

系统与网络软件安全专题前言*

向剑文¹, 陈厅², 王浩宇³, 罗夏朴⁴, 杨珉⁵

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(华中科技大学 网络空间安全学院, 湖北 武汉 430074)

⁴(香港理工大学 电子计算学系, 香港 999077)

⁵(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; 王浩宇, E-mail: haoyuwang@hust.edu.cn;
罗夏朴, E-mail: csxluo@comp.polyu.edu.hk; 杨珉, E-mail: m_yang@fudan.edu.cn

中文引用格式: 向剑文, 陈厅, 王浩宇, 罗夏朴, 杨珉. 系统与网络软件安全专题前言. 软件学报, 2024, 35(8): 3551-3552.
<http://www.jos.org.cn/1000-9825/7125.htm>

近年来, 随着移动通信、云计算、人工智能、区块链等技术的快速发展, 传统系统软件与网络应用被赋予新特性和新场景, 新兴系统软件与网络应用也不断涌现. 与此同时, 各类系统攻击、网络犯罪等安全问题频繁发生, 给社会和国家安全带来了极大的危害. 一方面, 新兴系统软件和网络软件的程序逻辑复杂、运行环境多样、漏洞层出不穷, 针对它们的攻击行为形式多样, 对抗手段变化多端; 另一方面, 新兴系统软件和网络软件的开放特性促进了黑灰产的发展, 从移动终端的暗扣话费和勒索软件, 到区块链数字货币和去中心化应用的洗钱和地下犯罪, 黑灰产不仅给用户带来隐私泄露、财产损失、名誉损害等威胁, 同时也加深社会信任危机感. 因此, 如何提升系统软件和网络软件的安全性和可靠性, 对于保障国家网络空间安全和提升我国软件系统产业的信息安全保障能力至关重要. 本专题内容重点围绕网络空间中新兴系统软件与网络软件的安全检测、防御与溯源等技术和研究.

本专题公开征文, 共收到投稿 35 篇. 论文均通过了形式审查, 内容涉及移动应用黑灰产、恶意代码检测、固件安全测试、网络告警、隐私合规和隐私保护技术等, 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 2023 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.

《[基于 TEE 和 SE 的移动平台双离线匿名支付方案](#)》提出了一种专为移动平台设计的高效双离线匿名支付方案, 从安全性和效率两方面均能满足移动用户对中央银行数字货币双离线交易的实际需求.

《[UEFI 的启发式逆向分析与模糊测试方法](#)》提出了一种面向统一可扩展固件接口的启发式逆向分析方法, 可以有效提升函数测试覆盖率.

《[FirmDep: 利用动态分析的嵌入式应用托管方案](#)》提出了一种基于动态分析辅助的固件托管方案, 可有效识别嵌入式设备应用的环境依赖问题, 提高固件托管的成功率.

《[基于多元数据融合的网络侧告警排序方法](#)》提出了一种基于多元数据融合的网络侧告警排序方法, 能够有效且稳定地排序网络侧告警.

《[基于双分支特征提取和自适应胶囊网络的 DGA 域名检测方法](#)》提出了一种基于双分支特征提取和自适应胶囊网络的 DGA 域名检测方法, 可有效提高 DGA 域名的检测精度.

《[面向漏洞检测模型的强化学习式对抗攻击方法](#)》提出了一种面向漏洞检测模型的强化学习式对抗攻击方法, 可显著降低基于深度学习漏洞检测模型的检测准确性.

* 收稿时间: 2024-01-05; jos 在线出版时间: 2024-01-08



《移动应用隐私权声明内容合规性检验方法》提出了一种移动应用隐私权声明的多标签分类方法,能够自动解析隐私权声明语句和检测隐私权声明违规问题。

《一种基于突变流量的在野黑产应用采集方法》提出了一种基于突变流量分析的黑产应用批量捕获方法,能够快速发现正处于传播阶段的新兴在野黑产应用。

《基于负数据库的隐私保护图神经网络推荐系统》提出了一种负表示图数据的发布方案,并将将该方案应用到图数据的隐私保护中。

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,反映了我国学者在系统软件与网络软件的安全检测、防御与溯源等技术领域最新的研究进展。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,可靠性工程等。



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,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。



王浩宇(1991—),男,博士,华中科技大学教授,博士生导师,CCF 专业会员,主要研究领域为新兴软件系统安全。



罗夏朴(1977—),男,博士,香港理工大学教授,博士生导师,CCF 专业会员,主要研究领域为移动安全和隐私,区块链/智能合约,网络安全和隐私,软件工程。



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,恶意代码检测,漏洞分析挖掘,AI 安全,区块链安全,Web 安全和系统安全机制等。