

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2015 年 10 月 22 日 (22.10.2015)



(10) 国际公布号
WO 2015/158228 A1

- (51) 国际专利分类号:
H04L 9/32 (2006.01)
- (21) 国际申请号: PCT/CN2015/076424
- (22) 国际申请日: 2015 年 4 月 13 日 (13.04.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201410149579.8 2014 年 4 月 15 日 (15.04.2014) CN
- (71) 申请人: 中国银联股份有限公司 (CHINA UNION-PAY CO., LTD.) [CN/CN]; 中国上海市浦东新区含笑路 36 号银联大厦, Shanghai 200135 (CN)。
- (72) 发明人: 赵海 (ZHAO, Hai); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。徐燕军 (XU, Yanjun); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。陈芳 (CHEN, Fang); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。周皓 (ZHOU, Hao); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。章明 (ZHANG, Ming); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。周明 (ZHOU, Ming); 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。

(74) 代理人: 中国专利代理 (香港) 有限公司 (CHINA PATENT AGENT (HK) LTD.); 中国香港特别行政区香港湾仔港湾道 23 号鹰君中心 22 字楼, Hong Kong (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告 (条约第 21 条 (3))。

(54) Title: SERVER, USER EQUIPMENT, AND METHOD FOR USER EQUIPMENT TO INTERACT WITH SERVER

(54) 发明名称: 一种服务器、用户设备以及用户设备与服务器的交互方法



图 1 / Fig. 1

AA User equipment
BB Website
CC Server

(57) Abstract: Disclosed are a server capable of sending website authentication information to a user equipment, the user equipment capable of receiving the website authentication information from the server, and a method for the user equipment to interact with the server. At least one or more server public keys and user equipment private keys are stored on the user equipment.

(57) 摘要: 本发明公开能够向用户设备发送网站认证信息的服务器、能够从服务器接收网站认证信息的用户设备、用户设备与服务器的交互方法。用户设备至少存储一个或多个服务器公钥、用户设备私钥。



WO 2015/158228 A1

一种服务器、用户设备以及用户设备与服务器的交互方法

技术领域

[0001] 本发明涉及网络安全，并且尤其涉及服务器、用户设备以及用户设备与服务器的交互方法。

背景技术

[0002] 可以通过在用户端安装防钓鱼的客户端软件或是浏览器插件来鉴别网站真伪。这种方法包括静态鉴别和动态鉴别。静态鉴别通常通过用户举报、网络扫描等在服务器端维护恶意网站黑名单，该方法应用广泛、实施成本低，但由于钓鱼网站不断出现，造成黑名单的覆盖面较窄、更新频率过慢，导致恶意网站漏报率较高。动态鉴别方法建立基于网站域名、图片、页面脚本等的网站行为分析模型，在用户浏览网页时实时地对网站真伪进行鉴别，其较静态的传统方法，鉴别效率有所提升，但由于不断发展的网站伪造技术，动态鉴别方法仍存在误报和漏报，而且由于动态鉴别方法通过软件实现，其容易受到木马等恶意程序的干扰和阻断，可靠性较低。

发明内容

[0003] 提供一种能够向用户设备发送网站认证信息的服务器，该服务器至少存储一个或多个用户设备公钥、服务器私钥，

该服务器被配置成执行如下过程：

经由网站接收用户设备签名、用户设备签名要素，并从该网站接收网站信息，

根据所述网站信息判断该网站是否经过认证，当确定该网站经过认证时，

根据所述用户设备签名要素确定用户设备公钥，并利用所述用户设备公钥验证所述用户设备签名，

当所述验证成功时，使用动态口令加密该网站认证信息，并使用服务器私钥对经加密的网站认证信息签名得到服务器签名，以及将该服务器签名、作为服务器签名要素的经加密的网站认证信息、服务器信息经由该网站发送至该用户设备使得该用户设备能够基于所述服务器信息得到服务器公钥来验证所述服务器签名。

[0004] 提供一种能够从服务器接收网站认证信息的用户设备，该用户设备至少存储一个或多个服务器公钥、用户设备私钥，

该用户设备被配置成执行如下过程：

使用所述用户设备私钥基于用户设备签名要素产生用户设备签名，并将该用户设备签名、该

用户设备签名要素经由网站发送至所述服务器，
经由网站从所述服务器接收该服务器签名、作为服务器签名要素的经加密的网站认证信息、服务器信息，
基于所述服务器信息得到服务器公钥来验证所述服务器签名，
当所述验证成功时，使用动态口令来解密所述经加密的网站认证信息。

[0005] 提供一种用户设备与服务器的交互方法，该服务器至少存储一个或多个用户设备公钥、服务器私钥，

该方法包括：

所述服务器经由网站接收用户设备签名、用户设备签名要素，并从该网站接收网站信息，
所述服务器根据所述网站信息判断该网站是否经过认证，
当确定该网站经过认证时，所述服务器根据所述用户设备签名要素确定用户设备公钥，并利用所述用户设备公钥验证所述用户设备签名，
当所述验证成功时，所述服务器使用动态口令加密该网站认证信息，并使用服务器私钥对经加密的网站认证信息签名得到服务器签名，以及将该服务器签名、作为服务器签名要素的经加密的网站认证信息、服务器信息经由该网站发送至该用户设备使得该用户设备能够基于所述服务器信息得到服务器公钥来验证所述服务器签名。

[0006] 提供一种用户设备与服务器的交互方法，

该用户设备至少存储一个或多个服务器公钥、用户设备私钥，

该方法包括：

该用户设备使用所述用户设备私钥基于用户设备签名要素产生用户设备签名，并将该用户设备签名、该用户设备签名要素经由网站发送至所述服务器，
该用户设备经由网站从所述服务器接收该服务器签名、作为服务器签名要素的经加密的网站认证信息、服务器信息，
该用户设备基于所述服务器信息得到服务器公钥来验证所述服务器签名，
当所述验证成功时，该用户设备使用动态口令来解码所述经加密的网站认证信息。

[0007] 根据实施例的一个场景，网站真伪由统一的服务器进行鉴别，鉴别结果真实可信。

[0008] 根据实施例的一个场景，服务器与用户设备间建立双向认证安全信道，并且返回的鉴别结果通过用户设备显示，鉴别方法安全可靠。

[0009] 根据实施例的一个场景，在不影响用户设备的在线支付体验的同时，能帮助用户判断网站的合法性，而且鉴别过程方便快捷。

[0010] 根据一个或多个实施例，在物理链路上，仅网站可以与后台服务器通信，验证信息通过透传经过安全控件、网站到达用户设备，中间环节无法解密。

[0011] 根据一个或多个实施例，通过用户设备的安全芯片进行解密和显示，可靠性高。

附图说明

[0012] 在参照附图阅读了本发明的具体实施方式以后，本领域技术人员将会更清楚地了解本发明的各个方面。本领域技术人员应当理解的是，这些附图仅仅用于配合具体实施方式说明本发明的技术方案，而并非意在对本发明的保护范围构成限制。

[0013] 图 1 是根据一个实施例的用户设备与服务器的交互架构示意图。

[0014] 图 2 是根据一个实施例的服务器与用户设备的交互示意图。

[0015] 图 3 是根据一个实施例的服务器与用户设备的交互示意图。

[0016] 图 4 是根据一个实施例的鉴别网站的流程图。

具体实施方式

[0017] 下面参照附图，对本发明的具体实施方式作进一步的详细描述。在下面的描述中，为了解释的目的，陈述许多具体细节以便提供对实施例的一个或多个方面的透彻理解。然而，对于本领域技术人员可以显而易见的是，可以这些具体细节的较少程度来实践实施例的一个或多个方面。另外，尽管可以仅关于实施例的一个公开了该实施例的特定特征或方面，但可针对任何给定的或特定的应用所期望和有利的那样，该特征或方面可与其它实施例的一个或多个特征或方面相组合。因此下面的描述不被视为局限性的，而是通过所附权利要求来限定保护范围。

[0018] 图 1 是用户设备与服务器的交互架构示意图。用户设备与服务器的交互经由网站进行。用户设备与服务器的交互可以基于双向验证，从而建立安全通道。可以在用户设备中配置服务器公钥证书、用户设备公私钥对，在服务器中配置用户设备公钥证书、服务器公私钥对用于双向验证。

[0019] 在一个实例中，可以由服务器对用户设备进行管理，在其中预置服务器公钥证书、用户设备公私钥对。

[0020] 在一个实例中，用户设备可以是移动通信装置例如手机，或者个人计算机。

[0021] 在一个实例中，可以在用户设备中装载安全芯片，在安全芯片中设置服务器公钥证书、用户设备公私钥对。安全芯片也可以被设置在能够与用户设备通信的独立硬件设备。

[0022] 用户设备与服务器的交互可以在服务器对网站进行认证的基础上进行。在一个实例中，服务器对通过认证的网站签发站点证书，并维护经认证网站的白名单。

[0023] 以下是服务器认证网站的一个示例性实例：

网站向服务器发起“站点证书”的申请请求，该申请请求包含网站身份信息；

服务器收到请求后，对网站身份信息进行核实，判断是否为合法网站；

若为合法网站，则服务器签发“站点证书”，否则拒绝申请。

[0024] 在一个实例中，经认证的网站可以在其页面上添加该网站支持真伪鉴别的标识。

[0025] 在一个实例中，服务器可以在网站上设置安全控件，用户设备经由该安全控件与服务器交互。

[0026] 图 2 是根据一个实施例的服务器与用户设备的交互示意图。在图 2 中，服务器至少存储一个或多个用户设备公钥、服务器私钥。其中，服务器与用户设备的交互包括服务器被配置成执行如下过程：

经由网站接收用户设备签名、用户设备签名要素，并从网站接收网站信息，

根据网站信息判断网站是否经过认证，

当确定网站经过认证时，根据用户设备签名要素确定用户设备公钥，并利用用户设备公钥验证用户设备签名，

当验证成功时，使用动态口令加密网站认证信息，并使用服务器私钥对经加密的网站认证信息签名得到服务器签名，以及将服务器签名、作为服务器签名要素的经加密的网站认证信息、服务器信息经由网站发送至用户设备使得用户设备能够基于服务器信息得到服务器公钥来验证服务器签名。

[0027] 在一个实例中，用户设备签名要素基于用户设备序列号、用户签名时间戳，服务器被配置成根据用户设备序列号确定用户设备公钥。

[0028] 在一个实例中，网站信息包括用于让服务器判断网站是否经过认证的站点证书，服务器被配置成判断站点证书是否由其签发。

[0029] 可以在用户设备与服务器中分别设置用户设备种子密钥，用于对网站认证信息加解密。由此，在一个实例中，服务器还存储一个或多个用户设备种子密钥，服务器被配置成基于用户设备种子密钥产生动态口令。

[0030] 在一个实例中，该服务器被配置成接收来自一个或多个网站的认证请求，并且在认证通过后向该一个或多个网站发送站点证书，该服务器被配置成通过判断来自该网站的站点证书是否真实来判断该网站是否适于用户设备访问。

[0031] 在一个实例中，服务器被配置成当确定该网站未经过认证时，拒绝与该网站通信。

[0032] 在一个实例中，服务器被配置成当所述验证失败时，提醒网站验证结果。

[0033] 图 3 是根据一个实施例的服务器与用户设备的交互示意图。在图 3 中，用户设备至少存储一个或多个服务器公钥、用户设备私钥，服务器与用户设备的交互包括用户设备被配置成执行如下过程：

使用用户设备私钥基于用户设备签名要素产生用户设备签名，并将用户设备签名、用户设备签名要素经由网站发送至服务器，

经由网站从服务器接收服务器签名、作为服务器签名要素的经加密的网站认证信息、服务器信息，

基于服务器信息得到服务器公钥来验证服务器签名，

当验证成功时，使用动态口令来解码经加密的网站认证信息。

[0034] 在一个实例中，用户设备签名要素基于用户设备序列号、用户签名时间戳，用户设备被配置成根据服务器信息确定服务器公钥。

[0035] 在一个实例中，用户设备还存储用户设备种子密钥，用户设备被配置成基于用户设备种子密钥产生动态口令。

[0036] 在一个实例中，解密的网站认证信息被显示在用户设备上。网站认证信息能够用于提醒用户网站真伪。

[0037] 图 4 是根据一个实施例的鉴别网站的流程图。

[0038] 在 1 中，用户设备用“设备私钥”对设备 SN 号、时间等信息进行签名，并将该数字签名及参与签名的要素经安全控件上送至网站；

在 2 中，网站按照约定的格式要求，组织网站真伪鉴别请求报文，并上送至服务器。该报文中至少应包含设备签名信息、参与签名的要素、“站点证书”；

在 3 中，服务器收到请求报文后，完成报文解析，判断上送的“站点证书”是否有效；

在 4 中，若为有效的“站点证书”，则服务器通过设备 SN 号索引得到对应的“设备公钥”，判断上送的设备签名信息是否有效；否则进入异常处理 A；

在 5 中，若为有效的设备签名信息，则服务器组织并回传网站真伪鉴别应答报文：

（1）通过 SN 号索引得到对应的“设备种子密钥”，计算得到当前的动态口令，并用该动态口令对网站认证信息进行加密，形成“网站真伪凭证”；

（2）用“服务器私钥”对“网站真伪凭证”进行签名；

（3）组成报文并经网站和安全控件回传至用户设备中，应答报文中至少应包含服务器签名信息、参与签名的要素及服务器信息；

否则进入异常处理 B；

在 6 中，用户设备收到应答报文后，完成报文解析，并通过预置的“服务器公钥”判断服务器签名信息是否有效；

在 7 中，若为有效的服务器签名信息，则由预置的“设备种子密钥”计算得到当前的动态口令，对“网站真伪凭证”进行解密，在用户设备上显示网站认证信息；否则进入异常处理 C。

[0039] 异常处理可以例如为：

A-拒绝网站请求；

B-回复网站“非合法的用户设备”；

C-在用户设备上显示“非合法的网站真伪凭证”。

[0040] 上述实施例基于非对称密码体系和动态口令技术，通过设计安全通道而有效地鉴别网站真伪。其有以下这些优势：“网站真伪凭证”可信度高，抗伪造，“网站真伪凭证”由服务器产生，且服务器与用户设备间进行了双向认证，互相之间能识别伪造的用户设备或是后台服务器。“网站真伪凭证”抗篡改，抗重放攻击，“网站真伪凭证”被由动态口令加密形成，能防止攻击者通过开放的互联网环境对其进行篡改，或是截取后的重放攻击。鉴别结果的显示直观且可靠性高，用户设备将鉴别结果给予直观的显示，能有效提示用户当前访问网站的信息，且“网站真伪凭证”的解密与显示均可以在安全芯片中完成，不会被木马等恶意软件劫持或篡改。用户使用门槛低，整个网站真伪的鉴别流程由用户设备、安全控件和服务端配合完成。

权利要求

1. 一种能够向用户设备发送网站认证信息的服务器，其特征在于，
该服务器至少存储一个或多个用户设备公钥、服务器私钥，
该服务器被配置成执行如下过程：
经由网站接收用户设备签名、用户设备签名要素，并从该网站接收网站信息，
根据所述网站信息判断该网站是否经过认证，
当确定该网站经过认证时，根据所述用户设备签名要素确定用户设备公钥，并利用所述用户设备公钥验证所述用户设备签名，
当所述验证成功时，使用动态口令加密该网站认证信息，并使用服务器私钥对经加密的网站认证信息签名得到服务器签名，以及将该服务器签名、作为服务器签名要素的经加密的网站认证信息、服务器信息经由该网站发送至该用户设备使得该用户设备能够基于所述服务器信息得到服务器公钥来验证所述服务器签名。
2. 如权利要求 1 所述的服务器，其特征在于，
所述用户设备签名要素基于用户设备序列号、用户签名时间戳，
所述服务器被配置成根据所述用户设备序列号确定用户设备公钥。
3. 如权利要求 1 所述的服务器，其特征在于，
所述网站信息包括用于让服务器判断该网站是否经过认证的站点证书，
所述服务器被配置成判断该站点证书是否由其签发。
4. 如权利要求 1 所述的服务器，其特征在于，
所述服务器还存储所述一个或多个用户设备种子密钥，
所述服务器被配置成基于所述用户设备种子密钥产生所述动态口令。
5. 一种能够从服务器接收网站认证信息的用户设备，其特征在于，
该用户设备至少存储一个或多个服务器公钥、用户设备私钥，
该用户设备被配置成执行如下过程：
使用所述用户设备私钥基于用户设备签名要素产生用户设备签名，并将该用户设备签名、该用户设备签名要素经由网站发送至所述服务器，

经由网站从所述服务器接收该服务器签名、作为服务器签名要素的经加密的网站认证信息、服务器信息，

基于所述服务器信息得到服务器公钥来验证所述服务器签名，

当所述验证成功时，使用动态口令来解码所述经加密的网站认证信息。

6. 如权利要求 5 所述的用户设备，其特征在于，

所述用户设备签名要素基于用户设备序列号、用户签名时间戳，

所述用户设备被配置成根据所述服务器信息确定服务器公钥。

7. 如权利要求 5 所述的服务器，其特征在于，

所述用户设备还存储用户设备种子密钥，

所述用户设备被配置成基于所述用户设备种子密钥产生所述动态口令。

8. 一种用户设备与服务器的交互方法，其特征在于，

该服务器至少存储一个或多个用户设备公钥、服务器私钥，

该方法包括：

所述服务器经由网站接收用户设备签名、用户设备签名要素，并从该网站接收网站信息，

所述服务器根据所述网站信息判断该网站是否经过认证，

当确定该网站经过认证时，所述服务器根据所述用户设备签名要素确定用户设备公钥，并利用所述用户设备公钥验证所述用户设备签名，

当所述验证成功时，所述服务器使用动态口令加密该网站认证信息，并使用服务器私钥对经加密的网站认证信息签名得到服务器签名，以及将该服务器签名、作为服务器签名要素的经加密的网站认证信息、服务器信息经由该网站发送至该用户设备使得该用户设备能够基于所述服务器信息得到服务器公钥来验证所述服务器签名。

9. 如权利要求 8 所述的方法，其特征在于，

所述用户设备签名要素基于用户设备序列号、用户签名时间戳，

该方法包括：

所述服务器根据所述用户设备序列号确定用户设备公钥。

10. 如权利要求 8 所述的方法，其特征在于，

所述网站信息包括用于让服务器判断该网站是否经过认证的站点证书，

该方法包括：

所述服务器判断该站点证书是否由其签发。

11. 如权利要求 8 所述的方法，其特征在于，

所述服务器还存储所述一个或多个用户设备种子密钥，

该方法包括：

所述服务器基于所述用户设备种子密钥产生所述动态口令。

12. 一种用户设备与服务器的交互方法，其特征在于，

该用户设备至少存储一个或多个服务器公钥、用户设备私钥，

该方法包括：

该用户设备使用所述用户设备私钥基于用户设备签名要素产生用户设备签名，并将该用户设备签名、该用户设备签名要素经由网站发送至所述服务器，

该用户设备经由网站从所述服务器接收该服务器签名、作为服务器签名要素的经加密的网站认证信息、服务器信息，

该用户设备基于所述服务器信息得到服务器公钥来验证所述服务器签名，

当所述验证成功时，该用户设备使用动态口令来解码所述经加密的网站认证信息。

13. 如权利要求 12 所述的方法，其特征在于，

所述用户设备签名要素基于用户设备序列号、用户签名时间戳，

该方法包括：

所述用户设备根据所述服务器信息确定服务器公钥。

14. 如权利要求 12 所述的方法，其特征在于，

所述用户设备还存储用户设备种子密钥，

该方法包括：

所述用户设备基于所述用户设备种子密钥产生所述动态口令。

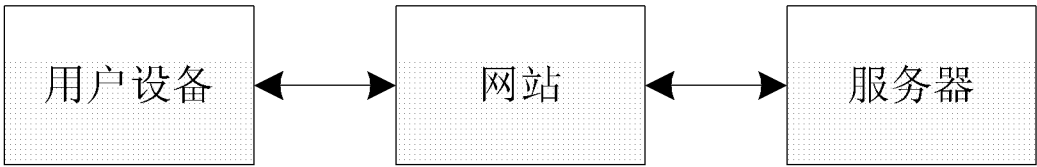


图 1

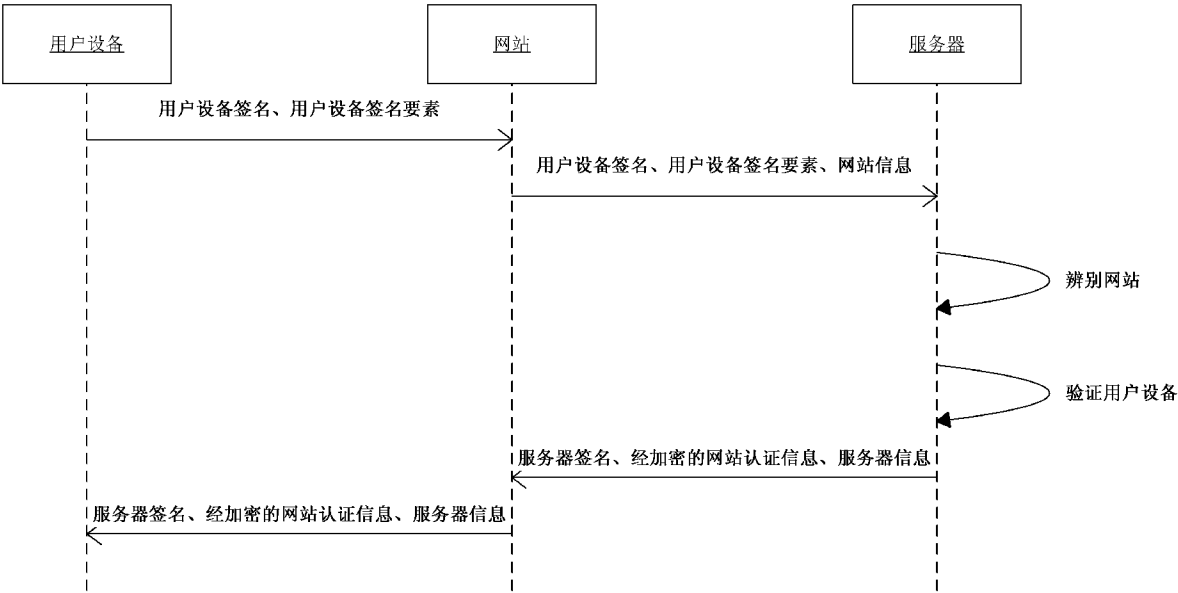


图 2

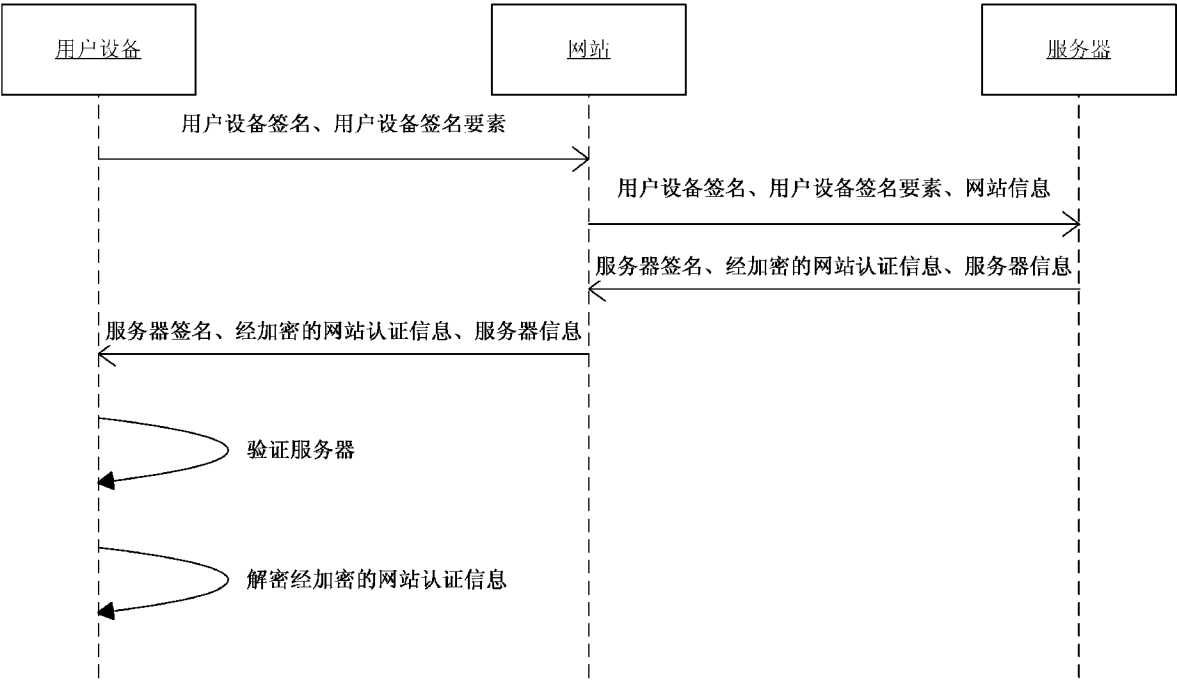


图 3

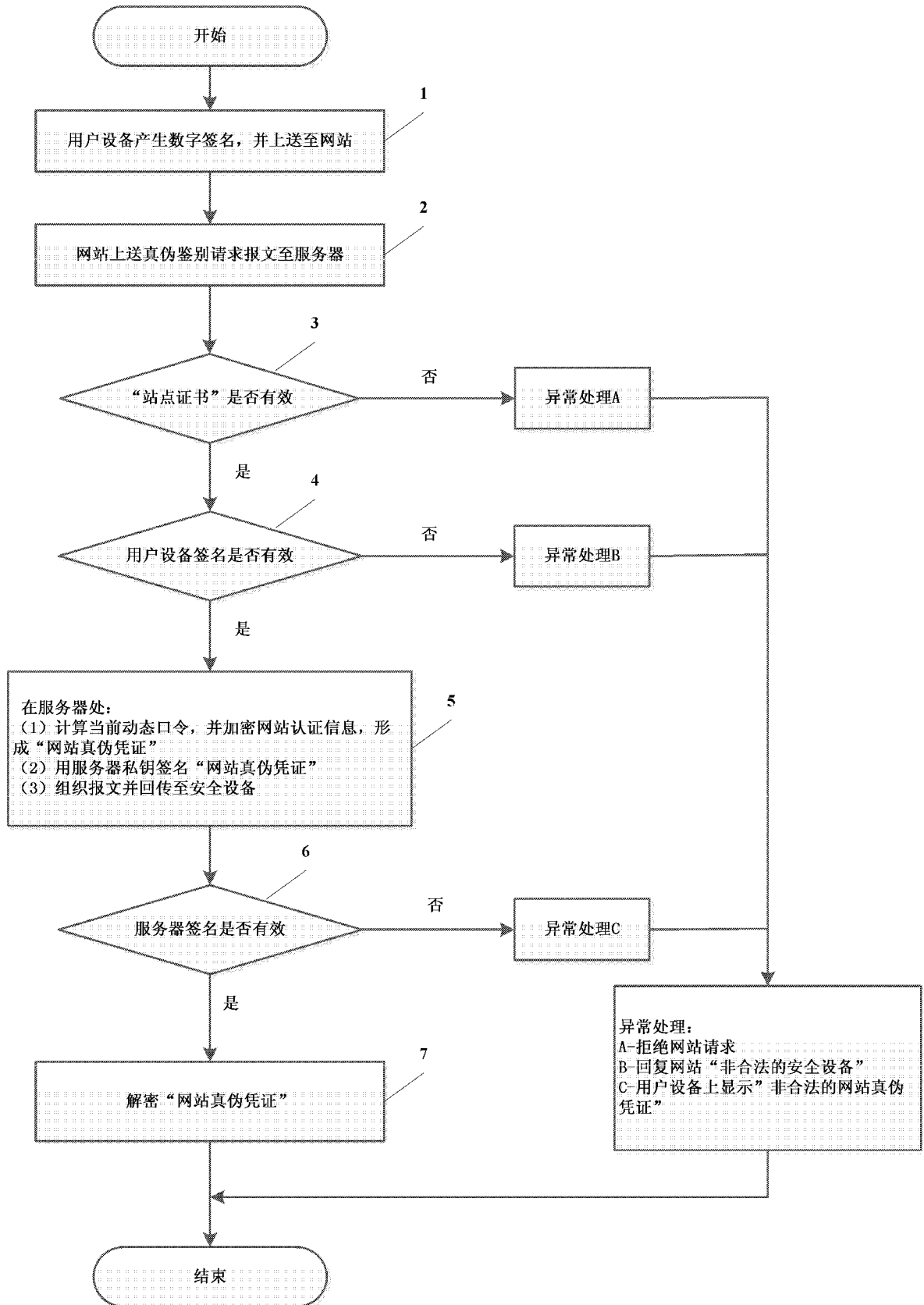


图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/076424

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC: phishing, fraud, web, authenticat+, mutual, third, two way

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 103634307 A (BEIJING QIHOO TECHNOLOGY CO. et al.) 12 March 2014 (12.03.2014) description, paragraphs [0053]-[0083]	1-14
A	CN 102143134 A (HUAWEI TECH CO., LTD.) 03 August 2011 (03.08.2011) the whole document	1-14
A	US 8332627 B1 (CISCO TECHNOLOGY, INC.) 11 December 2012 (11.12.2012) the whole document	1-14

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&” document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 01 July 2015	Date of mailing of the international search report 17 July 2015
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer LIAO, Jiajia Telephone No. (86-10) 62413304

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/076424

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103634307 A	12 March 2014	WO 2015074547 A1	28 May 2015
CN 102143134 A	03 August 2011	None	
US 8332627 B1	11 December 2012	None	

国际检索报告

国际申请号

PCT/CN2015/076424

A. 主题的分类

H04L 9/32 (2006.01) i

按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献 (标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用))

CNPAT, CNKI, WPI, EPODOC: 钓鱼, 伪造, 假冒, 网站, 网页, 认证, 验证, 三方, 双向, phishing, fraud, web, authenticat+, mutual, third, two way

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
A	CN 103634307 A (北京奇虎科技有限公司等) 2014年 3月 12日 (2014 - 03 - 12) 说明书第[0053]-[0083]段	1-14
A	CN 102143134 A (华为技术有限公司) 2011年 8月 3日 (2011 - 08 - 03) 全文	1-14
A	US 8332627 B1 (CISCO TECHNOLOGY, INC.) 2012年 12月 11日 (2012 - 12 - 11) 全文	1-14

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2015年 7月 1日

国际检索报告邮寄日期

2015年 7月 17日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局 (ISA/CN)
北京市海淀区蓟门桥西土城路6号
100088 中国

传真号 (86-10) 62019451

授权官员

廖佳佳

电话号码 (86-10) 62413304

PCT/CN2015/076424

表 PCT/ISA/210 (同族专利附件) (2009年7月)