



(12) 发明专利

(10) 授权公告号 CN 1859096 B

(45) 授权公告日 2011.04.13

(21) 申请号 200510100660.8

(22) 申请日 2005.10.22

(73) 专利权人 华为技术有限公司

地址 518129 广东省深圳市龙岗区坂田华为
总部办公楼

(72) 发明人 位继伟 郑志彬 李超

(51) Int. Cl.

H04L 9/32 (2006.01)

G06K 9/00 (2006.01)

(56) 对比文件

CN 1520090 A, 2004.08.11, 说明书第 6 页第 6
段至第 11 页第 1 段。

审查员 姚雅倩

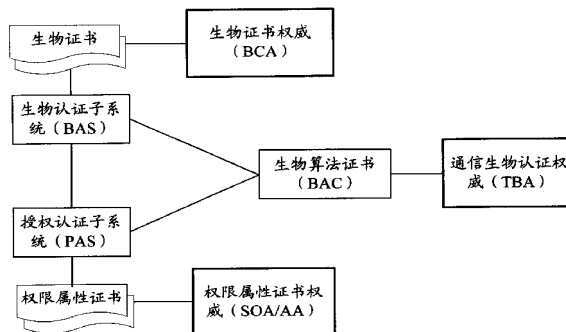
权利要求书 1 页 说明书 6 页 附图 2 页

(54) 发明名称

一种安全认证系统及方法

(57) 摘要

本发明适用于网络安全领域，提供了一种安全认证系统及方法，所述安全认证系统包括：权限认证子系统，用于输出对用户身份进行生物识别认证所需要的用户属性参数信息；生物算法证书，用于保存与所述用户属性参数信息对应的生物识别参数信息；以及生物认证子系统，用于获取所述生物识别参数信息，并根据所述生物识别参数信息对用户身份进行生物识别认证。本发明将生物认证与 PMI 权限认证进行结合，提高了 PMI 中身份认证的安全性，同时扩大了生物认证的适用范围。



1. 一种安全认证系统，其特征在于，所述安全认证系统包括：

权限认证子系统，用于输出对用户身份进行生物识别认证所需要的用户属性参数信息；所述用户属性参数信息包括权限属性信息，以及与所述权限属性信息对应的安全级别信息；

生物算法证书，用于保存与所述用户属性参数信息对应的生物识别参数信息；以及

生物认证子系统，用于获取所述生物识别参数信息，并根据所述生物识别参数信息对用户身份进行生物识别认证。

2. 如权利要求 1 所述的安全认证系统，其特征在于，所述生物识别参数信息包括生物特征类型标识、生物识别算法标识以及安全级别和生物识别相关参数对应列表；

所述安全级别和生物识别相关参数对应列表包括安全级别信息以及与所述安全级别信息对应的识别门限。

3. 如权利要求 1 所述的安全认证系统，其特征在于，所述生物识别参数信息进一步包括用户权限信息。

4. 一种安全认证方法，其特征在于，所述方法包括下述步骤：

A. 输出对用户身份进行生物识别认证所需要的用户属性参数信息；所述用户属性参数信息包括权限属性信息，以及与所述权限属性信息对应的安全级别信息；

B. 获取与所述用户属性参数信息对应的生物识别参数信息；

C. 利用所述生物识别参数信息对用户身份进行生物识别认证。

5. 如权利要求 4 所述的安全认证方法，其特征在于，所述生物识别参数信息包括生物特征类型标识、生物识别算法标识以及安全级别和生物识别相关参数对应列表；

所述安全级别和生物识别相关参数对应列表包括安全级别信息以及与所述安全级别信息对应的识别门限。

6. 如权利要求 4 所述的安全认证方法，其特征在于，所述生物识别参数信息进一步包括用户权限信息。

一种安全认证系统及方法

技术领域

[0001] 本发明属于网络安全领域，尤其涉及一种通过生物识别进行安全认证的系统及方法。

背景技术

[0002] PMI (Privilege Management Infrastructure, 授权管理基础设施) 是 PKI (PublicKey Infrastructure, 公钥基础设施) 的扩展，是一种通过为用户发放权限属性证书为其提供享有访问某些受保护资源的特权的机制。一个用户可以有多个权限属性证书，分别表明其拥有的各种权限。一般地，一个申请访问某个资源的用户持有特定的权限属性证书，PMI 系统在验证其权限属性证书的合法性之前，先要确定其身份的真实性，即先需要其进行身份认证，身份认证通过后才进行权限属性验证，验证通过，就给予用户访问相关资源的权利，否则拒绝服务。

[0003] 生物认证是利用人的生物特征，如指纹、虹膜、语音及签名等进行身份认证的一种手段。随着计算机技术的发展以及各种算法的不断改进，生物认证技术作为一种准确、快速和高效的身份认证方法越来越广泛地应用于各种安全领域。

[0004] 现有的 PMI 中，以用户口令或者密钥配合 PKI 公钥进行身份认证，由于用户口令或密钥容易被黑客通过各种方法来破译，从而对网络安全造成威胁。与此相比，生物认证具有安全、不易攻破等特点，因此将生物认证和 PMI 相结合，利用生物识别对用户身份进行认证，可以增强 PMI 认证的安全性。

发明内容

[0005] 本发明目的在于解决现有技术中 PMI 认证中通过用户口令或者密钥配合 PKI 公钥对用户身份进行认证时安全性比较低的问题。

[0006] 为实现上述发明目的，本发明提供了一种安全认证系统，所述安全认证系统包括：

[0007] 权限认证子系统，用于输出对用户身份进行生物识别认证所需要的用户属性参数信息；所述用户属性参数信息包括权限属性信息，以及与所述权限属性信息对应的安全级别信息；

[0008] 生物算法证书，用于保存与所述用户属性参数信息对应的生物识别参数信息；以及

[0009] 生物认证子系统，用于获取所述生物识别参数信息，并根据所述生物识别参数信息对用户身份进行生物识别认证。

[0010] 所述生物识别参数信息包括生物特征类型标识、生物识别算法标识以及安全级别和生物识别相关参数对应列表；

[0011] 所述安全级别和生物识别相关参数对应列表包括安全级别信息以及与所述安全级别信息对应的识别门限。

[0012] 所述生物识别参数信息进一步包括用户权限信息。

[0013] 为了更好地实现发明目的，本发明进一步提供了一种安全认证方法，所述方法包括下述步骤：

[0014] A. 输出对用户身份进行生物识别认证所需要的用户属性参数信息；所述用户属性参数信息包括权限属性信息，以及与所述权限属性信息对应的安全级别信息；

[0015] B. 获取与所述用户属性参数信息对应的生物识别参数信息；

[0016] C. 利用所述生物识别参数信息对用户身份进行生物识别认证。

[0017] 所述生物识别参数信息包括生物特征类型标识、生物识别算法标识以及安全级别和生物识别相关参数对应列表；

[0018] 所述安全级别和生物识别相关参数对应列表包括安全级别信息以及与所述安全级别信息对应的识别门限。

[0019] 所述生物识别参数信息进一步包括用户权限信息。

[0020] 本发明将生物认证与 PMI 权限认证进行结合，提高了 PMI 中身份认证的安全性，同时扩大了生物认证的适用范围。

附图说明

[0021] 图 1 是本发明提供的通过生物识别进行安全认证的系统架构示意图；

[0022] 图 2 是本发明提供的通过生物识别进行安全认证的系统结构；

[0023] 图 3 是在本发明的提供的一个实施例中对用户进行安全认证的实现流程图；

[0024] 图 4 是在本发明的提供的另一个实施例中对用户进行安全认证的实现流程图。

具体实施方式

[0025] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0026] 图 1 示出了本发明提供的基于生物认证的安全认证系统的框架结构。该系统将基于生物证书的 BAI (Biometric Authentication Infrastructure, 生物认证基础设施) 和 PMI 相结合，实现对用户的身份认证和权限认证，尤其适用于安全级别要求不高的领域。

[0027] CA (Certificate Authority, 认证中心)、BCA (Biometric Certificate Authority, 生物证书权威)、SOA (Source of Authentication, 信任源点)、TBA (Telebiometric Authority, 通信生物认证权威) 都是可信任的权威机构。

[0028] CA 为 PKI 中负责产生、分配并管理数字证书 (公钥证书) 的可信赖的第三方权威机构，是 PKI 安全体系的核心环节，通常采用多层次的分级结构。上级认证中心负责签发和管理下级认证中心的证书，最下一级的认证中心直接面向最终用户。

[0029] SOA 为 PMI 中的中心业务节点，也是整个 PMI 中的最终信任源和最高管理机构，负责授权管理策略的管理、应用授权受理、AA (Attribution Authority, 属性权威机构) 中心的设立审核及管理以及授权管理体系业务的规范化等。

[0030] AA 是 PMI 的核心服务节点，是对应于具体应用系统的授权管理分系统，与 SOA 中心通过业务协议达成相互的信任关系，负责应用授权受理、权限属性证书的发放和管

理，以及 AA 代理点的设立审核和管理等。AA 需要为其所发放的所有权限属性证书维持一个历史记录和更新记录。

[0031] BAI 是使用生物证书对用户身份进行认证的基础设施，其基础要素是生物证书和数字签名。用户提供生物证书和生物特征数据给认证系统，认证系统根据 BAC (Biometric Algorithm Certificate, 生物算法证书) 提供的生物识别参数进行生物识别认证。

[0032] BAC 负责保存各种生物识别算法、识别门限、安全认证级别等生物识别参数，可以保存为目录形式，或者由验证服务器保管。

[0033] TBA 是为各种生物识别算法进行权威认证的可信任第三方机构。TBA 为经过其认证的生物识别算法颁发 BAC。

[0034] BCA 为 BAI 中颁发包含数字签名和生物特征模板的生物证书的第三方权威机构。

[0035] 生物识别认证的结果通过判断生物特征匹配结果在是否有效范围内来得到，因此使用的是近似匹配，而不像密码系统那样进行精确匹配。决定生物识别的有效性因系统不同而不同，取决于生物特征的类型和系统使用的生物识别算法。在生物识别算法中，识别门限一个重要的参数值，生物识别算法通过识别门限可以实施生物识别。识别门限影响识别结果的精确度，即不同的门限设置，可能会导致生物识别算法的识别结果发生变化。

[0036] 所有的生物认证都有一个可配置参数：误接收率 (FAR) 和误拒绝率 (FRR)。FAR 是衡量用户本应该遭受拒绝却被系统接受的参数，FRR 是衡量用户本应该被系统接受却遭到拒绝的参数。FAR 和 FRR 相互制约，而 FAR 和 FRR 的大小又直接由识别门限决定。如果用严格的策略使非法用户进入系统的可能性 FAR 减少以提高系统安全级别，就需要提高识别门限，那么合法用户被拒绝的概率 FRR 就增加。如果减少系统拒绝合法用户的可能性 FRR，就需要降低识别门限，那么非法用户得到授权的概率 FAR 就增加，认证系统的安全级别也相应的降低。

[0037] 在基于 BAI 认证的 PMI 系统中，在逻辑上 BAI 和 PMI 是相对独立的，但是在结合生物认证的 PMI 应用系统中使用权限证书进行授权服务时，二者又相互关联。BAI 中身份的创建和维护是独立于 PMI 的，BAI 的建立往往早于 PMI。基于生物证书的 BAI 对用户进行身份认证时，必须能够获得可信任生物识别参数如生物识别门限。因此在 BAI 建立的同时必须建立可提供生物识别参数的生物证书目录 BAC。

[0038] 图 2 示出了实现本发明的认证系统的结构。生物认证子系统 (Biometric Authentication System, 简称 BAS) 和授权认证子系统 (Privilege Authentication System, 简称 PAS) 分别是应用 BAI 和 PMI 对用户身份和用户权限进行安全认证的系统，PAS 与 BAS 之间通过 BAC 实现结合。PAS、BAS 实现属于现有技术，形式可以有多种，本发明不作具体描述。

[0039] 在本发明中，PAS 提供生物认证所需要的用户属性参数，BAC 根据 PAS 提供的用户属性参数向 BAS 提供与用户属性参数对应的生物识别参数，BAS 根据 BAC 提供的生物识别参数选择相应的生物识别算法，利用生物证书对用户的生物特征数据进行验证，从而实现对用户身份的识别认证。PAS 对通过身份认证的用户进行权限认证。

[0040] 生物证书是绑定了用户身份和生物特征数据并经过数字签名的数据结构，BCA 是颁发生物证书的权威机构。

[0041] 作为本发明的一个实施例，PAS 提供生物认证准确度参数，对 BAS 的生物识别认证进行指导，以满足对具有不同安全级别权限的用户进行身份认证的要求。该生物认证准确度参数是 PAS 根据被访问资源的安全性要求而作出的。

[0042] 为了结合生物认证，本发明对 PMI 的权限属性证书进行修改，将生物认证所需要的用户属性参数加入权限属性证书中，具体可以放在权限属性证书的扩展信息中。属性证书的扩展信息主要是声明和证书应用相关的一些策略信息。

[0043] 作为本发明的一个实施例，在权限属性证书的扩展信息中加入属性安全级别列表，即证书中所声称的各权限属性对应的安全级别列表，该安全级别直接反映了生物认证结果的置信度。

[0044] 属性安全级别列表参考结构如下：

[0045] Attribute Security Level List(属性安全级别列表)

[0046] {

[0047] Privilege attribute(权限属性)；

[0048] Security Level(安全级别)；

[0049] }

[0050] 在支持角色的属性证书中，角色所对应的权限属性也有一个属性安全级别列表，以便权限验证者获知该权限要求的安全级别。

[0051] 相应的，BAC 包含一个安全级别和生物识别相关参数对应列表，记录不同生物类型的不同识别算法所对应的不同的生物识别参数。BAC 的目录结构参考如下：

[0052] Biometric Type Identifier(生物特征类型标识) -> Biometric AlgorithmIdentifier(生物识别算法标识) -> Security Level BioRef List(安全级别和生物识别相关参数对应列表)。

[0053] Security Level BioRef List Structure(安全级别和生物识别相关参数对应列表结构)

[0054] {

[0055] Security Level(安全级别)；

[0056] Threshold Value(识别门限)；

[0057] Other BioRef(其他参数)；

[0058] }

[0059] 其中，生物特征类型标识指示生物识别采用何种生物特征类型，例如指纹、虹膜、语音等。

[0060] 生物识别算法标识指示出针对一种生物特征类型，采用何种识别算法。

[0061] 安全级别和生物识别相关参数对应列表指示在某安全级别下对应的在特定识别算法下的生物识别参数。具体关于生物识别参数的描述可以参考 NISTIR6529: Common Biometric Exchange File Format(CBEFF) 中的描述和定义。在本发明的一个实施例中，生物识别参数为识别门限。

[0062] 以下通过两个实施例具体描述 BAS 和 PAS 结合实现身份和权限认证过程：

[0063] 结合图 3 对实施例一进行详细说明如下：

[0064] 用户请求访问某特定资源，BAS 和 PAS 系统分别向用户发送身份认证和权限认证请求；

[0065] 1. 用户响应 BAS 的身份认证请求，协商认证方式，并发送生物证书；

[0066] 2. 在执行 1 的同时，用户响应 PAS 的权限认证请求，声明对资源的访问权限，并发送权限属性证书；

[0067] 3. BAS 根据协商的认证方式和生物识别算法向 BAC 发送生物识别参数如识别门限的请求；

[0068] 4. 在执行 3 的同时，PAS 根据用户声明的权限将权限属性证书中的用户属性参数信息，例如该用户的权限属性所对应的安全级别发送给 BAC；

[0069] 5. BAC 根据 3 中的参数请求和 4 发送的安全级别，检索到 3 中请求的参数发送给 BAS；

[0070] 6. BAS 根据 BAC 提供的生物识别参数对用户身份进行识别认证，如果身份认证通过则进行由 PAS 对用户权限进行验证，否则直接拒绝；

[0071] 7. 如果身份认证和权限认证全部通过，则用户可以按照其声称的权限访问资源。

[0072] 结合图 4 对实施例二进行详细说明如下：

[0073] 用户请求访问某特定资源，BAS 和 PAS 系统分别向用户发送身份认证和权限认证请求；

[0074] 1. 用户响应 BAS 的身份认证请求，协商认证方式，并发送生物证书；

[0075] 2. 在执行 1 的同时，用户响应 PAS 的权限认证请求，声明对资源的访问权限，并发送权限属性证书；

[0076] 3. PAS 将权限属性证书中的用户属性参数信息，例如该用户的权限属性所对应的安全级别发送给 BAS；

[0077] 4. BAS 根据安全级别和用户协商生物认证方式；

[0078] 5. BAS 根据协商好的认证方式，确定生物识别算法，并向 BAC 发送生物识别参数如识别门限的请求，发送请求时携带生物识别类型、识别算法和属性安全级别等相关参数；

[0079] 6. BAC 根据 5 中请求携带的参数，检索到与请求匹配的生物识别参数发送给 BAS；

[0080] 7. BAS 根据 BAC 提供的生物识别参数对用户身份进行识别认证，如果身份认证通过则进行由 PAS 对用户权限进行验证，否则直接拒绝；

[0081] 8. 如果身份认证和权限认证全部通过，则用户可以按照其声称的权限访问资源。

[0082] 在实施例一中，BAS 和 PAS 间交互较少，BAS 和 PAS 系统相对独立运行，BAS 没有参考访问权限的安全级别就直接与用户协商认证方式。在实施例二中，BAS 和 PAS 间交互较多，BAS 进行身份认证时参考了访问权限安全级别后再与用户协商认证方式。两个实施例可以根据实际情况来选择适用，也可以根据具体情况设计其他认证方式。

[0083] 在本发明中，也可以通过生物算法证书的扩展信息中加入 PMI 认证所需要的权限信息来实现 BAI 和 PMI 的结合，具体过程不再赘述。

[0084] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

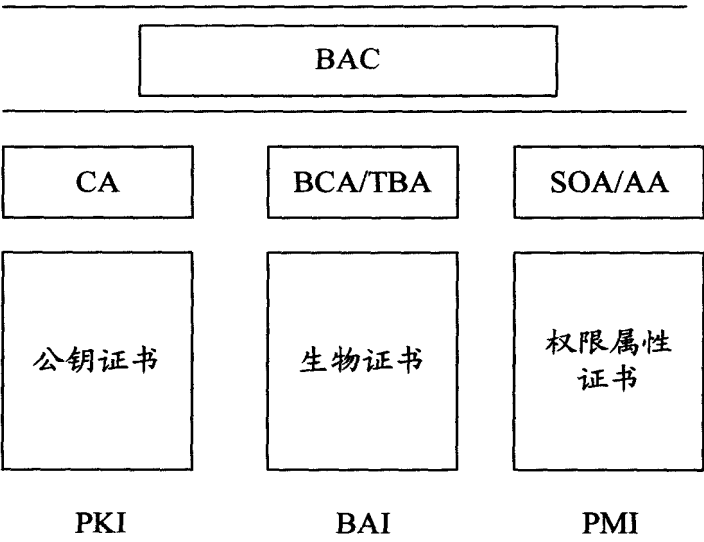


图 1

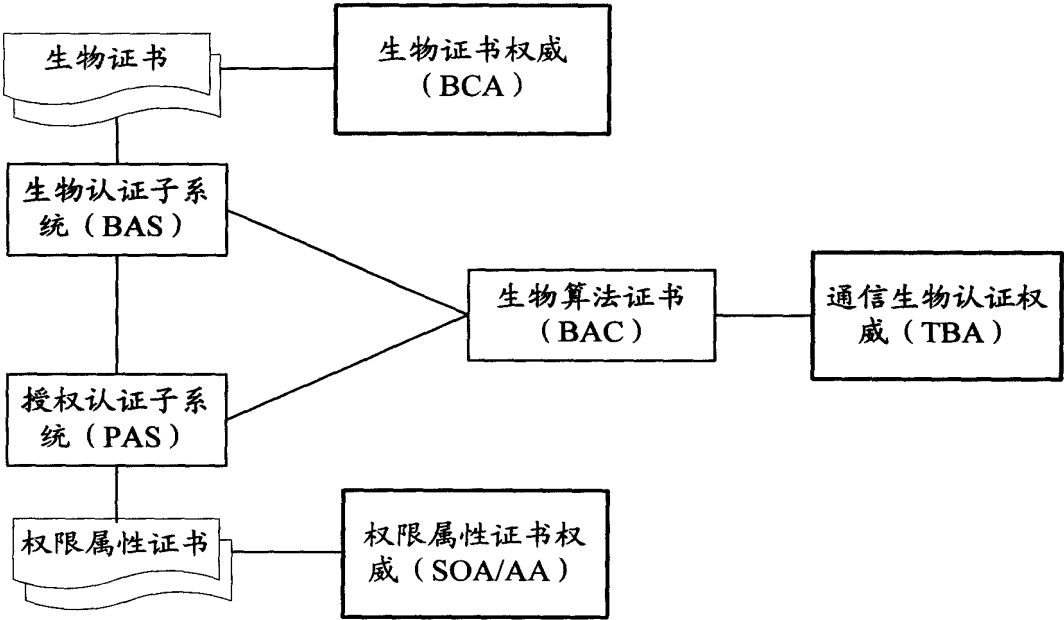


图 2

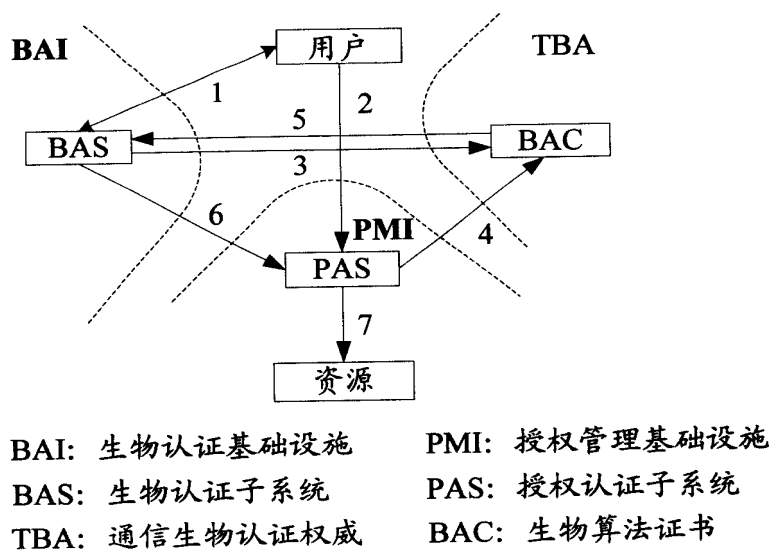


图 3

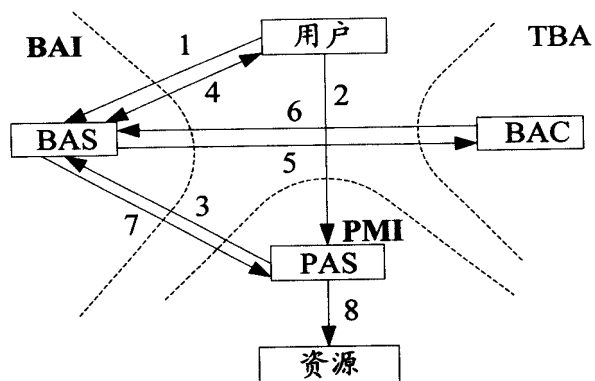


图 4