计算机工程与应用 2010 46 (8): 96-98 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

一种新的无证书代理签名方案的分析与改进

申军伟[1]，杨晓元[1,2]，梁中银[1]，陈海滨[1]

1.武警工程学院，西安 710086

2.西安电子科技大学 网络信息安全教育部重点实验室，西安 710071

收稿日期 2008-9-18 修回日期 2008-12-22 网络版发布日期 2010-3-11 接受日期

摘要 樊睿等人提出了一种新的无证书代理签名方案，该方案的安全性是基于CDH困难性假设。对该代理签名方案进行了安全性分析，指出该方案不仅泄露了原始签名者的私钥，而且不能抵抗替换公钥攻击和恶意但被动的KGC攻击，从而不满足代理签名的安全性要求。同时提出了一个改进方案，改进方案不仅弥补了原方案的安全缺陷，而且改善了协议的性能。

关键词 无证书公钥密码体制 代理签名 替换公钥攻击 密钥生成中心 恶意但被动的KGC攻击

分类号 TP309

Security analysis and improvement of new certificateless proxy signature

SHEN Jun-wei[1]，YANG Xiao-yuan[1,2]，LIANG Zhong-yin[1]，CHEN Hai-bin[1]

1.Engineering College of Armed Police Force，Xi’an 710086，China

2.Key Laboratory of Network & Information Security of the Ministry of Education，Xidian University，Xi’an 710071，China

Abstract

This paper analyzes the security of a new certificateless proxy signature proposed by Fan Rui recently.The security of Fan Rui’s scheme relies on the CDH problem.It shows that Fan’s proxy signature reveals the private key of original signer and is insecure against a key replacement attack and malicious-but-passive KGC attack.It also gives a modified scheme.The improvement is secure against the key replacement attack and the malicious-but-passive KGC attack.This paper elaborately eliminates the defect of the original scheme and improves the efficiency of the protocol.

Key words certificateless public key cryptography proxy signature public key replacement attack Key Generation Center（KGC） malicious-but-passive KGC attack

DOI: 10.3778/j.issn.1002-8331.2010.08.027

通讯作者 申军伟 jhkplwfnsjw@163.com