郝 宇

更新日期: April, 2025
邮箱: yhao016@ucr.edu
电话: 150292145321

个人主页: zhyfeng.github.io
[Google Scholar] [DBLP] [Github]

我的研究集中在系统安全和程序分析上，改进了多种程序分析和测试技术（例如模糊测试、符号执行、静态分析和大语言模型用于程序分析），并且结合这些技术的优点，系统地和自动地提高现实世界软件系统（例如 Linux 内核，现专注于鸿蒙系统）的安全性。我的研究成果发表在多个著名的国际顶级学术会议（例如 S&P、CCS、USENIX Security、NDSS、ICSE、FSE、OOPSLA）和期刊（例如 TSE）。我的开源工具吸引了学术界、开源社区（例如 Linux Security Summit）和工业界（例如 Google Research Papar Rewards、Qualcomm Security Summit）的兴趣并被应用。此外，我还为 Linux 内核报告漏洞和 CVE，并贡献补丁。

教育经历

09/2018 – 09/2024 **博士**，加州大学河滨分校，美国，计算机科学，导师: Zhiyun Qian

09/2015 – 06/2018 **硕士**，西安交通大学，控制科学与工程，导师: 刘烃

09/2011 – 06/2015 **学士**，西安交通大学，控制科学与工程

09/2008 – 06/2011 呼和浩特第二中学, 内蒙古自治区

工作经历

10/2024 – 至今 **系统安全研究员，天才少年 Offer**
华为, 中国

06/2023 – 09/2023 **Research Intern**, 导师: Weidong Cui
Systems Security and Privacy Research Group, 微软研究院, 美国

06/2022 – 09/2022 **Research Intern**, 导师: Kris Alder
Android Security Team, 谷歌, 美国

毕业论文

[博士] Expanding the Boundaries of OS Kernel Fuzzing Permalink
- [C9, ICSE 22][C10, S&P 23][C17, CCS 25]

[硕士] 基于并行程序不确定时序交织的恶意代码隐藏方法研究
- [C3, QRS 21, Best Paper Award][J3, *IEEE Transactions on Reliability*]

出版论文

[C]: 会议, [J]: 期刊, [P]: 预印本
小计: CCF-A 类会议 12 篇 (一作 3 篇, 二作 6 篇), CCF-A 类期刊 1 篇, 正式发表论文 20 篇

[C17] CCS 25 SyzSpec: Specification Generation for Linux Kernel Fuzzing via Under-Constrained Symbolic Execution
Yu Hao, Juefei Pu, Xingyu Li, Zhiyun Qian, Ardalan Amiri Sani
ACM SIGSAC Conference on Computer and Communications Security, CCS 25.

[C16] S&P 25 SCAD: Towards a Universal and Automated Network Side-Channel Vulnerability Detection
Keyu Man, Zhongjie Wang, **Yu Hao**, Shenghan Zheng, Xin'an Zhou, Yue Cao, Zhiyun Qian
IEEE Symposium on Security and Privacy, S&P 25.

[C15] USENIX Security 24 SymBisect: Accurate Bisection for Fuzzer-Exposed Vulnerabilities
Zheng Zhang, **Yu Hao**, Weiteng Chen, Xiaochen Zou, Xingyu Li, Haonan Li, Yizhuo Zhai, Zhiyun Qian, Billy Lau
USENIX Security Symposium 2024.

[C14] OOPSLA 24 Enhancing Static Analysis for Practical Bug Detection: An LLM-Integrated Approach
Haonan Li, **Yu Hao**, Yizhuo Zhai, Zhiyun Qian
ACM SIGPLAN International Conference on Object-Oriented Programming Systems, Languages, and Applications, OOPSLA 24. Tool

[C13] S&P 24 SyzGen++: Dependency Inference for Augmenting Kernel Driver Fuzzing
Weiteng Chen, **Yu Hao**, Zheng Zhang, Xiaochen Zou, Dhilung Kirat, Shachee Mishra, Douglas Schales, Jiyong Jang, Zhiyun Qian
IEEE Symposium on Security and Privacy, S&P 24. Tool

[C12] SyzBridge: Bridging the Gap in Exploitability Assessment of Linux Kernel Bugs in the Linux Ecosystem
NDSS 24 Xiaochen Zou, **Yu Hao**, Zheng Zhang, Juefei Pu, Weiteng Chen, Zhiyun Qian
Network and Distributed System Security Symposium, NDSS 24. Tool

[P1] E&V: Prompting Large Language Models to Perform Static Analysis by Pseudo-code Execution and Verification
Yu Hao, Weiteng Chen, Ziqiao Zhou, Weidong Cui *arXiv*
- [AGI Leap Summit 2024] [Symposium on the Science of Security 24]

[C11] Assisting Static Analysis with Large Language Models: A ChatGPT Experiment
FSE 23 Haonan Li, **Yu Hao**, Yizhuo Zhai, Zhiyun Qian
IVR *The ACM International Conference on the Foundations of Software Engineering, Ideas, Visions and Reflections, FSE 23 IVR* Tool *arXiv*

[C10] SyzDescribe: Principled, Automated, Static Generation of Syscall Descriptions for Kernel Drivers
S&P 23 **Yu Hao**, Guoren Li, Xiaochen Zou, Weiteng Chen, Shitong Zhu, Zhiyun Qian, Ardalan Amiri Sani
IEEE Symposium on Security and Privacy, S&P 23. Tool Result
- [Linux Security Summit 23] [Qualcomm Security Summit 23]
- [Symposium on the Science of Security 24]

[C9] Demystifying the Dependency Challenge in Kernel Fuzzing
ICSE 22 **Yu Hao**, Hang Zhang, Guoren Li, Xingyun Du, Zhiyun Qian, Ardalan Amiri Sani
IEEE/ACM International Conference on Software Engineering, ICSE 22. Tool Result
- [Google Research Paper Rewards]

[C8] Progressive Scrutiny: Incremental Detection of UBI bugs in the Linux Kernel
NDSS 22 Yizhuo Zhai, **Yu Hao**, Zheng Zhang, Weiteng Chen, Guoren Li, Zhiyun Qian, Chengyu Song, Manu Sridharan, Srikanth V. Krishnamurthy, Trent Jaeger, Paul Yu
Network and Distributed System Security Symposium, NDSS 22. Tool
- [2023 Cyber Security CRA Capstone Poster]

[C7] Eluding ML-based Adblockers With Actionable Adversarial Examples
ACSAC 21 Shitong Zhu, Zhongjie Wang, Xun Chen, Shasha Li, Keyu Man, Umar Iqbal, Zhiyun Qian, Kevin S Chan, Srikanth V Krishnamurthy, Zubair Shafiq, **Yu Hao**, Guoren Li, Zheng Zhang, Xiaochen Zou
Annual Computer Security Applications Conference, ACSAC 21. Tool

[C6] Themis: Ambiguity-Aware Network Intrusion Detection based on Symbolic Model Comparison
CCS 21 Zhongjie Wang, Shitong Zhu, Keyu Man, Pengxiong Zhu, **Yu Hao**, Zhiyun Qian, Srikanth V. Krishnamurthy, Tom La Porta, Michael J. De Lucia
ACM SIGSAC Conference on Computer and Communications Security, CCS 21. Tool

[C5] Statically Discovering High-Order Taint Style Vulnerabilities in OS Kernels
CCS 21 Hang Zhang, Weiteng Chen, **Yu Hao**, Guoren Li, Yizhuo Zhai, Xiaochen Zou, Zhiyun Qian
ACM SIGSAC Conference on Computer and Communications Security, CCS 21. Tool

[C4] UBITect: A Precise and Scalable Method to Detect Use-before-Initialization Bugs in Linux Kernel
FSE 20 Yizhuo Zhai, **Yu Hao**, Hang Zhang, Daimeng Wang, Chengyu Song, Zhiyun Qian, Mohsen Lesani, Srikanth V. Krishnamurthy, Paul Yu
ACM SIGSOFT International Symposium on Foundations of Software Engineering, FSE 20. Tool
- [2023 Cyber Security CRA Capstone Poster]

[J3] ConcSpectre: Be Aware of Forthcoming Malware Hidden in Concurrent Programs
Yang Liu, Ming Fan, Ting Liu, **Yu Hao**, Zisen Xu, Kai Chen, Hao Chen, and Yan Cai
IEEE Transactions on Reliability Code Result

[C3] ConcSpectre: Be Aware of Forthcoming Malware Hidden in Concurrent Programs
QRS 21 Yang Liu, Ming Fan, Ting Liu, **Yu Hao**, Zisen Xu, Kai Chen, Hao Chen, and Yan Cai
IEEE International Conference on Software Quality, Reliability, and Security, QRS 21. Code Result
- [Best Paper Award]

[J2] Tell You a Definite Answer: Whether Your Data is Tainted During Thread Scheduling
TSE Xiaodong Zhang, Zijiang Yang, Qinghua Zheng, **Yu Hao**, Pei Liu, Ting Liu
*IEEE Transactions on Software Engineering, **TSE*** Tool Benchmarks Result
- [S&P 17 Poster] Patent: [PCT] [CN]

[J1] Debugging Multithreaded Programs as if They Were Sequential
Xiaodong Zhang, Zijiang Yang, Qinghua Zheng, **Yu Hao**, Pei Liu, Lechen Yu, Ting Liu
IEEE Access Tool

[C2] Automated Testing of Definition-Use Data Flow for Multithreaded Programs
ICST 17 Xiaodong Zhang, Zijiang Yang, Qinghua Zheng, Pei Liu, Jialiang Chang, **Yu Hao**, Ting Liu
IEEE International Conference on Software Testing, Verification and Validation, ICST 17. Tool

[C1] Debugging Multithreaded Programs as if They Were Sequential
SATE 17 Xiaodong Zhang, Zijiang Yang, Qinghua Zheng, **Yu Hao**, Pei Liu, Lechen Yu, Ming Fan, Ting Liu
IEEE International Conference on Software Analysis, Testing and Evolution, SATE 16. Tool

专利

WO2017181628 - TAINT ANALYSIS METHOD EMPLOYING SYMBOLIC COMPUTATION AND USED FOR DYNAMIC PARALLEL PROGRAM [PCT] [CN]

演讲，报告

- E&V: Prompting Large Language Models to Perform Static Analysis by Pseudo-code Execution and Verification
  - *AGI Leap Summit 2024* Website
  - *Symposium on the Science of Security, HoTSoS 2024* Website
- SyzDescribe: Principled, Automated, Static Generation of Syscall Descriptions for Kernel Drivers
  - *Linux Security Summit North America 2023* Website Slides Recording
  - *Qualcomm Security Summit 2023* Website
  - *44th IEEE Symposium on Security and Privacy, S&P 2023* Website Recording
  - *Symposium on the Science of Security, HoTSoS 2024* Website
- Demystifying the Dependency Challenge in Kernel Fuzzing
  - *44rd IEEE/ACM International Conference on Software Engineering, ICSE 2022* Website Slides Recording

荣誉，奖励

2024 Laxmi Bhuyan Fellowship Award, University of California, Riverside
Dissertation Completion Fellowship Award, University of California, Riverside
2023 IEEE S&P Student Travel Grant
Google Research Paper Rewards
The Linux Foundation's Travel Fund
2021 QRS 2021 Best Paper Award
2018 Dean's Distinguished Fellowship, University of California, Riverside
西安交通大学优秀硕士毕业生
2017 胜寒协会成员
2013 西安交通大学程序设计竞赛，二等奖
西安交通大学数学建模竞赛，二等奖
2010 内蒙古高中数学联赛，一等奖
内蒙古高中物理联赛，三等奖
内蒙古高中化学联赛，三等奖
2007 全国奥林匹克数学竞赛，金牌

学术服务

审稿人	TIFS 2023, 2024. EAI SecureComm 2023.
外部审稿人	S&P 2020, 2021, 2024, 2025. CCS 2024. USENIX Security 2021, 2025. NDSS 2020, 2021, 2025.
Program Committee	FORGE@ICSE 2024, 2025. MSR 2024(Junior PC).
AEC	EuroSys 2023. ISSTA 2024. ECOOP 2024.

推荐人

博士导师 **Zhiyun Qian** *Everett and Imogene Ross* 教授
加州大学河滨分校，计算机科学与技术学院
联系方式: zhiyunq@cs.ucr.edu

论文合作者 **Ardalan Amiri Sani** 副教授
加州大学尔湾分校，计算机科学与技术学院
联系方式: ardalan@uci.edu

论文合作者 **Srikanth V. Krishnamurthy** 教授, *IEEE Fellow*
加州大学河滨分校，计算机科学与技术学院
联系方式: krish@cs.ucr.edu

硕士导师 **刘烃** 教授，副院长
西安交通大学，网络空间安全学院
联系方式: tingliu@mail.xjtu.edu.cn