ZHAOXUAN (ISAAC) JIN

811 Emerson St, Evanston, IL, 60201

📞 (608) 949-0667 ✉ zhaoxuanjin2025@u.northwestern.edu 💼 linkedin.com/in/zhaoxuan-jin 🐙 github.com/WHALEEYE

Education

Northwestern University	**Sep. 2023 – Dec. 2024**
Master of Science in Computer Science	*Evanston, Illinois*
Southern University of Science and Technology	**Sep. 2019 – Jun. 2023**
Bachelor of Engineering in Computer Science and Technology	*Shenzhen, Guangdong, China*

Relevant Coursework

- DFIR[1] - A
- Computer Security - A
- Internet Security - A
- Operating Systems - A
- CAT[2] - A
- Compilers - A
- Computer Networks - A
- Machine Learning - A

Internship Experience

Eigent AI — **Jun. 2024 – Present**
AI Developer — *United States*

- One of the core maintainers of CAMEL open-source project (5.3K stars on GitHub).
- Responsible for the docker solutions of the project, maintaining the ghcr registry and the CI/CD pipeline.
- Work on solutions that make multiple LLM agents collaborate to solve tasks.
- Gained expertise in developing LLM agents with comprehensive functionalities based on different backend models, and deploying applications with docker and CI/CD pipelines.

Hangzhou MagicShield Information Technology Co., Ltd — **Jun. 2022 – Aug. 2022**
Cloud Security Research Intern — *Hangzhou, Zhejiang, China*

- The company specialized in providing Kubernetes in-cluster security solutions for enterprises.
- Collaborated with company engineers and Zhejiang University PhD students on researching automating network policy generation for cloud-native applications.
- Solely developed MicroShield, an eBPF-based system that auto-generates policies from in-cluster east-west traffic, with Python and GoLang. This system is now integrated as a submodule in the company's product.
- Gained proficiency in Kubernetes, Docker, cloud-native architecture, and eBPF applications.

Projects

DFIR Simulation for Credential Leaks | *Windows, Linux, DFIR* — **May. 2024**

- Simulated a digital forensics and incident response (DFIR) process for a credential leak incident involving a hotel chain.
- Developed hypotheses on the attack chain based on the network topology and created detailed investigation plans.
- Performed malware analysis, memory forensics, and log analysis to construct a timeline of the incident, identify the attack vector, trace the malicious IP address, and assess the extent of data exfiltration.
- Compiled a comprehensive report detailing the attack chain, attack vector, timeline, indicators of compromise, and recommended remediation steps.
- Gained hands-on experience in DFIR, enhancing expertise in real-world incident response processes and approaches.

Multi-Layer Compiler | *C++* — **Jan. 2024**

- Individually developed a multi-layer compiler with modern compiler techniques and architecture.
- This compiler mainly focuses on the front-end and back-end of a modern compiler, including converting source code to intermediate representation (IR) and generating assembly code layer by layer.
- Applied techniques like reaching definition analysis, liveness analysis, graph coloring register allocation, etc.
- Applied simple optimizations like dead code elimination, got the 5th place at the final competition of the course.

LLVM Middle End | *LLVM, C++* — **Dec. 2023**

- LLVM is a compiler infrastructure that provides a collection of reusable compiler and toolchain components.
- developed a middle-end pass for LLVM, which focused on optimizing the intermediate representation (IR) of LLVM.
- Applied techniques like constant folding, dead code elimination, and loop unrolling to optimize the IR.

Technical Skills

Languages: Java, C/C++, Python, Rust, JavaScript, HTML, TypeScript
Technologies/Tools: Linux, Windows, PostgreSQL, FTK Imager, Volatility, RegRipper, GDB, Markdown, React.js

---

[1]Digital Forensics and Incident Response
[2]Code Analysis and Transformation