

(12) 发明专利申请

(10) 申请公布号 CN 102281137 A

(43) 申请公布日 2011. 12. 14

(21) 申请号 201010199297. 0

(22) 申请日 2010. 06. 12

(71) 申请人 杭州驭强科技有限公司

地址 310053 浙江省杭州市滨江区江南大道
3778 号元天科技大楼 A 座 F5004

(72) 发明人 高智勇 童寅 杨晓

(74) 专利代理机构 北京市盛峰律师事务所

11337

代理人 李贺香

(51) Int. Cl.

H04L 9/32(2006. 01)

H04L 29/06(2006. 01)

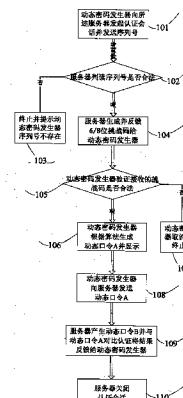
权利要求书 1 页 说明书 3 页 附图 1 页

(54) 发明名称

一种双向认证式挑战应答机制的动态密码认
证方法

(57) 摘要

本发明公开了一种双向认证式挑战应答机制
的动态密码认证方法,包括:动态密码发生器向
服务器发起认证会话和发送动态密码发生器序列
号;所述服务器根据接收到的动态密码发生器序列号
进行处理形成挑战码反馈给所述的动态密码发生器;
所述的动态密码发生器对接收的挑战码进
行验证,如果合法动态密码发生器生成动态口令A并显示,
否则取消显示并终止;所述的动态密码发生器用户向所述的服
务器发送当前动态密码发生器显示的动态口令A;服务器接收到动态口令A后采用产生动态口令B,并将两个动态口令进行
对比将结果反馈给动态密码发生器并关闭认证会
话。本发明动态密码发生器会对服务器端提供的
挑战码进行验证,能够更好的防护钓鱼网站和中
间人攻击。



1. 一种双向认证式挑战应答机制的动态密码认证方法,通过至少一服务器和至少一用户动态密码发生器实现,其特征在于:包括如下步骤:

S1,所述动态密码发生器向所述服务器发起认证会话,并向所述服务器发送所述动态密码发生器序列号;

S2,所述服务器根据接收到的密码发生器序列号使用加密算法进行处理,形成挑战码反馈给所述的动态密码发生器;

S3,所述的动态密码发生器对接收到的挑战码进行验证,如果挑战码不合法动态密码发生器取消显示并终止流程,如果挑战码合法则动态密码发生器根据加密算法生成动态口令A并显示;

S4,所述的动态密码发生器向所述的服务器发送当前动态密码发生器显示的动态口令A;

S5,所述的服务器接收到动态口令A后,采用与所述的动态密码发生器相同的算法产生动态口令B,并将动态口令A和动态口令B进行对比得到认证结果,反馈给所述的动态密码发生器并关闭认证会话。

2. 根据权利要求1所述的双向认证式挑战应答机制的动态密码认证方法,其特征在于:

S2中所述挑战码通过AES加密算法实现,具体包括:

S2-1,所述的服务器产生一个随机数,

S2-2,根据接收到的所述动态密码发生器序列号及其所对应的参数密码种子使用aes加密算法运算,取所得结果的两个特定字节分别对10取模;

S3-3,将取模结果拼接到所述的服务器产生的随机数的末尾,形成挑战码。

3. 根据权利要求2所述的双向认证式挑战应答机制的动态密码认证方法,其特征在于:S2中,所述服务器根据接收到的密码发生器序列号使用加密算法进行处理之前,还包括:对所述的动态密码发生器序列号进行验证的步骤。

4. 根据权利要求3所述的双向认证式挑战应答机制的动态密码认证方法,其特征在于:所述对所述的动态密码发生器序列号进行验证,其方式为:在所述服务器上预存所述的动态密码发生器序列号,当所述服务器接收到所述的动态密码发生器发送的序列号后将预存的动态密码发生器序列号与接收的所述的动态密码发生器序列号进行对比,如果一致则向下进行,否则终止流程。

5. 根据权利要求4所述的双向认证式挑战应答机制的动态密码认证方法,其特征在于:当所述的动态密码发生器序列号进行对比不一致后,进一步还包括:向所述动态密码发生器发送提示序列号不存在的信息的步骤。

6. 根据权利要求1所述的双向认证式挑战应答机制的动态密码认证方法,其特征在于:所述的动态口令生成进一步包括:使用AES算法加密种子,以Salt为密钥,使用ECB方式即直接调用加密函数,生成一个128位的密文块;

使用这个密文块的高端N个字节,将其分别除以10的余数作为最终所述动态口令其中的一位,最终得到一个N个十进制位的动态口令。

一种双向认证式挑战应答机制的动态密码认证方法

技术领域

[0001] 本发明涉及动态密码认证，尤其涉及一种双向认证式挑战应答机制的动态密码认证方法。

背景技术

[0002] 随着电子商务的发展，客户的帐户安全已成为一个重要问题，单一依靠静态密码进行交易的身份确认方式，存在严重的被破取、猜测破解等问题，采用动态密码令牌方式可以解决上述问题，但目前在认证模式上存在一定缺陷，多数密码产品采用单向认证模式，即由动态密码令牌传统的挑战应答模式在给与客户端挑战码时只给予随机数字来进行动态口令的运算，在安全性以及防护钓鱼攻击、中间人攻击时表现上有所欠缺。

发明内容

[0003] 针对上述问题，本发明提供了一种增加了对服务器端的进行认证的双向认证式挑战应答机制的动态密码认证方法。

[0004] 本发明采用的技术方案如下

[0005] 一种双向认证式挑战应答机制的动态密码认证方法，通过至少一服务器和至少一用户动态密码发生器实现，包括如下步骤：

[0006] S1，所述动态密码发生器向所述服务器发起认证会话，并向所述服务器发送所述动态密码发生器序列号；

[0007] S2，所述服务器根据接收到的密码发生器序列号使用加密算法进行处理，形成挑战码反馈给所述的动态密码发生器；

[0008] S3，所述的动态密码发生器对接收到的挑战码进行验证，如果挑战码不合法动态密码发生器取消显示并终止流程，如果挑战码合法则动态密码发生器根据加密算法生成动态口令A并显示；

[0009] S4，所述的动态密码发生器向所述的服务器发送当前动态密码发生器显示的动态口令A；

[0010] S5，所述的服务器接收到动态口令A后，采用与所述的动态密码发生器相同的算法产生动态口令B，并将动态口令A和动态口令B进行对比得到认证结果，反馈给所述的动态密码发生器并关闭认证会话。

[0011] 进一步地，S2中所述挑战码通过AES加密算法实现，具体包括：

[0012] S2-1，所述的服务器产生一个随机数，

[0013] S2-2，根据接收到的所述动态密码发生器序列号及其所对应的参数密码种子使用aes加密算法运算，取所得结果的两个特定字节分别对10取模；

[0014] S3-3，将取模结果拼接到所述的服务器产生的随机数的末尾，形成挑战码。

[0015] 进一步地，S2中，所述服务器根据接收到的密码发生器序列号使用加密算法进行处理之前，还包括：对所述的动态密码发生器序列号进行验证的步骤。

[0016] 进一步地，所述对所述的动态密码发生器序列号进行验证，其方式为：在所述服务器上预存所述的动态密码发生器序列号，当所述服务器接收到所述的动态密码发生器发送的序列号后将预存的动态密码发生器序列号与接收的所述的动态密码发生器序列号进行对比，如果一致则向下进行，否则终止流程。

[0017] 进一步地，当所述的动态密码发生器序列号进行对比不一致后，进一步还包括：向所述动态密码发生器发送提示序列号不存在的信息的步骤。

[0018] 进一步地，所述的动态口令生成进一步包括：使用 AES 算法加密种子，以 Salt 为密钥，使用 ECB 方式即直接调用加密函数，生成一个 128 位的密文块；

[0019] 使用这个密文块的高端 N 个字节，将其分别除以 10 的余数作为最终所述动态口令其中的一位，最终得到一个 N 个十进制位的动态口令。

[0020] 本发明的有益效果

[0021] 利用本发明动态密码发生器会对服务器端提供的挑战码进行验证，这种双向认证机制能够更好的防护钓鱼网站和中间人攻击。

附图说明

[0022] 图 1 为本发明一具体实施例流程图。

具体实施方式

[0023] 为更好地描述本发明，下面结合附图详细说明一下本发明。

[0024] 本方案在传统的挑战应答机制的动态口令认证方式（动态口令一般由一种内置电源、算法芯片和显示屏的手持终端根据专门的算法动态生成，其特点是每隔一定的时间变化一次，使用一次后的密码和过往的密码均无效）中加入了客户端对服务器端的认证，具体如下：

[0025] 所述动态密码发生器通过步骤 101 向所述服务器发起认证会话，并向所述服务器端发送所述动态密码发生器序列号；

[0026] 服务器根据步骤 102 对所述的动态密码发生器序列号进行验证，验证其是否合法，验证方式为：在所述服务器上预存所述的动态密码发生器序列号，当所述服务器接收到所述的动态密码发生器发送的序列号后将预存的动态密码发生器序列号与接收的所述的动态密码发生器序列号进行对比，如果一致则进行步骤 104，否则通过步骤 103 终止流程并提示动态密码发生器序列号不存在。

[0027] 所述服务器通过步骤 104 根据接收到的密码发生器序列号，将接收到的动态密码发生器序列号所对应的某个特定参数作为密钥进行 aes 运算，将所得结果的特定两位数对 10 取模，并将取模结果拼接到服务器产生的随机数的末尾，形成 6/8 位挑战码反馈给动态密码发生器；

[0028] 所述的动态密码发生器通过步骤 105 对接收到的挑战码进行验证，如果挑战码不合法动态密码发生器通过步骤 107 取消显示并终止流程，如果挑战码合法则动态密码发生器通过步骤 106 根据加密算法生成动态口令 A 并显示；

[0029] 所述的动态密码发生器通过步骤 108 向所述的服务器发送当前动态密码发生器显示的动态口令 A；

[0030] 服务器接收到动态口令 A 后,通过步骤 109 采用与所述的动态密码发生器相同的算法产生动态口令 B,并将动态口令 A 和动态口令 B 进行对比得到认证结果,反馈给所述的动态密码发生器并通过步骤 110 关闭认证会话。

[0031] 以上所述动态口令的算法原理如下:

[0032] 动态口令采用 AES 算法:动态密码发生器根据一个 128 位的种子 (seed) 和一个 128 位 salt 生成 6 位十进制的一次性密码。对于确定的动态密码发生器来说,种子 (Seed) 是一个 128 位的真正随机的数,在生产时写入手持终端中保存,因此对于一个确定的手持终端,这是一个常数。Salt 是由序列号、时间和填充位构成的 128 位数据。在目前的算法中,每分钟产生一个密码,以分钟单位计算,实时时钟秒位在参与计算时用 0 来填充;为了进一步增加被破解难度,我们可以修改算法,为每 30s 产生一个密码,或根据客户要求定制。

[0033] 以上所述生成 OTP 即动态口令的过程是:使用 AES 算法 (128 位数据,128 位密钥的版本) 加密种子,以 Salt 为密钥,使用 ECB 方式(就是直接调用加密函数),没有填充(Padding)。这会生成一个 128 位的密文块,在这个基础上,为了得到一个 N 个十进制位(目前实现中 N = 6,或根据用户要求定制长度)的 OTP 密码,我们使用这个密文块的高端 N 个字节,将这次字节分别除 10 的余数作为最终 OTP 的一位。

[0034] 例如,如果 AES 算法得到以下的密文块:

[0035] 0x11 0x22 0x33 0x44 0x55 0x66 0x77 0x88

[0036] 0x990xAA 0xBB 0xCC 0xDD 0xEE 0xFF0x00

[0037] 此时取 0x11 0x22 0x33 0x44 0x55 0x66(17,34,51,68,85,102)

[0038] 截断后可以得到:741852

[0039] 以上通过具体实施例详细描述了本发明,但本领域技术人员应该理解,本发明并不局限于以上所述实施例,凡在本发明的精神和原则之内,所作的任何修改、等同替换等,均应包含在本发明的保护范围之内。

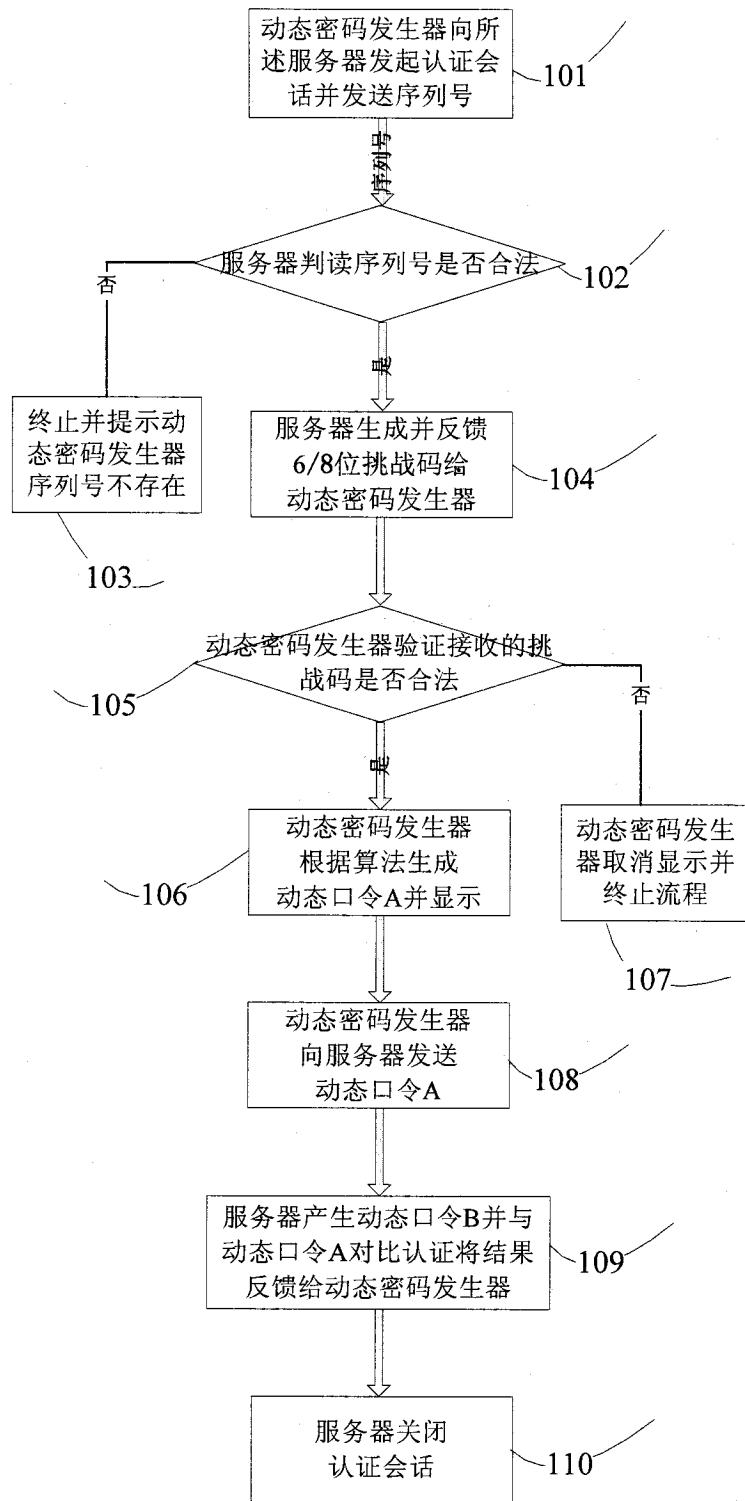


图 1