Yongheng **Chen**

Georgia Institute of Technology, Atlanta, GA, USA. 30332

☎ (+1) 8143251330 | ✉ changochen1@gmail.com | ⌂ Changochen.github.io | Changochen

“Only those who are crazy enough to think they can change the world are the ones who do.”

Education

Georgia Institute of Technology
Atlanta, GA, US

PhD student in Computer Science *Sept. 2019 - now*

- Computer security and program analysis, advised by Prof. Wenke Lee.

Nanjing University
Nanjing ,China

B.S. in Computer Science. *Sept. 2015 - June. 2019*

- **Elite program**(only top 19 out of over 200 students can enter it) GPA:4.26/5

Work Experience

Software Engeering Intern
Remote, US

Google, Team SunDew *May - August, 2023*

- Support RPC service fuzzing in Google’s FuzzTest.

Software Engeering Intern
Remote, US

Google, Team CastCloud *May - August, 2022*

- Develop an internal debugging tool and improve bussiness code in Java.

Software Engeering Intern
Remote, US

Google, Team SunDew *May - August, 2021*

- Support grammar fuzzing in FuzzTest, Google’s next generation fuzzing framework for c++ applications.

Project Experience

(C++) Program Property Validation With Fuzzing

property-based Fuzzing, DSL design *2023-now*

- Combine the expressiveness of static analysis and scalability of fuzzing to find property violation.

(Python, C++) Language Fuzzing with LLM-augmented Mutation

Fuzzing, Natural Language Processing *2023-now*

- Utilize transformer-based LLM to generate code segument to augment mutation of language fuzzing.

(C++) FuzzTest: Google’s Next Generation Fuzzing Framework

Fuzzing, property-based testing *2021-now*

- A fuzzing framework that bridges the gap between fuzzing and property-based testing for C++ programs.

(Rust) Scalable Parallel Fuzzing Framework

Fuzzing, asynchronous programming, System design *2021-2022*

- A scalable parallel fuzzing framework using micro-serivce architecture.

(Java) Mobile Application Debloating

Android, Program analysis *2021-2022*

- Remove unnessary code features from android apk according to users’ needs.

(C++) Database & Language Processors Testing

Fuzzing, Program analysis *2019-2020, 2023*

- Found over 280 bugs and 40 CVEs in popular software: SQLite, MySQL, PHP, Chrome, etc.
- Adopted by MariaDB, AntGroup, Redis.

(C++) Exploit Generation For Augmenting Control Flow Hijacking

Symbolic Execution, Taint Analysis *2020*

- Augmenting RIP control with arbitrary argument control.

(Python) Testing Compilers For Optimization Issues

PROGRAM ANALYSIS, DIFFERENTIAL ANALYSIS *2020*

- Perform differential analysis with symbolic execution using Angr.

Skills

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

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

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

Publication

µFuzz: Redesign of Parallel Fuzzing Using Microservice Architecture *Usenix Sec*

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 *AsiaCCS*

MALWARE ANALYSIS *2021*

SQUIRREL: Testing Database Management Systems with Language Validity and Coverage Feedback *CCS*

FUZZING, HTTPS://GITHUB.COM/S3TEAM/SQUIRREL *2020*

Automated Finite State Machine Extraction *FEAST 2019*

PROGRAM ANALYSIS *2019*

PT-DBG: Automatically anti-debugging bypassing based on Intel Processor Trace *S&P, Poster*

MALWARE ANALYSIS *2018*

Honors & Awards

HACKING COMPETITION

2018-2023	**Finalist**, DEFCON CTF World Final	*Las Vegas, U.S.A & remote*
2018-2019	**Champion**, XCTF 2018 International CTF Final and **3 times** champions in XCTF Final	*China*
2019	**Champion**, Tencent CTF 2019 Final	*International*
2018	**Runner-Up**, 34c3CTF 2018	*International*
2018	**Champion & Runner Up**, Defcon China CTF Qual, Defcon China CTF Final	*Beijing, China*

SCHOLARSHIP

2018	**Specialty Scholarship**, Elite Program Scholarship	*Nanjing University*
2017	**Specialty Scholarship**, Elite Program Scholarship	*Nanjing University*