Jinsheng Ba

Personal Website | GitHub | Google Scholar

National University of Singapore
Email: bajinsheng@u.nus.edu

Education

National University of Singapore — Singapore
Ph.D. Candidate in Computer Science — *Jan 2020 – Present*
Advisor: Manuel Rigger

Shandong University — Shandong, China
B.Eng. in Computer Science — *Sep 2013 – Jun 2017*

Publications

Testing Database Engines via Query Plan Guidance — ICSE'23
Jinsheng Ba**, Manuel Rigger* — ***ACM SIGSOFT Distinguished Paper Award
The 45th International Conference on Software Engineering, 2023
https://github.com/sqlancer/sqlancer/issues/641

Finding Performance Issues in Database Engines via Cardinality Estimation Testing — Preprint
***Jinsheng Ba**, Manuel Rigger*
Arxiv, 2023
https://github.com/sqlancer/sqlancer/issues/822

Efficient Greybox Fuzzing to Detect Memory Errors — ASE'22
Jinsheng Ba**, Gregory J Duck, and Abhik Roychoudhury* — ***ACM SIGSOFT Distinguished Paper Award
The 37th IEEE/ACM International Conference on Automated Software Engineering, 2022
https://github.com/bajinsheng/ReZZan

Stateful Greybox Fuzzing — SEC'22
***Jinsheng Ba**, Marcel Böhme, Zahra Mirzamomen, Abhik Roychoudhury*
The 31st USENIX Security Symposium, 2022
https://github.com/bajinsheng/SGFuzz

Work Experience

Security Engineer — Jul 2017 – Dec 2019
Huawei — *Beijing, China*

- Analyze the security device log (IPS, WAF, Host-Guard, etc.) on the cloud to extract **threat intelligence** using Spark, Kafka, HBase.
- Optimize the machine learning algorithms to detect malware from dynamic execution traces and improve the recall by **13%**.
- Write virus analysis report and help customers to prevent attacks.

Teaching Experience

- Teaching Assistant for BT2102 Data Management and Visualisation (2022-2023 Semester 2)
- Teaching Assistant for BT2102 Data Management and Visualisation (2022-2023 Semester 1)
- Teaching Assistant for CS2040 Data Structures and Algorithms (2022-2023 Semester 1)

Services

- Program Committee for FSE'23 Artifact Evaluation.
- Program Committee for DEBT'23 Workshop at ISSTA'23.
- Program Committee for PLDI'23 Artifact Evaluation.
- Student Volunteer for FSE'22.

Awards

- Dean's Graduate Research Excellence Award. (Aug 2023, NUS)
- ACM SIGSOFT Distinguished Paper Award. (Feb 2023, ICSE)
- Research Achievement Award. (Jan 2023, NUS)
- ACM SIGSOFT Distinguished Paper Award. (Oct 2022, ASE)
- Research Scholarship. (Aug 2022, NUS)
- Outstanding Graduate of Shandong Province. (Jun 2017, China)
- Outstanding Undergraduate Research Assistant. (Dec 2016, SDU)
- Outstanding Leader of Association in Shandong Province, the only one in SDU (Sep 2016, China)
- First Prize Scholarship of Shandong University. (Sep 2016, SDU)
- Second Prize for Microsoft Imagine Cup Contest (Jun 2015, Microsoft)

Talks

- Open day at School of Computing, National University of Singapore: Testing Database Engines via Query Plan Guidance. (Feb 2023, Singapore)
- Seminar at Tsinghua University: Testing Database Engines via Query Plan Guidance. (Dec 2022, China)
- Seminar at TiDB company: Testing Database Engines via Query Plan Guidance. (Nov 2022, China)
- Security workshop at School of Computing, National University of Singapore: Efficient Greybox Fuzzing to Detect Memory Errors (Nov 2022, Singapore)
- Software engineering workshop at School of Computing, National University of Singapore: Testing Database Engines via Query Plan Guidance. (Nov 2022, Singapore)
- 37th IEEE/ACM International Conference on Automated Software Engineering: Efficient Greybox Fuzzing to Detect Memory Errors. (Oct 2022, USA)
- 31st USENIX Security Symposium: Stateful Greybox Fuzzing. (Aug 2022, USA)
- Mayday workshop at School of Computing, National University of Singapore: Stateful Greybox Fuzzing. (May 2022, Singapore)

Research Philosophy

My research interests focus on software security. My vision is to make the software more reliable. I aim to research novel and practical methods to solve real-world problems of software security. My research has found around 100 bugs, of which 78 are public, in real-world systems. I commit to and have always made the code of my research public for purposes of reproducibility and real-world impact.