计算机应用 2008, 28(7) 1807-1809 DOI: ISSN: 1001-9081 CN: 51-1307/TP

论文

基于数字签名认证的IKE协议安全性分析及改进

何韦伟 季新生 刘彩霞

解放军信息工程大学国家数字交换系统工程技术研究中心

摘要：

IKE协议的复杂性使得其存在一些安全漏洞。简要介绍基于数字签名认证方式的IKE协议工作机制之后，分析了IKE协议容易遭受的两种中间人攻击，针对中间人攻击导致用户身份泄漏的安全缺陷，提出两种改进方案并给出改进前后定量的性能分析。

关键词： IKE 数字签名 中间人攻击 公钥

Security analysis and improvement of IKE protocol with signature authentication

Abstract:

The complexity of Internet Key Exchange (IKE) protocol causes some potential security flaws. After the mechanism of IKE with signature was introduced, the two kinds of man-in-middle attack were analyzed. In order to protect the users' identities from being exposed to the outside, two solutions with some improvements were proposed. Finally the paper made a quantitative capability analysis on the whole.

Keywords: Internet Key Exchange(IKE) digital signature man-in-middle attack public key

收稿日期 2008-01-14 修回日期 1900-01-01 网络版发布日期

DOI:

基金项目:

通讯作者: 何韦伟

作者简介:

参考文献：

本刊中的类似文章

1．刘茂福 胡慧君 何炎祥.主成分分析在图像Zernike矩特征降维中的应用[J]. 计算机应用, 2007,27(3): 696-698

2．张伟伟 夏利民 .基于多特征融合和Bagging神经网络的人耳识别[J]. 计算机应用, 2006,26(8): 1870-1872

3．王忠 孙钰.基于Zernike不变矩的零水印算法[J]. 计算机应用, 2008,28(9): 2233-2235

4．王红春 靳斌 樊旭升 马士明.基于神经网络的脱机中文签名鉴别系统的研究[J]. 计算机应用, 2008,28(9): 2389-2391

文章评论 (请注意:本站实行文责自负, 请不要发表与学术无关的内容!评论内容不代表本站观点.)

反馈人		邮箱地址	
反馈标题		验证码