计算机工程 2007 33 (05): 112-113 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

基于逻辑编程的EKE协议分析

王全来1,2，韩继红1，王亚弟1

（1. 解放军信息工程大学电子技术学院，郑州 450004；2. 解放军防空兵指挥学院，郑州 450052）

收稿日期 修回日期 网络版发布日期 2007-3-1 接受日期

摘要 基于逻辑编程规则及Spi演算提出了一种验证密码协议安全性的新方法，利用该方法可以对密码协议的安全性质以程序化的方式进行验证。通过对EKE协议进行的分析，不但证明了协议已知的漏洞，而且发现了针对EKE协议的一个新的攻击——并行会话攻击。很好地验证了该新方法对密码协议的分析能力。

关键词 进程演算 逻辑编程 自动验证 密码协议

分类号

DOI:

通讯作者:

作者个人主页: 王全来1;2;韩继红1;王亚弟1