

软件学报 *Software* Journal of



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 29 卷第 5 期
2018 年 5 月

目次

软件安全漏洞检测专题

软件安全漏洞检测专题前言 王林章 陈 恺 王 戟 (1177)

缓冲区溢出漏洞分析技术研究进展
..... 邵思豪 高 庆 马 森 段富尧 马 骁 张世琨 胡津华 (1179)

一种利用补丁的未知漏洞发现方法 李 赞 边 攀 石文昌 梁 彬 (1199)

面向漏洞生命周期的安全风险度量方法
..... 胡 浩 叶润国 张红旗 常德显 刘玉岭 杨英杰 (1213)

数值稳定性相关漏洞隐患的自动化检测方法
..... 沈维军 汤恩义 陈振宇 陈 鑫 李 彬 翟 娟 (1230)

大规模源代码增量式资源泄漏检测方法
..... 高志伟 计卫星 石剑君 王一拙 高五金 廖心怡 罗 辉 石 峰 (1244)

可编程模糊测试技术
..... 杨梅芳 霍 玮 邹燕燕 尹嘉伟 刘宝旭 龚晓锐 贾晓启 邹 维 (1258)

基于模式生成的浏览器模糊测试技术
..... 霍 玮 戴 戈 史 记 龚晓锐 贾晓启 宋振宇 刘宝旭 邹 维 (1275)

一种面向模糊测试的 GUI 程序空转状态实时检测方法 .. 张 兴 冯 超 雷 菁 唐朝京 (1288)

基于自适应模糊测试的 IaaS 层漏洞挖掘方法 .. 沙乐天 肖 甫 杨红柯 喻 辉 王汝传 (1303)

基于分布式信息流控制的无障碍辅助性服务安全加固 李晓娟 陈海波 (1318)

基于 IPT 硬件的内核模块 ROP 透明保护机制 王心然 刘宇涛 陈海波 (1333)

区块链的安全检测模型 叶聪聪 李国强 蔡鸿明 顾永跟 (1348)

基于运行时验证的无人飞行系统安全威胁检测方法
..... 杨 栋 史 浩 董 威 刘宗林 周 戈 (1360)

面向 Android 生态系统中的第三方 SDK 安全性分析 马 凯 郭山清 (1379)

基于宿主权限的移动广告漏洞攻击技术 王持恒 陈 晶 苏 涵 何 琨 杜瑞颖 (1392)

基于动态行为分析的网页木马检测方法 张卫丰 刘蕊成 许 蕾 (1410)

系统软件与软件工程

对软件工程中经验研究的调查 张 莉 蒲梦媛 刘奕君 田家豪 岳 涛 蒋 竞 (1422)

一种保持编排与参与者间行为一致的映射方法
..... 代 飞 陈凤强 莫 启 王 炜 李 彤 梁志宏 (1451)

计算机图形学与计算机辅助设计

医学影像计算机辅助检测与诊断系统综述 郑光远 刘峡壁 韩光辉 (1471)

《软件学报》投稿指南 (封三)

期刊基本参数: CN11-2560/TP*1990*m*16*340*zh+en*P*¥70*2018*20*2018-05

Contents**SPECIAL TOPIC ON SOFTWARE VULNERABILITY DETECTION**

- 1177 Preface
WANG Lin-Zhang, CHEN Kai, WANG Ji
- 1179 Progress in Research on Buffer Overflow Vulnerability Analysis Technologies
SHAO Si-Hao, GAO Qing, MA Sen, DUAN Fu-Yao, MA Xiao, ZHANG Shi-Kun, HU Jin-Hua
- 1199 Approach of Leveraging Patches to Discover Unknown Vulnerabilities
LI Zan, BIAN Pan, SHI Wen-Chang, LIANG Bin
- 1213 Vulnerability Life Cycle Oriented Security Risk Metric Method
HU Hao, YE Run-Guo, ZHANG Hong-Qi, CHANG De-Xian, LIU Yu-Ling, YANG Ying-Jie
- 1230 Method for Automated Detection of Suspicious Vulnerability Related to Numerical Stability
SHEN Wei-Jun, TANG En-Yi, CHEN Zhen-Yu, CHEN Xin, LI Bin, ZHAI Juan
- 1244 Incremental Resource Leak Detection for Large Scale Source Code
GAO Zhi-Wei, JI Wei-Xing, SHI Jian-Jun, WANG Yi-Zhuo, GAO Yu-Jin, LIAO Xin-Yi, LUO Hui, SHI Feng
- 1258 Programmable Fuzzing Technology
YANG Mei-Fang, HUO Wei, ZOU Yan-Yan, YIN Jia-Wei, LIU Bao-Xu, GONG Xiao-Rui, JIA Xiao-Qi, ZOU Wei
- 1275 Browser Fuzzing Technique Based on Pattern-Generation
HUO Wei, DAI Ge, SHI Ji, GONG Xiao-Rui, JIA Xiao-Qi, SONG Zhen-Yu, LIU Bao-Xu, ZOU Wei
- 1288 Real Time Idle State Deception Method in Fuzzing Test in GUI Program
ZHANG Xing, FENG Chao, LEI Jing, TANG Chao-Jing
- 1303 Vulnerability Discovery Method for Virtualization in IaaS Based on Self-Adapting Fuzzing Test
SHA Le-Tian, XIAO Fu, YANG Hong-Ke, YU Hui, WANG Ru-Chuan
- 1318 Security Reinforcement of Accessibility Service Based on Decentralized Information Flow Control
LI Xiao-Juan, CHEN Hai-Bo
- 1333 Transparent Protection of Kernel Module Against ROP with Intel Processor Trace
WANG Xin-Ran, LIU Yu-Tao, CHEN Hai-Bo
- 1348 Security Detection Model of Blockchain
YE Cong-Cong, LI Guo-Qiang, CAI Hong-Ming, GU Yong-Gen
- 1360 Security and Safety Threat Detection Method for Unmanned Aerial System Based on Runtime Verification
YANG Dong, SHI Hao, DONG Wei, LIU Zong-Lin, ZHOU Ge
- 1379 Security Analysis of the Third-Party SDKs in the Android Ecosystem
MA Kai, GUO Shan-Qing
- 1392 Mobile Advertising Loophole Attack Technology Based on Host APP's Permissions
WANG Chi-Heng, CHEN Jing, SU Han, HE Kun, DU Rui-Ying
- 1410 Web Page Trojan Detection Method Based on Dynamic Behavior Analysis
ZHANG Wei-Feng, LIU Rui-Cheng, XU Lei

SYSTEM SOFTWARE AND SOFTWARE ENGINEERING

- 1422 Investigation of Empirical Researches in Software Engineering
ZHANG Li, PU Meng-Yuan, LIU Yi-Jun, TIAN Jia-Hao, YUE Tao, JIANG Jing
- 1451 Projection Approach for Keeping the Behavior Consistency Between Choreography and Peers
DAI Fei, CHEN Feng-Qiang, MO Qi, WANG Wei, LI Tong, LIANG Zhi-Hong

COMPUTER GRAPHICS AND COMPUTER AIDED DESIGN

- 1471 Survey on Medical Image Computer Aided Detection and Diagnosis Systems
ZHENG Guang-Yuan, LIU Xia-Bi, HAN Guang-Hui