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, Rank:10/19.

Work Experience

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*

- Develop a new fuzzing framework for c++ applications.

Project Experience

(Rust) Scalable Distributed Fuzzing Framework

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

- Develop a scalable fuzzing framework that can run across machines.

(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*

- Found over 230 bugs and 40 CVEs in popular software: SQLite, MySQL, PHP, Chrome, etc.
- Used by MariaDB, AntGroup.

(Python) Testing Compilers For Optimization Issues

Program Analysis, Differential Analysis *2020*

- Perform differential analysis with symbolic execution using Angr. 3 bugs found in SQLite.

Skills

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

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

Open source contributor: CTF wiki(https://github.com/ctf-wiki/ctf-wiki);

Squirrel(https://github.com/s3team/Squirrel); PolyGlot(https://github.com/s3team/Polyglot)

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/s3team/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 (CCS workshop)*
Program analysis *2019*

PT-DBG: Automatically anti-debugging bypassing based on Intel Processor Trace *S&P, Poster*
Malware analysis *2018*

Honors & Awards

Hacking Competition

2018-2022	**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*