Yicheng Zhang

University of California, Riverside
+1 9492312128
Website: yichez.site
yzhan846@ucr.edu

Education

University of California, Riverside — Riverside, CA
P.h.D in Electrical Engineering, GPA: 3.67/4.00 — 2021.9–Current
- Advisors: Prof. Nael Abu-Ghazaleh

University of California, Irvine — Irvine, CA
M.S. in Computer Engineering, GPA: 3.78/4.00 — 2018.9–2021.6
- Thesis: "Stealing Deep Learning Model Secret through Remote FPGA Side-channel Analysis"

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"

Professional Experience

University of California, Riverside — Riverside, CA
Research Assistant in Secure and Efficient Architectures and Systems (SEAS) Lab — 2021.9–Current
- 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

University of California, Irvine — Irvine, CA
Teaching Assistant in Department of Electrical Engineering and Computer Science — 2018.9–2021.6
- Assisted course instructors in course website design, grading, and lecturing

Peer-reviewed Publications

Conference Papers

1. Carter Slocum, **Yicheng Zhang**, Jiasi Chen, Nael B. Abu-Ghazaleh, "Going through the motions: AR/VR keylogging from user head motions", *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

Teaching Assistant at University of California, Irvine — Spring 2021
Organization of Digital Computers (EECS112)

Teaching Assistant at University of California, Irvine — Winter 2021
Next Generation Search Systems (CS125)

Teaching Assistant at University of California, Irvine — Fall 2020
Object Oriented System & Programming (EECS40)

Teaching Assistant at University of California, Irvine — Spring 2020
Sytem Software (EECS111)

Teaching Assistant at University of California, Irvine — Winter 2019
Continuous-Time Signals and Systems (EECS150)

Presentations and 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, Linux (Bash), Assembly
- **Tools:** Altera Quartus, Xilinx Vivado/ISE, Vivado HLS, Jupyter Notebook
- **Softwares:** Matlab, Arduino, Unity, Unreal Engine, Android Studio

Professional Service

- Reviewer for ICPS' 20, CYBER' 21, CYBER' 22, IEEE TIFS, IEEE TC, IJACT
- Artifact Evaluation for Micro' 22

Research Projects

AR/VR typing inference using head motion tracking

- 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.
- The related paper was accepted in Usenix Security 2023.

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 five end-to-end side-channel attacks that illustrate three types of targets: Inferring (1) user interactions (hand gesture inputs, voice commands, 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).
- The related paper was accepted by Usenix Security 2023 (First author).

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

- Developed a novel FPGA power side-channel-based attack on Machine learning models.
- Used NearestNeighbors, GradientBoosting, DecisionTree, RandomForest, NeuralNetwork, NaiveBayes, AdaBoost, and XGB classifiers to recover hyper-parameters of victim model from side-channel signals.
- The related paper was accepted by FPGA 2021 and IEEE TIFS (First author).

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 of VGG16, ZFNET, AlexNet and MLP.
- The related paper was accepted by IEEE DSN 2020 (First author).

Academic Supervision and Mentorship

Undergraduate Students

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

Graduate Students

- Sriraksha Srirangapatna Arun — UCR CSE, 2023–Current

Honors and Awards

- Student Travel Grant for gem5 Boot Camp — 2022
- 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

Volunteering, Diversity & Inclusion

- **Mentor** at UCR Graduate Student Mentorship Program (GSMP) — 2022-2023
- **Mentor** at UCR International Student Peer Mentor Program (ISPMP) — 2022-2023
- **Mentor** domestic and international undergraduate students in UCI — 2019-2020
- **Volunteer** at 120th Anniversary of Sichuan University — 2016.9