计算机工程与应用 2009 45 (28): 96-98 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

增强EAP-AKA协议安全性的改进方案

张 艳，王 赜

天津工业大学 计算机技术与自动化学院，天津 300160

收稿日期 2009-4-2 修回日期 2009-5-25 网络版发布日期 2009-9-29 接受日期

摘要 针对EAP-AKA协议中存在的安全问题，提出了改进方案。通过在3G和WLAN接入网络间增设共享密钥实现了两者间的相互认证，并用串空间模型和认证测试方法进行了形式化分析，通过加密传输NAI实现了对IMSI的加密保护，通过引入密钥更新机制实现了对用户和3G网络间的共享密钥的安全更新。

关键词 EAP-AKA 3G 无线局域网络 串空间 认证测试方法

分类号 TP393.08

Improved method of enhancing EAP-AKA protocol security

ZHANG Yan，WANG Ze

Department of Computer Technology and Automation，Tianjin Polytechnic University，Tianjin 300160，China

Abstract

An improved method is proposed in order to solve problems of EAP-AKA protocol.It implements mutual authentication between 3G networks and WLAN access networks by adding shared keys，which can be proved through strand space model and authentication test，the protection to IMSI by transmitting the encrypted NAI and the secure updating of shared keys between users and 3G networks by introducing key updating strategy.

Key words Extensible Authentication Protocol-Authentication and Key Agreement（EAP-AKA） 3G Wireless Local Area Network（WLAN） strand space authentication test

DOI: 10.3778/j.issn.1002-8331.2009.28.028

通讯作者 张 艳 zhangyandoudous@163.com