计算机工程与应用 2009 45 (23): 100-103 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

TLS协议认证测试模型与形式化分析

孔 娟，曹利培

安阳工学院 计算机科学与信息工程系，河南 安阳 455000

收稿日期 2009-3-23 修回日期 2009-5-26 网络版发布日期 接受日期

摘要

TLS协议是一种重要的传输层安全协议，得到了广泛的应用。在结合串空间理论和方法的基础上，通过构造TLS握手协议的认证测试模型，提出了TLS协议的DH参数签名认证测试方案，分析和证明了协议的保密性和认证性等关键属性。结果表明TLS协议满足其安全性说明。

关键词

传输层安全协议 认证测试 串空间 形式化分析

分类号 TP393

Formalized analysis for authentication test model of TLS

KONG Juan，CAO Li-pei

Department of Computer Engineering，Anyang Institute Technology，Anyang，Henan 455000，China

Abstract

TLS protocol is an important transport layer security protocol，and is widely used.Based on strand space theory，this paper points out the DH parameter signature certification testing program，analyzes and proves the confidentiality and authentication of the agreement.The result shows that the TLS protocol meets their security statement.

Key words

Transport Layer Security（TLS） protocol authentication test strand space formalized analysis

DOI: 10.3778/j.issn.1002-8331.2009.23.028

通讯作者 孔 娟 lkongjuan2000@yahoo.cn