Haoxuan Xu

haoxxu@student.ethz.ch | github.com/TerryXhx | terryxu.site

Education

University of Southern California 01/2026 (Expected)
Ph. D in Computer Science, advised by Prof. Mengyuan Li Los Angeles, US

ETH Zürich 09/2023 – 12/2025 (Expected)
Master of Science in Computer Science (Major in Secure and Reliable Systems) Zürich, Switzerland

- GPA: 5.71/6.0
- Highlight Courses: Hardware Security (6.0/6.0), Network Security (6.0/6.0), Advanced Systems Lab (6.0/6.0), Information Security Lab (6.0/6.0), Cloud Computing Architecture (6.0/6.0), System Security (5.75/6.0)

Shanghai Jiao Tong University 09/2019 – 06/2023
B. Eng in Computer Science and Technology (IEEE Honor Class) Shanghai, China

- GPA 91.55/100, Rank 2/38
- A+ Courses: Parallel and Distributed Programming, Computer Network, Programming Languages, etc.

Research Experience

Cache Attacks on Non-Inclusive AMD 3D V-Cache 06/2025 – Now
Research Assistant, advised by Prof. Mengyuan Li, Los Angeles, US (remote)

- **First** to reverse engineer **L2 set** indexing and **L3 slice/set** indexing functions for AMD 3D V-Cache, including both linear and non-linear components on Ryzen 7800X3D and EPYC 9184x (Zen 4).
- Reverse engineered the **core topology** using timing analysis to reveal latency differences when accessing data across slices.
- Discovered and characterized **stack + slice** contention, showing that accesses targeting the same slice and stack trigger measurable interference, and leveraged this effect to build a **covert communication channel**.

Wave: Leveraging Architecture Observation for Privacy-Preserving Model Oversight 01/2025 – 08/2025
Research Assistant, advised by Prof. Mengyuan Li, Los Angeles, US (remote)

- Developed Wave, a **hardware-grounded runtime verification framework** using GPU performance counters (PMCs) to monitor LLM inference in a privacy-preserving manner.
- Designed a two-stage analysis pipeline: (i) **architectural inference** of model properties (layers, hidden dimensions, etc.) from PMC traces, and (ii) **SMT-based formal verification** to check consistency with advertised model specifications.
- Demonstrated accurate LLM fingerprinting with an average **6.8% error** in estimating model depth and structure, enabling detection of substitute or downsized models.
- Paper accepted to **ASPLOS 2026** as **co-first author**.

Rowhammer attacks on ECC DDR4 DRAM 03/2024 – 10/2024
Research Assistant, advised by Patrick Jattke, Prof. Kaveh Razavi Zürich, Switzerland

- Reversed engineered **bank functions** and **row mapping** for a Cascade Lake CPU using DRAMA, an oscilloscope and EDAC error data.
- Validated the functionality and correctness of ECC error reporting by manually injecting errors.
- Figured out the Linux kernel's **soft-offline mechanism** for faulty pages.
- Examined hammering process, including double-sided nature, mitigation techniques, synchronization, and activation rates.
- Successfully triggered corrected errors on **four** ECC DDR4 DIMMs.

Latte: Layered Attestation for Portable Enclaved Applications 03/2022 – 10/2024
Research Assistant, advised by Prof. Guoxing Chen Shanghai, China

*In this project, we propose a framework to support **portable** software on **heterogeneous** trusted execution environment (TEE) platforms with a **unified and layered** attestation flow, and present a prototype implementation with the adoption of **WebAssembly** (WASM) as the **portable language**, and **Intel SGX** and **RISC-V Penglai** as **heterogenerous TEEs**.*

- Implemented the mechanism to **derive machine-code measurements** (identity of enclaves) from **portable identity** to **support the unified attestation flow**.
- Ported WAMR to Penglai with WebAssembly System Interface (WASI) support, and added attestation-related APIs to **enable WASM programs to perform attestation**.
- Modified loader in linux-sgx-sdk and driver in Penglai-sdk to ensure the **same sequential order** of measurement calculation between derived ones and actual ones, and **validate the correctness** of the unified attestation flow.
- Paper accepted to **Euro S&P 2025** as **co-first author**.

Publication

- **Xu H***, Xiang J*, Huang Z, et al. LATTE: Layered Attestation for Portable Enclaved Applications (**EuroS&P 2025**)
- **Xu H***, Chen G*, Beijie L*, et al. WAVE: Leveraging Architecture Observation for Privacy-Preserving Model Oversight (**ASPLOS 2026**, to appear)

Projects

Hardware Security Attacks | C, C++ 09/2023 – 12/2023

- Implemented cache attacks, **breaking ASLR** via side channeling the MMU with AnC.
- Extracted sensitive data using **Meltdown** and **Spectre** vulnerabilities.
- Developed **Blacksmith**, **a Rowhammer fuzzer**, from scratch, successfully triggering bit flips on multiple DDR4 DIMMs.
- Implemented an end-to-end **privilege escalation** attack with Blacksmith by exploiting the Linux buddy allocator and recycling the exploitable page with a page table page.

Selected Awards and Honors

- Shanghai Jiao Tong University Outstanding Graduate 06/2023
- Huatai Securities Technology Scholarship (**Top 5%**) 12/2022
- Foresight and Sequoia Capital Talent Development Fund (**Top 1%**) 12/2021
- Undergraduate Honors Scholarship (**Top 5%**) 12/2020

Others

Programming Languages: C/C++, Python, Coq, Rust
Tech Skills: Git, Vim, LaTex, SGX, PyTorch, CUDA Programming, AVX, VTune
Languages: English (C1, TOEFL 107), Mandarin (Native), German (Beginner, A1.2)

Last Updated in November, 2025