

## 安全技术

一种增加型的IKE协议签名认证

刘旭东, 李占才, 王 沁

(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 2006-9-26 接受日期

**摘要** 由于IKE协议中签名认证方式易受中间人攻击, 因此IKE协议存在用户ID泄漏的安全隐患。针对该问题, 文章提出了一种隐藏用户ID的解决方案。此方案既保持了ISAKMP的框架结构又可以有效地抵御中间人攻击和暴力破解手段, 而且付出的系统代价很小。此方案已被一款IPSec协处理器的设计所采纳。

**关键词** [Internet密钥交换](#) [中间人攻击](#) [IPSec](#) [信息安全](#)

分类号

**DOI:**

对应的英文版文章: [2006-19-057](#)

通讯作者:

作者个人主页: 刘旭东; 李占才; 王 沁

### 扩展功能

本文信息

▶ [Supporting info](#)

▶ [PDF \(127KB\)](#)

▶ [\[HTML全文\] \(0KB\)](#)

▶ [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“Internet密钥交换”的 相关文章](#)

▶ [本文作者相关文章](#)

· [刘旭东](#)

· [李占才](#)

· [王 沁](#)