Yang Lan

Email: lanyang0908@gmail.com Mobile: +86-17812061756

Research Interests

My research focuses on system security. I have recently concentrated on building an extensible general fuzzing framework from scratch, which can automatically adopt the most advanced fuzzing strategy throughout the fuzzing campaign. Additionally, we decompose kernel fuzzing process and implement a modular kernel fuzzer based on this framework. My research systematically and comprehensively analyzes the performance of popular fuzzers (e.g., Syzkaller) and improves fuzzing technique to test system and software programs (e.g., Linux kernel), having published two research papers in prestigious conferences (e.g., ASE, USENIX Security). I also report bugs and CVE for Linux kernel and contribute patches.

Education

- **Peking University** — Beijing, China
  Master of Software Engineering — *Sept 2018 - June 2021*
- **China University Of Petroleum** — Qingdao, China
  Bachelor of Computer Science — *Sept 2014 - June 2018*

Experience

- **Zhongguancun Laboratory & Tsinghua University** — Mentor: **Chao Zhang**
  Software Engineer — *June 2021 - Present*
  - **Linux Kernel Security, Fuzzing, Static Analysis**

Projects

- **xFUZZ: A Flexible and Extensible Fuzzing Framework for Runtime Schedule.** [2023.7-present, Code Contribution]
  We develop a flexible and extensible fuzzing framework from scratch, which decomposes fuzzing process into various plugins to support fine-grained, runtime-adaptive strategy composition. We propose an adaptive algorithm based on Sliding-Window Thompson Sampling to dynamically select the optimal fuzzing strategy throughout the fuzzing campaign. In addition, we implement a modular kernel fuzzer based on xFUZZ, which can adopt practical fuzzing strategies and support various kernel fuzzing, including Linux, Windows, and Android.
  - 75k C++, 0.8k Python LoC for Xfuzz and glue scripts.
- **Thunderkaller: Profiling and Improving the Performance of Syzkaller.** [2021.7-2023.7, Lead]
  We undertake a substantial measurement study (e.g., Throughput on different workloads and kernel configurations, several variants of Syzkaller) to dissect the cost of Syzkaller, which gives a systematic understanding of the major overheads. According to our measurement, we propose KID to reduce unnecessary instrumentation, come up with three optimizations, and implement a tool dubbed Thunderkaller to improve the performance of Syzkaller.
  - 3.7k C/C++, 0.8k Golang, 0.5k Python LoC for measurement pipeline, kernel image duplication, and three optimizations.
- **AIFORE: Smart Fuzzing Based on Automatic Input Format Reverse.** [2021.7-2022.10, Code Contribution].
  We utilize taint analysis and minimum cluster algorithm to identify field boundary and relationships between input bytes and basic blocks. Moreover, we leverage the CNN model to predict the type of input fields processed by basic blocks. Based on knowledge of programs' input format, we design a novel format-based power scheduling algorithm to explore infrequent types of inputs, which substantially enhances fuzzing performance.
  - 5k C++, 7k Python LoC for the taint analysis engine and format analysis modules.

Publications

- **xFUZZ: A Flexible Framework for Fine-Grained, Runtime-Adaptive Fuzzing Strategy Composition**
  Dongsong Yu, Yiyi Wang, Chao Zhang, **Yang Lan**, Zhiyuan Jiang, Shuitao Gan, Zheyu Ma, and Wende Tan
  Under Review
- **Thunderkaller: Profiling and Improving the Performance of Syzkaller** [**PDF**]
  Yang Lan*, Di Jin*, Zhun Wang, Wende Tan, Zheyu Ma, and Chao Zhang
  In 2023 38th IEEE/ACM International Conference on Automated Software Engineering (ASE 2023).
  *Co-first authors
- **AIFORE: Automatic Input Format Reverse Engineering** [**PDF**]
  Ji Shi*, Zhun Wang*, Zhiyao Feng, **Yang Lan**, Shisong Qin, Wei You, Wei Zou, Mathias Payer, and Chao Zhang
  In 32nd USENIX Security Symposium (USENIX Security 23).
  *Co-first authors

Honors and Awards

- Silver Medal in the 41th ACM-ICPC Asia East Continent Final 2016
- Silver Medal in the 41th ACM-ICPC Asia Regionals Dalian site 2016
- Gold Medal(3rd place) in the 7th ACM-ICPC Shandong Province 2016
- Excellent Graduate Student of Peking University 2019
- The Scholarship of China University Of Petroleum 2016

Skills Summary

- **Languages** C/C++, Golang, Shell, Python, etc.
- **Soft Skills** Team-spirited, Determination, and Self-movtivated.

Volunteer Experience

- **BCTF AutoPwn 2022** Beijing, China
  Designed competition problems, including stack overflow and directed fuzzing. *Dec 2022*
- **The 44th ACM-ICPC Asia Regionals Qingdao site** Qingdao, China
  Designed competition problems and conducted online and offline technical services. *Oct 2019*