

软件可信性与供应链安全前沿进展专题前言*

向剑文¹, 郑征², 申文博³, 常瑞³, 田聪⁴



¹(交通物联网技术湖北省重点实验室(武汉理工大学 计算机与人工智能学院), 湖北 武汉 430070)

²(北京航空航天大学 自动化科学与电气工程学院/软件学院, 北京 100191)

³(浙江大学 计算机科学与技术学院/网络空间安全学院, 浙江 杭州 310027)

⁴(西安电子科技大学 计算机科学与技术学院, 陕西 西安 710126)

通信作者: 向剑文, Email: jwxiang@whut.edu.cn

中文引用格式: 向剑文, 郑征, 申文博, 常瑞, 田聪. 软件可信性与供应链安全前沿进展专题前言. 软件学报, 2023, 34(6): 2507–2508. <http://www.jos.org.cn/1000-9825/6854.htm>

随着计算机应用的不断发展, 软件已经渗透到国民经济和国防建设的各个领域, 在信息社会中发挥着至关重要的作用. 同时, 各行各业依赖各类软件, 软件的可信性与供应链安全已成为学术界和工业届不可忽视的根本性问题. 一方面, 人们对软件的可靠性、安全性、防危性等传统可信性质以及可解释性、隐私性和公平性等新兴可信性质提出了更多和更高的要求; 另一方面, 复杂的软件供应链引入的一系列安全问题, 导致信息系统的整体安全防护难度也越来越大. 保证软件供应链安全是一项宏大的系统化工程, 包含软件供应链上软件设计与开发的各个阶段中来自本身的编码过程、工具、设备或供应链上游的代码、模块和服务的安全, 以及软件交付渠道安全. 因此, 软件可信性和软件供应链安全性问题已具有重大的挑战性, 也是众多国内外学者迫切探索的科研热点和关注焦点, 亟需国内外学者对软件的开发和运行中的软件可信性以及软件供应链的各个环节、各种新兴技术展开广泛的探索、研究和交流. 因此, 本专题的主题将围绕软件可信性方面的理论、方法和技术, 以及软件供应链中软件开发、测试、交付、运行、维护等各个环节的安全风险, 探讨包含固件、操作系统、系统软件、编译器、应用软件等各个层次软件的可信性和供应链安全问题.

本专题公开征文, 共收到投稿 29 篇. 论文均通过了形式审查, 内容涉及软件可信性和软件供应链安全等方向. 特约编辑先后邀请了 50 多位专家参与审稿工作, 每篇投稿至少邀请 2 位专家进行评审. 稿件经过初审、复审、CCF ChinaSoft 2022 会议宣读和终审 4 个阶段, 历时 6 个月, 最终有 8 篇论文入选本专题. 根据主题, 这些论文可以分为 2 组.

(1) 软件可信性

《GKCI: 改进的基于图神经网络的关键类识别方法》基于图神经网络技术提出了一种有监督的软件系统关键类识别方法, 通过识别关键类来提高软件的可靠性和稳定性.

《图卷积网络的抗混淆安卓恶意软件检测》将应用的程序语义提取为函数调用图, 保留语义信息的同时采用抽象 API 技术将调用图转换为抽象图, 以减少运行开销并增强鲁棒性.

《基于图神经网络的切片级漏洞检测及解释方法》提出基于图神经网络的切片级漏洞检测及解释方法, 可有效提高漏洞检测和漏洞解释的性能.

《结合情节挖掘的软件实体演化耦合分析方法》提出基于关联规则挖掘、情节挖掘、潜在语义索引模型结合的演化耦合分析方法(association rule, MINEPI and LSI based method, AR-MIM), 挖掘有“距离”的共同变更关系.

《基于凸优化的无人驾驶汽车转向角安全性验证》提出了一种自动验证技术, 通过结合凸优化和深度学习验证工具 DLV 来保障无人驾驶汽车的转向角安全.

* 收稿时间: 2023-01-17

(2) 软件供应链安全

《面向软件供应链的异常分析方法综述》对适用于库函数的异常分析方法从精度和效率两方面分别进行总结归纳,对于每种异常分析方法的基本思想和重要过程进行阐述,并针对库函数异常分析面临的挑战给出初步解决思路。

《面向 Java 语言生态的软件供应链安全分析技术》给出软件供应链安全领域的组件依赖关系和影响力等重要指标的形式化定义,提出基于索引文件的增量式组件配置收集和基于 POM 语义的多核并行依赖解析,并设计实现了 Java 开源生态组件依赖关系提取与解析框架。

《基于指标依赖模型构建与监控的攻击检测方法》提出基于攻击指标依赖模型的攻击检测方法以更有效应对攻击变种,着眼于漏洞利用后对系统的影响而非变化多样的攻击行为,具有更强的泛化能力。

本专题主要面向软件可信性和软件供应链安全等领域的研究人员和工程人员,反映了我国学者在相关领域最新的研究进展。感谢《软件学报》编委会、CCF 数据库专委会和 CCF 系统软件专委会对专题工作的指导和帮助,感谢专题全体评审专家及时、耐心、细致的评审工作,感谢踊跃投稿的所有作者。希望本专题能够对软件可信性和软件供应链安全等相关领域的研究工作有所促进。



向剑文(1975—),男,武汉理工大学计算机与人工智能学院教授,博士生导师,副院长,湖北省百人计划特聘专家,湖北省创新群体负责人,CCF 系统软件专委会与软件工程专委会执行委员,中国电子学会可靠性分会委员,工业软件工程化与应用技术工信部重点实验室与工业控制系统安全与可靠测评共性技术工信部重点实验室学术委员会委员。主要研究方向包括软件可靠性工程与可信计算等。相关工作发表在 IEEE TR、IEEE TIFS、IEEE TETC、RESS、ISSRE 等期刊和会议上,担任 ISSRE 2021 等多个国际会议大会主席。



郑征(1980—),男,北京航空航天大学教授,博士生导师,副院长,CCF 软件工程专委会和容错计算专委会执行委员,航空学会测试专委会委员,获得 2019 年国防科技进步一等奖,2022 年航空学会技术发明二等奖,2012 年军队科技进步三等奖。主要研究方向为软件可靠性与测试,智能软件可靠性工程。相关工作发表在 IEEE TSE、IEEE TDSC、IEEE TIFS、FSE、ISSRE 等期刊和会议上,担任《IEEE Trans. on Reliability》、《Knowledge-based Systems》和《Int'l Journal of Computational Intelligence Systems》副主编,担任《IEEE Trans. on Dependable and Secure Computing》“软件可靠性与可信性工程”专刊客座主编,担任 PRDC 2019 等程序委员会主席,担任 DeIS 2020 等大会主席。



申文博(1989—),男,浙江大学百人计划研究员,博士生导师,浙江大学计算机科学与工程系副主任,移动终端安全-浙江省工程中心副主任,CCF 系统软件专委会委员。主要研究方向为操作系统安全,云原生系统安全,软件供应链安全,芯片安全机制。在 IEEE S&P、ACM CCS、USENIX Security 等计算机安全、系统、网络国际顶级会议、期刊上发表论文 30 余篇,获得 3 项杰出论文奖(NDSS 16、AsiaCCS 17、ACSAC 22)。主持国家自然科学基金、科技部重点研发课题等 10 余项科研项目。常年活跃于系统/软件安全攻防的第一线,通过分析实际攻击,设计相应的系统保护方案,具有学术界和工业界的双重研究经历和视野;多年来设计、实现并主导部署了多种软件及操作系统安全机制,保护超过亿部设备系统安全。



常瑞(1981—),女,浙江大学副教授,博士生导师,CCF 高级会员,CCF 系统软件、体系结构和形式化方法专委会委员。从事系统安全方向的科研与教学 10 余年,于解放军信息工程大学获得计算机科学与技术博士学位,并获 ACM 中国优秀博士学位论文分会奖。研究成果曾获省部级教学成果一等奖 1 项、省部级科技进步二等奖 2 项等,被评为全军优秀教师。研究方向包括系统安全、软件供应链安全、程序分析、形式化验证等,相关研究工作发表在 ASPLOS、TDSC、TSE、DAC、S&P 等国际顶级会议/期刊上。近 3 年指导学生多次获奖。



田聪(1981—),女,西安电子科技大学研究生院常务副院长,计算机科学与技术学院教授,博士生导师,教育部“长江学者”特聘教授,获国家自然科学基金优秀青年基金,教育部新世纪优秀人才资助。主要研究方向为软件安全、智能软件开发方法、可信软件基础理论与方法,相关工作发表于 TSE、TOSEM、LICS 等 CCF A 类期刊、会议以及著名国际期刊 TCS。现任国际期刊《JOCO》编委、《软件学报》编委,中国计算机学会杰出会员、形式化方法专委会常委、女工委委员。担任 ICFEM 2017 组织委员会主席(获优秀组织者奖)以及 COCOON 2019、SATE 2019 等程序委员会主席。获教育部自然科学一等奖和陕西省科学技术一等奖。