(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 107547494 B
(45)授权公告日 2020.12.18

(21)申请号 201610867335.2
(22)申请日 2016.09.29
(65)同一申请的已公布的文献号
申请公布号 CN 107547494 A
(43)申请公布日 2018.01.05
(30)优先权数据
2016125283 2016.06.24 RU
15/237,738 2016.08.16 US
(73)专利权人 卡巴斯基实验室股份制公司
地址 俄罗斯莫斯科
(72)发明人 德米特里·L·彼得罗维切夫
阿提姆·O·巴拉诺夫
叶夫根尼·V·贡恰罗夫
(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 黄志华 何月华
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
(56)对比文件
WO 2013089771 A1,2013.06.20
WO 2013089771 A1,2013.06.20
US 2011321139 A1,2011.12.29
CN 105516169 A,2016.04.20
CN 105429934 A,2016.03.23
US 2014180931 A1,2014.06.26
审查员 舒维莹

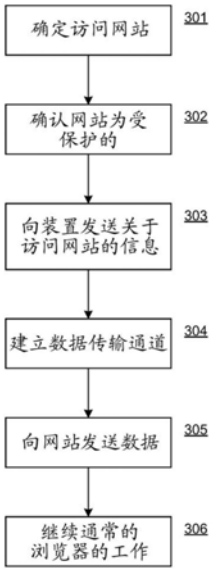
权利要求书3页 说明书9页 附图5页

(54)发明名称

用于安全在线认证的系统和方法

(57)摘要

本发明公开了一种用于安全在线认证的系统和方法。示例性方法包括:经由计算装置的处理器,确定在安装在计算机系统上的浏览器应用程序与受保护的网站之间建立连接;响应于从所述受保护的网站获得用于认证的请求,获得有关所述受保护的网站的信息;与所述受保护的网站建立受保护的数据传输通道,以接收所述受保护的网站的至少一个证书;执行认证并向所述受保护的网站发送认证数据;以及响应于来自所述受保护的网站的成功的认证的指示,向所述浏览器应用程序发送识别信息,以使得能够访问所述受保护的网站。



CN 107547494 B

1.一种用于安全在线认证的计算机实现的方法,所述方法包括:

经由安全连接装置的处理器,确定在安装在计算机系统上的浏览器应用程序与受保护的网站之间建立连接,其中,所述计算机系统不同于所述安全连接装置;

响应于所述浏览器应用程序的插件确定了所述计算机系统已经从所述受保护的网站获得用于认证的请求,在所述安全连接装置处获得有关所述受保护的网站的信息;

在所述安全连接装置与所述受保护的网站之间建立受保护的数据传输通道,以在所述安全连接装置处接收所述受保护的网站的至少一个证书;

从所述浏览器应用程序的插件接收与所述受保护的网站相关联的除了根证书以外的完整的证书树;

基于存储在所述安全连接装置上的根证书的列表,验证所述完整的证书树的有效性;

当所述完整的证书树的有效性未通过验证时,断开所述受保护的数据传输通道;

响应于所述完整的证书树已通过验证,执行认证并从所述安全连接装置向所述受保护的网站发送存储在所述安全连接装置上的认证数据;以及

响应于来自所述受保护的网站的成功的认证的指示,从所述安全连接装置向所述浏览器应用程序的所述插件发送新的会话的标识符,以使得能够访问所述受保护的网站。

2.根据权利要求1所述的计算机实现的方法,其中,确定在安装在所述计算机系统上的所述浏览器应用程序与所述受保护的网站之间建立连接包括:

经由通过所述浏览器应用程序所提供的应用程序接口API获得所述受保护的网站的统一资源标识符URI地址。

3.根据权利要求1所述的计算机实现的方法,其中,确定在安装在所述计算机系统上的所述浏览器应用程序与所述受保护的网站之间建立连接包括:

经由安装在所述安全连接装置上的驱动器拦截所述浏览器应用程序与所述受保护的网站之间的网络流量,以获得所述受保护的网站的统一资源标识符URI地址。

4.根据权利要求1所述的计算机实现的方法,还包括针对通过所述计算机系统所访问的受保护的网站的地址列表确认所述受保护的网站。

5.根据权利要求4所述的计算机实现的方法,还包括在所述安全连接装置上,存储通过所述计算机系统所访问的所述受保护的网站的地址列表和有关所述受保护的网站的加密数据。

6.根据权利要求1所述的计算机实现的方法,其中,有关所述受保护的网站的所述信息包括:URI地址、有关所述受保护的网站的所述至少一个证书的信息、关于所述受保护的网站的域的WHOIS信息、所述URI地址中的从针对请求的回答所获得的标头的列表、有关以卷积或散列和的形式的下载的脚本的信息。

7.根据权利要求1所述的计算机实现的方法,还包括:

基于所获得的有关所述受保护的网站的信息,检查所述受保护的网站的有效性,所述信息包括所获得的标头或在建立所述连接时下载的脚本的列表。

8.根据权利要求1所述的计算机实现的方法,还包括:

获得第二认证因素,以用于执行所述认证并向所述受保护的网站发送所述认证数据。

9.根据权利要求1所述的计算机实现的方法,还包括:

在向所述浏览器应用程序发送识别信息以使得能够访问所述受保护的网站之后,继续

使用浏览器应用程序访问所述受保护的网站。

10.根据权利要求8所述的计算机实现的方法,还包括:

在所述安全连接装置上存储与所述计算机系统的用户相关联的个人数据;和

在从所述插件接收到登录形式信息后,建立所述受保护的数据传输通道。

11.根据权利要求10所述的计算机实现的方法,还包括:

加密和存储关于用户账户以及所述安全连接装置上的交易的支付数据。

12.根据权利要求11所述的计算机实现的方法,还包括:

响应于获得所述第二认证因素,解密所述支付数据;和

将所述支付数据传输到所述受保护的网站。

13.根据权利要求1所述的计算机实现的方法,还包括:

由所述安全连接装置请求与所述计算机系统的最近防病毒活动有关的信息;

根据一系列规则验证接收到的所述信息;和

根据所述验证确定所述受保护的数据传输通道的设置。

14.一种用于安全在线认证的系统,包括:

安全连接装置的至少一个处理器,所述至少一个处理器被配置成:

确定在安装在计算机系统上的浏览器应用程序与受保护的网站之间建立连接,其中,所述计算机系统不同于所述安全连接装置;

响应于所述浏览器应用程序的插件确定了所述计算机系统已经从所述受保护的网站获得用于认证的请求,获得有关所述受保护的网站的信息;

在所述安全连接装置与所述受保护的网站之间建立受保护的数据传输通道,以在所述安全连接装置处接收所述受保护的网站的至少一个证书;

从所述浏览器应用程序的插件接收与所述受保护的网站相关联的除了根证书以外的完整的证书树;

基于存储在所述安全连接装置上的根证书的列表,验证所述完整的证书树的有效性;

当所述完整的证书树的有效性未通过验证时,断开所述受保护的数据传输通道;

响应于所述完整的证书树已通过验证,执行认证并从所述安全连接装置向所述受保护的网站发送存储在所述安全连接装置上的认证数据;以及

响应于来自所述受保护的网站的成功的认证的指示,从所述安全连接装置向所述浏览器应用程序的所述插件发送新的会话的标识符,以使得能够访问所述受保护的网站。

15.根据权利要求14所述的系统,其中,为了确定在安装在所述计算机系统上的所述浏览器应用程序与所述受保护的网站之间建立连接,所述处理器被配置成:

经由通过所述浏览器应用程序所提供的应用程序接口API获得所述受保护的网站的统一资源标识符URI地址;或者

经由驱动器拦截所述浏览器应用程序与所述受保护的网站之间的网络流量,以获得所述受保护的网站的统一资源标识符URI地址。

16.根据权利要求14所述的系统,其中,所述处理器还被配置成:

存储通过所述计算机系统所访问的受保护的网站的地址列表和有关所述受保护的网站的加密数据;以及

针对通过所述计算机系统所访问的受保护的网站的所述地址列表确认所述受保护的

网站。

17.根据权利要求14所述的系统，其中，有关所述受保护的网站的所述信息包括：URI地址、有关所述受保护的网站的所述至少一个证书的信息、关于所述受保护的网站的域的WHOIS信息、所述URI地址中的从针对请求的回答所获得的标头的列表、有关以卷积或散列和的形式的下载的脚本的信息。

18.根据权利要求14所述的系统，其中，所述处理器还被配置成：

基于所获得的有关所述受保护的网站的信息，检查所述受保护的网站的有效性，所述信息包括所获得的标头或在建立所述连接时下载的脚本的列表。

19.根据权利要求14所述的系统，其中，所述处理器还被配置成：

在向所述浏览器应用程序发送识别信息以使得能够访问所述受保护的网站之后，继续使用浏览器应用程序访问所述受保护的网站。

用于安全在线认证的系统和方法

[0001] 相关申请的交叉引用

[0002] 本申请要求2016年6月24日提交的俄罗斯申请No.2016125283的优先权权益，该俄罗斯申请通过引用并入本文。

技术领域

[0003] 本发明总体涉及数据安全领域，更具体地，涉及一种安全在线认证的系统和方法。

背景技术

[0004] 当前存在大量的用于执行各种在线交易的软件。许多的在线交易涉及银行服务和电子转账。这些交易通常经由标准的互联网浏览器和单独的银行客户端(应用程序)来执行，这在移动平台上尤其受欢迎。在有关在线交易的其它应用程序中，电子货币系统可以充当示例，例如WebMoney或PayPal、或者在线游戏，该在线游戏使用它们自身的微交易系统，用户在微交易期间用真实的资金(例如通过使用他们的信用卡)购买游戏中的物品或游戏中的货币。

[0005] 随着在线支付的增长，黑客已经变得对该服务行业非常感兴趣并且出于非法(欺骗性)的资金转移的目的而积极地尝试拦截交易数据的可能的方法。在一个示例中，这种数据的盗窃可以使用恶意程序(或者使用网络钓鱼)来进行，恶意程序(或者网络钓鱼)接触上用户的计算机(感染它们)。通常，这些程序可以通过感染流行的互联网浏览器而接触计算机，拦截正从数据输入装置(例如键盘或鼠标)输入的数据，或者拦截正在网络上发送的数据。例如，感染浏览器的恶意程序访问浏览器文件并且搜索在访问网页时所保存的浏览历史和密码。例如，数据输入拦截器(键盘记录器)可以从键盘或鼠标拦截数据的输入，拍摄屏幕的照片(截屏)并使用各种隐匿技术隐藏它们在系统中的存在。类似的技术也可以用来创建网络数据包的拦截器(流量嗅探器)，其在发送网络数据包时拦截该网络数据包并从该网络数据包提取有价值的信息，例如密码和其它的个人数据。应当注意的是，感染很多时候是由于软件中的漏洞而发生，软件中的漏洞使得可以执行各种漏洞利用以进入计算机系统然后安装恶意软件。

[0006] 现有的防病毒技术(例如签名或启发式分析的使用、主动防御方法或可信应用程序的列表(白名单)的使用)可以能够检测用户的计算机上的一些恶意程序，但是不可能总是能够确定它们的新的修改，新的修改的出现频率可能每天都在增大。因此，期望有用于安全防护便于用户在线支付的程序的强健的解决方案。

[0007] 一些现有的软件和硬件解决方案介绍了认证的补充因素，例如向用户的移动电话或者经由使用用于用户认证的硬件发送一次性密码(one-time password，OTP)。然而，这些解决方案也可以是有漏洞的。可拦截OTP的有害程序的一个示例可以包括恶意程序宙斯。因此，需要改进的解决方案以便保护用户的数据以防在在线交易期间被拦截。

发明内容

[0008] 公开了用于安全在线认证的系统和方法。在一个示例性方面中，一种用于安全在线认证的计算机实现的方法包括：经由计算装置的处理器，确定在安装在计算机系统上的浏览器应用程序与受保护的网站之间建立连接；响应于从所述受保护的网站获得用于认证的请求，获得有关所述受保护的网站的信息；与所述受保护的网站建立受保护的数据传输通道，以接收所述受保护的网站的至少一个证书；执行认证并向所述受保护的网站发送认证数据；以及响应于来自所述受保护的网站的成功的认证的指示，向所述浏览器应用程序发送识别信息以使得能够访问所述受保护的网站。

[0009] 在另一示例性方面中，确定在安装在所述计算机系统上的所述浏览器应用程序与所述受保护的网站之间建立连接包括：经由通过所述浏览器应用程序所提供的应用程序接口(API)获得所述受保护的网站的统一资源标识符(URL)地址；或者经由驱动器拦截所述浏览器应用程序与所述受保护的网站之间的网络流量，以获得所述受保护的网站的统一资源标识符(URL)地址。

[0010] 在又一示例性方面中，所述方法还包括：针对通过所述计算机系统所访问的所述受保护的网站的地址列表确认所述受保护的网站；在所述计算装置上，存储通过所述计算机系统所访问的所述受保护的网站的地址列表和有关所述受保护的网站的加密数据。

[0011] 在另一示例性方面中，有关所述受保护的网站的所述信息包括：URL地址、有关所述受保护的网站的所述至少一个证书的信息、关于所述受保护的网站的域的WHOIS信息、所述URL地址中的从针对请求的回答所获得的标头的列表、有关以卷积或散列和的形式的下载的脚本的信息。

[0012] 在又一示例性方面中，与所述受保护的网站建立所述受保护的数据传输通道包括：经由安装在所述计算机系统上的驱动器建立所述受保护的数据传输通道；从所述驱动器获得用于所述受保护的网站的完整的证书树，以检查所述至少一个证书的有效性；以及使用所述计算装置的根证书的列表，确定用于所述受保护的网站的所述完整的证书树的有效性。

[0013] 在另一示例性方面中，所述方法还包括：基于所获得的有关所述受保护的网站的信息，检查所述受保护的网站的有效性，所述信息包括所获得的标头或在建立所述连接时下载的脚本的列表；以及获得第二认证因素，以用于执行所述认证并向所述受保护的网站发送所述认证数据。

[0014] 在另一示例性方面中，所述方法还包括：在向所述浏览器应用程序发送识别信息以使得能够访问所述受保护的网站之后，继续使用浏览器应用程序访问所述受保护的网站。

[0015] 在另一示例性方面中，一种安全在线认证的系统包括计算装置的至少一个处理器，所述至少一个处理器被配置成：确定在安装在计算机系统上的浏览器应用程序与受保护的网站之间建立连接；响应于从所述受保护的网站获得用于认证的请求，获得有关所述受保护的网站的信息；与所述受保护的网站建立受保护的数据传输通道，以接收所述受保护的网站的至少一个证书；执行认证并向所述受保护的网站发送认证数据；以及响应于来自所述受保护的网站的成功的认证的指示，向所述浏览器应用程序发送识别信息以使得能够访问所述受保护的网站。

[0016] 以上对本发明的示例方面的简要概述用来提供对本发明的基本理解。该概述并不是对所有预期方面的广泛综述，并且既不旨在识别所有方面的关键要素或重要要素，也不旨在描绘本发明的任何方面或所有方面的范围。它的唯一目的是以简化形式呈现一个或多个方面，作为随后的对本发明的更详细的描述的前奏。为了实现前述目的，本发明的一个或多个方面包括权利要求中所描述和示例性指出的特征。

附图说明

[0017] 并入本说明书中并构成本说明书的一部分的附图示出了本发明的一个或多个示例性方面，以及连同详细的描述一起用来阐述这些示例性方面的原理和实现方式。

[0018] 图1示出用户在不可信环境的条件中访问网站的过程。

[0019] 图2示出用于在不可信环境的条件中安全的在线认证的示例性系统。

[0020] 图3示出安全在线认证的示例性方法。

[0021] 图4示出安全在线认证的示例性方法的展开图。

[0022] 图5示出其上可实施所公开的系统和方法的方面的通用计算机系统的示例配置。

具体实施方式

[0023] 本文中在安全在线认证的系统、方法和计算机程序产品的上下文中描述了示例性方面。本领域的普通技术人员将认识到，以下描述仅仅是说明性的，而不旨在以任何方式进行限制。其它方面将容易地将其自身暗示给了解本发明的优点的本领域的技术人员。现在将详细地参考如附图中所示的示例性方面的实现方式。贯穿附图和以下描述将尽可能地使用相同的附图标记来指代相同或类似的项目。

[0024] 图1示出了用户在不可信环境的条件中访问网站的过程。不可信环境可以包括计算机系统100，即使在计算机系统100上安装防病毒应用程序110，也会仍然有存在恶意应用程序120的风险，恶意应用程序120会危害用户150通过浏览器130使用受保护的网站140(即，利用需要在与其交互时保护正被接收和发送的数据的网站)的工作。可以将防病毒应用程序110设计成针对漏洞和恶意应用程序的存在扫描安装在计算机系统100上的操作系统。防病毒扫描的结果可以表明以下状态：已经发现了多少和哪些恶意程序和漏洞。如上面所指出的，搜索并检测恶意应用程序的防病毒技术可能无法保证检测到并去除所有恶意应用程序，这是由于恶意应用程序的创建者可能针对避开防病毒扫描的方式而不断地工作。例如，已知用于混淆待执行的代码以使得签名和启发式分析更加困难的方法，以及可以避免通过防病毒应用程序在恶意应用程序的仿真期间检测恶意应用程序的反-仿真的方法。因此，需要用于保护正从网站140接收和发送的数据的解决方案。

[0025] 图2示出了用于在不可信环境的条件中安全的在线认证的示例性系统。相较于图1，可以增加用于安全的数据传输的装置115和浏览器中的插件135。更具体地，可以将插件135设计成确定用户150已经建立经由浏览器130到受保护的网站140的连接，并且将已经与受保护的网站140发生连接的信息发送到用于安全的数据传输的装置115。在一些方面，插件135可被提供为防病毒应用程序110的一部分。

[0026] 连接的建立可以通过插件135经由应用程序接口(application programming interface，API)来确定，API由浏览器130来提供，并且在API中可以通过GET或POST请求的

分析来确定网站140的统一资源标识符(uniform resource identifier,URL)地址。

[0027] 可替选地,插件135可以要求安装单独的驱动器136(其可以是插件135的一部分或者是单独的应用程序),以用于拦截浏览器130与网站140之间的网络流量。至少基于所拦截的数据,可以确定网站140的URL地址。这种驱动器也可以用来建立装置115与网站140之间的单独的连接。该驱动器还可以获得关于网站140的信息,例如网站140的证书。

[0028] 受保护的地址的列表连同认证所需要的加密的数据可以存储在用于安全的数据传输的装置115上。在装置115激活(连接到计算机100)时,受保护的地址的列表可被下载到插件135的存储器,插件135可以针对正由用户所访问的每一个地址在该列表上的存在扫描该地址。插件135可以将地址的列表保存在其自身的存储器中或计算机系统100的硬盘上。

[0029] 因此,受保护的网站的地址的列表可被保存在插件135中或用于安全的数据传输的装置115中。通常,这种列表可以由用户150自身创建或者由用于安全的数据传输的装置115或插件135的开发者(通常为用于安全的数据传输的装置115和插件135中的一者的开发者或二者的开发者)创建。根据本发明的多个方面,可以有多个确保用户安全访问网站的方式。确保安全访问网站的技术的一个示例可以包括由卡巴斯基实验室所开发的“安全支付”技术。

[0030] 响应于从受保护的网站140获得用于认证的请求,插件135可以将该地址和请求(包括关于该网站的信息,例如认证的形式)本身发送到装置115。插件135还可以发送用于在装置115上扫描的补充信息,例如:URL地址、关于网站的一个或多个证书的信息、关于域的WHOIS信息、URL地址中的从针对请求的回答所获得的标头的列表、关于以卷积形式的下载的脚本的信息(散列和)。

[0031] 在一个示例性方面中,装置115可以包括真实的软件和/或硬件装置、系统、部件、由使用硬件所实现的部件的组(例如集成微电路(专用集成电路(application-specific integrated circuit,ASIC))或可编程门阵列(现场可编程门阵列(field-programmable gate array,FPGA)))或例如以软件和硬件的组合的形式的部件的组(例如微处理器系统和一组程序指令)、或者基于神经突触芯片的部件的组。

[0032] 在一个示例性方面,用于安全的数据传输的装置115可以包括处理器、用于存储并使用暂存数据的存储器模块、具有创建并加密分区的能力的数据介质以及用于连接到计算机系统100的最少一个适配器(通常为USB)以及用于输入/获得用户认证因素的装置。如上面所讨论的,装置115可以将受保护的网站的地址的列表以及有关这些网站的加密的数据(这通常可以包括登录名/密码关联和认证形式的其它数据,而且还可以包括其它的例如支付数据的机密用户数据)一起保存。该列表可以从装置115下载到插件的存储器中,以用于与每一个后续的请求相比较。

[0033] 紧接在接收由插件135所发送的用于认证的请求之后,装置115可以启动新的受保护的到网站140的连接的创建,装置115可以从网站140获得证书。新的受保护的连接可以由驱动器136来创建。为了检查(验证)所接收到的证书,装置115可以针对除了根证书以外的用于网站140的完整的证书树质询安装在计算机100上的驱动器136。使用其自身的根证书列表,装置115可以检查用于网站140的整个的证书链的有效性(可信赖性)。如果检查不成功,则可以断开受保护的连接。装置115还可以使用来自插件135的其它的信息(例如,在建立连接时所获得的下载的脚本的标头或列表),以用于检查网站140。例如,装置115可以将

从插件135获得的、来自于网站140的下载的脚本的卷积(散列和)与其自身的可保存在装置115上的散列和进行比较,如果卷积不匹配,则可以断开到网站140的连接。

[0034] 在一个示例性方面中,信息(例如用户的个人数据)可以存储在装置115中的数据介质上,并且在从插件135接收数据时可以实现可执行的代码。在一个方面中,使用装置115的工作可以仅仅利用插件135来进行。例如,公钥基础设施(Public Key Infrastructure,PKI)架构可以用于数据的认证和交换。用于装置115的私有密钥可以由给定的装置的开发商提供。

[0035] 在另一示例性方面中,插件135可以通过使用单独的API要求访问可存储在插件135的存储器中的数据,这可以允许类似于装置115的外部装置的开发商来使用给定的插件。

[0036] 装置115的另一功能可以包括第二用户认证因素的实现。第二认证因素的使用可以利用OTP、用户的数字签名的确认或用户的生物识别数据来实现。这使得可以保护用户的认证数据免于在被偷窃时装置115的存储转储。仅仅在接收第二认证因素之后,装置115才能够解密用户的认证数据并将其发送到网站140,犹如该数据已被填写并通过使用浏览器130而进行发送。

[0037] 装置115可以执行认证并发送有关网站140的必要的认证数据。除了该认证数据,装置115还可以存储其它信息,例如用户的账户/交易的支付数据。这种信息可以以加密的形式进行存储并且可以仅仅在获得关于第二认证因素的执行的信息之后才可被解密。响应于从网站140获得关于成功的认证的响应,装置115可以向插件135发送新的会话的标识符和识别已认证的用户所需的其它信息,插件135可以响应于浏览器向网站140分发原始的请求而向浏览器130分发新的会话的标识符和识别已认证的用户所需的其它信息。因此,浏览器130马上可以获得用户的新的会话的数据,由此继续通常的网上冲浪,而且现在对于网站作为已认证的用户。

[0038] 在另一示例性方面中,用户的信息可以经由具有已经由银行(其还拥有网站140)所包含的用户数据的装置115的出售而存储在装置115上。可替选地,插件135可以记录在网站140(例如它可以扮演密码管理者的角色)上的用户的信息并将该信息发送到装置115。

[0039] 在另一示例性方面中,可以向网站140发送用户150的认证数据。来自装置115的信息可以响应于网站140而以至少一种以下方式来发送:

[0040] • 将该数据插入到网站140的网页上。某一数据(例如登录名和密码)可以与该网页的URL地址相关联并且可以被插入在一定的字段中(作为规则,用于插入登录名和密码的字段具有多个属性(例如标签“输入(input)”的属性“密码(password)”),可以通过这些多个属性来计算这些字段)。

[0041] • 该数据可以预先以GET/POST请求的形式来准备,并且可以在特定时刻或者在某一事件发生时被分发到服务器。最简单的示例可以包括在从网站接收针对用于网页的GET请求的响应之后,分发具有以所述形式插入的登录名和密码数据的POST请求,所述登录名和密码需要被插入到网页中。

[0042] 图3示出了根据本发明的方面的安全在线认证的示例性方法。在步骤301中,可以确定用户使用浏览器130访问网站(用户已经完成了连接),在该步骤之后,在步骤302中,可以确定该网站为受保护的网站140。关于网站140的地址的确定的更多的细节已经在图2的

描述中在插件135的工作的描述的上下文中给出。在步骤303中，装置115可以从插件135接收关于用户访问网站140的这一事实的信息(即，用户可能已经完成了连接)，在步骤303之后，在步骤304中装置115可以建立并使用受保护的数据传输通道。在一个方面中，受保护的数据通道可以包括超文本传输协议安全(Hyper Text Transfer Protocol over Secure Socket Layer，HTTPS)连接。在步骤305中，装置115可以提取关于网站140的所有信息并经由受保护的数据传输通道发送该所有信息。在步骤306中，用户可以继续以通常的方式在浏览器130中工作。

[0043] 参照图4，在用户经由浏览器130的普通网上冲浪期间(步骤1)，认证形式可以来自网站140(步骤2)，插件135可以拦截该认证形式并将其发送到装置115(步骤3)。装置115可以使用插件135与网站140建立额外的、直接的https连接(步骤4)并接收该网站的证书(步骤5)。为了检查该证书的有效性，装置115可以从来自用户的计算机的插件135请求完整的证书树(步骤6)。使用装置115的自身的根证书的列表(存储在装置115上)，可以在装置115上执行所接收(步骤7)的证书的有效性的检查(步骤8)，并且可以对应于网站140，在装置115上为给定的计算机检索认证数据(步骤9)。然后可以向用户发送请求，以获得第二认证因素(例如直接输入到装置115中的指纹或密码)(步骤10)，并且可以解密装置115的存储器中的认证数据(步骤11)。在成功的执行前述步骤之后，装置115(在插件135的帮助下，插件135可以仅仅建立TCP连接并向装置115发送数据)可以完成建立与网站140的https连接(步骤12)，并且向网站140发送填写的认证形式(步骤13)。对于服务器(网站140)，这可能看起来像从浏览器130获得填写的形式。从服务器获得的响应(步骤14)可以通过装置115中继至插件135，插件135可以将该响应直接发送到浏览器130(步骤15)，从而浏览器130马上可以获得新的会话(步骤16)，具有完整传递的认证机制。

[0044] 在另一示例性方面中，可以在装置115与网站140之间建立安全的数据传输通道。如上面所讨论的，计算机系统100可能感染有未被防病毒应用程序110所检测到的恶意应用程序120。假定装置115可能没有访问计算机系统110的资源并且可能没有执行该系统的补充扫描，则装置115也可以定期地或在向防病毒应用程序110请求的时候从防病毒应用程序110请求以下数据，以向网站140发送数据：

[0045] • 上一次防病毒扫描的时间和状态；

[0046] • 防病毒数据库的更新状态；

[0047] • 到互联网的连接的类型；

[0048] • 关于最近已知的计算机威胁的信息，该信息由防病毒软件(antivirus software，AV)的所有供应商提供，例如卡巴斯基实验室在参与卡巴斯基安全网络(Kaspersky Security Network，KSN)的上下文中提供这种信息。

[0049] 在获得给定的信息之后，该信息的验证可以在一系列规则的帮助下在装置115上发生：该一系列规则可以在装置115与网站140之间确定安全的数据传输通道的设置的选择。

[0050] 示例1：

[0051] 上一次防病毒扫描的时间和状态：一分钟前，未发现有害的软件。

[0052] 防病毒数据库的更新状态：已下载防病毒数据库的最新版本。

[0053] 到互联网的连接的类型：虚拟专用网络(Virtual Private Network，VPN)。

[0054] 关于最近已知的计算机威胁的信息:未发现。

[0055] 决定:可以通过插件135以解密的形式提供数据。

[0056] 示例2:

[0057] 上一次防病毒扫描的时间和状态:一分钟前,未发现有害的软件。

[0058] 防病毒数据库的更新状态:已下载防病毒数据库的最新版本。

[0059] 到互联网的连接的类型:开放访问。

[0060] 关于最近已知的计算机威胁的信息:检测到新种类的恶意软件宙斯。

[0061] 决定:可以通过插件135以加密的形式提供数据。

[0062] 示例3:

[0063] 上一次防病毒扫描的时间和状态:一星期前,发现有害的软件。

[0064] 防病毒数据库的更新状态:一个多星期前更新防病毒数据库。

[0065] 到互联网的连接的类型:开放访问。

[0066] 关于最近已知的计算机威胁的信息:未发现数据。

[0067] 决定:应当通过单独的受保护的连接以加密的形式提供数据。

[0068] 防病毒应用程序110可以将这些决定应用在计算机系统100上。在一些方面中,可以提供VPN连接的创建和使用。此外,可以对浏览器130和插件135的进程的地址空间提供补充的保护,以免受对恶意应用程序120的一部分的可能的扫描,以及还提供对剪贴板和进程间通信(IPC)信道的保护。

[0069] 图5示出了示例性计算机系统(其可以是个人计算机或服务器),根据示例性方面,所公开的系统(包括一个或多个模块)和方法可以在该示例性计算机系统上实现。如图所示,该计算机系统20可以包括中央处理单元21、系统存储器22和连接各种系统部件的系统总线23,各种系统部件包括与中央处理单元21相关联的存储器。系统总线23像现有技术已知的任何总线结构一样来实现,该任何总线结构依次包括总线存储器或总线存储器控制器、外围总线和本地总线,能够与任何其它的总线架构交互。系统存储器包括只读存储器(ROM)24和随机存取存储器(RAM)25。基本输入/输出系统(basic input/output system,BIOS)26包括确保在个人计算机20的元件之间的信息传输的基本程序,例如在使用ROM 24加载操作系统时的那些基本程序。

[0070] 然后,个人计算机20包括用于数据的读取和写入的硬盘27、用于在可移动磁盘29上读取和写入的磁盘驱动器28和用于在可移动光盘31(例如CD-ROM、DVD-ROM和其它的光学信息介质)上读取和写入的光盘驱动器30。硬盘27、磁盘驱动器28、和光盘驱动器30分别经过硬盘接口32、磁盘接口33和光盘驱动器接口34而连接到系统总线23。驱动器和对应的计算机信息介质为用于存储个人计算机20的计算机指令、数据结构、程序模块和其它数据的电源独立的模块。

[0071] 本发明提供了使用硬盘27、可移动磁盘29和可移动光盘31的系统的实现方式,但是应当理解的是,可以采用能够存储以计算机可读的形式的数据的其它类型的计算机信息介质56(固态驱动器、闪存卡、数字盘、随机存取存储器(RAM)等),该其它类型的计算机信息介质56经由控制器55连接到系统总线23。

[0072] 计算机20具有存储记录的操作系统35的文件系统36、以及另外的程序应用37、其它的程序模块38和程序数据39。用户能够通过使用输入设备(键盘40、鼠标42)将命令和信

息输入到个人计算机20中。可以使用其它的输入设备(未示出):麦克风、操纵杆、游戏控制器、扫描器等等。这样的输入设备通常通过串行端口46而插接到计算机系统20中,该串行端口46转而连接至系统总线,但这样的输入设备可以以其它方式(例如使用并行端口、游戏端口或通用串行总线(USB))被连接。监控器47或其它类型的显示设备也经过接口(诸如视频适配器48)连接至系统总线23。除了监控器47外,个人计算机还可以配备有其它的外围输出设备(未示出),诸如扬声器、打印机等。

[0073] 个人计算机20能够使用与一个或多个远程计算机49的网络连接,在网络环境中操作。一个或多个远程计算机49也是个人计算机或服务器,其具有在描述个人计算机20的性质时使用的上述元件中的大多数元件或全部元件,如图5所示。其它的设备也可以存在于计算机网络中,例如路由器、网站、对等设备或其它的网络节点。

[0074] 网络连接可以形成局域计算机网络(Local-Area computer Network,LAN)50和广域计算机网络(Wide-Area computer Network,WAN),该局域计算机网络诸如有线和/或无线网络。这种网络用在企业计算机网络和公司内部网络中,并且它们通常有权访问因特网。在LAN或WAN网络中,个人计算机20通过网络适配器或网络接口51连接到局域网50。当使用网络时,个人计算机20可以采用调制解调器54或其它的用于提供与广域计算机网络(例如因特网)的通信的模块。作为内部设备或外部设备的调制解调器54通过串行端口46连接至系统总线23。应当注意的是,网络连接仅仅是示例并且不需要描述网络的准确配置,即实际上具有通过技术通信模块(诸如蓝牙)建立一个计算机到另一个计算机的连接的其它方式。

[0075] 在各个方面中,本文所描述的系统和方法可以在硬件、软件、固件或它们的任何组合中实施。如果在软件中实施,则该方法可以被存储为在永久性计算机可读介质上的一个或多个指令或代码。计算机可读介质包括数据存储器。以示例性而非限制性的方式,这种计算机可读介质可以包括RAM、ROM、EEPROM、CD-ROM、闪存或其它类型的电存储介质、磁存储介质或光存储介质、或任何其它介质,该任何其它介质可用来承载或存储以指令或数据结构形式的所期望的程序代码并可以被通用计算机的处理器访问。

[0076] 如上所述,在各个方面中,本发明中所描述的系统和方法可以按照模块来处理。再次申明,本文所使用的术语“模块”指的是:现实世界的设备;部件;或使用硬件(例如通过专用集成电路(ASIC)或现场可编程门阵列(field-programmable gate array,FPGA))实施的部件的布置;或硬件和软件的组合,例如通过微处理器系统和实现模块功能的指令组,该指令组(在被执行时)将微处理器系统转换成专用设备。一个模块还可以被实施为两个模块的组合,其中单独地通过硬件促进某些功能,通过硬件和软件的组合促进其它功能。在某些实现方式中,模块的至少一部分、以及在某些情况下模块的全部可以被执行在通用计算机(例如上文在图5中更详细描述的通用计算机)的处理器上。因此,每一个模块可以以各种适合的配置来实现,而不应受限于本文所示例化的任何示例性实现方式。

[0077] 为了清楚起见,本文没有公开各个方面的所有例行特征。应当领会的是,在本发明的任何实际的实现方式的开发中,必须做出许多特定实现方式的决定,以便实现开发者的特定目标,并且这些特定目标将对于不同的实现方式和不同的开发者变化。应当理解的是,这种开发努力可能是复杂且费时的,但对于了解本发明的优点的本领域的普通技术人员来说仍然是工程的例行任务。

[0078] 此外,应当理解的是,本文所使用的措辞或术语出于描述而非限制的目的,从而本

说明书的术语或措辞应当由本领域技术人员根据本文所提出的教导和指导结合相关领域技术人员的知识来解释。此外,不旨在将本说明书或权利要求中的任何术语归于不常见的或特定的含义,除非明确如此阐述。

[0079] 本文所公开的各个方面包括本文以说明性方式所提到的已知模块的现在和未来知道的等同物。此外,尽管已经示出并描述了各个方面和应用,但是对于了解本发明的优点的本领域技术人员将显而易见的是,许多比上面所提及的内容更多的修改是可行的,而不脱离本文所公开的发明构思。

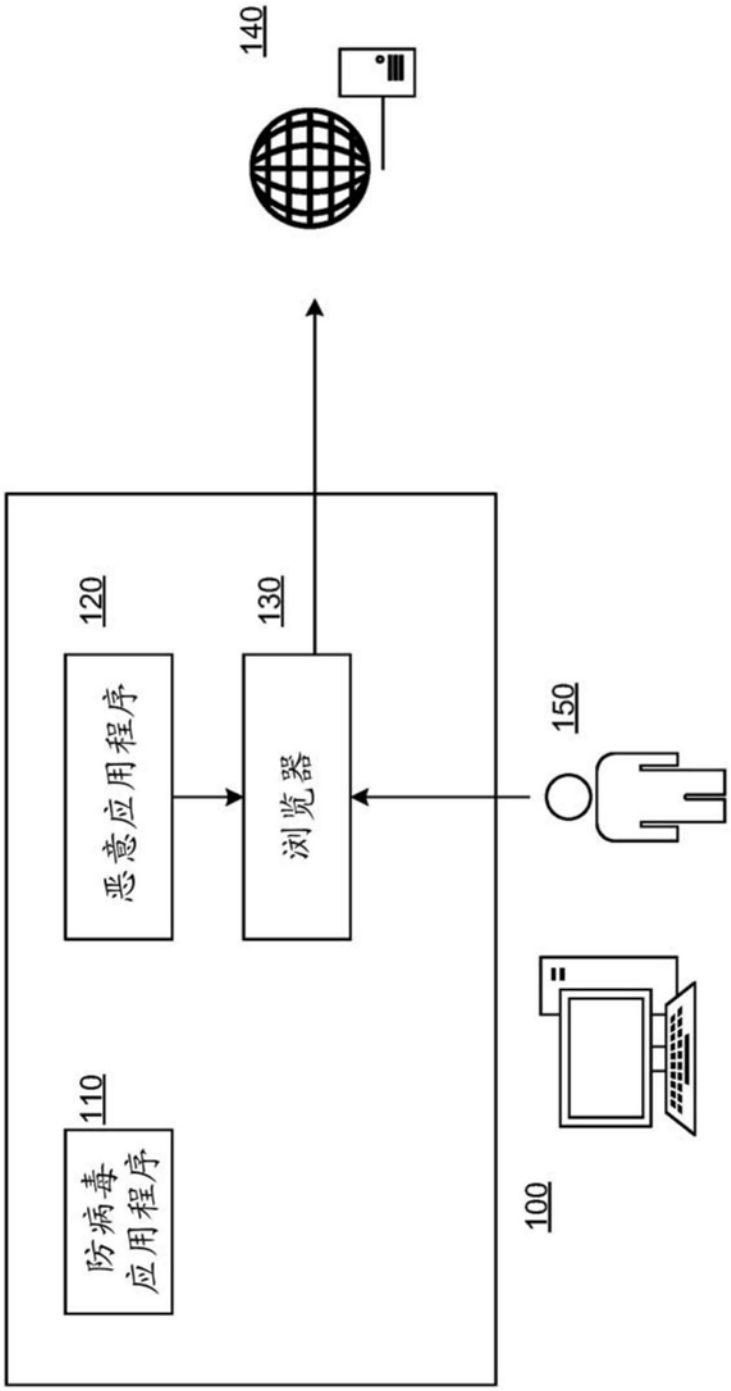


图1

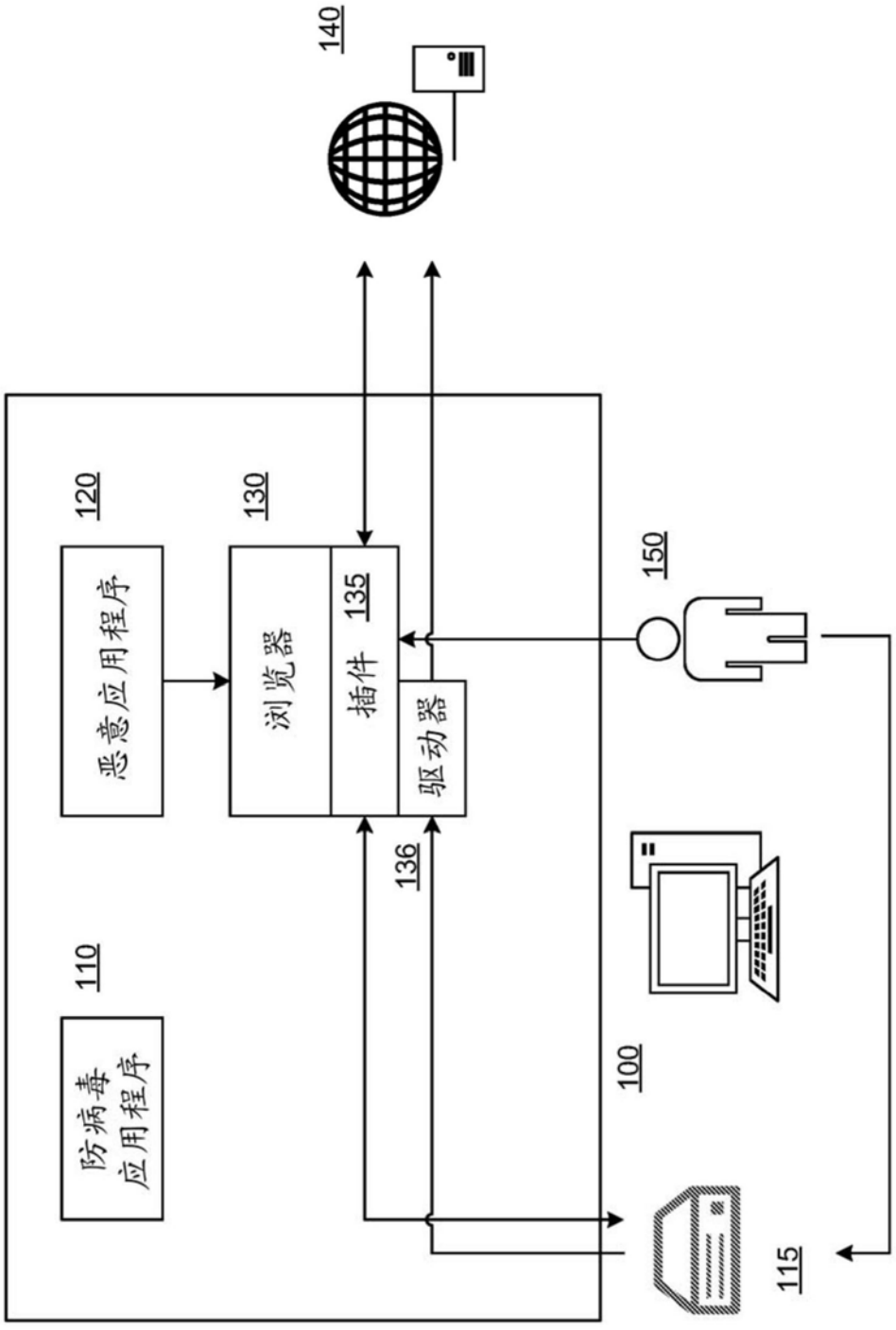


图2

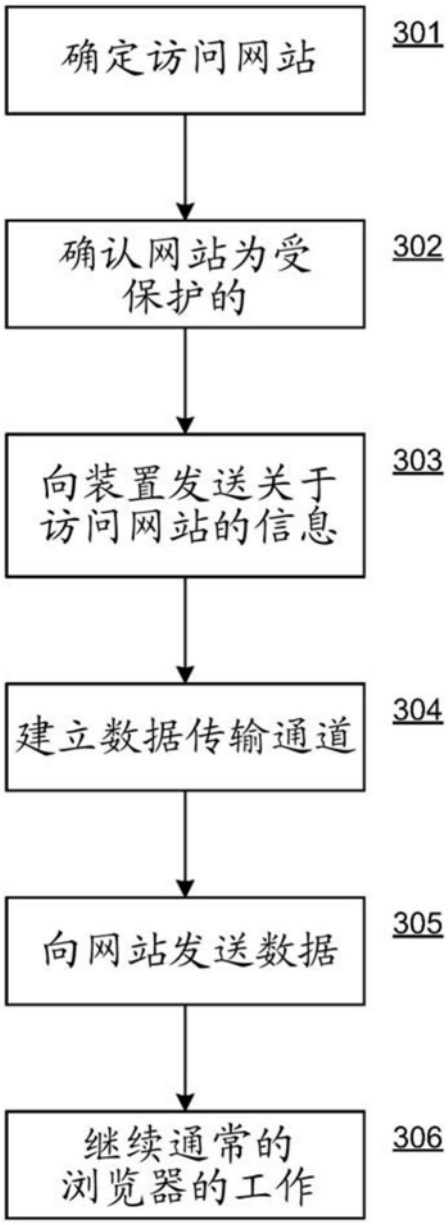

确定访问网站
301
确认网站为受保护的
302
向装置发送关于访问网站的信息
303
建立数据传输通道
304
向网站发送数据
305
继续通常的浏览器的工作
306

图3

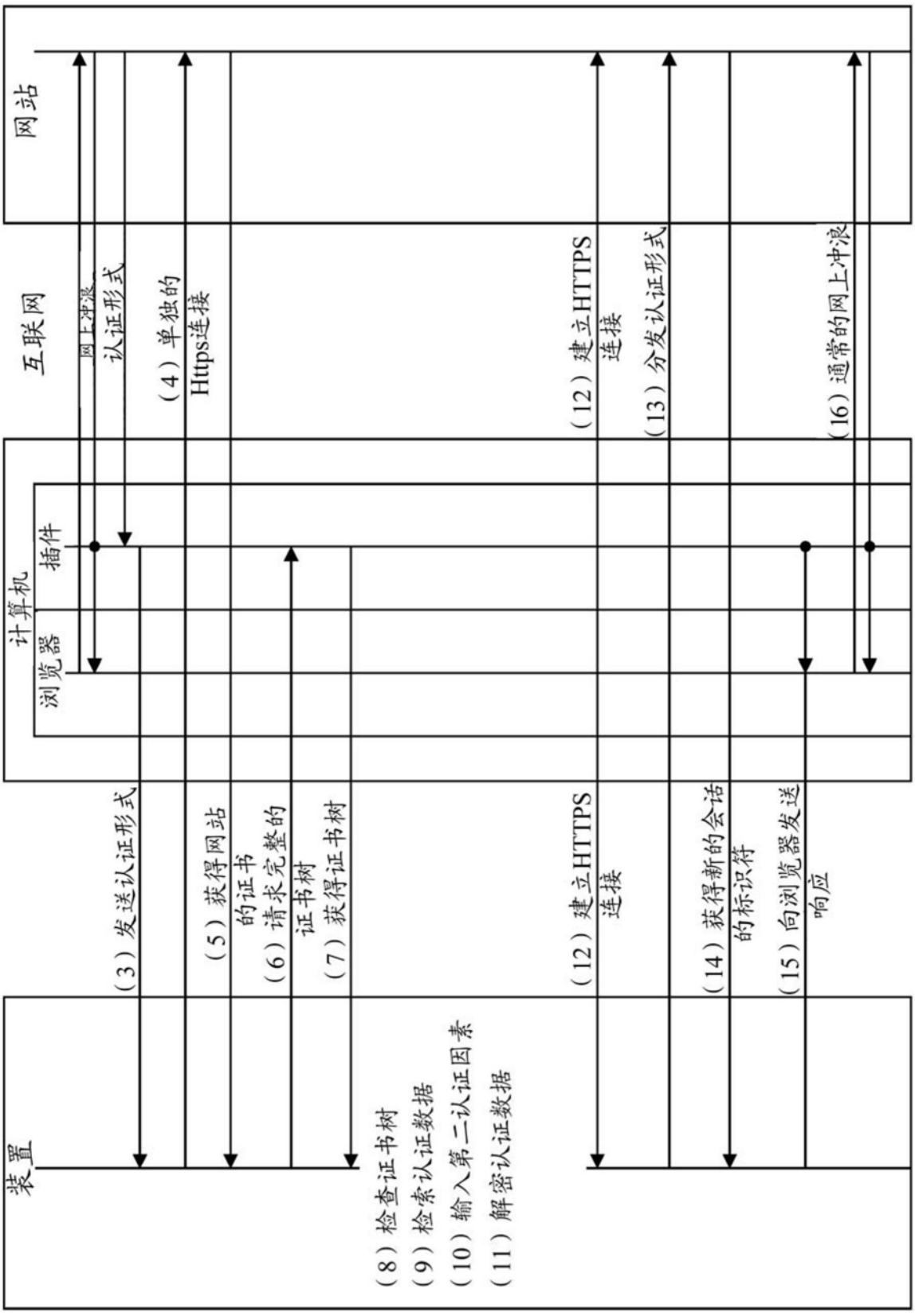

网站
互联网
网上冲浪
认证形式
(4)单独的
Https连接
计算机
浏览器
插件
(12)建立HTTPS
连接
(13)分发认证形式
(16)通常的网上冲浪
(3)发送认证形式
(5)获得网站
的证书
(6)请求完整的
证书树
(7)获得证书树
(12)建立HTTPS
连接
(14)获得新的会话
的标识符
(15)向浏览器发送
响应
装置
(8)检查证书树
(9)检索认证数据
(10)输入第二认证因素
(11)解密认证数据

图4

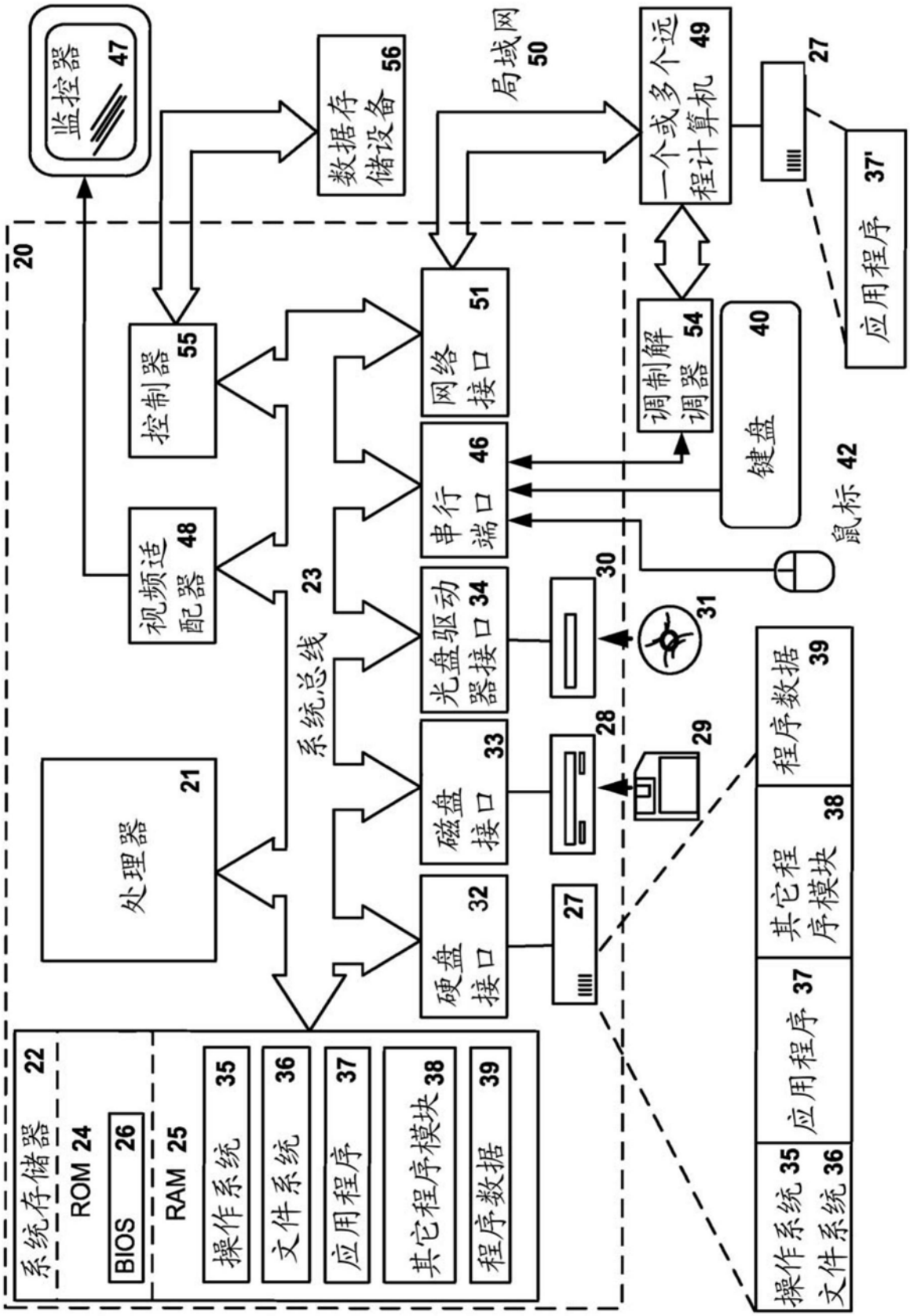

监控器 47
数据存储设备 56
局域网 50
一个或多个远程计算机 49
27
应用程序 37'
20
控制器 55
网络接口 51
调制解调器 54
40
键盘
视频适配器 48
串行端口 46
鼠标 42
系统总线 23
光盘驱动器接口 34
30
31
处理器 21
磁盘接口 33
28
29
程序数据 39
硬盘接口 32
27
其它程序模块 38
应用程序 37
操作系统 35
文件系统 36
系统存储器 22
ROM 24
BIOS 26
RAM 25
操作系统 35
文件系统 36
应用程序 37
其它程序模块 38
程序数据 39

图5