器位置,并且如果扩展管理器检测到浏览器扩展不正确地访问通信端口或存储器的一部分,则扩展管理器可以将浏览器扩展归为恶意浏览器扩展,并禁用该恶意浏览器扩展。

[0042] 在一些实现方式中,除了或者代替利用恶意扩展数据库134来识别恶意或潜在恶意的浏览器扩展,扩展管理器132还可以监控扩展130的动作以确定扩展130是否正在执行表明是恶意或潜在恶意浏览器扩展的功能。例如,扩展管理器132可以监视浏览器扩展130a的活动以确定浏览器扩展130a是否阻止由第三方内容提供者110提供的用于由浏览器126呈现的第三方内容112的一些或全部连同网页的主要内容一起由浏览器126显示(即,内容拦截器型恶意浏览器扩展)。浏览器扩展130a的这种活动可以由扩展管理器132用来将浏览器扩展130a识别为恶意或潜在恶意的浏览器扩展。作为另一示例,扩展管理器132可以确定浏览器扩展130a是否阻止浏览器126显示从发布者104接收的主要内容的全部或部分。

[0043] 作为另一示例,扩展管理器132可以监视浏览器扩展130a的动作以确定浏览器扩展130a是否与一个或多个不可信或恶意的外部计算系统进行通信。扩展管理器132可以通过例如识别外部计算系统的URL或IP地址来识别与浏览器扩展130a通信的外部计算系统。然后,扩展管理器132可以将用于外部计算系统的这种识别信息与先前存储的一系列所识别的恶意或不可信的计算系统进行比较,以确定浏览器扩展130a是否正与恶意或不可信的计算系统进行通信。这种活动可以用于将浏览器扩展130a识别为恶意或潜在恶意的浏览器扩展。恶意或不可信的计算系统可以包括被识别为第四方内容供应者(诸如第四方内容供应者118)的计算系统、与内容拦截浏览器扩展相关联的计算系统、被识别为钓鱼式计算系统的计算系统、或被识别为与其他不想要的或不需要的活动相关联的计算系统。

[0044] 在一些实施方式中,与外部计算系统通信的频率由扩展管理器132用来确定浏览器扩展130a是恶意或潜在恶意的浏览器扩展。该频率可以是由浏览器扩展130a启动的外部通信的总频率、或者与一个或多个(例如,如由IP地址或URL标识的)特定外部计算系统进行外部通信的频率,诸如先前所识别的恶意或不可信的外部计算系统。扩展管理器132可以将由浏览器扩展130a所识别的通信的频率与阈值进行比较,以确定浏览器扩展130a是否是恶意或潜在恶意的浏览器扩展。

[0045] 作为另一示例,扩展管理器132可以监视浏览器扩展130a的动作,以确定浏览器扩展130a是否响应于执行包括由浏览器126呈现的网页中的代码正在使浏览器126显示未由浏览器126请求的第四方内容。例如,扩展管理器132可以确定浏览器扩展130a已经请求了来自第四方内容供应者118的不想要的第四方内容120,并且确定由浏览器扩展130a启动的没有由包括在通过浏览器126正加载的网页中的代码正指示的对第四方内容120的请求。这样的活动可以由扩展管理器132用来确定浏览器扩展130a是恶意或潜在恶意的浏览器扩展。在一些实现方式中,如果第四方内容120显示在网页的一部分上(例如,在网页的主要内容的一部分上,或响应于执行包括在显示在内容项时隙中的网页中的代码而请求的一个或

多个第三方内容项112的一部分上)，则扩展管理器132仅将浏览器扩展130a识别为恶意或潜在恶意的浏览器扩展。

[0046] 作为另一示例，扩展管理器132可以识别使浏览器126显示隐藏网页的主要内容或第三方内容112的部分或全部的信息的扩展130(即使由扩展130所显示的信息不是从第四方内容供应者118接收)为恶意或潜在恶意的浏览器扩展。作为另一示例，扩展管理器132可以监视浏览器扩展130a的活动，以确定浏览器扩展130a是否在诱导客户端设备106a的用户输入特定信息。这种活动可以用于将浏览器扩展130a标记为恶意或潜在恶意的浏览器扩展。作为又一个示例，扩展管理器132可以监视浏览器扩展130a以(例如，通过将链接或图像插入网页、或者通过将链接或可选图像包括在显示在浏览器126显示器的外围中的工具栏中)确定浏览器扩展130a是否尝试将客户端设备106a的用户引导至潜在恶意或不可信的外部服务器。扩展管理器132可以通过例如识别外部计算系统的URL或IP地址来识别该些外部计算系统，其中浏览器扩展130a试图将用户引导至该些外部计算系统。然后，扩展管理器132可以将用于外部计算系统的该识别信息与先前存储的一系列所识别的恶意或不信任的计算系统进行比较，以确定浏览器扩展130a是否试图将用户再引导到恶意或不可信的计算系统。这种活动可以用于将浏览器扩展130a识别为恶意或潜在恶意的浏览器扩展。

[0047] 在一些实现方式中，扩展管理器132可以自动地禁用被识别为恶意浏览器扩展的所有扩展130。扩展管理器132可以通过例如停用扩展130来禁用恶意浏览器扩展130。停用恶意扩展130使得恶意扩展130安装在客户端设备106a上，但是恶意扩展130处于休眠状态，并且确实不在客户端设备106a上执行。作为另一示例，扩展管理器132可以通过从客户端设备106a卸载恶意扩展130(其可以包括启动使安装在用户设备106a上的浏览器126或其他软件卸载恶意扩展130的过程)来禁用恶意扩展130。作为又一示例，扩展管理器132可以通过防止恶意扩展130改变浏览器126的功能或通过防止恶意扩展130执行某些功能(包括防止恶意扩展130与特定外部计算设备通信)而禁用恶意扩展130。

[0048] 在一些实现方式中，扩展管理器132在将的浏览器扩展识别为恶意或潜在恶意的浏览器扩展之后不会立即禁用这些恶意或潜在恶意的浏览器扩展。在这样的实现方式中，扩展管理器132可以向客户端设备106a的用户提供对话以识别要禁用哪些恶意或潜在恶意的浏览器扩展。在一些实现方式中，扩展管理器132可以将被识别为恶意或潜在恶意的浏览器扩展的扩展130与一“白系列”的浏览器扩展进行比较，该“白系列”的浏览器扩展指示用户(或另一个人)已经将其识别为可接受的浏览器扩展的浏览器扩展。例如，用户可以通过将特定内容注入器浏览器扩展包括在一白系列好的浏览器扩展中而指示向由浏览器126加载的所有网页添加笑脸的该特定内容注入器浏览器扩展不应该由扩展管理器132禁用。

[0049] 在一些实现方式中，扩展管理器132在完成识别并禁用恶意或潜在恶意的浏览器扩展之后从客户端设备106a卸载本身，扩展管理器132从客户端设备106a卸载本身。这样的功能可以包括启动使安装在用户设备106a上的浏览器126或其他软件卸载扩展管理器132的过程。因为扩展管理器132在卸载之后将不再占用存储器空间或者处理能力，所以这种自动卸载可以最大化客户端设备106a的资源。

[0050] 尽管扩展管理器132在示例环境100中被示为位于客户端设备106a处，但是在一些实现方式中，扩展管理器132可能位于远程计算设备上并且与客户端设备106a通信来识别和禁用恶意浏览器扩展。例如，诸如发布者104之一的内容提供者可以包括扩展管理器，该

扩展管理器(在用户请求时)与客户端设备106a通信以识别和禁用恶意浏览器扩展。作为另一个示例,与浏览器126相关联的远程计算系统可以为客户端设备106a提供远程扩展管理功能。在一些实现方式中,扩展管理器132的一些功能可以由远程计算系统执行,而扩展管理器132的其他功能在客户端设备106a处执行。例如,远程计算系统在接收到识别恶意和潜在恶意的浏览器扩展的用户请求之后可以与浏览器126通信以识别安装在浏览器126上的恶意和潜在恶意的浏览器扩展。在识别出恶意和潜在恶意的浏览器扩展之后,远程计算系统可以给用户下载和安装扩展管理器的选项,该扩展管理器可以禁用所识别的恶意和潜在恶意的浏览器扩展并且然后从客户端设备106a卸载本身。

[0051] 转向图2,示例浏览器200可以呈现包括主要内容204的网页202。浏览器200可以是例如图1的在客户端设备106a上执行的浏览器126。网页202响应于用户与浏览器200的交互(例如用户在浏览器200的URL栏中键入URL)可以从图1的发布者104a被接收。浏览器200可以包括安装在浏览器200上以改变浏览器200的功能的多个浏览器扩展206。例如,扩展A可以改变浏览器200的外观或“主题”以显示特定运动队的标志。作为另一个示例,扩展B可以使用于浏览器200的用户的优选互联网无线电台的音频播放器显示在浏览器200的显示器内的某处,以使得用户可以控制互联网无线电台的回放和其他设置而无需访问互联网无线电台的网页。

[0052] 在一些实现方式中,浏览器200包括安装在浏览器200上的浏览器扩展206(诸如图2中的示例中所示的那些)的可视化表示。在一些实现方式中,只有一些浏览器扩展206在浏览器200的显示器中具有可视化表示,而另一些浏览器扩展206不具有可视化表示。在一些实现方式中,浏览器扩展206中没有一个在浏览器200的主显示器中具有可视化表示。在一些实现方式中,浏览器200的用户(例如,通过访问浏览器200的“设置”控件)可以访问列出安装在浏览器200上的浏览器扩展206的单独的浏览器扩展控制屏幕列出安装在浏览器200上的浏览器扩展206。

[0053] 在图2示出的示例中,浏览器200包括使搜索栏208被包括在浏览器200的显示器中的浏览器扩展206。搜索栏208例如可以适应某些显示特征以与浏览器的另一些显示方面200融合,但是当搜索字符串由用户输入到搜索栏208中时,可以将用户引导到较不理想的搜索站点。

[0054] 在一些情况下,浏览器扩展206由浏览器200的用户有意地安装在浏览器200上。例如,用户可能想要安装将股票行情自动收录器反馈添加到浏览器200显示窗口的一部分的浏览器扩展。用户可以在线搜索浏览器扩展并将浏览器扩展安装在浏览器200中。在一些情况下,浏览器扩展206被无意地安装。例如,一些浏览器扩展206在用户选择网页中的特定超链接时可以自动安装,即使用户不打算安装该特定浏览器扩展206。作为另一示例,用户可以将软件安装在包括浏览器200的用户设备上。除了用户设备上的其他程序之外,该软件可以自动安装浏览器扩展206。在一些情况下,用户可以安装浏览器扩展206,并且然后稍后发现所安装的浏览器扩展206不具有所宣传的功能,或者具有用户认为不需要的不同功能。

[0055] 如上所讨论的,浏览器200显示包括主要内容204的网页202。由浏览器200显示的网页202还可以包括第三方内容项。例如,诸如图像210和212以及视频内容214的第三方内容项可以被显示为网页202的一部分。在一些实现方式中,第三方内容项响应于在浏览器200执行包括在网页202中的代码时所生成的由浏览器200生成的请求由第三方内容提供者

(诸如图1中的第三方内容提供者110)提供。例如,网页202可以通过网络从发布者接收并且包括主要内容204以及在由浏览器200执行时使浏览器200产生对图像210和212以及视频内容214的请求的代码。第三方内容的其他示例可以包括文本,例如用于其他网页的主要内容的预览;音频内容;或文本、图形、音频或视频内容的组合。

[0056] 在一些实现方式中,浏览器扩展206中的一个或多个是恶意浏览器扩展。例如,扩展A可以是内容拦截器型浏览器扩展,当其安装在浏览器200上时防止浏览器200显示图像212以及网页202的其他内容,即使网页202包括用于启动请求图像212与网页202一起显示的代码。作为另一示例,扩展B可以是将不想要的第四方内容添加至网页202的显示的内容注入器型浏览器扩展。例如,扩展B可以检测到浏览器200正在加载网页202,并且作为响应,联系第四方内容服务器以从第四方内容项请求第四方内容项216。扩展B然后可以使浏览器200显示第四方内容项216作为网页202的显示的一部分,即使包括在网页202中的代码没有命令浏览器200显示第四方内容项216。在一些情况下,第四方内容项216可以尝试模仿网页202的其他部分以诱导用户选择第四方内容项216以被引导到不可信的服务器系统或引诱用户输入提供给不可信的服务器系统的信息。其他浏览器扩展206也可以是其他类型的恶意浏览器扩展,如上关于图1所描述的。

[0057] 在一些情况下,对于浏览器200的用户卸载一个或多个浏览器扩展206可能是困难的。例如,在一些实现方式中,浏览器200可以包括浏览器扩展控制屏幕,其包括用于禁用或卸载包括在安装在浏览器200上的一系列浏览器扩展206中的浏览器扩展206的选项。然而,某些禁用或卸载控件可能本身被禁用或“变灰”,以使得用户不能使用浏览器扩展控制屏幕来禁用或卸载某些浏览器扩展206。特别对于安装在浏览器200上的恶意浏览器扩展206更是如此。

[0058] 浏览器200可以包括作为浏览器扩展安装在浏览器上的扩展管理器。替代地,扩展管理器可以安装在包括浏览器200但不作为浏览器扩展安装的计算设备上。扩展管理器可以使用如上关于图1描述的技术来识别恶意或潜在恶意的浏览器扩展并且然后禁用所识别的恶意或潜在恶意的浏览器扩展。例如,扩展管理器可以将浏览器扩展206的识别信息与包括在恶意浏览器扩展的数据库中的浏览器扩展识别信息进行比较,以确定浏览器扩展206中的任何浏览器扩展206是否是恶意或潜在恶意的浏览器扩展。作为另一个示例,扩展管理器可以监视浏览器扩展206的动作,以确定浏览器扩展206中的任意浏览器是否正在执行指示其是恶意浏览器扩展的动作。

[0059] 在一些实现方式中,扩展管理器自动禁用(例如,停用、卸载或限制其功能/访问)所识别的恶意浏览器扩展。在一些实现方式中,扩展管理器然后在禁用所识别的恶意浏览器扩展之后可以继续自动卸载本身。

[0060] 转向图3,在一些实现方式中,在扩展管理器从安装在浏览器200上的浏览器扩展206中已经识别出恶意或潜在恶意的浏览器扩展之后,扩展管理器可以向浏览器200的用户呈现扩展管理器对话框220。扩展管理器对话框220包括由扩展管理器识别为恶意或潜在恶意浏览器扩展的一系列浏览器扩展206。扩展管理器对话框220可以包括允许用户识别要禁用的所识别的浏览器扩展206的控件,诸如例如复选框。扩展管理器对话框220进一步包括控件222,当(例如,通过在触摸屏上的点击鼠标或手指敲击来交互)由用户选择该控件时,该控件222使扩展管理器禁用所识别的浏览器扩展206。在一些实施方式中,扩展管理器对

话框220可以允许用户指定如何禁用所识别的浏览器扩展206。例如，扩展管理器对话框220可以允许用户指定是否停用、卸载所识别的浏览器扩展206、所识别的浏览器扩展206具有某些功能或访问受限制、或者以另一方式被禁用所识别的浏览器扩展206。例如，可以在用户界面中呈现使用户能够选择如何停用浏览器扩展206的用户界面元素。

[0061] 在一些实现方式中，在扩展管理器响应于用户选择控件222而已经禁用了所识别的浏览器扩展206之后，扩展管理器启动从浏览器200和/或其上存在有浏览器200的用户设备上卸载本身的卸载例程。

[0062] 图4是用于识别和停用恶意浏览器扩展的示例过程400的流程图。过程400可以由一个或多个数据处理装置来执行，诸如图1的用户设备106。具体地，在客户端设备106a上执行的扩展管理器132可以执行过程400。过程400的操作可以通过存储在非暂时性计算机可读介质上的指令来实现，其中指令的执行使一个或多个数据处理装置执行过程400的操作。

[0063] 识别被配置为修改客户端设备的浏览器的操作的浏览器扩展(402)。例如，安装在客户端设备上的软件模块(诸如扩展管理器)可以识别安装在客户端设备上的浏览器扩展，以使得浏览器扩展修改安装在客户端设备上的浏览器的操作。例如，扩展管理器可以通过访问安装在客户端设备上的用于识别浏览器扩展的程序的注册表来识别浏览器扩展。作为另一示例，扩展管理器可以与浏览器交互以识别安装在客户端设备上的浏览器扩展。例如，浏览器可以保留注册表或安装在客户端设备上的一系列浏览器扩展，这些浏览器扩展被配置为修改浏览器的操作。浏览器可以将此信息通信至扩展管理器，以允许扩展管理器识别安装在客户端设备上的一个或多个浏览器扩展。

[0064] 浏览器扩展被确定为恶意浏览器扩展(404)。例如，扩展管理器可以使用一种或多种技术来识别浏览器扩展是恶意浏览器扩展，该技术包括将浏览器扩展的识别信息与包含在所识别的恶意浏览器扩展的数据库中的信息进行比较并监控浏览器扩展的活动以识别指示其是恶意浏览器扩展的动作(诸如拦截浏览器中的内容显示)、将额外的不想要的第四方内容注入到浏览器上的显示器上、与先前所识别的不可信的远程计算系统通信、或尝试访问受限制的存储器位置。

[0065] 可选地向客户端设备的用户显示一系列潜在恶意的浏览器扩展(406)。例如，如上面关于图3所讨论的，可向用户显示扩展管理器对话框(诸如图3的扩展管理器对话框220)，该扩展管理器对话框包括安装在客户端设备上的一系列所识别的恶意和潜在恶意的浏览器扩展。扩展管理器对话框可以包括允许用户指示应该被禁用的浏览器扩展的控件。例如，扩展管理器对话框可以允许用户敲击或点击选择将被禁用的浏览器扩展的控件。

[0066] 指示来自一系列潜在恶意的浏览器扩展的浏览器扩展的用户输入可选地从用户接收(408)。例如，用户可以使用所显示的扩展管理器对话框中的控件(诸如图3中示出的控件222)来选择要禁用的浏览器扩展。作为另一示例，用户可以键入用户希望已经由扩展管理器禁用的恶意或潜在恶意的浏览器扩展的识别信息(诸如浏览器扩展名)。

[0067] 恶意浏览器扩展被禁用(410)。在一些实现方式中，扩展管理器可以通过停用恶意浏览器扩展、从客户端设备卸载恶意浏览器扩展、或者通过限制恶意浏览器扩展的动作来禁用恶意浏览器扩展。例如，扩展管理器可以限制恶意浏览器扩展与远程计算系统(所有远程计算系统或一系列指定的不可信的远程计算系统)通信的能力。例如，可以响应于确定所识别的浏览器扩展是恶意浏览器扩展而自动执行恶意浏览器扩展的这种禁用。在一些实现

方式中，扩展管理器响应于指示应该被禁用的恶意浏览器扩展的(例如，在步骤408处接收到的)用户输入来禁用该恶意浏览器扩展。

[0068] 扩展管理器在完成禁用恶意浏览器扩展之后卸载本身(412)。例如，扩展管理器可以确定恶意浏览器扩展的禁用已经成功完成。然后，扩展管理器可以启动其自身的卸载过程，以使客户端设备卸载扩展管理器，并且从而释放以其他方式由扩展管理器使用的额外计算资源。

[0069] 图5是可用于执行如上所述的操作的示例计算机系统500的框图。系统500包括处理器510、存储器520、存储设备530和输入/输出设备540。部件510、520、530和540中的每一个可以例如使用系统总线550互连。处理器510能够处理用于在系统500内执行的指令。在一个实现方式中，处理器510是单线程处理器。在另一个实现方式中，处理器510是多线程处理器。处理器510能够处理存储在存储器520中或存储设备530上的指令。

[0070] 存储器520存储系统500内的信息。在一个实现方式中，存储器520是计算机可读介质。在一个实现方式中，存储器520是易失性存储单元。在另一个实现方式中，存储器520是非易失性存储器单元。

[0071] 存储设备530能够为系统500提供大容量存储。在一个实现方式中，存储设备530是计算机可读介质。在各种不同的实现方式中，存储设备530可以包括例如硬盘设备、光盘设备、由多个计算设备(例如，云存储设备)在网络上共享的存储设备、或者一些其他大容量存储设备。

[0072] 输入/输出设备540为系统500提供输入/输出操作。在一个实现方式中，输入/输出设备540可以包括网络接口设备(例如以太网卡)、串行通信设备(例如RS-232端口)和/或无线接口设备(例如802.11卡)中的一个或多个。在另一个实现方式中，输入/输出设备可以包括被配置为接收输入数据并将输出数据发送到其他输入/输出设备(例如，键盘、打印机和显示设备560)的驱动器设备。然而，也可以使用其他实施方式，诸如移动计算设备、移动通信设备、机顶盒电视客户端设备等。

[0073] 尽管在图5中已经描述了示例处理系统。本说明书中描述的主题的实现方式和功能操作可以在其他类型的数字电子电路中或者计算机软件、固件或硬件中实现，包括本说明书中公开的结构及其结构等同物或者它们中的一个或多个的组合。

[0074] 本说明书中描述的主题的实施例和操作可以在数字电子电路中实现或者在计算机软件、固件或硬件中实现，包括本说明书中公开的结构及其结构等同物或者它们中一个或多个的组合。本说明书中描述的主题的实施例可以被实现为编码在计算机存储介质上的一个或多个计算机程序(即计算机程序指令的一个或多个模块)，用于由数据处理装置执行或者控制数据处理装置的操作。替代地或附加地，程序指令可以被编码在人工生成的传播信号(例如机器生成的电信号、光信号或电磁信号)上，该传播信号被生成以对信息编码以便传输至合适的接收器装置用于由数据处理装置执行。计算机存储介质可以是计算机可读存储设备、计算机可读存储基板、随机或串行存取存储器阵列或设备或者它们中的一个或多个的组合，或者计算机存储介质可以被包括在计算机可读存储设备、计算机可读存储基板、随机或串行存取存储器阵列或设备或者它们中的一个或多个的组合中。此外，尽管计算机存储介质不是传播信号，但是计算机存储介质可以是在人工生成的传播信号中编码的计算机程序指令的来源或目的地。计算机存储介质也可以是一个或多个单独的物理部件或介

质(例如,多个CD、磁盘或其他存储设备)或被包括在一个或多个单独的物理部件或介质(例如,多个CD、磁盘或其他存储设备)中。

[0075] 本说明书中描述的操作可以被实现为由数据处理装置对存储在一个或多个计算机可读存储设备上的或从其他来源接收到的数据执行的操作。

[0076] 术语“数据处理装置”涵盖用于处理数据的所有类型的装置、设备和机器,举例来说,包括可编程处理器、计算机、片上系统,或者前述的多个或组合。该装置可以包括专用逻辑电路,例如FPGA(现场可编程门阵列)或ASIC(专用集成电路)。除了硬件之外,该装置还可以包括为在涉及的计算机程序创建执行环境的代码,例如构成处理器固件、协议栈、数据库管理系统、操作系统、跨平台运行时间环境、虚拟机或它们中的一个或多个的组合的代码。装置和执行环境可以实现各种不同的计算模型基础设施,诸如Web服务、分布式计算和网格计算基础设施。

[0077] 计算机程序(也称为程序、软件、软件应用程序、脚本或代码)可以用任何形式的编程语言来编写,包括编译或解释的语言、说明性或过程语言,并且它可以以任何形式被部署,包括部署为独立程序或适合在计算环境中使用的模块、部件、子程序、对象或其他单元。计算机程序可能但不必对应于文件系统中的文件。程序可以存储在保存其他程序或数据(例如,存储在标记语言文档中的一个或多个脚本)的文件的一部分中、专用于在涉及的程序的单个文件中、或者多个协调文件(例如,存储一个或多个模块、子程序或部分代码的文件)中。计算机程序可以被部署为在一台计算机上或位于一个站点处或跨多个站点分布并通过通信网络互连的多台计算机上执行。

[0078] 本说明书中描述的过程和逻辑流可以由执行一个或多个计算机程序的一个或多个可编程处理器来执行,以通过对输入数据进行操作并生成输出来执行动作。过程和逻辑流也可以由专用逻辑电路(例如,FPGA(现场可编程门阵列)或ASIC(专用集成电路))来自执行,并且装置也可以实现为专用逻辑电路(例如,FPGA(现场可编程门阵列)或ASIC(专用集成电路))。

[0079] 举例来说,适合于执行计算机程序的处理器包括通用微处理器和专用微处理器两者以及任何种类的数字计算机中的任何一个或多个处理器。通常,处理器将从只读存储器或随机存取存储器或两者接收指令和数据。计算机的基本元件是用于根据指令执行动作的处理器和用于存储指令和数据的一个或多个存储器设备。通常,计算机还将包括用于存储数据的一个或多个大容量存储设备(例如磁盘、磁光盘或光盘),或者计算机可操作地被联接以从用于存储数据的一个或多个大容量存储设备(例如磁盘、磁光盘或光盘)接收数据或将数据传输到用于存储数据的一个或多个大容量存储设备(例如磁盘、磁光盘或光盘)或两者。然而,计算机不需要这种设备。

[0080] 此外,计算机可以被嵌入另一个设备中,例如移动电话、个人数字助理(PDA)、移动音频或视频播放器、游戏控制台、全球定位系统(GPS)接收器或便携式存储设备(例如,通用串行总线(USB)闪存驱动器),仅举几例。适合于存储计算机程序指令和数据的设备包括所有形式的非易失性存储器、介质和存储设备,举例来说,该存储设备包括半导体存储设备(例如EPROM、EEPROM和闪存设备)、磁盘(例如内部硬盘或可擦除磁盘)、磁光盘和CDROM和DVD-ROM盘。处理器和存储器可以由专用逻辑电路补充或并入其中。

[0081] 为了提供与用户的交互,本说明书中描述的主题的实施例可以在具有用于向用户

显示信息的显示设备(例如,CRT(阴极射线管)或LCD(液晶显示器)监视器)和通过其用户可以向计算机提供输入的键盘和指向设备(例如鼠标或跟踪球)的计算机上实现。其他类型的设备也可以用于提供与用户的交互,例如,提供给用户的反馈可以是任何形式的感官反馈,例如视觉反馈、听觉反馈或触觉反馈;并且可以以任何形式接收来自用户的输入,包括声学、语音或触觉输入。另外,计算机可以通过向由用户使用的设备发送文档和从该设备接收文档来与用户交互,例如通过响应于从网络浏览器接收到的请求,将网页发送到用户的客户端设备上的网络浏览器。

[0082] 本说明书中描述的主题的实施例可以在包括后端部件(例如作为数据服务器)的计算系统中或包括中间件部件(例如应用服务器)的计算系统中或包括前端部件(例如具有通过其用户可以与本说明书中描述的主题的实现方式交互的图形用户界面或Web浏览器的客户端计算机)的计算系统中、或者包括一个或多个这样的后端部件、中间件部件或前端部件的任何组合的计算系统中实现。系统的部件可以通过任何形式或数字数据通信(例如通信网络)的介质互连。通信网络的示例包括局域网(“LAN”)和广域网(“WAN”)、网间网络(例如因特网)和对等网络(例如,ad-hoc对等网络)。

[0083] 计算系统可以包括客户端和服务器。客户端和服务器通常彼此远离并且典型地通过通信网络交互。客户端和服务器之间的关系是通过运行在各个计算机上并且彼此具有客户端-服务器关系的计算机程序而产生。在一些实施例中,(例如,出于向与客户端设备交互的用户显示数据和从用户接收用户输入的目的)服务器向客户端设备输送数据(例如,HTML页面)。可以在服务器处从客户端设备接收在客户端设备处生成的数据(例如,用户交互的结果)。

[0084] 尽管本说明书包含许多特定的实现方式细节,但是这些不应被解释为对任何发明或可要求保护的范围的限制,而是作为专用于特定发明的特定实施例的特征的描述。本说明书中在单独实施例的背景下描述的某些特征也可以在单个实施例中组合实现。相反地,在单个实施例的背景下描述的各种特征也可以在多个实施例中单独地或以任何合适的子组合来实现。此外,尽管如上可以将特征描述为以某些组合起作用并且甚至最初如此要求,但是来自所要求保护的组合的一个或多个特征可以在某些情况下从组合中删去,并且所要求保护的组合可以针对子组合或子组合的变型。

[0085] 类似地,尽管在附图中以具体顺序图示了操作,但是这不应该被理解为要求以所示出的具体顺序或按相继次序执行这些操作,或者执行所有示出的操作以实现期望的结果。在某些情况下,多任务和并行处理可能是有利的。此外,如上所述的实施例中的各种系统部件的分离不应当被理解为在所有实施例中都需要这种分离,并且应该理解,所描述的程序部件和系统通常可以一起集成在单个软件产品中或者封装到多个软件产品中。

[0086] 因此,已经描述了主题的具体实施例。其他实施例在以下权利要求的范围内。在某些情况下,权利要求中列举的动作可以以不同的顺序执行并且仍然实现期望的结果。另外,附图中图示的过程不必须需要所示的具体顺序或相继次序,以实现期望的结果。在某些实现方式中,多任务和并行处理可能是有利的。

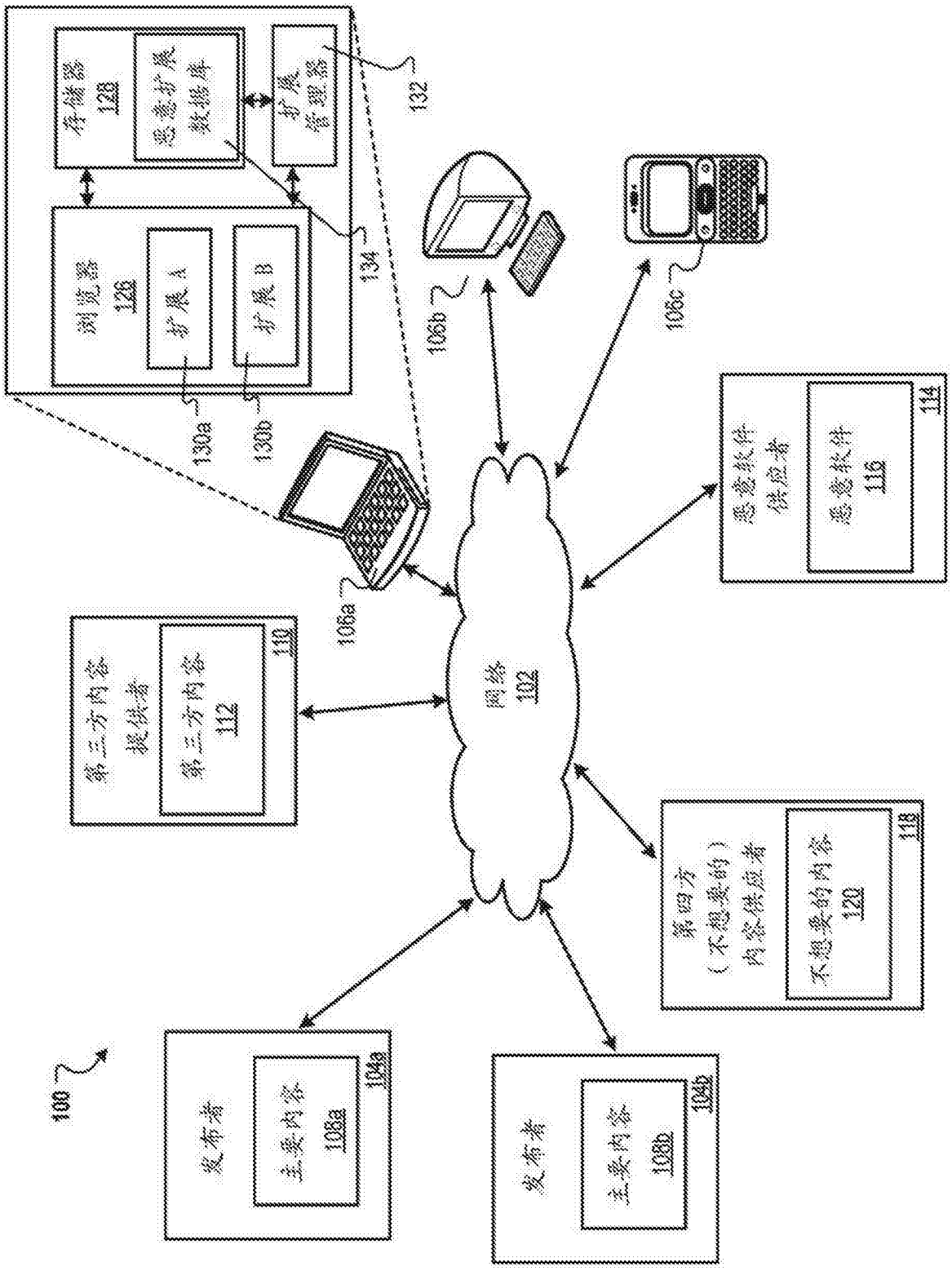

存储器
128
恶意扩展数据库
扩展管理器
132
浏览器
126
扩展 A
扩展 B
134
130a
130b
106b
106c
106a
网络
102
恶意软件供应者
114
恶意软件
116
第三方内容提供者
110
第三方内容
112
第四方（不想要的）内容供应者
118
不想要的内容
120
发布者
主要内容
108a
104a
发布者
主要内容
108b
104b
100

图1


200
好的浏览器
www.newssiteexample.com/
206
扩展 A
扩展 B
扩展 C
208
敏捷的搜索栏
在此搜索！
开始
新闻站点示例.com 你的新闻资源！
纽约篮球队大胜
202
在进入接近终点的比赛中，纽约篮球队拉出一个胜利的拥抱。随着控球后卫 Al Smith 投出一个压哨球将球队二十年来首次送入季后赛。“我只是看到了这个机会并且明白我必须要抓住它，” Smith 强调到。“对于这次胜利，我不应受这个荣誉，让我们在正确的位置投出决胜球是全努力的结果。”球队在季后赛的第一轮将面对达拉斯。球票销售中.....
204
210
212
214
点击播放视频
216
在此处键入你的信用卡信息，让你的问题消失！

图2

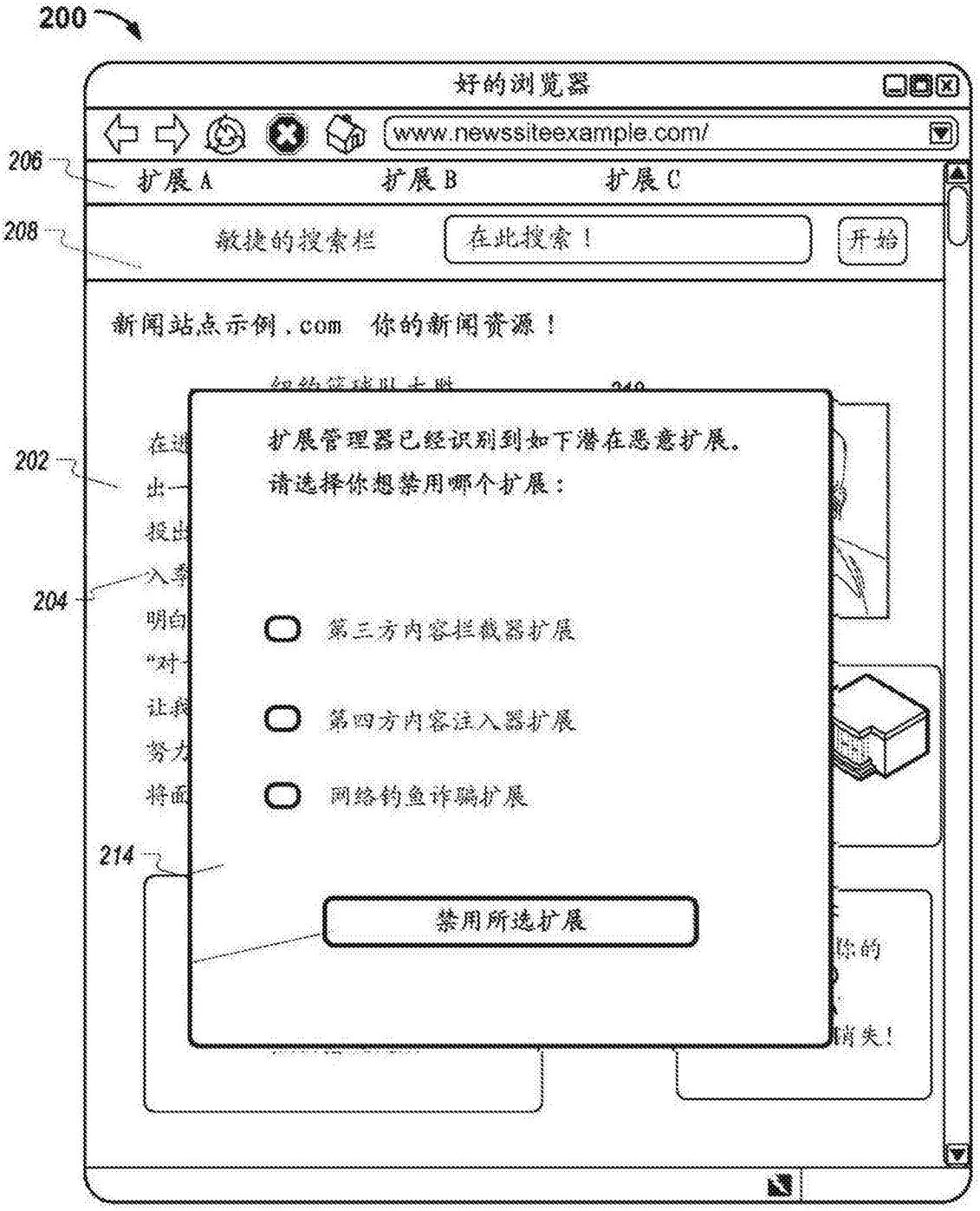

200
好的浏览器
www.newssiteexample.com/
206
扩展 A
扩展 B
扩展 C
208
敏捷的搜索栏
在此搜索！
开始
新闻站点示例.com 你的新闻资源！
202
扩展管理器已经识别到如下潜在恶意扩展。
请选择你想禁用哪个扩展：
204
第三方内容拦截器扩展
第四方内容注入器扩展
网络钓鱼诈骗扩展
214
禁用所选扩展

图3

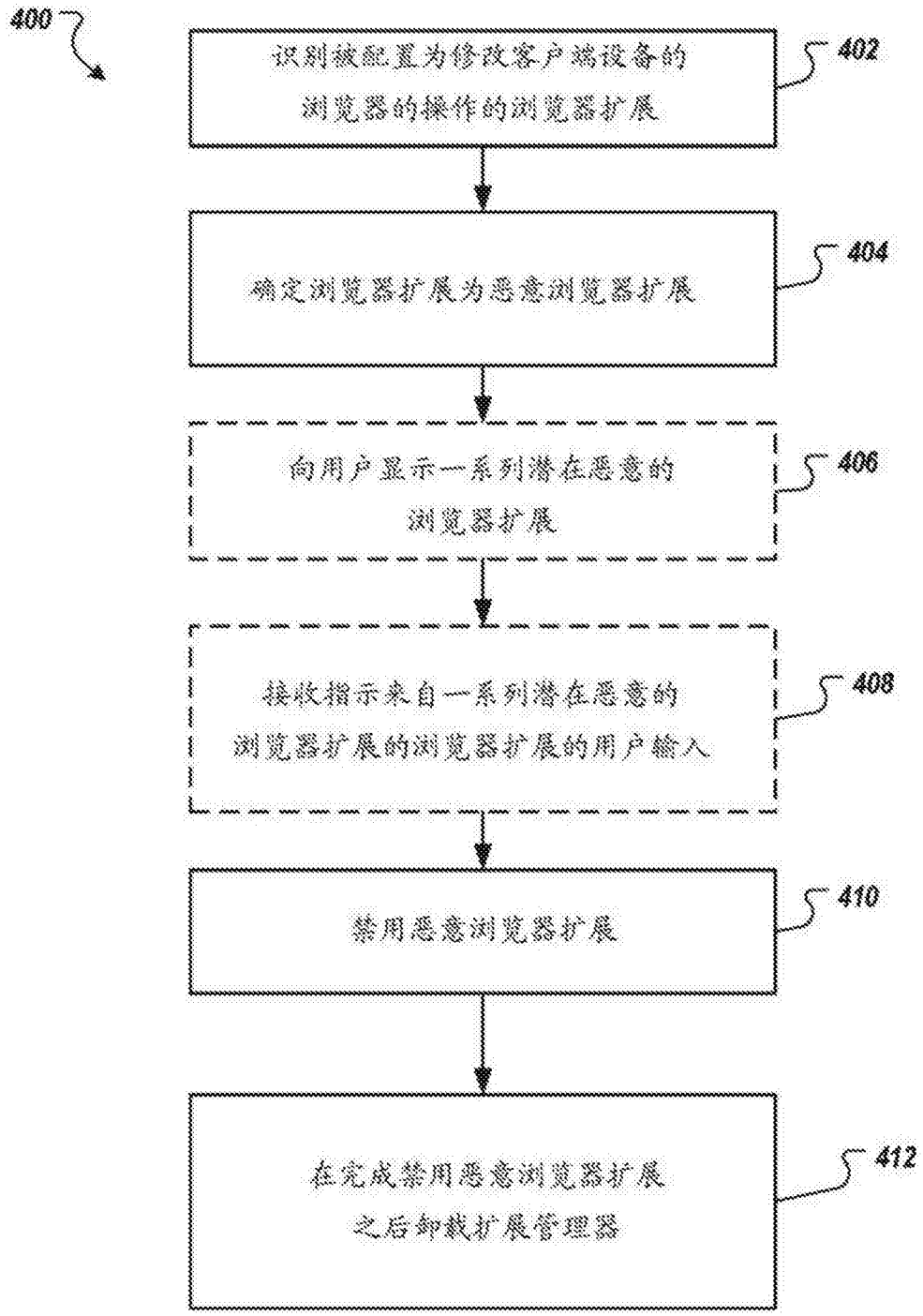

400
识别被配置为修改客户端设备的浏览器的操作的浏览器扩展
402
确定浏览器扩展为恶意浏览器扩展
404
向用户显示一系列潜在恶意的浏览器扩展
406
接收指示来自一系列潜在恶意的浏览器扩展的浏览器扩展的用户输入
408
禁用恶意浏览器扩展
410
在完成禁用恶意浏览器扩展之后卸载扩展管理器
412

图4

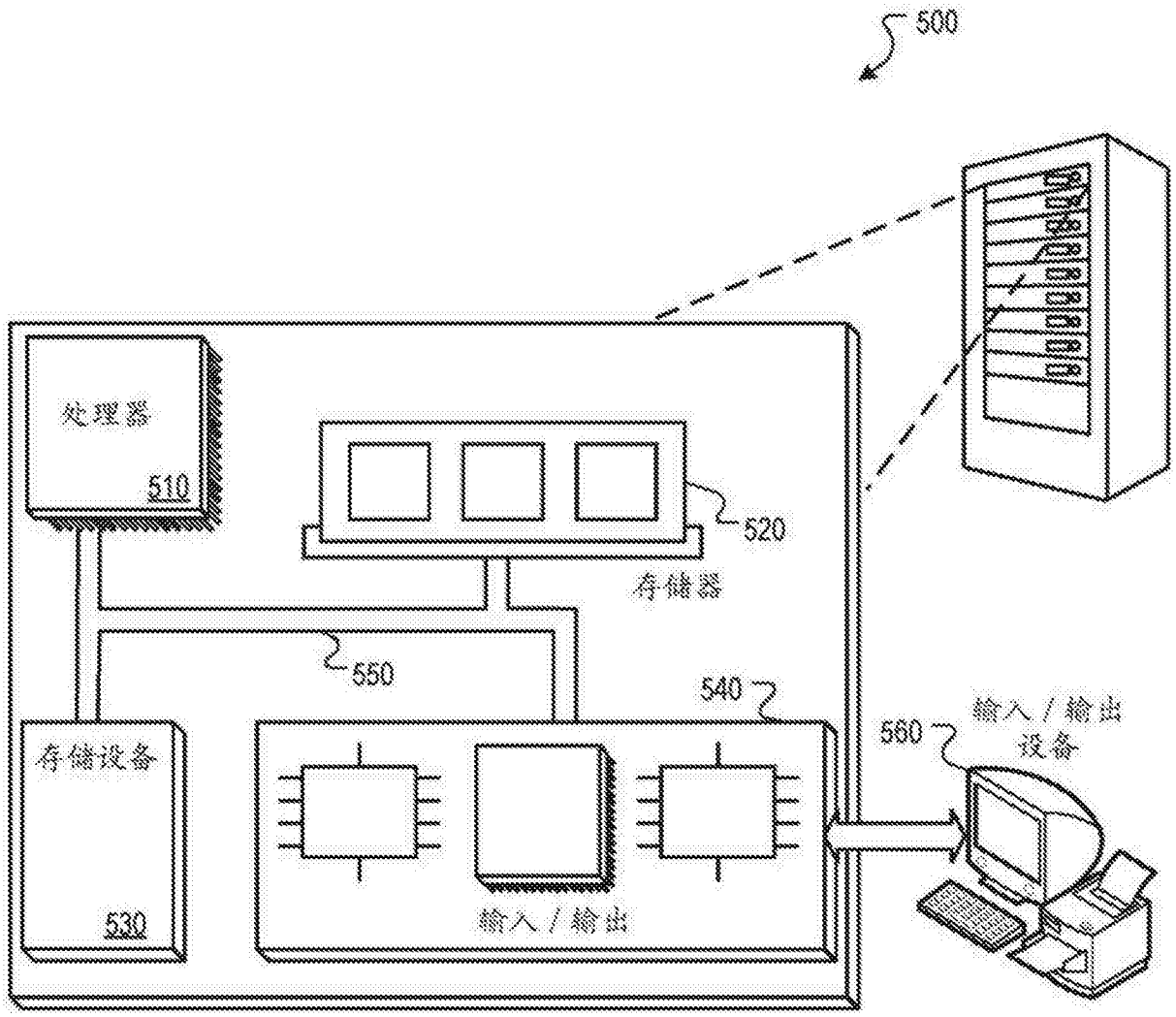


图5