Ruijie Meng (She/Her)

Ph.D. Candidate
School of Computing
National University of Singapore (NUS)
COM3-02-20, Singapore 119391

ruijie@comp.nus.edu.sg
(+65) 8949 8841
Homepage: https://mengrj.github.io/
GitHub: https://github.com/mengrj

Research Interests

My research interests are in Software Security and Software Engineering. My research focuses on developing practical and effective solutions that take a variety of techniques such as fuzz testing, software model checking and generative artificial intelligence to improve the reliability and security of software systems

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
- 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

Selected Awards

- Selected as a Participant for the 13th Global Young Scientists Summit 2024
- 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

PUBLICATIONS

- **Large Language Model assisted Hybrid Fuzzing** Under Review

  Ruijie Meng, Gregory J. Duck, Abhik Roychoudhury

  Under Review, 2024.

- **AFLNet Five Years Later: On Coverage-Guided Protocol Fuzzing** Under Review

  Ruijie Meng, Van-Thuan Pham, Marcel Böhme, Abhik Roychoudhury

  Under Review, 2024.

- **Program Environment Fuzzing** CCS'24

  Ruijie Meng, Gregory J. Duck, Abhik Roychoudhury

  31st ACM Conference on Computer and Communications Security (CCS), 16.9% acceptance rate

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

  Ruijie Meng, Martin Mirchev, Marcel Böhme, Abhik Roychoudhury

  31st Network and Distributed System Security Symposium (NDSS), 20.2% acceptance rate

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

  Ruijie Meng, George Pirlea, Abhik Roychoudhury, Ilya Sergey

  30th ACM Conference on Computer and Communications Security (CCS), 19.15% acceptance rate

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

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

  44th IEEE/ACM International Conference on Software Engineering (ICSE), 28.5% acceptance rate

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

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

  42nd IEEE/ACM International Conference on Software Engineering (ICSE), 20.9% acceptance rate

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

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

  34th IEEE/ACM International Conference on Automated Software Engineering Tool (ASE)

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

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

  27th ACM European Software Engineering Conference/Symposium on the Foundations of Software Engineering (ESEC/FSE), 24.4% acceptance rate

• **ConRS: A Requests Scheduling Framework for Increasing Concurrency Degree of Server Programs** COMPSAC'19

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

43rd IEEE International Computer Software and Applications Conference (COMPSAC)

SECURITY FINDINGS

*My research helped uncover **100+** previously unknown vulnerabilities in widely-used software systems, with many of them granted with CVEs. In CVSS severity level, **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

OPEN-SOURCE SOFTWARE

Open-sourced tools received much interest from both academia and industry (i.e., Oracle and Intel)

- EnvFuzz: EnvFuzz is a generic greybox fuzzer designed to fuzz the full interactions between a program and its execution environments. It is capable of almost fuzzing anything including network protocols, GUI/UI applications, editors, compilers, drivers and more:
  https://github.com/GJDuck/EnvFuzz
- ChatAFL: ChatAFL is a network protocol fuzzer that can chat with LLMs to extract machine-readable information from protocol specifications in natural language, including protocol states, message grammars and message types:
  https://github.com/ChatAFLndss/ChatAFL
- Mallory: Mallory is the first greybox fuzzer for distributed systems guided by model behaviors and it is also a reactive fuzzer that adaptively decides the input to inject based on observed states. It takes a trade-off between easy-of-use and effectiveness:
  https://github.com/dsfuzz/mallory
- LTL-Fuzzer: LTL-Fuzzer is a testing tool to find violations of deep specifications (LTL properties). It is inspired by software model checking to enhance the bug-finding capability of greybox fuzzing:
  https://github.com/ltlfuzzer/LTL-Fuzzer

RESEARCH GRANT

Assisted in the preparation and writing of research proposals for the following grants/industry gifts:

- 2023 – present: Fuzz Testing, NRF National Cybersecurity R&D in Singapore, founded amount: $6.7M: I helped write the proposal of reactive system fuzzing and contribute to the research
- 2024 – present: Automated Vulnerability Detection and Remediation, Oracle Labs, founded amount: $227K: I worked on the proposal writing of vulnerability detection and the research

TEACHING AND MENTORING

*I dedicated 15% of my time to teaching: taught courses in **undergraduate level (3×)**, **graduate level (2×)** and **industrial level (1×)**, and formally and informally mentored multiple students within and beyond NUS*

- For courses with available anonymous feedback (Automated Software Validation), received 4.6/5.0 and 4.4/5.0 scores, with students highlighting my teaching to ***enhance critical thinking and increase interest in the subject***
- Competition infrastructure and evaluation datasets developed for the summer school were ***adopted by other universities***
- I was nominated for the ***NUS Teaching Fellowship*** for excellence in teaching

- Lecturer for Hackathon Competition in Fuzzing and Software Security Summer School May 2024
  Led a practical-focused bug-finding competition for 72 participants from academia and industry
- Teaching Assistant for CS5219 Automated Software Validation in NUS Aug – Dec 2023
  32 graduate students, designed and delivered assignments, mentored students, graded and provided feedback
- Teaching Assistant for CS2040 Data Structures and Algorithms in NUS Jan – Apr 2023
  ~250 undergraduate students, delivered tutorials that supplemented lecture content
- Teaching Assistant for CS5219 Automated Software Validation in NUS Aug – Dec 2022
  34 graduate students, designed and delivered assignments, mentored students, graded and provided feedback
- Teaching Assistant for CS2040 Data Structures and Algorithms in NUS Jan – Apr 2022
  ~250 undergraduate students, mentored students on course assignments
- Teaching Assistant for CS2040S Data Structures and Algorithms in NUS Aug – Dec 2021
  ~250 undergraduate students, developed and graded course assignments
- Student Advising on Research Projects 2020 – present
  Informally advised multiple undergraduate, master's, and junior Ph.D. students within and beyond NUS, and helped advise one undergraduate thesis titled "LLM-based Test Harness Generation"

ACADEMIC SERVICES

- Reviewer for ACM Transactions on Software Engineering and Methodology (TOSEM), 2024
- 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, 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 Ada Workshop'22, ***supporting female and underrepresented researchers***
- Student Volunteer for ESEC/FSE 2022

REFERENCES

Abhik Roychoudhury (thesis advisor)
Provost's Chair Professor of School of Computing
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 of Department of Computing
Imperial College London
c.cadar@imperial.ac.uk

Rupak Majumdar
Scientific Director,
Max Planck Institute for Software Systems
rupak@mpi-sws.org

Jens Palsberg
Professor of Computer Science,
University of California, Los Angeles
palsberg@ucla.edu