[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/28
H04L 9/32

[12] 发明专利申请公开说明书

[21] 申请号 03156541.7

[43] 公开日 2004 年 8 月 25 日

[11] 公开号 CN 1523809A

[22] 申请日 2003.9.8 [21] 申请号 03156541.7

[71] 申请人 赵忠华
地址 518020 广东省深圳市红岗路红岗大厦 2808 室
[72] 发明人 赵忠华

权利要求书 4 页 说明书 6 页 附图 1 页

[54] 发明名称 可变密码身份验证技术

[57] 摘要

一种应用于信息系统的密码可变的用户身份验证技术，有别于传统密码的用户身份验证技术。在本技术中，用于验证用户身份的密码是变化的，密码算法由用户定义，保存于系统服务器。进行身份验证时，用户只根据自己定义的密码算法计算出当次密码进行输入。每个密码只用一次，每次均用一个任何人事先无法预知新的密码。而作为保密核心的密码算法，其形式定义和记忆非常简单，比传统密码更容易记忆，记住一个密码算法，可以应用到多个保密账号中，其产生出的密码内容变化无穷，保密性极高，密码算法在使用中不在网络上传输或在用户输入密码的现场暴露，彻底杜绝了用户密码被遗忘、非法盗取、破译的弊端。

ISSN1008-4274

1、一种密码可变的用户身份验证技术，其特征是：

用户每次被要求输入的密码是可变的，有别于传统的不变密码；

传统密码在合法使用过程中，如果用户或系统管理员不改变它，验证用户身份的密码一直保持不变；

可变密码系统在使用过程中，每次验证用户身份的密码是变化的，密码相同的情况只是偶尔的特例；

可变密码的算法是事先设定好的，每次进行验证用户身份时，用户根据现场参数（即密码算法参数）按照设定好的密码算法计算出一个密码值，进行验证。

2、权利要求 1 所述的密码字符及密码算法参数包括数字、字母、符号等，执行如下标准：

英文字符集标准：ASCII 字符集基本集（美国信息交换标准码）

中文字符集标准：GB2312-80 字符集基本集（双八位）

3、权利要求 1 所述的用于生成密码的算法由用户自己定义，其形式包括但不限于如下形式：

(1)函数公式：根据一个函数公式来计算密码；

(2)数据序列：指定一系列密码值，符合一定条件时使用其中一个；

(3)输入条件：指密码输入时的附加条件。

密码算法保存于用户信息库中，在用户建立时定义，以后随时都可以按用户的要求修改。

4、权利要求 3 所述的函数公式形式的可变密码算法可用下述式子表达：

$$Y=F(x)$$

Y 为生成的密码值，是在用户身份验证时被要求输入的当次密码

x 为密码算法参数，是用户和用户身份验证系统计算密码的参数

值

F( )为密码算法公式，由数学运算符及其他函数等构成

5、权利要求 3 所述的数据序列指用户事先定义好的一组密码值，使用时根据不同条件选择，包括但不限于如下形式：

（1）无规律字符串集：指没有变化规律的一组字符串，来自权利 2 要求的字符集，如 123453、defgh4、we45y 等；

（2）用户可将自己熟悉的某些事物的一组特征参数（如自己的身体上的各项参数，身高、体重、视力等）作为密码数据序列。

6、权利要求 4 所述的密码算法参数，来自权利要求 2 的字符集，包括但不限于如下形式：

（1）系统随机数：由用户身份验证系统随机给出，可以事先设定一定的范围及规则，如 6 位数字，由软件随机函数生成；

（2）规律变化序列：根据确定规律变化的可预见其取值的有序数字或字符序列，如日期、时间或与日期时间同步变化的其他序列；

（3）用户指定序列，由用户自定义的一串数字或字符，如 1,3,5,7,9,a,b,c。

7、权利要求 4 所述的可变密码计算公式，是对密码算法参数本身或将其分解后进行的数学运算、字符位置变换、字符对应序列值变换或其他形式的变化，包括但不限于如下形式：

（1）字符位置变换例子：

对密码算法参数中的部分或全部字符分解，然后重新排列位置

如密码算法参数为 123456

（a）密码算法规则：倒序排列

则生成密码：654321

（b）密码算法规则：依次提取偶数字符和奇数字符先后排列（参数必须是数字串）

则生成密码：246135

（2）数字计算例子：

对密码算法参数的部分或全部字符分解，然后进行数学运算

如密码算法参数为 123456

（a）密码算法规则：每位数字加 5，结果大于或等于 10 时取个位数

则生成密码：678901

（b）密码算法规则：每位数字加其后面一位数字，最后一位数字加首位数字，结果大于或等于 10 时取个位数

则生成密码：357917

（3）综合变换例子：

兼有位置变换及数字计算特点

如密码算法参数为 123456

（a）密码算法规则：倒序排列，并对每位数字加 1，结果大于或等于 10 时取个位数

则生成密码：765432

（b）密码算法规则：首尾两数字互换，其它数字加 1，结果大于或等于 10 时取个位数

则生成密码：634561

（4）字母表变换例子：

每个字母取其字母表中后一个(如果是最后一个就取第一个)，并且大小写互换（即遇以小写字母时将其变成大写，遇到大写字母时将其变成小写）

密码算法参数：aDjkDz

生成密码值：BeKLeA

（5）字母序列变换例子：

英文字母 a 至 z 按顺序对应其序列值 1 至 26，按此规律将由字母

构成的字符串变换成数字字符串。

密码算法参数：abcxyz

生成密码值：123242526

8、权利要求3所述的输入条件，指可变密码输入时的附加条件，也是可变密码的一项重要内容，如果可变密码系统设置了输入条件，在输入密码时必须满足这个条件，否则视为密码输入无效，下面是输入条件的一个例子，但不限于例子中的形式。

输入时间条件

指输入密码时必须满足指定的时间条件，如在限定的条件内输完密码，否则视为非法入侵，系统自动锁死。对一些安全性要求很高的保密项目，可指定较短的输入时间限制，只有对自己密码系统非常熟悉的用户，才能做到快速连续不间断输入。

9、在进行用户身份验证时，验证系统根据事先设定的密码算法和当时的密码算法参数生成一个临时密码，用户也根据事先定义的密码算法和当时的密码算法参数计算出一个密码并输入，系统将用户输入的密码与临时密码对照，如果完全一致，验证通过，否则验证不能通过，用户无法登录系统。

可变密码身份验证技术

发明领域

本发明涉及一种用于用户身份验证的可变密码加密技术，适用于任何信息化安全系统。

技术背景

随着全社会范围内信息化的迅速普及，用户密码成了身份验证重要手段，但是，传统的密码没有自动变化的功能，用户使用密码时，总会留下现场痕迹，容易泄密，如记录下用户输入密码的全过程或截留下用户的密码信息，就可破译用户密码，从而冒充用户登录，对用户信息安全构成巨大威胁。目前各类金融卡、电信卡、服务消费卡、软件、专用仪器等以及网上的各类服务都大量使用密码作为用户身份验证的唯一手段，用户密码泄露就意味着犯罪分子可以肆意侵犯用户的各种权利，使用用户蒙受巨大损失。目前因密码泄露引发的案件逐年大幅上升，已成为一个严重的社会问题。传统密码技术已受到严重挑战。

发明概述

本发明是以解决现有用户身份验证技术的上述问题为目标而产生的，它本身的目的是提供一种不暴露加密核心（密码算法）的随机可变的用户身份验证方法。

在信息化时代，密码被广泛用来验证用户身份。用户需要有个性化的服务时，为了保护个人权益及隐私，在提供服务的系统中开设个人帐户，获得一个唯一的帐号，并设定一个密码，以后用户进入系统时，要求输入自己的帐号及密码，帐号及密码正确是进入服务系统的充分条件。因此帐号及密码成为信息时代的通行证，验证帐号及密码

的过程全由电脑自动完成，由于电脑是只认数据不认人，用户的帐号及密码一旦被别人盗取，别人就能以真实用户的身份进入用户的系统，进行各类侵犯用户利益的活动。由于帐号在使用中是公开的，因此密码也就成了用户维护自己权益的唯一手段。

由于密码保护手段简便易行，在现代社会被广泛使用，几乎所有需要受保护的服务项目都靠密码去实现，造成了现代人需要记住大量的密码。密码忘记或被盗对用户来说都是不幸的，往往要遭受巨大的精神及物质损失，记住大量密码及防止密码泄露成了现代人的一大负担。为了记住密码，力求密码越简单越好，为了防止密码泄露，就要将密码设得复杂一些，而且经常更换。这是一对矛盾，稍有不慎，灾难便会降临。

近年来，专门盗取用户密码而进行犯罪的事件层出不穷，尤其进入网络时代，各类网上服务均是通过密码进行的，用户输入密码的现场及密码资料在网上传输时，很容易被非法截取并破译。如金融及电信领域是密码犯罪的高发区，用户使用银行卡提款、购物消费，享受电信服务时，一切都依靠密码，而作为保密核心的密码的输入是完全暴露在密码使用现场的，犯罪分子很容易窃取用户密码，从而导致严重后果。可见信息化在为现代人带来便利的同时威胁及担忧也结伴而生。

在目前的密码管理机制下，用户的密码是不能自动变化的，即用户设定自己的密码后一直是固定不变而且有效的，除非用户再次修改或指定有效期。在实际应用中，要求用户经常去改密码是不现实的，用户也容易自己忘记。犯罪分子窃取到密码后，往往是立即行动，除非要求用户每使用一次密码就改一下，每次使用一个新密码，这样更加不可能。

用户使用密码时，均要通过各类输入设备输入自己的密码，在下

列方式下，用户的密码很容易泄露：

1、截取用户的密码资料并破译

2、在输入终端上做手脚，记录用户输入的密码

3、在用户输入密码的现场周围进行暗中观测获取密码

4、根据用户的密码使用习惯猜测其密码

许多用户为了图省事，将自己的生日、电话号码等设为密码，或将多个服务项目的密码设成相同的，这种方式极不安全，很容易泄密。

可见现行的密码体系存在极大的缺陷，本发明就是为解决上述问题而产生的一套全新的密码方案，密码是随机的、可变的。一般情况下一个密码只用一次，即使盗取了用户某次使用的密码，用户下次使用的又是一个新密码，事先无法预知，只有用户自己知道，也无须专门记忆。从而彻底解决了现行密码体系中的记忆难及易泄露的难题。

从下表的对照中就能更加清晰地看到本方方案的优势：

	保密方案核心	保密核心在使用中	密码泄露后果	用户记忆难度
传统密码方案	密码	暴露	极其严重	很大
可变密码方案	密码算法	不暴露	毫无影响	很小

本可变密码方案的核心是，用户在某个系统开户后，得到一个帐号，在设定密码时，不是设定一个具体密码值，而是设定一个密码算法，即密码生成公式，以后用户登录系统时，系统和用户均根据登录现场参数，利用事先设定的密码算法计算出一个密码值，用户将计算出的密码值输入系统进行验证，如果系统计算出的密码值与用户计算的密码值相同，验证通过。在本方案的密码验证过程中，核心密码算法始终没有暴露出来，即使有人暗中跟踪分析用户的密码使用过程，得到的也只是一些毫无价值的密码值，无法得取密码算法，从而有效地保护了用户的系统不被非法侵入。

下面是一个密码验证例子。

用户在某个银行开户得到一张提款卡，并为自己的提款卡设定一个密码算法：

密码＝随机码各位数字加 1（逢 10 取尾数）

当用户某次在商场购物消费时，刷过卡后，系统提供一个随机码：349012

根据用户设定的密码算法，计算出的密码值应为：450123

用户如果正确输入这个密码值，则验证通过。

在上述例子中，用户的提款卡密码是变化的，每次一个新密码，在任何公共场合可以放心使用，无须担心别人跟踪分析。生成密码的密码算法保存在系统服务器，使用时只在服务器内部完成密码的计算分析，无须担心被截留破译。用户根据系统的提示计算输入密码时，使用的密码算法是事先自己定义好的，与服务器中的相同，这个密码算法也是存在自己心中，别人无法得知。系统提示的随机码是系统随机生成的，随机码根据密码算法公式的计算就生成了当次的用户密码，这个密码是自动变化的，任何人都事先无法得知，从而彻底杜绝了非法盗取、破译用户密码而进行犯罪的企图。

本可变密码技术不但解决了密码的泄露被盗问题，也无须记忆大量的复杂密码。在传统的保密技术中，每个服务项目至少要求设置一个密码，有时好几个，如银行卡有查询、取款等多个密码。现代人要面临大量的需要保密的服务项目，大量的密码管理是现代人的一项沉重负担，将多个服务项目密码设置成相同就会后患无穷。实施了本发明的可变密码技术，只记住自己定义的密码算法（密码生成公式），就能以不变（密码算法）应万变（密码）。解决了密码的记忆难及易泄露两大难题。

该系统实施简单，成本极低，对传统的密码系统软件进行必要的

调整就可以了。对于保密性极高的特殊场合，可以设定较为复杂的密码算法，并设计密码算法计算器，在普通计算器或手机中内置可变密码系统，用户将复杂的密码算法输入，每次用到密码时拿出密码算法计算器时临时计算一下就可以了。

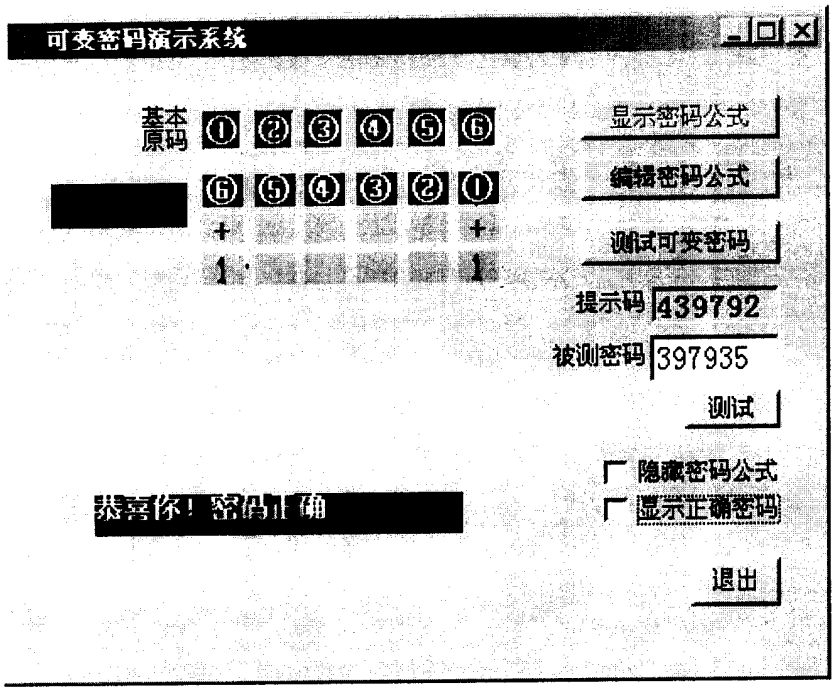
附图是可变密码方案的一个演示例子软件，基本了体现可变密码方案思路。由电脑给出一个随机原始密码字串，这里定为 6 位数字，由于这个原始密码串是随机给出的，作为用户输入自己密码时的提示码（当然也可以是日期值，不过采用随机串，更安全可靠，无须记忆）。要使用这个可变密码方案，用户事先要自定义自己的一个密码算法（加密公式），在本软件中有详尽的介绍。密码算法的主要作用是对电脑给出的随机原始密码串进行任意变换，之后生成的密码才是系统识别用户身份的真密码，当然这个密码是根据用户设定的方式变换来的，变换方式只存在用户的心中，在任何使用密码的场合都不暴露出来，所以任何人无法盗取。即使别人收集了大量的输入密码，仅根据这些信息来破解想得到密码算法（密码计算公式）也几乎不可能，因为变化太多，即使最高级的计算机，也不一定能从中找出规律。

公式的复杂性可根据用户的保密要求设置，如果是普通的金融卡，简单的变换公式就可以了。如图所示，把公式设置为“将随机原始密码串中所有数字倒序排列，首尾两个数字再加上 1”。点击“测试可变密码”按钮，系统给出一个提示码（随机码）“439792”，按照设定的密码公式，正确的密码应该是“397935”。记住这个自己定义的简单的规律，再也不必去背大量的密码了，使用密码时再也不必担心被人盗取或破解了。

该方案的可行性

用户通过各种方式将自己的密码算法（密码公式）输入识别系统就可以了，除了电脑输入外，在电话机、手机上也可以操作输入，并可以随时更改自己的密码算法（密码公式）。

在不脱离本发明精神或本质特征的基础上，本发明能够以多种形式实施。因此本发明实施例在各种情况下都被认为是示例性的而不是限制性的，本发明的范围由所附权利要求书而不是前述的说明限定，并且所有落入权利要求的等同物的意义和范围内的更改将被认为包括在权利要求内。


可变密码演示系统
基本
原码
① ② ③ ④ ⑤ ⑥
⑥ ⑤ ④ ③ ② ①
显示密码公式
编辑密码公式
测试可变密码
提示码 439792
被测密码 397935
测试
隐藏密码公式
显示正确密码
退出