Ruijie Meng (孟瑞杰)

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 - Present
- Major: Computer Science, School of Computing
- Advisor: Abhik Roychoudhury (Provost's Chair Professor)
- 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 dedicated to developing effective and practical techniques to automatically validate **distributed, concurrent and stateful reactive systems at scale**, which are widely adopted by today's software applications to meet demands for robustness, scalability, and responsiveness in complex and dynamic environments.

Traditionally, the validation of such systems has heavily relied on software model checking. My research goes beyond traditional approaches by harnessing the concepts of software model checking to enhancing the bug-finding capabilities of fuzzing – an increasingly promising technique in the realm of bug detection. My approaches can thus achieve deep and systematic analysis of reactive systems.

The produced techniques represent a paradigm shift, significantly improving the bug-finding capabilities while preserving the scalability and usability inherent from fuzzing. This synergy between model checking and fuzzing

not only enhances the effectiveness of uncovering deep security bugs and vulnerabilities, but also makes the validation process more practical and efficient even when applied into complex and real-world systems.

My current projects are over three main perspectives:

• **Validating complex test oracles (ICSE'22):** 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 by state reasoning (CCS'23, NDSS'24):** Existing code feedback is not effective in guiding search towards deep states of reactive systems. We leverage LLMs to reason protocol states in testing network protocols and also create the first greybox fuzzer for distributed systems guided by model behaviors.

• **Capturing effect of complex program environment (arXiv'24):** As reactive systems interact with complex execution environments, we propose fuzz testing to automatically capture effect of different environments, avoiding environment modelling and manual-effort involving.

Besides these, I also worked on detection of concurrency bugs and vulnerabilities via program analysis.

PUBLICATIONS

• **Program Environment Fuzzing** arXiv'24

Ruijie Meng, Gregory J. Duck, Abhik Roychoudhury

arXiv preprint arXiv:2404.13951

• **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 Degree of Server Programs** COMPSAC'19

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 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 Summer School Lecturer	National University of Singapore May 2024
• CS5219 Automated Software Validation Teaching assistant	National University of Singapore Aug 2023 – Dec 2023
• CS2040 Data Structures and Algorithms Teaching assistant	National University of Singapore Jan 2023 – Apr 2023
• CS5219 Automated Software Validation Teaching assistant	National University of Singapore Aug 2022 – Dec 2022
• CS2040 Data Structures and Algorithms Teaching assistant	National University of Singapore Jan 2022 – Apr 2022

- CS2040S Data Structures and Algorithms
  Teaching assistant

National University of Singapore
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 University 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