Yicheng Zhang

University of California, Irvine
+1 9492312128
https://yichez16.github.io/yicheng.github.io/
yichez16@uci.edu

Education

University of California, Irvine — Irvine, CA
M.S. in Computer Engineering, GPA: 3.75/4.00 — 2018.9–Current
- Advisors: Mohammad Abdullah Al Faruque and Zhou Li

Sichuan University — Chengdu, China
B.S. in Electrical Engineering and Automation, GPA: 3.53/4.00 — 2014.9–2018.6
- Thesis: "Fault detection in power transmission system using Machine Learning."

Experience

University of California, Irvine — Irvine, CA
Research Assistant in Embedded & Cyber-Physical Systems Lab — 2018.9–Current
- Embedded and Cyber-Physical System Security, Computer Microarchitecture.
- I worked with my advisor Prof. Mohammad Abdullah Al Faruque on research topics including security in Embedded & Cyber-Physical Systems and side-channel attack & defense.

University of California, Irvine — Irvine, CA
Research Assistant in Data-driven Security and Privacy (DSP) Lab — 2018.9–Current
- Machine learning privacy and defense.
- I worked with my advisor Prof. Zhou Li on research topics including machine learning privacy attack and hardware security.

University of California, Irvine — Irvine, CA
Teaching Assistant in Department of Electrical Engineering and Computer Science — 2019.12–2020.6
- Assisted course instructors in course website design, grading, and lecturing.

University of California, San Diego — San Diego, CA
Visiting undergraduate researcher in Adaptive Computing and Embedded Systems (ACES) Lab — 2017.9–2017.12
- PUFs security.
- I worked with my advisor Prof. Farinaz Koushanfar on research topics related to security of PUFs.

Publications

1. Wei Junyi*, **Yicheng Zhang***, Zhe Zhou, Zhou Li, and Mohammad Abdullah Al Faruque, "Leaky DNN: Stealing Deep-Learning Model Secret with GPU Context-Switching Side-Channel.", *2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (**DSN'2020**), Valencia, Spain, June, 2020.*
*__Junyi Wei and Yicheng Zhang are both first author.__

2. **Yicheng Zhang**, Rozhin Yasaei, Hao Chen, Zhou Li and Mohammad Abdullah Al Faruque, "Poster: Stealing Neural Network Structure through Remote FPGA Side-channel Analysis", *In 29th ACM/SIGDA International Symposium on Field-Programmable Gate Arrays (**FPGA'2021**).*

3. Anomadarshi Barua, **Yicheng Zhang** and Mohammad Abdullah Al Faruque, "BayesMem: An End-to-End Bayesian Memory-Deduplication based Rowhammer Attack on Industrial Control Systems", *Under review in ACM Conference on Computer and Communications Security (**CCS'2021**).*

Teaching

- **Teaching Assistant** at University of California, Irvine — Winter 2019
  EECS 150 Continuous-Time Signals and Systems
- **Teaching Assistant** at University of California, Irvine — Spring 2020
  EECS 111 Sytem Software
- **Teaching Assistant** at University of California, Irvine — Fall 2020
  EECS 40 Object Oriented System Programming
- **Teaching Assistant** at University of California, Irvine — Winter 2021
  CS 125 Next Generation Search Systems

Computer Skills

- **Programming:** C/C++, CUDA C, Python, Verilog, Bash Script(Linux), Java
- **Assembly:** MIPS, 8051
- **CAD Tools:** Altera Quartus, Xilinx ISE, Vivado, Vivado HLS, Xilinx SDK
- **Softwares:** Matlab and Simulink, Arduino

Languages

- **English:** Fluent
  - **EXAM:** Score 102 for TOEFL iBT test
- **Chinese:** Native

Projects

Machine Learning Model Stealing Attacks on GPU

- Developed a novel GPU side-channel based on context-switching penalties.
- Implementation of LSTM-based inference model to identify the structural secret.
- Extracted the fine-grained structural secret of VGG16/ZFNET/AlexNet/MLP.

Remote Side-Channel Attack on FPGA to Steal Neural Network Structure

- Developed a novel FPGA power side-channel based attack on a Machine learning models.
- Implementation of VGG16, AlexNet, and MLP models on FPGA accelerator as victim models and a ring oscillator-based circuit to extract power side-channel of victim models.
- Used NearestNeighbors, GradientBoosting, DecisionTree, RandomForest, NeuralNetwork, NaiveBayes, AdaBoost, and XGB classifiers to recover hyper-parameters of victim model from side-channel signals.

Bayesian Memory-Deduplication based Rowhammer Attack on Industrial Control Systems

- Developed a new technique to duplicate the .bss section of the target control DLL file, which requires less memory and time compared to recent works.
- Created a Hardware-in-the-Loop (HIL) testbed with a scaleddown model of a practical engine cooling system of thermo-electric plants as an example of ICS.
- Used the Beremiz softPLC to create the automation platform and connect the softPLC to clouds using industry-standard cloud protocols.

Scholarships and Awards

- Sichuan University Scholarship (China) — 2014,2015,2016,2017
- Outstanding Students Leader of Sichuan University — 2016.10

Extracurricular Activities

- Member at University of California Irvine Cycling Club — 2018–Current

- Member at Chinese Students Scholars Association at UCI (UCI-CSSA) 2018–Current
- Head of Practice Department of Sichuan University Cycling Club 2014–2018
- Volunteers at 120th Anniversary of Sichuan University 2016.9
- Volunteers at HIV Propaganda and Education 2015.10