计算机工程与应用 2010 46 (2): 79-82 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

安全协议验证模型的高效自动生成

吴 昌[1]，肖美华[1]，罗 敏[2]，刘俏威[1]，熊 昊[1]
1.南昌大学 信息工程学院，南昌 330031
2.江西省计算技术研究所，南昌 330002

收稿日期 2008-8-12 修回日期 2008-10-29 网络版发布日期 2010-1-20 接受日期

摘要 为了能高效地利用模型检测技术对安全协议进行分析与验证，提高工作效率，提出了一种适用范围广，自动化程度及验证效率均较高的建模算法。开发了一个基于该建模算法“网络安全协议验证模型生成系统”，该系统可高效地对安全协议进行分析与验证，系统在对攻击者建模时采用偏序规约、语法重定序及类型检查等优化策略以提高验证效率，有效地缓解了模型检测过程中的状态爆炸问题。

关键词 安全协议 模型检测 简单进程元语言解释器 状态爆炸
分类号 TP393.08

Effective automatic generation of security protocol’s verification model

WU Chang[1]，XIAO Mei-hua[1]，LUO Min[2]，LIU Qiao-wei[1]，XIONG Hao[1]

1.Information Engineering School of Nanchang University，Nanchang 330031，China
2.Jiangxi Insititute of Computing Technology，Nanchang 330002，China

Abstract
Aiming at a more efficient analysis and verification of the security protocol with the model checking technology，this paper proposes a more efficient modeling algorithm with a wider applicability and higher level of automation.Based on this modeling algorithm，the“Generative System of Network Security Protocol Verification Model” is developed.This system can efficiently analyze and verify the security protocol.During the modeling of the intruder，the system improves the efficiency of verification and solves the problem of state explosion by using such optimization strategies as the partial order reduction，syntax reordering and type checking.

Key words security protocol model checking Simple PROMELA Interpreter（SPIN） state explosion

DOI: 10.3778/j.issn.1002-8331.2010.02.025

通讯作者 吴 昌 gooaler@163.com