

沈煜恒

软件系统安全保障小组

政治面貌：中共党员

出生日期：1997 年 12 月

电话：(+86) 18890365286

邮箱：syh1308@gmail.com

主页：<https://rrooach.github.io>



教育背景

清华大学，软件学院	2025.8–至今
博士后，水木学者 导师：姜宇长聘副教授	
清华大学，软件学院	2020.9–2025.7
软件工程专业博士 导师：姜宇长聘副教授	
湖南农业大学，信息科学与技术学院	2016.9–2020.7
计算机科学与技术专业学士	

研究方向：软件工程，系统安全

研究内容聚焦在系统软件的安全性、可靠性保障。通过程序分析、模糊测试等自动化技术研究通用操作系统、嵌入式操作系统、机器人操作系统等复杂系统的程序缺陷。近五年在各类上行业顶级期刊和会议上发表论文 20 篇，含第一作者与共同一作论文 7 篇，通讯作者 1 篇。相关研究成果已累计发现超过 100 个重要缺陷。

代表成果

第一及通讯作者发表论文

- **Yuheng Shen**, Jianzhong Liu, Qiming Guo, Yifei Chu, Qiang Zhang, Heyuan Shi, Yu Jiang. “Effective On-Hardware Fuzzing of Embedded Operating Systems”. Eurosyst’26 (CCF-A，系统领域顶会)
- **Yuheng Shen**, Jianzhong Liu, Yuhang Chen, Yifei Chu, Qiang Zhang, Guoyu Yin, Heyuan Shi, Yu Jiang. “Configuration-Sensitive Linux Kernel Fuzzing”. ICSE’26 (CCF-A，软工领域顶会)
- **Yuheng Shen**, Jianzhong Liu, Yuhang Chen, Qiang Zhang, Runzhe Wang, Heyuan Shi, Yu Jiang “Directed Real-time Linux Fuzzing with Configuration Awareness”. TECS’25 (CCF-B，嵌入式领域顶刊)
- Yuhang Chen, **Yuheng Shen**, Guoyu Yin, Fan Ding, Runzhe Wang, Tao Ma, Xiaohai Shi, Qiang Fu, Ying Fu, Heyuan Shi. “Linux Kernel Fuzzing Guided by Distribution-Specific Runtime Parameter Interfaces”. ASE’25 (CCF-A，软工领域顶会，共同第一作者)
- **Yuheng Shen**, Jianzhong Liu, Yiru Xu, Hao Sun, Mingzhe Wang, Nan Guan, Heyuan Shi, Yu Jiang. “Enhancing ROS System Fuzzing through Callback Tracing”. ISSTA’24 (CCF-A，软工领域顶会)
- **Yuheng Shen**, Shijun Chen, Jianzhong Liu, Yiru Xu, Qiang Zhang, Runzhe Wang, Heyuan Shi, Yu Jiang. “Brief Industry Paper: Directed Kernel Fuzz Testing on Real-time Linux”. RTSS’23 (CCF-A，嵌入式领域顶会)
- **Yuheng Shen**, Yiru Xu, Hao Sun, Jianzhong Liu, Zichen Xu, Aiguo Cui, Heyuan Shi, Yu Jiang. “Tardis: Coverage-Guided Embedded Operating System Fuzzing”. TCAD’22 (CCF-A，嵌入式领域顶刊)

- **Yuheng Shen**, Hao Sun, Yu Jiang, Heyuan Shi, Yixiao Yang, Wanli Chang. “Rtkaller: State-aware task generation for RTOS fuzzing”. EMSOFT’21 (CCF-B，嵌入式领域顶会)
- Heyuan Shi, Shijun Chen, Runzhe Wang, Yuhan Chen, Weibo Zhang, Qiang Zhang, **Yuheng Shen**, Xiaohai Shi, Chao Hu, Yu Jiang. “Industry Practice of Directed Kernel Fuzzing for Open-source Linux Distribution”. ASE’24 (CCF-A，软工领域顶会，通讯作者)

共同作者发表论文 (节选)

- Hao Sun, **Yuheng Shen**, Jianzhong Liu, Yiru Xu, Yu Jiang. “KSG: Augmenting Kernel Fuzzing with System Call Specification Generation”. ATC’22. (CCF-A，系统领域顶会)
- Hao Sun, **Yuheng Shen**, Cong Wang, Jianzhong Liu, Yu Jiang, Ting Chen, Aiguo Cui. HEALER: Relation learning guided kernel fuzzing, SOSP’ 23 (CCF-A，系统领域顶会)
- Jianzhong Liu, **Yuheng Shen**, Yiru Xu, Hao Sun, Yu Jiang. “Horus: Accelerating Kernel Fuzzing through Efficient Host-VM Memory Access Procedures” TOSEM’23 (CCF-A，软工领域顶刊)
- Jianzhong Liu, **Yuheng Shen**, Yiru Xu, Hao Sun, Yu Jiang. “SnapCC: Effective File System Consistency Testing Using Systematic State Exploration”. TOSEM’25 (CCF-A，软工领域顶刊)
- Jianzhong Liu, **Yuheng Shen**, Yiru Xu, Yu Jiang. “Leveraging Binary Coverage for Effective Generation Guidance in Kernel Fuzzing” CCS’24 (CCF-A，安全领域顶会)
- Qiang Zhang, **Yuheng Shen**, Jianzhong Liu, Yiru Xu, Heyuan Shi, Yu Jiang, Wanli Chang. “ECG: Augmenting Embedded Operating System Fuzzing via LLM-Based Corpus Generation”. TCAD’24 (CCF-A，嵌入式领域顶刊)
- Yiru Xu, Hao Sun, Jianzhong Liu, **Yuheng Shen**, Yu Jiang. “SATURN: Host-gadget synergistic USB driver fuzzing”. S&P’24 (CCF-A, 安全领域顶会)
- Hao Sun, Yiru Xu, Jianzhong Liu, **Yuheng Shen**, Nan Guan, Yu Jiang. “Finding correctness bugs in EBPF verifier with structured and sanitized program”. EuroSys’24 (CCF-A, 系统领域顶会)

发表专利

- 沈煜恒；刘健中；许意如；姜宇 (2024). 机器人操作系统的漏洞检测优化方法、装置及设备. 已公开，公布号：118427834.
- 沈煜恒；刘健中；许意如；姜宇 (2023). 测试嵌入式操作系统的处理方法、装置、设备及介质. 已公开，公布号：118069531.
- 沈煜恒；许意如；刘健中；姜宇 (2023). 应用系统测试方法、装置、电子设备及存储介质. 已公开，公开号：118093421.

科研项目

- | | |
|----------------------------------|-----------|
| • 鸿蒙并发竞争检测诊断测试技术，来源：华为合作项目 | 2024-2025 |
| • 安卓内核测试技术方法研究，来源：小米公司合作项目 | 2024-2025 |
| • 面向下一代云原生关键基础构建的模糊测试，来源：阿里云合作项目 | 2023-2024 |
| • 智能制造软件栈安全分析，来源：自然科学基金委 | 2022-2024 |

获奖经历

• 博士后基金面上项	2025
• 清华大学水木学者	2025
• 清华大学一等奖学金	2024
• 清华大学一等奖学金	2022

学术兼职

• 外部审稿人, International Symposium on Software Reliability Engineering (ISSRE), CCF-B	2021
• 期刊审稿, IEEE Transactions on Dependable and Secure Computing (TDSC), CCF-A	2024
• 期刊审稿, IEEE Transactions on Dependable and Secure Computing (TDSC), CCF-A	2025
• 期刊审稿, Transactions on Information Forensics and Security (TIFS), CCF-A	2025
• 期刊审稿, ACM Transactions on Embedded Computing Systems (TECS), CCF-B	2025

教学活动经历

• 计算机程序设计基础, 授课教师: 乔林, 清华大学研究生课程	2024-2025 秋季学期
• 基于 Linux 的 C++ 程序设计, 授课教师: 乔林, 清华大学研究生课程	2023-2024 夏季学期
• 计算机程序设计基础, 授课教师: 乔林, 清华大学研究生课程	2023-2024 春季学期
• 计算机程序设计基础, 授课教师: 黄维通, 清华大学研究生课程	2023-2024 秋季学期
• 计算机程序设计基础, 授课教师: 乔林, 清华大学研究生课程	2022-2023 秋季学期