Chongzhou Fang

Davis, CA
Google Scholar
Personal Website Linkedin
Email: czfang@ucdavis.edu

SKILLS

Programming skills: C/C++, Python, MATLAB, Parallel Computing (Cilk), Heterogeneous Computing (OpenCL, OPAE/IOFS)

Hardware Design: Verilog RTL Level Design, OpenCL for Intel FPGA

Simulation and Prototyping: Implementing behavior simulator for large systems

EDUCATION

University of California, Davis, CA 09/2020-Present
Ph.D. in Electrical and Computer Engineering GPA: 3.9/4.0
Southeast University, Nanjing, China 08/2016 - 06/2020
B.Eng. in Information Science GPA: 3.9/4.0

INDUSTRY EXPERIENCE

PSG Graduate Intern, Intel 06/2022 – 09/2022

- Work on developing a demo for new security features in Intel FPGAs.
- Utilize IOFS to build a library that handles host-FPGA communication and attestation protocols.

RESEARCH EXPERIENCE

Research Assistant, UC Davis, CA, United States 09/2020 – Present
Advised by Dr. H. Homayoun and Dr. K. Khasawneh **Research focus: Cloud Security, FPGA security**

- Prove that cloud schedulers are susceptible to being exploited by malicious users to achieve co-location with victim instances, which opens the door for future micro-architectural attacks. Experiments are conducted in Kubernetes. (Work published at NDSS'22).
- Quantitatively model cluster and application heterogeneity and provide methods to quantitatively evaluate the security level of a running cluster. (Work published at NDSS'23).
- Work on improving the scheduling quality and security of SLURM deployed in a university's computing center by integrating plugins that utilize machine learning algorithms to conduct performance modeling into the scheduler. (In collaboration with UC Davis High-Performance Computing Center)
- Prove that FPGA PCIe side channels can be used to fingerprint customized circuits on FPGA clouds. (Work accepted for publication at CCS'23).
- Work on developing a novel C++-based cloud infrastructure simulator targeting the security community. It aims to integrate scheduler-level simulation and performance modeling.
- Work on researching LLM-based code analysis, especially LLM-based code obfuscation and de-obfuscation methods.

Research Assistant, Southeast University, China 04/2017 – 06/2020
School of Information Science and Engineering **Research Focus: Hardware Design**

- Targeting the application scenario of HLS, developed a hardware architecture generator.
- According to algorithmic description, it automatically generates synthesizable Verilog HDL description.
- Published in IEEE ASICON 2019, won Excellent Student Paper Award

SELECTED PAPERS

1. (Published) **C. Fang** *et al.* "Repttack: Exploiting Cloud Schedulers to Guide Co-Location Attacks," *Network and Distributed Systems Security (NDSS) Symposium 2022.* (Acceptance rate 16%)
2. (Published) **C. Fang** et al. "HeteroScore: Evaluating and Mitigating Cloud Security Threats Brought by Heterogeneity," Network and Distributed Systems Security (NDSS) Symposium 2023. (Acceptance rate 16%)
3. (Accepted) **C. Fang** *et al.* "Gotcha! I Know What You are Doing on the FPGA Cloud: Fingerprinting Co-Located Cloud FPGA Accelerators via Measuring Communication Links," ACM Conference on Computer and Communications Security (CCS) 2023. (Acceptance rate: 18.0%)