

软件学报

Journal of Software

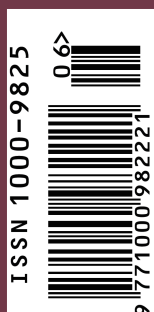
# 软件学报 *Software*

## Journal of

2022 年第 33 卷 第 6 期

系统软件安全专题  
定理证明理论与应用专题

科学出版社



主办



中国科学院软件研究所



中国计算机学会

出版



科学出版社



2013年全国百强科技期刊



2015年全国百强科技期刊



中国精品科技期刊



中国计算机学会会刊

# 软件学报

(Ruanjian Xuebao)

第33卷第6期  
2022年6月

## 目次

### 系统软件安全专题

系统软件安全专题前言 .....	杨珉	张超	宋富	张源	(1959)
反例引导的C代码空间流模型检测方法 .....	于银菠	刘家佳	慕德俊		(1961)
TaintPoint: 使用活跃轨迹高效挖掘污点风格漏洞 .....	方浩然	郭帆	李航宇		(1978)
基于前馈神经网络的编译器测试用例生成方法 .....					
.....	徐浩然	王勇军	黄志坚	解培岱	范书琿 (1996)
面向SGX2代新型可信执行环境的内存优化系统 .....		李明煜	夏虞斌	陈海波	(2012)
基于深度学习的Linux内核引用计数字段识别方法 .....	谈心	杨悉瑜	曹家俊	张源	(2030)
基于Toast重复绘制机制的口令攻击技术 .....					
.....	凌振	杨彦	刘睿钊	张悦	贾康 杨明 (2047)
开源C/C++静态软件缺陷检测工具实证研究 .....		李广威	袁挺	李炼	(2061)
面向缓解机制评估的自动化信息泄露方法 .....	杨松涛	陈凯翔	王准	张超	(2082)
一种采用对抗学习的跨项目缺陷预测方法 .....					
.....	邢颖	钱晓萌	管宇	章世豪	赵梦赐 林婉婷 (2097)

### 定理证明理论与应用专题

定理证明理论与应用专题前言 .....	曹钦翔	詹博华	赵永望	(2113)
机械化验证一个高效的迭代数据流求解算法 .....	江南	汪吕蒙	张晓瞳	何炎祥 (2115)
步进索引模型下的语义及其形式化 .....			郭昊	曹钦翔 (2127)
多旋翼飞控推进子系统的Coq形式化验证 .....	石正璞	崔敏	谢果君	陈钢 (2150)
支持索引式的PPTL定理证明器的实现 .....	王小兵	寇蒙莎	李春奕	赵亮 (2172)
基于精化的可信执行环境内存隔离机制验证 .....				
.....	靳翠珍	张倩颖	马雨薇	李希萌 王国辉 施智平 关永 (2189)
基于Coq的杨忠道定理形式化证明 .....		严升	郁文生	付尧顺 (2208)
基于Coq的矩阵代码生成技术 .....			麻莹莹	陈钢 (2224)
机器人碰撞检测方法形式化 .....	陈善言	关永	施智平	王国辉 (2246)
一种基于分离逻辑的块云存储系统验证工具 .....	张博闻	金钊	王捍贫	曹永知 (2264)

### 系统软件与软件工程

重复软件缺陷报告检测方法综述 .....					
.....	郑炜	王晓龙	陈翔	夏鑫	廖慧玲 刘程远 孙瑞阳 (2288)
面向安全关键内存管理系统分层验证方法 .....					
.....	李少峰	乔磊	杨孟飞	张锦坤	马智 刘洪标 (2312)

### 数据库技术

面向查询式实体解析的多属性数据索引技术 .....	孙琛琛	申德荣	肖迎元	李玉坤	(2331)
---------------------------	-----	-----	-----	-----	--------

### 计算机网络与信息安全

基于混洗差分隐私的直方图发布方法 .....	张啸剑	徐雅鑫	夏庆荣	(2348)
------------------------	-----	-----	-----	--------

期刊基本参数: CN11-2560/TP\*1990\*m\*16\*405\*zh+en\*P\*¥70\*2022\*22\*2022-06

## Contents

### **SPECIAL TOPIC ON SYSTEMS SOFTWARE SECURITY**

- 1959 Preface  
*YANG Min, ZHANG Chao, SONG Fu, ZHANG Yuan*
- 1961 Counterexample-guided Spatial Flow Model Checking Methods for C Codes  
*YU Yin-Bo, LIU Jia-Jia, MU De-Jun*
- 1978 TaintPoint: Fuzzing Taint Flow Efficiently with Live Trace  
*FANG Hao-Ran, GUO Fan, LI Hang-Yu*
- 1996 Compiler Fuzzing Test Case Generation with Feed-forward Neural Network  
*XU Hao-Ran, WANG Yong-Jun, HUANG Zhi-Jian, XIE Pei-Dai, FAN Shu-Hui*
- 2012 Memory Optimization System for SGXv2 Trusted Execution Environment  
*LI Ming-Yu, XIA Yu-Bin, CHEN Hai-Bo*
- 2030 Refcount Field Identification for Linux Kernel Based on Deep Learning  
*TAN Xin, YANG Xi-Yu, CAO Jia-Jun, ZHANG Yuan*
- 2047 Repeating Toast Drawing Based Password Inference Attack Technique  
*LING Zhen, YANG Yan, LIU Rui-Zhao, ZHANG Yue, JIA Kang, YANG Ming*
- 2061 Study of State-of-the-art Open-source C/C++ Static Analysis Tools  
*LI Guang-Wei, YUAN Ting, LI Lian*
- 2082 Exploit-oriented Automated Information Leakage  
*YANG Song-Tao, CHEN Kai-Xiang, WANG Zhun, ZHANG Chao*
- 2097 Cross-project Defect Prediction Method Using Adversarial Learning  
*XING Ying, QIAN Xiao-Meng, GUAN Yu, ZHANG Shi-Hao, ZHAO Meng-Ci, LIN Wan-Ting*

### **SPECIAL TOPIC ON THEOREM PROVING: THEORY AND APPLICATIONS**

- 2113 Preface  
*CAO Qin-Xiang, ZHAN Bo-Hua, ZHAO Yong-Wang*
- 2115 Mechanized Verification of Efficient Iterative Data-flow Algorithm  
*JIANG Nan, WANG Lü-Meng, ZHANG Xiao-Tong, HE Yan-Xiang*
- 2127 Semantics under Step-indexed Model and Formalization  
*GUO Hao, CAO Qin-Xiang*
- 2150 Coq Formalization of Propulsion Subsystem of Flight Control System for Multicopter  
*SHI Zheng-Pu, CUI Min, XIE Guo-Jun, CHEN Gang*
- 2172 Implementation of Theorem Prover for PPTL with Indexed Expressions  
*WANG Xiao-Bing, KOU Meng-Sha, LI Chun-Yi, ZHAO Liang*
- 2189 Refinement-based Verification of Memory Isolation Mechanism for Trusted Execution Environment  
*JIN Cui-Zhen, ZHANG Qian-Ying, MA Yu-Wei, LI Xi-Meng, WANG Guo-Hui, SHI Zhi-Ping, GUAN Yong*
- 2208 Formalization of C.T.Yang's Theorem in Coq  
*YAN Sheng, YU Wen-Sheng, FU Yao-Shun*
- 2224 Coq-based Matrix Code Generation Technology  
*MA Ying-Ying, CHEN Gang*
- 2246 Formalization of Collision Detection Method for Robots  
*CHEN Shan-Yan, GUAN Yong, SHI Zhi-Ping, WANG Guo-Hui*
- 2264 Tool for Verifying Cloud Block Storage Based on Separation Logic  
*ZHANG Bo-Wen, JIN Zhao, WANG Han-Pin, CAO Yong-Zhi*

### **SYSTEM SOFTWARE AND SOFTWARE ENGINEERING**

- 2288 Systematic Literature Review of Duplicated Bug Report Detection Methods  
*ZHENG Wei, WANG Xiao-Long, CHEN Xiang, XIA Xin, LIAO Hui-Ling, LIU Cheng-Yuan, SUN Rui-Yang*
- 2312 Verification Method of Hierarchical for Safety-critical Memory Management Systems  
*LI Shao-Feng, QIAO Lei, YANG Meng-Fei, ZHANG Jin-Kun, MA Zhi, LIU Hong-Biao*

### **DATABASE TECHNOLOGY**

- 2331 Multi-attribute Data Indexing for Query Based Entity Resolution  
*SUN Chen-Chen, SHEN De-Rong, XIAO Ying-Yuan, LI Yu-Kun*

### **COMPUTER NETWORKS AND INFORMATION SECURITY**

- 2348 Histogram Publication under Shuffled Differential Privacy  
*ZHANG Xiao-Jian, XU Ya-Xin, XIA Qing-Rong*