基于 PKI 的生物认证电力安全系统

李 科[1],展 巍[2],张 伟[2]

(1.信息产业部电子第六研究所 研究生部,北京 100083;
2.北京六所和瑞科技发展有限公司,北京 100083)

摘 要:将 PKI 技术和生物认证相结合,提出了基于生物证书的身份认证和权限管理的生物认证系统,相对原来单一基于 PKI 的认证系统具有更高安全性。

关键词:PKI;PMI;生物认证;生物证书

中图分类号:TP302.1;TP311.5 **文献标识码**:A

Electricity security system of biometric authentication based on PKI

LI Ke[1], ZHAN Wei[2], ZHANG Wei[2]

(1 Graduate Department, The Sixth Research Institute(Electronics) of MII, Beijing 100083, China;
2.Beijing Sriharvest Technology Development Co., Ltd., Beijing 100083, China)

Abstract: This paper presents a certificate authentication and rights management of bio-authentication system with combination of PKI technology and bio-based certificate, corresponding to the original single PKI-based authentication systems with higher security.

Key words: public key infrastructure; privilege management infrastructrue; biometric authentication; biological certificate

随着国家电力信息网的建设,电力工业中网络应用的数量不断增加,信息技术给电力工业发展带来了诸多便利的同时,也将其负面影响波及到了电力系统。随着计算机、网络等技术的蓬勃发展,信息技术的软件和硬件环境均发生了巨大的变化,电力工业的信息安全已成为影响电力系统稳定运行的主要问题。公网上的黑客和病毒的日益盛行,在电力系统通信网络中也发现了黑客活动的踪迹。与此同时,电力工业市场化改革使得具备潜在攻击能力和知识的内部用户数量增加,内部攻击威胁不容忽视。因此,电力工业的信息安全已成为影响电力系统稳定运行的重要问题。

电力工业信息安全包括电网调度自动化、配电网自动化、厂站自动化、电力市场运营、企业管理信息系统等有关生产、经营、管理的各个方面。研究范围包括信息网络安全体现结构、安全需求与策略分析、基础支持系统的时间与应用、信息系统与业务系统的安全保障措施、系统的安全评估和容侵能力等多个方面[1]。

本文结合生物认证系统,对用户访问电力信息系统的身份认证和访问控制提出了基于公钥基础设施的访问安全解决方案。

1 访问安全技术分析

1.1 PKI

对于传统的电力企业应用系统,认证和授权功能都嵌在应用(提供特定功能的程序集合)的内部,增加了应用的复杂性。对于用户来说,需要设定多个用户名和口令,因此,在使用中很容易混淆。而对于管理者而言,需要多个管理者来管理用户名/口令列表和接入控制列表,增加了管理的费用,并且各个管理者各自为政,很难使用通用的安全策略。

公共密钥基础设施 PKI (Public Key Infrastructure)可以部分地解决以上的问题。PKI 是一种运用非对称密码技术实施并提供安全服务的具有普遍适用性的网络安全基础设施。作为一种基础安全平台,PKI 能为各种不同安全需求的用户提供各种不同的安全服务。目前 PKI 可以提供的安全服务包括:身份认证、数据保密性、数据完整性、不可抵赖性等。用户可以利用 PKI 所提供的这些安全服务,进行安全电子交易、电子政务等服务。PKI 可以提供认证、完整性和机密性等核心服务,还可支撑

安全通信、安全时间戳、公正、不可否认等服务。这时认证功能放到了应用的外部，但是授权功能(即接入控制列表的管理)仍然需要嵌入到应用中。此时的用户从设定和记忆多个用户名、多个口令中解放出来，用户只需设定、记忆单个用户名和单个口令[2]。

1.2 生物认证技术

生物特征认证是指通过验证人的生理或行为特征来确认身份，一般应该满足以下4点要求：

(1)普遍性：每个人都应该拥有该特征。

(2)唯一性：两个人之间不存在相同的该特征。

(3)稳定性：这种特征至少在一段时间内是不变的。

(4)可采集性：该特征可以定量采集。

在实际应用中，很难找到能够同时满足以上所有条件的生物特征。同时，对于一个实际应用系统，还要考虑一些其他指标，例如：

(1)性能：包括识别准确率，识别速度，系统鲁棒性，系统所需资源和影响系统性能的因素等。

(2)可接受性：指用户对系统的接受度。

(3)可欺骗性：用欺诈的方法骗过系统的难易度。

因此，一个实际的生物特征识别系统应做到以下3点：

(1)在合理的资源需求下实现可接受的识别准确度和速度。

(2)对人没有伤害而且可为人们所接受。

(3)对各种欺诈方法有足够的防御性。

目前人们研究和使用的生物特征识别技术主要有：指纹识别、人脸识别、虹膜识别、掌形识别、掌纹识别、签名识别、语音识别、键击识别等。

2 生物特征认证技术

2.1 生物认证系统基本框架

身份认证验证者根据用户的生物特征数据、生物证书BC、生物算法证书BAC、生物设备证书BDC和系统的环境、策略设置等对用户进行身份认证。基于生物证书的生物认证系统框架如图1所示。

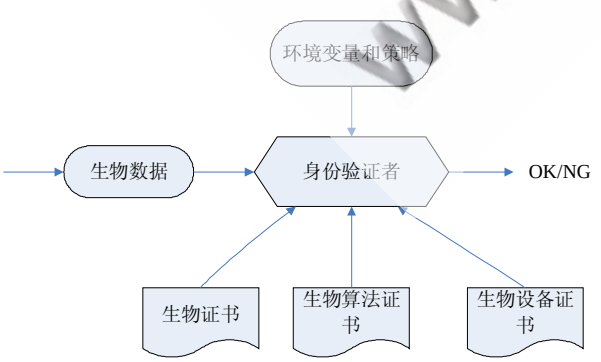

图1 生物认证系统基本框架

身份验证者(IDV)是对用户进行身份验证的部分。IDV根据采集的用户生物数据及其生物证书，结合生物算法证书、系统环境变量和策略设置等对用户进行身份认证。系统环境变量和测试对于身份认证系统十分重要。认证系统的安全级别可以由系统直接设置也可以由扩展定义后属性证书提供。系统的生物识别算法可以由系统直接设定也可以根据生物算法证书确定。同时，生物认证系统内的各种相关设备必须保证其安全性。基于组件的生物认证系统，最大的优点就是能够将各个组件灵活地结合运用起来，实现满足客户不同需求的应用系统[3]。

2.2 结合PKI技术的生物认证机制

基于生物认证系统基本认证模型，将生物识别技术和PKI技术融合，创建了一种新的生物认证系统。根据认证系统进行生物比对匹配的位置不同，设计了2种不同的实现方法。

客户端进行生物比对匹配的认证系统的工作流程如图2所示，具体步骤如下：

(1)用户通过客户端向应用服务器申请服务。

(2)客户端和服务端设备互相发送生物设备证书，验证对方的生物认证设备是否合法。如果互认证成功，则进行下一步操作。

(3)用户和服务端协商生物认证机制和模型等参数。

(4)用户输入公钥证书PKC和生物证书BC，如果系统需要，还将输入生物算法证书BAC。

(5)验证公钥证书和生物证书(及生物算法证书)的有效性，并解析生物证书(生物算法证书)。如果发现证书被篡改，则直接跳到步骤8。

(6)用户通过生物数据采集设备输入个人生物信息。

(7)客户端设备根据系统设置或者从生物算法证书中解析出的认证策略和参数，将用户生物特征和从BC中解析出的生物特征模板进行比对。如果比对失败，则认为用户是冒充者。

(8)使用用户的私钥对生物认证的结果进行数字签名。生物认证的结果可以用处理代码表示，如公钥证书被篡改可以用“PKC-Alteration”表示、公钥证书过期可以用“PKC-Outdate”表示、生物证书被篡改可以用“BC-Alteration”表示、生物算法证书被篡改可以用“BAC-Alteration”表示、身份认证失败发现冒充可以用“Identity-Impersonating”表示、身份认证成功可以用“Identity-Success”表示等等。

(9)将签名后的认证结果发送给服务端。

(10)应用服务器使用用户的公钥对认证结果进行验证。

(11)应用服务器根据认证结果，通知客户端用户，身份认证完成。

在客户端有能力进行生物认证比对时，服务端不具备生物比对功能或者不适合进行生物比对。在信任客户端的前提下，客户端进行生物比对无疑成为生物认证系统一个很好的选择。该机制在客户端直接比对完成后通

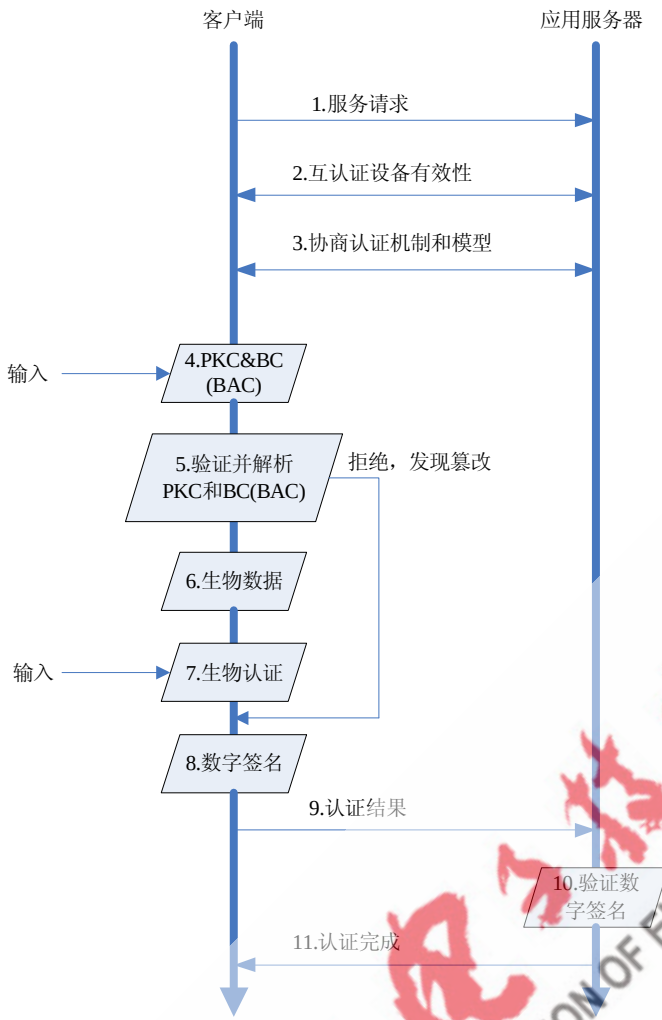

图 2 在客户端进行比对的认证流程

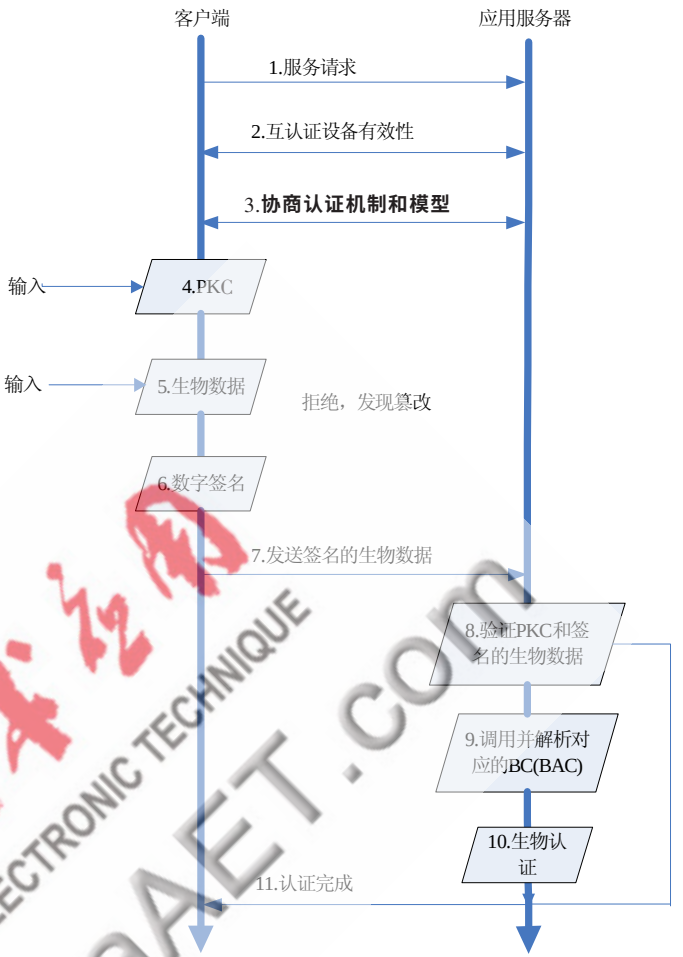

图 3 在服务器端进行比对的认证流程

知服务端认证结果，攻击者可能利用该环节的脆弱性进行攻击，冒充真实用户申请服务端服务。因此，在客户端比对时，必须保证客户端的可靠性。比如从物理环境上，保证客户端处于一个绝对安全的环境中，防止攻击者在客户端破坏系统，冒充真实用户申请服务端服务[4]。

在服务端进行生物比对匹配认证系统的工作流程如图 3 所示。

(1)用户通过客户端向应用服务器申请服务。

(2)客户端和服务端设备互相发送生物设备证书，验证对方的生物认证设备是否合法。如果互认证成功，则进行下一步操作。

(3)用户和服务端协商生物认证机制和模型等参数。

(4)用户输入其公钥证书 PKC。

(5)用户通过生物数据采集设备输入个人生物信息。

(6)使用用户的私钥对生物数据进行加密和数字签名。

(7)将加密签名后的生物数据发送给应用服务器。

(8)验证用户 PKC 的有效性和签名后的生物数据是否被篡改，如果发现篡改，直接跳到步骤 11。

(9)根据 PKC 的序列号调出相对应用户的生物证书，并解析用户生物特征模板。如果系统是生物算法证书，同时调出对应生物算法证书并解析出认证相关参数。

(10)应用服务器根据系统设置或者从生物算法证书中解析出认证策略和参数，将用户生物特征和从 BC 中解析出的生物特征模板进行比对。如果比对失败，则认为用户是冒充者。

(11)将认证结果发送给客户端用户。

在服务端进行生物比对的认证机制，避免了攻击者利用客户端直接输出认证结果，对服务端进行攻击，而且客户端简化了操作，降低了客户端的复杂度，相对于在客户端进行比对的认证机制，系统实施更简单、成本更低廉。

将生物识别技术和 PKI 技术相结合，实现生物认证系统组件之间的安全通信了。生物认证系统利用 PKI 技术实现组件间的相互认证，建立了安全通信管道，防止黑客窃听，保证了系统的整体安全性，提高了系统的可接受度。

参考文献

[1] 段斌.基于 PKI/PMI 的变电站自动化系统访问安全管

理[J].电力系统自动化,2005,23.
[2] 冯登国.PKI 技术及其发展现状[J].计算机安全,2001(1):46-51.
[3] 田捷,杨鑫.生物特征识别技术理论与运用[J].北京:电子工业出版社,2005.
[4] WAYMAN J L.Fundamentals of biometric authentication technologies [J].Int.J.Image Graph,2001,1(1):93-113.
[5] SANDHU R,COYNE E J,FEINSTEIN H L.Role-based access control models[J].IEEE Computer,1996,29(2):38-46.

(收稿日期:2009-02-09)