软件学报 ISSN 1000-9825, CODEN RUXUEW
2026,37(7):2691−2693 [doi: 10.13328/j.cnki.jos.007591] [CSTR: 32375.14.jos.007591]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

智能化基础软件可信构造和供应链安全专题前言*

王林章[1], 司徒凌云[2], 钟 浩[3], 向剑文[4], 张 路[5]

[1](南京大学 计算机学院, 江苏 南京 210046)

[2](南京大学 信息管理学院, 江苏 南京 210046)

[3](上海交通大学 计算机学院, 上海 200240)

[4](武汉理工大学 计算机与人工智能学院, 湖北 武汉 430070)

[5](北京大学 计算机学院, 北京 100871)

通信作者: 王林章, E-mail: lzwang@nju.edu.cn; 司徒凌云, E-mail: stly@nju.edu.cn; 钟浩, E-mail: zhonghao@sjtu.edu.cn; 向剑文, E-mail: jwxiang@whut.edu.cn; 张路, E-mail: zhanglucs@pku.edu.cn

中文引用格式: 王林章, 司徒凌云, 钟浩, 向剑文, 张路. 智能化基础软件可信构造和供应链安全专题前言. 软件学报, 2026, 37(7): 2691–2693. http://www.jos.org.cn/1000-9825/7591.htm

在“人机物”三元融合的万物智能互联时代, 以系统软件、人工智能框架系统、关键基础设施控制软件、嵌入智能模型的领域软件系统为代表的智能化基础软件将成为软件定义之本、信息技术之魂、数字社会之基. 智能化基础软件可信构造和供应链安全对于支撑经济社会发展、提升国家安全保障能力具有重要意义. 本专题主要致力于融合软件工程、计算机科学与技术、网络空间安全、人工智能、信息资源管理、国家安全学等多学科交叉创新能力, 汇聚多领域方向专家力量, 探索基于开源/AIGC 的智能化基础软件可信构造、智能化基础软件供应链成分分析与异常检测、智能化基础软件供应链缺陷/漏洞检测与预测等关键技术, 突破智能化基础软件可信构造和供应链安全关键技术瓶颈, 实现自主可控, 保障关键信息基础设施安全.

本专题公开征文, 第 1 轮 ChinaSoft 2025 专题论坛征稿共收到 25 篇投稿, 第 2 轮《软件学报》专题征稿共收到 29 篇投稿. 论文通过形式审查, 内容涉及智能化基础软件可信构造和供应链安全相关议题. 特约编辑先后邀请了国内外近 40 位专家参与两轮审稿工作, 每篇投稿邀请不少于 2 位专家进行评审. 稿件经过第 1 轮 ChinaSoft 2025 专题论坛的初审及复审、第 2 轮《软件学报》专题的初审及复审、ChinaSoft 2025 会议现场汇报与专家质询、特约编辑终审阶段, 历时 5 月有余, 最终有 10 篇论文入选本专题. 根据从软件可信构造到供应链安全的主题顺序, 这些论文可以分为 3 组.

(1) 基于开源/AIGC 的智能化基础软件可信构造

《基于大语言模型的 Java 新特性测试程序生成》针对现有工作难以对语言新特性进行有效测试的问题, 提出一种基于大语言模型 (large language model, LLM) 的 Java 新特性测试程序生成方法 LimiX. 该方法利用 LLM 的文本理解能力生成语言新特性的使用描述, 基于程序分析从种子程序中识别可复用的程序元素, 并将新特性使用描述与可复用程序元素相结合, 借助 LLM 的代码生成能力生成能够覆盖语言新特性的测试程序. 在对最新发布的 Java 编译器及虚拟机的测试中, 累计发现 16 个未知缺陷, 其中 12 个已被开发人员确认或修复.

《Python 软件包库中 C/C++外部语言调用的安全性分析》构建了 Python-C/C++互操作程序的漏洞基准套件, 评估了已有的先进 Python-C/C++互操作漏洞检查工具, 对比分析了现有研究和工具的可靠性、完备性和可扩展性, 在 Python 软件供应链高下载量的项目中发现了多个漏洞, 总结了 Python-C/C++互操作安全分析的现状和不足.

《面向 Discord 平台的开源软件实践者沟通实证研究》围绕 Discord 平台上开源软件实践者的沟通开展了大规模实证研究. 基于构建的两个数据集, 从消息层面与对话层面两个维度, 系统刻画了开源软件实践者的沟通特

* 收稿时间: 2025-12-26; jos 在线出版时间: 2025-12-26

征, 分析了不同沟通特征对对话响应时间与问题解决状态的影响. 在此基础上, 总结了对在线交流平台设计的启示, 提出了针对开源社区管理的建议, 指出了未来研究方向.

《产业研发视角下的开源软件供应链攻击问题研究》基于产业研发视角, 剖析研发效率与软件安全之间的内生矛盾, 揭示当前组织流程合规中存在的隐性共识. 结合实际案例, 论证了基于流程合规的安全体系难以有效应对开源软件供应链攻击, 进而提出基于产业视角的开源软件供应链攻击分类演化框架与安全再平衡体系, 为学术研究与产业实践提供理论分析框架与安全实践指引.

(2) 智能化基础软件供应链成分分析与异常检测

《CAnalyzer: 面向 C/C++ 源代码的软件成分分析技术》针对软件成分分析 (software composition analysis, SCA) 技术在 C/C++生态中存在的限制: 特征库覆盖不全、检测与报告粒度不一致、依赖关系分析能力不足, 提出 CAnalyzer, 构建覆盖全面的第三方库特征库, 引入多级阈值检测机制, 并基于模块划分构建依赖图. CAnalyzer 已落地应用于 OpenHarmony 社区, 在 689 个仓库中成功识别出 166 项外部组件.

《PCLog: 近端策略优化与行为克隆自适应日志异常检测》提出了一种新型日志异常检测框架. 针对现有方法难以适应系统升级导致的日志模式变化、缺乏高效反馈机制等问题, 该方法将检测模型建模为强化学习智能体, 以日志语义向量为状态, 以日志事件为动作, 通过近端策略优化 (proximal policy optimization, PPO) 算法最大化正常序列累计奖励, 学习系统正常行为模式. 当检测性能下降时, 收集错误预测样本作为专家示范, 结合行为克隆方法微调模型, 实现自适应修正. 在 HDFS、BGL 与 OpenStack 数据集上的实验结果表明, 该方法检测精度与动态适应能力优异, 为动态系统日志异常检测提供了可靠解决方案.

《基于异常检查点植入的软件缺陷定位方法》提出在更为广泛、真实的环境中利用程序异常信息开展缺陷定位, 通过为错误程序自动植入临时的异常处理语句作为对运行时内部状态的检查点, 设计更加先进的程序语句风险值计算方法, 将先前所提出 SOTA 方法的适用范围拓展到不包含异常处理语句的更普遍程序, 有效泛化异常触发信息这一缺陷定位轻量、高效源数据的应用场景, 并大幅缓解困扰缺陷定位技术的语句风险值捆绑问题.

(3) 智能化基础软件供应链缺陷/漏洞检测与预测

《软件供应链安全中 LLM 生成代码逻辑性缺陷检测》提出了一种融合符号执行的供应链 LLM 生成代码缺陷检测方法, 通过符号执行挂载机制自动识别 LLM 生成代码的输入参数并进行适配和符号挂载, 制导符号执行引擎对程序的关键路径进行精确的约束分析, 生成高效的边界测试用例, 检测深层逻辑性程序缺陷.

《面向 Web 应用漏洞检测的多数据流静态分析方法》提出了一种面向 Web 安全漏洞检测的多数据流静态分析方法, 通过引入多段数据流分析与多标签数据流分析两类技术, 对传统污点分析算法能力进行多维度扩展, 实现了面向 Java/JavaScript Web 应用的漏洞检测原型系统 MultiFlow, 提升了漏洞检测能力与泛用性.

《基于个性化联邦学习的跨项目软件缺陷预测方法》针对跨项目软件缺陷预测中数据隐私与项目异构性的双重挑战, 提出了名为 PRIDE-SDP 的创新框架. 该框架深度融合 3 项关键技术: 采用个性化联邦学习范式为异构项目定制专属预测模型, 集成 (ε, δ)-差分隐私机制保障数据不出本地, 并设计时间-上下文融合网络 (temporal-contextual fusion network, TCFN) 以高效捕捉软件度量特征. 在覆盖 27 个开源项目和 3 个企业项目的 6 个数据集组上, 实验验证了框架的有效性: 与先进基线方法相比, *AUC* 平均提升 10.7%, 且在提供较强隐私保障时性能保持率仍达 98% 以上.

本专题主要面向软件工程、计算机科学与技术、网络空间安全、人工智能、信息资源管理、国家安全学等多领域的研究人员和工程人员, 反映了我国学者在智能化基础软件可信构造和供应链安全领域最新的研究进展. 感谢《软件学报》编委会、系统软件专委会和中国软件大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. 希望本专题能够对智能化基础软件可信构造和供应链安全相关领域的研究工作有所促进.

作者简介

王林章, 博士, 南京大学教授, 博士生导师, CCF 会士, 主要研究领域为系统软件, 软件工程, 智能化软件分析与测试, 大规模复杂基础软件

的可信保障. 担任全国信息技术标准化委员会委员、CCF 理事、江苏省计算机学会常务理事、软件专委会主任, 曾任中国计算机学会系统软件专委会副主任、秘书长. 在程序语言、软件工程、系统软件等软件领域旗舰期刊和会议上发表多篇论文, 获 OOPSLA 2020 杰出论文奖和 OOPSLA 2013 最佳论文奖. 参与制定多项国家标准, 主持国家自然科学基金重点项目、国家重点研发计划、华为等头部企业技术攻关项目多项, 成果服务于国家重大需求和产业应用, 成效显著.

司徒凌云, 博士, 南京大学特聘研究员, 博士生导师, CCF 专业会员, 主要研究领域为软件供应链安全, 漏洞情报分析, 开源生态治理. 出版学术专著 1 部. 在领域核心期刊和高水平学术会议上发表论文 30 余篇, 获最佳论文奖 2 次, 优秀论文一等奖 1 次. 申请发明专利 7 项, 完成科技成果转化 4 项. 自主研发多个重要的漏洞检测工具与数据库系统, 实际应用于华为等国际一流 IT 企业.

钟浩, 博士, 上海交通大学研究员, 博士生导师, CCF 专业会员, 主要研究领域为经验软件工程和挖掘软件工程数据. 曾获得 ACM 杰出论文奖、ASE 最佳论文奖和 APSEC 最佳论文奖. 曾多次担任 ICSE、ASE、ESEC/FSE 等软件工程领域顶级会议的程序委员. 现为软件工程领域顶级期刊 TSE 的副主编.

向剑文, 博士, 武汉理工大学教授, 博士生导师, CCF 专业会员, 主要研究领域为网络安全, 可靠性工程. 担任高可信软件技术湖北省国际科技合作基地主任、交通信息与安全教育部工程研究中心副主任. 曾主持国家重点研发计划、国家自然科学基金、国家 242 信息安全专项、湖北省重大专项、湖北省重点研发计划、湖北省创新群体等项目 20 余项, 担任 ISSRE 指导委员会副主席和多个国际会议大会主席或 PC 主席, 在中国软件大会 2022–2024 年连续 3 年成功举办论文专题论坛.

张路, 博士, 北京大学计算机学院教授, 博士生导师, CCF 杰出会员, 主要研究领域为软件分析与测试. 在软件工程领域重要期刊和会议上发表论文 100 余篇. 现任《Science China: Information Science》《软件学报》编委, 曾任 2017 年 ICSME 程序委员会共同主席和 FSE、OOPSLA、ASE、ISSTA 等重要国际会议的程序委员会委员.