计算机工程与应用 2010 46 (5): 73-75 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

# 一种基于零知识证明的互联网密钥交换协议

王世峰[1]，张龙军[2]，杨晓元[1，3]

1.武警工程学院 电子技术系 网络与信息安全武警部队重点实验室，西安 710086
2.武警工程学院 通信工程系，西安 710086
3.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 2008-11-24 修回日期 2009-2-4 网络版发布日期 2010-2-8 接受日期

摘要 IKE协议由于交换过程及密钥交换过程复杂，容易受到多种攻击。在分析其弱点的基础上，利用零知识证明的基本思想，提出了一种新的协议。该协议在减小系统消耗代价的同时，能够有效抵抗MITM（Man-In-The-Middle），暴力破解攻击等。方案适用于对数据的安全性要求较高的用户。

关键词 零知识证明 密钥交换协议 中间人攻击

分类号 TP309

# Internet key exchange protocol based on zero knowledge proof

WANG Shi-feng[1]，ZHANG Long-jun[2]，YANG Xiao-yuan[1，3]

1.Key Laboratory of Network & Information Security of APF，Engineering College of APF，Xi’an 710086，China
2.Department of Communication Engineering，Engineering College of APF，Xi’an 710086，China
3.Key Laboratory of Network & Information Security of the Ministry of Education，Xidian University，Xi’an 710071，China

**Abstract**

IKE protocol，with its complexity，is vulnerable to multiple attacks.This paper first analyzes its flaws，and then based on the idea of zero knowledge proof，proposes a new protocol，which can resist MITM attack efficiently as well as reduce system consumption.This protocol fits the users who need more strong security protect for their data.

**Key words** zero knowledge proof Internet Key Exchange（IKE） Man-In-The-Middle（MITM）

DOI: 10.3778/j.issn.1002-8331.2010.05.022

通讯作者 王世峰 wsfmrrl@163.com