计算机工程　2007 33 (06): 126-128　ISSN: 1000-3428　CN: 31-1289/TP

安全技术

Otway-Rees协议并行攻击的SG逻辑分析

王小锐1，陈连俊2，季庆光3，曹正君2

（1. 解放军信息工程大学电子技术学院，郑州 450004；2. 总参51所，北京 100072； 3. 中国科学院软件研究所信息安全国家重点实验室，北京 100080）

收稿日期　修回日期　网络版发布日期 2007-3-9　接受日期

摘要　网络信息安全很大程度上取决于密码协议的安全，重放攻击和并行攻击是对密码协议的常见攻击，能够分析并行攻击的形式化分析方法并不多见。该文介绍了一种分析密码协议并行攻击和重放攻击的逻辑方法——SG逻辑，应用它对改进版的Otway-Rees协议进行了分析，找出了BAN类逻辑所不能分析出来的缺陷，针对该缺陷给出了协议的进一步改进，并推证了改进后的协议对SG逻辑的分析是安全的。

关键词　SG逻辑　并行攻击　Otway-Rees协议　安全性分析

分类号

DOI:

对应的英文版文章：2007-6-055

通讯作者:

作者个人主页: 王小锐1;陈连俊2;季庆光3;曹正君2