计算机工程与应用 2008 44 (10): 106-107 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

基于USB key的零知识证明双向认证方案

周先存[1], 侯整风[2], 刘仁金[1]
1．皖西学院 计算机科学与技术系，安徽 六安 237012
2．合肥工业大学 计算机与信息学院，合肥 230009

收稿日期 2007-11-6 修回日期 2008-1-21 网络版发布日期 2008-3-22 接受日期

摘要 基于USB key和零知识证明思想，构造一种双向交互认证方案，不仅实现了对用户的身份认证，而且实现了对用户的公钥认证。分析表明，该方案具有安全性高，计算复杂性低的特点。

关键词 USB key 零知识证明 身份认证 公钥认证
分类号

Mutual authentication scheme based on USB key and zero-knowledge proof

ZHOU Xian-cun[1],HOU Zheng-feng[2],LIU Ren-jin[1]

1.Department of Computer Science and Technology，West Anhui University，Liu’an，Anhui 237012，China
2.School of Computer and Information，Hefei University of Technology，Hefei 230009，China

Abstract
Based on USB key and zero-knowledge proof，a mutual authentication scheme is proposed in this paper，which has realized to user’s authentication，moreover has realized to user’s public key authentication.The analysis indicates that the scheme is secure and the computation complexity is low.

Key words USB key zero-knowledge proof authentication authentication of public key

DOI:

通讯作者 周先存 zxcjsj@126.com

扩展功能
本文信息
Supporting info
PDF(411KB)
[HTML全文](0KB)
参考文献
服务与反馈
把本文推荐给朋友
加入我的书架
加入引用管理器
复制索引
Email Alert
文章反馈
浏览反馈信息
相关信息
本刊中 包含“USB key”的相关文章
本文作者相关文章
· 周先存
· 侯整风
· 刘仁金