Haoxin Tu

PhD in Computer Science · Software Engineering

21 Lower Kent Ridge Road, Singapore 119077, National University of Singapore

☎ (+65) 81766631 | ✉ haoxintu.2020@smu.edu.sg | 🏠 https://haoxintu.github.io/ | 💻 https://github.com/haoxintu | 🐦 @tuhaoxin

"Stay hungry. Stay foolish."

Research Interests

Software systems written by humans or AI tend to be unreliable and insecure. My research interests focus on developing practical techniques and tools that can help improve the *reliability* and *security* of software systems (mainly targeting system software such as *compilers* and *Linux kernels*). I am quite interested in developing advanced automated approaches, based on program analysis techniques such as *fuzzing* and *symbolic execution*, to resolve labor-intensive engineering tasks, e.g., automatic bug/vulnerability detection and exploit generation.

Work Experience

National University of Singapore   *Singapore*
Research Fellow at Abhik's Group   *May. 2025 - Present*
- Work on building practical agents to improve software security and reliability.

Max Planck Institute for Security and Privacy (MPI-SP)   *Bochum, Germany*
Research Intern at Marcel's Group   *May. 2024 - Sep. 2024*
- Work on building practical concolic/symbolic execution-based solutions for highly structured test input generation.

Education

Singapore Management University   *Singapore*
P.h.D in Computer Science (Supervisor: Lingxiao Jiang & Xuhua Ding)   *Aug. 2020 - May. 2025*
- Thesis topic: "Boosting Symbolic Execution for Vulnerability Detection".

Dalian University of Technology   *Dalian, China*
P.h.D in Software Engineering (Supervisor: He Jiang)   *Sep. 2019 - Dec. 2023*
- Thesis topic: "Research on Test Program Construction Approaches for Compiler Testing and Debugging".

Dalian University of Technology   *Dalian, China*
Master in Software Engineering   *Sep. 2017 - Jul. 2019*

Northeast Forestry University   *Harbin, China*
Bachelor in Electronic Information Engineering   *Sep. 2013 - Jul. 2017*

Publications

Conference Papers

- [ICSE'24] **Haoxin Tu**, Lingxiao Jiang, Debin Gao, and He Jiang, **"Beyond a Joke: Dead Code Elimination Can Delete Live Code"**, in International Conference on Software Engineering (ICSE-NIER 2024). [PDF] [Code(☆1)]
    - A new problem to investigate and a new approach to tackle the problem.
- [CCS'23] Pansilu Pitigalaarachchi, Xuhua Ding, Haiqing Qiu, **Haoxin Tu**, Jiaqi Hong, and Lingxiao Jiang, **"KRover: A Symbolic Execution Engine for Dynamic Kernel Analysis"**, in Conference on Computer and Communications Security, Research Track. [PDF] [Code(☆1)]
    - A new flavor of kernel symbolic execution with binary intimacy, high speed, noise-free nature, and programmable invocation.
- [ICSE'23] **Haoxin Tu**, **"Boosting Symbolic Execution for Heap-based Vulnerability Detection and Exploit Generation"**, in International Conference on Software Engineering, Doctoral Symposium Track. [PDF]
    - A new path exploration strategy, a new memory model, and a new environment modeling for boosting symbolic execution.
- [FSE'22] **Haoxin Tu**, Lingxiao Jiang, Xuhua Ding, and He Jiang, **"FastKLEE: Faster Symbolic Execution via Reducing Redundant Bound Checking of Type-Safe Pointers"**, in Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering, Tool Demonstrations Track. [PDF] [Code(☆16)]
    - Combine static analysis (Ccured) to reduce redundant pointer comparison checking for speeding up symbolic execution.
- [ISSRE'22] **Haoxin Tu**, He Jiang, Xiaochen Li, Zhilei Ren, Zhide Zhou, and Lingxiao Jiang, **"RemGen: Remanufacturing A Random Program Generator for Compiler Testing"**, in International Symposium on Software Reliability Engineering, Research Track. [PDF] [Code(☆ 5)]

– Remanufacturing an old/tamed program generator to be new again (yield 56 bug reports for GCC and LLVM).

Journal Papers

- [TSE'24] **Haoxin Tu**, Zhide Zhou, He Jiang, Imam Nur Bani Yusuf, Yuxian Li, and Lingxiao Jiang, ***"Isolating Compiler Bugs by Generating Effective Witness Programs with Large Language Models"***, in IEEE Transactions on Software Engineering. [PDF] [Code(☆4)]
    – Static program analysis for prompt generation and reinforcement learning for prompt selection.
- [TSE'24] **Haoxin Tu**, Lingxiao Jiang, Jiaqi Hong, Xuhua Ding, and He Jiang, ***"Concretely Mapped Symbolic Memory Locations for Memory Error Detection"***, in IEEE Transactions on Software Engineering. [PDF] [Code(☆2)]
    – A new modeling of memory address and several new bug-detection strategies based on symbolic address.
- [TR'22] **Haoxin Tu**, He Jiang, Zhide Zhou, Yixuan Tang, Zhilei Ren, Lei Qiao, and Lingxiao Jiang, ***"Detecting C++ Compiler Front-end Bugs via Grammar Mutation and Differential Testing"***, in IEEE Transactions on Reliability. [PDF]
    – Combine grammar-aware C++ test program generation with differential testing (yield 131 bug reports for GCC and LLVM).

Workshops

- [KLEE'24] **Haoxin Tu**, Lingxiao Jiang, Xuhua Ding, and He Jiang, ***"FastKLEE: Faster Symbolic Execution via Reducing Redundant Bound Checking of Type-Safe Pointers"***, in the 4th International KLEE Workshop on Symbolic Execution April 2024.
- [KLEE'24] **Haoxin Tu**, Lingxiao Jiang, Jiaqi Hong, Xuhua Ding, and He Jiang, ***"Concretely Mapped Symbolic Memory Locations for Memory Error Detection"***, in the 4th International KLEE Workshop on Symbolic Execution, April 2024.

Under Review Papers

- [Under-review] **Haoxin Tu**, Lingxiao Jiang, and Marcel Böhme, ***"Vital: Vulnerability-Oriented Symbolic Execution via Type-Unsafe Pointer-Guided Monte Carlo Tree Search"***, Submitted to a Top-tier Software Engineering Conference.
    – A new vulnerability-oriented path exploration strategy for symbolic execution.

Research Impact

The list of bugs and vulnerabilities found through my research (counted on September 30th, 2023).

- GCC Bug Reports: 121 (in total) / 76 (confirmed or fixed)   Links: in GCC Bugzilla
- LLVM Bug Reports: 137 (in total) / 88 (confirmed or fixed)   Links: [GitHub issues from llvm-project]
- GNU Coreutils Bug Reports: 2 (in total) / 2 (fixed)   Links: [GNU Coreutils Bugzilla]
- Angr Bug Reports: 3 (in total) / 2 (fixed)   Links: [GitHub issues from Angr]
- S2E Bug Reports: 1 (in total) / 1 (fixed)   Links: [GitHub issues from S2E]
- To be continued ...

Teaching Experience

2024	**Teaching Assistant for "CS706: Software Mining and Analysis"**, Singapore Management University	*Singapore*
2022	**Teaching Assistant for "CS443: System Security"**, Singapore Management University	*Singapore*
2019	**Teaching Assistant for "Operating Systems"**, Dalian University of Technology	*Dalian, China*

Honors & Awards

2022	**Excellent Postgraduate Students**, Dalian University of Technology (Top 1%)	*Dalian, China*
2022	**National Scholarship for Postgraduate Students**, Dalian University of Technology (Top 1%)	*Dalian, China*
2020	**PhD Full Scholarship**, from Singapore Management University	*Singapre*
2019	**Third Prize**, National Software and Application Academic Conference (Proposition-based Competition)	*Shanghai, China*
2019	**Third Prize**, National Post-Graduate Mathematical Contest in Modeling (Top 20%)	*Dalian, China*
2017	**Outstanding Graduates**, Northeast Forestry University (Top 5%)	*Harbin, China*

Academic Service

2024	**Reviewer**, for TOSEM, Shadow PC for ICSE'25	
2023	**Student Volunteer**, for International Conference on Software Engineering (ICSE 2023)	*Melbourne*
2022	**Reviewer**, for IEEE Transactions on Reliability	

Hobbies

I am an avid tennis enthusiast.