



(12)发明专利

(10)授权公告号 CN 105262605 B

(45)授权公告日 2018.09.25

(21)申请号 201410342583.6

(22)申请日 2014.07.17

(65)同一申请的已公布的文献号  
申请公布号 CN 105262605 A

(43)申请公布日 2016.01.20

(73)专利权人 阿里巴巴集团控股有限公司  
地址 英属开曼群岛大开曼资本大厦一座四  
层847号邮箱

(72)发明人 蒋春华

(74)专利代理机构 北京晋德允升知识产权代理  
有限公司 11623

代理人 杨移

(51)Int.Cl.  
H04L 12/24(2006.01)

(56)对比文件

- CN 103067398 A, 2013.04.24,
- CN 1784673 A, 2006.06.07,
- CN 103581145 A, 2014.02.12,
- CN 101541002 A, 2009.09.23,
- US 2001045451 A1, 2001.11.29,
- US 2014165174 A1, 2014.06.12,

审查员 范玲

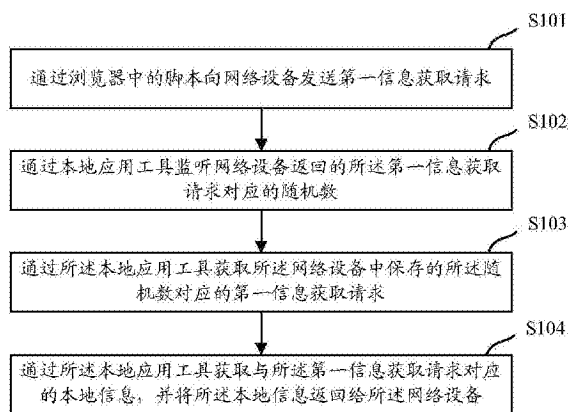
权利要求书2页 说明书10页 附图5页

(54)发明名称

一种获取本地信息的方法、装置及系统

(57)摘要

本申请公开了一种获取本地信息的方法、装置及系统,用以解决现有通过浏览器插件技术获取本地信息导致浏览器不稳定的问题,以及网站维护困难的问题。所述方法包括:通过浏览器中的脚本向网络设备发送第一信息获取请求,其中,所述第一信息获取请求用于指示本地应用工具获取本地信息;通过所述本地应用工具监听网络设备返回的所述第一信息获取请求对应的随机数;通过所述本地应用工具获取所述网络设备中保存的所述随机数对应的第一信息获取请求;其中,所述随机数与所述第一信息获取请求的对应关系是由所述网络设备建立并保存的;通过所述本地应用工具获取与所述第一信息获取请求对应的本地信息,并将所述本地信息发送给所述网络设备。



1. 一种获取本地信息的方法,其特征在于,包括:

通过浏览器中的脚本向网络设备发送第一信息获取请求,其中,所述第一信息获取请求用于指示本地应用工具获取本地信息;

通过所述本地应用工具监听网络设备返回的所述第一信息获取请求对应的随机数;

通过所述本地应用工具获取所述网络设备中保存的所述随机数对应的第一信息获取请求;其中,所述随机数与所述第一信息获取请求的对应关系是由所述网络设备建立并保存的;

通过所述本地应用工具获取与所述第一信息获取请求对应的本地信息,并将所述本地信息发送给所述网络设备。

2. 如权利要求1所述的方法,其特征在于,通过所述本地应用工具获取的所述第一信息获取请求为加密后的第一信息获取请求;

通过所述本地应用工具获取与所述第一信息获取请求对应的本地信息之前,还包括:

通过所述本地应用工具对所述第一信息获取请求进行解密处理。

3. 如权利要求1所述的方法,其特征在于,所述脚本包括JavaScript脚本。

4. 一种获取本地信息的方法,其特征在于,包括:

接收终端通过浏览器中的脚本发送的第一信息获取请求,其中,所述第一信息获取请求用于指示终端的本地应用工具获取本地信息;

确定并保存所述第一信息获取请求对应的随机数;

将所述随机数返回所述终端;

接收终端通过所述本地应用工具发送的第二信息获取请求;

向终端返回所述第二信息获取请求中携带的随机数对应的第一信息获取请求;

接收终端通过所述本地应用工具获取的与接收到的所述第一信息获取请求对应的本地信息。

5. 如权利要求4所述的方法,其特征在于,向终端返回所述第二信息获取请求中携带的随机数对应的第一信息获取请求之前,还包括:

对所述第二信息获取请求中携带的随机数对应的第一信息获取请求进行加密处理。

6. 一种获取本地信息的装置,其特征在于,包括:

第一信息获取请求发送模块,用于通过浏览器中的脚本向网络设备发送第一信息获取请求,其中,所述第一信息获取请求用于指示本地应用工具获取本地信息;

随机数监听模块,用于通过所述本地应用工具监听网络设备返回的所述第一信息获取请求对应的随机数;

第一信息获取请求获取模块,用于通过所述本地应用工具获取所述网络设备中保存的所述随机数对应的第一信息获取请求;其中,所述随机数与所述第一信息获取请求的对应关系是由所述网络设备建立并保存的;

本地信息获取模块,用于通过所述本地应用工具获取与所述第一信息获取请求对应的本地信息;

本地信息发送模块,用于通过所述本地应用工具将所述本地信息发送给所述网络设备。

7. 根据权利要求6所述的装置,其特征在于,所述第一信息获取请求获取模块通过所述

本地应用工具获取的所述第一信息获取请求为加密后的所述第一信息获取请求；

所述装置还包括：解密模块，用于在所述本地信息获取模块通过所述本地应用工具获取与所述第一信息获取请求对应的本地信息之前，对所述第一信息获取请求获取模块获取的所述第一信息获取请求进行解密处理。

8. 根据权利要求6所述的装置，其特征在于，所述脚本包括JavaScript脚本。

9. 一种获取本地信息的装置，其特征在于，包括：

第一信息获取请求接收模块，用于接收终端通过浏览器中的脚本发送的第一信息获取请求，其中，所述第一信息获取请求用于指示终端的本地应用工具获取本地信息；

随机数确定模块，用于确定所述第一信息获取请求对应的随机数；

随机数发送模块，用于将所述随机数返回所述终端；

存储模块，用于保存所述第一信息获取请求对应的随机数；

第二信息获取请求接收模块，用于接收终端通过所述本地应用工具发送的第二信息获取请求；

第一信息获取请求发送模块，用于向终端返回所述第二信息获取请求中携带的随机数对应的所述第一信息获取请求；

本地信息接收模块，用于接收终端通过所述本地应用工具获取的与接收到的所述第一信息获取请求对应的本地信息。

10. 根据权利要求9所述的装置，其特征在于，所述装置还包括：加密模块，用于在所述第一信息获取请求发送模块向终端返回所述第二信息获取请求中携带的随机数对应的所述第一信息获取请求之前，对所述第二信息获取请求中携带的随机数对应的所述第一信息获取请求进行加密处理。

11. 一种获取本地信息的系统，其特征在于，包括：

终端，用于通过浏览器中的脚本向网络设备发送第一信息获取请求，其中，所述第一信息获取请求用于指示本地应用工具获取本地信息；通过所述本地应用工具监听网络设备返回的所述第一信息获取请求对应的随机数；通过所述本地应用工具获取所述网络设备中保存的所述随机数对应的所述第一信息获取请求；以及通过所述本地应用工具获取与所述第一信息获取请求对应的本地信息，并将所述本地信息发送给所述网络设备；

网络设备，用于接收所述终端发送的第一信息获取请求；确定并保存所述第一信息获取请求对应的随机数；将所述随机数返回所述终端；接收终端通过所述本地应用工具发送的第二信息获取请求；向终端返回所述第二信息获取请求中携带的随机数对应的所述第一信息获取请求；以及接收所述终端发送的本地信息。

## 一种获取本地信息的方法、装置及系统

### 技术领域

[0001] 本申请涉及计算机技术领域,尤其涉及一种获取本地信息的方法、装置及系统。

### 背景技术

[0002] 网页(Web)应用是用户界面驻留在浏览器中的应用程序,例如,网上银行或网上支付等在线Web应用。

[0003] 在使用某些Web应用时,网络设备需要获取终端的本地信息。例如,用户通过终端实现网上银行或网上支付的相关操作时,为了保证信息安全,网络设备需要获取终端的本地信息以完成整个操作过程。以网上支付为例,在用户登录支付宝页面的过程中,终端可通过浏览器中的脚本获取该终端自身的本地信息,并提交给网络设备。所述本地信息可以为用于确认该终端可靠性的本地数字证书的验证结果等。

[0004] 但是,出于信息安全考虑,浏览器不能直接获取其所在的终端的本地信息。因此,在现有技术中,一般通过浏览器插件技术实现对本地信息的获取。具体的,上述网上支付实例,用户需要在浏览器的提示下,在本地预先安装验证数字证书的插件。则终端通过浏览器中的脚本直接调用所述插件,并通过该插件获取数字证书的验证结果,最后将验证结果提交给网络设备。

[0005] 然而,采用上述浏览器插件技术获取本地信息存在以下不足:首先,浏览器与插件之间还存在兼容性的问题,当当前获取本地信息的浏览器与本地安装的相应插件的兼容性不高或者完全不兼容时,容易导致网页上获取本地信息无法进行,甚至还会导致浏览器崩溃,从而导致浏览器使用不稳定。此外,不同类型的浏览器或同一类型浏览器的不同版本对应的插件技术可能不同(如,插件与不同浏览器进行交互的接口不同),因此,这就需要网站适配不同浏览器插件技术,这会大大增加网站维护的难度。

### 发明内容

[0006] 本申请实施例提供一种获取本地信息的方法和装置,用以解决现有通过浏览器插件技术获取本地信息导致浏览器不稳定的问题,以及网站维护困难的问题。

[0007] 为实现上述目的,本申请实施例提供了一种获取本地信息的方法,包括:

[0008] 通过浏览器中的脚本向网络设备发送第一信息获取请求,其中,所述第一信息获取请求用于指示本地应用工具获取本地信息;

[0009] 通过所述本地应用工具监听网络设备返回的所述第一信息获取请求对应的随机数;

[0010] 通过所述本地应用工具获取所述网络设备中保存的所述随机数对应的第一信息获取请求;其中,所述随机数与所述第一信息获取请求的对应关系是由所述网络设备建立并保存的;

[0011] 通过所述本地应用工具获取与所述第一信息获取请求对应的本地信息,并将所述本地信息发送给所述网络设备。

[0012] 本申请实施例提供的另一种获取本地信息的方法,包括:

[0013] 接收终端通过浏览器中的脚本发送的第一信息获取请求,其中,所述第一信息获取请求用于指示终端的本地应用工具获取本地信息;

[0014] 确定并保存所述第一信息获取请求对应的随机数;

[0015] 将所述随机数返回所述终端;

[0016] 接收终端通过所述本地应用工具发送的第二信息获取请求;

[0017] 向终端返回所述第二信息获取请求中携带的随机数对应的第一信息获取请求;

[0018] 接收终端通过所述本地应用工具获取的与接收到的所述第一信息获取请求对应的本地信息。

[0019] 本申请实施例提供的一种获取本地信息的装置,包括:

[0020] 第一信息获取请求发送模块,用于通过浏览器中的脚本向网络设备发送第一信息获取请求,其中,所述第一信息获取请求用于指示本地应用工具获取本地信息;

[0021] 随机数监听模块,用于通过所述本地应用工具监听网络设备返回的所述第一信息获取请求对应的随机数;

[0022] 第一信息获取请求获取模块,用于通过所述本地应用工具获取所述网络设备中保存的所述随机数对应的第一信息获取请求;其中,所述随机数与所述第一信息获取请求的对应关系是由所述网络设备建立并保存的;

[0023] 本地信息获取模块,用于通过所述本地应用工具获取与所述第一信息获取请求对应的本地信息;

[0024] 本地信息发送模块,用于通过所述本地应用工具将所述本地信息发送给所述网络设备。

[0025] 本申请实施例提供的另一种获取本地信息的装置,包括:

[0026] 第一信息获取请求接收模块,用于接收终端通过浏览器中的脚本发送的第一信息获取请求,其中,所述第一信息获取请求用于指示终端的本地应用工具获取本地信息;

[0027] 随机数确定模块,用于确定所述第一信息获取请求对应的随机数;

[0028] 随机数发送模块,用于将所述随机数返回所述终端;

[0029] 存储模块,用于保存所述第一信息获取请求对应的随机数;

[0030] 第二信息获取请求接收模块,用于接收终端通过所述本地应用工具发送的第二信息获取请求;

[0031] 第一信息获取请求发送模块,用于向终端返回所述第二信息获取请求中携带的随机数对应的第一信息获取请求;

[0032] 本地信息接收模块,用于接收终端通过所述本地应用工具获取的与接收到的所述第一信息获取请求对应的本地信息。

[0033] 本申请实施例提供的一种获取本地信息的系统,包括:

[0034] 终端,用于通过浏览器中的脚本向网络设备发送第一信息获取请求,其中,所述第一信息获取请求用于指示本地应用工具获取本地信息;通过所述本地应用工具监听网络设备返回的所述第一信息获取请求对应的随机数;通过所述本地应用工具获取所述网络设备中保存的所述随机数对应的第一信息获取请求;以及通过所述本地应用工具获取与所述第一信息获取请求对应的本地信息,并将所述本地信息发送给所述网络设备;

[0035] 网络设备,用于接收所述终端发送的第一信息获取请求;确定并保存所述第一信息获取请求对应的随机数;将所述随机数返回所述终端;接收终端通过所述本地应用工具发送的第二信息获取请求;向终端返回所述第二信息获取请求中携带的随机数对应的第一信息获取请求;以及接收所述终端发送的本地信息。

[0036] 本申请通过终端的本地应用工具监听网络设备返回的与自身接收到的第一信息获取请求对应的随机数,获取网络设备保存的与所述随机数对应的第一信息获取请求,获取所述第一信息获取请求对应的本地信息,以及将所述本地信息提交给网络设备供其他设备获取使用。由于本地应用工具与浏览器之间无需任何用于信息交互的接口,因此,浏览器与本地应用工具之间不存在兼容性的问题,从而可有效避免通过浏览器插件技术获取本地信息时因兼容性导致浏览器不稳定的问题,也可有效降低网站维护的难度。

### 附图说明

[0037] 此处所说明的附图用来提供对本申请的进一步理解,构成本申请的一部分,本申请的示意性实施例及其说明用于解释本申请,并不构成对本申请的不当限定。在附图中:

[0038] 图1为本申请实施例提供的获取本地信息的方法流程示意图之一;

[0039] 图2为本申请实施例提供的获取本地信息的方法流程示意图之二;

[0040] 图3为本申请实施例提供的获取本地信息的方法流程示意图之三;

[0041] 图4为本申请实施例提供的获取本地信息的装置结构意图之一;

[0042] 图5为本申请实施例提供的获取本地信息的装置结构意图之二;

[0043] 图6为本申请实施例提供的获取本地信息的系统结构意图。

### 具体实施方式

[0044] 本申请实施例基于信息安全的考虑,终端的浏览器不能直接获取其所在的终端的本地信息,而如果浏览器直接调用插件获取本地信息,又要求浏览器与插件具有较高的兼容性。因此,在浏览器不直接获取本地信息这个前提下,本申请终端通过浏览器中的脚本向网络设备发送用于获取本地信息的获取请求,并通过本地应用工具从网络设备中获取该获取请求,再根据该获取请求获取相应的本地信息,最后将该本地信息提供给网络设备。这样,浏览器既不直接获取本地信息,保证了信息安全,又不直接与本地应用工具进行交互,无需与本地应用工具兼容,从而可有效避免浏览器与插件不兼容而导致浏览器不稳定的问题,也可有效避免网站维护难度的问题。

[0045] 为使本申请的目的、技术方案和优点更加清楚,以下将结合本申请具体实施例及相应的附图对本申请技术方案进行清楚、完整地描述。显然,所描述的实施例仅是本申请一部分实施例,而不是全部的实施例。基于本申请中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本申请保护的范围。

[0046] 下面将从终端侧说明本申请实施例提供的获取本地信息的方法。

[0047] 参见图1,为本申请实施例提供的获取本地信息的方法,包括:

[0048] S101、终端通过浏览器中的脚本向网络设备发送第一信息获取请求,其中,所述第一信息获取请求用于指示本地应用工具获取本地信息。

[0049] 本申请实施例所述的脚本为浏览器可以解析并执行的脚本,具体的,所述脚本包

包括但不限于JavaScript脚本,简称JS脚本。

[0050] 不同的Web应用可能需要终端提供不同的本地信息,本申请所述的本地信息包括但不限于:本地用户的数字证书的验证结果、本地设备标识信息、系统应用程序接口信息(如,系统应用(Application,App)接口信息)、本地文件系统信息等。

[0051] 下面以Web应用为支付应用为实例进行说明,假设用户要登录该支付应用的页面,则该支付应用的服务器(即,网络设备)需要终端提供对该终端的本地数字证书的验证结果(该验证结果即为本地信息)。

[0052] 其中,所述的本地应用工具可以为能够对本地数字证书进行验证并提供验证结果的可执行程序。所述的可执行程序可存储在所述终端自身的存储介质(如,该终端的硬盘)中,或者存储在与该终端相连的外部存储介质(如,与该终端相连的移动硬盘)中。

[0053] 需要说明的是,所述终端通过浏览器中的脚本向网络设备发送第一信息获取请求的步骤可以是由终端向网络设备发送业务请求的步骤触发的。当然,也可以是与业务请求同时发送的(如,将第一信息获取请求和业务请求整合为一个请求消息发送给网络设备)。

[0054] 具体的,沿用上述实例,用户在登录该支付应用的页面的过程中,终端需要先通过浏览器向该支付应用的服务器发送登录请求(该登录请求即为业务请求),从而,浏览器触发通过JS脚本向服务器发送第一信息获取请求的步骤。该第一信息获取请求用于指示该终端的本地应用工具获取该终端的本地数字证书的验证结果。

[0055] 其中,该JS脚本可以是当服务器接收到该登录请求后向浏览器返回并安装在浏览器中的。当然,也可以是预先配置在浏览器中的。

[0056] S102、终端通过所述本地应用工具监听网络设备返回的所述第一信息获取请求对应的随机数。

[0057] 本申请实施例所述的随机数为明文的随机数,即,该随机数是未经过加密的随机数,从而,本地应用工具监听到该随机数后可直接读取。

[0058] 网络设备在接收到终端发送的第一信息获取请求后,则可生成一个随机数,作为该第一信息获取请求对应的随机数,并返回给终端。当终端接收到该随机数时,终端中的本地应用工具即可监听到网络设备返回的该随机数。当然,网络设备自身也要保存生成的该随机数与该第一信息获取请求的对应关系。

[0059] 进一步的,在实际应用场景中,终端与网络设备是基于超文本传输安全协议(Hypertext Transfer Protocol Securehttps,HTTPS)进行信息交互的,其中,HTTPS协议是超文本传输协议(Hypertext Transfer Protocol,HTTP)和安全套接层(Secure Sockets Layer,SSL)协议的组合,也即,终端每次通过浏览器中的JS脚本向网络设备发送一个信息获取请求时,终端都会与网络设备基于SSL协议进行一次安全连接过程,在安全连接过程执行完毕后,网络设备才会基于由该安全连接过程所建立的安全通道接收到该信息获取请求。而在该安全连接过程的密钥协商过程中,终端和网络设备会分别生成随机数并提供给对方,并且安全连接过程中终端和网络设备之间交互的随机数均为明文的随机数。因此,在本申请实施例中,网络设备在接收到终端通过浏览器中的JS脚本发送的第一信息获取请求后,不必再专门针对该第一信息获取请求生成随机数并返回,可直接利用该网络设备自身在安全连接过程中所生成的随机数,建立该随机数与后续接收到的该第一信息获取请求的对应关系并保存即可。而由于在安全连接过程中,网络设备已经将该随机数返回给了终端,

终端的本地应用工具也已经监听到了该随机数,因此,网络设备建立并保存了的安全连接过程中所生成的随机数与后续接收到的该第一信息获取请求的对应关系后,也无需再次向终端返回该随机数,以达到避免网络设备重复生成和返回随机数而浪费资源的问题。终端中的本地应用工具监听到了该安全连接过程中的随机数后,则可周期性的向网络设备发送携带该随机数的第二信息获取请求,用以获取该随机数对应的第一信息获取请求。

[0060] 而且,如果将安全连接过程中网络设备返回的随机数作为该第一信息获取请求对应的随机数,则终端中的本地应用工具在监听安全连接过程中网络设备返回的随机数时,可采用信息过滤和复制的方法进行监听,以避免影响密钥协商过程。具体的,终端通过本地应用工具监听密钥协商过程中网络设备返回的随机数时,可通过预先设置驱动层的SSL协议,使得本地应用工具在驱动层对终端与网络设备之间的交互信息进行过滤,读取终端与网络设备之间密钥协商过程中网络设备返回的随机数,从而快捷有效地获取网络设备返回的随机数。另外,还需要保证终端通过所述本地应用工具监听到的随机数与所述第一信息获取请求唯一对应,即需要保证网络设备每次返回给终端的随机数唯一,以避免终端提供给网络设备的本地信息不准确的问题。

[0061] 具体的,本申请可以通过设置网络设备用于SSL协议密钥协商过程的随机数的生成算法,首先保证每次生成的随机数是唯一的。还可以通过设置SSL协议使得会话缓存(SSL session cache)指令和安全连接(connection keepalive)指令在终端通过浏览器中的脚本向网络设备发送第一信息获取请求之后关闭,避免因会话缓存中保存的随机数被网络设备在与终端安全连接过程中重复使用,从而又保证了网络设备返回给终端的随机数唯一。

[0062] S103、终端通过所述本地应用工具获取所述网络设备中保存的所述随机数对应的第一信息获取请求;其中,所述随机数与所述第一信息获取请求的对应关系是由所述网络设备建立并保存的。

[0063] 终端可主动获取网络设备中保存的随机数对应的第一信息获取请求,也可被动获取网络设备发送的随机数对应的第一信息获取请求。

[0064] 具体的,终端可通过本地应用工具主动向网络设备发送携带监听到的随机数的第二信息获取请求,则网络设备会根据所述第二信息获取请求中携带的随机数返回给终端与所述随机数对应的第一信息获取请求。或者,终端可通过本地应用工具被动接收网络设备提供的携带第一信息获取请求和随机数的响应消息,则本地应用工具接收到该响应消息后,可验证该响应消息中携带的随机数与自身监听到的随机数是否一致,若一致,则可通过后续的步骤S104获取本地信息,若不一致,则可丢弃该响应信息。

[0065] S104、终端通过所述本地应用工具获取与所述第一信息获取请求对应的本地信息,将所述本地信息发送给所述网络设备。

[0066] 继续延用上述实例,该第一信息获取请求为获取本地数字证书的验证结果的获取请求。步骤S103中本地应用工具从网络设备中获取到该第一信息获取请求后,则可根据该第一信息获取请求,对本地数字证书的验证,再将本地数字证书的验证结果发送给网络设备,而由于终端发送该第一信息获取请求的步骤是在终端向网络设备发送登录该支付应用的页面的登录请求时触发的,因此,网络设备接收到该验证结果(也即,本地信息)后,可根据该验证结果,相应处理终端发送的登录请求,即,如果验证结果为验证成功,则允许终端的登录请求,允许终端登录该支付应用的界面,如果验证结果为验证失败,则拒绝终端的登



录请求。

[0067] 本申请上述实施例提供的获取本地信息的方法,终端并非通过浏览器中的脚本直接获取本地信息,而是通过本地应用工具获取本地信息,因此保证了HTTPS协议下信息交互的安全性。而且,浏览器也并非直接调用本地应用工具,以获取本地信息,而是通过脚本向网络设备发送第一信息获取请求,本地应用工具再从网络设备中获取该第一信息获取请求,并根据该第一信息获取请求获取本地信息,因此,本地应用工具无需提供任何与浏览器兼容的接口,二者之间不存在兼容性的问题,可避免浏览器直接调用插件过程中,浏览器与插件不兼容而导致浏览器不稳定的问题,也可进一步避免为了保证不同类型浏览器或不同版本浏览器与本地应用工具兼容而导致网站维护困难的难度。

[0068] 为了保证网络设备向终端的本地应用工具提供第一信息获取请求时,该第一信息获取请求不被第三方截获并修改,在本申请实施例中,网络设备将第一信息获取请求提供给终端的本地应用工具之前,可先对该第一信息获取请求进行加密处理,再将加密后的第一信息获取请求提供给终端的本地应用工具。

[0069] 具体的,如果终端的本地应用工具主动根据监听到的随机数获取第一信息获取请求,则网络设备在接收到终端的本地应用工具发送的第二信息获取请求时,可先对该第二信息获取请求中携带的随机数对应的第一信息获取请求进行加密处理,再将加密后的第一信息获取请求返回给终端的本地应用工具。

[0070] 相应的,终端的本地应用工具接收到该加密后的第一信息获取请求后,则可对所述第一信息获取请求进行解密处理,再根据解密后的第一信息获取请求,获取本地信息,并将本地信息发送给网络设备。

[0071] 下面将从网络设备侧说明对应于上述实施例的另一种获取本地信息的方法。

[0072] 参见图2,本申请实施例提供的另一种获取本地信息的方法,包括:

[0073] S201、网络设备接收终端通过浏览器中的脚本发送的第一信息获取请求,其中,所述第一信息获取请求用于指示终端的本地应用工具获取本地信息;

[0074] S202、网络设备确定并保存所述第一信息获取请求对应的随机数。

[0075] 具体的,网络设备可在接收到该第一信息获取请求时,生成该第一信息获取请求对应的随机数,并保存该第一信息获取请求与该随机数的对应关系,也可直接利用在接收到该第一信息获取请求之前与终端进行安全连接过程中产生的随机数,将该随机数确定为第一信息获取请求对应的随机数,这里不再赘述。

[0076] S203、将所述随机数返回所述终端。

[0077] 网络设备将第一信息获取请求对应的随机数返回给终端后,终端的本地应用工具即可监听到该随机数,并向网络设备发送用于获取该第一信息获取请求的第二信息获取请求。

[0078] 需要说明的是,如果网络设备直接将安全连接过程中所产生的随机数作为该第一信息获取请求对应的随机数,则步骤203可以省略,即,安全连接过程中网络设备已经将该随机数发送给了终端,因此网络设备在接收到第一信息获取请求后也就无需再次发送该随机数。

[0079] S204、网络设备接收终端通过所述本地应用工具发送的第二信息获取请求,所述第二信息获取请求携带本地应用工具监听到的随机数。

[0080] S205、网络设备向终端返回所述第二信息获取请求中携带的随机数对应的第一信息获取请求。

[0081] 其中,该过程为终端主动向网络设备获取第一信息获取请求的过程。终端可通过本地应用工具周期性的向网络设备发送携带该随机数的第二信息获取请求,网络设备则可在每次接收到该第二信息获取请求时,查找自身是否保存有该第二信息获取请求中携带的随机数对应的第一信息获取请求,若查找到,则直接返回相应的第一信息获取请求,若未查找到,则可直接丢弃该第二信息获取请求。

[0082] 当然,网络设备也可以在执行完步骤S203后直接向终端返回携带该随机数以及该第一信息获取请求的响应消息,则终端被动接收网络设备发送的响应消息,这里不再赘述。

[0083] S206、网络设备接收终端通过所述本地应用工具获取的与接收到的所述第一信息获取请求对应的本地信息。

[0084] 也即,网络设备通过步骤S205将第一信息获取请求返回给终端后,终端即可通过本地应用工具根据该第一信息获取请求获取本地信息,并将本地信息发送给网络设备。

[0085] 本申请实施例提供的上述两种获取本地信息的方法中,所述的网络设备可包括网关和服务器,则生成随机数的步骤可由网关执行,建立随机数与第一信息获取请求的对应关系可由网关执行,也可由服务器执行,随机数与第一信息获取请求的对应关系保存在服务器中,以供终端的本地应用工具获取。进一步的,所述的服务器还可包括业务服务器和安全通道服务器,则可由安全通道服务器保存随机数与第一信息获取请求的对应关系,以确保第一信息获取请求的安全性。

[0086] 下面以网络设备包括网关、安全通道服务器和业务服务器为例,对登录支付应用的页面的过程进行详细说明。

[0087] 参见图3,获取本地信息的方法包括以下步骤:

[0088] 步骤a1、终端通过浏览器向业务服务器发送登录请求。

[0089] 步骤a2、业务服务器向终端返回脚本。

[0090] 具体的,所述的脚本可以是JS脚本。

[0091] 步骤a3、终端将接收到的脚本安装在浏览器中,并通过浏览器中安装的脚本向网关发送第一信息获取请求。

[0092] 终端可通过执行安装在浏览器中的脚本,生成该第一信息获取请求并向网关发送。

[0093] 步骤a4、网关向所述终端发起安全连接,将安全连接过程中生成的随机数发送给所述终端。

[0094] 步骤a5、网关建立该随机数与接收到的第一信息获取请求的对应关系,将该随机数、第一信息获取请求以及该对应关系透传给安全通道服务器保存。

[0095] 步骤a6、终端通过本地应用工具监听该终端接收到的来自网关的随机数。

[0096] 步骤a7、终端通过本地应用工具向安全通道服务器发送携带其监听到的随机数的第二信息获取请求。

[0097] 步骤a8、安全通道服务器查询第二信息获取请求中携带的随机数对应的第一信息获取请求,将与查询到的第一信息获取请求返回终端。

[0098] 步骤a9、终端根据接收到的第一信息获取请求,通过本地应用工具验证所述本地

数字证书,并将验证结果返回安全通道服务器。

[0099] 步骤a10、安全通道服务器保存验证结果,供业务服务器查询。

[0100] 业务服务器从所述安全通道服务器查询到该验证结果(也即,本地信息)后,可根据该验证结果,相应处理终端发送的登录请求,即,如果验证结果为验证成功,则允许终端的登录请求,允许终端登录该支付应用的界面,如果验证结果为验证失败,则拒绝终端的登录请求。

[0101] 以上为本申请实施例提供的获取本地信息的方法,基于同样的思路,本申请实施例还提供了获取本地信息的装置和系统,如图4、图5、图6所示。

[0102] 参见图4,为本申请实施例提供的获取本地信息的装置,该装置包括:

[0103] 第一信息获取请求发送模块11,用于通过浏览器中的脚本向网络设备发送第一信息获取请求,其中,所述第一信息获取请求用于指示本地应用工具获取本地信息;

[0104] 随机数监听模块12,用于通过所述本地应用工具监听网络设备返回的所述第一信息获取请求对应的随机数;

[0105] 第一信息获取请求获取模块13,用于通过所述本地应用工具获取所述网络设备中保存的所述随机数对应的第一信息获取请求;其中,所述随机数与所述第一信息获取请求的对应关系是由所述网络设备建立并保存的;

[0106] 本地信息获取模块14,用于通过所述本地应用工具获取与所述第一信息获取请求对应的本地信息;

[0107] 本地信息发送模块15,用于通过所述本地应用工具将所述本地信息发送给所述网络设备。

[0108] 本申请实施例中的随机数监听模块12、第一信息获取请求获取模块13、本地信息获取模块14,和本地信息发送模块15可以设置在所述本地应用工具中。

[0109] 进一步地,第一信息获取请求获取模块13通过所述本地应用工具获取的所述第一信息获取请求为加密后的第一信息获取请求。因此,图4所示的装置还包括:解密模块16,用于在所述本地信息获取模块通过所述本地应用工具获取与所述第一信息获取请求对应的本地信息之前,对所述第一信息获取请求获取模块获取的第一信息获取请求进行解密处理。

[0110] 本申请实施例中,所述脚本可以但不限于为JavaScript脚本。

[0111] 参见图5,为本申请实施例提供的获取本地信息的另一种装置,该装置包括:

[0112] 第一信息获取请求接收模块21,用于接收到终端通过浏览器中的脚本发送的第一信息获取请求,其中,所述第一信息获取请求用于指示终端的本地应用工具获取本地信息;

[0113] 随机数确定模块22,用于确定所述第一信息获取请求对应的随机数;

[0114] 随机数发送模块23,用于将所述随机数返回所述终端;

[0115] 存储模块24,用于保存随机数确定模块22确定的第一信息获取请求对应的随机数,即保第一信息获取请求、随机数以及该第一信息获取请求和随机数的对应关系;

[0116] 第二信息获取请求接收模块25,用于接收终端通过所述本地应用工具发送的第二信息获取请求;

[0117] 第一信息获取请求发送模块26,用于向终端返回所述第二信息获取请求中携带的随机数对应的第一信息获取请求;

[0118] 本地信息接收模块27,用于接收终端通过所述本地应用工具获取的与接收到的所述第一信息获取请求对应的本地信息。

[0119] 存储模块24还用于存储本地信息接收模块27接收的本地信息。

[0120] 第二信息获取请求接收模块25,第一信息获取请求发送模块26和本地信息接收模块27设置于安全通道服务器中。

[0121] 对应于图4所示的装置中的解密模块16,图5所示的装置还包括:加密模块28,用于在所述第一信息获取请求发送模块26向终端返回所述第二信息获取请求中携带的随机数对应的第一信息获取请求之前,对所述第二信息获取请求中携带的随机数对应的第一信息获取请求进行加密处理。

[0122] 参见图6,为本申请实施例提供的一种获取本地信息的系统,包括:

[0123] 终端100,用于通过浏览器101中的脚本向网络设备发送第一信息获取请求,其中,所述第一信息获取请求用于指示本地应用工具获取本地信息;通过所述本地应用工具102监听网络设备返回的所述第一信息获取请求对应的随机数;通过所述本地应用工具获取所述网络设备中保存的所述随机数对应的第一信息获取请求;以及通过所述本地应用工具获取与所述第一信息获取请求对应的本地信息,并将所述本地信息发送给所述网络设备;

[0124] 网络设备200,用于接收所述第一信息获取请求,生成随机数,以及将所述随机数发送给所述终端;该过程可以通过网络设备200中的网关201执行。

[0125] 还用于建立并保存所述随机数与所述第一信息获取请求的对应关系;接收终端通过所述本地应用工具发送的第二信息获取请求;向终端返回所述第二信息获取请求中携带的随机数对应的第一信息获取请求;以及接收所述终端返回的本地信息。该过程可以通过与网关201相连的安全通道服务器202执行。

[0126] 综上所述,本申请实施例基于信息安全的考虑,终端的浏览器不能直接获取其所在的终端的本地信息,而如果浏览器直接调用插件获取本地信息,又要求浏览器与插件具有较高的兼容性。因此,在浏览器不直接获取本地信息这个前提下,本申请终端通过浏览器中的脚本向网络设备发送用于获取本地信息的获取请求,并通过本地应用工具从网络设备中获取该获取请求,再根据该获取请求获取相应的本地信息,最后将该本地信息提供给网络设备。这样,浏览器既不直接获取本地信息,保证了信息安全,又不直接与本地应用工具进行交互,无需与本地应用工具兼容,从而可有效避免浏览器与插件不兼容而导致浏览器不稳定的问题,也可有效降低网站维护的难度。

[0127] 还需要说明的是,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0128] 本领域技术人员应明白,本申请的实施例可提供为方法、系统或计算机程序产品。因此,本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且,本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0129] 以上所述仅为本申请的实施例而已,并不用于限制本申请。对于本领域技术人员来说,本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等,均应包含在本申请的权利要求范围之内。

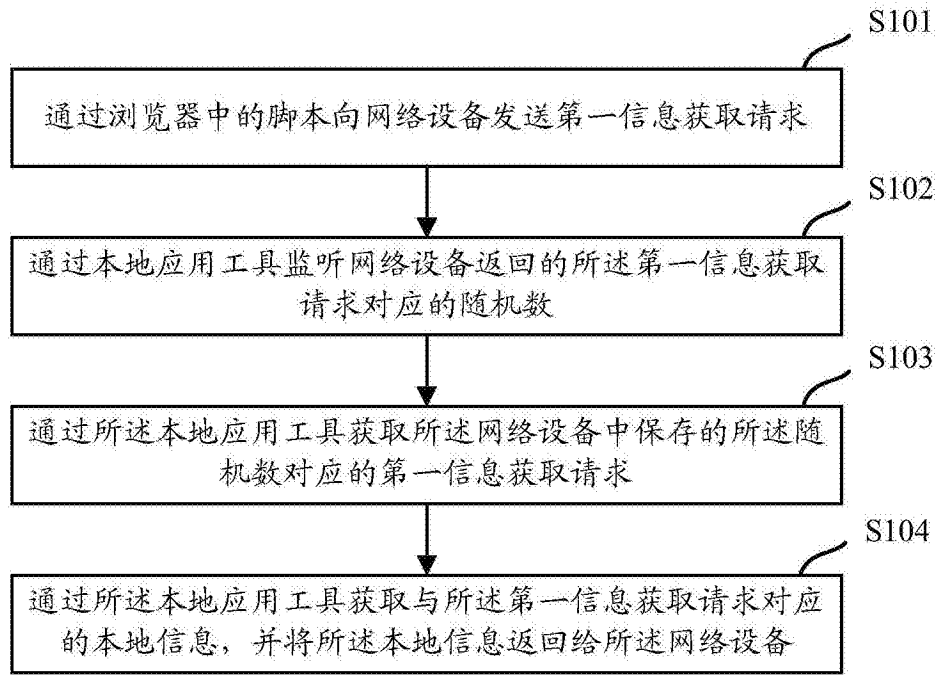


图1

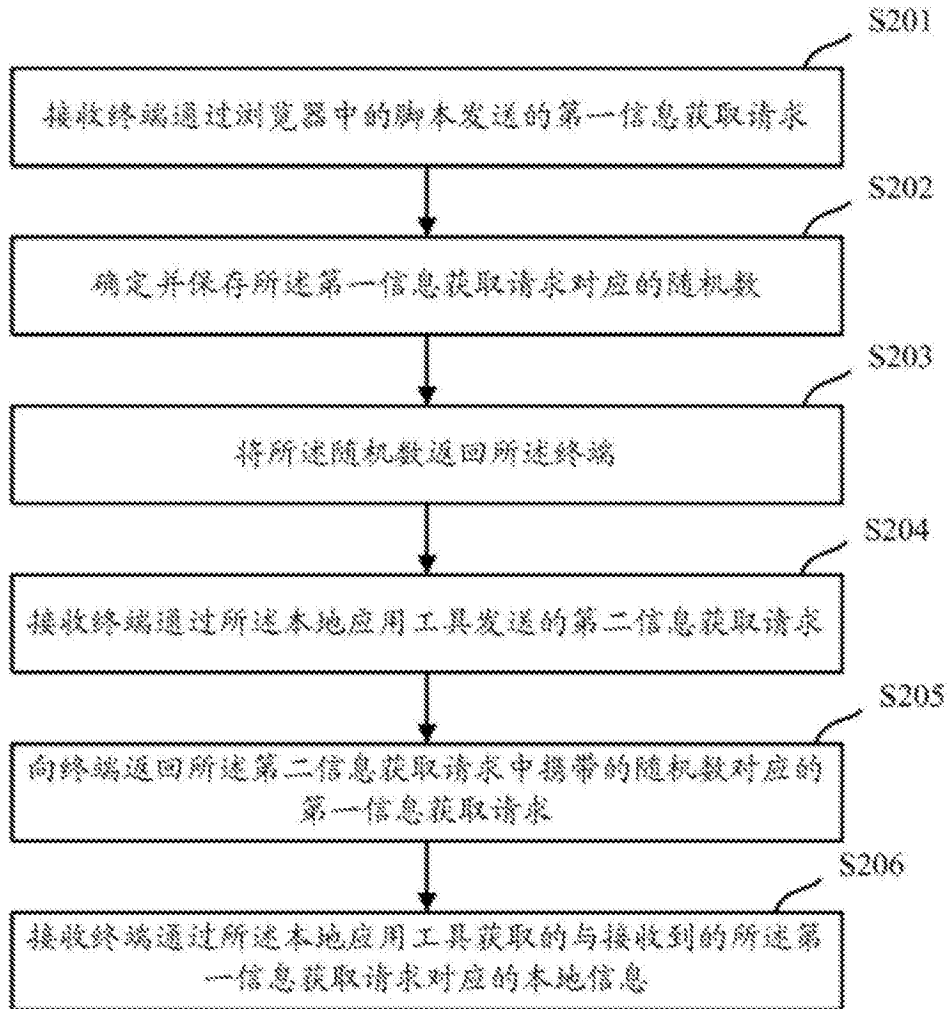


图2

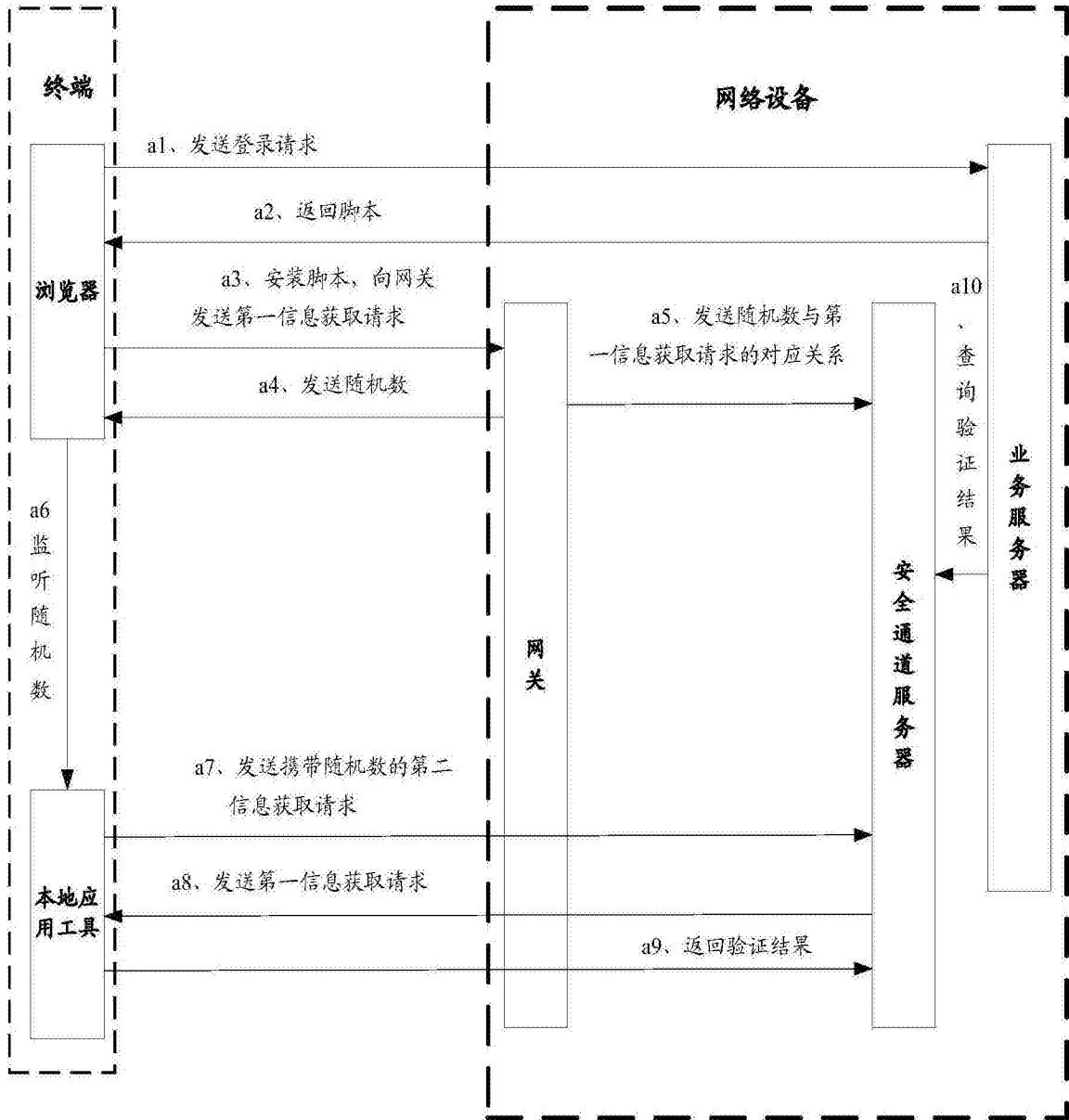


图3



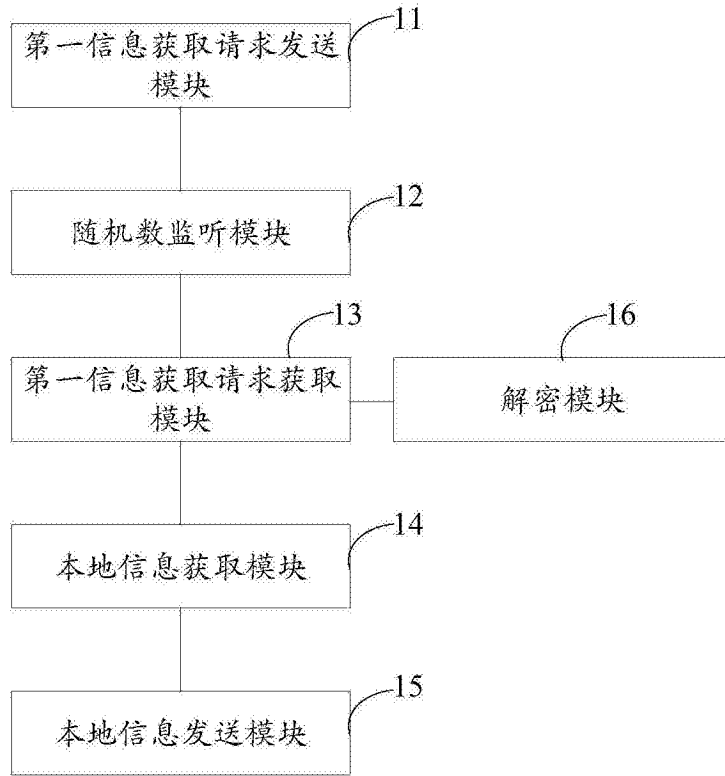


图4

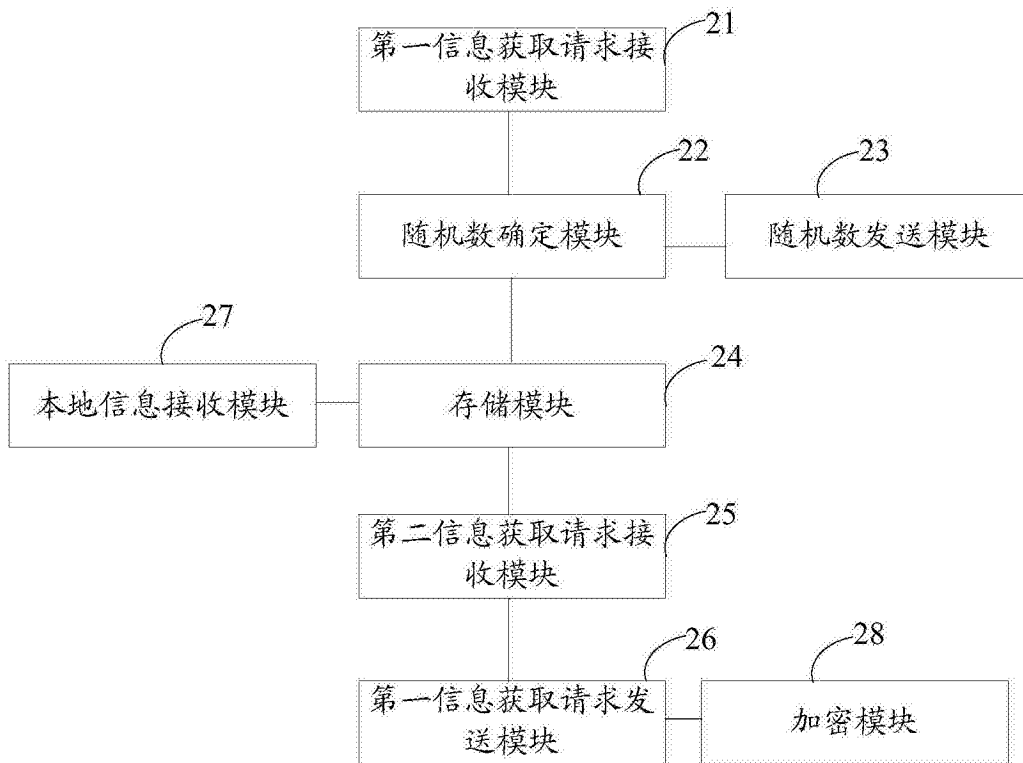


图5

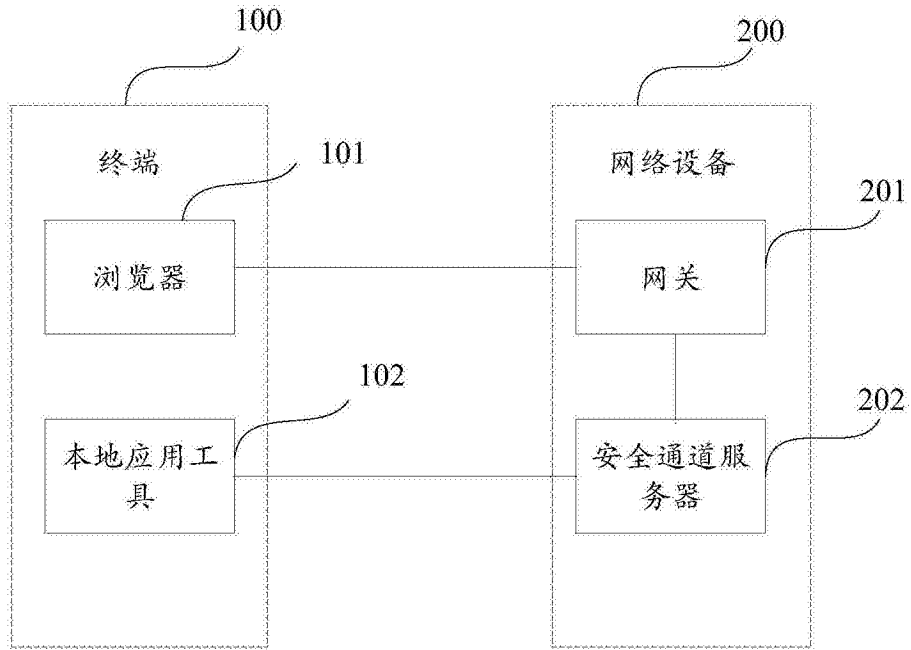


图6