

YICHENG ZHANG

+1-949-231-2128 yzhan846@ucr.edu [/Linkedin](#) [/Github](#) [/Personal Page](#)

EDUCATION

Ph.D candidate in Electrical Engineering | UC Riverside 09/2021 - 12/2025 (Expected)
M.S. in Computer Engineering | UC Irvine 09/2018 - 06/2021
B.S. in Electrical Engineering and Automation | Sichuan University 09/2014 - 06/2018

WORK EXPERIENCE

Associate Instructor | University of California, Riverside 06/2024 - 09/2024
Lecturing for upper-division undergraduate class CS 153 - Design of Operating Systems
Research Intern | Pacific Northwest National Laboratory 06/2023 - 09/2023
Research on micro-architecture security in multi-GPU systems (NVLink)

RESEARCH AREA

Hardware Security; GPU Security; Android & Linux File System; Multi-GPU System; AR/VR System; Machine Learning; Rowhammer Attack; Side Channel Attacks

*** 9 peer-reviewed papers (6 papers as the 1st author), 3 papers in submission, 5 talks, 1 poster, 4 media coverages, 10 mentored students (Major publications: USENIX Security (4), SC, DSN, SEED, FPGA, TIFS, ISMAR)

TECHNICAL SKILLS

Programming Languages & Software: C++, Python, Linux perf, NVIDIA Nsight, CUDA, TensorFlow, MATLAB, PyTorch, Verilog, Xilinx Vivado, C#, Unity, Unreal Engine, gem5, Blender, Adobe CS

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)

SELECTED PROJECTS ([GOOGLE SCHOLAR](#))

Research Assistant | [University of California, Riverside, Riverside, CA](#) 09/2021 - present

****Acoustic Injection Attacks Targeting IMU Sensors in AR/VR Systems* ([Under review in Usenix Security'25](#))

- Revealed the vulnerability of accelerometers and gyroscopes to resonant frequencies, allowing attackers to manipulate IMU outputs and mislead AR/VR user experiences.
- Demonstrated acoustic injection attacks that target IMU sensors in AR/VR headsets (Hololens2 and Quest 3), significantly impacting SLAM performance and device accuracy.

****Attacking Android & Linux File System via System Call Syncfs* ([Preprint, advanced to 2nd round in Oakland'25](#))

- Reverse-engineered Android and Linux's system call *syncfs* and identified how it leaks victim's I/O operations.
- Conducted fingerprinting attacks that classify websites, videos, and apps accessed by the victim, achieving high accuracy in both closed and open-world scenarios on Linux and Android.

****Attacking NVIDIA GPUs (GDDR6 and LPDDR5) using RFM Rowhammer Mitigation* ([Accepted to Usenix Security'25](#))

- Reverse-engineered the RFM operation and identified opportunities for timing leakage.
- Demonstrated a series of RFM-based covert channel and side-channel attacks on NVIDIA GPUs and SoCs.

****Shared State Attacks in Multi-User Augmented Reality Applications* ([Usenix Security'24](#), [SafeAR'24](#))

- Demonstrated a series of innovative and robust attacks on multiple AR frameworks with shared states, focusing on three publicly frameworks (Mapillary, ARCore and Geospatial API) from Meta and Google.
- Proposed several potential mitigation strategies that help enhance the security of multi-user AR applications.

****AR/VR Typing Inference using Head Motion Tracking* ([Usenix Security'23](#))

- Developed a system named **TyPose** on XR headsets (Quest 2 and Hololens 2) that autonomously deduces words and characters typed by users from their head motion sensor data.
- 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.
- Received media coverage from [UCR News](#) and [ZME Science](#).

***Side-Channel Attacks on AR/VR Systems via Rendering Performance Counters ([Usenix Security'23](#))

- 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.
- Received media coverage from [UCR News](#), [Tech Xplore](#) and [Analytics Insight](#).

Research Intern | [Pacific Northwest National Laboratory, Richland, WA](#)

06/2023 - 09/2023

***Covert and Side-Channel Attacks on NVIDIA's NVLink ([SEED'24](#), under review in [ISCA'25](#))

- Reverse-engineered timing and performance counters of NVIDIA Multi-GPU's NVLink interconnect.
- Performed covert and side-channel attacks on the NVIDIA DGX system and Google Compute Platform.

Accuracy-Constrained Efficiency Optimization for Detecting Drainage Crossing ([SC Workshop'23](#))

- 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.

Research Assistant | [University of California, Irvine, Irvine, CA](#)

08/2018 - 06/2021

***Remote Side-Channel Attack on FPGA to Steal Neural Network Structure ([IEEE TIFS'21](#), [FPGA'21](#))

- Developed a novel ring oscillator (RO)-based remote power attack on FPGAs to steal machine learning models.
- Employed a range of classifiers to effectively recover the hyperparameters of the victim model from side-channel leakages.

***DNN Model Stealing Attack via GPU Context-Switching Side-Channel ([DSN'20](#))

- Developed a novel GPU side-channel based on context-switching penalties.
- Implemented LSTM-based inference models to identify the structural secrets of a group of CNN models.

MEDIA COVERAGE

Side channel attacks on AR/VR headset via rendering performance counters

- Reported by [UCR News](#), [ZME Science](#), [Tech Xplore](#), [Analytics Insight](#), [Gillett News](#), 2023

AR/VR keylogging from user head motions

- Reported by [UCR News](#), [Fagen Wasanni](#), [Analytics Insight](#), [Game Is Hard](#), [Knowridge](#), [Inside](#), 2023

PRESENTATIONS AND TALKS

- "Beyond the Bridge: Contention-Based Covert and Side Channel Attacks on Multi-GPU Interconnect" at IEEE SEED'24
- "Accuracy-Constrained Efficiency Optimization and GPU Profiling of CNN Inference for Detecting Drainage Crossing Locations" at SC'23 Workshop
- "It's all in your head(set): side-channel attacks on augmented reality systems" at USENIX Security'23
- "Poster: Stealing Neural Network Structure through Remote FPGA Side-channel Analysis" at FPGA'21
- "Leaky DNN: Stealing Deep-Learning Model Secret with GPU Context-Switching Side-Channel" at DSN'20

TEACHING EXPERIENCE

Associate Instructor at University of California, Riverside

- Design of Operating Systems (CS 153) – [Syllabus](#)

Summer 2024

Teaching Assistant at University of California, Irvine

- Five undergraduate courses

Winter 2019 - Spring 2021

HONORS AND AWARDS

- International Peer Educator Training Program Certification (IPTPC) Level 1 2023
- 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