(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 108140077 A
(43)申请公布日 2018.06.08

(21)申请号 201680057774.5

(22)申请日 2016.09.09

(30)优先权数据
15306588.3 2015.10.08 EP

(85)PCT国际申请进入国家阶段日
2018.04.03

(86)PCT国际申请的申请数据
PCT/EP2016/071301 2016.09.09

(87)PCT国际申请的公布数据
WO2017/060037 EN 2017.04.13

(71)申请人 汤姆逊许可公司
地址 法国伊西莱穆利诺

(72)发明人 克里斯托弗·诺伊曼
奥利维耶·赫恩 拉斐尔·盖洛兹

(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 倪斌

(51)Int.Cl.
G06F 21/31(2006.01)
H04L 29/06(2006.01)
H04L 9/00(2006.01)

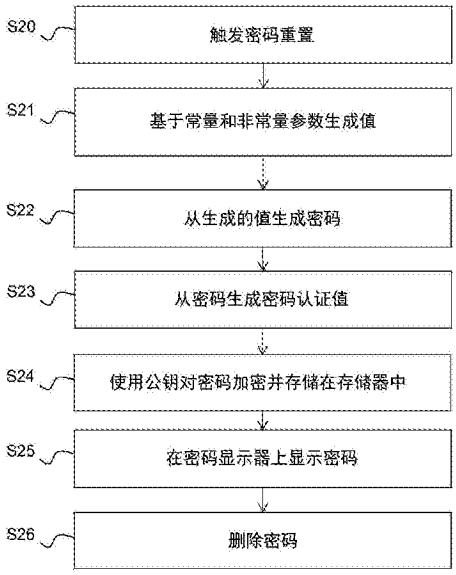
权利要求书2页 说明书4页 附图1页

(54)发明名称

用于在用户设备中生成密码的设备和方法

(57)摘要

一种设备(100)和一种密码生成方法。当密码生成被触发(S20)时，设备(100)的处理器(110)向设备(100)中或周围的常量和非常量参数应用(S21)函数以获得值，从该值生成(S22)密码。从密码生成(S23)密码认证值并存储。如果是管理员密码，则使用公钥对密码进行加密(S24)并存储；如果是网络密码，则通过单向连接将密码发送(S25)到诸如持久电子显示器(150)的存储设备，即使没有电力供应，信息也存放在该存储设备上。处理器(110)最终删除(S26)所生成的密码，以使其仅显示在显示器(150)上。



CN 108140077 A

1.一种用于生成网络密码的设备(100),所述设备(100)包括:

存储器(120),用于存储网络密码验证值;

存储单元(150),用于存储网络密码以供用户取回;以及

硬件处理器(110),被配置为:

从至少一个非静态参数生成所述网络密码;

处理所述网络密码以获得所述网络密码验证值;

将所述网络密码验证值存储在所述存储器(120)中;

通过单向连接将所述网络密码传输到所述存储单元(150);以及

在传输所述网络密码之后,从所述硬件处理器和所述存储器中的至少一个中删除所述网络密码,使得在所述设备中,所述网络密码仅由所述存储单元存储。

2.根据权利要求1所述的设备,其中所述存储单元(150)是显示器。

3.根据权利要求2所述的设备,其中所述显示器是持久显示器。

4.根据权利要求3所述的设备,其中所述持久显示器使用电子墨水或电子纸技术来实现。

5.根据权利要求1所述的设备,其中所述处理器被配置为还从至少一个静态参数生成所述密码。

6.根据权利要求1所述的设备,其中所述至少一个非静态参数包括WiFi噪声、环境温度、处理器负载以及与用户输入相关的参数中的至少一个。

7.根据权利要求1所述的设备,其中所述处理器被配置为通过从所述至少一个非静态参数获得第一值并且通过处理所述第一值以获得人类可读的文本字符串来生成所述密码。

8.根据权利要求1所述的设备,其中所述网络密码用于连接到由所述设备(100)管理的网络。

9.根据权利要求1所述的设备,其中所述网络密码是WiFi保护访问预共享密钥(WPA PSK),并且所述密码验证值是WiFi保护访问成对主密钥(WPA PMK)。

10.一种用于生成用于连接到网络的网络密码的方法,所述方法包括:在管理所述网络的设备的硬件处理器处:

从至少一个非静态参数生成(S22)网络密码;

处理(S23)所述网络密码以获得网络密码验证值;

将所述网络密码验证值存储(S23)在存储器(120)中;

通过单向连接将所述网络密码传输(S25)到所述设备的存储单元(150)以供用户取回;以及

从所述硬件处理器删除(S26)所述网络密码,使得所述网络密码仅由所述存储单元存储。

11.根据权利要求10所述的方法,其中所述存储单元(150)是显示器。

12.一种包括程序代码指令的计算机程序,所述程序代码指令可由处理器执行以实现根据权利要求10至11中至少一项所述的方法的步骤。

13.一种存储在非暂时性计算机可读介质上的计算机程序产品(160),其包括程序代码指令,所述程序代码指令可由处理器执行以实现根据权利要求10至11中的至少一项所述的方法的步骤。

14.一种设备(100),用于为所述设备生成管理员密码,所述设备(100)包括:

存储器(120),被配置为存储所述管理员密码的加密版本和管理员密码验证值;以及

硬件处理器(110),被配置为:

从至少一个非静态参数生成所述管理员密码;

处理所述管理员密码以获得所述管理员密码验证值;

将所述管理员密码验证值存储在所述存储器(120)中;

使用运营商或可信的第三方的公钥对所述管理员密码加密以获得加密的管理员密码;

将所述加密的管理员密码存储在所述存储器(120)中以供所述运营商取回;以及

删除所述管理员密码。

15.一种用于为设备生成管理员密码的方法,所述方法包括在所述设备的硬件处理器处:

从至少一个非静态参数生成(S22)所述管理员密码;

处理(S23)所述管理员密码以获得管理员密码验证值;

将所述管理员密码验证值存储(S23)在存储器中;

使用运营商或可信的第三方的公钥对所述管理员密码加密(S24)以获得加密的管理员密码;

将所述加密的管理员密码存储在所述存储器中以供所述运营商取回;以及

删除(S26)所述管理员密码。

用于在用户设备中生成密码的设备和方法

技术领域

[0001] 本公开一般性地涉及密码生成，并且具体涉及用户设备中的自动密码生成。

背景技术

[0002] 出于安全原因，许多用户设备受密码保护。这些设备包括(数字用户线，DSL)网关、电缆调制解调器和机顶盒。在下面，网关将被用作非限制性示例。

[0003] 网关通常至少有两个密码：网络密码，例如用于连接到网关管理的网络的WiFi密码(WPA(WiFi保护访问)PSK(预共享密钥)密码短语)；和用于管理网关本身的管理员密码。

[0004] 通常，每个网关都带有在制造期间设置的工厂密码。这些密码是由网关自身通过对网关内部可用的和专用于网关的信息(例如MAC(媒体访问控制)地址、序列号和加密密钥)应用基于混淆或加密(或其组合)的函数来计算的。由于函数是确定性的，并且该信息不会改变，因此即使在出厂重置后，给定设备的密码也始终相同。

[0005] 从可用性的角度来看，固定不变的密码是一个优点。由于密码不会更改，因此可以将其打印在网关上的不干胶标签上，并且用户仍可以对网关进行出厂重置，因为这不会更改密码。用户可以轻松读取网络密码以将设备连接到网关的WiFi网络，并且可以轻松读取管理员密码来管理网关。

[0006] 但是，对于安全性而言，使用固定不变的密码会造成缺陷。

[0007] 一方面，密码的熵往往很低，因为它们倾向于基于带有语义信息的固定内部值。

[0008] 另一方面，用于生成密码的所有信息都存储在网关上。这意味着能够访问网关的攻击者可以访问这些信息，除非网关典型地由可信平台模块(TPM)，或由其他昂贵的硬件保护措施进行适当保护。能够访问所有信息可以更容易地找到用于计算密码的函数。一旦攻击者找到了生成函数，就可以将其用来攻击使用相同函数的其他网关。过去，几种类型的网关遭到过这种方式的攻击，泄露了数百万个人网关的密码。

[0009] 因此希望开发一种密码生成解决方案来解决传统解决方案的至少一些问题。本公开提供了这样的解决方案。

发明内容

[0010] 在第一方面，本原理针对一种用于生成网络密码的设备。所述设备包括用于存储网络密码验证值的存储器；存储单元，用于存储网络密码以供用户取回；以及硬件处理器，被配置为从至少一个非静态参数生成所述网络密码，处理所述网络密码以获得所述网络密码验证值，将所述网络密码验证值存储在所述存储器中，通过单向连接将所述网络密码传输到所述存储单元，并且在传输所述网络密码之后，从所述硬件处理器和所述存储器中的至少一个删除所述网络密码，使得在所述设备中，所述网络密码仅由所述存储单元存储。

[0011] 第一方面的各种实施例包括：

[0012] • 存储单元是显示器。显示器可以是持久显示器，其可以使用电子墨水或电子纸技术来实现。

[0013] • 处理器被配置为还从至少一个静态参数生成密码。

[0014] • 至少一个非静态参数包括WiFi噪声、环境温度、处理器负载以及与用户输入相关的参数中的至少一个。

[0015] • 处理器被配置为通过从至少一个非静态参数获取第一值并且通过处理第一值以获取人类可读的文本字符串来生成密码。

[0016] • 网络密码用于连接到由所述设备管理的网络。

[0017] • 网络密码是WiFi保护访问预共享密钥(WPA PSK)，并且密码验证值是WiFi保护访问成对主密钥(WPA PMK)。

[0018] 在第二方面，本原理针对一种用于生成用于连接到网络的网络密码的方法。管理网络的设备的硬件处理器从至少一个非静态参数生成网络密码，处理所述网络密码以获得网络密码验证值，将所述网络密码验证值存储在存储器中，通过单向连接将所述网络密码传输到所述设备的存储单元以供用户取回，并且从所述硬件处理器删除所述网络密码，使得所述网络密码仅由所述存储单元存储。

[0019] 在第二方面的一个实施例中，存储单元是显示器。

[0020] 在第三方面，本原理针对一种包括程序代码指令的计算机程序，所述程序代码指令可由处理器执行以实现第二方面的方法的步骤。

[0021] 在第四方面，本原理针对一种存储在非暂时性计算机可读介质上的计算机程序产品(160)，其包括程序代码指令，所述程序代码指令可由处理器执行以实现第二方面的方法的步骤。

[0022] 在第五方面，本原理针对一种设备，其用于为所述设备生成管理员密码。该设备包括：存储器，被配置为存储管理员密码的加密版本和管理员密码验证值；以及硬件处理器，被配置为从至少一个非静态参数生成所述管理员密码，处理所述管理员密码以获得所述管理员密码验证值，将所述管理员密码验证值存储在所述存储器中，使用运营商或可信的第三方的公钥对所述管理员密码进行加密以获得加密的管理员密码，将所述加密的管理员密码存储在所述存储器中以供运营商取回以及删除所述管理员密码。

[0023] 在第六方面中，本原理涉及一种用于为设备生成管理员密码的方法。所述设备的硬件处理器从至少一个非静态参数生成所述管理员密码，处理所述管理员密码以获得管理员密码验证值，将所述管理员密码验证值存储在存储器中，使用运营商或可信的第三方的公钥对所述管理员密码进行加密以获得加密的管理员密码，将所述加密的管理员密码存储在所述存储器中供运营商取回，并删除所述管理员密码。

附图说明

[0024] 现在将参照附图通过非限制性实例描述本原理的优选特征，其中：

[0025] 图1示出了实现本原理的设备；以及

[0026] 图2示出了根据本原理的优选实施例的用于密码生成的方法。

具体实施方式

[0027] 图1示出了实施本原理的网关(仍用作非限制性示例)100。网关100包括至少一个硬件处理单元(“处理器”)110、外部或内部(或两者的组合)存储器120、被配置为使用例如

WiFi技术通信的第一(本地)网络接口130、以及用于与诸如互联网服务器之类的前端系统(head-end)通信的第二(外部)网络接口140。网关还包括密码显示器150。密码显示器是持久显示器,优选地使用诸如电子墨水、电子纸或只有在更新显示器时才吸收能量的其他无源显示器技术。本领域技术人员将会理解,为了清楚起见,所示设备是非常简化的,因此没有示出诸如内部连接和电源之类的特征。非暂时存储介质160存储具有指令的至少一个计算机程序,所述指令在由处理器执行时执行如图2所示的密码生成方法。

[0028] 如前所述,网关至少使用两个密码:网络密码和管理员密码。除非明确说明,否则解决方案适用于两者。

[0029] 图2示出了根据本原理的优选实施例的用于密码生成的方法。

[0030] 在步骤S20中,触发新密码的生成。这优选通过用户按下网关上的工厂重置按钮或另一个按钮来完成。

[0031] 在步骤S21中,处理器110使用优选用几个熵源提供种子的密码伪随机数发生器来生成值,这些熵源例如:

[0032] • 网关内部的并且通常特定于网关的静态参数,诸如其MAC地址、序列号和加密密钥,以及

[0033] • 非静态参数,诸如WiFi噪音、环境温度、处理器负载以及与用户输入相关的参数(例如,按下按钮的时间)。

[0034] 所生成的值被临时存储在存储器120中。

[0035] 在步骤S22中,优选地进一步处理该值以获得密码。此处理可以格式化密码以便将密码呈现为可以在显示器上打印的字符串。例如,任何二进制序列都可以格式化为用户更容易读取的十六进制字符串。对于WiFi,密码是WPA-PSK;对于管理员密码,优选是明文密码。

[0036] 一旦获得密码,在步骤S23中,从密码生成密码验证值并将其存储在存储器120中。

[0037] 对于网络密码,使用单向函数从密码导出密码验证值并将其持久存储在存储器120中以实现对连接到网络的设备的认证。在WiFi情况下,密码验证值是从WPA PSK和SSID计算出的所谓的WPA PMK(成对主密钥)。WPA PMK=some hash function(WPA PSK,SSID)。更确切地说:WPA PMK=PBKDF2(密码短语,SSID,4096,256),其中PBKDF2是一种如RFC2898中所指定的标准化方法,用于从密码短语导出密钥。

[0038] 对于管理员密码,密码优选地被盐化和散列,并且得到的密码验证值被持久地存储在存储器120中,以实现对尝试管理网关的用户的验证。

[0039] 请注意,密码的处理方式取决于认证协议。如果使用HTTP摘要认证,则可以简单地对密码进行散列处理而无需任何盐化。另一方面,对于安全远程密码协议(SRP),则存储盐化散列。

[0040] 在步骤S24中,使用运营商的公钥(通常是为网关提供互联网访问的运营商)对生成的密码进行加密。另一种可能性是使用可信第三方的公钥。然后将加密的密码持久存储在存储器120中。

[0041] 然后,如果需要的话,运营商可以使用例如所谓的TR-069来取回加密的密码,并使用其相应的私钥来解密加密的密码,从而获得明文的密码。

[0042] 在步骤S25中,用生成的密码更新密码显示器150。

[0043] 在步骤S26中，从存储器120中删除密码。

[0044] 需要注意的是，网关既不知道管理员密码也不能获得此信息，但网关能够验证输入密码，并且运营商可以取回密码的明文版本。对于网络密码，网关不存储并且无法获取密码WPA PSK，但它知道密码验证值WPA PMK，因此能够验证输入密码是正确的。

[0045] 在一个变型中，专门布置的存储器取代了密码显示器。存储器经由单向连接连接到网关，使得网关能够将密码写入存储器(可能作为文本文件)，但不能从存储器中读取它。有几种方法来实现。例如，存储器可以具有两个接口，第一接口仅被布置为从网关接收数据(即，密码)，第二接口被布置为将数据输出到另一个设备，诸如计算机。进一步的可能性是USB记忆棒，在该记忆棒上写入密码后，接口被禁用，直到进一步生成密码。

[0046] 在另一个变型中，处理器使用用户的智能手机或平板电脑的公钥(该智能手机或平板电脑存储相应的私钥)来加密密码。这样加密的密码然后能够经由无线接口传输到智能手机或平板电脑上存储，或者进一步传输到云端以存储在那里。然后可以通过智能手机或平板电脑取回此加密的密码，并使用私钥解密，使得用户可以使用该密码。

[0047] 应该理解，本原理可以提供在用户设备中提供安全密码重置机制的解决方案。

[0048] 说明书和(在适当的情况下)权利要求和附图中公开的每个特征可以独立地或以任何适当的组合提供。描述为以硬件实现的特征也可以用软件来实现，反之亦然。在权利要求中出现的附图标记仅仅是为了说明而且对权利要求的范围没有限制作用。


网关
处理器 110
存储器 120
密码显示器 150
本地网络接口 130
外部网络接口 140
160
100

图1

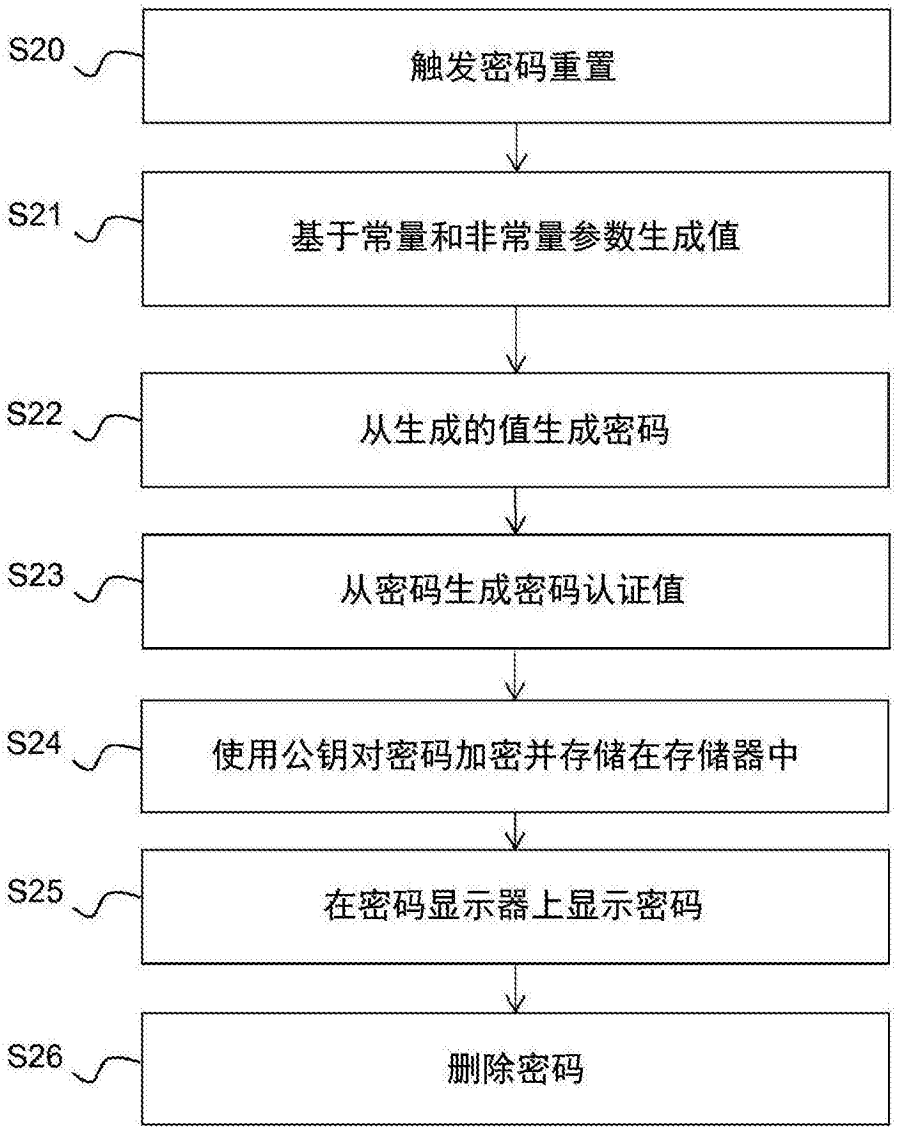

S20
触发密码重置
S21
基于常量和非常量参数生成值
S22
从生成的值生成密码
S23
从密码生成密码认证值
S24
使用公钥对密码加密并存储在存储器中
S25
在密码显示器上显示密码
S26
删除密码

图2