Cen Zhang

Curriculum Vitae

Cyber Security Lab
Nanyang Technological University
Singapore
✉ *blbllhy@gmail.com*
1995/05/07, Male

Education

2019 – 2023 (expected) **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

- *Fuzzing; Software Vulnerability; Software Security; System Security;*

General Information

- 70+ CVEs, hundreds of bugs for software in Linux and Mac OS
- Skillful in both static and dynamic software analysis techniques
- C/C++/Golang/Java/OCaml/Python/Bash
- 4+ years research experiences on fuzzing/software testing
- Skillful in vulnerability hunting, reverse engineering, and exploitation
- IELTS 7.5 (L8/R8.5/W6/S6.5)

Publications (First/Co-first Author)

- **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, IEEE S&P 2023*
- ***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, USENIX Security 23*
- ***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, USENIX Security 21* **Best paper award of Ant Financial Group in 2021**

- *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 2021* **Co-first author**
- ***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, ASE 2021* **Co-first author**

Publications (Not First/Co-first Author)

- *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, ISSTA 2022*
- *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, CCS 2021*
- *Yuekang Li, Guozhu Meng, Jun Xu, **Cen Zhang**, Hongxu Chen, Xiaofei Xie, Haijun Wang, and Yang Liu. Vall-nut: Principled anti-grey box fuzzing, ISSRE 2021*
- *Yuekang Li, Hongxu Chen, **Cen Zhang**, Siyang Xiong, Chaoyi Liu, and Yi Wang. Ori: A Greybox Fuzzer for SOME/IP Protocols in Automotive Ethernet, APSEC 2020* **Best Paper Award in ERA track**
- *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, USENIX Security 20*
- *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, ESEC FSE 2019*
- *Fan Jiang, **Cen Zhang**, and Shaoyin Cheng. Fffuzzer: Filter your fuzz to get accuracy, efficiency and schedulability, ACISP 2017*

Awards

- *Best Paper Award of Year 2021*, Most Influential Research Paper Election of Ant Finance
- *Best Early-Research-Achievement Paper*, APSEC 2020
- *1st Award in Prototype Competition (freestyle track)*, NASAC 2019
- *The Best New Employee Award of Year 2017*, IFLYTEK Co, Ltd

Public Services

- Program Committee, Artifical Evaluation Track, ASE 2022

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.**

Work Experience

Software Vulnerability

18/11 – 19/07 **Research Associate**
NTU, Singapore

16/06 – 16/10 **Intern of Department of Vulnerability Mining**
China Information Technology Security Evaluation Center, Beijing

15/08 – 16/02 **Intern of Vulcan Team**
Qihoo 360 Technology Co, Ltd, Beijing

Microservice

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