基于动态口令的 WiFi 身份认证方案研究

王增光，陈立云，卢　昱
（军械工程学院 信息工程系,河北 石家庄 050003）

摘　要： 针对日益严重的无线网络安全问题，从安全性和移动终端负载能力考虑，提出了一种 WiFi 环境下的轻量级双向身份认证方案.该方案基于挑战/应答机制，用户对认证服务器的认证通过基于异或运算的身份认证方式来实现；认证服务器对用户的认证通过基于公钥加密的身份认证方式实现.通过性能分析可知，该方案认证简洁，减轻了客户端的运算量和存储量，同时又能抵抗重放攻击、小数攻击、网络窃听和冒充攻击，适合应用到对安全性要求较高的 WiFi 环境下.

关键词： 无线网络；身份认证；动态口令；轻量级

Research on WiFi Identity Authentication Scheme Based on Dynamic Password

WANG Zeng-guang, CHEN Li-yun, LU Yu
(Department of Information Engineering, Ordnance Engineering College, Shijiazhuang 050003, China)

Abstract：A lightweight authentication scheme of WiFi environment is raised from the perspective of security and the load capacity mobile terminal according to the increasing serious of wireless network security. The new scheme is based on the challenge/response. The authentication of user to authentication server is realized by lightweight authentication. The authentication of authentication to user is realized by identity authentication based on public key encryption. Through the analysis of performance, the scheme is simple and the computation and storage of the client are reduced. What's more, the scheme can resist replay attack, network eavesdropping and posing as attack, which is suitable for the application to the WiFi environment with high security requirements.

Key words：wireless network; authentication; OTP; lightweight

作者简介：
王增光　　男，(1991-)，硕士研究生.研究方向为网络安全与信息对抗.E-mail:wang1223797579@163.com.