计算机工程与应用 2009 45 (1): 129-130 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

对改进的无线认证协议SSM的分析

郭宇燕[1], 魏仕民[2], 卓泽朋[3]

1.宿州学院 计算机科学与技术系，安徽 宿州 234000
2.淮北煤炭师范学院 计算机科学与技术系，安徽 淮北 235000
3.淮北煤炭师范学院 数学系，安徽 淮北 235000

收稿日期 2007-12-27 修回日期 2008-3-13 网络版发布日期 2008-12-28 接受日期

摘要 针对刘霞提出的改进的Server-specific MAKEP协议，首次利用一种新兴的形式化分析工具—串空间模型对其进行分析。先对协议的机密性进行分析，并运用“理想”和“诚实”两个概念简化分析协议的步骤，证明了*rs*，*rc*是保密的，然后对协议的认证性进行分析，分析包括响应者认证和发起者认证。最终结果表明改进的SSM协议能够达到协议的安全目标。

关键词 SSM协议 串空间 机密性 认证性

分类号

Analyzing model of amended wireless authentication protocol SSM

GUO Yu-yan[1],WEI Shi-min[2],ZHUO Ze-peng[3]

1.Dept. of Computer Science & Technique，Suzhou University，Suzhou，Anhui 234000，China
2.Dept. of Computer Science & Technique，Huaibei Coal Industry Teachers’ College，Huaibei，Anhui 235000，China
3.Dept. of Mathematics，Huaibei Coal Industry Teachers’ College，Huaibei，Anhui 235000，China

Abstract

It is the first time to prove the Liu Xia’s modified version of server-specific MAKEP protocol with the theory of strand space which is a rising formal analysis tool.Firstly，its confidentiality is analyzed，and two concepts honest and ideal are used to simplify the process of verification.It indicates that rs，rc are secret.Then its authentication is analyzed，the analysis contains responser’s authentication and sponsor’s authentication.At last，the result shows that the amended SSM protocol can reach the goal of the protocol.

Key words SSM protocol strand space confidentiality authentication

DOI: 10.3778/j.issn.1002-8331.2009.01.040

扩展功能

本文信息

Supporting info

PDF(297KB)

[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“SSM协议”的 相关文章

本文作者相关文章

- 郭宇燕
- 魏仕民
- 卓泽朋

通讯作者 郭宇燕 guoyuyan428428@sohu.com