(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 107111699 A
(43)申请公布日 2017.08.29

(21)申请号 201580057458.3

(22)申请日 2015.10.21

(30)优先权数据
14306675.1 2014.10.22 EP

(85)PCT国际申请进入国家阶段日
2017.04.21

(86)PCT国际申请的申请数据
PCT/EP2015/074325 2015.10.21

(87)PCT国际申请的公布数据
WO2016/062749 FR 2016.04.28

(71)申请人 源讯科技公司
地址 法国伯宗

(72)发明人 斯特凡娜·科希 昆廷·阿拉默卢

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 梁丽超 田喜庆

(51)Int.Cl.
G06F 21/31(2013.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04L 29/06(2006.01)

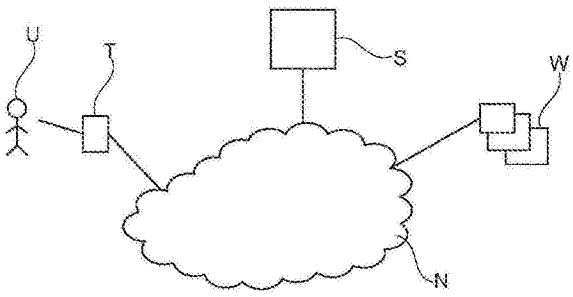
权利要求书1页 说明书11页 附图1页

(54)发明名称

通过印记评估通信终端采集的信息的置信水平

(57)摘要

本发明涉及一种由通讯终端(T)根据印记集合确定采集信息置信水平的方法，步骤包含：确定关联接近性标准和所述集合中每个印记的规则；通过所述通信终端(T)，根据所述规则和所述采集到的信息为所述集合的每个印记确定一个部分秘密；通过所述通信终端(T)，根据所述部分秘密计算总体得分，所述总体得分代表所述置信水平。



CN 107111699 A

1.一种由通讯终端(T)根据印记集合确定采集信息置信水平的方法,步骤包含:

-确定关联接近性标准和所述集合中每个印记的规则;

-通过所述通信终端(T),根据所述规则和所述采集到的信息为所述集合的每个印记确定一个部分秘密;

-通过所述通信终端(T),根据所述部分秘密计算总体得分,所述总体得分代表所述置信水平。

2.一种由通讯终端(T)根据印记集合确定采集信息置信水平的方法,步骤包含:

-确定关联接近性标准和所述集合中每个印记的规则

-通过所述通信终端(T),根据所述规则和所述采集到的信息为所述集合的每个印记确定一个部分秘密;

-通过所述通信终端(T),根据所述部分秘密计算总体秘密,所述总体秘密用来确保已达到所述置信水平。

3.根据权利要求1或2中任一项所述的方法,某些所述印记被存储在所述通信终端(T)和所述用户(U)的数据中。

4.根据前述权利要求中任一项所述的方法,其中所述数据属于一个群组,所述群组包含IMEI识别码、SIM卡识别码、操作系统识别码、安装在所述通信终端(T)内的软件应用列表、所述用户(U)的联系人列表、所述通信终端(T)已知的网络列表、所述通信终端(T)的地理定位、所述通信终端(T)的电池电量、个人数据、数字证书、U盘、生理数据或者所述用户(U)的手写签名。

5.根据前述权利要求中任一项所述的方法,其中所述终端(T)预先接收待加入所述印记集合的印记指标。

6.根据前述权利要求中任一项所述的方法,其中所述规则传输至所述通信终端(T)。

7.根据前述权利要求中任一项所述的方法,包含一个预先注册的阶段,在此阶段个人资料信息与每个印记相关联,并确定每个印记的初始部分秘密。

8.一种认证方法,为某个已知服务在认证服务器(S)认证通信终端(T)的用户(U),包括:

-一个预先注册阶段,其中根据前述权利要求确定第一总体秘密;

-一个认证阶段,其中根据前述权利要求确定第二总体秘密;

-根据所述第一和第二总体秘密确定是否认证所述用户。

9.一种包含运算装置的通信终端(T),用于为印记集合中每个印记确定部分秘密,借助所述规则,所述集合的每个印记与接近性标准相关联,所述运算装置用于根据所述规则和所述通信终端(T)采集的信息确定所述部分秘密,以及用于根据部分秘密计算总体得分;所述总体得分表示根据所述印记集合采集信息的置信水平。

10.包含至少一台根据前述权利要求的通信终端(T)和一个认证服务器(S)的系统,它们由一个通信网络(N)连接。

通过印记评估通信终端采集的信息的置信水平

技术领域

[0001] 发明涉及通过预先建立的印记集合，评估通过通信终端采集的信息的置信水平。

[0002] 发明应用于在认证服务器上认证通信终端(通常是手机)用户，通常用于互联网上的电子商务领域。

背景技术

[0003] 电子商务正在飞速发展，尤其是凭借技术装置的普及和线上供应量的增加。总的来说，电子商务催生了支付机制和其它需要识别通信终端用户的机制，从而能够将用户列入商务行为中(以及相应的金钱交易)。

[0004] 这样的交易需要双方相互信任。因此需要对终端的用户进行认证。

[0005] 这种交易应当经过认证，来防止恶意行为，尤其是侵权和身份盗用。此外，确保一定等级的充分认证能够消除用户的疑虑从而增加线上交易的营业额。

[0006] 采用能够确保一定等级的充分认证的机制，这点非常重要。

[0007] ANSSI(国家信息系统安全局)特别推荐进行较强的认证方式，也就是说依靠至少两项下列认证因素：

[0008] -记忆因素，AF1(人们已知的)：例如密码、出生日期等等。

[0009] -物质因素，AF2(人们获得的)：例如芯片、数码证书、U盘等。

[0010] -生理生物识别因素，AF3(人们自有的)：例如指纹、瞳孔特征、语音签名等。

[0011] -行为因素AF4(人们所做的)：例如手写签名等。

[0012] 然而，同样重要的是，这些机制不能因为实施或使用起来过于复杂而对线上交易造成阻碍，或者可能意味着带来较高的成本，尤其是因为使用特定的设备。

[0013] 并且，通常来说，数字数据的认证通常基于散列函数或者密码机制。这样的方法可有效应用于密码、出生日期或SIM卡编号等，或者其它完全限定的数据，也就是说不接受任何哪怕是微小的变化。

[0014] 然而，有些数据可以接收变化：例如在手写签名的情况下，签名不可能始终完全一致。对此类数据应用散列函数或者编码机制不能获得预期效果，因为输入时微小的差别可能造成输出时具有判断上的差别。因此，如果我们想要尝试使用惯用的密码机制(例如密码系统、散列函数等)来保护认证，那么具有轻微差别的手写签名可能会造成无法认证用户。

发明内容

[0015] 本发明的目标在于提供一个至少能够部分解决所述问题的认证方法。

[0016] 出于此目的，本发明提供一种方法，用于根据印记集合确定通信终端采集信息的置信水平，所述方法包含以下步骤：

[0017] -确定关联接近性标准和所述集合中每个印记的规则；

[0018] -通过所述通信终端，根据所述规则和所述采集到的信息为所述集合的每个印记确定一个部分秘密；

[0019] -通过所述通信终端，根据所述部分秘密计算总体得分，所述总体得分代表所述置信水平。

[0020] 本发明的另一个方面涉及一种根据印记集合确定由通信终端关联采集信息的置信水平的方法，所包含的步骤为：

[0021] -确定关联接近性标准和所述集合中每个印记的规则；

[0022] -通过所述通信终端，根据所述规则和所述采集到的信息为所述集合的每个印记确定一个部分秘密；

[0023] -通过所述通信终端，根据所述部分秘密计算总体秘密，所述总体秘密用来确保已达到该置信水平。

[0024] 根据实施例，本发明包含下列一种或多种特征，这些特征可以单独或部分组合或全部组合运用：

[0025] -某些所述印记被存储在所述通信终端和所述用户的数据中；

[0026] -所述数据属于一个群组，群组包含IMEI识别码、SIM卡识别码、操作系统识别码、安装在所述通信终端内的软件应用列表、所述用户的联系人列表、所述通信终端已知的网络列表、所述通信终端的地理定位、所述通信终端的电池电量、个人数据、数字证书、U盘、生理数据或者所述用户的手写签名；

[0027] -所述终端预先接收待加入所述印记集合的印记指标；

[0028] -将所述规则传输至所述通信终端；

[0029] -程序包括一个预先注册阶段，该阶段中个人资料信息和每个印记相结合，并且先为每个印记限定一个初始部分秘密。

[0030] 本发明的另一个方面涉及一个认证方法，为某个已知服务在认证服务器认证通信终端的用户，包括：

[0031] -根据所述权利要求，包括一个预先注册阶段，期间已限定第一总体秘密；

[0032] -根据所述权利要求，包括一个认证阶段，期间已限定第二总体秘密；

[0033] -根据所述第一和第二总体秘密限定是否认证所述用户。

[0034] 本发明的另一方向涉及一台包含运算装置的通信终端，用于为印记集合中每个印记限定部分秘密，借助所述规则，所述集合的每个印记与接近性标准相关联，所述运算装置用于根据所述规则和所述通信终端采集的信息限定所述部分秘密，以及用于根据部分秘密计算总体秘密，所述总体秘密用于确保达到所述置信水平。

[0035] 根据实施例，本发明还包括预先接收待加入所述印记集合的印记指标的装置。

[0036] 本发明的另一方面涉及一个系统，系统包含至少一台如前所述的通信终端和一个连接至通讯网络的认证服务器。

[0037] 因此，本发明能够通过预先建立的印记集合评估通信终端采集信息的置信水平。

[0038] 本发明能够提供一种方法，无需使用客户端专用的实体设备。该方法完全可以通过市面上已有的通信终端和服务器上布置的软件模块来实现。

[0039] 下文将提到，根据本发明的这一方法还能够通过使用接近性标准，考虑到某些印记的固有变化。

[0040] 此外，本发明还能够考虑到尊重隐私的方面，不会将任何敏感数据(有关隐私)传播到通信终端以外，因为有关这些数据的所有操作都在通信终端本体上进行，并且将始终

不会传输至服务器或者通信终端以外的外部实体。此处我们所说的有关隐私的敏感数据既指有关用户的数据也是指有关通信终端本体的数据。

[0041] 并且，任何关键值(注册时的印记值、部分秘密、总体秘密等)都不会存储在终端上，这当然是安全性方面的优势。例如，如果终端被盗，终端设备将无法访问任何被盗后的印记值，当然也无法访问注册时的印记值。因为印记可能同时为设备使用的印记和用户本身的印记，盗窃者将无法从新获得正确的总体秘密，因此也无法获得认证。

[0042] 通过阅读下文对本发明优选实施例的说明，借助示例和附图，可了解本发明的其它特征和优势。

附图说明

[0043] 图1为可以加入本发明的背景示例的示意图。

[0044] 图2为本发明可能实施例的方框图。

具体实施方式

[0045] 正如上文所述，本发明尤其适用于通信终端的用户和服务提供商之间进行交易的认证领域。

[0046] 并且也可以用于其他应用，例如电子保险箱等。事实上，电子保险箱也在于密码层面的敏感数据。因此也存在数字密钥的存储问题。所以，如果我们将此解密钥匙视作(或者关于)总体密钥(或总体秘密)，那么本发明能够解决此问题，并且重建总体密钥，从而完全解码数据并无需再长期存储数据。

[0047] 下文的说明涉及认证机制更为具体的示例，但是所展现的原理是可以进行归纳并用于其它应用的。

[0048] 在图1显示的示例中，用户U使用一台通信终端T，该终端与通讯网络N连接。此通讯网络可以用互联网代表：网络可能为下文未曾说明的多种网络的集合(接入网络、主干网或“骨干网”)，本发明可以独立于隐藏通讯架构而应用。

[0049] 通信终端T通常可以为移动通信终端(包括“智能手机”或数码平板电脑类型的终端)。也可以为例如台式电脑或手提电脑等终端。

[0050] 凭借此通讯网络N，通信终端可以与服务提供商W建立通信。此服务提供商W通常为商业网站，能够让用户U实行商业交易，通常为购买服务或商品。服务提供商W也可以为处理敏感信息的网站：例如用户可以查看账户的银行网站等。

[0051] 在通信网络上与服务提供商W进行交易的情况下，通常，为确保用户U的身份，需要通过认证服务器S进行认证。

[0052] 一般来说，该认证服务器S不同于服务提供商W。尤其可能在多种不同商业网站上同时进行商业交易的情况下。在“可靠的”服务提供商(例如银行)的情况下此认证服务器S可能纳入供应商本身。

[0053] 根据使用本发明的情况和应用的类型或服务，所希望获得的置信水平也有所不同。例如：

[0054] -高置信水平可能涉及对于至少一方(用户或服务提供商)具有高风险。例如，连接银行机构网站，或重要商业交易和/或转换银行信息的情况。

[0055] -较低的置信水平可能涉及风险较低的应用。可能为转账受限的账户或银行卡进行小金额支付,或者使用低敏感服务的情况。

[0056] 此外,对于同一个应用,如果用户在近期已经经过认证,可能需要较低的置信水平。

[0057] 根据服务以及所期待的置信水平,可以确定安全政策。

[0058] 此安全政策通常可以定义使用印记的集合。既定服务确立印记可以参考图1方框图中的S1。

[0059] 这些印记可以全部为保密信息(也就是说第三方无法知晓或复制),从而能够以独一无二的方式识别和确保用户的安全性。可以根据前文所述的认证因素分类为AF1、AF2、AF3和AF4。

[0060] 这些印记依靠用户U和/或用户使用的终端T的数据。因此,我们可以确保置信水平既关系到终端也关系到终端的用户。

[0061] 在认证应用的情况下,本发明可以认证终端T的用户U。因此,可以认证用户,或者认证终端,或者认证使用某终端的用户。这样可以确定是否为已知用户使用非惯用终端,并且如有需要在此情况下进行特殊处理。这样可以检测到对终端T的攻击。也可以确定是否为非惯用用户在使用已知终端,并且如有希望在此情况下进行特殊处理。

[0062] 可以用作印迹的所涉数据可以属于一个群组,该群组包含:

[0063] -终端T的IMEI识别码(国际移动设备标识),

[0064] -SIM(用户标志模块)卡的编码或识别码,

[0065] -操作系统的识别码:此识别码不仅表示所使用的操作系统(iOS、Android、Windows、Linux等)而且还可以表示版本,

[0066] -安装在通信终端T上的软件应用列表,

[0067] -用户U的联系人列表,特别是终端T或远程账户(“Google”联系人等)上的目录,

[0068] -通信终端T的已知网络列表,例如WIFI网络,

[0069] -通过蓝牙网络配对的设备列表,

[0070] -通信终端T的地理定位,

[0071] -通信终端T的电池电量,

[0072] -个人数据,例如生日,配偶姓名等,

[0073] -数字证书,

[0074] -包含安全信息的U盘,

[0075] -生物识别数据,例如指纹、瞳孔特征、语音签名等,

[0076] -用户U的手写签名……

[0077] 印记也可以为其它数据。随着通信网络和终端的技术发展,还可能出现别的印记数据。

[0078] 某些印记为生物识别印记,其它印记有关通信终端的软件或设备方面。根据本发明,此处印记的概念比严格的生物识别印记的含义更为广泛。

[0079] 在极端情况下,可以采用唯一印记;但是在一般情况下,可以使用多种印记进行组合来确定是否认证终端T的用户U。

[0080] 某些印记以独一无二和加密的方式来识别用户U,例如密码,或者用于识别终端T,

例如IMEI。

[0081] 其它印记无法达到这一程度，例如地理定位或者电池电量水平。在本发明的范围内，无法仅使用这些印记来认证终端的用户，但是把它们组合起来则可以构成一组相符的组合，可以从而确定认证。下文将详细说明此机制。

[0082] 对于每个印记，可以根据接近性标准定义其规则。这些规则可以包含在前述安全政策中。

[0083] 这一接近性标准的目的在于能够间接地测量所涉印记的第一值和第二值之间的差距，更准确地说，我们也将在下文详细叙述，分别为注册阶段确定的第一值，和属于之后通信终端采集信息的第二值。

[0084] 通过下文说明的部分秘密的计算，本发明涉及的机制无需直接比对即能够确保同一印记的两个值以接近性标准来看足够相近。事实上所谓的直接比对是不可行的，因为根据本发明，印记的值并未被存储。

[0085] 此接近性标准取决于印记的性质：

[0086] -对于地理位置，接近性标准可以为地理上的接近(地理距离)。

[0087] -对于字符链(密码、名字等等)，接近性标准可以为两个字符链的字符数量不同。

[0088] -对于电池电量，接近性标准可以为百分比的差别。这可以根据使用概况定义。

[0089] -对于指纹，可以使用图像分析算法来生成表示两个图像之间差距的度量指标。

[0090] -对于联系人列表或者安装的应用程序，接近性标准可以为两个列表中的元素数量。

[0091] -等等

[0092] 印记的性质(距离类型或是度量类型等)定义接近性标准。通常，还包含一个限定阈值或者间隔的值(也就是说容差极限)。

[0093] 对于某个既定性质，阈值根据印记而不同。例如，密码和通信地址为字符链，但是这两者都可以采用通过阈值识别的接近性标准(对于通信地址我们可以容忍误值，但是对于密码则不可以)；因此标准的性质是相同的(即两个字符链之间的差别)。

[0094] 一般来说，根据本发明的实施例，我们可以根据接近性标准的性质将印记分为4类：

[0095] -“静态”类：涉及例如SIM编号、IMEI识别码类型的参数：是指静态印记的值，不能容忍任何变化。为了计算部分秘密，我们也可以将它们应用在常用的密码程序中。

[0096] -“白名单”类：操作系统版本、内核版本等：印记的值应该包含在给定列表中(该列表应保持不公开)。

[0097] -“列表”类：联系人列表、已知网络等：第一和第二值应该相差不大。

[0098] -“欧氏距离”类：地理定位、电池电量等：印记第一值和第二值欧氏距离应小于某个阈值；

[0099] -“生物识别”类：严格意义上的生物识别印记(声音、虹膜、指纹、手写签名、步态等)每一种都需要专门处理。没有一个接近性标准可以将其分类。因此不能根据前述四类进行分类。每个具体情况都需要具体处理。

[0100] 根据所期望的服务和认证等级，根据已限定的安全政策和根据前文的描述，可能会考虑不同印记的集合。

[0101] 更具体地说，对于不高的认证登记，会考虑较少数量的印记或者较为简单的印记。如果印记不涉及用户U的操作(输入密码或者PIN码等)，则为简单印记。

[0102] 此外，用于印记的接近性标准也可以取决于期待的置信水平：该水平越高则接近性标准越严格。例如，对于“姓名”、“地址”类字符链的输入，我们可以根据所期待的置信水平容忍较大或较小的字符差距。

[0103] 加入印记集合的印记指标可以根据所期待的服务(也就是认证等级)由认证服务器S提供。也可以由服务提供商W(银行、电子商务网站等)提供。这些指标可让通信终端确定应该处理哪些印记(密码、生物识别密码等)。

[0104] 根据本发明的实施例，应该进行先决性的第一步：注册。这一步骤可参见图2中的S2。

[0105] 该步骤涉及对每个予以考虑的印记部分公开个人资料信息。此处个人资料因为是根据每个印记定义的，所以是部分资料。更准确地说，这个步骤涉及生成每个印记的部分秘密，也就是说可以涉及该印记的部分得分。

[0106] 认证机制可以包含这种先决性步骤，该步骤涉及发起对终端T的用户U的认证机制。这是一种启动方法，在这种方法中用户自行提供信息进行注册。

[0107] 在此注册步骤中，用户可以输入个人信息(姓氏、名字、出生日期、地址等)、初始生物识别信息或“个人资料”信息(手写签名等)、密码等等，这些将构成予以考虑的印记的集合中的至少某些印记的个人资料信息。

[0108] 以自动以及如有需要为透明的方式，通信终端也可以通过相应软件装置为其它印记(地理定位、安装的应用列表、联系人列表、SIM卡识别码、已知网络列表、电池电量、操作系统识别码等)提供个人资料信息。

[0109] 根据本发明，这些印记的值不会传输至通信终端T以外，也不会存储在通讯终端上，而是仅用于确定部分秘密。

[0110] 基于印记的值，初始部分秘密可以在步骤S2时确定，并且纳入个人资料信息。这个密码被称作“部分”是因为它关系到安全政策使用的印记集合中的唯一一个印记。

[0111] 总体秘密也可以由初始部分秘密根据安全政策确定。总体秘密能够证明总体得分，总体得分是根据部分秘密计算的。

[0112] 这里“总体”一词的含义涉及密码和得分关系到由安全政策限定的印记集合。

[0113] 总体秘密是一种密钥。在总体秘密的找回时，才能在终端上认证用户。事实上，因为总体秘密是所包含的值不能改变的密码钥匙，我们可以将其应用在标准密码程序中(密码系统、散列函数等)。

[0114] 在既定背景下，通过赋予总体得分一个阈值可以决定设备的置信水平。然而，不论由谁来确认是否达到某个得分，都应该能够确保已经确实达到了该得分。总体秘密能够带来确实达到该得分的数学证明。此总体秘密的重建事实上获得此总体得分的必要条件。

[0115] 因此，这些初始密码，不论部分还是总体秘密，都是与后期操作阶段确定的部分和总体秘密进行隐性比较的基础。这种能够提供一个得分的隐性比较能够评估置信水平。

[0116] 我们已经了解值是不会被存储的，那么通过隐性比较，就意味着我们不能直接进行比较。但是，是否能够成功重建总体秘密决定了是否能够间接地比较初始个人资料、注册时建立的个人资料和后期操作阶段中建立的个人资料中印记的值。

[0117] 确定初始密码的机制和在操作阶段确定密码(部分或总体)的机制是相同的:为了更为方便和表达更为明确,将仅在接下来的说明中详细展开,该机制与操作阶段的机制一致。

[0118] 当之后使用服务时(例如,连接至电子商务网站或银行网站等),展开严格意义上的操作阶段。

[0119] 该阶段包含了步骤S3,确定每个印记的部分秘密。

[0120] 步骤S3包含一个通过通信终端T采集信息的分步骤。它涉及向用户U请求和获取信息(密码等),或者向终端T自动获取信息。此分步骤类似于在注册时用于确定个人资料信息而进行的过程部分。

[0121] 采集到的信息(至少)对应所涉及的印记,并构成这些印记的第二值。

[0122] 因此,在这一阶段,我们已经隐性地掌握每个印记的个人资料信息(第一值)和采集到的信息(第二值)。

[0123] 然而,这些印记的值和部分秘密都不能直接获取;根据安全政策,只有进行总体秘密的找回才能确保达到总体分数,以及根据安全政策才能确保部分秘密的有效性,从而保证其中值的有效性。

[0124] 步骤S3涉及在采集信息的基础上展开用于确定每个印记部分秘密的规则驱动器。

[0125] 这些规则可以传输到通信终端T上。因此,终端应用规则经过实例化的安全政策,但是终端本身并不决策。

[0126] 更确切地说,部分秘密的确定用于将这些规则根据涉及每个印记的接近性标准独立地应用于对每个印记采集到的信息。

[0127] 在已经通过同样的方式预先确定了部分初始密码的情况下,通过总体秘密的找回并通过确定得分,可以进行隐性的比较;得分表现了在哪些情况下印记被识别,以及代表了该印记在采集信息中的置信水平。

[0128] 于是我们在步骤S4中确定是否认证用户U,或者更广泛地说,采集到的信息是否已达到足够的置信水平。事实上,如果所有部分秘密能够根据安全政策带来有效的总体秘密,那么我们可以确保已达到要求的置信水平。

[0129] 这个步骤涉及与认证过程相关的使用情况。在其他应用的范围内,该步骤应该以合理地方式配合使用部分秘密。

[0130] 当然也存在其它操作方式,但是通常采用“模糊提取器”来运行规则,模糊提取器用来通过已经采集到的信息或者个人资料信息和接近性标准确定部分秘密。规则详细说明了在哪种情况下,所采集到的信息会被识别为与个人资料信息“等效”,因为规则会生成相同的部分秘密。本发明的这一方面及其示例将在后文中说明。

[0131] 有关模糊提取器的完整说明可参照发明者的文章《模糊提取器:如何从生物识别和其它噪声数据生成强密钥(Fuzzy Extractors:How to Generate Strong Keys from Biometrics and Other Noisy Data)》,作者Yevgeniy Dodis、Leonid Reyzin和Adam Smith,发表于《密码学的发展(Advances in Cryptology)-Eurocrypt 2004》(ISBN978-3-540-21935-4)。

[0132] 例如,对于某已知印记,步骤S3中,按照相应的接近性标准,验证采集的信息是否足够接近于印记的初始值(即个人资料值)。如果接近,那么得分为正。相反,得分为负。

[0133] 得分可以属于一个值的离散区间，并且通过指明在什么范围内可识别印记来表示置信水平。

[0134] 然而，只有在重建总体秘密时，也就是步骤S4时，才能表现出是否具有正确得分。

[0135] 例如，结合得分所得的值，我们可以指定一个临界，也就是说确定某个印记不符是否是“致命”的。步骤S4时，不能识别致命印记则将自动造成无法认证终端T的用户U。但是非致命印记的不一致则不会造成这样的结果，我们可以考虑一定数量的非致命印记不一致才造成无法认证。

[0136] 下表为使用本发明的具体实例，表中采用了两种印记：联系人列表和应用列表。

[0137] 需再次提醒的是，根据本发明，不存在印记值之间的直接比较，但是下列示例展现了如何按照搜索结果确定一个准确的接近性函数，也就是说如何定义分类认可印记的范围和非认可印记的范围的接近性函数。

[0138]

印记	致命/非致命	容差极限	初始值或个人资料
联系人列表L	致命	3	C1,C2,C3,C4,C5, C6,C7,C8,C9,C10
应用列表	非致命	10	A1,A2,A3....An

[0139] 在本示例中，我们假设采用适用于联系人列表L_{ctc}的模糊提取器fe，可以生成相关的部分秘密S_{ctc}，以及根据L_{ctct}得出的相关部分公开个人资料信息IP_{ctc}和错误数量容差(此处为3)：

[0140] $(S_{ctc}, IP_{ctc}) = fe.generateEnrollmentValues(L_{ctc}, 3)$。

[0141] 如上所述，部分秘密S_{ctc}并不是长期存储的，但是IP_{ctc}是被存储的，因为不会泄露的任何关键信息。然后将根据下文所述IP_{ctc}将被用于重新计算部分秘密。

[0142] 在此我们假设在认证阶段印记的采集信息为：

[0143] L'_{ctc}=C1,C2,C'3,C4,C5,C6,C7,C8,C9,C'10

[0144] 此处两个联系人的采集信息和个人资料值不同：C'3和C'10。而此印记的容差极限为3，也就是说3个不同才会生成负得分。所以此处确定的得分为正得分；可以通过下列重新计算得出的相关部分秘密得以确认：

[0145] $S_{ctc} = fe.generateAut|enticationValue(L'_{ctc}, IP_{ctc})$

[0146] 此处，为了更清楚地说明，我们将前述发明者文章中的Gen和Rep程序分别重新命名为generateEnrollmentValues和generateAuthenticationValue

[0147] 相反地，如果采集到的信息为：

[0148] L*ctc=C'1,C2,C'3,C4,C5,C6,C7,C8,C'9,C'10

[0149] 此处差别为4个联系人，高于容差极限。我们可以确定得分为零或者为负甚至为致命。部分秘密($S^*_{ctc} = fe.generateAuthenticationValue(L^*_{ctc}, IP_{ctc})$)与注册时的$(S_{ctc})$不相等；所以因为安全政策的规定，将该印记定义为“致命”，因此不能重组有效的总体秘密。

[0150] 此外我们假设在认证阶段，应用列表的采集信息与个人资料值相差11个应用。但是此处只能确定得分为零或为负，而不是致命的。虽然相关的部分秘密仍然无效但不会阻碍正确的总体秘密的重建。

[0151] 根据此具体实例，建议实行以下机制：

[0152] -考虑三种印记:“致命”类的“联系人列表”,“非致命”类的“操作系统”和“应用列表”;

[0153] -“联系人列表”设4分;另外两个设3分。

[0154] -需达到的总体得分为5分;总体得分等于部分得分的总和。

[0155] -如果印记无效,也就是说所生成的部分秘密与已知部分秘密不一致,则分数为0;

[0156] -规则规定至少有一个有效的联系人列表(致命)和其它两个印记中(非致命)至少一个有效。

[0157] 通过获得正确的总体秘密来认证用户,条件是:

[0158] -三个印记全部有效,那么3个部分秘密都与注册时相同,得分为10分。

[0159] -印记“联系人列表”有效和另外两个印记中只有一个有效;那么只有两个部分秘密有效,其中包含致命类别的;得分为7分。

[0160] 但是,尽管两个印记“操作系统”和“应用列表”都有效,也就是获得了正确的部分秘密,但是不知道联系人列表是否无效,用户有可能被认证。

[0161] 在这种情况下,可获得6分(也就是说大于等于应达到的底限5分),但是如果根据先前建立的规则(即联系人列表属于“致命”类别)则仍然不能认证。那么,重建的总体秘密无法等于已获得的总体秘密。

[0162] 因此对于用户认证有利的场景必须是得分大于等于期待值,并且能够生成相同的证明置信水平和符合所提规则的总体秘密。

[0163] 如前所述,也可以使用其它印记。适用的模糊提取器应该根据印记类型考量。

[0164] 印记“操作系统识别码”也可以使用,因为通常同一台终端T只关联一个操作系统。根据安全政策,操作系统的改变(注册和认证时的不同)可能会造成得分为负或致命。

[0165] 操作系统识别码也可以包含版本编号。我们可以假设变化到更高版本(“升级”)是正常的行为,生成正得分;但是相反的向更低版本的变化则是可疑的,应该得分为负甚至视为致命。

[0166] 处理印记“手写签名”需要采用一种图像分析的算法。这种算法应该可以基于个人资料的签名和采集到的签名之间的接近性的测量而得到分数。为此,算法应该无需对细微的图像差异过于敏感,但是应该建立微小和重大的图像差异之间的阈值。

[0167] 在步骤S4中,按照对应印记集合中的印记的部分秘密,可以建立总体秘密,并且通过与初始总体秘密对比和表示对比结果的分数,能够确定终端T的用户U是否能得到认证。

[0168] 总体秘密的建立可以通过前文所述的规则驱动器实现。

[0169] 我们可以考虑印记集合中的一部分为“致命”型,一部分为“非致命”型。那么,可以生成一个“致命”型的总体秘密和一个“非致命”型的总体秘密。“致命”型整体秘密的构成为“致命”型部分秘密级联的散列函数的应用;“非致命”型整体秘密的构成符合未找回的“非致命”型部分秘密的可容忍误差数量的模糊提取器的输出,由安全政策规定容忍的误差数量的最大值。

[0170] 我们认为通过调整本发明机制的不同参数可实现不同政策,也就是说调整容忍阈值、印记的临界等等。

[0171] 通过机制的“模糊”特征,我们可以考虑具有一定变化性的印记,如手写签名等。

[0172] 也可以考虑新的印记,例如地理定位、电池电量等等,将它们与接近性原则和合理

的阈值相关联即可。这些新的印记能够丰富认证策略、带来新的可能性。

[0173] 本发明的机制可以在认证应用的范围内采用不同的架构操作。

[0174] 第一步中，认证服务器S根据安全性策略预先将用于所需服务的印记指标集合传输至通信终端T。

[0175] 终端T可以实施步骤S3，该步骤涉及确定每个印记的部分秘密，以及对应注册阶段的步骤S2。

[0176] 确定用户U是否被认证的步骤应当包括：

[0177] -根据部分秘密由终端T计算一个“总体”秘密，一部分在注册阶段期间计算，另一部分在操作阶段期间计算。

[0178] -在两个阶段中都将该密钥传输至认证服务器S。

[0179] -由服务器S根据两个密钥值确定是否认证用户。

[0180] 这个方法意味着用户U和服务器S之间存在一条安全信道。该方法的不便之处在于对于另一个服务器而言，可能会将服务器S视作用户U。

[0181] 此外，根据另一种实施例，步骤S4可以由终端计算密钥(即总体秘密)构成。根据此实施例，密钥不会被传输至认证服务器S，而是借助“知识证明”和“零知识证明”(英文术语分别为“proof of knowledge”和“zero knowledge proof”)的密码程序来确定是否认证用户。总的来说，根据这种实施例，终端T可以向认证服务器提供以下公共值：

[0182] -服务器S确信终端T了解总体密钥的值与注册时计算的值相同，如果没有所述总体密钥则不会提供该值。

[0183] -服务器S无法使用公共值，既不能“猜测”总体密钥值，也不能再次运用知识证明确信其了解总体秘密(或总体密钥)。

[0184] 此总体秘密或者总体密钥可以通过应用部分秘密集合的函数进行运算。然后可以与在注册阶段建立的个人资料值进行对比，从而确认是否认证。

[0185] 该函数可以为简单的部分秘密级联的散列函数。这一操作可以用于与“致命”得分相关的印记。只要部分秘密不同于个人资料值，那么总体秘密也不同，从而在此例中，不能认证。

[0186] 相同地，根据实施例，对于总体秘密的计算，一种方法是运用前文所述的“致命”类型的部分秘密，另一种方法是可以运用“非致命”部分秘密，方法如下：如果“较大”数量(由安全性策略定义“较大”)的部分秘密与注册时计算的部分秘密相对应，那么借助例如适用于“非致命”部分秘密的模糊提取器可以找回总体秘密。

[0187] 这种操作可以用于与“非致命”得分相关的印记。因此如果一个(或多个)部分与注册值不同，根据安全性策略，总体秘密保持不变，从而举例来说，能够生成认证。

[0188] 本发明可以根据该印记的接近性标准，并且在根据达到认证最低置信水平的容差极限以内，使用能够考虑印记值变化的终端认证用户。

[0189] 即使用户的某些印记无法符合容差极限，但是只要印记的有效性不是必要的(也就是说属于“非致命”类型)，本发明就还可以认证用户。

[0190] 我们也可以采用其它方法。通常，考虑方法时需根据需要实施的认证策略，并且根据部分得分(正/负、致命/负/正、值的连续谱等等)可以采用的值。

[0191] 本发明可以避免向发明以外的设备传输个人数据，本发明涉及一个认证服务器或

对等式交易或电子商务网站范畴内的另一个终端或者另一套设备。

[0192] 实际上可以根据一种策略(策略可以通过认证服务器或者其它设备传输)在本地处理个人数据;并且一个综合信息例如总体秘密(或密钥),根据本实施例,在保证尊重用户的隐私的情况下可以被传输至通信网络。

[0193] 另外,需要再次说明的是,注册印记值和部分秘密都不会存储在终端上,这可以确保更高的安全性:如果有攻击者盗窃了终端,那么因为这些值没有存储,所以他通过查看终端内存是不能找回印记/部分秘密值的。

[0194] 通信终端T限于应用接收到的规则,来首先确定部分秘密然后确定总体秘密或密钥。终端不能"作弊"通过无效印记找回正确的密钥。

[0195] 密钥既代表终端T也代表用户U(也就是说,代表个人资料信息和采集信息之间的一致),但是密钥不能重新识别用来生成密钥的信息(也就是印记值),从而保证了秘密性。

[0196] 因此,个人数据(密码、出生日期、联系人列表等)不会被传输:这不仅需要符合越来越严格的国家和国际机构的规定,而且对于用户的隐私和安全也是一种保护。

[0197] 实际上,如果认为有攻击者破坏了认证服务器,那么在本实施例有关零知识证明的情况下,攻击者无法获取用户的个人资料:只有总体秘密的知识证明才能找到个人数据,但是这种证明不能用来找回总体秘密并且不可"再次使用",所以对于攻击者无法使用该证明。

[0198] 此外,个人数据的不传输可以达到额外的安全等级。事实上,信道上传输的数据越少,非法截获和使用信息的风险越低。

[0199] 因此,本发明能够完全尊重用户隐私,避免信息被侵犯的风险。此外,密钥也不会被存储,用户的终端上不会有任何敏感信息,这也能够在终端被偷或丢失的情况下增加安全性。

[0200] 而且,终端T确保按照传输至终端的规则执行,在此之前终端并不了解规则。此机制也能够有利于本发明方法的稳定性。

[0201] 此外,本机制对于用户是透明的:部分秘密是由终端上装载的软件模块根据已存储或用户U当即提供的信息自动确定的。

[0202] 此外,如果通信终端在本地进行非常复杂的处理的情况下,本方法可以节省时间和提高处理效率:因为只有很少数量的数据通过通信网络传输。

[0203] 当然,本发明并不仅限于本文说明和描述的实施例,专业人士可以了解多种变化形式。

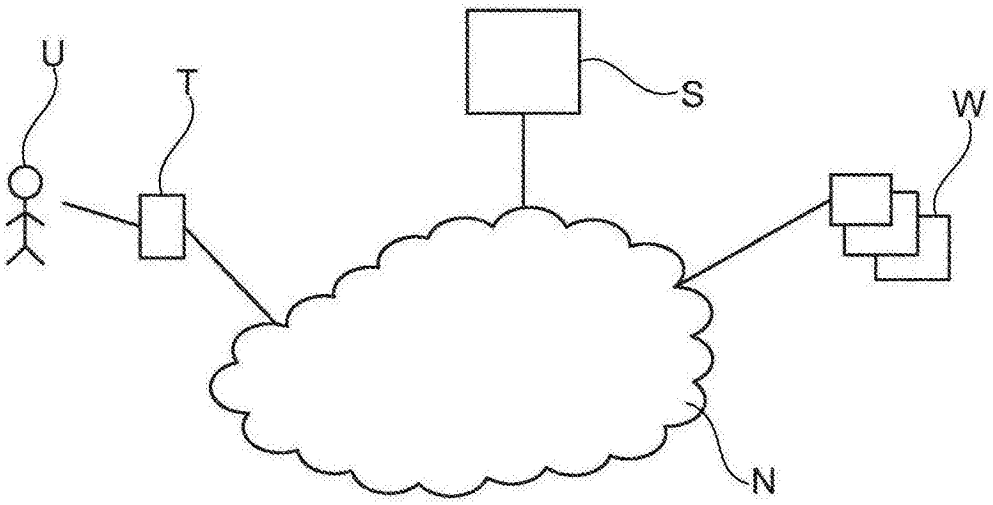


图1

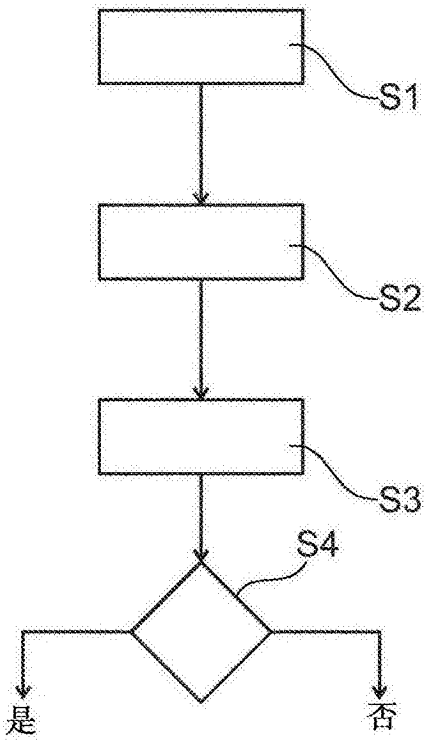


图2