(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 108234519 A
(43)申请公布日 2018.06.29

(21)申请号 201810117685.6

(22)申请日 2014.09.29

(30)优先权数据
14/042,042 2013.09.30 US

(62)分案原申请数据
201410513789.0 2014.09.29

(71)申请人 瞻博网络公司
地址 美国加利福尼亚州

(72)发明人 K·亚当斯

(74)专利代理机构 北京市金杜律师事务所 11256
代理人 王茂华 李峥宇

(51)Int.Cl.
H04L 29/06(2006.01)

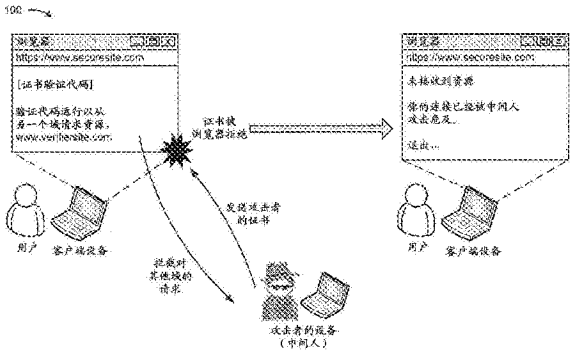
权利要求书3页 说明书14页 附图14页

(54)发明名称

检测和防止加密连接上的中间人攻击

(57)摘要

本申请涉及检测和防止加密连接上的中间人攻击。客户端设备可以向主机设备提供对访问主机域相关联的网站的请求。客户端设备可以基于该请求来接收验证代码，该验证代码标识验证域和与验证域相关联的资源，该验证域和该资源要被请求以用于验证公共密钥证书。验证域可以不同于主机域。客户端设备可以执行验证代码，并且可以基于执行该验证代码来从验证域请求该资源。客户端设备可以确定所请求的资源是否被接收，并且可以确定所请求的资源是否被接收来选择性地执行第一动作或第二动作。第一动作可以指示公共密钥证书无效，并且第二动作可以指示公共密钥证书有效。



CN 108234519 A

1.一种方法,包括:

由设备确定将被用于验证公共密钥证书的一个或多个验证域,

所述一个或多个验证域不同于与所述设备相关联的主机域;

由所述设备确定在所述公共密钥证书无效时将要执行的一个或多个动作;

由所述设备基于确定所述一个或多个验证域并且基于确定所述一个或多个动作来生成验证代码,以用于在不提示用户接受或拒绝所述公共密钥证书的情况下执行所述一个或多个动作;以及

由所述设备向客户端设备提供所述验证代码。

2.根据权利要求1所述的方法,其中所述一个或多个验证域包括顶级域和一个或多个次级域。

3.根据权利要求1所述的方法,其中确定所述一个或多个验证域包括:

标识将被用于验证所述公共密钥证书的多个验证域;以及

基于用户输入从所述多个验证域中选择所述一个或多个验证域。

4.根据权利要求1所述的方法,进一步包括:

确定将被请求以用于验证所述公共密钥证书的一个或多个资源,其中生成所述验证代码包括:

基于确定所述一个或多个验证域、基于确定所述一个或多个资源以及基于确定所述一个或多个动作来生成所述验证代码。

5.根据权利要求4所述的方法,其中所述一个或多个资源包括从所述一个或多个验证域中的验证域可访问的对象。

6.根据权利要求1所述的方法,其中所述一个或多个动作包括以下中的一个或多个:

第一动作,所述第一动作用于经由所述客户端设备提供与受危及的连接有关的通知,

第二动作,所述第二动作用于终止会话,或者

第三动作,所述第三动作用于要求所述用户从不同的局域网登陆。

7.根据权利要求1所述的方法,进一步包括:

将所述验证代码嵌入到用于网站的代码中,

其中提供所述验证代码包括:

提供具有所述验证代码的用于所述网站的代码,以用于由所述客户端设备的浏览器执行。

8.一种系统,包括:

一个或多个处理器,所述一个或多个处理器用于:

确定将被用于验证公共密钥证书的一个或多个验证域,

所述一个或多个验证域不同于主机域;

确定在所述公共密钥证书无效时将要执行的一个或多个动作;

基于确定所述一个或多个验证域并且基于确定所述一个或多个动作来生成验证代码,以用于在不提示用户接受或拒绝所述公共密钥证书的情况下执行所述一个或多个动作;以及

向客户端设备提供所述验证代码。

9.根据权利要求8所述的系统,其中所述一个或多个验证域包括顶级域和一个或多个

次级域。

10.根据权利要求8所述的系统，其中在确定所述一个或多个验证域时，所述一个或多个处理器用于：

标识将被用于验证所述公共密钥证书的多个验证域；以及

基于用户输入从所述多个验证域中选择所述一个或多个验证域。

11.根据权利要求8所述的系统，

其中所述一个或多个处理器进一步用于：

确定将被请求以用于验证所述公共密钥证书的一个或多个资源，以及

其中在生成所述验证代码时，所述一个或多个处理器用于：

基于确定所述一个或多个验证域、基于确定所述一个或多个资源以及基于确定所述一个或多个动作来生成所述验证代码。

12.根据权利要求11所述的系统，其中所述一个或多个资源包括从所述一个或多个验证域中的验证域可访问的对象。

13.根据权利要求8所述的系统，其中所述一个或多个动作包括以下中的一个或多个：

第一动作，所述第一动作用于经由所述客户端设备提供与受危及的连接有关的通知，

第二动作，所述第二动作用于终止会话，或者

第三动作，所述第三动作用于要求所述用户从不同的局域网登陆。

14.根据权利要求8所述的系统，

其中所述一个或多个处理器进一步用于：

将所述验证代码嵌入到用于网站的代码中，

其中在提供所述验证代码时，所述一个或多个处理器用于：

提供具有所述验证代码的用于所述网站的代码，以用于由所述客户端设备的浏览器执行。

15.一种存储指令的非瞬态计算机可读介质，所述指令包括：

一个或多个指令，所述一个或多个指令在由至少一个处理器执行时使得所述至少一个处理器：

确定将被用于验证公共密钥证书的一个或多个验证域，

所述一个或多个验证域不同于主机域；

确定在所述公共密钥证书无效时将要执行的一个或多个动作；

基于确定所述一个或多个验证域并且基于确定所述一个或多个动作来生成验证代码，以用于在不提示用户接受或拒绝所述公共密钥证书的情况下执行所述一个或多个动作；以及

向客户端设备提供所述验证代码。

16.根据权利要求15所述的非瞬态计算机可读介质，其中所述一个或多个验证域包括顶级域和一个或多个次级域。

17.根据权利要求15所述的非瞬态计算机可读介质，其中用于确定所述一个或多个验证域的一个或多个指令包括：

一个或多个指令，所述一个或多个指令用于：

标识将被用于验证所述公共密钥证书的多个验证域；以及

基于用户输入从所述多个验证域中选择所述一个或多个验证域。

18.根据权利要求15所述的非瞬态计算机可读介质，

其中所述指令进一步包括：

一个或多个指令，所述一个或多个指令用于确定将被请求以用于验证所述公共密钥证书的一个或多个资源，以及

其中用于生成所述验证代码的所述一个或多个指令包括：

一个或多个指令，所述一个或多个指令用于基于确定所述一个或多个验证域、基于确定所述一个或多个资源以及基于确定所述一个或多个动作来生成所述验证代码。

19.根据权利要求18所述的非瞬态计算机可读介质，其中所述一个或多个资源包括从所述一个或多个验证域中的验证域可访问的对象。

20.根据权利要求15所述的非瞬态计算机可读介质，其中所述一个或多个动作包括用于要求用户从不同的局域网登陆的动作。

检测和防止加密连接上的中间人攻击

[0001] 本申请为发明名称为“检测和防止加密连接上的中间人攻击”的原中国发明专利申请的分案申请。原申请的申请号为2014105137890，原申请的申请日为2014年09月29日，原申请的优先权日为2013年9月30日。

背景技术

[0002] 中间人攻击(man-in-the-middle attack)是一种形式的计算机安全漏洞，在该计算机安全漏洞中，攻击者(例如，黑客)制造与受害者的计算机的独立连接并且中继他们之间的消息，当事实上通信受到攻击者控制的时候，导致受害者相信受害者正在通过安全连接彼此直接通信。为了执行中间人攻击，攻击者拦截两个受害者之间的消息并且注入新的消息，这些新的消息然后被发送给受害者。如果受害者之间的连接被加密，攻击者可以通过哄骗用户(例如，客户端设备处的端用户)接受攻击者的公共密钥证书、而不是接受由认证机构认证的受信任的证书，来规避加密。攻击者可以从另一个受害者(例如，被托管在主机设备上的网站)接受受信任的证书。通过这种方式，攻击者可以与两个受害者使用证书，以与两个受害者建立加密通信会话，并且可以拦截、解密、告警、移除和插入受害者之间的消息，因此扮演中间人。

发明内容

[0003] 根据一些可能的实施方式，一种设备可以包括一个或多个处理器，该一个或多个处理器被配置为：提供对访问主机域的请求；基于对访问主机域的请求来接收验证代码，该验证代码标识验证域和经由验证域可访问的资源，该验证域和该资源用于验证公共密钥证书，其中该验证域不同于主机域；执行该验证代码；基于执行该验证代码来从验证域请求资源；确定所请求的资源是否被接收；以及基于所请求的资源是否被接收来选择性地执行第一动作或第二动作；其中基于确定所请求的资源未被接收，被标识在验证代码中的第一动作被执行；并且其中基于确定所请求的资源被接收，该第二动作被执行，并且其中第二动作不同于第一动作。

[0004] 根据一些可能的实施方式，一种计算机可读介质可以存储一个或多个指令，该一个或多个指令在被一个或多个处理器执行时使得该一个或多个处理器：向与主机域相关联的主机设备提供请求；基于该请求来从主机设备接收网页的内容，其中该网页的内容包括与验证代码有关的信息，该验证代码标识验证域和与验证域相关联的资源，该验证域和该资源要被用于验证公共密钥证书，其中该验证域不同于主机域；基于验证代码来从验证域请求该资源；确定所请求的资源是否被接收；以及基于所请求的资源是否被接收来由选择地执行第一动作或第二动作，其中第一动作指示公共密钥证书无效；其中第二动作指示公共密钥证书有效，并且其中第二动作不同于第一动作。

[0005] 根据一些可能的实施方式，一种方法可以包括：由客户端设备并且向主机设备提供对访问与主机域相关联的网站的请求；由客户端设备并且基于该请求来接收验证代码，该验证代码标识验证域和与验证域相关联资源，该验证域和该资源要被请求以用于验证公

共密钥证书，其中该验证域不同于主机域；由客户端设备执行验证代码；由客户端设备基于执行验证代码来从验证域请求该资源；由客户端设备确定所请求的资源是否被接收；以及基于确定所请求的资源是否被接收来选择性地执行第一动作或第二动作；其中第一动作指示公共密钥证书无效；并且其中第二动作指示公共密钥证书有效。

附图说明

[0006] 图1A和1B是本文中所描述的示例实施方式的概览的示图；

[0007] 图2是在其中本文中所描述的系统和/或方法可以被实施的示例环境的示图；

[0008] 图3是图2的一个或多个设备的示例部件的示图；

[0009] 图4是用于生成和提供用于使用第三方网站来验证公共密钥证书的代码的示例过程的流程图；

[0010] 图5A和5B是与图4示出的示例过程有关的示例实施方式的示图；

[0011] 图6是用于使用第三方网站来验证公共密钥证书的示例过程的流程图；

[0012] 图7是与图6中示出的示例过程有关的示例实施方式的示图；

[0013] 图8是用于使用附属域来验证公共密钥证书的示例过程的流程图；以及

[0014] 图9A-9D是与图8中示出的示例过程有关的示例实施方式的示图。

具体实施方式

[0015] 示例实施方式的以下详细描述参考了附图。在不同附图中的相同标号可以标识相同或相似元素。

[0016] 当客户端设备正建立与主机设备的安全通信会话(例如，安全套接层(SSL)会话)时，诸如当客户端设备的用户导航到由主机设备托管的安全网站时，主机设备通常向客户端设备发送公共密钥证书，以验证主机设备的身份。该证书可以标识针对该会话的初始加密密钥。如果客户端设备将该证书识别为有效(例如，如果运行在客户端设备上的浏览器能够验证该证书是由受信任的证书机构签名)，那么客户端设备可以允许用户访问该安全网站。如果客户端设备没有将该证书识别为有效，则客户端设备可能不允许用户访问该安全网站。

[0017] 在一些情况下，客户端设备可以将该证书标识为无效，但是用户可以提供指示以接受无效证书。因为一些用户可以接受无效证书，攻击者(例如黑客)可能能够通过向客户端设备发送无效证书来拦截客户端设备与主机设备之间的消息。当用户接受攻击者的无效证书时，由客户端设备发送的加密消息可以被攻击者的设备拦截和解密。攻击者可能还建立与主机设备的安全会话(例如，通过接受主机设备的有效证书)。攻击者然后可以通过拦截、告警、移除和/或插入客户端设备与主机设备之间的消息，来扮演中间人。

[0018] 这样的中间人攻击可能难以检测，因为主机设备可能仅看到来自攻击者设备的流量(例如，经由使用有效证书而被建立的连接)，并且可能未看到客户端设备与攻击者设备之间的流量(例如，经由使用无效证书而被建立的连接)。本文中描述的实施方式允许主机设备检测用户、诸如网站访问者何时已经接受针对由主机设备提供的网站的无效证书。

[0019] 图1A和1B是本文中所描述的示例实施方式100的概览的示图。如图1A所示，用户可以使用客户端设备来请求访问被示出为www.securesite.com的网站，该网站需要安全连接

被建立。客户端设备可以传输该请求，该请求目的在于与该网站相关联的主机设备，并且攻击者可以使用攻击者设备来拦截该请求。例如，该请求可以通过不完全网络(例如，不安全的WiFi网络)被传输，并且可以由攻击者设备经由不安全网络拦截。攻击者设备可以建立与主机设备的会话(例如，通过从主机设备接收有效证书)，并且可以向客户端设备发送无效证书(被示出为“攻击者的证书”)。

[0020] 在接收到无效证书时，客户端设备可以通知用户(例如，经由浏览器)该证书处于无效，并且可以提示用户指示是否接受该无效证书。如果用户提供指示以接受无效证书，加密会话可以在客户端设备与攻击者设备之间被建立。因为攻击者已经建立与客户端设备和主机设备两者的认证会话，攻击者可以通过拦截、告警、移除和/或插入在客户端设备与主机设备之间被通信的消息，来扮演中间人。通过该方式，攻击者可以获得对与用户相关联的机密信息的访问，该机密信息诸如信用卡号、银行账户号、密码等。

[0021] 如图1B所示，本文中描述的实施方式可以通过将证书验证代码插入到针对该网站的代码中，来检测和防止这样的中间人攻击。验证代码可以从除了www.securesite.com之外的域请求资源，诸如图像或脚本。例如，验证代码可以从被示出为www.verifiersite.com的网站请求资源。

[0022] 如进一步示出的，攻击者设备可以拦截针对来自其他域的资源的请求，并且可以发送攻击者的证书以尝试扮演客户端设备与其他域之间的中间人。然而，因为这个验证代码允许在背景中并且尝试嵌入主机网站(例如www.securesite.com)中的资源，该用户将不被提示接受攻击者的证书，并且攻击者的证书将被拒绝为无效。因此，主机网站将不能够获得该资源。如所示出的，浏览器可以检测该资源不被接收，并且可以做出适当的动作来阻挡中间人攻击，诸如通过终止会话、通知用户该攻击等。通过该方式，主机网站可以能够检测和防止中间人攻击，并且向网站访问者提供提升的安全性。

[0023] 图2是在其中本文中所描述的系统和/或方法可以被实施的示例环境200的示图。如图2中所示出的，环境200可以包括客户端设备210、主机设备220、一个或多个验证设备230、攻击者设备240以及网络250。环境200的设备可以经由有线连接、无线连接、或者有线和无线连接的组合来互连。

[0024] 客户端设备210可以包括一个或多个如下的设备，这些设备能够经由加密连接(例如，SSL连接、TLS连接等)接收和/或提供信息，和/或能够生成、存储和/或处理经由加密连接所接收和/或所提供的信息。例如，客户端设备210可以包括计算设备，诸如笔记本电脑、平板电脑、手提电脑、台式计算机、移动电话(例如智能电话、无线电话等)、个人数字助理、或者类似的设备。客户端设备210可以向主机设备220和/或验证设备230提供请求和/或从主机设备220和/或验证设备230接收响应(例如，经由网络250)。在一些实施方式中，请求和/或响应可能被攻击者设备240经由中间人攻击而拦截。客户端设备210可以经由加密连接而接收和/或提供信息，该加密连接诸如基于公共密钥证书而被建立的连接。

[0025] 主机设备220可以包括一个或多个如下的设备，这些设备能够经由加密连接而接收和/或提供信息，和/或能够生成、存储和/或处理经由加密连接所接收和/或所提供的信息。例如，主机设备220可以包括计算设备，诸如服务器(例如，应用服务器、内容服务器、主机服务器、web服务器等)、台式计算机、膝上型计算机、或者类似的设备。主机设备220可以从客户端设备210接收信息和/或向客户端设备210提供信息(例如，经由网络250)。在一些

实施方式中，该信息可能被攻击者设备240经由中间人攻击而拦截。主机设备220可以经由加密连接而接收和/或提供信息。主机设备220可以向客户端设备210和/或攻击者设备240提供公共密钥证书，以建立加密连接。在一些实施方式中，主机设备220可以向客户端设备210提供代码，该代码被用于验证正由客户端设备210用于访问与主机设备220相关联的网站的公共密钥证书。

[0026] (多个)验证设备230可以包括一个或多个如下的设备，这些设备能够经由加密连接而接收和/或提供信息，和/或能够生成、存储和/或处理经由加密连接所接收和/或所提供的信息。例如，验证设备230可以包括计算设备，诸如服务器(例如，应用服务器、内容服务器、主机服务器、web服务器等)、台式计算机、膝上型计算机、或者类似的设备。验证设备230可以从客户端设备210接收信息和/或向客户端设备210提供信息(例如，经由网络250)。在一些实施方式中，该信息可以被攻击者设备240经由中间人攻击而拦截。在一些实施方式中，经由客户端设备210的浏览器提供的网站可以从一个或多个验证设备230请求一个或多个资源，并且(多个)验证设备230可以响应该(多个)请求。

[0027] 攻击者设备240可以包括一个或多个如下的设备，这些设备能够经由网络(例如，网络250)与其他设备通信，和/或能够接收由另一个设备提供的信息。例如，攻击者设备240可以包括计算设备，诸如膝上型计算机、平板电脑、手提电脑、台式计算机、移动电话(例如智能手机、无线电话等)、个人数字助理、或类似的设备。在一些实施方式中，攻击者设备220可以使用无效(例如，未被认证和/或未受信任)证书来建立与客户端设备210的第一加密会话，并且可以使用有效证书来建立与主机设备220和/或验证设备230的第二加密会话。攻击者设备240可以拦截来自客户端设备210和/或主机设备220的流量，并且可以通过告警、移除或插入在客户端设备210与主机设备220之间被传送的流量，来扮演中间人。

[0028] 网络250可以包括一个或多个有线和/或无线网络。例如，网路250可以包括无线局域网(WLAN)、局域网(LAN)、宽域网(WAN)、城域网(MAN)、电话网络(例如，公共交换电话网(PSTN))、蜂窝网络、公用陆地移动通信网(PLMN)、自组织网络、内联网、互联网、基于光纤的网络、或者这些或其他类型的网络的组合。在一些实施方式中，网络250可以包括客户端设备210和攻击者设备240均连接到的不安全网络(例如，Wi-Fi网络、WiMAX网络、蓝牙网络等)。

[0029] 图2中示出的设备和网络的数量被提供为一个示例。在实践中，可以有另外的设备和/或网络、更少的设备和/或网络、不同的设备和/或网络，或者与图2中示出的那些相比被不同地布置的设备和/或网络。此外，图2中示出的一个或多个设备可以被实施在单个设备内，或者图2中示出的单个设备可以被实施为多个、分布式的设备。另外，环境200的设备中的一个或多个设备可以执行被描述为由环境200的另外的一个或多个设备所执行的一个或多个功能。

[0030] 图3是设备300的示例部件的示图，该设备300可以对应于客户端设备210、主机设备220、验证设备230和/或攻击者设备240。在一些实施方式中，客户端设备210、主机设备220、验证设备230和/或攻击者设备240可以包括一个或多个设备300和/或设备300的一个或多个部件。如图3中所示出的，设备300可以包括总线310、处理器320、存储器330、输入部件340、输出部件350和通信接口360。

[0031] 总线310可以包括允许设备300的部件之间的通信的部件。处理器320可以包括拦

截和/或执行指令的处理器(例如,中央处理单元、图像处理单元、经加速的处理单元)、微处理器、和/或处理部件(例如,现场可编程门阵列(FPGA)、专用集成电路(ASIC)等)。存储器330可以包括随机访问存储器(RAM)、只读存储器(ROM)、和/或另一个类型的动态或静态存储设备(例如,闪存、磁性或光学存储器),其存储用于由处理器320使用的信息和/或指令。

[0032] 输入部件340可以包括允许用户向设备300输入信息的部件(例如,触摸屏显示器、键盘、小型键盘(keypad)、鼠标、按钮、开关等)。输出部件350可以包括从设备300输出信息的部件(例如,显示器、扬声器、一个或多个发光二极管(LED)等)。

[0033] 通信接口360可以包括类收发器的部件,诸如收发器和/或分离的接收器和发射器,该类收发器的部件使得设备300能够诸如经由有线连接、无线连接或有线和无线连接的组合而与其他设备通信。例如,通信接口360可以包括以太网接口、光学接口、同轴电缆接口、红外接口、射频(RF)接口、通用串行总线(USB)接口、Wi-Fi接口等。

[0034] 设备300可以执行本文中描述的一个或多个过程。设备300可以响应于处理器320执行被包括在计算机可读介质、诸如存储器300中的软件指令而执行这些过程。计算机可读介质可以被定义为非瞬态存储设备。存储设备可以包括在单个物理存储设备内的存储空间或括多个物理存储设备伸展的存储空间。

[0035] 软件指令可以经由通信接口360、从另一个计算机可读介质或从另一个设备被读取到存储器330。当被执行时,被存储在存储器330中的软件指令可以使得处理器320执行本文中所描述的一个或多个过程。另外地或备选地,取代软件指令、或者与软件指令结合,硬线电路可以被用于执行本文中所描述的一个或多个过程。因此,本文中所描述的实施方式不局限于硬件电路和软件的任何具体组合。

[0036] 图3中示出的部件的数量被提供为一个示例。在实践中,设备300可以包括另外的部件、更少的部件、不同的部件、或者与图3中示出的那些相比不同地被布置的部件。

[0037] 图4是用于生成和提供用于使用第三方网站来验证公共密钥证书的代码的示例过程400的流程图。在一些实施方式中,图4的一个或多个过程框可以由主机设备220执行。在一些实施方式中,图4的一个或多个过程框可以由另一个设备或者独立于主机设备220或者包括主机设备220的一组设备来执行,该组设备诸如客户端设备210、验证设备230、和/或攻击者设备240。

[0038] 如图4中所示出的,过程400可以包括确定要被用于验证公共密钥证书的一个或多个验证域(框410)。例如,主机设备220可以确定要被用于验证公共密钥证书的一个或多个验证域。在一些实施方式中,主机设备220可以接收验证该一个或多个验证域的用户输入。验证域可以包括与网站和/或托管该网站的验证设备230相关联的域名和/或web地址。验证域可以包括顶级域和一个或多个次级域。例如,验证域可以包括字符串,该字符串标识验证域、网站、资源位置等。公共密钥证书(在本文中有时被称为证书)可以包括电子文档,该电子文档使用数字签名来用标识(例如,与域相关联的标识)掩蔽公共密钥。该证书可以被用于验证该公共密钥属于该域。

[0039] 在一些实施方式中,主机设备220可以确定(例如,基于用户输入)多个验证域,从该多个验证域中选择要被用于验证该公共密钥证书的一个或多个验证域。例如,主机设备220可以标识验证域的列表,并且可以从该列表中选择一个或多个验证域。在一些实施方式中,主机设备220可以从该列表中随机地选择一个或多个验证域。主机设备220可以生成如

下的代码，该代码标识该一个或多个验证域要被用于验证该公共密钥证书。

[0040] 在一些实施方式中，该一个或多个验证域可以不同于主机域。通过该方式，当主机设备220(例如，主机域)由于在中间人攻击期间无效证书已经被客户端设备210接受而已经被危及时，主机设备220可以通过检验(例如，与(多个)验证设备230相关联的)验证域来确定无效证书已经被接收，如本文中其他地方所描述的。

[0041] 如图4中进一步示出的，过程400可以包括确定一个或多个资源要被请求以用于验证公共密钥证书(框420)。例如，主机设备220可以确定要被从(多个)验证域请求并且要被用于验证该证书的一个或多个资源。在一些实施方式中，主机设备220可以接收标识该一个或多个资源的用户输入。资源可以包括例如从验证域可访问的对象，诸如图像、脚本、动画、音频、视频等。例如，该资源可以是使用包括验证域(例如，www.verifiersite.com/image.jpg)的指示符(例如，统一资源定位符)可访问的图像。作为另一个示例，该资源可以是使用包括验证域(例如，www.example.com/script.js)的指示符可访问的脚本。

[0042] 如本文中其他地方所描述的，当在与主机设备220相关联的网站上执行代码时，客户端设备210可以从(多个)验证域请求一个或多个资源，并且可以确定该一个或多个资源是否被适当地接收。如果该一个或多个资源由客户端设备210接收，那么客户端设备210可以确定由客户端设备210接收的针对该主机域的证书是有效的。如果该一个或多个资源未被客户端设备210接收，那么客户端设备210可以确定无效证书已经被接收，并且该连接已经受到中间人攻击危及。

[0043] 如图4中进一步示出的，过程400可以包括确定在公共密钥证书未被验证时要执行的一个或多个动作(框430)。例如，主机设备220可以确定在由攻击者设备240发送的无效公共密钥证书被客户端设备210接受时要执行的一个或多个动作。在一些实施方式中，主机设备220可以接收标识一个或多个动作的用户输入。动作可以包括例如经由客户端设备210(例如，经由浏览器)提供通知以向用户告警受危及的连接、终止该会话、要求用户从不同的网络地址(例如，经由不同的局域网)登陆、要求用户重设密码等。

[0044] 如图4进一步示出的，过程400可以包括基于(多个)验证域、(多个)资源和/或(多个)动作来生成和/或提供用于验证公共密钥证书的代码(框440)。例如，主机设备220可以生成如下的代码：标识(多个)验证域、标识要从(多个)验证域被请求以确定客户端设备210是否已经接受无效证书的(多个)资源、以及标识在代码执行确定客户端设备210已经接受无效证书时要被执行的(多个)动作。该代码可以包括例如超文本标记语言(HTML)代码、可扩展标记语言代码(XML)代码、层叠样式表(CSS)代码、JavaScript代码等。

[0045] 在一些实施方式中，主机设备220可以将该代码提供给客户端设备210。例如，客户端设备210的用户可以使用浏览器导航到与主机设备210相关联的主机网站，并且主机设备220可以将该代码与提供该网站以用于在浏览器中显示的其他代码一起提供。换而言之，主机设备220可以将该代码嵌入在该网站的HTML代码中，并且可以将嵌入的代码和其余HTML代码提供给客户端设备210，以由浏览器执行。在一些实施方式中，主机设备220可以在对来自客户端设备210的一个或多个HTML请求的一个或多个HTML响应中将该代码提供给客户端设备210。通过该方式，主机设备220可以在客户端设备210的用户已经接受来自执行中间人攻击的攻击者的无效证书的时候，保护客户端设备210的用户不受中间人攻击。

[0046] 尽管图4示出了过程400的示例框，在一些实施方式中，过程400可以包括另外的

框、更少的框、不同的框、或者与图4中示出的那些相比不同地布置的框。附加地或者备选地，过程400的框中的两个或更多框可以并行执行。

[0047] 图5A和5B是与图4中示出的示例过程400有关的示例实施方式500的示图。图5A和5B示出了管理员向主机设备220提供输入以指令主机设备220生成和/或向客户端设备210提供代码以验证公共密钥证书的示例。

[0048] 如图5A中所示出的，假设管理员与输入设备(例如，计算设备)交互以将设置信息提供给主机设备220，该设置信息与被示出为www.hostsite.com的域相关联。如由标号510示出的，假设管理员输入如下的信息，该信息标识要被用于验证访问www.hostsite.com的用户的证书的三个验证域，被示出为https://www.verifiersite.com、https://www.socialmediasite.com和https://www.popularsite.com。这些验证域被示出为示例，并且管理员可以输入另外的验证域、更少的验证域、或者不同的验证域。在一些实施方式中，管理员可以被提供有如下的选项：从所提供的验证域的列表中随机选择验证域，和/或可以被提供有如下的选项：设置要被用于验证证书的验证域的数量。

[0049] 如标号520所示出的，假设管理员输入三个资源，每个资源对应于这些域中的一个域。如所示出的，假设管理员输入如下的信息，该信息标识针对verifiersite域的image.gif的图像资源、针对socialmediasite域的logo.jpg的图像资源、以及针对popularsite域的banner.png的图像资源。如标号530所示出的，假设管理员输入在证书被确定为无效的时候要被执行的两个动作。第一动作将使得与无效证书相关联的会话被终止，并且第二动作将使得告警消息被提供到客户端设备210以供显示。

[0050] 如标号540所示出的，输入设备可以将设置信息和/或基于设置信息而生成的代码提供给主机设备220。在一些实施方式中，输入设备可以向主机设备220提供设置信息，诸如标识验证域、资源和动作的信息，并且主机设备220可以基于设置信息来生成代码。另外地或备选地，输入设备可以基于设置信息来生成代码并且将所生成的代码提供给主机设备220。另外地或备选地，管理员可以将代码输入给输入设备，并且输入设备可以将该代码提供给主机设备220。

[0051] 如图5B并且由标号550所示出的，主机设备220可以将验证代码提供给客户端设备210。例如，假设客户端设备210的用户与浏览器交互以导航到网站www.hostsite.com，使得客户端设备210从主机设备220请求该网站。假设主机设备220将该网站、包括该验证代码提供给客户端设备210。示例验证代码在图5B中被示出。

[0052] 如由标号560所示出的，验证代码可以标识如下的验证域和资源，该验证域和资源要被用于验证客户端设备210上被用于访问网站的证书。如标号570所示出的，验证代码可以包括用于访问该资源的代码，诸如通过基于被标识在验证代码中的图像资源而生成图像(或者在该资源是脚本的情况中通过执行脚本)。如标号580所示出的，验证代码可以包括如下的代码，该代码用于核查图像的尺寸和/或大小(或者核查脚本是否被执行)以确定图像资源(或者脚本资源)是否可由客户端设备210访问。如果该图像未被生成，这是客户端设备210具有主机域的无效证书的指示，因为客户端设备210的浏览器会自动地拒绝针对验证代码的无效证书而不提示用户接受或拒绝无效证书。通过该方式，主机域的管理员可以通过防止使用无效证书的中间人攻击，增加主机域网站的安全性。

[0053] 如以上所描述的，图5A和5B仅被提供作为示例。其他示例是可能的并且可以不同

于关于图5A和5B所描述的。

[0054] 图6是用于使用第三方网站来验证公共密钥证书的示例过程600的流程图。在一些实施方式中，图6的一个或多个过程框可以由客户端设备210执行。在一些实施方式中，图6的一个或多个过程框可以另一个设备或者独立于或包括客户端设备210的设备的群组来执行，诸如主机设备220、验证设备230和/或攻击者设备240。

[0055] 如图6所示，过程600可以包括执行代码，该代码标识用于验证公共密钥证书的一个或多个验证域以及一个或多个资源(框610)。例如，客户端设备210的用户可以请求访问与主机域相关联的网站，并且该请求可以经由来自攻击者设备240的中间人攻击而被拦截。攻击者设备240可以向客户端设备210发送无效证书，并且客户端设备210的用户可能接受该无效证书。攻击者设备240然后可以扮演客户端设备210与主机设备220之间的中间人，具有拦截、告警、删除和插入客户端设备210域主机设备220之间的消息的能力。为了删除这样的中间人攻击，当客户端设备210的用户使用浏览器来导航到与主机域相关联的网站时，与主机域相关联的主机设备220可以向客户端设备210提供验证代码(例如，连同用于显示浏览器中的网站的代码一起)。该验证代码可以标识被请求以用于验证由客户端设备210用于访问该网站的公共密钥证书的一个或多个验证域和/或一个或多个资源。

[0056] 如图6中进一步示出的，过程600可以包括从验证域请求资源(框620)。例如，客户端设备210可以从被标识在验证代码中的验证域请求(例如使用浏览器)被标识在验证代码中的资源。该资源可以包括例如可从验证域访问的对象，诸如图像、脚本、动画、音频、视频等。

[0057] 如图6中进一步示出的，过程600可以包括确定该资源是否被接收(框630)。例如，客户端设备210可以请求该资源并且可以确定所请求的资源是否被接收。例如，客户端设备210可以通过将与所请求的图像并且经由浏览器渲染的图像的尺寸和/或大小(例如，文件大小)与阈值(例如，所请求的图像的所期望的尺寸和/或所期望的大小)进行比较，来确定所请求的图像是否被接收。如果该图像的尺寸和/或大小满足该阈值(例如，小于该阈值)，这可以指示该图像未被接收、并且破损的图像图标被浏览器渲染。

[0058] 在一些实施方式中，客户端设备210可以确定从验证域所请求的脚本是否已经在客户端设备210上(例如，在浏览器中)被执行。例如，客户端设备210可以接收脚本执行失败的消息，指示客户端设备210的用户可能已经接受针对主机域的无效证书。作为另一个示例，客户端设备210可以确定所请求的动画、音频文件或者视频文件是否已经经由浏览器播放或者正在经由浏览器播放。例如，客户端设备210可以确定动画、音频文件或视频文件的长度。如果该长度等于零，这可能是所请求的资源未被接收、并且该用户已经接受针对主机域的无效证书的指示。

[0059] 如图6中进一步示出的，如果所请求的资源未被接收(框630-否)，那么过程600可以包括执行被标识在代码中的动作(框640)。例如，当客户端设备210确定所请求的资源未被接收时，客户端设备210可以执行被标识在验证代码中的一个或多个动作。在该资源未经由客户端设备210(例如，经由浏览器)接收和/或加载时，这可以是针对该验证域的证书是无效的指示。在一些实施方式中，客户端设备210可以接收该资源与具有无效证书的域相关联的指示。由于浏览器可能拒绝具有无效证书的嵌入资源而不提示用户接受或拒绝无效证书，这个技术可以被用于确定用户是否已经接受针对验证域的无效证书，因为攻击者可能

重新写入针对客户端设备210的、用户请求的每个域的证书。

[0060] 这些动作可以包括例如提供公共密钥证书无效的指示。该指示可以经由客户端设备210(例如,经由浏览器)而被提供和/或可以被提供到主机设备220。该动作可以包括例如终止连接,该连接诸如客户端设备210与攻击者设备240之间的、客户端设备210与主机设备220之间的和/或主机设备220与攻击者设备240之间的连接。在一些实施方式中,该动作可以包括关闭浏览器、退出网站、锁定用户的账户、改变用户的密码、终止活跃的会话等。

[0061] 在一些实施方式中,动作可以由客户端设备210执行(例如,经由浏览器提供指示、关闭浏览器等)。另外地或附加地,动作可以由主机设备220执行。例如,客户端设备210在确定连接被危及时可以向主机设备220提供危及的指示,并且主机设备220可以基于接收该指示而执行动作。在一些实施方式中,客户端设备210可以通过在请求(例如HTML请求)中包括标签、诸如URL串中的唯一标签,以及将具有该标签的请求发送给主机设备220,来向主机设备220提供指示。

[0062] 如图6中进一步示出的,如果所请求的资源被接收(框630-是),那么过程600可以包括确定是否存在更多验证域或资源用于验证公共密钥证书(框650)。例如,如果客户端设备210确定与第一域相关联的第一资源被接收,那么客户端设备210可以确定验证代码是否标识与第二域相关联的第二资源。

[0063] 如图6中进一步示出的,如果存在被标识在代码中的更多验证域或资源(框650-是),那么过程600可以包括从验证域请求资源(框620)、确定该资源是否被接收(框630)等等。如果不存在被标识在代码中的更多的验证域或资源(框650-否),那么公共密钥证书可以被验证(框660)。例如,客户端设备210可以确定不存在被标识在代码中的更多验证代码或资源(例如,所有被标识的资源已经被接收),并且可以确定公共密钥证书有效。在一些实施方式中,当公共密钥证书是有效时,客户端设备210和/或主机设备220可以继续正常地操作(例如,客户端设备210可以被授权访问该网站,可以向主机设备220传输请求,可以从主机设备220接收响应等)。另外地或附加地,客户端设备210可以经由浏览器提供指示和/或向主机设备220提供公共密钥证书已经被验证的指示。

[0064] 尽管图6示出了过程600的示例框,在一些实施方式中,过程600可以包括另外的框、更少的框、不同的框、或者与图6中示出的那些相比不同地布置的框。附加地或者备选地,过程600的框中的两个或更多框可以并行执行。

[0065] 图7是与图6中示出的示例过程600有关的示例实施方式700的示图。图7使出了其中客户端设备210从验证域请求图像资源、确定该图像资源未被接收并且采取动作保证与主机域的连接是安全的示例。

[0066] 出于图7的目的,假设客户端设备210已经请求访问网站www.hostsite.com、并且该请求经由来自攻击者设备240的中间人攻击而被拦截。假设攻击者设备240向客户端设备210发送无效证书、并且客户端设备210的用户接受该无效证书。假设攻击者设备240现在扮演客户端设备210和与www.hostsite.com相关联的主机设备220之间的中间人,具有拦截、告警、删除和插入客户端设备210与主机设备220之间的消息的能力。

[0067] 如图7中并且由标号710所示出的,假设客户端设备210(已经随着用于提供主机网站www.hostsite.com的代码一起接收验证代码)执行验证代码以从被示出为www.verifiersite.com的验证域请求图像资源。如由标号720所示出的,假设攻击者设备

240从客户端设备210拦截针对该图像资源的请求。如由标号730所示出的，假设攻击者设备240发送攻击者的证书（例如，无效证书）以在客户端设备210和验证域www.verifiersite.com之间建立中间人连接。

[0068] 如由标号740所示出的，假设浏览器拒绝攻击者的证书，因为该证书是无效的(例如，为被受信任的机构所识别)。进一步假设浏览器不提示用户接受攻击者的证书，因为浏览器默默地拒绝了针对具有无效证书的(例如，经由验证代码所请求的)嵌入资源的请求。如由标号750所示出的，假设因为浏览器拒绝该无效证书，所请求的图像未被接收。因为所请求的图像未被接收，客户端设备210确定针对www.hostsite.com的证书是无效的。如标号760所示出的，客户端设备210提供告警消息，该告警消息指示该证书是无效的并且该连接已经被危及。此外，客户端设备210可以做出另外的动作，诸如终止该连接、向主机设备220发送通知等。

[0069] 如以上所指示的，图7仅被提供为示例。其他示例是可能的并且可以不同于关于图7所描述的。

[0070] 图8是用于使用附属域来验证公共密钥证书的示例过程800的流程图。在一些实施方式中，图8的一个或多个过程框可以由客户端设备210执行。在一些实施方式中，图8的一个或多个过程框可以另一个设备或者独立于或包括客户端设备210的设备的群组来执行，该设备的群组诸如主机设备220、验证设备230和/或攻击者设备240。

[0071] 如图8中所示出的，过程800可以包括执行由主机设备提供的第一代码，该第一代码标识由附属域提供的第二代码(框810)。例如，客户端设备210的用户可以使用浏览器导航到主机域的网站，并且与主机域相关联的主机设备220可以向客户端设备210提供第一代码(例如，与用于在浏览器中显示网站的代码一起)。第一代码可以标识附属域并且可以标识经由附属域被访问的第二代码。附属域(例如，www.affiliatedomain.com)可以不同于主机域(例如，www.hostsite.com)，但是可以以某种方式与主机域相关联。例如，附属域可以被同一公司拥有作为主机域、可以由附属公司拥有(例如，母公司、子公司、附属公司等)、可以取代拥有主机域的公司而由具有协议的公司拥有、可以与相同的服务提供商或附属服务提供商相关联等。在一些实施方式中，在其中第一代码被包括在针对该网站的方式可以是随机化的。例如，主机设备220可以随机化网站代码内的第一代码的位置。

[0072] 第一代码(例如，src＝"https://www.affiliatedomain.com/script.js")，当被执行时，可以将浏览器指引向附属域(例如，https://www.affiliatedomain.com)并且可以标识在附属域上要由浏览器执行的代码。客户端设备210(例如，浏览器)可以使用加密连接(例如，SSL连接、TLS连接等)以访问附属域。在(例如，在附属服务器设备上被托管的)附属域上的代码可以包括例如脚本。

[0073] 如图8中进一步示出的，过程800可以包括执行第二代码以从一个或多个验证域请求一个或多个资源(框820)。例如，客户端设备210可以执行第一代码，其可以使得客户端设备210从附属域获得第二代码并且执行第二代码。第二代码在由客户端设备210执行时可以使得客户端设备210从一个或多个验证域请求一个或多个资源(例如，类似于本文中结合图6所讨论的验证代码)。

[0074] 如图8中进一步示出的，过程800可以包括确定一个或多个资源是否被接收(框830)。例如，客户端设备210可以从(例如，被标识在第二代码中的)一个或多个验证域请求

一个或多个资源，并且可以确定一个或多个所请求的资源是否被接收，如本文中结合图6所讨论的)。

[0075] 如在图8中所示出的，如果一个或多个资源未被接收(框830-否)，那么过程800可以包括执行被标识在第二代码中的动作(框840)。例如，当客户端设备210确定一个或多个所请求的资源未被接收时，客户端设备210可以执行被标识在第二代码中的一个或多个动作。当该接收未经由客户端设备210(例如，经由浏览器)接收和/或加载时，这可以是针对验证域和/或主机域的证书无效的指示。基于该确定，客户端设备210可以执行一个或多个动作(例如，被标识在第二代码中的)，如本文中结合图6所讨论的。另外地或备选地，主机设备220可以执行一个或多个动作，如本文中结合图6所讨论的。

[0076] 在一些实施方式中，动作可以包括向主机设备220发送指示，该指示是针对主机域的证书是无效的。在一些实施方式中，客户端设备210可以经由cookie(例如，无效证书cookie)发送该指示。在一些实施方式中，基于确定一个或多个资源未被接收，客户端设备210可以不向主机设备220发送指示和/或cookie。主机设备220可以从客户端设备210接收不包括该cookie的请求(例如，HTTP请求)，并且主机设备220可以将cookie的缺失看作是主机域具有无效证书的指示。

[0077] 如图8中所示出的，如果一个或多个资源被接收(框830-是)，那么过程800可以包括确定与客户端设备和主机设备之间的会话相关联的会话cookie值(框850)。例如，客户端设备210可以确定与客户端设备和主机设备之间的通信会话(例如，加密通信会话)相关联的会话cookie值。在初始会话被建立在客户端设备210与主机设备220之间时，会话cookie值可以例如由主机设备210提供给客户端设备210。

[0078] 如图8中进一步示出的，过程800可以包括基于会话cookie值和一个或多个验证域来生成哈希值(框860)。例如，客户端设备210可以使用会话cookie值和/或一个或多个验证域串来生成的哈希值，该一个或多个验证域串标识一个或多个验证域和/或一个或多个资源。在一些实施方式中，该哈希值可以基于一个或多个验证域来生成，该一个或多个验证域被用于验证该证书和/或被用于标识该证书的一个或多个资源(例如，资源标志符)(例如，https://www.verifiersite.com/image.gif)。在一些实施方式中，客户端设备210可以基于多个验证域串来生成哈希值。

[0079] 在一些实施方式中，验证域串可以包括域标志符、资源标志符和/或随机值。例如，验证域串可以包括被附加到资源标识符的末端的随机值(例如，https://www.verifiersite.com/image.gif?ABCDE)。例如，随机长度)的随机值可以在向附属域服务器设备提供验证代码的时候由主机设备220插入。随机值可以被用于防止攻击者确定完全的验证域串。

[0080] 客户端设备210可以使用哈希算法将验证域串和会话cookie组合，来生成哈希值。例如，客户端设备210可以使用安全哈希算(SHA)(例如，SHA-0、SHA-1、SHA-2、SHA-3等)、高级加密标准(AES)、RSA算法、消息吸收(message-digest)算法(例如，MD4、MD5等)等，以生成哈希值。

[0081] 如图8中进一步示出的，过程800可以包括提供哈希值以验证该证书(框870)。例如，客户端设备210可以向主机设备220提供哈希值。主机设备220可以使用该哈希值来验证该证书。例如，主机设备220可以验证所接收的哈希值是否是正确的哈希值(例如，通过基于

(多个)验证域串和会话cookie来将所接收的哈希值与所计算的哈希值进行比较)。如果该哈希值是正确的,那么该证书可以被验证,并且主机设备220可以正常地与客户端设备210通信。如果该哈希值是不正确的,主机设备220可以基于无效证书来执行一个或多个动作,如本文其他地方所描述的。

[0082] 通过该方式,客户端设备210和/或主机设备220可以验证与客户端设备210和主机设备220之间的通信会话相关联的证书是否有效,并且可以检测证书何时已经(例如,通过攻击者利用中间人攻击)被重新写入。通过验证证书的有效性,与主机设备220相关联的网站可以被做得更安全。

[0083] 尽管图8示出了过程800的示例框,在一些实施方式中,在一些实施方式中,过程800可以包括另外的框、更少的框、不同的框、或者与图8中示出的那些相比不同地布置的框。附加地或者备选地,过程800的框中的两个或更多框可以并行执行。

[0084] 图9A-9D是与图8中示出的示例过程800有关的示例实施方式900的示图。图9A-9D示出使用附属域验证公共密钥证书的示例。

[0085] 如图9A所示出的,假设主机设备220生成和向客户端设备210提供第一代码。例如,假设客户端设备210的用户与浏览器交互以导航到网站www.hostdomain.com,使得客户端设备210从主机设备220请求该网站。假设主机设备220向客户端设备210提供该网站,包括第一代码。示例第一代码被示出在图9A中。例如,如由标号905所示出的,假设第一代码包括验证域串,该验证域串将验证域标识为https://affiliatedomain.com,并且标识被示出为script.js的要被请求的资源,。

[0086] 如图9B所示出的,假设客户端设备210执行第一代码,该第一代码使得客户端设备210从附属域affiliatedomain.com获得第二代码,诸如验证代码。示例验证代码由标号910示出并且包括示例代码动作915、920、925和930。代码部分915标识三个验证域(例如,https://www.verifiersite.com、https://www.socialmedisite.com和https://www.popularsite.com)以及三个相应的资源标志符,这些资源标志符标识由验证域托管的资源(例如,image.gif、logo.jpg和banner.png)。被包括在代码部分915中的验证域串还包括随机串(例如,rand=ABCDE、rand=TTAHfhaf和rand=Faerags)。

[0087] 代码部分920包括用于访问和/或获得资源的代码,诸如通过基于被标识在验证代码中的图像资源来生成图像(或者在该资源是脚本的情况中通过执行脚本)。代码部分925包括如下的代码,该代码用于核查图像的尺寸和/或大小(或者核查脚本是否被执行)以确定图像资源(或者脚本资源)是否可由客户端设备210访问。代码部分925还包括如下的代码,该代码用于在图像资源未被接收和/或生成的时候设置cookie以指示无效证书。代码部分930包括如下的代码,该代码用于当图像资源被接收和/或生成的时候基于验证域串和会话cookie来生成哈希值,并且将所生成的哈希值作为cookie提供给主机设备220。

[0088] 图9C描绘了在其中主机设备220确定证书无效的若干场景。如由标号935所示出的,假设主机设备220生成和向客户端设备210提供第一代码,并且第一代码指向经由附属域提供的第二代码。如由标号940所示出的,假设(使用攻击者设备240的)攻击者阻挡从被传输到客户端设备210的第一代码。作为结果,第一代码和第二代码未由客户端设备210执行,并且因此主机设备220未接收将已经经由第二代码的执行而被生成的cookie,如由标号945所示出的。因此,主机设备220确定该证书处于无效,并且执行适当的动作,如由标号950

所示出的。

[0089] 在另一个场景中，假设攻击者没有阻挡第一代码，并且客户端设备210接收第一代码。如由标号955所示出的，客户端设备210执行第一代码和第二代码。如由标号960所示出的，假设被标识在第二代码中的资源请求已经失败(例如，图像未被接收，脚本未被执行等)。基于确定资源请求已经失败，客户端设备210生成无效证书cookie。如由标号965所示出的，假设攻击者设备阻挡那个无效证书cookie。因此，主机设备220未接收无效证书cookie，如由标号970所示出的。基于在来自客户端设备210的随后请求中未接收到无效证书cookie，主机设备220确定证书处于无效，并且执行适当的动作，如由标号950所示出的。

[0090] 在又一个场景中，假设攻击者没有阻挡无效证书cookie，并且主机设备220接收该无效证书cookie，如由标号975所示出的。基于接收到无效证书cookie，主机设备220确定证书处于无效，并且执行适当的动作，如由标号950所示出的。

[0091] 图9D描绘了在其中客户端设备210生成哈希值并且向主机设备210提供哈希值的两个场景：一个场景是其中哈希值由主机设备220确定为不正确，并且一个场景是其中哈希值由主机设备220确定为正确。如图9D所示出的，假设客户端设备210基于被标识在第二代码中的验证域串来从验证域请求资源，并且确定这些资源已经被接收。如由标号980所示出的，假设客户端设备210确定针对客户端设备210与主机设备220之间的会话的会话cookie值。如由标号985所示出的，假设客户端设备210使用验证域串和会话cookie来生成哈希值，并且随后将该哈希值提供给主机设备220。

[0092] 如由标号990所示出的，假设主机设备220确定该哈希值是正确的。基于该确定，主机设备220可以确定公关密钥证书是有效的，并且可以行进以如正常那样与客户端设备210通信。如由标号995所示出的，假设主机设备220确定该哈希值是不正确的。基于该确定，主机设备220可以确定公关密钥证书是无效的，并且可以执行适当的动作，诸如终止该连接、将警告指示符提供给客户端设备210等。

[0093] 如以上所指示的，图9A-9D仅被提供为示例。其他示例是可能的并且可以不同于关于图9A-9D所描述的。

[0094] 前述公开内容提供说明和描述，但是不旨在排他性或者将实施方式限制到所公开的准确形式。在以上公开内容的基础上，修改和改变是可能的，或者依据实施方式的实践，修改和改变可能需要的。

[0095] 如本文中所使用的，术语部件旨在与被宽泛地认为硬件、固件、或者硬件和固件的组合。

[0096] 如本文中所描述的系统和/或方法在附图所图示的实施方式中可以以软件、固件和硬件的许多不同的形式而被实施，这将是明显的。被用于实施这些系统和/或方法的实际软件代码或者专用控制硬件不限于这些实施方式。因此，系统和/或方法的操作和行为在不参照具体软件代码的情况下被描述—理解的是，软件和硬件可以被设计以基于本文中的描述而实施这些系统和/或方法。

[0097] 一些实施方式在本文中被描述为从设备接收信息或者向设备提供信息。这些短语可以指的是直接从设备接收信息或者直接向设备提供信息，而不需要信息经由沿着设备之间的通信路径放置的中间设备传送。另外地或备选地，这些短语可以指的是经由一个或多个中间设备(例如，网络设备)接收由一个设备提供信息，或者经由一个或多个中间设备向

一个设备提供信息。

[0098] 一些实施方式在本文中结合阈值被描述。如本文中所使用的，满足阈值可以指的是一个值大于该阈值，比该阈值更大，高于该阈值、大于或等于该阈值，小于该阈值，比该阈值更小，低于该阈值，小于或等于该阈值，等于该阈值，等等。

[0099] 即使特征的特定组合被记载在权利要求书中和/或被公开在说明书中，这些组合不旨在限制可能的实施方式的公开内容。事实上，这些特征中的许多特征可以以不是权利要求书中所记载的或者在说明书中所公开的方式来组合。尽管在以下列出的每个从属可以直接从属于仅一个权利要求，但是可能的实施例的公开内容包括每个从属权利要求与权利要求书中的每个其他权利要求的组合。

[0100] 本文中所使用的元件、动作或指令不应当被认为是重要的或必要的，除非明确地如此描述。而且，如本文中所使用的，(“a”、“an”)物品旨在于包括一个或多个项目，并且可以与“一个或多个”交互地使用。此外，如本文中所使用的，术语“集合”旨在于包括一个或多个项目，并且可以与“一个或多个”交互地使用。当仅旨在于一个项目时，术语“一个”或者类似的语言被使用。此外，短语“基于”旨在于意思是“至少部分地基于”，除非明确地如此描述。

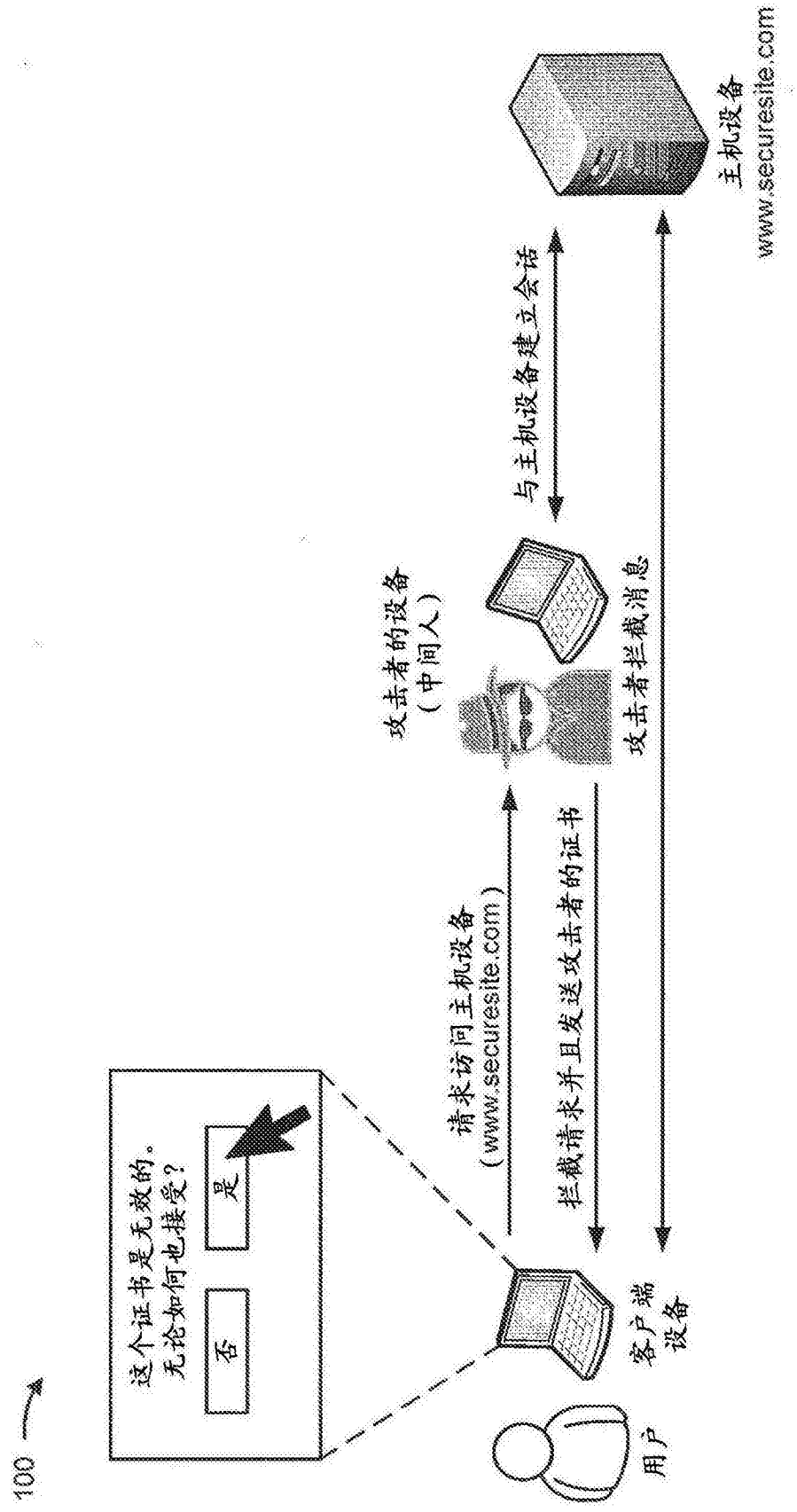

100
这个证书是无效的。
无论如何也接受？
否
是
用户
客户端
设备
请求访问主机设备
(www.securesite.com)
拦截请求并且发送攻击者的证书
攻击者的设备
(中间人)
攻击者拦截消息
与主机设备建立会话
主机设备
www.securesite.com

图1A

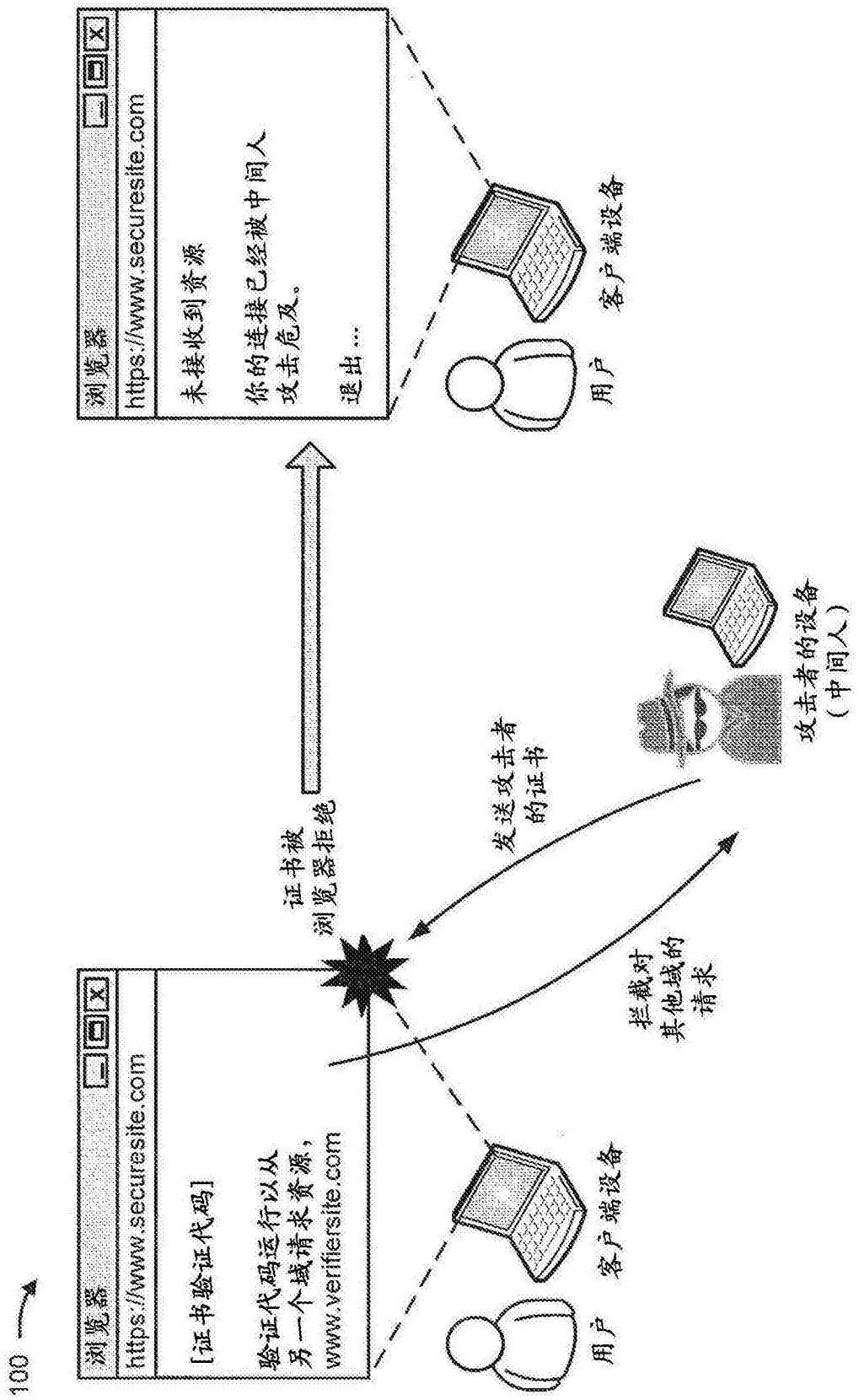

100
浏览器
https://www.securesite.com
[证书验证代码]
验证代码运行以从另一个域请求资源，www.verifiersite.com
用户
客户端设备
证书被浏览器拒绝
发送攻击者的证书
拦截对其他域的请求
攻击者的设备（中间人）
浏览器
https://www.securesite.com
未接收到资源
你的连接已经被中间人攻击危及。
退出 ...
用户
客户端设备

图1B

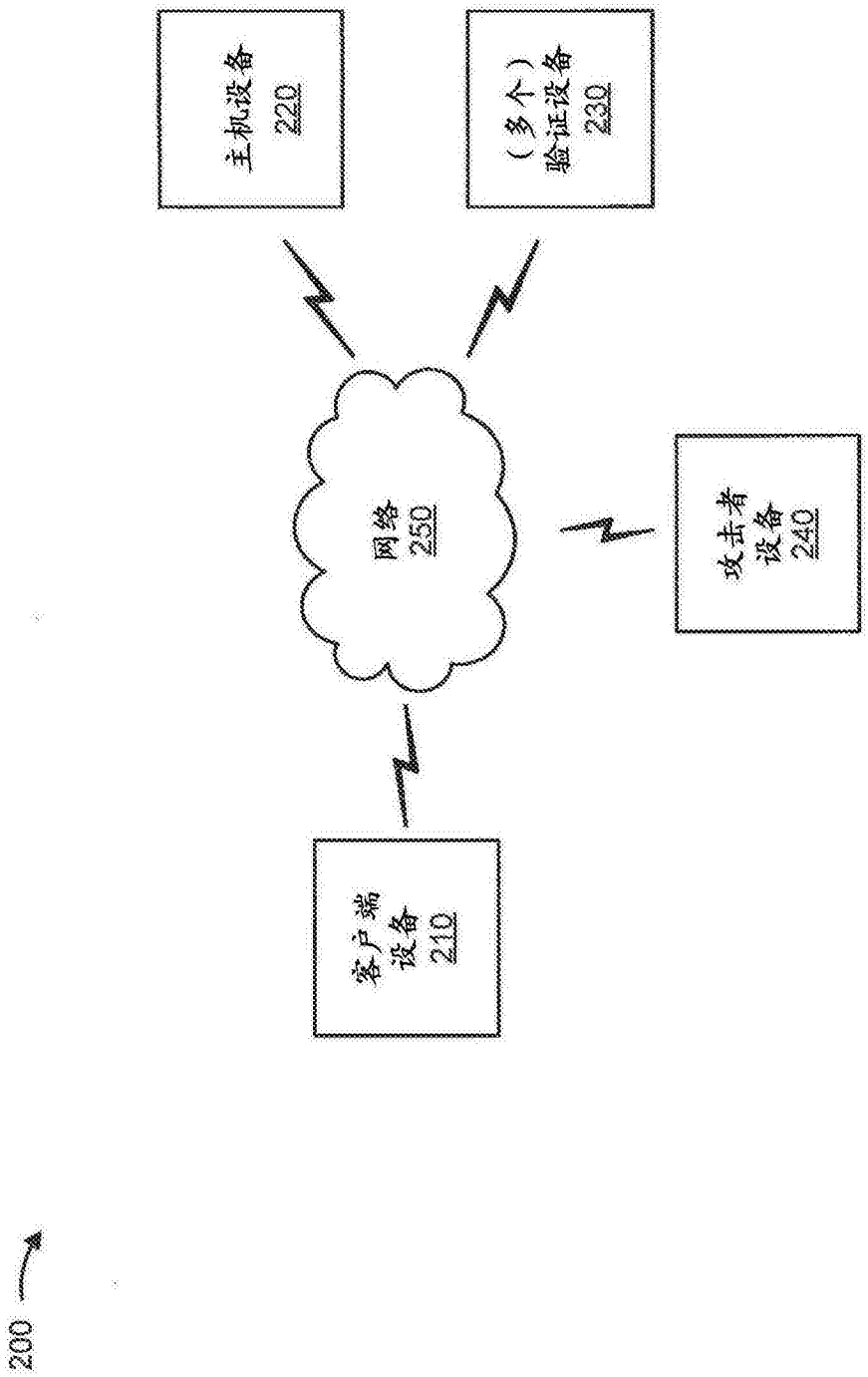


图2

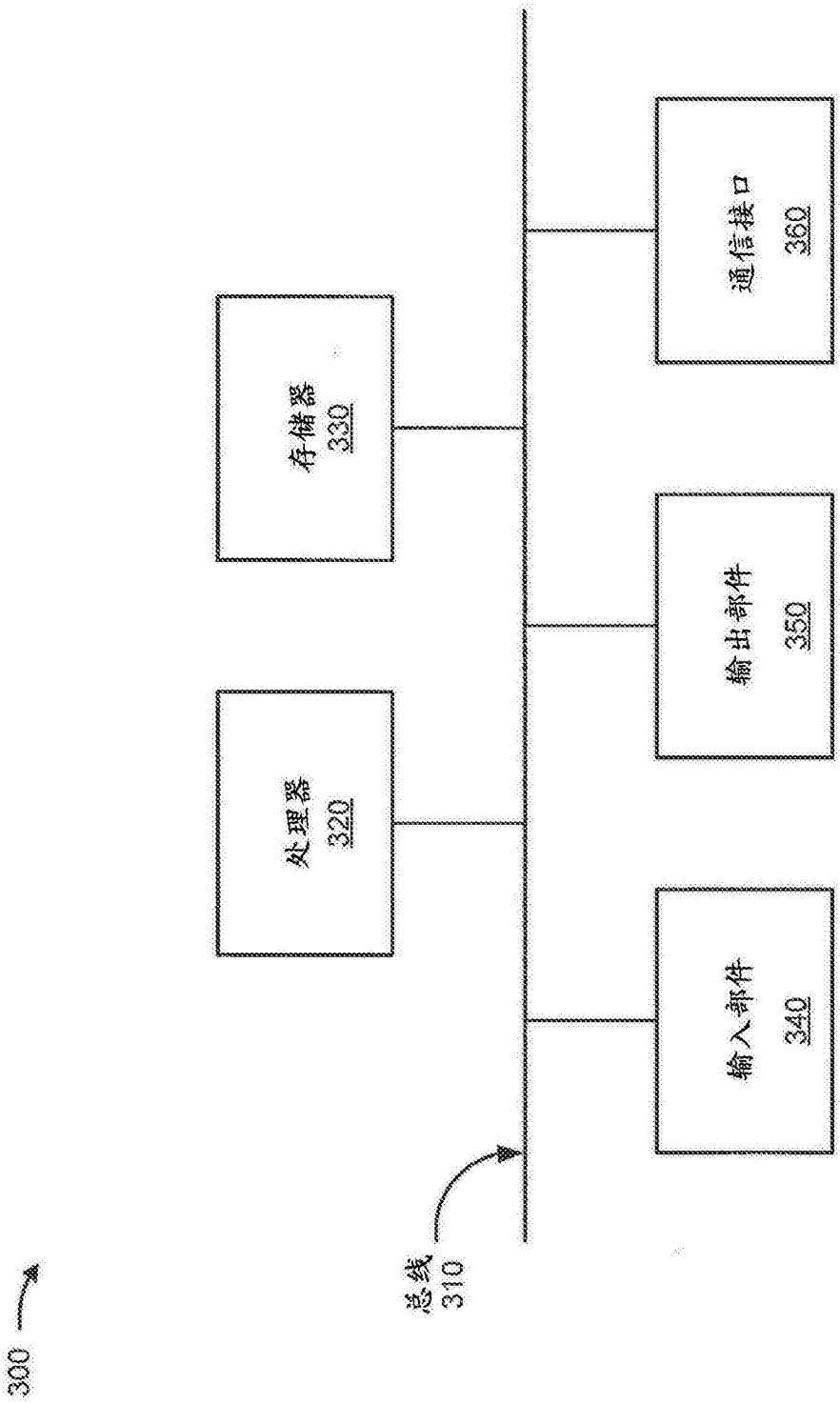


图3

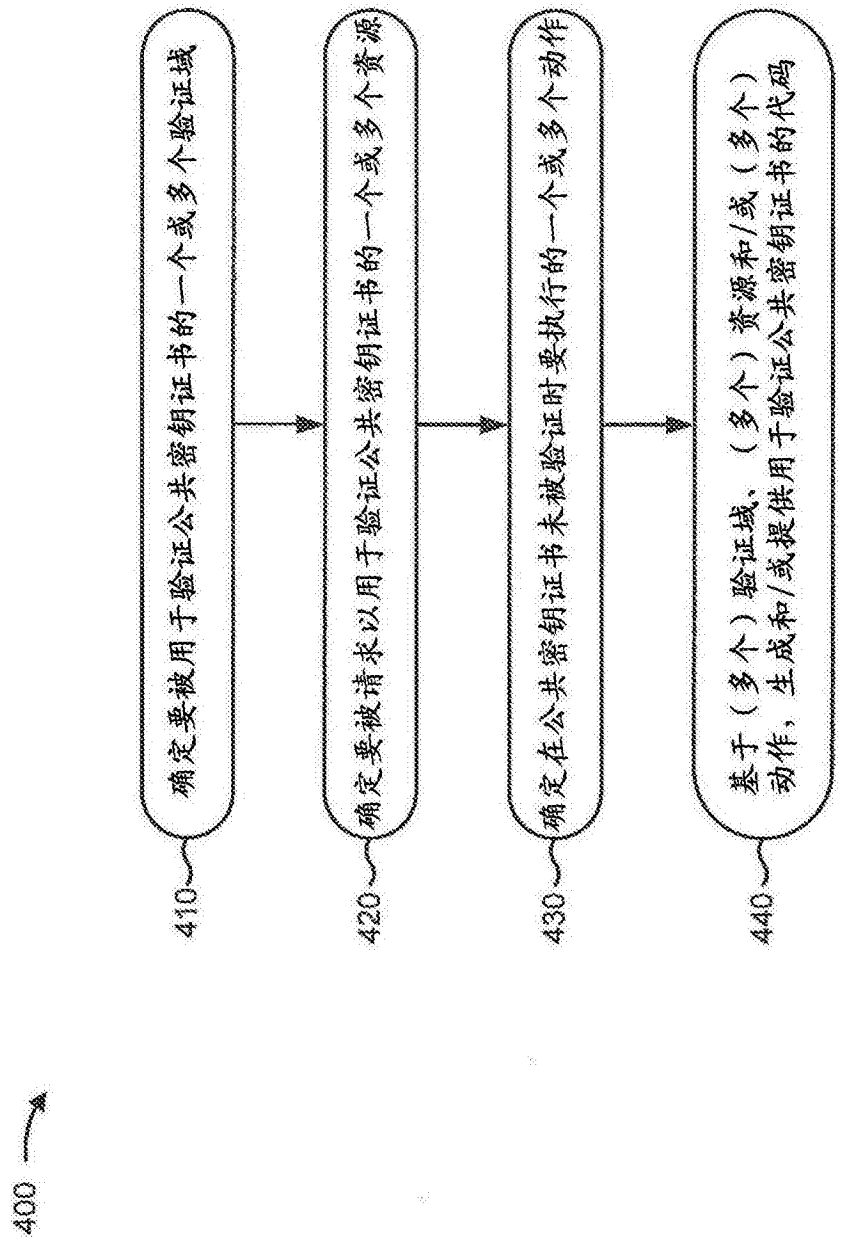

确定要被用于验证公共密钥证书的一个或多个验证域
410
确定要被请求以用于验证公共密钥证书的一个或多个资源
420
确定在公共密钥证书未被验证时要执行的一个或多个动作
430
基于（多个）验证域，（多个）资源和/或（多个）动作，生成和/或提供用于验证公共密钥证书的代码
440
400

图4

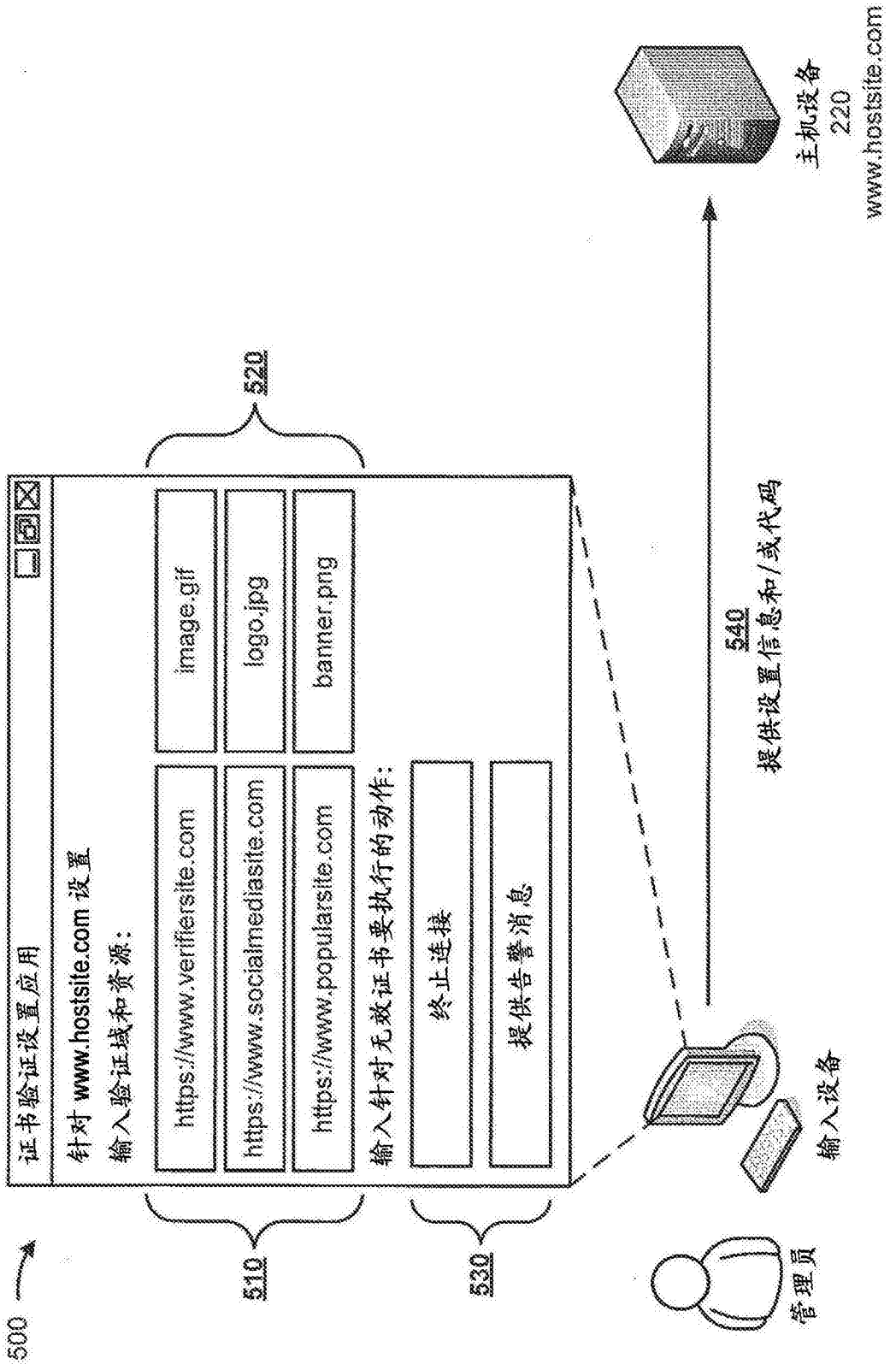

500
证书验证设置应用
针对 www.hostsite.com 设置
输入验证域和资源：
https://www.verifiersite.com
https://www.socialmediasite.com
https://www.popularsite.com
image.gif
logo.jpg
banner.png
520
510
输入针对无效证书要执行的动作：
终止连接
提供告警消息
530
540
提供设置信息和/或代码
主机设备
220
www.hostsite.com
管理员
输入设备

图5A

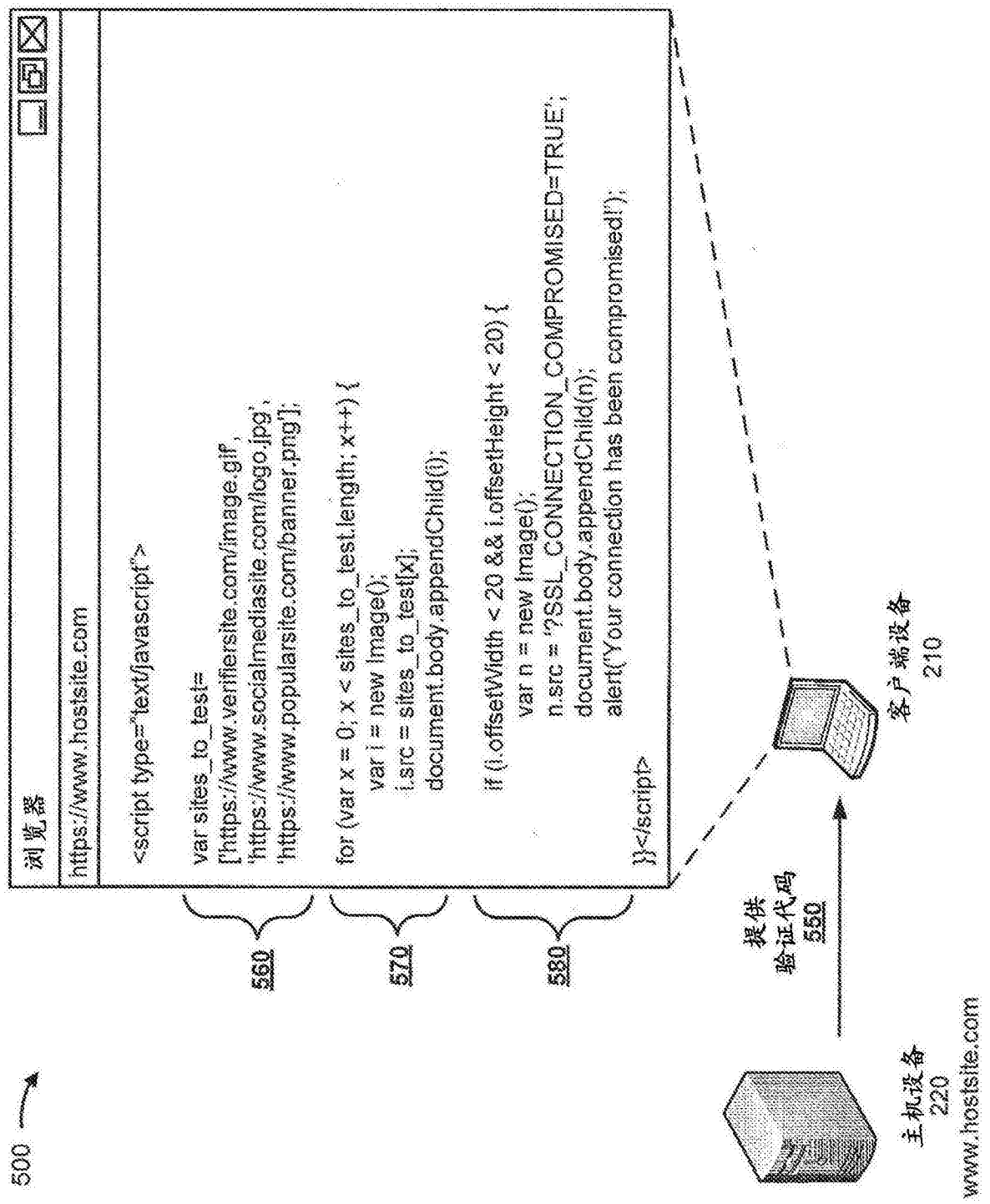

500
浏览器
https://www.hostsite.com
<script type="text/javascript">
var sites_to_test=
['https://www.verifiersite.com/image.gif',
'https://www.socialmediasite.com/logo.jpg',
'https://www.popularsite.com/banner.png'];
for (var x = 0; x < sites_to_test.length; x++) {
var i = new Image();
i.src = sites_to_test[x];
document.body.appendChild(i);
if (i.offsetWidth < 20 && i.offsetHeight < 20) {
var n = new Image();
n.src = '?SSL_CONNECTION_COMPROMISED=TRUE';
document.body.appendChild(n);
alert('Your connection has been compromised!');
}}</script>
560
570
580
提供
验证代码
550
客户端设备
210
主机设备
220
www.hostsite.com

图5B

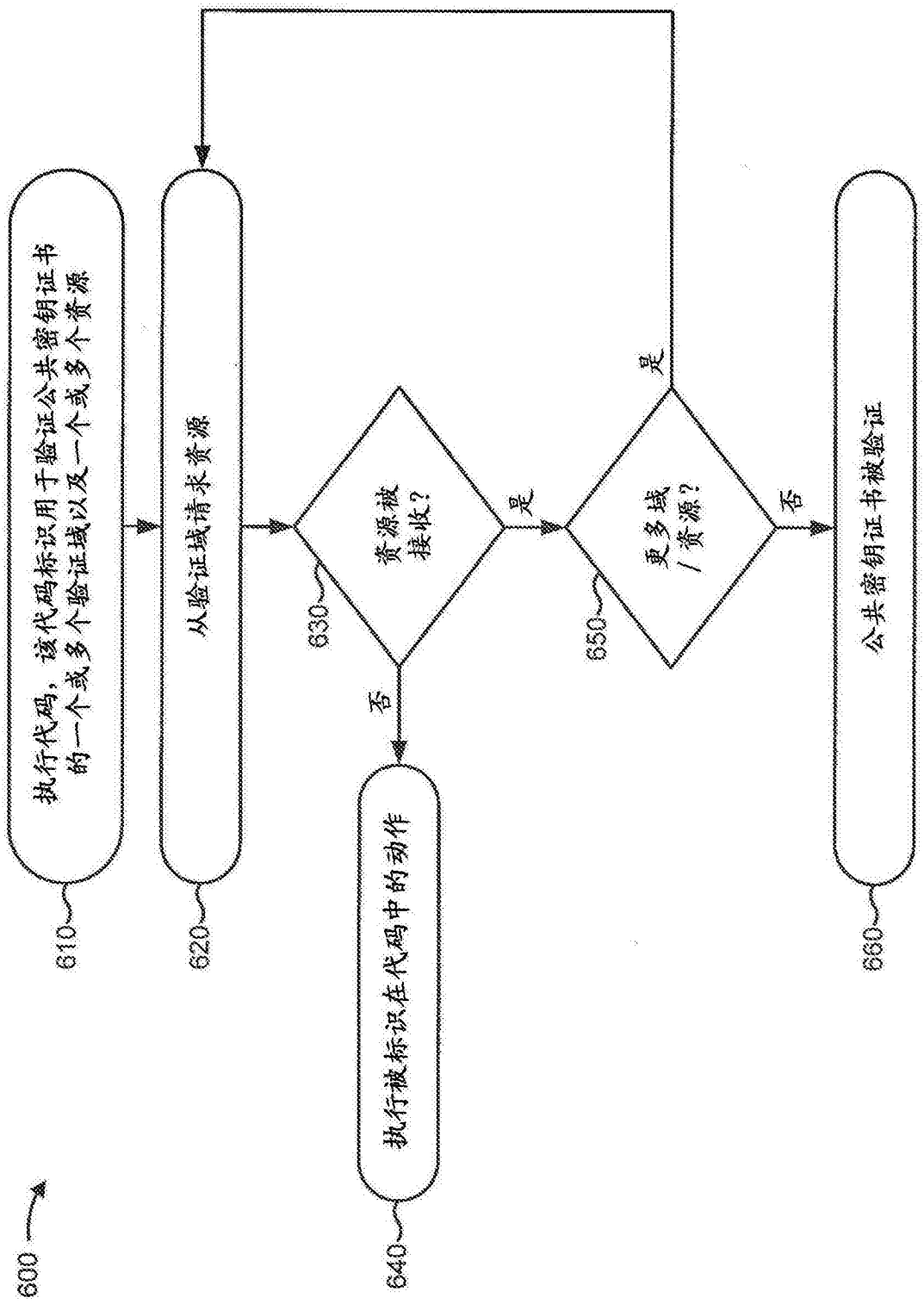

600
执行代码，该代码标识用于验证公共密钥证书的一个或多个验证域以及一个或多个资源
610
从验证域请求资源
620
资源被接收?
630
否
是
执行被标识在代码中的动作
640
更多域/资源?
650
是
否
公共密钥证书被验证
660

图6

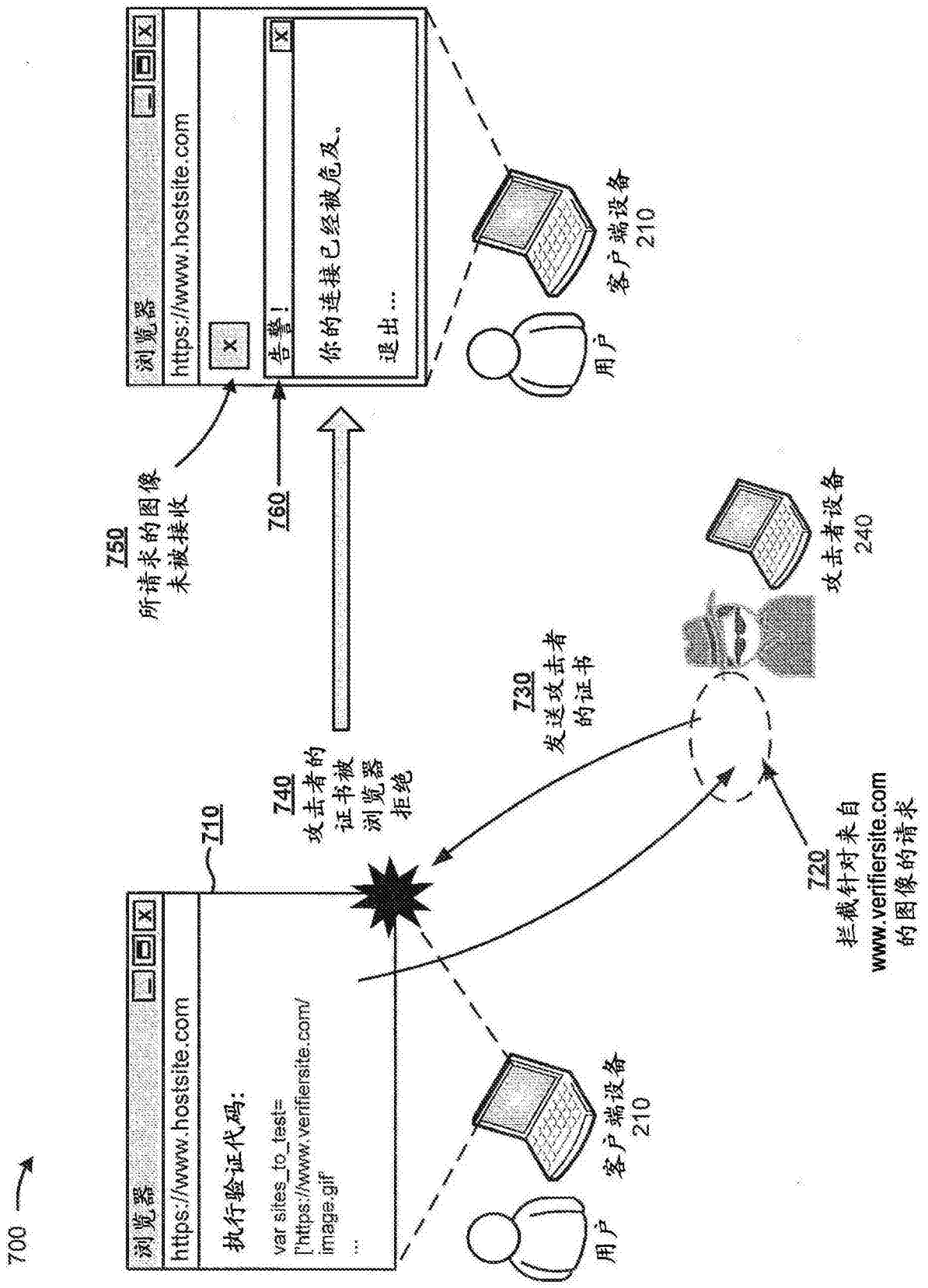

700
浏览器
https://www.hostsite.com
执行验证代码:
var sites_to_test=
['https://www.verifiersite.com/
image.gif
...
710
用户
客户端设备
210
740
攻击者的
证书被
浏览器
拒绝
730
发送攻击者
的证书
攻击者设备
240
720
拦截针对来自
www.verifiersite.com
的图像的请求
760
750
所请求的图像
未被接收
浏览器
https://www.hostsite.com
告警!
你的连接已经被危及。
退出...
用户
客户端设备
210

图7

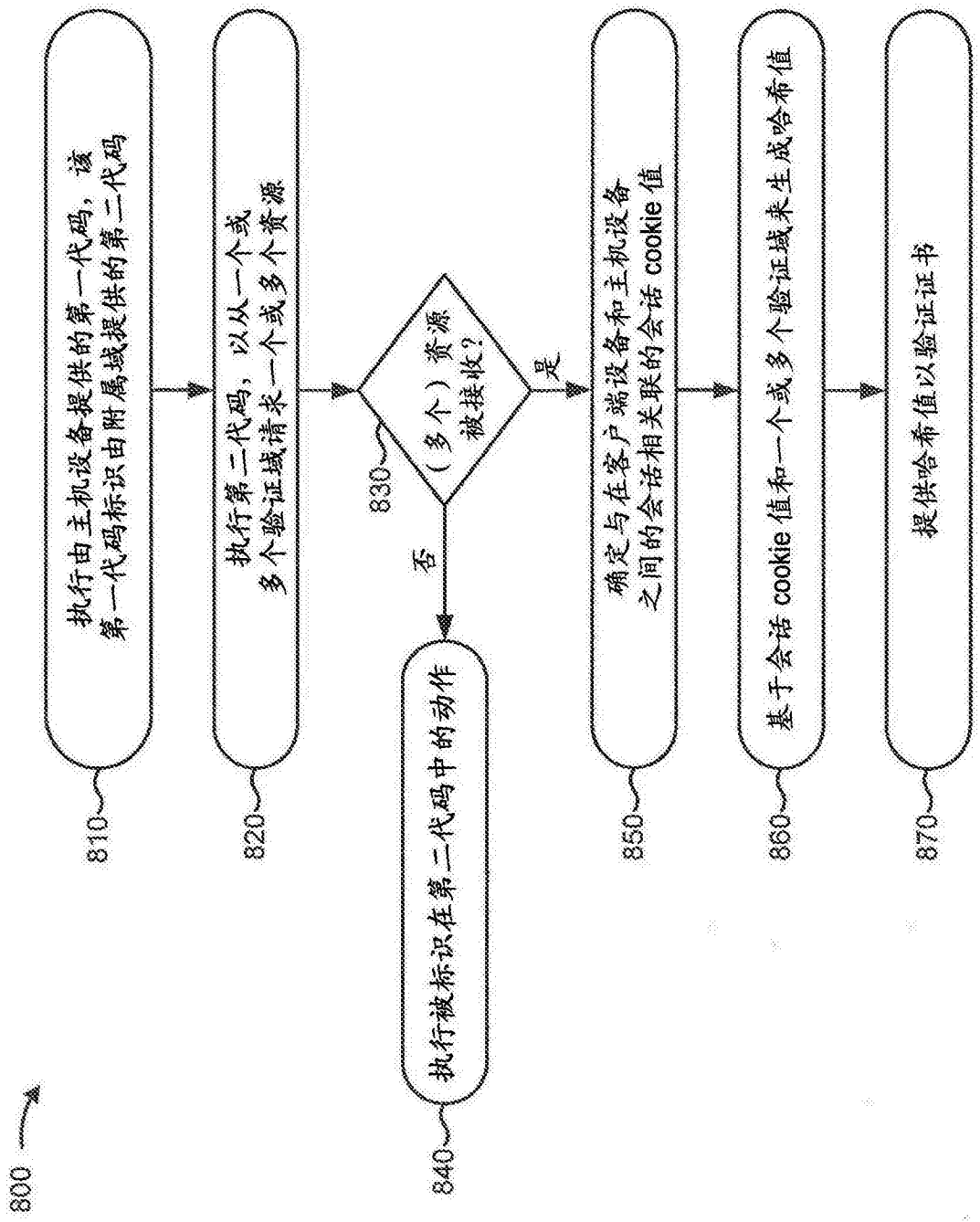

800
执行由主机设备提供的第一代码，该第一代码标识由附属域提供的第二代码
810
执行第二代码，以从一个或多个验证域请求一个或多个资源
820
（多个）资源被接收？
830
否
是
执行被标识在第二代码中的动作
840
确定与在客户端设备和主机设备之间的会话相关联的会话 cookie 值
850
基于会话 cookie 值和一个或多个验证域来生成哈希值
860
提供哈希值以验证证书
870

图8

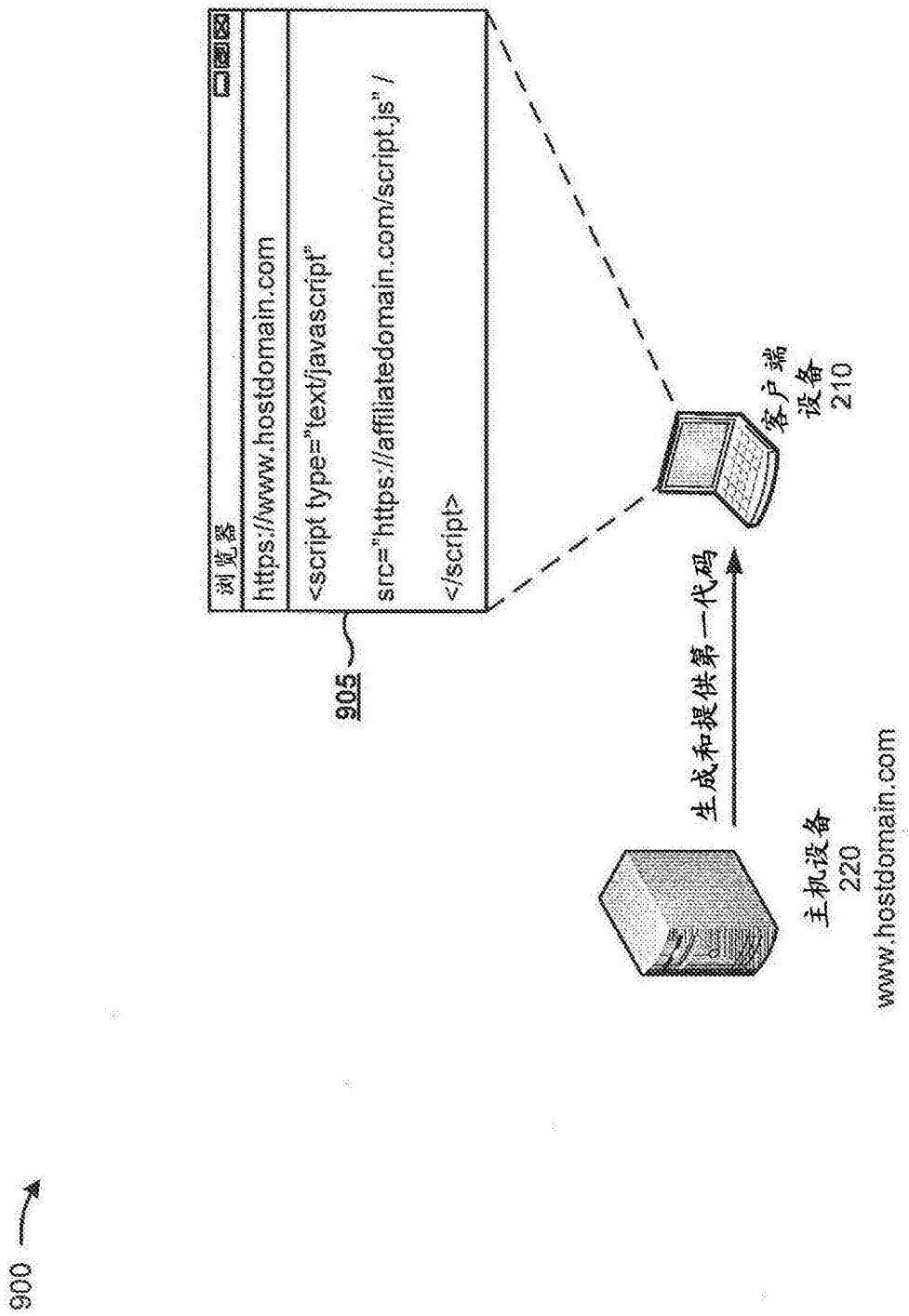

浏览器
https://www.hostdomain.com
<script type="text/javascript"
src="https://affiliatedomain.com/script.js" />
</script>
905
客户端
设备
210
生成和提供第一代码
主机设备
220
www.hostdomain.com
900

图9A

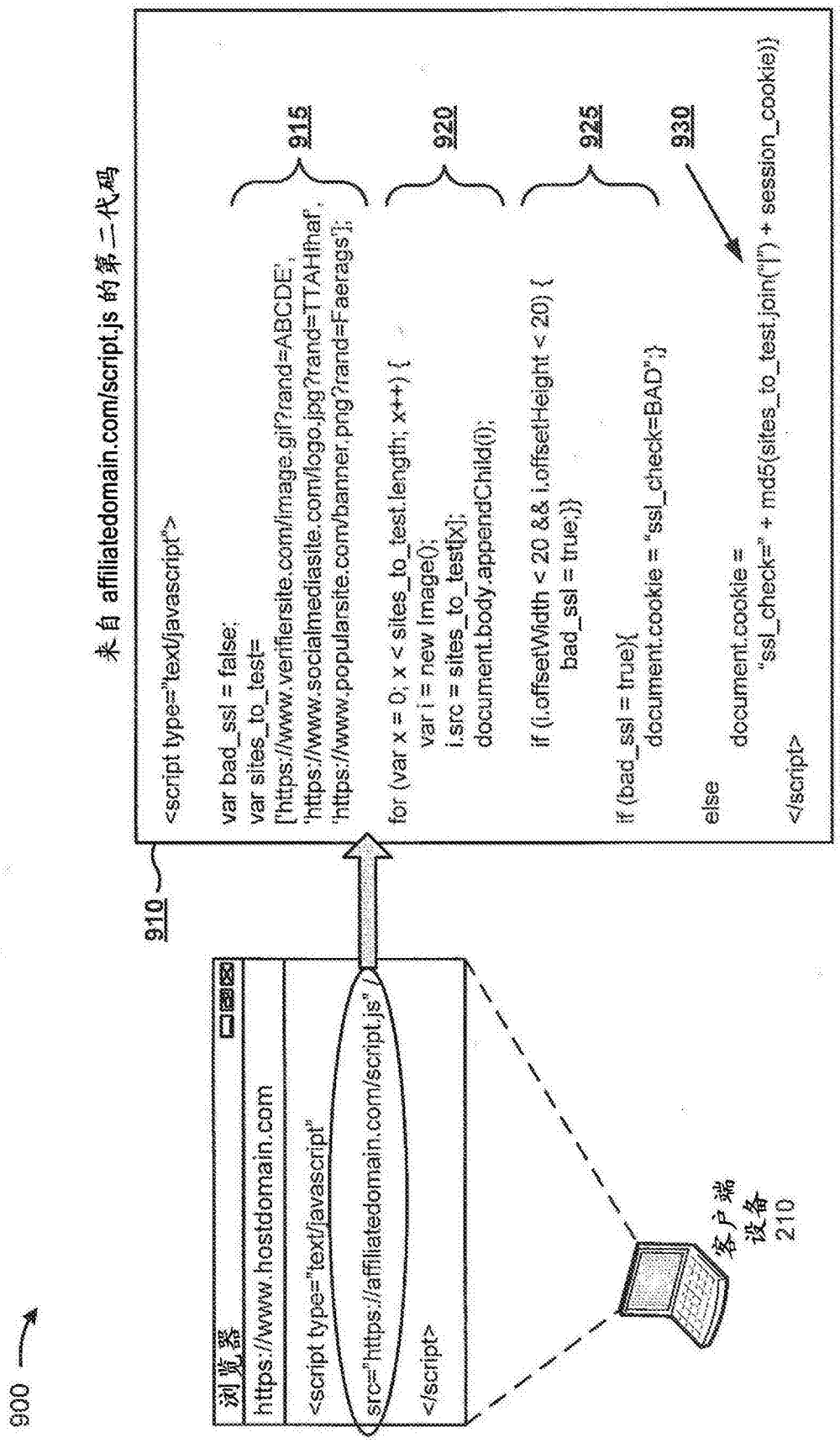

900
浏览器
https://www.hostdomain.com
<script type="text/javascript"
src="https://affiliatedomain.com/script.js" />
</script>
客户端设备 210
910
来自 affiliatedomain.com/script.js 的第二代码
<script type="text/javascript">
var bad_ssl = false;
var sites_to_test=
['https://www.verifiersite.com/image.gif?rand=ABCDE',
'https://www.socialmediasite.com/logo.jpg?rand=TTAHfmaf',
'https://www.popularsite.com/banner.png?rand=Faerags'];
for (var x = 0; x < sites_to_test.length; x++) {
var i = new Image();
i.src = sites_to_test[x];
document.body.appendChild(i);
if (i.offsetWidth < 20 && i.offsetHeight < 20) {
bad_ssl = true;}}
if (bad_ssl = true){
document.cookie = "ssl_check=BAD";}
else
document.cookie =
"ssl_check=" + md5(sites_to_test.join("|") + session_cookie)}
</script>
915
920
925
930

图9B

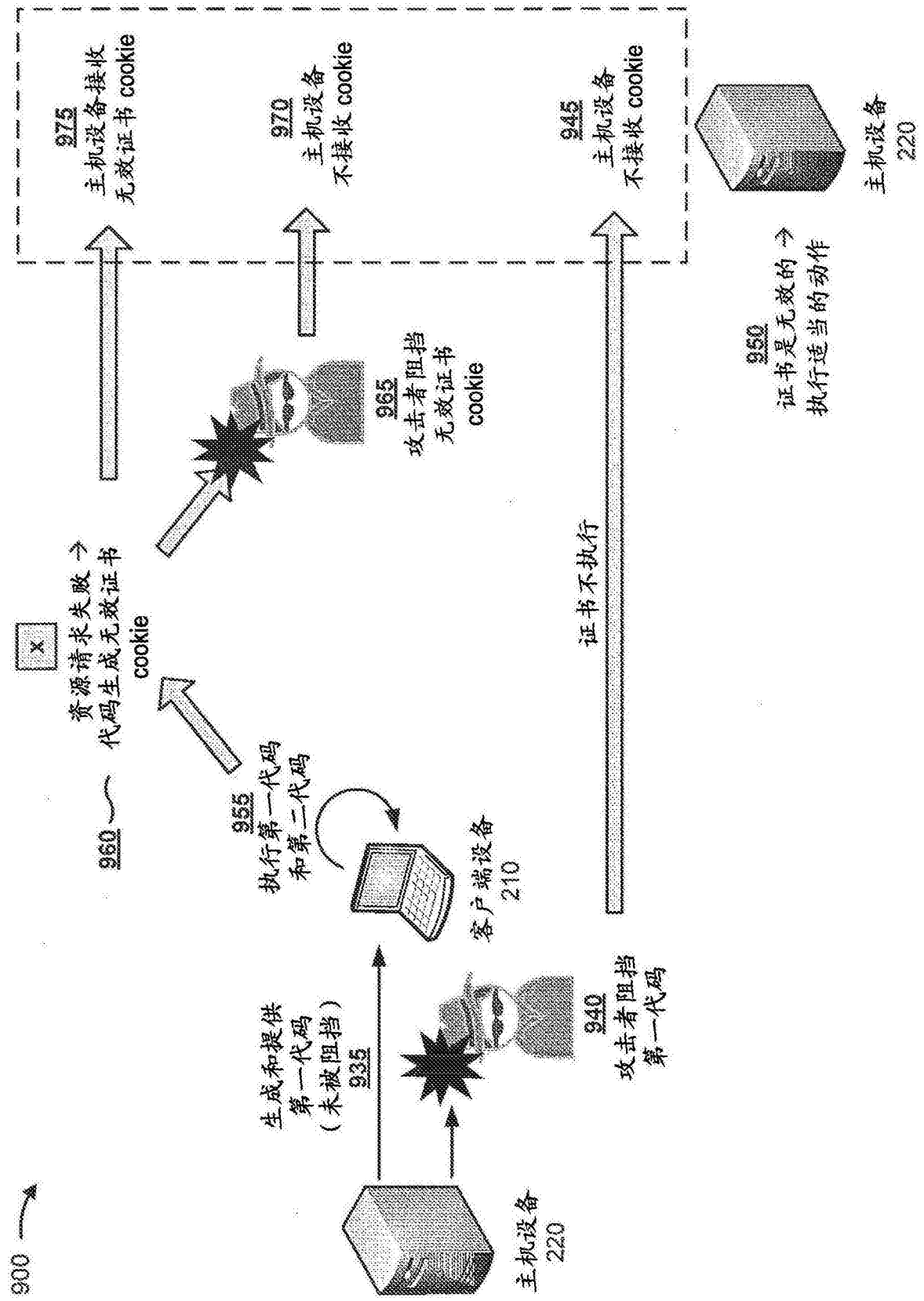

900
主机设备
220
生成和提供
第一代码
（未被阻挡）
935
940
攻击者阻挡
第一代码
客户端设备
210
955
执行第一代码
和第二代码
960
资源请求失败 →
代码生成无效证书
cookie
965
攻击者阻挡
无效证书
cookie
970
主机设备
不接收 cookie
975
主机设备接收
无效证书 cookie
证书不执行
945
主机设备
不接收 cookie
950
证书是无效的 →
执行适当的动作
主机设备
220

图9C

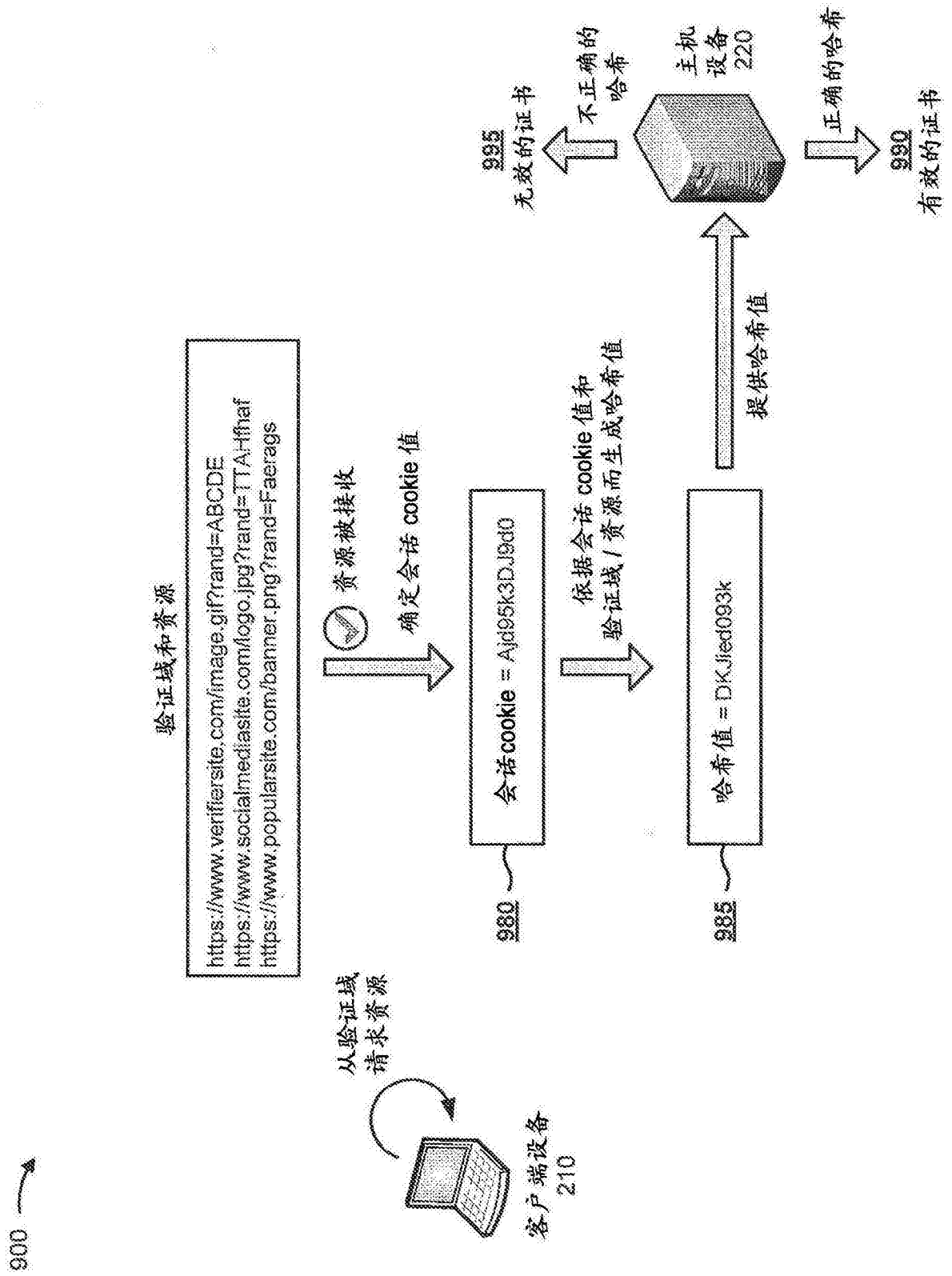

900
客户端设备
210
从验证域
请求资源
验证域和资源
https://www.verifiersite.com/image.gif?rand=ABCDE
https://www.socialmediasite.com/logo.jpg?rand=TTAHfhaf
https://www.popularsite.com/banner.png?rand=Faerags
资源被接收
确定会话 cookie 值
980
会话cookie = Ajd95k3DJ8d0
依据会话 cookie 值和
验证域 / 资源而生成哈希值
985
哈希值 = DKJied093k
提供哈希值
主机
设备
220
不正确的
哈希
995
无效的证书
正确的哈希
990
有效的证书

图9D