Yu Hao

Last updated: December, 2025
Website: zhyfeng.github.io
Email: yhao016@ucr.edu
[Google Scholar] [DBLP] [Github]
Phone: 951-783-7821

My research focuses on operating system security and program analysis (for C/C++). My research improves multiple program analysis and testing techniques (*e.g.,* **Fuzzing**, **LLMs for Security**, **Static Analysis** (based on LLVM/Clang), **Symbolic Execution**), thereby combining the advantages of those techniques to systematically and automatically improve the security for real world software system (*e.g.,* **Linux kernel**, **Hongmeng kernel**, concurrent program). My research has led to multiple papers published in several prestigious conferences (*e.g.,* S&P, USENIX Security, CCS, NDSS, ICSE, FSE) and journal (*e.g.,* TSE). The open source tools attract interest from and applied in academia, community and industry. Besides open source tools, I also report bugs and CVE for Linux kernel and contribute patches.

Education

09/2018 – 09/2024	**Ph.D.** in Computer Science, University of California, Riverside, USA. Advisor: Zhiyun Qian 🏷Operating System Security, LLMs for Security, Fuzzing, Symbolic Execution, Static Analysis
09/2015 – 06/2018	**Master** in Control Science and Engineering, Xi'an Jiaotong University, China. Advisor: Ting Liu 🏷Concurrency Security, Symbolic Execution
09/2011 – 06/2015	**Bachelor** in Control Science and Engineering, Xi'an Jiaotong University, China.
09/2008 – 06/2011	Hohhot No.2 High School, Inner Mongolia, China.

Experience

10/2024 – present	**Security Researcher** **HarmonyOS System Security Team**, **Huawei**, China 🏷HarmonyOS Security, Fuzzing, LLMs for Security, Static Analysis
06/2023 – 09/2023	**Research Intern**, Mentor: Weidong Cui **Systems Security and Privacy Research Group**, **Microsoft Research**, USA 🏷LLMs for Security
06/2022 – 09/2022	**Research Intern**, Mentor: Kris Alder **Android Security Team**, **Google**, USA 🏷Linux/Android Kernel Security, Fuzzing, Static Analysis
09/2018 – 09/2024	**Graduate Student Researcher**, Advisor: Zhiyun Qian Center for Research and Education in Cyber Security and Privacy (CRESP) University of California, Riverside, USA 🏷Operating System Security, LLMs for Security, Fuzzing, Symbolic Execution, Static Analysis
06/2013 – 06/2018	**Research Assistant**, Advisor: Ting Liu Ministry of Education Key Lab For Intelligent Networks and Network Security Xi'an JiaoTong University, China 🏷Concurrency Security, Symbolic Execution

Publications

[C]: Conference, [J]: Journal, [P]: Preprint

[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.* • [Distinguished Paper Award]
[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]
NDSS 24
SyzBridge: Bridging the Gap in Exploitability Assessment of Linux Kernel Bugs in the Linux Ecosystem
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]
FSE 23
IVR
Assisting Static Analysis with Large Language Models: A ChatGPT Experiment
Haonan Li, **Yu Hao**, Yizhuo Zhai, Zhiyun Qian
The ACM International Conference on the Foundations of Software Engineering, Ideas, Visions and Reflections, FSE 23 IVR 📄 🔗 ⚙ Tool 📄 *arXiv*

[C10]
S&P 23
SyzDescribe: Principled, Automated, Static Generation of Syscall Descriptions for Kernel Drivers
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 Product Security Summit 23]
- [Symposium on the Science of Security 24]

[C9]
ICSE 22
Demystifying the Dependency Challenge in Kernel Fuzzing
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]
NDSS 22
Progressive Scrutiny: Incremental Detection of UBI bugs in the Linux Kernel
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]
ACSAC 21
Eluding ML-based Adblockers With Actionable Adversarial Examples
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]
CCS 21
Themis: Ambiguity-Aware Network Intrusion Detection based on Symbolic Model Comparison
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]
CCS 21
Statically Discovering High-Order Taint Style Vulnerabilities in OS Kernels
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]
FSE 20
UBITect: A Precise and Scalable Method to Detect Use-before-Initialization Bugs in Linux Kernel
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]
QRS 21
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 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

Thesis

[PhD]	Expanding the Boundaries of OS Kernel Fuzzing 📄
	• [C9, ICSE 22, Google Research Paper Rewards][C10, S&P 23][C17, CCS 25, Distinguished Paper Award]
[Master]	Research on Malicious Code Hiding Methods Based on Uncertain Interleaving of Concurrent Programs 📄
	• [C3, QRS 21, Best Paper Award][J3, *IEEE Transactions on Reliability*]

Patent

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

Presentations, Talks

⬤ 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 Product 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

Honors, Awards

2025	CCS 2025, Distinguished Paper Award
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
	Excellent Graduated Student, Xi'an JiaoTong University
2017	Excellent Graduate Student, Xi'an JiaoTong University
	Graduate Student Fellowship, Xi'an JiaoTong University
	Sheng Han High IQ Association
	• 🔗 Website IQ >= 135, Club at the same level as Mensa
2016	Graduate Student Fellowship, Xi'an JiaoTong University
2015	Graduate Student Fellowship, Xi'an JiaoTong University

2014	Siyuan Scholarship, Xi'an JiaoTong University
2013	Siyuan Scholarship, Xi'an JiaoTong University
	Second Prize, Xi'an JiaoTong University ACM-ICPC Competition
	Second Prize, Xi'an JiaoTong University MCM Competition
2010	First Prize, Mathematical Olympiad in Provinces, Inner Mongolia

- Ranking 4th at that year in the province with population of 25 million

Third Prize, Physics Olympiad in Provinces, Inner Mongolia

Third Prize, Chemistry Olympiad in Provinces, Inner Mongolia

2007 · First Prize, National Mathematics Invitational Competition, Inner Mongolia

- A total of 4 at that year in the province with population of 25 million

Academic Service

Program Committee	CCS 2026. FORGE@ICSE 2025, 2024. MSR 2024(Junior PC).
Reviewer	TIFS 2024, 2023. TOSEM 2025. EAI SecureComm 2023.
Sub-Reviewer	S&P 2025, 2024, 2021, 2020. CCS 2024. USENIX Security 2025, 2021. NDSS 2025, 2021, 2020.
AEC	EuroSys 2023. ISSTA 2024. ECOOP 2024.

References

Advisor of Ph.D. Degree	**Zhiyun Qian** *Everett and Imogene Ross Professor* Computer Science and Engineering department, University of California, Riverside, USA Contact: zhiyunq@cs.ucr.edu
Collaborator	**Ardalan Amiri Sani** *Associate Professor* Computer Science Department, University of California, Irvine, USA Contact: ardalan@uci.edu
Collaborator	**Srikanth V. Krishnamurthy** *Professor, IEEE Fellow* Computer Science and Engineering department, University of California, Riverside, USA Contact: krish@cs.ucr.edu
Intern Mentor at Microsoft Research	**Weidong Cui** *Partner Research Manager* Systems Security and Privacy Research Group, Microsoft Research, Redmond, USA Contact: Weidong.Cui@microsoft.com
Advisor of Master Degree	**Ting Liu** *Professor, Associate Dean* School of Cyber Science and Engineering, Xi'an Jiaotong University, China Contact: tingliu@mail.xjtu.edu.cn