计算机应用 2006 26 (05): 1087-1089 ISSN: 1001-9081 CN: 51-1307/TP

信息安全

一种新的密码协议分析方法及其应用

文静华, 张梅, 李祥

贵州财经学院/贵州大学

收稿日期 2005-11-14 修回日期 网络版发布日期 接受日期

摘要 针对传统时序逻辑把协议看成封闭系统进行分析的缺点， 提出一种新的基于策略的ATL逻辑方法分析密码协议。最后用新方法对Needham-Schroeder协议进行了严格的形式化分析，结果验证了该协议存在重放攻击。工作表明基于博弈的ATL逻辑比传统的CTL更适合于描述和分析密码协议。

Abstract Aiming at the shortcoming that traditional temporal logic regards protocols as close system to analyse, this paper proposes a ATL(Alternating-time Temporal Logic)logical method based on game to analyse cryptographic protocols. In the end, we make strict formal analysis for Needham-Schroeder protocol with this new method, as a result we validate there exists reply attacks。 These works indicate that the ATL logic based on game is more suitable to describe and analyze cryptographic protocols than traditional CTL.

关键词 密码协议,安全性,形式化分析,ATL

Key words cryptographic protocols,security,formal analysis,ATL

分类号

DOI:

通讯作者:
文静华 jinghuawen@sohu.com

作者个人主页: 文静华; 张梅; 李祥