YICHENG ZHANG

yzhan846@ucr.edu /Linkedin /Github /Personal Page

EDUCATION

Ph.D in Electrical Engineering | University of California, Riverside 09/2021 - present
M.S. in Computer Engineering | University of California, Irvine 09/2018 - 06/2021
B.S. in Electrical Engineering and Automation | Sichuan University 09/2014 - 06/2018

WORK EXPERIENCE

Research Intern | Pacific Northwest National Laboratory 06/2023 - 09/2023
Research on micro-architecture security in multi-GPU systems

RESEARCH AREA

Hardware security; AR/VR Security; Side-channel Attacks; Machine Learning; Computer Architecture

TECHNICAL SKILLS

Programming Languages & Softwares: C++, Python, CUDA, TensorFlow, MATLAB, PyTorch, Verilog, Xilinx Vivado, Unity, Unreal Engine

SELECTED PROJECTSS (FULL PUBLICATION LIST)

Research Intern | Pacific Northwest National Laboratory, Richland, WA 06/2023 - 09/2023
Contention-based Covert and Side Channel Attacks on Multi-GPU Systems *(SEEE'24)*

- Identified a novel contention-based leakages vector on 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, Riverside, Riverside, CA 09/2021 - present
Shared State Attacks in Multi-User Augmented Reality Applications *(preprint)*

- Demonstrated a series of innovative and robust attacks on multiple AR frameworks with shared states, focusing on three publicly accessible frameworks 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** 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.

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.

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 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.

Model Stealing Attacks via GPU Context-Switching Side-Channel *(DSN'20)*

- 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.