(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 105553983 B
(45)授权公告日 2017.06.13

(21)申请号 201510956011.1

(22)申请日 2015.12.17

(65)同一申请的已公布的文献号
申请公布号 CN 105553983 A

(43)申请公布日 2016.05.04

(73)专利权人 北京海泰方圆科技股份有限公司
地址 100094 北京市海淀区东北旺西路8号中关村软件园9号楼国际软件大厦E座1-2层

(72)发明人 安晓江 叶家明 柳增寿

(74)专利代理机构 北京华夏正合知识产权代理事务所(普通合伙) 11017
代理人 韩登营 张焕亮

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)

(56)对比文件
CN 104506321 A,2015.04.08,
CN 102148837 A,2011.08.10,
CN 104333555 A,2015.02.04,
CN 103095662 A,2013.05.08,
JP 2012215985 A,2012.11.08,

审查员 吴志彪

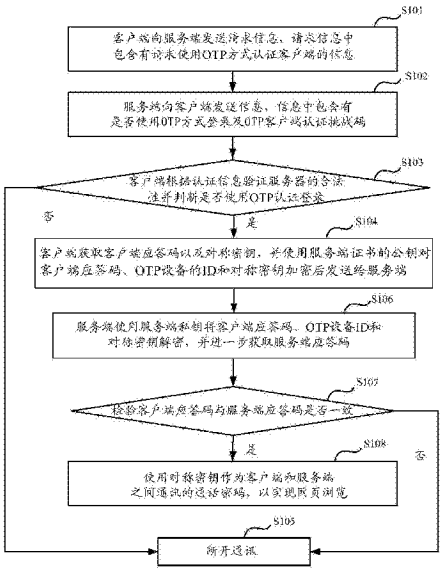
权利要求书1页 说明书4页 附图1页

(54)发明名称

一种网页数据保护方法

(57)摘要

本发明实施例公开了一种网页数据保护方法，所述方法包括：A、客户端浏览器向服务端发送客户端SSL协议的版本号、加密算法的种类、产生的随机数、以及使用OTP方式认证客户端信息的请求；B、服务端根据该请求反馈客户端SSL协议的版本号、加密算法的种类、产生的随机数及OTP客户端认证挑战码OTP客户端认证挑战码；C、客户端浏览器接收挑战码，由OTP设备根据该挑战码生成客户端应答码；并由客户端浏览器发送该客户端应答码和OTP设备的ID；D、服务端根据OTP设备ID确定出所存储的OTP种子，并根据该OTP种子和挑战码生成服务端应答码，据此对客户端应答码进行匹配认证通过后，进行与客户端浏览器网页数据的通讯。由上，本发明实施例规避了USBKey证书颁发的繁琐过程，且不需要直接连接客户端，可跨平台使用，提高了HTTPS的通信效率。



CN 105553983 B

1.一种网页数据保护方法,其特征在于,包括:

A、客户端浏览器向服务端发送客户端SSL协议的版本号、加密算法的种类、产生的随机数、以及使用OTP方式认证客户端信息的请求;

B、服务端根据所述请求反馈客户端SSL协议的版本号、加密算法的种类、产生的随机数及OTP客户端认证挑战码;

C、客户端浏览器接收所述挑战码,由OTP设备根据该挑战码生成客户端应答码;并由客户端浏览器发出该客户端应答码和OTP设备的ID;

D、服务端根据OTP设备ID确定出所存储的OTP种子,并根据该OTP种子和所述挑战码生成服务端应答码,据此对所述客户端应答码进行匹配认证通过后,进行与客户端浏览器网页数据的通讯。

2.根据权利要求1所述的方法,其特征在于,步骤B中还包括:服务端还将向客户端发送服务端证书;

相应的步骤C还包括:客户端还根据所述服务端证书对服务端进行合法性验证。

3.根据权利要求1所述的方法,其特征在于,所述步骤C包括:

客户端浏览器接收所述挑战码并显示,该挑战码被输入到OTP设备,由OTP据此生成客户端应答码,该客户端应答码和OTP设备ID分别被输入浏览器发出。

4.根据权利要求3所述的方法,其特征在于,所述客户端浏览器接收所述挑战码后还包括判断是否可以使用OTP认证登录的步骤。

5.根据权利要求1所述的方法,其特征在于,步骤C还包括:客户端浏览器产生一对称密钥,并发送给服务端;

相应的步骤D所述通讯采用该对称密钥加密通讯。

6.根据权利要求5所述的方法,其特征在于,步骤B还包括:由服务端发送服务端证书的公钥;

相应的,步骤C还包括:由客户端使用所述服务端证书的公钥对所述客户端应答码、OTP设备的ID和所述对称密钥进行加密;

相应的,步骤D还包括:由服务端使用服务端私钥对所述客户端应答码、OTP设备的ID和所述对称密钥进行解密。

一种网页数据保护方法

技术领域

[0001] 本发明涉及网络安全技术领域，特别涉及一种网页数据保护方法。

背景技术

[0002] 网页数据是构成网站的基本元素，是承载各种网站业务的基本形态。一个网页通常由文本数据和图片数据组成，也可以是pdf、word等其他格式的文件。它遵循特定标记语言格式，可以存放在任意一台计算机(服务端)中。网页数据是用户选择的web资源，通常由浏览器向服务端请求，并由浏览器将请求结果呈现出来。网页数据在网络通信传递的常用方法包括：HTTP(超文本传输)、HTTPS单向认证传输、HTTPS双向认证传输。

[0003] HTTP协议使用极为广泛，但却存在安全缺陷。HTTP协议数据为明文传送，同时并未对通信消息做完整性检测，容易遭受网络嗅探，攻击者可从传输过程当中分析出敏感的数据，例如管理员对web程序后台的登录过程等，从而获取网站管理权限。即使无法获取到后台登录信息，对于网页中的手机号码、身份证号码、信用卡卡号等重要资料的获取，也会导致严重的安全事故。

[0004] HTTPS单向认证传输是在网页数据通信过程中认证了服务端证书的合法性，解决了服务端的安全问题，但是并没有认证客户端合法性。在使用网银、政府机关等业务中，服务端无法确认客户端操作人的身份，攻击者可以通过“中间人”来窃取客户信息从而导致信息安全事故。

[0005] HTTPS双向认证传输同时认证了服务端(证书)和客户端(证书)的合法性，从而保证了网页数据在通信过程中不被破解、篡改。

[0006] 但是现有技术中，双向认证需要客户端申请对应服务端的用户证书，且客户端证书通常需要硬件载体(USBKey)来配合使用。硬件证书的使用通常需要安装硬件驱动，且跨平台性较差，使用过程较为繁琐，加大了客户的使用难度，同时由于计算机与硬件设备之间需要进行额外的安全认证，又影响了整个HTTPS的通信效率。

发明内容

[0007] 有鉴于此，本发明的主要目的在于优化现有SSL链路建立过程，使用OTP设备作为HTTPS双向认证，规避了USBKey证书颁发的繁琐过程，同时不影响SSL握手过程计算效率，同时认证设备(OTP)不需要直接连接客户端，可跨平台使用，提高了HTTPS的通信效率。

[0008] 本发明实施例中提供一种网页数据保护方法，包括以下步骤：

[0009] A、客户端浏览器向服务端发送客户端SSL协议的版本号、加密算法的种类、产生的随机数、以及使用OTP方式认证客户端信息的请求；

[0010] B、服务端根据所述请求反馈客户端SSL协议的版本号、加密算法的种类、产生的随机数及OTP客户端认证挑战码；

[0011] C、客户端浏览器接收所述挑战码，由OTP设备根据该挑战码生成客户端应答码；并由客户端浏览器发出该客户端应答码和OTP设备的ID；

[0012] D、服务端根据OTP设备ID确定出所存储的OTP种子，并根据该OTP种子和所述挑战码生成服务端应答码，据此对所述客户端应答码进行匹配认证通过后，进行与客户端浏览器网页数据的通讯。

[0013] 由上，使用OTP设备作为HTTPS双向认证，规避了USBKey证书颁发的繁琐过程，同时不影响SSL握手过程计算效率，且不需要直接连接客户端，可跨平台使用，提高了HTTPS的通信效率。

[0014] 优选地，步骤B中还包括：服务端还将向客户端发送服务端证书；

[0015] 相应的步骤C还包括：客户端还根据所述服务端证书对服务端进行合法性验证。

[0016] 由上，客户端根据服务端证书对服务端进行合法性验证，从而保证通信的安全性。

[0017] 优选地，所述步骤C包括：

[0018] 客户端浏览器接收所述挑战码并显示，该挑战码被输入到OTP设备，由OTP据此生成客户端应答码，该客户端应答码和OTP设备ID分别被输入浏览器发出。

[0019] 由上，通过OTP设备获取客户端应答码，用于后续与服务端应答码进行一致性对比。

[0020] 优选地，所述客户端浏览器接收所述挑战码后还包括判断是否可以使用OTP认证登录的步骤。

[0021] 优选地，步骤C还包括：客户端浏览器产生一对称密钥，并发送给服务端；

[0022] 相应的步骤D所述通讯采用该对称密钥加密通讯。

[0023] 由上，通过对称密钥加密通讯，提高通讯的安全性。

[0024] 优选地，步骤B还包括：由服务端发送服务端证书的公钥；

[0025] 相应的，步骤C还包括：由客户端使用所述服务端证书的公钥对所述客户端应答码和OTP设备的ID和所述对称密钥加密；

[0026] 相应的，步骤D还包括：由服务端使用服务端私钥对所述客户端应答码和OTP设备的ID和所述对称密钥进行解密。

[0027] 由上，通过公钥加密以及私钥解密，提高通讯的安全性。

[0028] 由上可以看出，本发明实施例通过使用OTP设备作为HTTPS双向认证，规避了USBKey证书颁发的繁琐过程，同时不影响SSL握手过程计算效率，且不需要直接连接客户端，可跨平台使用，提高了HTTPS的通信效率。

附图说明

[0029] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0030] 图1为本发明实施例提供的一种网页数据保护方法流程示意图。

具体实施方式

[0031] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是

本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0032] 为克服现有技术中的缺陷，本申请提供一种网页数据保护方法，使用OTP设备作为HTTPS双向认证，规避了USBKey证书颁发的繁琐过程，同时不影响SSL握手过程计算效率，且不需要直接连接客户端，可跨平台使用，提高了HTTPS的通信效率。

[0033] 如图1所示，为本发明实施例中的提出的一种网页数据保护方法的流程示意图，所述方法应用于包括客户端和服务端的系统中，所述客户端拥有已在服务端备案并激活的动态口令OTP设备，所述方法包括以下步骤：

[0034] S101，客户端的浏览器向服务端传送客户端SSL协议的版本号，加密算法的种类，产生的随机数，及其他服务端和客户端之间通讯所需要的各种信息，同时在扩展信息中添加请求使用OTP方式认证客户端信息。

[0035] S102，服务端向客户端传送SSL协议的版本号，加密算法的种类，随机数以及其他相关信息，同时服务端还将向客户端传送自己的证书及OTP扩展信息，扩展信息包括：是否可以使用OTP方式登录及OTP客户端认证挑战码。

[0036] S103，客户端利用服务端传送过来的信息验证服务端的合法性以及判断是否使用OTP认证登录，若所述服务端合法且判断结果为使用OTP方式登录，则执行S104，反之，则执行S105。

[0037] 在一个具体的实现过程中，客户端利用服务端发送过来的信息验证服务端的合法性，服务端的合法性包括：证书是否过期，发行服务端证书的CA是否可靠，发行者证书的公钥能否正确解开服务端证书的“发行者的数字签名”，服务端证书上的域名是否和服务端的实际域名相匹配。同时判断是否可以使用OTP认证登录，若合法性验证通过且可以使用OTP认证，则继续进行下一步，若合法性验证没有通过或者不可以使用OTP认证登录，通讯将断开。

[0038] S104，客户端浏览器显示服务端发送的挑战码，挑战码被用于输入到所述OTP设备以得到客户端应答码；

[0039] 客户端应答码和OTP设备ID被用于输入浏览器输入框，以产生客户端和服务端之间通讯的对称密钥；

[0040] 客户端使用从服务端发送的认证信息中获得的服务端证书的公钥将所述OTP设备ID、客户端应答码和对称密钥分别加密后发送给服务端；其中，OTP设备ID也可以用帐号来替代。

[0041] S105，断开通讯。

[0042] S106，服务端使用服务端的私钥将OTP设备ID、客户端应答码和对称密钥解密，并根据OTP设备ID在服务端数据库中取出对应OTP种子，用种子和挑战码并根据OTP专有算法接口运算得出服务端应答码，此处的公钥和私钥是相互关联的，公钥加密的数据只能用私钥解密，私钥只在服务端保留。

[0043] S107，检验客户端应答码和服务端应答码的一致性，若一致，则执行S108，反之，则执行S105。

[0044] S108，使用对称密钥作为客户端和服务端之间的通讯的通话密码，以实现网页浏览。

[0045] 在一个具体的实现过程中，所述使用对称密钥作为客户端和服务端之间的通讯的通话密码，包括：使用对称密钥对客户端和服务端之间的通讯进行加密或解密。

[0046] 同时还需要保证数据通讯的完整性，防止数据通讯中的任何变化。客户端向服务端发出信息，指明后面的数据通讯将使用对称密钥作为通话密码，同时通知服务端客户端的握手过程结束。服务端向客户端发出信息，指明后面的数据通讯将使用对称密钥作为通话密码，同时通知客户端服务端的握手过程结束。握手部分结束，安全通道的数据通讯开始，客户和服务端开始使用相同的对称密钥进行数据通讯，同时进行通讯完整性的检验。

[0047] 综上所述，与现有技术相比，本发明实施例使用OTP设备作为HTTPS双向认证，规避了USBKey证书颁发的繁琐过程，同时不影响SSL握手过程计算效率，且不需要直接连接客户端，可跨平台使用，提高了HTTPS的通信效率。

[0048] 本发明实施例中的服务端为服务器，其他能够实现本发明技术效果的服务端也同样适用。

[0049] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

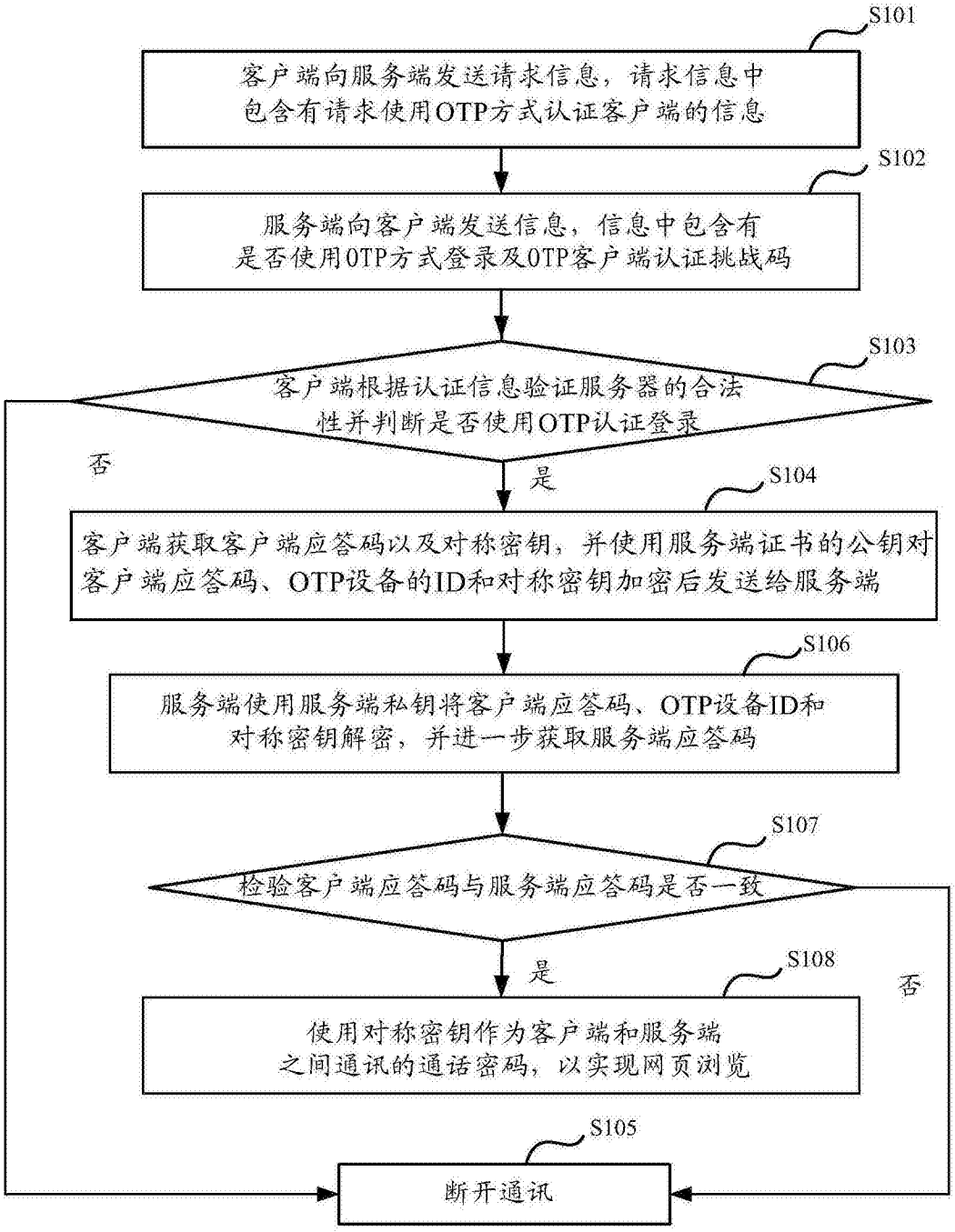

S101
客户端向服务端发送请求信息，请求信息中包含有请求使用OTP方式认证客户端的信息
S102
服务端向客户端发送信息，信息中包含有是否使用OTP方式登录及OTP客户端认证挑战码
S103
客户端根据认证信息验证服务器的合法性并判断是否使用OTP认证登录
否
是
S104
客户端获取客户端应答码以及对称密钥，并使用服务端证书的公钥对客户端应答码、OTP设备的ID和对称密钥加密后发送给服务端
S106
服务端使用服务端私钥将客户端应答码、OTP设备ID和对称密钥解密，并进一步获取服务端应答码
S107
检验客户端应答码与服务端应答码是否一致
是
否
S108
使用对称密钥作为客户端和服务端之间通讯的通话密码，以实现网页浏览
S105
断开通讯

图1