Zixuan Wang
Ph.D. Candidate
University of California, San Diego

www.thenetadmin.net
zxwang@ucsd.edu
725-600-1695

EDUCATION

University of California, San Diego — San Diego, CA, US
Ph.D. candidate in Computer Science. — *Sep. 2018 – Present*

Zhejiang University — Hangzhou, China
BS in Computer Science. — *Sep. 2014 – July. 2018*

EXPERIENCE

Graduate Research Assistant, STABLE Lab — UC San Diego
Advisor: Jishen Zhao, Steven Swanson — *Sep. 2018 – Present*

Software Engineering Intern — Confidential VM, Google Cloud
Enhanced cloud user data confidentiality with emerging AMD SEV-SNP SVSM. — *Jun. 2023 – Sep. 2023*

Part-Time Student Researcher — Network Infra, Meta
Deployed the confidential VM platform at scale. — *Sep. 2022 – Jan. 2023*

Software Engineering Intern — Network Infra, Meta
Initiated and developed Meta's first confidential VM platform. — *Jun. 2022 – Sep. 2022*

Software Engineering Intern — Confidential VM, Google Cloud
Modernizing Linux KVM testing with UEFI and AMD SEV confidential VM supports. — *Jun. 2021 – Sep. 2021*

Research Intern, SOLAB — SK Hynix USA
Mentors: Joonseop Sim, Euicheol Lim — *Jun. 2019 – Sep. 2019*

Undergraduate Research Assistant, Computer Architecture Lab — Zhejiang University
Advisors: Qingsong Shi, Wenzhi Chen — *Sep. 2015 – Jun. 2018*

PUBLICATIONS

[1] **CXLeak: Architectural Attacks via Practical CXL Systems**
Zixuan Wang, Milad Esrafilian, Daniel Moghimi, Jishen Zhao, Mohammadkazem Taram — *Work in progress*

[2] **Fork is All You Needed in the Era of Heterogeneous Computing**
Zixuan Wang, Jishen Zhao — *Work in progress*

[3] **NVLeak: Off-Chip Side-Channel Attacks via Non-Volatile Memory Systems**
Zixuan Wang, Mohammadkazem Taram, Daniel Moghimi, Steven Swanson, Dean Tullsen, Jishen Zhao — *USENIX Security, 2023*

[4] **Enabling Efficient Large-Scale Deep Learning Training with Cache Coherent Disaggregated Memory Systems**
Zixuan Wang, Joonseop Sim, Euicheol Lim, Jishen Zhao — *HPCA, 2022*

[5] **Characterizing and Modeling Non-Volatile Memory Systems**
Zixuan Wang, Xiao Liu, Jian Yang, Theodore Michailidis, Steven Swanson, Jishen Zhao — *IEEE Micro Top Picks, 2021*

[6] **Ayudante: A Deep Reinforcement Learning Approach to Assist Persistent Memory Programming**
Hanxian Huang, Zixuan Wang, Juno Kim, Steven Swanson, Jishen Zhao — *USENIX ATC, 2021*

[7] **Characterizing and Modeling Non-Volatile Memory Systems**
Zixuan Wang, Xiao Liu, Jian Yang, Theodore Michailidis, Steven Swanson, Jishen Zhao — *MICRO, 2020*

[8] **Characterizing WebAssembly Performance in the Era of Serverless Computing**
Jamshed Ashurov, Zixuan Wang, Jishen Zhao — *ISSTA SRC, 2023*

[9] **COLA: Characterizing and Optimizing the Tail Latency for Safe Level-4 Autonomous Vehicle Systems**
Haolan Liu, Zixuan Wang, Jishen Zhao — *ArXiV, 2023*

[10] **Enabling Fast Recovery for Autonomous Vehicle Systems with Linux Container Checkpointing**
Maximilian Apodaca, Shengye Wang, Zixuan Wang, Jishen Zhao — *SOSP SRC, 2021*

[11] **Basic Performance Measurements of the Intel Optane DC Persistent Memory Module**
Joseph Izraelevitz, Jian Yang, Lu Zhang, Juno Kim, Xiao Liu, Amirsaman Memaripour, Yun Joon Soh, Zixuan Wang, Yi Xu, Subramanya R. Dulloor, Jishen Zhao, Steven Swanson — *ArXiv, 2019*

[12] **Reliable and Flexible Large Scale Memory Network**
Zixuan Wang, Xiao Liu, Jongryool Kim, Hokyoon Lee, Jishen Zhao — *NVMW, 2019*

PROJECTS

Trusted Execution of Hypervisor Code within Guest Virtual Machine *June, 2023*

Initiated the AMD SEV-SNP SVSM support to enhance Google Cloud's confidential virtual machines.

- I built the initial SVSM support in Google Cloud's Linux kernel, hypervisor, guest firmware, and guest kernel.

Confidential Virtual Machine Platform *June, 2022*

Initiated and developed the first confidential VM platform at Meta, highlighted at Meta's Annual Security Summit.

- I built and deployed the software and operating system support for the first CVM platform at Meta.
- The project is highlighted at Meta's Annual Security Summit.

Modernizing Linux KVM Testing Infrastructure with Confidential VM *June, 2021*

Implement the first UEFI and AMD SEV/SEV-ES support in KVM-Unit-Tests, patches merged to upstream Linux KVM.

- It serves as a solid foundation for the future development of trusted execution in KVM.
- 19 patches have been merged in upstream Linux KVM, now used by all cloud companies.

Generic Programming Model in Heterogeneous Systems *In Progress*

Designing a new language runtime that programs multi-accelerator system using multi-threading model.

- Leveraging WebAssembly System Interface (WASI) threads to program multi-accelerator systems.
- Abstract accelerator operations as WASI threads.
- High-level program (C/C++/Rust) written in conventional multi-threading model and compies to WASI.
- High-level program does not need to call accelerator-specific APIs or library functions.
- WASI just-in-time compiles thread code to underlying accelerator's architecture.

Reverse Engineering and Attacking Main Memory Systems. *June, 2023*

Side-channel attacks in non-volatile main memory systems. Accepted by USENIX Security 2023.

- Reverse engineering the micro-architecture of non-volatile main memory.
- Side-channel attacks that leaks sensative information (database tables, private encryption keys).

Accelerating Distributed Training of Large Language Models. *Oct, 2021*

Memory-centric distributed ML training. Accepted by HPCA 2022.

- Accelerate distributed ML training with emerging cache-coherent interconnection.
- GPU direct access to memory devices over serial buses.

Profiling and Modeling Non-Volatile Memory. *July, 2020*

Reverse engineering and simulating non-volatile main memory. Accepted by MICRO 2020 and IEEE Micro TopPicks 2021.

- Develop LENS, a reverse engineering framework for main memory.
- LENS is a Linux kernel module written in C and x86 assembly.
- Reverse engineer the first NVRAM product, Intel Optane Persistent Memory.
- Develop a cycle-accurate performance model for NVRAM, written in C++ 17.
- github.com/TheNetAdmin/LENS-VANS

QEMU micro:bit *May, 2018*

A micro:bit emulator based on QEMU.

- Outstanding graduation thesis of the computer science department, 2018 Zhejiang University
- Emulator of an Arduino-like board.
- Implemented ARM Cortex-M0, virtual memory, interrupts, exceptions and peripherals.
- Capable of running unmodified ARM-Mbed OS and micro:bit Bootloader.
- github.com/TheNetAdmin/qemu-microbit

ZJUNIX Operating System *Apr, 2017*

Self-designed OS running on self-designed SoC.

- Buddy and Slub memory management, multi-process, file system, device drivers, etc.
- github.com/zjunix

ZJUNIX SoC *Dec, 2016*

Self-designed SOC on FPGA

- Self-implemented MIPS32 CPU with DDR3, VGA, PS2, SD controller on FPGA.
- Capable of running ZJUNIX Operating System.
- github.com/zjunix/zjunix-soc

SKILLS

Technologies: CXL, AMD SEV/SEV-ES/SEV-SNP, Linux KVM, Linux kernel, UEFI, QEMU, WebAssembly System Interface, CUDA, TensorFlow, FPGA, MongoDB
Skills: Performance profiling, confidential virtual machine, x86 bootstrapping, Linux upstream contributions, microarchitecture reverse engineering, side/covert channel attacks, programming language runtime system
Languages: C/C++, x86/ARM Assembly, Python, Rust, Shell, R, Verilog, Java, JavaScript

INVITED TALKS

NVLeak: Off-Chip Side-Channel Attacks via Non-Volatile Memory Systems
NVMW'23, PRISM Center at Semiconductor Research Corporation

Enabling Efficient Large-Scale Deep Learning Training with Cache Coherent Disaggregated Memory Systems
Intel Co., IBM Research, SK hynix Inc., Micron Inc., Alibaba Cloud USA Inc., Foundational Microarchitecture Research (FoMR), CRISP Center at Semiconductor Research Corporation

Characterizing and Modeling Non-Volatile Memory Systems
TECHCON'20, NVMW'21, Foundational Microarchitecture Research (FoMR), CRISP Center at Semiconductor Research Corporation

Trust but Verify: Co-Locating Hypervisor Services with User Code via AMD SEV-SNP SVSM
Google Cloud'23

Securing User Data with Confidential Virtual Machine
Meta Annual Security Summit'22

Modernizing KVM-Unit-Tests with UEFI and AMD Confidential Virtual Machine
Google Cloud'21, AMD'21

HONORS & AWARDS

MICRO PhD Forum Attendee: Selected as one of the presenters on the PhD Forum, 2023 MICRO
Google Peer Bonus: Awarded one peer bonuse recognizing the impact of my project, 2023 Google
NVMW Memorable Paper Finalist: Awarded to one of the most impactful paper in persistent memory research, 2023 NVMW
Meta Security Highlight: Highlight presentation on Meta's annual security summit, 2022 Meta
Google Peer Bonus: Awarded two peer bonuses recognizing the impact of my project, 2021 Google
IEEE Micro TopPicks: Annually awarded to 12 best papers in computer architecture area, 2021 IEEE
NVMW Memorable Paper Finalist: Awarded to one of the most impactful paper in persistent memory research, 2021 NVMW
Outstanding Dissertation: Outstanding undergraduate dissertation, 2018 Zhejiang University
He-Zhi-Jun Scholarship: Top 10 outstanding students of the computer science department, 2017 Zhejiang University
Outstanding Prize: Challenge Cup, National Undergraduate Academic Science and Technology Works Competition, 2017 China
Rising Star in Academic: Top 1% of computer science students in academic achievements, 2017 Zhejiang University
Academic Scholarship: Top 10% students of the computer science department
Second Prize: Digilent Design Contest, 2017 China
Third Prize: Advanced Computer Architecture Undergraduate Innovation Competition, 2016 CCF China

OPEN SOURCE PROJECTS

MightyPC *Jul 2021*
Mighty toolkit for conference Program Chairs.
- A toolkit for conference program chairs to manage submissions, assign reviewers, and organize TPC meetings.
- Initially developed for the MICRO 2021 conference, then used in other conferences, including HPCA 2022 and MICRO 2022.
- github.com/TheNetAdmin/MightyPC

VS Code LinkerScript *Aug 2018*
The first linker script language extension on VS Code.
- github.com/TheNetAdmin/vscode-linkerscript (196K Installations)

ZJU Thesis *May 2018*
LaTeX template for Zhejiang University graduation thesis.
- Thesis template in LaTeX, widely used by students at Zhejiang University.
- github.com/TheNetAdmin/zjuthesis (2,000★ 27K Downloads)

Makefile Templates *July 2017*
Makefile templates for C/C++ projects.
- github.com/TheNetAdmin/Makefile-Templates (500★)