基于指纹和智能卡的 PKI 双向认证系统①

黄朝阳

(厦门海洋学院 信息技术系, 厦门 361100)

摘 要: 提出将指纹识别、智能卡和 PKI 技术相结合的认证方案, 系统可实现双向认证功能, 给出了详细的系统认证流程, 并分析其安全性和可实现性.

关键词: 身份认证; 指纹; 生物证书; 智能卡

Mutual Authenticaflon System Based on Fingerprint and Smart Card for PKI

HUANG Chao-Yang

(Department of Information and Technology, Xiamen Ocean College, Xiamen 361100, China)

Abstract: An authentication scheme which combined the fingerprint recognition,smart card, PKI technologies together has been proposed.In this paper, we propose the specific identification procedure of the implementation of this authentication system which offers user verification and system identification function, the security and the feasibility of this authentication schemes is discussed at length.

Key words: identity authentication; fingerprint; biometric certificat; smart card

公共密钥基础设施 PKI(Public Key Infrastructure)提供可信的身份认证, 其安全基础之一是证书中的用户信息与真实用户一一对应. 而密钥管理机制的不完善成为制约 PKI 系统发展的最大因素[1]. 常见的解决方法是将智能卡和 PIN 认证技术相结合, 利用 PIN 码来保护私钥安全, 但是卡可能会被窃取, PIN 码也存在口令威胁问题. 指纹认证技术无需用户记忆和携带口令或密码, 以及指纹技术的通用性、唯一性、持久性、可采集性决定了它是最可靠的认证技术之一. 但是, 指纹特征识别是基于相似性, 而不是通过相等性来进行匹配的, 所以, 它不能直接应用在密码体系之中. 本文利用人体指纹的唯一性与不变性的生理特征, 把指纹信息作为安全因子嵌入用户的签字私钥信息中, 使用秘密分存机制把用户的私钥信息分为 PKI 用户私钥和指纹信息两个部分, 使私钥信息与用户唯一生物特征结合起来, 提高了私钥的安全性.

1 系统注册

确保证书中用户信息的可信性是公钥认证体系的安全基础. 由于指纹作为人的一种唯一生物特征可以满足用户身份识别的需要. 为防止手指受伤等情况, 用户采集两个不同指纹制作成特征模板, 并在卡内生成密钥对. 私钥存卡内, 将公钥、用户信息、两个指纹特征模板通过安全方式发送到注册中心 RA 进行注册. RA 审核通过后交由 CA 生成 X.509 公钥证书.

为增强安全性, 智能卡中存储的指纹特征模板数据必须防止被篡改或者破坏, 而数字签名是一种有效的用于保证数据完整性的手段. 文献[2]提出了通过 X.509 证书验证生物特征模板的方法, 通过创建一种新的经过数字签名的生物模板—生物证书, 在生物证书中加入证书的有效期和主体等信息, 通过 X.509 证书序列号, 使得 X.509 证书和指纹生物证书对应起来, 减小了伪造证书或生物模板破坏所带来的威胁. 将数

① 收稿时间:2012-02-20;收到修改稿时间:2012-04-05

字证书和指纹生物证书分别写入智能卡内部的数字证书文件和指纹模板证书文件中.

2 系统认证

认证系统主要完成证书的验证、活体指纹现场采集、指纹匹配等功能. 它由客户端和服务器端系统组成.

客户端主要读取智能签名卡中的数字证书、指纹生物证书, 交给 PKI 系统验证、解密, 并取得指纹特征模板; 采集用户现场活体指纹, 将采集的指纹数据进行预处理, 匹配特征模板; 匹配通过后, 取出存储在智能卡中的用户私钥, 用户使用私钥便可以从事电子商务的数字签名和加密等交易活动. 服务器端主要由 PKI 系统完成, 主要实现验证证书工作.

认证系统分为三个阶段, 分别是智能卡与读卡器之间的相互认证, 用户身份的认证和用户间的双向身份认证.

2.1 智能卡与读卡器的相互认证

当智能卡开始工作时, 读卡器和智能卡需相互确认一下真伪. 两者之间可采用命令/应答方式进行通信[3].

(1) 智能卡鉴别读卡器真伪 先由智能卡产生一个随机数, 由读卡器对随机数加密成密文, 再由智能卡对密文进行解密, 并将解密后的明文与随机数在卡内进行比对. 如比对正确, 卡承认读卡器是真的; 否则读卡器是伪造的.

(2) 读卡器鉴别卡的真伪 其过程与卡鉴别读卡器真伪的过程相似. 但随机数比对的操作是在读卡器中进行的.

2.2 用户身份认证

对持卡人的身份进行认证, 即确认该用户是否是智能卡的合法持有者.

用户身份认证过程基本原理是: 读卡器读出智能卡中保存的 X.509 证书和指纹生物证书发送到 CA, CA 对两者的有效性和对应关系进行验证; 若验证通过, 通知客户端指纹扫描仪采集指纹并计算得到指纹特征值, 取出智能卡内保存的指纹特征模板, 在卡内进行两者的匹配[4]; 若匹配成功, 则证明该用户就是智能卡的合法持有者, 从而完成该用户的身份认证过程; 认证通过后, 释放智能卡内保存的用户私钥, 以进行下一步的操作. 其处理流程如图 1 所示.

CA 接收到客户端的 X.509 证书和指纹生物证书后, 用给定的 Hash 算法对 X.509 证书进行摘要, 并利用其公钥解开 X.509 证书的数字签名, 若两个算法处理的结果相同, 且查阅 CA 中心的证书撤销清单列表 CRL 以确定证书是有效, 则 X.509 证书验证通过, 进行下一步处理, 否则说明其 X.509 证书内容被非法篡改.

取出指纹生物证书中的 X.509 证书序列号, 与 X.509 证书中的证书序列号进行比对, 若比对成功, 说明 X.509 证书与指纹生物证书相对应.

CA 用给定的 Hash 算法对指纹特征模板进行摘要, 并利用其公钥解开指纹生物证书的数字签名, 若两个算法处理的结果相同, 则指纹生物证书签名和验证通过, 进行下一步处理, 否则说明其指纹生物证书内容被非法篡改.

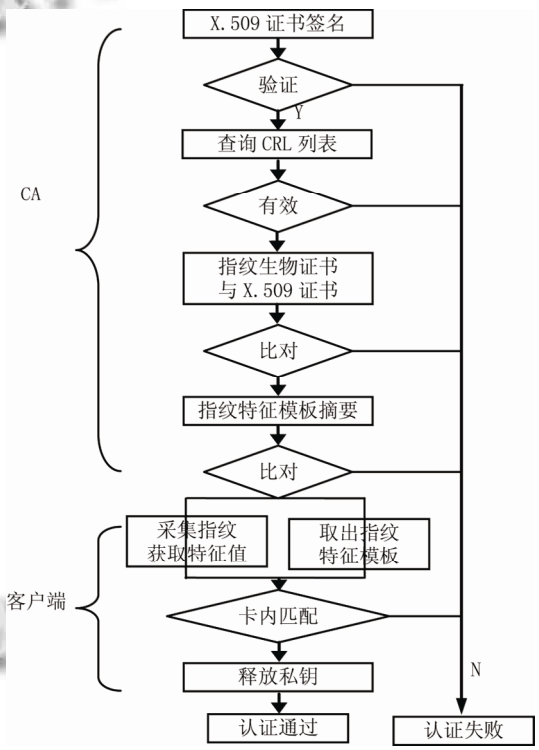

图 1 用户身份认证流程

CA 将验证结果通知客户端, 若验证通过, 系统提示用户扫描指纹, 通过指纹扫描仪中的集成预处理和特征提取算法, 提取出采集到的指纹的特征值, 并将该特征值输入智能卡. 智能卡[5]在智能卡操作系统 COS 的控制下, 读出内部的数据文件保存的两个指纹特征模板, 在智能卡内部[6]分别与采集到的特征值利用基于细节点的匹配算法进行特征值匹配, 若任一特征值模板匹配成功, 则证明该用户是智能卡的合法持有者, 同时在智能卡内部释放私钥文件中保存的用户私钥.

2.3 用户间双向身份认证

本系统提供双向身份认证模式, 实现发送端和接收端的相互认证, 以提高系统的安全性. 在此, 假设须要进行身份认证的双方为 A 和 B, 他们都已经登录到网络, 完成了用户身份认证过程, 并取得了自己的私钥, 并假设是 A 提出认证请求.

A 对 B 的身份认证: 系统在 A 端产生一个随机数 nl, 将 nl 发送至 B, 并将 nl 保存在 A 本地; B 将接收到的 nl 利用 B 的私钥进行数字签名, 然后系统在 B 端产生随机数 n2, 将 B 对 nl 的签名值、B 的 X.509 证书序列号和 n2 一起发送回 A, 并将 n2 保存在 B 本地; A 接收到 B 发送的信息, 根据 B 的 B 的 X.509 证书序列号到 CA 公钥目录服务器上下载 B 的 X.509 证书, 并通过查阅 CA 中心的证书撤销清单列表 CRL 以确定证书是否有效, 如果该证书有效, 利用得到的证书中的 B 的公钥对签名值进行解密, 如果解密结果与 A 端本地保存的 n1 相同, 则 A 对 B 的身份认证通过, 否则验证失败退出. B 对 A 的认证过程与上述相仿, 不再赘述.

至此, 双向身份认证结束, 双方进行正常通信.

3 安全性分析

本方案用指纹生物证书替代了传统的 PIN 码, 极大地提高了 PKI 系统的安全性:

(1) 引入生物证书--经过数字签名的生物模板的概念, 将 X.509 证书与生物证书通过序列号关联起来, 保证了指纹特征模板和公钥证书之间的对应关系的安全性, 在一定程度上减少了伪造公钥证书或指纹模板和破坏智能卡所带来的威胁.

(2) 指纹特征值模板不保存在后台数据库中, 与用户的数字证书一起存放在智能卡上, 由用户自己保存, 有效地避免了集中式处理的缺点和系统崩溃带来的严重后果, 分散化解了安全风险.

(3) 在不改变现有智能卡硬件结构的前提下, 数字证书、私钥和指纹模板证书都保存在智能卡内部, 卡内数据在没有匹配时不能被访问. 运算和加密过程都在卡内实现, 不提供外部访问的接口, 因此具有很好的安全性和隐私性.

(4) 以指纹识别为代表的生物识别技术, 拥有人自我管理, 减少了丢失、偷窃的可能; 减少了分发管理的负担; 同时拥有人对其具有控制权.

(5) 智能卡中保存两个甚至更多的指纹特征模板, 通过调用备份读取, 可以将错误拒绝率降到最低.

(6) 只有通过指纹认证的情况下才可以使用卡中存储的数字证书, 因此实际上可以免除 PIN 或者口令, 防止了人为的信息泄露.

(7) 私钥得以释放之后, 其对数据进行解密和签名等的操作应该在 COS 的控制下, 仅在智能卡内部完成, 私钥将由 COS 来控制其使用, 对卡外的应用程序完全透明, 避免私钥明文的泄露.

(8) 采用双向认证模式, 认证用户双方处于同等的地位, 防止了任何一方的假冒, 实现了数据来源的不可否认性、接收的不可否认性以及接收后的不可否认性.

4 结语

该方案将生物认证的高识别率、不易丢失, 智能卡良好的防伪、防攻击性和 PKI 对私钥的保护机制相结合, 并且弥补了各自的缺点, 大大提高了身份认证技术的安全性. 且指纹识别作为一个独立的模块嵌入到智能卡中的, 很容易与其他智能卡应用相结合, 实现智能卡的高安全性和多应用性. 在具体的应用环境中, 应该根据具体的功能需求和交易流程, 设计智能卡的文件结构和安全结构.

参考文献

1 孙美青,王如龙.PKI 技术及其在企业中的应用.计算机系统应用,2009,18(7):141−145.
2 辛阳,魏景芝等.基于 PKI 和 PMI 的生物认证系统研究.电子与信息学报,2008,30(1):1−5.
3 王爱英.智能卡技术:IC 卡.第 2 版.北京:清华大学出版社,2000.182−184.
4 陈平,孙宏伟顾明.基于指纹识别和智能卡的安全电子报税系统.计算机应用研究,2007,24(2):134−137.
5 王爱英.智能卡技术:IC 卡与 RFID 标签.第三版.北京:清华大学出版社,2009.326−337.
6 刘培顺,王建波,何大可.结合指纹信息的 PKI 认证系统.计算机工程,2005,31(9):59−60.