# Cen Zhang

*Curriculum Vitae*

*Georgia Institute of Technology*
*The United States*
*+1 470 808 2829*
*blbllhy@gmail.com*
*cenzhang.github.io*

## Earned Degrees

2019 – 2023 **Ph.D of Computer Science**
Nanyang Technological University, Singapore

2014 – 2017 **Master of Computer Science**
University of Science and Technology of China, Hefei, Anhui

2009 – 2013 **Bachelor of Computer Science**
North China Electric Power University, Baoding, Hebei

## Research Interests

My research has a focus on software security and vulnerability detection:

- AI x Vuln Detection
- Program Analysis x Vuln Detection
- Firmware Rehosting
- Software Testing

## Honors And Awards

2025 DARPA AIxCC Competition 1st Place Winner, $4.0M Prize

2024 Best Paper Award for Thrust B Projects, Continental-NTU Corporate Lab

2024 ACM SIGSOFT Distinguished Paper Award, ICSE 2024

2023 ACM SIGSOFT Distinguished Paper Award, ASE 2023

2021 Best Paper Award of Year 2021, Most Influential Research Paper Election, Ant Finance Co, Ltd

2020 Best Early-Research-Achievement Paper, APSEC 2020

2019 1st Award in Prototype Competition (freestyle track), NASAC 2019 (aka Chinasoft)

2017 The Best New Employee Award, IFLYTEK Co, Ltd

## Publications

By 2025 Sep, my **citation is 833 and H-index is 14** in Google Scholar.

** stands for co-first author, + for corresponding author*

Arxiv 25 Team Atlanta (**Cen Zhang** works as the Java sub-team leader), ATLANTIS: AI-driven Threat Localization, Analysis, and Triage Intelligence System. **Technical report for DARPA AIxCC Competition 1st Place Winner system.**

NDSS 26 *Chuan Qin, ***Cen Zhang**, Yaowen Zheng, Puzhuo Liu, Jian Zhang, Yeting Li, Weidong Zhang, Yang Liu, Limin Sun. User-Space Dependency-Aware Rehosting for Linux-Based Firmware Binaries.

Usenix Sec 25 Yeting Li, Yecheng Sun, Zhiwu Xu, Haiming Chen, Xinyi Wang, Hengyu Yang, Huina Chao, **Cen Zhang**, Yang Xiao, Yanyan Zou, Feng Li, Wei Huo. VULCANBOOST: Boosting ReDoS Fixes through Symbolic Representation and Feature Normalization. **Honorable Mentions, 6% (25/407) of the accepted papers.**

FSE 25 Ziqiao Kong, +**Cen Zhang**, Maoyi Xie, Ming Hu, Yue Xue, Ye Liu, Haijun Wang, Yang Liu. Smart Contract Fuzzing Towards Profitable Vulnerabilities.

ICSE 25 Jiageng Li, Zhen Dong, Chong Wang, Haozhen You, **Cen Zhang**, Yang Liu, Xin Peng. LLM-Based Input Space Partitioning Testing for Library APIs.

ACM Computing Surveys [*]Xiaohan Zhang, [*]**Cen Zhang**, Xinghua Li, Zhengjie Du, Bing Mao, Yuekang Li, Yaowen Zheng, Yeting Li, Li Pan, Yang Liu, Robert Deng. A Survey of Protocol Fuzzing.

ASE 24 Baijun Cheng, [+]**Cen Zhang**, Kailong Wang, Ling Shi, Yang Liu, Haoyu Wang, Yao Guo, Xiangqun Chen. Semantic-Enhanced Indirect Call Analysis with Large Language Models.

ISSTA 24 **Cen Zhang**, Yaowen Zheng, Mingqiang Bai, Yeting Li, Wei Ma, Xiaofei Xie, Yuekang Li, Limin Sun, Yang Liu. How Effective Are They? Exploring Large Language Model Based Fuzz Driver Generation.

ICSE 24 Yiming Liu, **Cen Zhang**, Feng Li, Yeting Li, Jianhua Zhou, Jian Wang, Lanlan Zhan, Yang Liu, Wei Huo. Semantic-Enhanced Static Vulnerability Detection in Baseband Firmware. **ACM SIGSOFT Distinguished Paper Award**

ISSTA 24 Jiongchi Yu, Xiaofei Xie, **Cen Zhang**, Sen Chen, Yuekang Li, Wenbo Shen. Bugs in Pods: Understanding Bugs in Container Runtime Systems.

Black Hat USA 24 Bohan Liu, Zong Cao, Zheng Wang, Yeqi Fu, **Cen Zhang**, Achilles' Heel of JS Engines: Exploiting Modern Browsers During WASM Execution.

ISSTA 24 Maoyi Xie, Ming Hu, Ziqiao Kong, **Cen Zhang**, Yebo Feng, Haijun Wang, Yue Xue, Hao Zhang, Ye Liu, Yang Liu. DeFort: Automatic Detection and Analysis of Price Manipulation Attacks in DeFi Applications.

WWW 24 Zhengjie Du, Yuekang Li, Yaowen Zheng, Xiaohan Zhang, **Cen Zhang**, Yi Liu, Sheikh Mahbub Habib, Xinghua Li, Linzhang Wang, Yang Liu, Bing Mao. Medusa: Unveil Memory Exhaustion DoS Vulnerabilities in Protocol Implementations.

Usenix Sec 23 **Cen Zhang**, Yuekang Li, Hao Zhou, Xiaohan Zhang, Yaowen Zheng, Xian Zhan, Xiaofei Xie, Xiapu Luo, Xinghua Li, Yang Liu, and Sheikh Mahbub Habib. Automata-Guided Control-Flow-Sensitive Fuzz Driver Generation.

Oakland 23 [*]Xinyi Wang, [*]**Cen Zhang**, Yeting Li, Zhiwu Xu, Shuailin Huang, Yi Liu, Yican Yao, Yang Xiao, Yanyan Zou, Yang Liu, and Wei Huo. Effective ReDoS Detection by Principled Vulnerability Modeling and Exploit Generation.

ASE 23 Yao Zhang, Xiaofei Xie, Yi Li, Sen Chen, **Cen Zhang**, Xiaohong Li. EndWatch: A Practical Method for Detecting Non-Termination in Real-World Software. **ACM SIGSOFT Distinguished Paper Award**

ASE 23 Yi Liu, Yuekang Li, Gelei Deng, Yao Du, **Cen Zhang**, Chengwei Liu, Yeting Li, Lei Ma, Yang Liu. Aster: Automatic Speech Recognition System Accessibility Testing for Stutterers.

ISSTA 22 Yaowen Zheng, Yuekang Li, **Cen Zhang**, Hongsong Zhu, Yang Liu, and Limin Sun. Efficient Greybox Fuzzing of Applications in Linux-Based IoT Devices via Enhanced User-Mode Emulation.

Usenix Sec 21 **Cen Zhang**, Xingwei Lin, Yuekang Li, Yinxing Xue, Jundong Xie, Hongxu Chen, Xinlei Ying, Jiashui Wang, and Yang Liu. APICraft: Fuzz Driver Generation for Closed-source SDK Libraries. **Best paper award of Ant Financial Group in 2021**

CCS 21 Muhui Jiang, Lin Ma, Yajin Zhou, Qiang Liu, **Cen Zhang**, Zhi Wang, Xiapu Luo, Lei Wu, and Kui Ren. ECMO: Peripheral Transplantation to Rehost Embedded Linux Kernels.

ASE 21 *Qiang Liu, *__Cen Zhang__, Lin Ma, Muhui Jiang, Yajin Zhou, Lei Wu, Wenbo Shen, Xiapu Luo, Yang Liu, and Kui Ren. FirmGuide: Boosting the Capability of Rehosting Embedded Linux Kernels Through Model-Guided Kernel Execution.

ASE 21 [*]**Cen Zhang**, [*]Yuekang Li, Hongxu Chen, Xiaoxing Luo, Miaohua Li, Anh Quynh Nguyen, and Yang Liu. BIFF: Practical Binary Fuzzing Framework for Programs of IoT and Mobile Devices. **1st Award in NASAC 2019 Competition**

ISSRE 21 Yuekang Li, Guozhu Meng, Jun Xu, **Cen Zhang**, Hongxu Chen, Xiaofei Xie, Haijun Wang, and Yang Liu. Vall-nut: Principled anti-grey box fuzzing.

APSEC 20 Yuekang Li, Hongxu Chen, **Cen Zhang**, Siyang Xiong, Chaoyi Liu, and Yi Wang. Ori: A Greybox Fuzzer for SOME/IP Protocols in Automotive Ethernet. **Best Paper Award in ERA track**

Usenix Sec 20 Hongxu Chen, Shengjian Guo, Yinxing Xue, Yulei Sui, **Cen Zhang**, Yuekang Li, Haijun Wang, and Yang Liu. MUZZ: Thread-aware grey-box fuzzing for effective bug hunting in multithreaded programs.

FSE 19 Yuekang Li, Yinxing Xue, Hongxu Chen, Xiuheng Wu, **Cen Zhang**, Xiaofei Xie, Haijun Wang, and Yang Liu. Cerebro: context-aware adaptive fuzzing for effective vulnerability detection.

## Academic Services

Program Committee

- ASE 2025, Research Track
- ASE 2025, NIER Track
- ACSAC 2025, Research Track
- ICDM 2025, LLM4Sec Workshop
- ISSTA 2025, EXPRESS Track
- ICECCS 2025, Research Track
- Internetware 2025, Tool Demonstration Track
- IJCAI 2025, Survey Track
- Oakland 2025, HMISA Workshop
- EuroSys 2025, Research Track (Shadow Program Committee)
- MSR 2025, Research Track (Junior Program Committee)

Session Chair

- PRDC 2023, System & Data Dependability Session

Artifact Evaluation Committee

- NDSS 2026
- NDSS 2025
- USENIX Security 2025
- ASE 2022

Journal Reviewer

- ACM Transactions on Software Engineering and Methodology (TOSEM)
- IEEE Transactions on Information Forensics and Security (TIFS)
- IEEE Transactions on Reliability (TR)
- IEEE Transactions on Dependable and Secure Computing (TDSC)

## Teaching

Guest Lecturer

23/08 **Introduction of Software Engineering**, Nanyang Technological University

Delivered a 3-hour lecture on the history and recent developments in software development and testing.

16/09 - 17/01 **Introduction of Information Security**, University of Science and Technology of China

Designed and taught six lab experiments covering malware analysis, fuzzing, reverse engineering, and vulnerability analysis.

Teaching Assistant

19/07 - 23/12 **Introduction of Software Engineering**, Nanyang Technological University (six semesters)

Lab management, advising students on coursework and assignments.

16/01 - 17/01 **Introduction of Information Security**, University of Science and Technology of China (two semesters)

Lab management, advising students on coursework and assignments.

## Research Grants

2022 - 2024 Co-Principal Investigator (Co-PI) of 500,000+ SGD government project

## Patents

- Control-flow-sensitive fuzz driver generation. **In the application progress of NTU-Conti Corp Lab.**
- Semi-automated harness generation for dynamic software analysis. **In the appliation progress of NTU-Conti Corp Lab.**
- Efficient Greybox fuzzing for Automotive Grade Linux (AGL) Applications. **In the appliation progress of NTU-Conti Corp Lab.**

## Employment History

Cybersecurity

24/11 - Present **Postdoctoral Researcher**
Georgia Institute of Technology, US

23/07 - 24/10 **Postdoctoral Researcher**
Nanyang Technological University, Singapore

Microservice

17/07 – 18/10 **Algorithm and Engine Development Engineer**
IFLYTEK Co, Ltd, Hefei, Anhui