

## Education

---

### University of California, Riverside

P.h.D in Electrical Engineering, GPA: 3.81/4.00

– Advisors: Prof. Nael Abu-Ghazaleh

Riverside, CA

2021.9–Current

### University of California, Irvine

M.S. in Computer Engineering, GPA: 3.78/4.00

– Thesis: “Stealing Deep Learning Model Secret through Remote FPGA Side-channel Analysis”

Irvine, CA

2018.9–2021.6

### Sichuan University

B.S. in Electrical Engineering and Automation, GPA: 3.53/4.00

– Thesis: “Fault detection in power transmission system using Machine Learning”

Chengdu, China

2014.9–2018.6

## Professional Experience

---

### University of California, Riverside

Research Assistant in Secure and Efficient Architectures and Systems (SEAS) Lab

– AR/VR Security, Computer Architecture Support for Security.

– I worked with my advisor Prof. Nael B. Abu-Ghazaleh on research topics including security in AR/VR systems and side-channel attack & defense on computer architecture

Riverside, CA

2021.9–Current

### University of California, Irvine

Teaching Assistant in Department of Electrical Engineering and Computer Science

– Assisted course instructors in course website design, grading, and lecturing

Irvine, CA

2018.9–2021.6

## Peer-reviewed Publications

---

### Conference Papers

1. Carter Slocum, **Yicheng Zhang**, Jiasi Chen, Nael B. Abu-Ghazaleh, “Going through the motions: AR/VR typing inference using head motion tracking”, *Under review in Proceedings of the 32nd USENIX Security Symposium (USENIX Security)*, Anaheim, CA, USA, August, 2023.
2. **Yicheng Zhang**, Carter Slocum, Jiasi Chen, Nael B. Abu-Ghazaleh, “It’s all in your head(set): side-channel attacks on augmented reality systems”, *In Proceedings of the 32nd USENIX Security Symposium (USENIX Security)*, Anaheim, CA, USA, August, 2023.
3. 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”, *In 2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Valencia, Spain, June, 2020.  
\*Junyi Wei and Yicheng Zhang are both first author.

### Journal Articles

1. **Yicheng Zhang**, Rozhin Yasaei, Hao Chen, Zhou Li and Mohammad Abdullah Al Faruque, “Stealing Neural Network Structure through Remote FPGA Side-channel Analysis”, *In IEEE Transactions on Information Forensics and Security (TIFS)*, August, 2021.

## Posters

1. **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)*, February, 2021.

## Teaching Experience

---

<b>Teaching Assistant</b> at University of California, Irvine <i>Organization of Digital Computers (EECS112)</i>	Spring 2021
<b>Teaching Assistant</b> at University of California, Irvine <i>Next Generation Search Systems (CS125)</i>	Winter 2021
<b>Teaching Assistant</b> at University of California, Irvine <i>Object Oriented System &amp; Programming (EECS40)</i>	Fall 2020
<b>Teaching Assistant</b> at University of California, Irvine <i>Sytem Software (EECS111)</i>	Spring 2020
<b>Teaching Assistant</b> at University of California, Irvine <i>Continuous-Time Signals and Systems (EECS150)</i>	Winter 2019

## Presentations & Talks

---

1. “Poster: Stealing Neural Network Structure through Remote FPGA Side-channel Analysis” at FPGA’21, virtual, February 2021
2. “Leaky DNN: Stealing Deep-Learning Model Secret with GPU Context-Switching Side-Channel” at DSN’20, virtual, June 2020

## Skills

---

- **Programming:** C/C++, Python, Java, Verilog/System Verilog, TensorFlow, PyTorch, Numpy, Assembly
- **Tools:** Altera Quartus, Xilinx Vivado/ISE, Vivado HLS, Jupyter Notebook
- **Softwares:** Matlab, Arduino, Unity, Unreal Engine

## Professional Service

---

- Reviewer for ICPS’ 20, CYBER’ 21, CYBER’ 22
- Artifact Evaluation for Micro’ 22

## Projects

---

### AR/VR typing inference using head motion tracking

- Showed that there is a serious security risk of typed text in the foreground being inferred by a background application, without requiring any special permissions.
- Developed a system, **TyPose**, that automatically infers words and characters typed by a user, including a Segmenter to divide a stream of sensor readings into the corresponding words/characters and a Classifier to infer the text corresponding to those segments.
- Collected user traces of AR/VR typing behavior, and evaluated our attack on these traces. The results show that **TyPose** can detect segments and identify words with high accuracy.

### Side-channel attacks on Mixed Reality systems via Rendering Performance Counters

- Presented a taxonomy of the potential targets and leakage sources of software-based side-channel attacks on AR/VR devices and applications.
- Demonstrated four end-to-end side-channel attacks that illustrate three types of targets: Inferring (1) user interactions (hand gesture inputs and virtual keyboard inputs); (2) information about concurrent applications (fingerprinting newly launched applications); and (3) information about the environment (detecting and ranging a person in the environment).
- Discussed potential mitigations based on: (a) limiting the access to performance counters, (b) monitoring for abnormal contention, and (c) an explicit permission management system.

### **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 scaled-down 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.

### **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.

### **Machine Learning Model Stealing Attacks via GPU Context-Switching Side-Channel**

- 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.

## **Mentoring Experience**

---

### **Undergraduate Students**

- Cheng Gu UCR CSE, 2022-
- Xuchang Zhan UCI EECS, 2019-2020

## **Selected Honors & Awards**

---

- Student Travel Grant for ACM Conference on Computer and Communications Security 2021
- Student Travel Grant for USENIX Security Symposium 2021
- Student Travel Grant for IEEE Symposium on Security and Privacy 2021,2022
- Dean's Distinguished Fellowship Award (UC Riverside) 2021

## **Outreach Activities**

---

- **Mentor** at UCR Graduate Student Mentorship Program 2022-2023
- **Mentor** domestic and international undergraduate students in UCI 2019-2020
- **Chair** of Practice Department of Sichuan University Cycling Club 2015-2016
- **Volunteer** at 120th Anniversary of Sichuan University 2016.9