

HAN ZHENG

BC 156, EPFL, 1015 Lausanne

han.zheng@epfl.ch

EDUCATION

École Polytechnique Fédérale de Lausanne

2023 Aug - Now

PhD candidate in Computer Science

Supervisor: Prof. Mathias Payer

University of Chinese Academy of Science

2020 Aug - 2023 Jun

M.E. in Electronic Information Engineering

Xidian University

2016 Aug - 2020 Jun

B.E. in Information Countermeasure Technique

EXPERIENCE

École Polytechnique Fédérale de Lausanne

2021 Dec - 2022 Dec

Visiting Student in HexHive.

Supervisor: Prof. Mathias Payer

PROJECTS

FishFuzz: Catch Deeper Bugs by Throwing Larger Nets

USENIX Sec'23

Boosting the Multi-Target Directed Greybox Fuzzing by improving the precision of distance calculation and dynamically adjusting target priority. FishFuzz found 38 CVEs in exhaustively tested programs.

🏆 **FishFuzz (’s extension) won 2nd Place in SBFT’24.**

MendelFuzz: The Return of the Deterministic Stage

FSE’25

Analyzing the key limitation of the deterministic stage in Greybox Fuzzing, further improves the deterministic stage by skipping redundant mutations. MendelFuzz proposes a new deterministic stage with higher efficiency than the havoc stage, and outperforms AFL++ both in coverage and bug findings.

🏆 **MendelFuzz became the default mode in AFL++.**

AWARDS AND SCHOLARSHIPS

Chromium Vulnerability Reward Program (2024), 25,000 USD, Google

2025 Jan

SBFT FuzzBench Competition 2nd Place, 300 EUR, Google

2024 Apr

EDIC PhD Fellowship, 54,000 CHF, EPFL

2023 Sep

IC Master Scholarship, 22,400 CHF, EPFL

2021 Dec

Visiting Scholarship, 23,400 CHF, China Scholarship Council

2021 Dec

BUG HUNTING

Google Leaderboard Ranking: #42 in Google VRP 2024

ChromeOS: CVE-2025-2509 (Virglrenderer, Medium)

Chrome: CVE-2025-0438 (Tracing, High), CVE-2025-0436 (Skia, High), b/365802556 (Blink, High), CVE-2024-7968 (UI, High), b/349253666 (UI, Medium), CVE-2024-5846 (PDF, Medium), CVE-2024-5847 (PDF, Medium), CVE-2024-7018 (PDF, Medium)

Wireshark: CVE-2024-0209, CVE-2024-0210

Apple Font: CVE-2022-26981, CVE-2022-31783

SERVICE

Technical Program Committee FUZZING'25

Journal Reviewer TSE (CCF-A), TOSEM (CCF-A), TIFS (CCF-A)

Shadow TPC NDSS'24 (CCF-A), ISSTA'24 (CCF-A)

SKILLS

Coding: C, Python, gdb, LLVM, AFL/AFL++, Docker

Languages: Chinese (Mother Tough), English (IELTS 7.0)

TALK

SBFT24@ICSE, Lisbon, Portugal FuzzBench competition report

2024 Apr

Research Seminar at HUST, Wuhan, China Hosted by Prof. Wei Zhou

2023 Jun

PUBLICATIONS

- [4] **Han Zheng**, Flavio Toffalini, Marcel Böhme, and Mathias Payer. Mendelfuzz: The return of the deterministic stage. In *Proceedings of the 33rd ACM International Conference on the Foundations of Software Engineering*, 2025
- [3] **Han Zheng**, Flavio Toffalini, and Mathias Payer. Tunefuzz: Adaptively exploring target programs. In *Proceedings of the 17th ACM/IEEE International Workshop on Search-Based and Fuzz Testing*, pages 61–62, 2024
- [2] **Han Zheng**, Jiayuan Zhang, Yuhang Huang, Zezhong Ren, He Wang, Chunjie Cao, Yuqing Zhang, Flavio Toffalini, and Mathias Payer. {FISHFUZZ}: Catch deeper bugs by throwing larger nets. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 1343–1360, 2023
- [1] Zezhong Ren, **Han Zheng**, Jiayuan Zhang, Wenjie Wang, Tao Feng, He Wang, Yuqing Zhang, et al. A review of fuzzing techniques. 2021