Yuancheng Jiang

Research Fellow, School of Computing, National University of Singapore

dcsyua@nus.edu.sg | https://yuanchengjiang.github.io/ | Google Scholar | GitHub

Research Profile

My research bridges software engineering and security, combining security mindsets with systematic software testing methodologies. I develop automated testing techniques that leverage program semantics to generate test inputs and derive correctness oracles, enabling fuzzers to explore complex execution states and uncover subtle defects, including silent correctness errors and security vulnerabilities, in interpreters, compilers, and database systems. My research has led to the discovery of numerous previously unknown bugs in mainstream foundation software systems, including LLVM, GCC, Python, PHP, and AI compilers, and my FlowFusion fuzzer has been integrated into PHP's official repository. Beyond software testing, I have rich experience in system security, including offensive and defensive solutions. My long-term goal is to combine software engineering and security perspectives to improve the robustness and correctness of foundational software systems and agentic software stacks.

Education and Research Experience

Research Fellow (Postdoctoral) Oct 2026 – Present

School of Computing, National University of Singapore, Singapore

Supervisor: Asst. Prof. Manuel Rigger

Ph.D. in Computer Science Jan 2022 – Oct 2026

School of Computing, National University of Singapore, Singapore

Thesis: Semantic-guided Testing and Bug Discovery in Complex Execution Engines
Supervisors: Assoc. Prof. Roland H. C. Yap and Assoc. Prof. Zhenkai Liang
Collaborators: Asst. Prof. Manuel Rigger and Prof. Alastair F. Donaldson (Imperial College London)

Master of Computing Aug 2020 – Jan 2022

School of Computing, National University of Singapore, Singapore

Thesis: Benchmark for Security Effectiveness Evaluation of Memory Error Defences

Bachelor of Science (Information Security) Sep 2016 – Jun 2020

Fudan University, Shanghai, China

Thesis: Security Assessment and Dynamic Analysis of Embedded Browsers

Awards & Honors

- **Dean's Graduate Research Excellence Award**, School of Computing, NUS — AY 2025–2026
- **Distinguished Paper Award**, the 34th USENIX Security Symposium (USENIX Security'25) — 2025
- **Singapore Open Research Award** (Robustifying Data-Centric Systems) — 2024

Publications

- **Scalable Fusion-based Fuzzing for Compilers and Interpreters** (Under Review)
  Yuancheng Jiang, Yeqi Fu, Roland Yap, Alastair Donaldson, Manuel Rigger
- **OSS-Bench: Benchmark Generator for Coding LLMs** (Preprint)
  Yuancheng Jiang, Roland Yap, Zhenkai Liang
- **ACME: Automated Clause Mapping Engine for Testing Emerging Database Systems**
  Yuancheng Jiang, Jianing Wang, Chuqi Zhang, Roland Yap, Zhenkai Liang, Manuel Rigger
  The 34th ACM International Conference on the Foundations of Software Engineering (**FSE'26**)
- **ZendDiff: Differential Testing of PHP Interpreter**
  Yuancheng Jiang*, Jianing Wang*, Qiange Liu, Yeqi Fu, Jian Mao, Roland Yap, Zhenkai Liang (*Equal contribution)
  The 40th IEEE/ACM International Conference on Automated Software Engineering (**ASE'25**)
- **Fuzzing the PHP Interpreter via Dataflow Fusion** **(Distinguished Paper Award)**
  Yuancheng Jiang, Chuqi Zhang, Bonan Ruan, Jiahao Liu, Manuel Rigger, Roland Yap, Zhenkai Liang
  The 34th USENIX Security Symposium (**USENIX Security'25**)
- **Detecting Logic Bugs in Graph Database Management Systems via Injective and Surjective Graph Query Transformation**
  Yuancheng Jiang, Jiahao Liu, Jinsheng Ba, Roland Yap, Zhenkai Liang, Manuel Rigger
  The 46th International Conference on Software Engineering (**ICSE'24**)
- **EVCFI: Extensible Virtual Call Integrity**
  Yuancheng Jiang, Gregory J. Duck, Roland Yap, Zhenkai Liang, Pinghai Yuan
  The 27th European Symposium on Research in Computer Security (**ESORICS'22**)
- **RecIPE: Revisiting the Evaluation of Memory Error Defenses**
  Yuancheng Jiang, Roland Yap, Zhenkai Liang, Hubert Rosier
  The 17th ACM ASIA Conference on Computer and Communications Security (**AsiaCCS'22**)

- **Shoot the Honey, Cloak the Player: Towards Zero-Runtime-Overhead Proactive Defense and Detection for Visual Game Cheating**
  Jianing Wang, Chuqi Zhang, **Yuancheng Jiang**, Adil Ahmad, Shanqing Guo
  The 33rd ACM Conference on Computer and Communications Security (**CCS'26**)
- **Metamorphic Coverage**
  Jinsheng Ba, **Yuancheng Jiang**, Manuel Rigger
  The 35th ACM SIGSOFT International Symposium on Software Testing and Analysis (**ISSTA'26**)
- **Erebor: A Drop-In Sandbox Solution for Private Data Processing in Untrusted Confidential Virtual Machines**
  Chuqi Zhang, Rahul Priolkar, **Yuancheng Jiang**, Yuan Xiao, Mona Vij, Zhenkai Liang, Adil Ahmad
  The 20th ACM European Conference on Computer Systems (**EuroSys'25**)
- **Evaluating Disassembly Errors With Only Binaries**
  Lambang Akbar, **Yuancheng Jiang**, Roland Yap, Zhenkai Liang, Zhuohao Liu
  The 20th ACM ASIA Conference on Computer and Communications Security (**AsiaCCS'25**)
- **FlowMatrix: GPU-Assisted Information-Flow Analysis through Matrix-Based Representation**
  Kaihang Ji, Jun Zeng, **Yuancheng Jiang**, Zhenkai Liang, Zheng Leong Chua, Prateek Saxena, Abhik Roychoudhury
  The 31st USENIX Security Symposium (**USENIX Security'22**)

Research Impact

My research extends beyond prototypes to improve widely used software systems through tool adoption and bug discovery. FlowFusion has been integrated into PHP's official toolchain, and we have also developed FusionFuzz, a new fuzzing framework. Our work has identified **787 bugs spanning 28 Common Weakness Enumeration (CWE) categories**, including heap-based buffer overflows and use-after-free vulnerabilities. These findings span language processors: LLVM (87, across Clang, Flang, and MLIR), PHP (415), Swift (50), CPython (78), TypeScript (9), Rust (10), Julia (2), LFortran (15), Go (8), GCC (9), Ruby (8), R (1), and GHC (2); machine learning and GPU compilation: TVM (6), XLA (8), Mojo (2), Triton (2), Naga (4), and Tint (7); and database systems: Neo4j (19) and QuestDB (45). Our contributions have been publicly acknowledged by QuestDB developers.

Teaching Experience

Teaching Assistant, CS3213: Foundations of Software Engineering
National University of Singapore — Semester 2, AY 2023/24 and AY 2024/25
Led weekly labs for about 25 students and supervised 5 project teams each semester

Industry & Other Experience

- **Huawei Research Internship** — *Jun 2019 – Aug 2019*
  Huawei, Shanghai, China
- **CTF Competitive Security**, Team Sixstars — *2017 – 2020*
  Fudan University, Shanghai, China
- **NUS Summer Workshop on Cyber Security** — *Jul 2018 – Aug 2018*
  National University of Singapore, Singapore