Chijin Zhou (周炽金)

System Security Assurance Lab
Tsinghua University, Beijing, China

☎ (+86) 15624952117
✉ zcj18@mails.tsinghua.edu.cn

EDUCATION

Master Student, Software Engineering 2018.9 – Present

Supervisor: Prof. Yu Jiang
School of Software, Tsinghua University

Bachelor, Software Engineering 2014.9 – 2018.7

GPA: 88/100 (Rank: 9th out of 180 students)
School of Computer Science & Technology, Beijing Institute of Technology

RESEARCH INTERESTS

Software Security, Automatic Vulnerability Detection, System Security

RESEARCH EXPERIENCE

Master Student

Supervisor: Prof. Yu Jiang
System Security Assurance Lab, Tsinghua University, Beijing, 2018.9 - Present

- Researched on effective large system fuzzing.
- Proposed a zero-overhead instrumentation for effective coverage collection (namely Zeror, published in ASE'20), which improves the execution speed by 159.80% of the state-of-the-art fuzzers like AFL.
- Proposed and implemented a visualization tool for fuzzing (namely VisFuzz, published in ASE'19 demo track) so that higher coverage is achieved by fuzzers with the aid of human knowledge.
- Participated in the development of DFuzz (submitted to Security'21), which specializes in fuzzing complex distributed systems. 55 bugs (of PostgreSQL, Comdb2 and Redis) have been discovered by DFuzz.
- Participated in the development of PAFL (published in FSE'18) and EnFuzz (published in USENIX Security'19). Both focus on higher fuzzing effectiveness in parallel mode.

Security Research Intern

Tencent Blade Team, Tencent, Shenzhen, 2020.6-2020.8

- Researched on cloud native security and container security.
- Discovered two vulnerabilities on Kubernetes, one (CVE-2020-8560) may cause path traversal attack and incorrect assess control, another (CVE-2020-8556) may cause denial of service.
- Discovered an out-of-range bug in a standard library of Golang, which may cause denial of service.

PUBLICATIONS

- Mingzhe Wang, Zhiyong Wu, Xinyi Xu, Jie Liang, **Chijin Zhou**, Huafeng Zhang and Yu Jiang. Industry Practice of Coverage-Guided Enterprise-Level DBMS Fuzzing. In Proceedings of *ICSE'21-SEIP*.
- Mingzhe Wang, Jie Liang, **Chijin Zhou**, Yuanliang Chen, Zhiyong Wu, Yu Jiang. Industrial Oriented Evaluation of Fuzzing Techniques.In Proceedings of *ICST'21-industry*.
- **Chijin Zhou**, Mingzhe Wang, Jie Liang, Zhe Liu, Yu Jiang. Zeror: Speed Up Fuzzing with Coverage-sensitive Tracing and Scheduling. In Proceedings of *ASE'20*.
- **Chijin Zhou**, Mingzhe Wang, Jie Liang, Zhe Liu, Chengnian Sun, Yu Jiang. VisFuzz: Understanding and Intervening Fuzzing with Interactive Visualization. In Proceedings of *ASE'19-demo*.
- Yuanliang Chen, Yu Jiang, Fuchen Ma, Jie Liang, Mingzhe Wang, **Chijin Zhou**, Xun Jiao, Zhuo Su. Enfuzz: Ensemble fuzzing with seed synchronization among diverse fuzzers. In Proceedings of *USENIX Security'19*.
- Jie Liang, Yu Jiang, Yuanliang Chen, Mingzhe Wang, **Chijin Zhou**, Jiaguang Sun. Pafl: extend fuzzing optimizations of single mode to industrial parallel mode. In Proceedings of *FSE'18-industry*.

UNDER REVIEW PAPERS

- Mingzhe Wang, Jie Liang, **Chijin Zhou**, Zhiyong Wu, Yu Jiang. DFuzz: Inter-Process Fuzzing of Distributed Systems. Submitted to *USENIX Security'21, under review*.
- Jie Liang, Mingzhe Wang, **Chijin Zhou**, Zhiyong Wu, XinYi Xu, Zhe Liu, Yu Jiang. PATA: Fuzzing with Path Aware Taint Analysis. Submitted to *S&P'21, under review*.

CONFERENCE PRESENTATIONS

- The 35th IEEE/ACM International Conference on Automated Software Engineering, 21-25 September 2020, online presentation.
- The 34th IEEE/ACM International Conference on Automated Software Engineering, 10-15 November 2019, San Diego, USA (oral).

HONORS AND AWARDS

2019	The THUNISOFT Scholarship, Tsinghua University
2019	The MITSUBISHI Scholarship, Tsinghua University
2018	Outstanding Graduate Award, Beijing Institute of Technology
2016	The CASC Scholarship, Beijing Institute of Technology
2016	Grand prize of ”Century Cup” Technology Competition, Beijing Institute of Technology

VULNERABILITY DISCLOSURE

- Independently discovered 30+ vulnerabilities in several open-source projects including Kubernetes, Golang, PostgresSQL, libjpeg, etc., and 17 of them have CVE IDs.
  See: `https://github.com/ChijinZ/security_advisories`.

MISCELLANEOUS

- Language: Chinese (Native), English (Fluent, IELTS band 7).
- Coding skills: Rust, Python, C++, JavaScript.
- Program analysis: fuzzing (AFL, libFuzzer, etc.), Clang-Static Analyzer, llvm.