ZHANG ZIHAN

Curriculum Vitae

ShenZhen, Guangdong — 12311124@mail.sustech.edu.cn — https://shentoumengxin.github.io

Education

Southern University of Science and Technology (SUSTech) Shenzhen, China
B.S. in Computer Science and Technology 2023 – present

- **GPA:** 3.62/4.0
- **Core Courses:** Computer Security(100), Algorithm Design and Analysis(96),Computer Organization(91), Advanced Programming(95), Principles of Compilers(87).

PUBLICATIONS

Manuscripts Under Review

- **Zihan Zhang**, Wenqi Lin, Lingna Sun, Hongyi Wang, Jingyi Wang, Yanshu Mei, and Fengwei Zhang*. *MirrorShield: Cross-Architecture Linux Malware Analysis via Lightweight Emulation and LLM*. Under review (double-blind), 2026.

Research Experience

COMPASS Lab, SUSTech Undergraduate Researcher
Advisor: Prof. Fengwei Zhang *May 2025 – Present*

MirrorShield: Cross-Architecture Linux Malware Analysis **Under review (double-blind)**

- **Grant:** Project Leader (Applicant), Guangdong College Students Sci-Tech Innovation Program (RMB 20,000).
- Built a lightweight multi-architecture dynamic analysis framework via containerized QEMU-user and eBPF monitoring; evaluated on **11 CPU architectures** with $< 10\times$ runtime overhead.
- Integrated an LLM-assisted pipeline for evidence-grounded reports; achieved **94.7%** accuracy (F1=0.946) and **80.7%** Evidence Match; maintained $> 90\%$ detection under $2{,}000\times$ injected log noise.

National University of Singapore Summer Workshop Participant
Computer Security – Defence against the Dark Arts *May 2025 – Jul 2025*
*(**Transcript: A+**; Instructor: Hugh Anderson)*

QemuGuardian: An Emulation-Based Malware Analysis Tool **First Prize (Best Project)**

- Browser-integrated workflow to isolate and analyze downloaded ELF executables across architectures.
- Combined QEMU-user emulation with eBPF runtime monitoring to capture syscall-level behaviors with minimal overhead.This prototype later evolved into *MirrorShield*.

Professional Experience

Sangfor Technologies Inc., Security Division Kunming, China
Cybersecurity Intern Jan 2026 – Feb 2026

- Reproduced and validated high-severity vulnerabilities (e.g., deserialization, command injection) and wrote verification reports.
- Assisted incident response using XDR for endpoint anomaly triage; supported on-site remediation and post-incident reporting.
- Performed asset fingerprinting and exposure assessment using OSINT/scanning to identify weak credentials and unauthorized access risks.

Selected Projects

MCM/ICM 2025: Olympic Medal Prediction Modeling **Meritorious Winner (Team Lead)**

- Built a hybrid forecasting pipeline combining Random Forest and K-Means clustering; used Elbow Rule and Grid Search to mitigate small-sample imbalance and overfitting.
- Engineered interpretable features and performed feature-importance analysis to improve explainability.
- Conducted global sensitivity analysis and OAT tests; achieved ROC-AUC of **0.89** under feature perturbations.

Honors & Awards

- China Information Security Competition (**CTF competition**): Guangdong Provincial Rank #66 (Semifinalist) 2026.
- SUSTech Outstanding Student, twice.
- SUSTech Scholarship (Second Class); SUSTech Scholarship (Third Class).
- Blue Bridge Cup National Software (Lanqiao Cup), C/C++ Algorithm Track: Guangdong Provincial Third Prize.
- National Information Security Professional Certification (NISP), **Level 2**.
- University dance team member, Achievements include two National Special Prize (Top Award), one Provincial Champion, and three City Champion.