# Haoxin **Tu**

PhD in Computer Science and Software Engineering

*81 Victoria Street, Singapore 188065, Singapore Management University*

(+65) 81766631 | haoxintu.2020@phdcs.smu.edu.sg | https://haoxintu.github.io/ | https://github.com/haoxintu | @tuhaoxin


*"Stay hungry. Stay foolish."*

## Research Interests

Software systems written by humans 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.

## Education

**Singapore Management University (No.3 in Software Engineering on CSRanking)** — *Singapore*

P.h.D in Computer Science (Supervisor: Lingxiao Jiang & Xuhua Ding) — *Aug. 2020 - Dec. 2024 (Expected)*

- Thesis topic: "Boosting Symbolic Execution for Software Reliability and Security". (Proposed)

**Dalian University of Technology ("985", "211")** — *Dalian, China*

P.h.D in Software Engineering (Supervisor: He Jiang) — *Sep. 2019 - Dec. 2023 (Expected)*

- Thesis topic: "Research on Test Program Construction Approaches for Compiler Testing and Debugging".

**Dalian University of Technology ("985", "211")** — *Dalian, China*

Master in Software Engineering — *Sep. 2017 - Jul. 2019*

**Northeast Forestry University ("211")** — *Harbin, China*

Bachelor in Electronic Information Engineering — *Sep. 2013 - Jul. 2017*

## Skills

| | |
|---|---|
| **General Software** | GCC, LLVM, KLEE, Angr, S2E, Z3, Frama-C, etc |
| **Programming** | C/C++, Python, Shell, MATLAB, etc |
| **Language** | Chinese (Fluent), English |

## Publications

### Conference Papers

- [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

- [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).

Under Review Papers

- [TSE] **Haoxin Tu**, Lingxiao Jiang, Jiaqi Hong, Xuhua Ding, and He Jiang, ***"Concretely Mapped Symbolic Memory Locations for Memory Error Detection"***, Submitted to IEEE Transactions on Software Engineering (Major Revision).
  - A new modeling of memory address and several new bug-detection strategies based on symbolic address.
- [TSE] **Haoxin Tu**, Zhide Zhou, He Jiang, Imam Nur Bani Yusuf, Yuxian Li, and Lingxiao Jiang, ***"LLM4CBI: Taming LLMs to Generate Effective Test Programs for Compiler Bug Isolation"***, Submitted to IEEE Transactions on Software Engineering (Major Revision). [Pre-print]
  - Static program analysis for prompt generation and reinforcement learning for prompt selection.
- [Conference] **Haoxin Tu**, and others, ***"Beyond a Joke: Dead Code Elimination Can Delete Live Code"***, Submitted to a Top-tier Conference in Software Engineering (Under Review).
  - A new problem to investigate and a new approach to tackle the problem.

## Practical Impacts

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: 1 (in total) / 1 (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 ...

## Work Experience

**Huawei Technologies Co. Corp.** *Beijing, China*

Software Engineer (Summer Intern) *Jun. 2018 - Sep. 2018*

- Android JNI developing: built a library component of an Android application that allows Java applications running in the Java Virtual Machine (JVM) to call native applications and libraries written in languages such as C, C++, and Assembly.

## Teaching Experience

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

2023 **Student Volunteer**, for International Conference on Software Engineering (ICSE 2023) *Melbourne*

2022 **Reviewer**, for IEEE Transactions on Reliability

2022 **External Reviewer**, for ASE 2019, SANER 2022, QRS 2022/2023

## Hobbies

I am an avid tennis enthusiast.