计算机工程 2012, 38(3) 137-138 DOI: 10.3969/j.issn.1000-3428.2012.03.046 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

基于生物特征的鲁棒远程用户认证方案

张韶远，卢建朱

(暨南大学信息科学技术学院，广州 510632)

摘要： 将生物特征信息、单向哈希函数和智能卡等技术相结合，提出一种基于生物特征识别的身份认证方案。利用时戳生成一次性共享信息，以提高系统的鲁棒性。分析结果证明，该方案可防止伪装攻击、重放攻击和拒绝服务攻击。用户与服务器仅需2次握手即可实现相互认证，由此节约系统的通信成本，提高认证效率。

关键词： 基于生物特征的认证 单向哈希函数 时间戳 远程用户 智能卡 可信第三方 一次性共享密钥

Biometrics-based Robust Remote User Authentication Scheme

ZHANG Shao-yuan, LU Jian-zhu

(College of Information Science and Technology, Jinan University, Guangzhou 510632, China)

Abstract: An efficient biometrics-based mutual authentication scheme is proposed, which is based on personal biometrics, one-way Hash function and smart card. For enhancing the system security, a one-time key is generated by using the timestamp. In the scheme, the authentication process can resist all known attacks including replay attacks and the DoS attacks, and needs only twice online message transmissions. Analysis shows that the scheme is secure and effective.

Keywords: biometrics-based authentication one-way Hash function timestamp remote user smart card trusted third party one-time shared key

收稿日期 2011-07-07 **修回日期** **网络版发布日期** 2012-02-05

DOI: 10.3969/j.issn.1000-3428.2012.03.046

基金项目:

广东省产学研基金资助项目(2008B090500201, 2009B010 800023)

通讯作者:

作者简介: 张韶远(1986－)，男，硕士研究生，主研方向：无线网络安全；卢建朱，副教授、博士

通讯作者E-mail: zhangshaoyuan@foxmail.com

参考文献：

[1] 曹 健, 王武军, 韩 飞, 等. 基于局部特征的目标识别技术研究[J].计算机工程.2010, 36(10):203-205 浏览

[3] Lin Chu-Hsing, Lai Yi-Yi. A Flexible Biometrics Remote User Authentication Scheme [J].Computer Standards and Interfaces.2004, 27(1):19-23

[4] Lee J K, Ryu S R, Yoo K Y. Fingerprint-based Remote User Authentication Scheme Using Smart Cards[J].Electronic Letters.2002, 38(12):554-555

[5] Hsieh B T.[J].Yeh H Y, Sun H M, et al. Cryptanalysis of a Fingerprint-based Remote User Authentication Scheme Using Smart Cards[C]//Proc. of the 37th Annual International Carnahan Conference on Security Technology. Washington D. C., USA: IEEE Press.2003,:-

[6] Li Chun-Ta, Hwang Min-Shiang. An Efficient Biometrics-based Remote User Authentication Scheme Using Smart Cards[J].Journal of Network and Computer Applications.2010, 33 (1):1-5

本刊中的类似文章

1. 王秀利, 王萌.一种应用于双重数字签名的电子拍卖方案[J]. 计算机工程, 2012,38(04): 4-6
2. 张淑苗, 张书晔, 冯全, 杨梅.基于双方交集计算的指纹认证方案[J]. 计算机工程, 2012,38(04): 126-128
3. 张建中, 马冬兰.一种高效的门限部分盲签名方案[J]. 计算机工程, 2012,38(01): 130-131,134
4. 戚世杰, 卢建朱, 胡吉旦.增强型相互认证密钥协商方案[J]. 计算机工程, 2012,38(01): 108-110
5. 原变青, 张忠.支持授权撤销的代理签名分析与改进[J]. 计算机工程, 2012,38(01): 135-136
6. 胡吉旦, 卢建朱.无线网络中一种基于智能卡的匿名认证方案[J]. 计算机工程, 2012,38(01): 122-124
7. 刘雪艳, 张强.基于生物特征的可变角色用户认证机制[J]. 计算机工程, 2011,37(9): 168-170
8. 张永强, 王强.基于Tcl的智能卡软件测试方法[J]. 计算机工程, 2011,37(8): 50-51
9. 池亚平, 李兆斌, 方勇.基于Java智能卡的可信计算环境研究[J]. 计算机工程, 2011,37(4): 140-141
10. 汪付强, 曾鹏, 张晓玲, 梁炜, 于海斌.无线传感器网络时间同步综述[J]. 计算机工程, 2011,37(22): 70-73

文章评论

反馈人		邮箱地址	
反馈标题		验证码	9629