

软件学报 *Software* *Journal of*



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 30 卷第 8 期
2019 年 8 月

目次

面向自主安全可控的可信计算专题

面向自主安全可控的可信计算专题前言	张焕国	贾春福	林璟锵	(2227)
恶意代码演化与溯源技术研究	宋文纳	彭国军	傅建明	张焕国 陈施旅 (2229)
软件实时可信度量:一种无干扰行为可信性分析方法	张帆	徐明迪	赵涵捷	张聪 刘小丽 胡方宁 (2268)
基于 Duplication Authority 的 TPM2.0 密钥迁移协议	谭良	宋敏		(2287)
基于区块链的分布式可信网络连接架构	刘明达	拾以娟	陈左宁	(2314)
Midori-64 算法的截断不可能差分分析	李明明	郭建胜	崔竞一	徐林宏 (2337)
Piccolo 算法的相关密钥-不可能差分攻击	徐林宏	郭建胜	崔竞一	李明明 (2349)
基于倒排索引的可验证混淆关键字密文检索方案	杜瑞忠	李明月	田俊峰	吴万青 (2362)
无线传感器网络下多因素身份认证协议的内部人员攻击	李文婷	汪定	王平	(2375)
基于 Laplace 机制的普适运动传感器侧信道防御方案	唐奔宵	王丽娜	汪润	赵磊 陈青松 (2392)
面向中文文本倾向性分类的对抗样本生成方法	王文琦	汪润	王丽娜	唐奔宵 (2415)

系统软件与软件工程

面向模式软件体系结构合成中的冲突消解方法	徐永睿	梁鹏		(2428)
一种基于时变 Petri 网的服务组合质量检验方法	韩敏	孙国庆	郑丹晨	周惠巍 (2453)

计算机网络与信息安全

网络隐蔽信道关键技术研究综述	李彦峰	丁丽萍	吴敬征	崔强	刘雪花	关贝	王永吉	(2470)
移动边缘网络中计算迁移与内容缓存研究综述	张开元	桂小林	任德旺	李敬	吴杰	任东胜		(2491)
一种面向公有云的密文共享方案	罗王平	冯朝胜	秦志光	袁丁	廖娟平	刘霞		(2517)
无源感知网络中能耗和延迟平衡的机会路由协议	高宏超	陈晓江	徐丹	彭瑶	汤战勇	房鼎益		(2528)

计算机图形学与计算机辅助设计

非刚性三维形状匹配中基于谱分析的形状描述符综述	张丹	武仲科	王醒策	吕辰雷	刘香圆	周明全		(2545)
-------------------------------	----	-----	-----	-----	-----	-----	--	--------

《软件学报》投稿指南 (封三)

期刊基本参数: CN11-2560/TP*1990*m*16*344*zh+en*P*¥70*2019*18*2019-08

Contents

SPECIAL TOPIC ON AUTONOMOUS AND CONTROLLABLE TRUSTED COMPUTING

- 2227 Preface
ZHANG Huan-Guo, JIA Chun-Fu, LIN Jing-Qiang
- 2229 Research on Malicious Code Evolution and Traceability Technology
SONG Wen-Na, PENG Guo-Jun, FU Jian-Ming, ZHANG Huan-Guo, CHEN Shi-Lü
- 2268 Real-time Trust Measurement of Software: Behavior Trust Analysis Approach Based on Noninterference
ZHANG Fan, XU Ming-Di, CHAO Han-Chieh, ZHANG Cong, LIU Xiao-Li, HU Fang-Ning
- 2287 TPM2.0 Key Migration-protocol Based on Duplication Authority
TAN Liang, SONG Min
- 2314 Distributed Trusted Network Connection Architecture Based on Blockchain
LIU Ming-Da, SHI Yi-Juan, CHEN Zuo-Ning
- 2337 Truncated Impossible Differential Cryptanalysis of Midori-64
LI Ming-Ming, GUO Jian-Sheng, CUI Jing-Yi, XU Lin-Hong
- 2349 Related-key Impossible Differential Attack on Piccolo
XU Lin-Hong, GUO Jian-Sheng, CUI Jing-Yi, LI Ming-Ming
- 2362 Verifiable Obfuscated Keyword Ciphertext Retrieval Scheme Based on Inverted Index
DU Rui-Zhong, LI Ming-Yue, TIAN Jun-Feng, WU Wan-Qing
- 2375 Insider Attacks Against Multi-factor Authentication Protocols for Wireless Sensor Networks
LI Wen-Ting, WANG Ding, WANG Ping
- 2392 General Side Channel Defense Schema of Motion Sensor Based on Laplace Mechanism
TANG Ben-Xiao, WANG Li-Na, WANG Run, ZHAO Lei, CHEN Qing-Song
- 2415 Adversarial Examples Generation Approach for Tendency Classification on Chinese Texts
WANG Wen-Qi, WANG Run, WANG Li-Na, Tang Ben-Xiao

SYSTEM SOFTWARE AND SOFTWARE ENGINEERING

- 2428 Conflict Resolution Approach in Pattern-oriented Software Architectural Synthesis
XU Yong-Rui, LIANG Peng
- 2453 Test Method to Quality of Service Composition Based on Time-varying Petri Net
HAN Min, SUN Guo-Qing, ZHENG Dan-Chen, ZHOU Hui-Wei

COMPUTER NETWORKS AND INFORMATION SECURITY

- 2470 Survey on Key Issues in Networks Covert Channel
LI Yan-Feng, DING Li-Ping, WU Jing-Zheng, CUI Qiang, LIU Xue-Hua, GUAN Bei, WANG Yong-Ji
- 2491 Survey on Computation Offloading and Content Caching in Mobile Edge Networks
ZHANG Kai-Yuan, GUI Xiao-Lin, REN De-Wang, LI Jing, WU Jie, REN Dong-Sheng
- 2517 Ciphertext Sharing Scheme for the Public Cloud
LUO Wang-Ping, FENG Chao-Sheng, QIN Zhi-Guang, YUAN Ding, LIAO Juan-Ping, LIU Xia
- 2528 Balance of Energy and Delay Opportunistic Routing Protocol for Passive Sensing Network
GAO Hong-Chao, CHEN Xiao-Jiang, XU Dan, PENG Yao, TANG Zhan-Yong, FANG Ding-Yi

COMPUTER GRAPHICS AND COMPUTER AIDED DESIGN

- 2545 Survey on Shape Descriptors Based on Spectral Analysis for Non-rigid 3D Shape Matching
ZHANG Dan, WU Zhong-Ke, WANG Xing-Ce, LÜ Chen-Lei, LIU Xiang-Yuan, ZHOU Ming-Quan