Zu-Ming Jiang

Email: jjzuming@outlook.com Mob: (86)17816861042

RESEARCH INTEREST

Fuzzing, System Software Reliability, Program Analysis

EDUCATION

Tsinghua University (Advisor: Prof. Shi-Min Hu) *Sep. 2018-Jun. 2021 (expected)*
M.E. in Computer Technology, GPA: **3.97/4.00**, Ranking: **4/138**
Main Courses: Advanced Operating Systems (98/100), Modern Method for Optimal Calculation (98/100), Computer System Performance Measurement (92/100), Parallel Computing (92/100), Computer Network Architecture (92/100)
Honor & Award: **Siebel Scholar** (awarded annually for academic excellence to over 90 top students in the world)

Zhejiang University *Sep. 2014-Jun. 2018*
B.E. in Electrical Engineering and Automation, GPA: **3.86/4.00**
Minor: Advanced Honor Class of Engineering Education (ACEE) in Chu Kochen Honors College
Main Courses: Fundamentals of Computer Science (99/100), Computer Network and Communication (93/100), Fundamentals of Data Structures (93/100), Computing Method (94/100)
Honor & Award: Outstanding Bachelor Thesis, Meritorious Winner of Mathematical Contest in Modeling

PUBLICATION

[1] **Zu-Ming Jiang**, Jia-Ju Bai, Kangjie Lu, Shi-Min Hu. Fuzzing Error Handling Code using Context-Sensitive Software Fault Injection. USENIX Security, 2020.
[2] **Zu-Ming Jiang**, Jia-Ju Bai, Julia Lawall, Shi-Min Hu. Fuzzing Error Handling Code in Device Drivers Based on Software Fault Injection. ISSRE, 2019.
[3] Qiu-Liang Chen, Jia-Ju Bai, **Zu-Ming Jiang**, Julia Lawall, Shi-Min Hu. Detecting Data Races Caused by Inconsistent Lock Protection in Device Drivers. SANER, 2019.

RESEARCH & EXPERIENCE

Project I: Research on the method for testing error handling code in device drivers Beijing, China
Project core member *Sep. 2018-May. 2019*
1. Propose a new fuzzing strategy based on software fault injection to effectively cover error handling code.
2. Develop a kernel-level fuzzing tool named FIZZER to effectively test error handling code in device drivers. FIZZER has successfully found 22 new real bugs on 18 device drivers in Linux 4.19.
3. Conclude the aforementioned work into a paper which has been accepted by **ISSRE 2019**.

Project II: Effective fuzzing framework for bug detection in error handling code Beijing, China
Project core member *Jun. 2019-Dec. 2019*
1. Propose a novel context-sensitive error sequence model to perform finer-grained software fault injection.
2. Propose a new fuzzing approach which can dynamically inject faults based on both locations of error sites and their calling contexts, to cover hard-to-trigger error handling code.
3. Develop a practical fuzzing framework named FIFUZZ to effectively test error handling code. FIFUZZ has successfully found 50 unique bugs on 9 well-tested and widely-used C applications like OpenSSL, Clamav.
4. Conclude the aforementioned work into a paper which has been accepted by **USENIX Security 2020**.

Project III: Concurrency fuzzing framework for data race detection Beijing, China
Project core member *Jan. 2020-May. 2020*
1. Propose a novel concurrency fuzzing approach to explore thread interleavings using a new concurrency-coverage metric.
2. Develop a novel fuzzing framework which has found dozens of real data races in some user-level and kernel-level programs.
3. The paper of this project is under review.

SKILLS

- Dynamic analysis based on LLVM
- Linux kernel programming
- Programming language: C/C++, Python and Java