Yicheng Zhang

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

Education

University of California, Riverside — Riverside, CA
P.h.D in Electrical Engineering, GPA: 3.71/4.00 — 2021.9–Current

- Advisor: 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"
- Thesis Advisors: Prof. Mohammad Abdullah Al Faruque and Prof. 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"
- Thesis Advisor: Prof. Yang Liu

Professional Experience

Pacific Northwest National Laboratory — Richland, WA
Research Intern at the Center for Advanced Technology Evaluation (CENATE) — 2023.6–2023.9

- Mentors: Dr. Kevin J. Barker, Dr. Andres Marquez, and Dr. Sankha Baran Dutta
- Topic: Microarchitecture Security in Multi-GPU Systems

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

- Mentor: Prof. Nael B. Abu-Ghazaleh
- Topic: AR/VR Security, Computer Architecture Support for Security

University of California, Riverside — Riverside, CA
Graduate Student Mentor in UCR Graduate Student Mentorship Program (GMSP) — 2022.9–2023.6

- Mentor: Prof. Philip Brisk
- I worked with Prof. Philip Brisk to help first-year graduate students transition from undergraduate programs or careers into graduate study

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

My research interest lies in **hardware security, AR/VR, side-channel attacks, and computer architecture**.
Full profile on Google Scholar: https://scholar.google.com/citations?user=X3LwPLAAAAAJ&hl=en

Conference Papers

C5. **Yicheng Zhang**, Ravan Nazaraliyev, Sankha Baran Dutta, Nael Abu-Ghazaleh, Andres Marquez and Kevin Barker, "Beyond the Bridge: Contention-Based Covert and Side Channel Attacks on Multi-GPU Interconnect", *In Proceedings of the 2024 IEEE International Symposium on Secure and Private Execution Environment Design (**SEED**), Orlando, FL, USA, January 2024.*

C4. Carter Slocum*, **Yicheng Zhang***, Erfan Shayegani, Pedram Zaree, Nael B. Abu-Ghazaleh, and Jiasi Chen, "That Doesn't Go There: Attacks on Shared State in Multi-User Augmented Reality Applications", *In Proceedings of the 33rd USENIX Security Symposium (**USENIX Security**), Philadelphia, PA, USA, August 2024.*
***Equal contribution.**

C3. Carter Slocum, **Yicheng Zhang**, Jiasi Chen, and 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.*

C2. **Yicheng Zhang**, Carter Slocum, Jiasi Chen, and 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.*

C1. 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.*
***Equal contribution.**

Journal Articles

J1. **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 (**IEEE TIFS**), August 2021.*

Workshop Papers

W1. **Yicheng Zhang**, Dhroov Pandey, Di Wu, Turja Kundu, Ruopu Li and Tong Shu, "Accuracy-Constrained Throughput Optimization and Performance Profiling of CNN Inference for Detecting Drainage Crossing Locations", *In Proceedings of the SC'23 Workshops of The International Conference on High Performance Computing, Network, Storage, and Analysis (**SC'23 Workshop**), Denver, CO, USA, November 2023.*

Posters

P1. **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. "Accuracy-Constrained Efficiency Optimization and GPU Profiling of CNN Inference for Detecting Drainage Crossing Locations" at SC'23 Workshop, Denver, CO, USA, November, 2023
2. "It's all in your head(set): side-channel attacks on augmented reality systems" at USENIX Security'23, Anaheim, CA, USA, August, 2023
3. "Poster: Stealing Neural Network Structure through Remote FPGA Side-channel Analysis" at FPGA'21, virtual, February 2021
4. "Leaky DNN: Stealing Deep-Learning Model Secret with GPU Context-Switching Side-Channel" at DSN'20, virtual, June 2020

Skills and Selected Courses

- **Programming:** C/C++, CUDA C++, C#, Python, Java, Verilog, TensorFlow, PyTorch, Linux (Bash), Assembly
- **Tools:** Altera Quartus, Xilinx Vivado/ISE, Vivado HLS, Jupyter Notebook
- **Softwares:** Matlab, Arduino, Unity, Unreal Engine, Android Studio
- **Selected Courses:** Autonomous Cyber-Physical Systems (A+), GPU Architecture & Parallel Programming (A), Advanced Operating Systems (A), Pattern Recognition (A), Advanced Computer Vision (A), Advanced System Security (A), Machine Learning & Artificial Intelligence (A)

Service and Professional Activities

Service to Profession - Program Committee

- TPC Member, International Conference on Emerging Information Security and Applications (EISA), 2023.
- TPC Member, International Workshop on Security (IWSEC), 2023.
- TPC Member, International Conference on Cyber-Technologies and Cyber-Systems (CYBER), 2021, 2022, 2023.
- TPC Member, International Conference on Edge Computing and IoT: Systems, Management and Security (EAI ICECI), 2024.

Service to Profession - Conference and Journal Reviewer

- Reviewer, IEEE International Conference on Industrial Cyber-Physical Systems (ICPS), 2020.
- Reviewer, EAI International Conference on Sec. and Pri. in Communication Networks (EAI SecureComm), 2023.
- Reviewer, IEEE Transactions on Information Forensics and Security (IEEE TIFS), 2023.
- Reviewer, Journal of Computer Security (JCS), 2023.
- Reviewer, IEEE Transactions on Computers (IEEE TC), 2023.
- Reviewer, International Journal of Applied Cryptography (IJACT), 2023.
- Reviewer, Security and Communication Networks (SCN), 2023.
- Reviewer, Journal of Systems Architecture (JSA), 2023.
- Reviewer, EURASIP Journal on Information Security (EURASIP JINS), 2023.

Other Activities:

- Artifact Evaluation, IEEE/ACM International Symposium on Microarchitecture (MICRO), 2022.
- Student Volunteer, IEEE International Symposium on Secure and Private Exe. Env. Design (SEED), 2024.

Research Projects

Contention-based Covert and Side Channel Attacks on Multi-GPU Systems

- Demonstrated contention-based covert and side channels attack on NVIDIA GPU's NVLink interconnect.
- The related paper is under review in **SEED 2024** [C5] (First author).

Shared State Attacks in Multi-User Augmented Reality Applications

- Demonstrated a series of innovative and robust attacks on multiple AR frameworks with shared states, focusing on three publicly accessible frameworks.
- Proposed several potential mitigation strategies that help enhance the security of multi-user AR applications.
- The related paper is under review in **Usenix Security 2024** [C4] (First author).

Accuracy-Constrained Efficiency Optimization for Detecting Drainage Crossing

- Demonstrated the efficacy of resource-aware Neural Architecture Search (NAS) in refining the hyperparameters of SPP-Net, leading to significant enhancements in inference efficiency.
- Performed comprehensive profiling of the drainage crossing detection models on GPU systems, pinpointing the performance bottlenecks unique to single GPU configurations.
- The related paper was accepted in **SC'23 Workshop** [W1] (First author).

AR/VR typing inference using head motion tracking

- Developed a system named **TyPose** that autonomously deduces words and characters typed by a user.
- Collected tens of user traces depicting AR/VR typing behavior and conducted a thorough evaluation of our attack on these traces, achieving a high level of accuracy.
- The related paper was accepted in **Usenix Security 2023** [C3].

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

- Introduced a taxonomy outlining potential targets and sources of leakage for software-based side-channel attacks on AR/VR systems.
- Demonstrated five end-to-end side-channel attacks across three distinct AR/VR-specific attack scenarios, achieving a high degree of accuracy.
- The related paper was accepted by **Usenix Security 2023** [C2] (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.
- Employed a range of classifiers including Nearest Neighbors, Gradient Boosting, Decision Tree, RandomForest, Neural Network, Naive Bayes, AdaBoost, and XGBoost to effectively recover hyper-parameters of the victim model from side-channel leakages.
- The related papers were accepted by **FPGA 2021** [P1] (First author) and **IEEE TIFS** [J1] (First author).

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 CNN models.
- The related paper was accepted by **IEEE DSN 2020** [C1] (First author).

Academic Supervision and Mentorship

Undergraduate Students

- Gabriel Haresco — UCR CSE, 2023–Current
- Clarity Shimoniak — UCR CSE, 2023–Current
- Cheng Gu — UCR CSE, 2022–Current
- Xuchang Zhan — UCI EECS, 2019-2020, Now at VISA
- Kendus Tisdale-Jeffries — Alabama A&M, 2019 Summer

Graduate Students

- Sriraksha Srirangapatna Arun — UCR CSE, 2023 Spring
- Yuxin Qiu — UCR CSE, 2022–2023
- Ziyang Men — UCR CSE, 2022–2023

Media Coverage

Side-channel attacks on AR/VR systems

- Reported by **UCR News**, **ZME Science**, **Tech Xplore**, **Analytics Insight**, **Gillett News**, **Fagen Wasanni**, **Analytics Insight**, **Game Is Hard**, **Knowridge**, **Inside**, 2023

Honors and Awards

- Student Travel Grant for DL-GPU Workshop — 2023
- International Peer Educator Training Program Certification (IPTPC) Level 1 — 2023
- UCR GSA Conference Travel Grant — 2023
- Student Travel Grant for gem5 Boot Camp — 2022
- Student Travel Grant for IEEE Symposium on Security and Privacy — 2021,2022
- Student Travel Grant for ACM Conference on Computer and Communications Security — 2021
- Student Travel Grant for USENIX Security Symposium — 2021
- Dean's Distinguished Fellowship Award (UC Riverside) — 2021
- Sichuan University Scholarship (China) — 2014–2018

Membership

IEEE Student Member, ACM Student Member.

Volunteering, Diversity & Inclusion

- **Challenge Course Judge** at Inland Empire Regional Seaperch Competition — 2024
- **Volunteer** at ACM ASPLOS 2024 — 2024
- **Volunteer** at IEEE International Symposium on Secure and Private Execution Environment Design (SEED) — 2024
- **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