(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110830465 B
(45)授权公告日 2022.11.25

(21)申请号 201911059619.9

(22)申请日 2019.11.01

(65)同一申请的已公布的文献号
申请公布号 CN 110830465 A

(43)申请公布日 2020.02.21

(73)专利权人 大唐微电子技术有限公司
地址 100094 北京市海淀区永嘉北路6号

(72)发明人 母智弘 王小文 刘立黎 尚微

(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
专利代理师 凌齐文 龙洪

(51)Int.Cl.
H04L 9/40(2022.01)

(56)对比文件
CN 107566407 A,2018.01.09
CN 109728909 A,2019.05.07

审查员 张玉

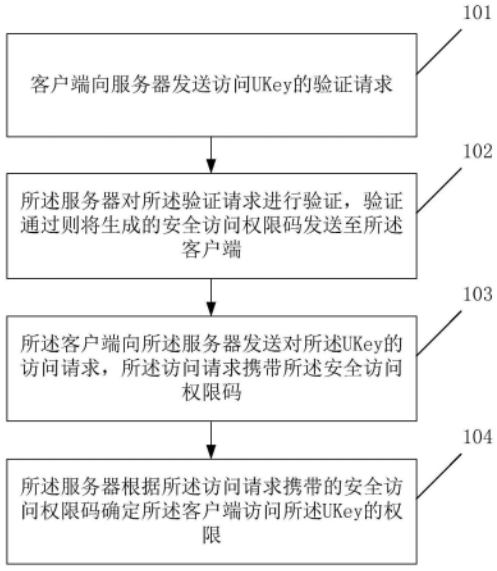
权利要求书2页 说明书9页 附图2页

(54)发明名称

一种访问UKey的安全防护方法、服务器和客户端

(57)摘要

一种访问UKey的安全防护方法、服务器和客户端，所述方法包括：服务器接收客户端发送的访问UKey的验证请求，验证通过则将生成的安全访问权限码发送至所述客户端；所述服务器接收所述客户端对所述UKey的访问请求，根据所述访问请求携带的安全访问权限码确定所述客户端访问所述UKey的权限。本申请实施例通过采用安全访问权限码，避免了安全隐患，保障了对UKey资源访问的安全性。



CN 110830465 B

1.一种访问智能密码钥匙UKey的安全防护方法,其特征在于,包括:

服务器接收客户端发送的访问UKey的验证请求,验证通过则将生成的安全访问权限码发送至所述客户端;

所述服务器接收所述客户端对所述UKey的访问请求,根据所述访问请求携带的安全访问权限码确定所述客户端访问所述UKey的权限;

所述方法还包括:

所述服务器根据所述访问请求携带的访问递增序列码确定所述访问请求是否为恶意攻击;其中,所述访问递增序列码是所述客户端根据本地的时间戳确定的;

所述服务器根据所述访问请求携带的访问递增序列码确定所述访问请求是否为恶意攻击,包括:

在所述服务器本地保存有访问递增序列码时,所述服务器将所述访问请求携带的访问递增序列码与本地保存的访问递增序列码进行比对,若所述访问请求携带的访问递增序列码小于等于本地保存的访问递增序列码,则确定访问请求为恶意攻击;若所述访问请求携带的访问递增序列码大于本地保存的访问递增序列码,则确定所述访问请求为正常请求,根据所述访问请求携带的访问递增序列码更新本地保存的访问递增序列码。

2.根据权利要求1所述的方法,其特征在于,所述根据所述访问请求携带的安全访问权限码确定所述客户端访问所述UKey的权限,包括:

所述服务器比较本地保存的安全访问权限码与所述访问请求携带的安全访问权限码是否一致,若一致则确定所述客户端具有访问所述UKey的权限,若不一致则确定所述客户端没有访问所述UKey的权限。

3.根据权利要求1或2所述的方法,其特征在于,

所述安全访问权限码为所述服务器生成的16字节随机数。

4.一种访问UKey的安全防护方法,其特征在于,包括:

客户端向服务器发送访问UKey的验证请求,接收所述服务器发送的安全访问权限码;

所述客户端向所述服务器发送对所述UKey的访问请求,所述访问请求携带所述安全访问权限码,以使所述服务器根据所述安全访问权限码确定所述客户端访问所述UKey的权限;

所述方法还包括:

所述客户端向所述服务器发送对所述UKey的访问请求时,所述访问请求还携带访问递增序列码,以使所述服务器根据所述访问递增序列码确定所述访问请求是否为恶意攻击;

所述方法还包括:

所述客户端根据本地的时间戳确定所述访问递增序列码;

确定所述访问请求是否为恶意攻击,包括:

在所述服务器本地保存有访问递增序列码时,所述服务器将所述访问请求携带的访问递增序列码与本地保存的访问递增序列码进行比对,若所述访问请求携带的访问递增序列码小于等于本地保存的访问递增序列码,则确定访问请求为恶意攻击;若所述访问请求携带的访问递增序列码大于本地保存的访问递增序列码,则确定所述访问请求为正常请求,根据所述访问请求携带的访问递增序列码更新本地保存的访问递增序列码。

5.一种服务器,包括:存储器、处理器及存储在存储器上并可在处理器上运行的计算机

程序,其特征在于,所述处理器执行所述程序时实现如权利要求1～3中任意一项所述的方法。

6.一种客户端,包括:存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,其特征在于,所述处理器执行所述程序时实现如权利要求4所述的方法。

一种访问UKey的安全防护方法、服务器和客户端

技术领域

[0001] 本文涉及信息安全领域，尤指一种访问UKey的安全防护方法、服务器和客户端。

背景技术

[0002] 综合安全管理平台是按照国密局的相关规范，为公共安全视频监控联网信息安全系统涉及到的设备(包括前端设备、业务平台、信令控制服务器、媒体服务器、路由网关)提供数字证书的签发、更新、注销及用户身份认证、授权及访问控制以及信令及音视频数据加解密的综合安全支撑平台，满足信息的保密性、完整性、可靠性和抗抵赖性等安全性要求。在综合安全管理平台中，需要使用UKey(UsbKey，智能密码钥匙)存储用户信息、用户证书和秘钥对等数据，并提供符合国密/国际标准的加解密和签名验签等秘钥算法接口。

[0003] 当前使用浏览器访问本地UKey有两种模式。

[0004] 第一种是浏览器插件模式，该模式需要兼容不同的浏览器(如微软IE浏览器、谷歌浏览器、火狐浏览器、苹果Safari浏览器等)，并且还要再随着浏览器的升级对插件不断进行升级。这种模式的开发耗时耗力，并且维护工作量很大。

[0005] 第二种模式是基于WSS(WebSocket Security，WebSocket安全)/HTTPS(Hyper Text Transfer Protocol over SecureSocket Layer，超文本传输安全协议)协议的B/S(客户机/服务器)模式，即浏览器作为客户端，通过WSS/HTTPS协议来访问本地WebSocket/HTTP服务器，服务器对Ukey进行操作，并将对UKey的操作结果打包返回给客户端(即浏览器)，完成对客户端的请求进行响应。基于WSS/HTTPS的数据传输，是使用SSL(Secure Socket Layer，安全套接字层协议)或TLS(Transport Layer Security，传输层安全协议)进行传输，上述两种协议都是基于TCP(Transmission Control Protocol，传输控制协议)来提供一种安全可靠的端到端服务，且使用加密技术使得数据以密文形式在网络中进行传输，确保整个传输过程中数据不被监听和篡改，保证了数据的机密性和完整性。

[0006] 将上述两种UKey访问模式进行比较，第二种模式兼容性更好，后期维护量更小，但它还存在着严重不足。

[0007] UKey在使用中有如下操作特点：UKey会要求外部访问提供PIN(Personal identification number，个人身份识别码)码或指纹，然后利用PIN码或指纹进行校验，一旦校验成功则不会再对后续操作请求进行校验或检测。因此，恶意访问者会利用这一特性，在UKey已经对PIN码或指纹校验成功后，通过任意未拥有正确PIN码或指纹的客户端，申请对UKey进行其权限允许范围内的操作(如：加解密、签名验签、证书的导入导出等)，此时，UKey对操作请求不再做任何权限检测，因此这些操作请求都能被UKey成功响应，所以存在严重的安全隐患。

发明内容

[0008] 本申请提供了一种访问UKey的安全防护方法、服务器和客户端，以保障UKey资源的安全性。

[0009] 本申请实施例提供了一种访问UKey的安全防护方法,包括:

[0010] 服务器接收客户端发送的访问UKey的验证请求,验证通过则将生成的安全访问权限码发送至所述客户端;

[0011] 所述服务器接收所述客户端对所述UKey的访问请求,根据所述访问请求携带的安全访问权限码确定所述客户端访问所述UKey的权限。

[0012] 在一实施例中,所述根据所述访问请求携带的安全访问权限码确定所述客户端访问所述UKey的权限,包括:

[0013] 所述服务器比较本地保存的安全访问权限码与所述访问请求携带的安全访问权限码是否一致,若一致则确定所述客户端具有访问所述UKey的权限,若不一致则确定所述客户端没有访问所述UKey的权限。

[0014] 在一实施例中,所述安全访问权限码为所述服务器生成的16字节随机数。

[0015] 在一实施例中,所述方法还包括:

[0016] 所述服务器根据所述访问请求携带的访问递增序列码确定所述访问请求是否为恶意攻击。

[0017] 在一实施例中,所述服务器根据所述访问请求携带的访问递增序列码确定所述访问请求是否为恶意攻击,包括:

[0018] 在所述服务器本地保存有访问递增序列码时,所述服务器将所述访问请求携带的访问递增序列码与本地保存的访问递增序列码进行比对,若所述访问请求携带的访问递增序列码小于等于本地保存的访问递增序列码,则确定访问请求为恶意攻击;若所述访问请求携带的访问递增序列码大于本地保存的访问递增序列码,则确定所述访问请求为正常请求,根据所述访问请求携带的访问递增序列码更新本地保存的访问递增序列码。

[0019] 本申请实施例还提供一种访问UKey的安全防护方法,包括:

[0020] 客户端向服务器发送访问UKey的验证请求,接收所述服务器发送的安全访问权限码;

[0021] 所述客户端向所述服务器发送对所述UKey的访问请求,所述访问请求携带所述安全访问权限码,以使所述服务器根据所述安全访问权限码确定所述客户端访问所述UKey的权限。

[0022] 在一实施例中,所述方法还包括:

[0023] 所述客户端向所述服务器发送对所述UKey的访问请求时,所述访问请求还携带访问递增序列码,以使所述服务器根据所述访问递增序列码确定所述访问请求是否为恶意攻击。

[0024] 在一实施例中,所述方法还包括:

[0025] 所述客户端根据本地的时间戳确定所述访问递增序列码。

[0026] 本申请实施例还提供一种服务器,包括:存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,所述处理器执行所述程序时实现所述访问UKey的安全防护方法。

[0027] 本申请实施例还提供一种客户端,包括:存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,所述处理器执行所述程序时实现所述访问UKey的安全防护方法。

[0028] 本申请实施例还提供一种计算机可读存储介质，存储有计算机可执行指令，所述计算机可执行指令用于执行所述访问UKey的安全防护方法。

[0029] 与相关技术相比，本申请包括：服务器接收客户端发送的访问UKey的验证请求，验证通过则将生成的安全访问权限码发送至所述客户端；所述服务器接收所述客户端对所述UKey的访问请求，根据所述访问请求携带的安全访问权限码确定所述客户端访问所述UKey的权限。本申请实施例通过采用安全访问权限码，避免了安全隐患，保障了对UKey资源访问的安全性。

[0030] 在一示例性的实施例中，本申请实施例还通过采用访问递增序列码，有效阻挡了对UKey的无效访问或恶意破坏。

[0031] 本申请的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本申请而了解。本申请的其他优点可通过在说明书、权利要求书以及附图中所描述的方案来实现和获得。

附图说明

[0032] 附图用来提供对本申请技术方案的理解，并且构成说明书的一部分，与本申请的实施例一起用于解释本申请的技术方案，并不构成对本申请技术方案的限制。

[0033] 图1为本申请实施例的访问UKey的安全防护方法的流程图；

[0034] 图2为本申请实施例的访问UKey的安全防护方法的流程图(应用于服务器)；

[0035] 图3为本申请实施例的访问UKey的安全防护方法的流程图(应用于客户端)；

[0036] 图4为本申请实施例的访问UKey的安全防护装置(应用于服务器)；

[0037] 图5为本申请实施例的访问UKey的安全防护装置(应用于客户端)。

具体实施方式

[0038] 本申请描述了多个实施例，但是该描述是示例性的，而不是限制性的，并且对于本领域的普通技术人员来说显而易见的是，在本申请所描述的实施例包含的范围内可以有更多的实施例和实现方案。尽管在附图中示出了许多可能的特征组合，并在具体实施方式中进行了讨论，但是所公开的特征的许多其它组合方式也是可能的。除非特意加以限制的情况以外，任何实施例的任何特征或元件可以与任何其它实施例中的任何其他特征或元件结合使用，或可以替代任何其它实施例中的任何其他特征或元件。

[0039] 本申请包括并设想了与本领域普通技术人员已知的特征和元件的组合。本申请已经公开的实施例、特征和元件也可以与任何常规特征或元件组合，以形成由权利要求限定的独特的发明方案。任何实施例的任何特征或元件也可以与来自其它发明方案的特征或元件组合，以形成另一个由权利要求限定的独特的发明方案。因此，应当理解，在本申请中示出和/或讨论的任何特征可以单独地或以任何适当的组合来实现。因此，除了根据所附权利要求及其等同替换所做的限制以外，实施例不受其它限制。此外，可以在所附权利要求的保护范围内进行各种修改和改变。

[0040] 此外，在描述具有代表性的实施例时，说明书可能已经将方法和/或过程呈现为特定的步骤序列。然而，在该方法或过程不依赖于本文所述步骤的特定顺序的程度上，该方法或过程不应限于所述的特定顺序的步骤。如本领域普通技术人员将理解的，其它的步骤顺

序也是可能的。因此，说明书中阐述的步骤的特定顺序不应被解释为对权利要求的限制。此外，针对该方法和/或过程的权利要求不应限于按照所写顺序执行它们的步骤，本领域技术人员可以容易地理解，这些顺序可以变化，并且仍然保持在本申请实施例的精神和范围内。

[0041] 使用基于WSS/HTTPS的B/S模式访问本地UKey资源时，虽然可以保证数据在传输过程中的机密性和完整性，但是没有解决UKey资源对外部访问的安全权限控制，也无法防护UKey可能受到来自外部的攻击性访问，具体包括如下两种情况：

[0042] 1、不能分辨客户端的请求有无访问权限。比如某客户端(如浏览器A)首先请求UKey进行PIN码或指纹校验，在校验成功后，如果新客户端(如浏览器B)对该UKey提出操作请求，或浏览器A退出后又打开，并对该UKey提出操作请求，或浏览器A新开一个页面对该UKey发起操作请求，在上述几种情况下，UKey都会成功响应请求，进行相应操作。这样就不能保证所有外部对UKey的操作都是拥有该UKey硬件及其PIN码或指纹的用户的真实使用。

[0043] 2、基于WSS/HTTPS协议的数据传输模式能够保证数据在整个传输过程中不被篡改和监听，可以保证数据的机密性和完整性，但是对于恶意攻击者来说，这种保护并不完善。攻击者往往不需要窥探数据信息或者篡改数据内容，只要将客户端发往服务器的数据截取下来，并持续不断地将该数据原样发往服务器，就可能破坏UKey中的用户数据或占用UKey的运行资源，使得服务器对拥有该UKey硬件及其PIN码或指纹的用户的真实请求的响应变慢甚至变得无响应，从而达到恶意攻击的目的。

[0044] 本申请实施例中，提出了对UKey访问的组合式安全防护模式，即基于WSS/HTTPS协议的B/S模式，利用安全访问权限码和访问递增序列码组合进行安全防护。

[0045] 如图1所示，本申请实施例的访问UKey的安全防护方法，包括：

[0046] 步骤101，客户端向服务器发送访问UKey的验证请求。

[0047] 其中，验证请求可以是PIN码或指纹校验的请求。

[0048] 步骤102，所述服务器对所述验证请求进行验证，验证通过则将生成的安全访问权限码发送至所述客户端。

[0049] 其中，服务器调用本地UKey的对应接口进行校验；如果校验成功，服务器产生一个安全访问权限码并保存，同时返回给发起请求的客户端。

[0050] 在一实施例中，安全访问权限码为16字节随机数。

[0051] 步骤103，所述客户端向所述服务器发送对所述UKey的访问请求，所述访问请求携带所述安全访问权限码。

[0052] 所述客户端接收并保存所述安全访问权限码，所述客户端后续对UKey进行操作时都需要向服务器发送所述安全访问权限码。

[0053] 步骤104，所述服务器根据所述访问请求携带的安全访问权限码确定所述客户端访问所述UKey的权限。

[0054] 所述服务器将本地保存的安全访问权限码和来自客户端的安全访问权限码进行比对，来判断发起请求的客户端是否有权访问UKey资源。

[0055] 在一实施例中，所述服务器比较本地保存的安全访问权限码与所述访问请求携带的安全访问权限码是否一致，若一致则确定所述客户端具有访问所述UKey的权限，若不一致则确定所述客户端没有访问所述UKey的权限。

[0056] 若确定所述客户端具有访问所述UKey的权限，则继续执行该客户端对UKey的访问

请求,若确定所述客户端没有访问所述UKey的权限,则服务器则中断客户端对UKey的访问请求并返回异常。

[0057] 在一实施例中,所述方法还包括:

[0058] 所述客户端向所述服务器发送对所述UKey的访问请求时,所述访问请求还携带访问递增序列码,所述服务器根据所述访问请求携带的访问递增序列码确定所述访问请求是否为恶意攻击。

[0059] 其中,客户端每次向服务器发起UKey请求时,同时发送一个访问递增序列码;服务器收到客户端请求并获取其中的访问递增序列码,再与服务器本地保存的上一次成功请求的访问递增序列码进行比对,来判断当前的客户端请求是否为恶意攻击包。

[0060] 在一实施例中,所述客户端根据本地的时间戳确定所述访问递增序列码。

[0061] 所述时间戳的精度可以是10ns。

[0062] 在一实施例中,在所述服务器本地保存有访问递增序列码时,所述服务器将所述访问请求携带的访问递增序列码与本地保存的访问递增序列码进行比对,若所述访问请求携带的访问递增序列码小于等于本地保存的访问递增序列码,则确定访问请求为恶意攻击;若所述访问请求携带的访问递增序列码大于本地保存的访问递增序列码,则确定所述访问请求为正常请求,根据所述访问请求携带的访问递增序列码更新本地保存的访问递增序列码。

[0063] 在所述服务器本地没有保存有访问递增序列码时,在所述服务器按照所述安全访问权限码确定所述客户端具有访问所述UKey的权限时,将所述访问请求中携带的访问递增序列码保存在本地。

[0064] 如果服务器确定访问请求为恶意攻击时,则中断本次客户端请求操作并返回异常。

[0065] 本申请实施例通过采用安全访问权限码,避免了安全隐患,可有效防范无访问权限码的客户请求,保障了对UKey资源访问的安全性。而且,通过采用访问递增序列码,有效阻挡了对UKey的无效访问或恶意破坏。

[0066] 下面分别针对服务器和客户端进行阐述。

[0067] 如图2所示,本申请实施例提供一种访问UKey的安全防护方法,应用于服务器,包括:

[0068] 步骤201,服务器接收客户端发送的访问UKey的验证请求,验证通过则将生成的安全访问权限码发送至所述客户端。

[0069] 其中,验证请求可以是PIN码或指纹校验的请求。服务器调用本地UKey的对应接口进行校验;如果校验成功,服务器产生一个安全访问权限码并保存,同时返回给发起请求的客户端。

[0070] 在一实施例中,所述安全访问权限码为所述服务器生成的16字节随机数。

[0071] 步骤202,所述服务器接收所述客户端对所述UKey的访问请求,根据所述访问请求携带的安全访问权限码确定所述客户端访问所述UKey的权限。

[0072] 所述服务器将本地保存的安全访问权限码和来自客户端的安全访问权限码进行比对,来判断发起请求的客户端是否有权访问UKey资源。

[0073] 在一实施例中,在所述服务器本地保存有访问递增序列码时,所述服务器将所述

访问请求携带的访问递增序列码与本地保存的访问递增序列码进行比对，若所述访问请求携带的访问递增序列码小于等于本地保存的访问递增序列码，则确定访问请求为恶意攻击；若所述访问请求携带的访问递增序列码大于本地保存的访问递增序列码，则确定所述访问请求为正常请求，根据所述访问请求携带的访问递增序列码更新本地保存的访问递增序列码。

[0074] 若确定所述客户端具有访问所述UKey的权限，则继续执行该客户端对UKey的访问请求，若确定所述客户端没有访问所述UKey的权限，则服务器则中断客户端对UKey的访问请求并返回异常。

[0075] 在一实施例中，所述方法还包括：

[0076] 所述服务器根据所述访问请求携带的访问递增序列码确定所述访问请求是否为恶意攻击。

[0077] 在一实施例中，在所述服务器本地保存有访问递增序列码时，所述服务器将所述访问请求携带的访问递增序列码与本地保存的访问递增序列码进行比对，若所述访问请求携带的访问递增序列码小于等于本地保存的访问递增序列码，则确定访问请求为恶意攻击；若所述访问请求携带的访问递增序列码大于本地保存的访问递增序列码，则确定所述访问请求为正常请求，根据所述访问请求携带的访问递增序列码更新本地保存的访问递增序列码。

[0078] 在所述服务器本地没有保存有访问递增序列码时，在所述服务器按照所述安全访问权限码确定所述客户端具有访问所述UKey的权限时，将所述访问请求中携带的访问递增序列码保存在本地。

[0079] 如果服务器确定访问请求为恶意攻击时，则中断本次客户端请求操作并返回异常。

[0080] 如图3所示，本申请实施例提供一种访问UKey的安全防护方法，应用于客户端，包括：

[0081] 步骤301，客户端向服务器发送访问UKey的验证请求，接收所述服务器发送的安全访问权限码。

[0082] 其中，验证请求可以是PIN码或指纹校验的请求。所述安全访问权限码可以是所述服务器生成的16字节随机数。

[0083] 步骤302，所述客户端向所述服务器发送对所述UKey的访问请求，所述访问请求携带所述安全访问权限码，以使所述服务器根据所述安全访问权限码确定所述客户端访问所述UKey的权限。

[0084] 所述客户端接收并保存所述安全访问权限码，所述客户端后续对UKey进行操作时都需要向服务器发送所述安全访问权限码。

[0085] 在一实施例中，所述方法还包括：

[0086] 所述客户端向所述服务器发送对所述UKey的访问请求时，所述访问请求还携带访问递增序列码，以使所述服务器根据所述访问递增序列码确定所述访问请求是否为恶意攻击。

[0087] 其中，客户端每次向服务器发起UKey请求时，同时发送一个访问递增序列码；服务器收到客户端请求并获取其中的访问递增序列码，再与服务器本地保存的上一次成功请求

的访问递增序列码进行比对，来判断当前的客户端请求是否为恶意攻击包。

[0088] 在一实施例中，所述方法还包括：

[0089] 所述客户端根据本地的时间戳确定所述访问递增序列码。

[0090] 所述时间戳的精度可以是10ns。

[0091] 针对基于WSS/HTTPS协议的B/S模式访问UKey资源的安全性漏洞，本申请实施例创造性地提出了对UKey访问的组合式安全防护模式，即基于WSS/HTTPS协议的B/S模式的安全访问权限码和访问递增序列码组合。下面以一些应用实例进行说明。

[0092] 对UKey安全防护的流程如下：

[0093] 一、针对无权限客户端访问UKey的安全防护流程

[0094] 1、客户端向服务器发出PIN码或指纹校验的请求，服务器调用本地UKey的对应接口进行校验并校验成功后，服务器产生一个安全访问权限码(16字节随机数)并保存；

[0095] 2、服务器将安全访问权限码返回给发起请求的客户端，客户端接收到信息并校验成功后，保存安全访问权限码；

[0096] 3、该客户端后续对UKey的每一个操作都需要向服务器发送安全访问权限码；

[0097] 4、服务器每次收到客户端的请求时，首先比较服务器保存的安全访问权限码和来自客户端安全访问权限码是否一致，如果一致，则表明该请求者拥有访问UKey的权限，继续执行该客户端对UKey的访问请求；否则表示该请求者无访问UKey权限，服务器则中断客户端对UKey的访问请求并返回异常。

[0098] 二、针对重复数据包恶意攻击UKey的防护流程

[0099] 1、客户端每次向服务器发送UKey访问请求时，同时向服务器发送一个访问递增序列码。本应用实例使用的访问递增序列码是获取本地时间戳来实现的，时间戳使用10ns精度；

[0100] 2、服务器每次收到客户端的UKey访问请求时，解密出访问递增序列码并与服务器本地保存的访问递增序列码进行比较；

[0101] 3、如果客户端的访问递增序列码小于等于服务器保存的上一次成功请求的访问递增序列码，则服务器确认本次客户端请求为恶意攻击，中断本次客户端请求操作并返回异常；

[0102] 4、如果客户端的访问递增序列码大于服务器保存的上一次成功请求的访问递增序列码，则服务器确认本次客户端请求为正常请求，并且如果该次请求也通过了安全访问权限码的校验，服务器将保存本次请求的访问递增序列码，以备下次客户端请求时进行比较使用。

[0103] 通过该组合式安全防护，可有效防范无访问权限码的客户请求(比如UKey对PIN码或指纹校验成功后，在新浏览器中对UKey的操作请求、或浏览器退出后重打开又对UKey进行操作请求，或在浏览器新页面对UKey进行操作请求)，并使用访问递增序列码有效保护UKey不被重复攻击或数据被篡改，在服务器操作UKey前就有效阻挡了对UKey的无效访问或恶意破坏。通过本发明的组合式安全防护，使得通过B/S模式访问本地UKey资源时能有效保证所有外部对UKey的访问是拥有该UKey硬件及其PIN码或指纹的用户的真实使用。

[0104] 如图4所示，本申请实施例还提供一种访问UKey的安全防护装置，应用于服务器，包括：

[0105] 安全访问权限码发送模块41,用于接收客户端发送的访问UKey的验证请求,验证通过则将生成的安全访问权限码发送至所述客户端;

[0106] 安全访问权限确定模块42,用于接收所述客户端对所述UKey的访问请求,根据所述访问请求携带的安全访问权限码确定所述客户端访问所述UKey的权限。

[0107] 在一实施例中,所述安全访问权限确定模块42,用于:

[0108] 比较本地保存的安全访问权限码与所述访问请求携带的安全访问权限码是否一致,若一致则确定所述客户端具有访问所述UKey的权限,若不一致则确定所述客户端没有访问所述UKey的权限。

[0109] 在一实施例中,所述安全访问权限码为所述服务器生成的16字节随机数。

[0110] 在一实施例中,所述装置还包括:

[0111] 攻击确定模块,用于根据所述访问请求携带的访问递增序列码确定所述访问请求是否为恶意攻击。

[0112] 在一实施例中,所述攻击确定模块,用于:

[0113] 在本地保存有访问递增序列码时,将所述访问请求携带的访问递增序列码与本地保存的访问递增序列码进行比对,若所述访问请求携带的访问递增序列码小于等于本地保存的访问递增序列码,则确定访问请求为恶意攻击;若所述访问请求携带的访问递增序列码大于本地保存的访问递增序列码,则确定所述访问请求为正常请求,根据所述访问请求携带的访问递增序列码更新本地保存的访问递增序列码。

[0114] 如图5所示,本申请实施例还提供一种访问UKey的安全防护装置,应用于客户端,包括:

[0115] 验证请求模块51,用于向服务器发送访问UKey的验证请求,接收所述服务器发送的安全访问权限码;

[0116] 访问请求模块52,用于向所述服务器发送对所述UKey的访问请求,所述访问请求携带所述安全访问权限码,以使所述服务器根据所述安全访问权限码确定所述客户端访问所述UKey的权限。

[0117] 在一实施例中,所述访问请求模块52,还用于:

[0118] 向所述服务器发送对所述UKey的访问请求时,所述访问请求还携带访问递增序列码,以使所述服务器根据所述访问递增序列码确定所述访问请求是否为恶意攻击。

[0119] 在一实施例中,所述访问请求模块52,还用于:

[0120] 根据本地的时间戳确定所述访问递增序列码。

[0121] 本申请实施例还提供一种服务器,包括:存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,所述处理器执行所述程序时实现所述访问UKey的安全防护方法。

[0122] 本申请实施例还提供一种客户端,包括:存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,所述处理器执行所述程序时实现所述访问UKey的安全防护方法。

[0123] 本申请实施例还提供一种计算机可读存储介质,存储有计算机可执行指令,所述计算机可执行指令用于执行所述访问UKey的安全防护方法。

[0124] 在本实施例中,上述存储介质可以包括但不限于:U盘、只读存储器(ROM,Read-

Only Memory)、随机存取存储器(RAM,Random Access Memory)、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

[0125] 本领域普通技术人员可以理解,上文中所公开方法中的全部或某些步骤、系统、装置中的功能模块/单元可以被实施为软件、固件、硬件及其适当的组合。在硬件实施方式中,在以上描述中提及的功能模块/单元之间的划分不一定对应于物理组件的划分;例如,一个物理组件可以具有多个功能,或者一个功能或步骤可以由若干物理组件合作执行。某些组件或所有组件可以被实施为由处理器,如数字信号处理器或微处理器执行的软件,或者被实施为硬件,或者被实施为集成电路,如专用集成电路。这样的软件可以分布在计算机可读介质上,计算机可读介质可以包括计算机存储介质(或非暂时性介质)和通信介质(或暂时性介质)。如本领域普通技术人员公知的,术语计算机存储介质包括在用于存储信息(诸如计算机可读指令、数据结构、程序模块或其他数据)的任何方法或技术中实施的易失性和非易失性、可移除和不可移除介质。计算机存储介质包括但不限于RAM、ROM、EEPROM、闪存或其他存储器技术、CD-ROM、数字多功能盘(DVD)或其他光盘存储、磁盒、磁带、磁盘存储或其他磁存储装置、或者可以用于存储期望的信息并且可以被计算机访问的任何其他的介质。此外,本领域普通技术人员公知的是,通信介质通常包含计算机可读指令、数据结构、程序模块或者诸如载波或其他传输机制之类的调制数据信号中的其他数据,并且可包括任何信息递送介质。

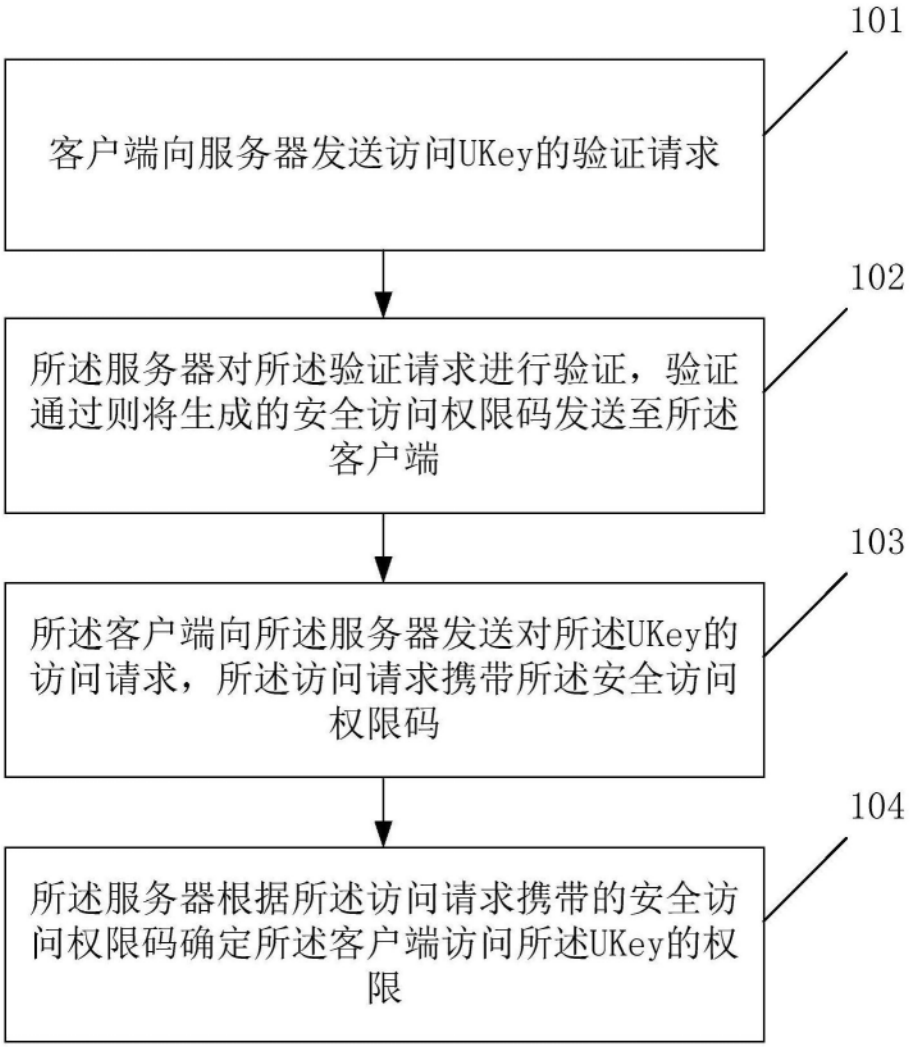

101
客户端向服务器发送访问UKey的验证请求
102
所述服务器对所述验证请求进行验证，验证通过则将生成的安全访问权限码发送至所述客户端
103
所述客户端向所述服务器发送对所述UKey的访问请求，所述访问请求携带所述安全访问权限码
104
所述服务器根据所述访问请求携带的安全访问权限码确定所述客户端访问所述UKey的权限

图1

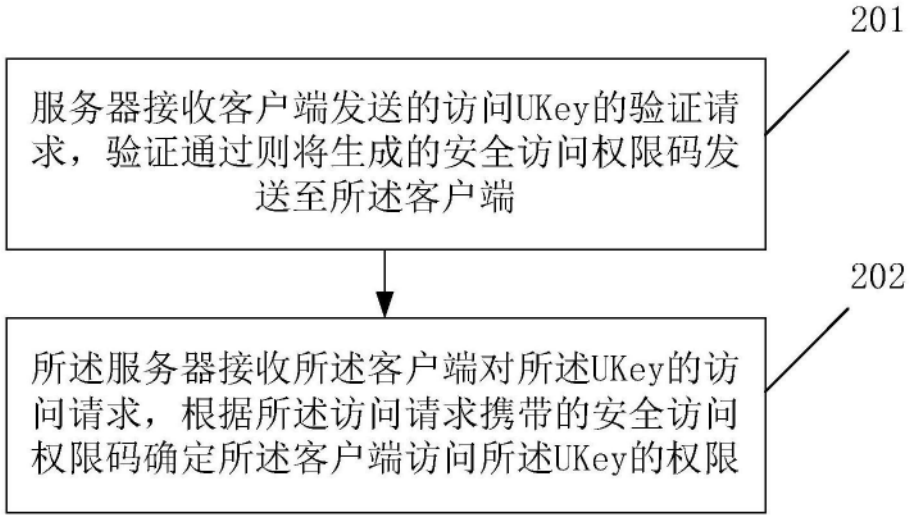

201
服务器接收客户端发送的访问UKey的验证请求，验证通过则将生成的安全访问权限码发送至所述客户端
202
所述服务器接收所述客户端对所述UKey的访问请求，根据所述访问请求携带的安全访问权限码确定所述客户端访问所述UKey的权限

图2

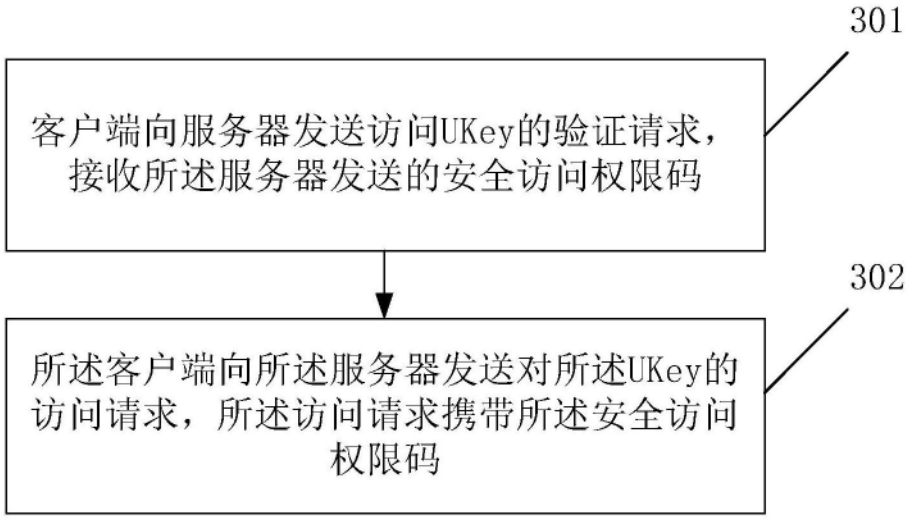

301
客户端向服务器发送访问UKey的验证请求，接收所述服务器发送的安全访问权限码
302
所述客户端向所述服务器发送对所述UKey的访问请求，所述访问请求携带所述安全访问权限码

图3

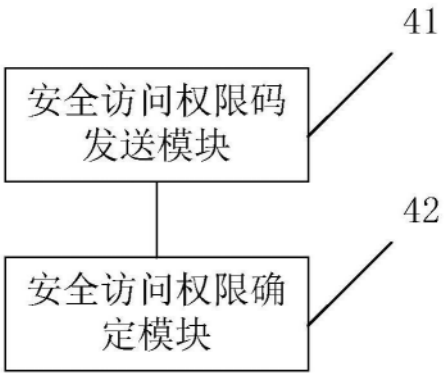

41
安全访问权限码发送模块
42
安全访问权限确定模块

图4

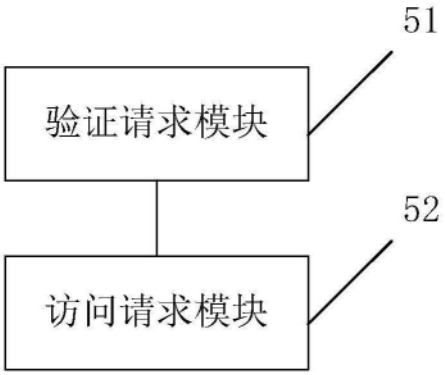

51
验证请求模块
52
访问请求模块

图5