软件学报 ISSN 1000-9825, CODEN RUXUEW
2025,36(7):2927−2928 [doi: 10.13328/j.cnki.jos.007342] [CSTR: 32375.14.jos.007342]

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

新兴软件与系统的可信赖性与安全专题前言*

向剑文[1], 陈 厅[2], 杨 珉[3], 周俊伟[1]

[1](武汉理工大学 计算机与人工智能学院, 湖北 武汉 430070)

[2](电子科技大学 计算机科学与工程学院, 四川 成都 611731)

[3](复旦大学 计算机科学技术学院, 上海 200433)

通信作者: 向剑文, E-mail: jwxiang@whut.edu.cn; 陈厅, E-mail: brokendragon@uestc.edu.cn;
杨珉, E-mail: m_yang@fudan.edu.cn; 周俊伟, E-mail: junweizhou@whut.edu.cn

中文引用格式: 向剑文, 陈厅, 杨珉, 周俊伟. 新兴软件与系统的可信赖性与安全专题前言. 软件学报, 2025, 36(7): 2927–2928. http://www.jos.org.cn/1000-9825/7342.htm

随着人工智能技术的发展, 特别是通用人工智能的快速发展, 新兴软件与系统快速智能化, 同时带来巨大的复杂性和不确定性, 其可靠性与安全挑战更加复杂多样, 涉及面更广, 风险更难以预测和控制. 一方面, 这种复杂性和不确定性给新兴软件与系统本身的可靠性与稳定性带来巨大的挑战. 例如, 新兴软件与系统包括复杂功能、架构和交互等, 增加了系统出错的可能性, 同时增加了故障排除的难度; 在新兴软件与系统的开发过程中, 快速迭代和持续更新引入新问题; 新兴软件与系统往往依赖于众多第三方库、框架和服务, 不合理的依赖导致系统不稳定或不可用等; 人工智能自身在脆弱性、可预测性、可解释性等方面存在的安全隐患或问题, 转移或嫁接到新兴软件与系统上. 另一方面, 随着技术的不断进步, 针对新兴软件与系统的安全威胁与攻击相继出现, 攻击手法也在不断演变. 例如, 针对人工智能系统的对抗样本攻击、对抗性机器学习攻击、模型篡改和注入攻击等, 针对开源软件系统的软件供应链攻击, 针对传统密码系统的量子霸权攻击, 针对区块链系统的 51% 攻击、智能合约漏洞利用等, 都是传统软件系统所不具备的新型攻击手法. 本专题关注新兴软件与系统的可信赖与安全性技术, 特别是人工智能和新兴软件与系统交叉融合过程中伴生的可信赖与安全问题、人工智能赋能的攻击和防御技术.

本专题公开征文, 共收到投稿 42 篇. 论文均通过了形式审查, 内容涉及分布式系统测试、编译器灰盒测试、深度学习编译器缺陷实证研究、代码异味检测、安全虹膜识别技术、漏洞检测等, 特约编辑先后邀请了 40 多位专家参与审稿工作, 每篇投稿至少邀请 3 位专家进行评审. 稿件经初审、复审、CCF 中国软件大会 2024 宣读和终审 4 个阶段, 历时 6 个月, 最终有 9 篇论文入选本专题. 这些论文的内容如下所示.

《eDPRF: 高效的差分隐私随机森林训练算法》提出了一种高效的差分隐私随机森林训练算法, 有效地改善了树模型在扰动情况下的学习能力, 平衡了隐私保护与模型准确性之间的矛盾.

《语义可感知的灰盒编译器模糊测试》提出了一种语义可感知的灰盒模糊测试方法, 设计并实现了一系列语义可感知的变异操作符, 并开发了高效的选择策略, 显著提升了代码覆盖率.

《分布式系统动态测试技术研究综述》提出了分布式系统 4 层缺陷威胁模型, 并基于该模型分析了分布式系统的测试需求与主要挑战, 讨论了新趋势及未来发展方向.

《面向函数内联场景的二进制到源代码函数相似性检测方法》提出了面向一对多匹配的二进制到源代码函数相似性检测方法, 不仅提升了现有检测能力, 而且还能找到内联的源代码函数, 能够更好地应对内联挑战.

《深度学习编译器缺陷实证研究: 现状与演化分析》从多个角度深入挖掘深度学习编译器缺陷的分布特征, 为更好地检测、定位和修复深度学习编译器缺陷, 提供了一系列可行的指导方案.

《Java 依赖异味的实证研究与统一检测技术》提出了依赖异味概念, 以解决日益复杂的依赖管理问题. 通过

* 收稿时间: 2024-12-12; jos 在线出版时间: 2024-12-12

大规模实证研究, 总结出 13 类依赖异味及其根源和影响特征, 并设计了实现的检测工具.

《结合特征生成与重放的可扩展安全虹膜识别》提出了基于生成特征重放的和基于隐私保护模板重放的安全增量虹膜识别方法. 其方案具备有效的可扩展性, 能够在新的用户注册下依旧保持性能.

《面向智能体路径规划算法的动态随机测试方法》将动态随机测试思想引入路径规划算法中, 提出了面向路径规划算法的动态随机测试方法, 可以生成更多能够暴露被测算法性能缺陷的测试用例.

《基于函数间结构特征关联的软件漏洞检测方法》通过门控图神经网络提取函数内的独立结构特征, 并利用特征之间的相似性构建函数间的关联网络, 基于图注意力网络提取函数间的关联信息, 提升漏洞检测的性能.

本专题主要面向软件工程、系统安全、网络安全等多领域的研究人员和工程人员, 反映了我国学者在新兴软件与系统的安全检测、防御与溯源等技术领域的最新研究进展. 感谢《软件学报》编委会、软件工程专委会和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工程、系统软件等相关领域的研究工作有所促进.

向剑文(1975－), 男, 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, 可信计算, 软件工程.

陈厅(1987－), 男, 博士, 电子科技大学教授, 博士生导师, CCF 高级会员, 主要研究领域为软件安全, 尤其是区块链攻击交易检测, 智能合约行为识别, 区块链资源滥用防御.

杨珉(1979－), 男, 博士, 复旦大学教授, 博士生导师, CCF 杰出会员, 主要研究领域为网络安全, 主要包括恶意代码检测, 漏洞分析挖掘, AI 安全, 区块链安全, Web 安全, 系统安全机制.

周俊伟(1986－), 男, 博士, 武汉理工大学教授, 博士生导师, CCF 专业会员, 主要研究领域为系统安全, 日志分析.