Ruijie Meng

Ph.D. Candidate
School of Computing
National University of Singapore (NUS)

Email: ruijie@comp.nus.edu.sg
Address: COM3-02-20, 11 Research Link, Singapore 119391
Mobile: (+65) 89498841
Academic Homepage: https://mengrj.github.io/

RESEARCH INTERESTS

- **Software Engineering:** software testing, program analysis, fuzz testing, LLMs for testing
- **Software Security:** security vulnerability detection
- **Formal Methods:** software verification and validation, model checking

EDUCATION

Ph.D. Candidate, National University of Singapore (NUS), *Singapore* Aug 2020 - June 2025 (Expected)

- Major: Computer Science, School of Computing
- Advisor: Abhik Roychoudhury
- GPA: 4.83/5

M.Eng., University of Chinese Academy of Sciences (UCAS), *Beijing, China* Sep 2017 - Jun 2020

- State Key Laboratory of Computer Science, Institute of Software Chinese Academy of Sciences
- Advisor: Yan Cai
- GPA: 3.81/4 (Rank: 1/102)

B.Eng., Tianjin University (TJU), *Tianjin, China* Sep 2013 - Jun 2017

- Major: Software Engineering, School of Computer Software
- GPA: 3.79/4 (Rank: 3/113)

B.Ec., Nankai University (NKU), *Tianjin, China* Sep 2014 - Jun 2017

- Minor**:** Finance, School of Finance

RESEARCH PROJECTS

My recent research has been focused on developing effective and practical techniques to automatically validate **distributed, concurrent and stateful reactive software systems at scale**.

Specifically, my projects are over the following main dimensions:

• Validating More Complex Test Oracles: We leverage the concept of automat-theoretic model checking to direct fuzzing to search for LTL-property violations, getting close to the verification effect as in model checking.

• Searching for Deep States assisted by LLMs: Existing code feedback is not effective in guiding fuzzing towards deep states of reactive systems. We leverage LLMs to reason protocol states in network protocol fuzzing.

• Capturing Effect of Complex Program Environment: As reactive systems interact with complex execution environments, we propose fuzz testing to capture effect of different environments, avoiding environment modelling.

• Handling Distributed Systems: We developed the first greybox fuzzer for distributed systems guided by model behaviors, bringing distributed-system testing closer to the rigor of formal verification.

In addition, I worked on detection of concurrency bugs and vulnerabilities via program analysis.

PUBLICATIONS

• **Program Environment Fuzzing** CCS'24

Ruijie Meng, Gregory J. Duck, Abhik Roychoudhury

ACM Conference on Computer and Communications Security (CCS), 2024.

• **Large Language Model guided Protocol Fuzzing** NDSS'24

Ruijie Meng, Martin Mirchev, Marcel Böhme, Abhik Roychoudhury

Network and Distributed System Security Symposium (NDSS), 2024.

• **Greybox Fuzzing of Distributed Systems** CCS'23

Ruijie Meng, George Pirlea, Abhik Roychoudhury, Ilya Sergey

ACM Conference on Computer and Communications Security (CCS), 2023.

• **Linear-time Temporal Logic guided Greybox Fuzzing** ICSE'22

Ruijie Meng, Zhen Dong, Jialin Li, Ivan Beschastnikh, Abhik Roychoudhury

IEEE/ACM International Conference on Software Engineering (ICSE), 2022.

• **Low-Overhead Deadlock Prediction** ICSE'20

Yan Cai, **Ruijie Meng**(co-first author), Jens Palsberg

IEEE/ACM International Conference on Software Engineering (ICSE), 2020.

• **ConVul: An Effective Tool for Detecting Concurrency Vulnerabilities** ASE'19

Ruijie Meng, Biyun Zhu, Hao Yun, Haicheng Li, Yan Cai, Zijiang Yang

IEEE/ACM International Conference on Automated Software Engineering Tool (ASE), 2019.

• **Detecting Concurrency Memory Corruption Vulnerabilities** ESEC/FSE'19

Yan Cai, Biyun Zhu, **Ruijie Meng**, Hao Yun, Liang He, Purui Su, Bin Liang

ACM European Software Engineering Conference/Symposium on the Foundations of Software Engineering (ESEC/FSE), 2019.

• **ConRS: A Requests Scheduling Framework for Increasing Concurrency** COMPSAC'19

Degree of Server Programs

Biyun Zhu, **Ruijie Meng**, Zhenyu Zhang, W.K.Chan

IEEE International Computer Software and Applications Conference (COMPSAC), 2019.

SECURITY FINDINGS

Our tools have uncovered 100+ zero-day vulnerabilities in widely-used software systems, with many of them granted with CVEs. In CVSS severity level, over 20 CVEs are classified as CRITICAL/HIGH:

• CVE-2023-37117 • CVE-2023-51713 • CVE-2023-31654 • CVE-2023-31655 • CVE-2023-3138

- CVE-2023-30635
- CVE-2023-30636
- CVE-2023-30637
- CVE-2021-38386
- CVE-2021-38387
- CVE-2021-42141
- CVE-2021-42142
- CVE-2021-42143
- CVE-2021-42144
- CVE-2021-42145
- CVE-2021-42146
- CVE-2021-42147
- CVE-2021-38311
- CVE-2021-40523
- CVE-2021-40524

ACADEMIC SERVICES

- Program Committee for ASE 2024 Tool Demonstration Track, 2024
- Reviewer for Software Testing, Verification, and Reliability (STVR), 2024
- Reviewer for the Journal of Systems & Software (JSS), 2024
- Program Committee for ISSTA 2024 Artifact Evaluation, 2024
- Reviewer for IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), 2023
- Reviewer for ACM Transactions on Software Engineering and Methodology (TOSEM), 2023
- Program Committee for ISSTA 2023 Artifact Evaluation, 2023
- Program Committee for FUZZING 2022 Workshop@NDSS Artifact Evaluation, 2022
- Program Committee for ISSTA 2022 Artifact Evaluation, 2022
- Program Committee for ICSE 2022 Artifact Evaluation, 2022
- Student Volunteer for ESEC/FSE 2022

TEACHING EXPERIENCE

- Fuzzing and Software Security Summer School — National University of Singapore
  Lecturer — May 2024
- CS5219 Automated Software Validation — National University of Singapore
  Teaching assistant — Aug 2023 – Dec 2023
- CS2040 Data Structures and Algorithms — National University of Singapore
  Teaching assistant — Jan 2023 – Apr 2023
- CS5219 Automated Software Validation — National University of Singapore
  Teaching assistant — Aug 2022 – Dec 2022
- CS2040 Data Structures and Algorithms — National University of Singapore
  Teaching assistant — Jan 2022 – Apr 2022
- CS2040S Data Structures and Algorithms — National University of Singapore
  Teaching assistant — Aug 2021 – Dec 2021

SELECTED AWARDS

- NUS Dean's Graduate Research Excellence Award — 2023
- NUSGS Research Incentive Award — 2023 - 2024
- NUS Teaching Fellowship Nomination — 2023
- NUS SoC Research Achievement Award — 2023

- Singapore President's Graduate Fellowship 2020 - 2024
- Outstanding Graduate of Beijing (*Top 2%*) 2020
- Outstanding Graduate of University of Chinese Academy of Sciences (*Top 2%*) 2020
- President's Fellowship of Chinese Academy of Sciences (*Top 2%*) 2020
- China National Scholarship (*Top 2%*) 2019
- ACM SIGAI Scholarship 2019
- ACM SIGSOFT CAPS fund 2019
- First Prize Scholarship of University of Chinese Academy of Sciences (*Top 10%*) 2018, 2019
- Outstanding Bachelor Thesis of Tianjin University (*Top 10%*) 2017
- Outstanding Graduate of Tianjin University (*Top 10%*) 2017

REFERENCES

- **Abhik Roychoudhury** (thesis advisor)
  Provost's Chair Professor, National University of Singapore
  abhik@comp.nus.edu.sg
- **Marcel Böhme**
  Head of the Software Security Group, Max Planck Institute for Security and Privacy
  marcel.boehme@mpi-sp.org
- **Cristian Cadar**
  Professor, Imperial College London
  c.cadar@imperial.ac.uk
- **Rupak Majumdar**
  Scientific Director, Max Planck Institute for Software Systems
  Amazon Scholar, Amazon Web Services
  rupak@mpi-sws.org
- **Jens Palsberg**
  Professor of Computer Science, University of California, Los Angeles
  palsberg@ucla.edu