计算机工程 2012, 38(3) 121-123 DOI: 10.3969/j.issn.1000-3428.2012.03.041 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

基于Hoare逻辑的密码软件形式化验证系统

郝耀辉，郭渊博，罗 婷，燕菊维

(解放军信息工程大学电子技术学院，郑州 450004)

摘要： 在Hoare逻辑理论和ACSL语法规范的基础上，设计一种针对密码软件的形式化验证系统，由程序规范、验证推理规则、可靠性策略、验证推理等模块组成。以OpenSSL中RC4算法的软件实现为例，对其功能正确性、保险性和信息流安全性进行验证，结果表明，该系统具有较高的自动化水平，可在一定程度上降低形式化验证方法的复杂度。

关键词： Hoare逻辑 密码软件 形式化验证 程序规范 RC4算法

Formal Verification System of Cryptographic Software Based on Hoare Logic

HAO Yao-hui, GUO Yuan-bo, LUO Ting, YAN Ju-wei

(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004, China)

Abstract: Based on Hoare logic and ANSI/ISO C Specification Language(ACSL) specification, this paper presents a formal verification system for cryptographic software, which is composed of program specification, inference rules, reliability strategy and verification module. It takes the software realization of RC4 algorithm in OpenSSL as an example, the functional correctness, safety properties and information flow security are tested and verified. Results show that this system can reduce the complexity of formal verification method and has a high level of automation.

Keywords: Hoare logic cryptographic software formal verification program specification RC4 algorithm

收稿日期 2011-05-17 **修回日期** **网络版发布日期** 2012-02-05

DOI: 10.3969/j.issn.1000-3428.2012.03.041

基金项目:

国家“863”计划基金资助项目“基于规范的容忍入侵中间件关键技术与平台”(2007AA01Z405)；河南省科技创新杰出青年计划基金资助项目(104100510025)

通讯作者:

作者简介: 郝耀辉(1978－)，女，讲师、硕士，主研方向：信息安全，密码学，数据库技术；郭渊博，副教授、博士；罗 婷，硕士研究生；燕菊维，助教、硕士

通讯作者E-mail: hao_yaohui@126.com

参考文献：

[2] 杨 静. 用Hoare 逻辑验证程序的一般方法及实例[J].通讯和计算机.2007, 4(2):79-81

[3] Baudin P, Cuoq P, Jean-Christophe F, et al. ACSL: ANSI/ISO C Specification Language Version 1.5[EB/OL]. [2011-02-21]. http:// frama-c.com/download/acsl.pdf.

[4] Almeida J B, Barbosa M, Pinto J S, et al. Deductive Verification of Cryptographic Software [J].Innovations in Systems and Software Engineering.2010, 6(3):203-218

[5] 李兆鹏, 陈意云, 葛 琳, 等. 一种汇编程序的形式验证框 架[J].计算机研究与发展.2008, 45(5):825-833

[6] Vieira B. Formal Verification of Security Policies of Crypto- graphic Software[EB/OL]. (2010-09-03). http://www3.dsi.uminho. pt/seeum2010/CD/abstracts/2165-4.pdf.

[7] Correnson L, Cuoq P, Puccetti A. Frama-c User Manual[EB/OL]. (2011-02-01). http://frama-c.com/download/frama-c-user-manual. pdf.

[8] The Coq Development Team. The Coq Proof Assistant Reference Manual[EB/OL]. (2010-12-23). http://coq.inria.fr/distrib/V8.3pl1/ files/Reference-Manual.pdf.

本刊中的类似文章

1. 常亚勤.对流密码RC4的区分攻击[J]. 计算机工程, 2011,37(3): 119-120,123
2. 陈亚莎, 胡俊, 沈昌祥.可信应用环境的安全性验证方法[J]. 计算机工程, 2011,37(23): 152-154
3. 梁盟磊, 王小平, 薛小平, 李刚.基于TLA的UML模型形式化验证[J]. 计算机工程, 2011,37(2): 72-74
4. 刘宴兵, 田四梅, 唐浩坤, 吕淑品.基于混沌的RC4流加密算法[J]. 计算机工程, 2011,37(2): 136-138
5. 全嘉辉, 张欢欢.基于FeaVer的MINIX 3验证和改进[J]. 计算机工程, 2010,36(22): 46-48
6. 喻超, 毋国庆.基于SAT工具的限界模型检测归约方法[J]. 计算机工程, 2010,36(17): 60-62
7. 方小丽;陈昊鹏.基于SOFL规约的复审理论及实现[J]. 计算机工程, 2006,32(18): 61-63

文章评论

反馈人		邮箱地址	
反馈标题		验证码	3284
	5		