软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, 2022,33(6):1959−1960 [doi: 10.13328/j.cnki.jos.006572]

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

系统软件安全专题前言*

杨 珉[1], 张 超[2], 宋 富[3], 张 源[1]

[1](复旦大学 计算机科学技术学院, 上海 200438)

[2](清华大学 网络科学与网络空间研究院, 北京 100084)

[3](上海科技大学 信息科学与技术学院, 上海 201210)

通信作者: 杨珉, E-mail: m_yang@fudan.edu.cn; 张超, E-mail: chaoz@tsinghua.edu.cn;
宋富, E-mail: songfu@shanghaitech.edu.cn; 张源, E-mail: yuanxzhang@fudan.edu.cn

中文引用格式: 杨珉, 张超, 宋富, 张源. 系统软件安全专题前言. 软件学报, 2022, 33(6): 1959–1960. http://www.jos.org.cn/1000-9825/6572.htm

系统软件是控制和协调计算机底层硬件及外部设备、支持应用软件开发和运行的系统核心基础软件, 涵盖了操作系统、编程语言、编译器、解释器、数据库、运行时环境、集成开发环境等. 随着人工智能、物联网、区块链、系统编程语言、云计算、开源指令集等领域的快速发展, 相关系统软件的安全问题大量涌现, 比如利用 CPU 预测执行的 Meltdown“熔断”和 Spectre“幽灵”攻击、利用软件供应链发起的后门攻击和漏洞攻击. 发现、缓解和防御系统软件存在的安全风险与问题, 对于保障各类计算机系统的安全至关重要.

近年来, 网络空间安全和国产基础软件已经成为保障国家网络空间安全的重要战略方向, 各部委也发布了众多研发项目以支持相关研究, 国内学者在这一重要方向上也取得一系列重要进展. 为此, 我们组织系统软件安全专题, 探讨各类新兴技术相关系统软件所面临的挑战, 及时反映我国在该领域的研究进展、促进国内系统软件安全的发展和相关学者的广泛交流.

本专题采取公开征文、自由投稿的方式, 共收到 21 篇投稿. 特约编辑邀请了 20 多位国内外领域专家参与审稿, 除 4 篇投稿由于不符合本次专题主题或技术创新不足之外, 其余 17 篇投稿的每篇投稿至少邀请 2 位专家进行初审, 13 篇论文通过初审, 每篇录用稿件都经过初审和复审两轮评审, 部分稿件经过了两轮复审.通过初审的稿件还在 ChinaSoft 2021 大会上进行了线上报告, 作者现场回答了与会者的问题, 并听取了与会者的修改建议. 最终 9 篇论文入选本专题. 其中,

论文《反例引导的 C 代码空间流模型检测方法》通过结合模型检测与稀疏值流分析方法, 设计了一种空间流模型, 实现了对 C 程序在符号变量层面和地址空间层面的状态行为的有效描述, 并提出了一种反例引导的抽象细化和稀疏值流强更新算法(CEGAS), 实现了 C 程序指向信息敏感的形式化验证.

论文《TaintPoint: 使用活跃轨迹高效挖掘污点风格漏洞》详细分析现有反馈机制在检测污点风格漏洞时不够高效的原因, 提出了专用于污点风格漏洞挖掘的模糊器 TaintPoint.

论文《基于前馈神经网络的编译器测试用例生成方法》针对现有方法生成测试用例的语法正确率不足、生成效率低的问题, 提出一种基于前馈神经网络的编译器模糊测试用例生成方法,并设计实现了原型工具 FAIR.

论文《面向 SGX2 代新型可信执行环境的内存优化系统》针对配置大容量安全内存引起的两个新问题, 该文提出一种全新的轻量级代码迁移方案, 将普通应用的代码动态迁移入安全内存中, 而数据保留在原地不动, 迁移后的代码可使用安全内存, 避免因磁盘换页导致的剧烈性能下降.

论文《基于深度学习的 Linux 内核引用计数字段识别方法》针对传统基于代码模式匹配的引用计数字段识别方法需要专家经验总结规则、人工开销大和总结的模式无法覆盖所有情况等局限, 提出了内核引用计数

* 收稿时间: 2022-02-16

字段表征特征，设计实现了基于多模态深度学习的引用计数字段识别方法，并在 Linux 内核上进行了实证研究.

论文《基于 Toast 重复绘制机制的口令攻击技术》利用 Android 系统中 Toast 机制的设计缺陷,结合 Android 无障碍服务提出了一种新型口令攻击,在真实应用场景中进行攻击实验，揭示了 Android 系统中可以被攻击者利用的安全隐患.

论文《开源 C/C++静态软件缺陷检测工具实证研究》在 Juliet 基准测试集和 37 个良好维护的开源软件项目上对现有较为完善的开源 C/C++静态缺陷检测工具的检测效果进行了深入研究，归纳了导致静态缺陷检测工具产生误报的关键原因，总结出了当下静态分析工具的发展方向和未来趋势，有助未来静态分析技术的优化和发展，从而实现静态缺陷检测工具的普及应用.

论文《面向缓解机制评估的自动化信息泄露方法》针对存在数据执行保护(DEP)和地址空间布局随机化(ASLR)等保护机制时漏洞利用样本自动生成的挑战，提出了基于程序的执行迹分析的自动生成漏洞利用样本方案 EoLeak.

论文《一种采用对抗学习的跨项目缺陷预测方法》针对跨项目缺陷预测时源项目与目标项目存在差异的问题，提出了基于对抗学习(GAN)的方法来调整目标项目的特征向量，使其接近源项目的特征分布，从而使得源项目的分类器能够更准确地对目标项目进行预测.

本专题重点关注系统软件缺陷和漏洞的检测、评估、管理、修复、缓解和新型攻击,反映了我国学者在相关领域最新的研究进展. 读者群体包括系统软件、程序语言、软件工程等相关领域人员和专业软件工程师、测试工程师、安全工程师等. 感谢《软件学报》编委会和系统软件专委会对专刊工作的指导和帮助，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. 希望本专题能够对系统软件安全的研究工作有所促进.

杨珉(1979－)，男，博士，复旦大学教授，博士生导师，第 8 届国务院学位委员会网络安全学科评议组成员，教育部长江学者特聘教授，国家 973 项目首席科学家. 聚焦于智能系统安全研究，在恶意代码分析、漏洞检测和 AI 系统安全等领域中取得较大进展. 指导的安全战队“复旦白泽”在国内外安全竞赛中屡获佳绩，为行业输送了一批高水平人才.

张超(1986－)，男，博士，清华大学长聘副教授，CCF 高级会员，蓝莲花战队教练. 获得国家级青年人才计划、清华大学学术新人奖、MIT TR35 China、求是杰出青年学者等荣誉. 兼任中国青年科技工作者协会第 6 届理事、中国人工智能学会人工智能与安全专委会常务委员等. 主要研究软件和系统安全，尤其是智能攻防方向，在国际四大安全会议发表论文 20 余篇. 研发的自动攻防系统获得美国国防部 DARPA CGC 机器自动攻防竞赛初赛防御第一、决赛攻击第二.

宋富(1983－)，男，博士，上海科技大学长聘副教授，研究员，博士生导师，入选上海市浦江人才计划、上海市晨光学者，CCF 高级会员，形式化方法专委会和系统软件专委会委员. 主持/参与了国家自然科学基金重大、重点、中德国际合作、面上等项目，发表论文 60 多篇，包括软件工程领域顶级期刊和会议 IEEE TSE、ACM TOSEM、CAV、ICSE、ISSTA、ASE，系统安全领域顶级会议和期刊 IEEE S&P、IEEE TDSC 等. 获得欧洲软件科学与技术协会最佳论文奖 1 项. 主要研究软件和 AI 安全的基础理论和应用理论研究.

张源(1987－)，男，博士，复旦大学副教授，博士生导师，CCF 专业会员，入选上海市启明星计划，获 ACM SIGSAC 中国新星奖. 主要研究方向为软件安全和程序分析，相关工作主要发表于网络与系统安全顶会和软件工程顶会. 担任 IEEE S&P、USENIX Security、WWW 等会议的程序委员会委员，Empirical Software Engineering Journal (EMSE)编委. 带领团队获得 2020/2021 年全国大学生信息安全创新实践能力赛冠军，2019/2020 年全国高校网安联赛团队赛冠军、个人赛冠军.