计算机工程与应用 2008 44 (27): 21-23 ISSN: 1002-8331 CN: 11-2127/TP

博士论坛

TTS组密钥协商协议的安全性分析与改进

郭现峰

西南民族大学 计算机科学与技术学院，成都 610041

收稿日期 2008-5-19 修回日期 2008-6-16 网络版发布日期 2008-9-18 接受日期

摘要 针对动态对等通信中的组密钥协商协议进行了分析和研究，指出王志伟等人提出的基于树结构和门限思想的组密钥协商协议（TTS）存在密钥控制和不等献性等缺陷，进而给出了一个改进的方案（I-TTS）。安全性分析表明，I-TTS协议不仅克服了TTS协议中的前向安全性和密钥控制缺陷，还满足等献性。

关键词 密钥协商 密钥控制 等献性 前向安全性

分类号

Cryptanalysis and improvement of TTS group key agreement protocol

GUO Xian-feng

College of Computer Science and Technology，Southwest University for Nationalities，Chengdu 610041，China

Abstract

This work investigates the group key agreement protocols，and points out that Wang et al’s key agreement protocol （Tree and Threshold Scheme，TST） is not only non-contributory，but also vulnerable to key control i.e.the sponsor of the key agreement can predetermine the group key.To over come the security flaws，this paper presents an improve scheme （I-TTS）.Security analysis indicate that I-TTS scheme is contributory，and no one can predetermine the negotiated group key.Further more，the I-TTS scheme is perfect forward secrecy.

Key words key agreement key control contributory forward secrecy

DOI: 10.3778/j.issn.1002-8331.2008.27.007

通讯作者 郭现峰 guoxianf@126.com

扩展功能

本文信息

Supporting info

PDF(535KB)

[HTML全文](0KB)

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

复制索引

Email Alert

文章反馈

浏览反馈信息

相关信息

本刊中 包含“密钥协商”的相关文章

本文作者相关文章

· 郭现峰