Yongheng Chen

Email: changochen1@gmail.com | HomePage: https://changochen.github.io/

WORK EXPERIENCE

Google DeepMind **Mountain View, US**
Software Engineer *Jan 2025-now*

- Confidential LLM inference

Google **Sunnyvale, US**
Software Engineer *June 2024-Jan 2025*

- Make Rust/C++ interop effortless

Google **Remote, US**
Software Engineering Intern, Team Sundew *May 2023-Aug 2023*

- Support RPC service fuzzing in FuzzTest, Google's next generation fuzzing framework.

Google **Remote, US**
Software Engineering Intern, Team CastCloud *May 2022-Aug 2022*

- Develop an internal debugging tool and improve Google Nest RPC services.

Google **Remote, US**
Software Engineering Intern, Team Sundew *May 2021-Aug 2021*

- Support grammar fuzzing in FuzzTest, Google's next generation fuzzing framework.

EDUCATION

Georgia Institute of Technology **Atlanta, US**
PhD, Computer Science, advised by Prof. Wenke Lee *2019-2024*

- Research interests: Software Security, AI security, Fuzzing

Nanjing University **Nanjing, China**
BS, Computer Science, Elite program *2015-2019*

PROJECT EXPERIENCE

(Rust) Private Memory: Make AI stateful in a privacy-preserving way
AI, Confidential Computing *2025-now*

- https://github.com/project-oak/oak/tree/main/oak_private_memory

(C++) Effective Programmable Fuzzing Oracle for Non-Crashing Bugs
Fuzzing, Programming Language, Program Analysis *2023-now*

- Develop fuzzing oracles with an expressive specification language.
- Describe the bugs as easy as CodeQL, and fuzz for the bugs with concrete PoCs.

(C++) Database & Language Processors Testing With LLM Augmentation
Fuzzing, NLP, Database, Program Analysis *2019-now*

- Generic language fuzzing framework with transformer-based LLM augmentation.
- Found over 280 bugs and 40 CVEs in popular software: SQLite, MySQL, PHP, Chrome, etc.
- Used by MariaDB, Palo Alto Networks, Redis, etc.

(C++) FuzzTest: Google's Next Generation Fuzzing Framework
Fuzzing, Property-based Testing *2021-now*

- Bridge the gap between fuzzing and property-based testing for C++ programs.
- A fuzzing framework for replacing AFL/libfuzzer in Google.

(Rust) Scalable Parallel Fuzzing Framework
Fuzzing, Microservice, Async Programming *2022*

- A scalable parallel fuzzing framework using microservice architecture.

(Java) Mobile Application Debloating
Android, Program Analysis *2021*

- Remove unnecessary code features from android apk based on user profiles.

(C++) Exploit Generation For Augmenting Control Flow Hijacking
Symbolic Execution, Taint Analysis *2020*

- Augmenting RIP control with arbitrary argument control to achieve RCE.

(Python) Testing Compilers For Optimization Issues
Differential Analysis, Program Analysis, Compiler *2020*

- Perform differential analysis with symbolic execution using Angr.

SKILLS

Programming Languages: C/C++, Rust, Java, Python, Go, Haskell, TypeScript

Frameworks: Tensorflow, PyTorch, Keras, Angular, LLVM

CTF player: Windows & Linux userspace and kernel exploitation, browser exploitation, VM escape.

Open source contributor: https://github.com/OMH4ck

PUBLICATION

Towards Generic Database Management Systems Fuzzing **Usenix Security**
Fuzzing *2024*

µFuzz: Redesign of Parallel Fuzzing Using Microservice Architecture **Usenix Security**
Fuzzing, https://github.com/OMH4ck/mufuzz *2023*

One Engine to Fuzz ‘em All: Generic Language Processor Testing with Semantic Validation **S&P**
Fuzzing, https://github.com/OMH4ck/PolyGlot *2021*

Identifying Behavior Dispatchers for Malware Analysis **Asia CCS**
Malware Analysis *2021*

SQUIRREL: Testing Database Management Systems with Language Validity and Coverage Feedback **CCS**
Fuzzing, https://github.com/OMH4ck/Squirrel *2020*

Automated Finite State Machine Extraction **FEAST**
Program Analysis *2019*

PT-DBG: Automatically anti-debugging bypassing based on Intel Processor Trace **S&P (poster)**
Malware Analysis *2019*

HONORS & AWARDS

Finalist, DEFCON CTF World, five times	2018-2023, Las Vegas, US
Champion, XCTF Final	2018-2019, China
Champion, Tencent CTF 2019 Final	2019, China
Runner-Up, 34C3 CTF	2018, Online
Champion & Runner Up, Defcon China CTF Qual, Defcon China CTF Final	2018, China
Specialty Scholarship, Elite Program Scholarship	2018, Nanjing University, China
Specialty Scholarship, Elite Program Scholarship	2017, Nanjing University, China

TALKS

The Art of Fuzzing FCIS 2023, Shanghai, China