计算机工程与应用 2007 43 (15): 157-159 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信与安全

基于认证测试方法的EAP-AKA协议分析

王 鹏，李谢华，陆松年

上海交通大学 信息安全工程学院，上海 200240

收稿日期 修回日期 网络版发布日期 2007-5-9 接受日期

摘要 EAP-AKA(Extensible Authentication Protocol-Authentication and Key Agreement)是WLAN的认证和密钥分配协议；认证测试是一种以串空间理论为基础的安全协议分析验证方法。运用认证测试方法对EAP-AKA协议的双向身份认证过程进行了分析证明，结果说明EAP-AKA能够保证移动终端和认证服务器之间的双向认证。

关键词 EAP-AKA协议 认证测试方法 串空间模型 3G WLAN 形式化方法

分类号

Formal analysis of EAP-AKA protocol based on authentication tests

WANG Peng，LI Xie-hua，LU Song-nian

School of Information Security Engineering，Shanghai Jiaotong University，Shanghai 200240，China

Abstract

EAP-AKA（Extensible Authentication Protocol-Authentication and Key Agreement） is authentication and key agreement protocol of WLAN；Authentication tests is a method based on the strand space model for analyzing and verifying the security protocols.This paper uses authentication tests to analyze EAP-AKA protocol，and proves that EAP-AKA protocol can ensure the mutual authentication between WLAN-UE and 3GPP AAA.

Key words EAP-AKA protocol authentication tests strand space model 3G WLAN formal method

DOI:

通讯作者 王 鹏 E-mail：karus@sjtu.edu.cn