(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105871546 A
(43)申请公布日 2016.08.17

(21)申请号 201610392886.8

(22)申请日 2016.05.24

(71)申请人 张雪莱
地址 266100 山东省青岛市崂山区香港东路395号山水名园二期27-1-101

(72)发明人 张雪莱

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/14(2006.01)

权利要求书1页 说明书2页

(54)发明名称

一种静态密码与动态密码结合的验证方法及终端设备

(57)摘要

本发明涉及一种动态密码验证方法，其特征在于用户输入的密码包含静态和动态两部分字符，用户在创建或设置帐户时事先约定动态密码的计算方法，该计算方法使用日期等变量数据，经过简单变换得到验证时使用的动态密码；需要验证密码时，用户在终端设备或客户端软件界面上输入静态密码和经过简单计算形成的动态密码，或使用动态密码加密静态密码得到的字符串提交验证；终端设备或客户端软件将获得的输入分解出静态密码和动态密码字符串或使用动态密码解密输入字符串得到静态密码；服务器把收到的加密静态密码跟预先保存的用户密码比对，如需要，把收到的动态密码跟按照相同算法得出的字符串比对，判断是否可以通过验证。

CN 105871546 A

1.一种动态密码验证方法，其特征在于用户输入的密码包含静态和动态两部分字符，用户在创建或设置帐户时事先约定密码的某几位是动态密码以及动态密码的计算方法，该计算方法使用用户和验证方之间无异议的变量数据，例如当前日期时间及本次交易金额中的数字或当前页面上特定位置的字符，经过四则运算位置交换等简单变换得到验证时使用的动态密码；需要验证密码时，用户在终端设备或客户端软件界面上输入静态密码和经过简单计算形成的动态密码，提交验证；终端设备或客户端软件将获得的输入分成静态密码字符串和动态密码字符串并分别加密后传送到服务器验证；服务器把收到的加密静态密码跟预先保存的用户密码比对，把收到的加密动态密码跟按照相同算法得出的字符串比对，只有这两串密码都相符才可以通过验证。

2.如权利要求项1所述的动态密码验证方法，其特征在于作为一种简化方案，动态密码不经过加密步骤。

3.一种采用权利要求项1或2所述动态密码验证方法的银行卡POS机，其特征是可以一次性输入静态密码和动态密码的组合字符串，并分离出动态密码部分和静态密码部分，根据服务器方的加密要求上传验证两个密码的报文数据。

4.一种采用权利要求项1或2所述动态密码验证方法的银行卡POS机，其特征是可以先输入静态密码或动态密码字符串，根据服务器方的加密要求上传验证数据，然后根据服务器方的应答消息中的进一步要求，要求用户输入另一密码并上传验证。

5.一种采用权利要求项1或2所述动态密码验证方法登录的软件客户端、Web页面或操作系统。

6.一种动态密码验证方法，其特征在于用户输入的密码是以动态密码为密钥加密过的静态密码，用户在创建或设置帐户时事先约定动态密码的来源及排列、变换的计算方法，同时约定使用动态密码作为密钥简单加密静态密码的算法，该来源使用用户和验证方之间无异议的变量数据，例如当前日期时间及本次交易金额中的数字或当前页面特定位置的显示字符，经过定义的计算方法的简单变换得到验证时使用的动态密码；需要验证密码时，用户在终端设备或客户端软件界面上输入经过以动态密码作为密钥的简单加密的静态密码，提交验证；终端设备或客户端软件将获得的输入利用根据用户帐号信息事先取得本次交易使用的动态密码作为密钥解密得到静态密码字符串后按照服务器软件的加密要求加密后传送到服务器验证；服务器把收到的静态密码密文跟预先保存的用户密码密文比对，如两串密码相符则通过验证。

7.一种采用权利要求项6所述动态密码验证方法的银行卡POS机，其特征是在刷卡时获得该用户本次交易要使用的动态密码，验证密码时对用户输入的密码解密得到静态密码字符串，并根据服务器方的加密要求上传验证数据。

8.一种采用权利要求项6所述动态密码验证方法登录的软件客户端、Web页面或操作系统。

一种静态密码与动态密码结合的验证方法及终端设备

技术领域

[0001] 本发明涉及一种密码验证方法及相应的终端设备，适用于软件客户端或操作系统的登陆以及金融卡消费等需要密码鉴权的应用。

背景技术

[0002] 通常我们登陆软件账号或使用银行卡时使用固定的静态密码。静态密码如果被非法获取并恶意使用就会造成巨大的损失。目前使用的银行卡可以通过复制磁条、偷窥密码及非法改装POS机记录磁条及按键顺序破译及盗刷。动态密码是进一步提升系统的安全性的方案，传统的动态密码依靠额外的密码器等独立设备或经过手机短信等途径传递，独立密码设备成本较高，短信密码仍然有被木马软件截获的风险。

发明内容

[0003] 本发明所要解决的技术问题是设计一种低成本的安全的密码系统。

[0004] 本发明所提供的技术方案是：采用静态密码与动态密码结合的方案，动态密码使用用户和验证方之间无异议的变量数据，例如当前日期时间及本次交易金额中的数字以及当前页面特定位置显示的字符，经过四则运算位置交换等简单变换得到。这样设计的优点在于密码容易记忆、动态密码不需要额外设备，密码的计算参数与算法不需要在客户端与服务器之间传递因而不会被非法软件截获；与静态密码结合使系统升级简单平稳；如果某次验证时输入的密码被偷窥或被非法软件截获也不用担心帐户被盗用。

具体实施方式

[0005] 本方案涉及的动态密码需要在创建或设置帐户时指定算法，可以提供多种计算公式供用户选择，例如(并不局限于)提供2至3个可选变量以及变量之间的运算符，每个变量可以是月份、日期、时间、星期的数字以及本次交易的金额的前几位或者上述几个变量的倒序，还可以是某个固定值或当前页面特定位置显示的字符。如果需要限定动态密码的位数，还要设定截断或补位的策略。假设某用户设置动态密码公式为：当前月份+当前日期的倒序+32，当前日期是05月09日，则生成的动态密码为：05+90+32＝127，如果限定密码长度为2且取后两位，则密码位27。

[0006] 用户输入的密码由静态密码和动态密码结合而成。静态密码跟动态密码的组合顺序可以整个系统统一规定，也可以由用户自己设定。例如密码的第2第3位是动态密码；或者前6位为静态密码，后2位为动态密码。假设用户的静态密码是123456，本次交易要使用的动态密码为78，约定密码的前两位是动态密码，则本次要输入的密码是78123456。

[0007] 需要验证密码时，用户在终端设备或客户端软件界面上输入静态密码和经过简单计算形成的动态密码的组合字符串，提交验证；终端设备或客户端软件将获得的输入分成静态密码字符串和动态密码字符串并分别加密后传送到服务器验证；服务器把收到的加密静态密码跟预先保存的用户密码比对，把收到的加密动态密码跟按照相同算法得出的字符

串比对，只有这两串密码都相符才可以通过验证。

[0008] 用户也可以采用使用动态密码作为密钥加密静态密码的方法得到本次要输入的密码串，该加密算法由用户设置账户时约定，一般采用按位叠加等便于心算的算法，终端设备或客户端软件按照加密算法的逆运算解密得到要送往服务器验证的静态密码。例如静态密码为123456，本次使用的动态密码为21，加密算法为每两位叠加动态密码则输入的密码为123456+212121＝335577，客户端把335577减212121得到123456按照传统方式送服务器验证。