软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2020,31(5):1241−1242 [doi: 10.13328/j.cnki.jos.005958]

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

系统软件构造与验证技术专题前言*

赵永望[1], 刘 杨[2], 王 戟[3,4]

[1](北京航天航空大学 计算机学院,北京 100191)

[2](School of Computer Science and Engineering, Nanyang Technological University, Singapore 639798, Singapore)

[3](国防科技大学 计算机学院,湖南 长沙 410073)

[4](高性能计算国家重点实验室(国防科技大学),湖南 长沙 410073)

通讯作者: 赵永望, E-mail: zhaoyw@buaa.edu.cn

中文引用格式: 赵永望,刘杨,王戟.系统软件构造与验证技术专题前言.软件学报,2020,31(5):1241−1242. http://www.jos.org.cn/1000-9825/5958.htm

系统软件是计算机系统的核心基础软件,涵盖基础系统软件,如操作系统、语言及编译器、中间件、数据库等;领域系统软件,如无人系统、工业控制、航空航天飞行器等的核心控制软件;人工智能系统软件和区块链关键基础软件等新型软件.系统软件的安全可靠性关系到整个系统,如何构造并验证高质量的系统软件仍然是学术界和工业界面临的重大问题.尤其是系统软件构造与验证过程中,提高系统软件开发效率、提升系统软件质量、增强系统软件安全可靠性相关的理论与方法、技术与工具、应用与案例等,对于我国从事系统软件的研发人员,具有重要的参考价值.

本专题公开征文,共收到投稿 22 篇(包括第 18 届全国软件与应用学术会议(NASAC 2019)推荐的 12 篇高质量论文).其中,17 篇论文通过了形式审查,内容涉及系统软件的设计、分析、测试、形式化验证等.特约编辑先后邀请了 20 多位专家参与审稿工作,每篇投稿至少由 2 位专家进行评审.稿件经初审、复审、NASAC 2019 会议宣读和终审 4 个阶段,历时 6 个月,最终有 9 篇论文入选本专题.根据主题,这些论文可以分为 2 组.

(1) 系统软件测试与分析技术

《静态程序分析并行化研究进展》调研了静态程序分析并行化的最新研究进展以及代表性的分析工具,综述并讨论了静态分析并行化方面的研究动态和未来可能的研究方向.

《深度神经网络测试研究综述》从深度神经网络测试度量指标、测试输入生成、测试预言等角度进行了系统梳理,分析了相关数据集和应用成果.

《面向顺序存储结构的数据流分析》建立了用于顺序存储结构的内存模型,提出了 C 程序顺序存储结构相关的数据流分析和内存泄漏缺陷检测算法,并对 5 个开源 C 工程进行检测.

《基于深度学习的安全缺陷报告预测方法实证研究》采用深度文本挖掘模型构建安全缺陷报告预测模型并进行优化,通过大规模实证研究,表明该模型在 80%的实验案例中优于传统机器学习分类算法.

《Web 应用前后端融合的遗传算法并行化测试用例生成》将种群并行化计算引入到基于遗传算法的 Web 应用前后端融合的测试用例生成中,实现 Web 应用的测试用例生成过程并行化,提高其测试用例生成效率.

(2) 系统软件设计与验证技术

《CRDT 协议的 TLA+描述与验证》采用 TLA+形式化规约语言构建了一个可复用的 CRDT 协议描述与验证框架,并使用 TLC 模型检验工具验证协议的正确性.

《嵌入式实时操作系统内核混合代码的自动化验证框架》提出了一个自动化验证操作系统内核混合代码的框架,并对两种硬件平台的嵌入式实时操作系统内核 μC/OS-II 进行了验证.

《区域控制器的安全需求建模与自动验证》提出了一种安全需求自动验证方法,使用半形式化的问题框架

* 收稿时间: 2020-03-27

方法来建模和分解安全需求,自动生成安全需求的验证模型和验证性质,并通过 Design Verifier 验证器对需求进行组合验证.

《基于 TEE 的主动可信 TPM/TCM 设计与实现》提出了可信 3.0 阶段中构建 TPM/TCM 部件所面临的难点问题,并基于 ARM TrustZone 机制设计了满足主动可信要求的 TCM,验证了性能,为设计实现下一代 TPM/TCM 给出了理论和实践参考.

本专题主要面向操作系统、软件工程、程序分析、形式化方法等多领域的研究人员和工程人员,反映了我国学者在系统软件构造与验证技术领域的最新研究进展.感谢《软件学报》编委会、CCF 系统软件专委会和软件工程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.希望本专题能够对系统软件构造与验证相关领域的研究工作有所促进.

赵永望(1979－),男,浙江绍兴人,博士,副教授,博士生导师,CCF 高级会员.担任 ARINC653 国际操作系统标准委员会委员、国际信息技术安全评估标准操作系统内核技术委员会委员、CCF 系统软件专委会和形式化方法专委会委员.主要研究领域为形式化方法,操作系统,软件安全可靠性.主持了国家自然基金、国家重点研发计划课题、载人航天计划重点课题等 10 余项课题.相关研究成果得到美国波音、法国空客和国际知名实时操作系统厂商的认可,被纳入国际标准,并在开源实时操作系统社区产生影响力.

刘杨(1982－),男,博士,新加坡南洋理工大学(NTU)领袖论坛讲席教授.担任网络安全实验室主任、HP-NTU 公司实验室项目主任以及新加坡国家卓越卫星副主任.主要研究领域为软件验证,软件安全,软件工程.在顶级会议和顶级期刊上发表了超过 300 篇文章.获得多项著名奖项,包括 MSRA fellowship、TRF Fellowship、南洋助理教授、Tan Chin Tuan Fellowship、Nanyang Research Award 2019、NRF Investigatorship,以及 ASE、FSE、ICSE 等顶级会议 10 项最佳论文奖和最具影响力软件奖.

王戟(1969－),男,博士,教授,博士生导师.主要研究领域为软件方法学,软件分析与验证,并行与分布计算.