

安全技术

基于预共享密钥认证的IKE协议分析与改进

武涛, 郑雪峰, 姚宣霞, 李明祥

(北京科技大学信息工程学院, 北京 100083)

收稿日期 修回日期 网络版发布日期 2008-4-11 接受日期

**摘要** 对基于预共享密钥认证的主模式IKE协议进行研究, 针对其安全漏洞以及不支持移动用户的缺陷, 提出相应的改进建议。该方案能及时发现并阻止中间人攻击和拒绝服务攻击, 同时保护双方的身份, 没有固定IP地址的限制。性能分析表明, 该方案是安全、高效的。

**关键词** [IKE协议](#); [预共享密钥认证](#); [主模式交换](#); [IPSec协议](#)

**分类号** [TP393.08](#)

**DOI:**

对应的英文版文章: [080846](#)

通讯作者:

作者个人主页: [武涛](#); [郑雪峰](#); [姚宣霞](#); [李明祥](#)

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF \(103KB\)](#)
- ▶ [\[HTML全文\] \(0KB\)](#)
- ▶ [参考文献 \[PDF\]](#)
- ▶ [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](#)
- ▶ [引用本文](#)
- ▶ [Email Alert](#)
- ▶ [文章反馈](#)
- ▶ [浏览反馈信息](#)

相关信息

- ▶ [本刊中包含“IKE协议; 预共享密钥认证; 主模式交换; IPSec协议”的相关文章](#)
- ▶ [本文作者相关文章](#)

- [武涛](#)
- [郑雪峰](#)
- [姚宣霞](#)
- [李明祥](#)