Ziyu Lin

linziyu0205@gmail.com • GitHub • https://www.linziyu.me

Education

Singapore Management University, Singapore, Singapore 05/2024 – 05/2025(expected)

Visiting Master Student supervised by Prof. Robert Deng and Prof. Daoyuan Wu

Fuzhou University, Fuzhou, China 09/2022 – 06/2025(expected)

Master in Computer Science supervised by Prof. Ximeng Liu

Fujian Agriculture and Forestry University, Fuzhou, China 09/2018 – 06/2022

B.S. in Statistics

Publications

- **Ziyu Lin**, Zhiwei Lin, Ximeng Liu, Jianjun Chen, Run Guo, Cheng Chen, Shaodong Xiao, "CDN Cannon: Exploiting CDN Back-to-Origin Strategies for Amplification Attack," in **Usenix Security'24**
- **Ziyu Lin**, Zhiwei Lin, Ximeng Liu, Zuobin Ying, Cheng Chen, "Unveiling the Bandwidth Nightmare: CDN Compression Format Conversion Attacks," in **BDPC'24 (Best Paper)**
- **Ziyu Lin**, Zhiwei Lin, Run Guo, Jianjun Chen, Mingming Zhang, Ximeng Liu, Tianhao Yang, Zhuoran Cao, Robert H Deng, "Detecting and Measuring Security Implications of Entangled Domain Verification in CDN" **NDSS'24 (Under Review)**

Experience

Singapore Management University Singapore, Singapore

Research Assistant (supervised by Prof. Robert Dengand Prof. Daoyuan Wu) 05/2024 – present

- DexScope: Fast Search of Android Bytecode Methods for LLM-Empowered Code Intention Analysis (inprogress)

Network and Information Security Lab (NISL), Tsinghua University Beijing, China

Research Assistant (supervised by Prof. Jianjun Chen) 01/2023 – present

- Implemented a tool *CDNFinder* to detect CDN for given domains with python.
- Present a new class of HTTP amplification attacks exploiting CDN Back-to-Origin Strategies, with a max amplification factor of up to 104862. These vulnerabilities have received acknowledgments from well-known CDN vendors such as Azure, Alibaba, G-core, Cachefly, Qiniu, and Upyun.
- Find a new class of CDN Domain Ownership Verification vulnerabilities, which allow attackers to take over the domain and implement a tool, DAHunter, to detect vulnerabilities.
- Present a new class of Denial of Service attacks exploiting HTTP/3 protocol vulnerabilities.

HUST and Ant Group Hangzhou, China

Research Intern (supervised by Prof. Weijie Liu and Prof. Zhi Li) 03/2022 – 12/2022

- Implemented PoC for 50 CVEs related to Docker and Kubernetes.
- Implemented an LSTM-based anomaly detection system for detecting malicious dockerfile.
- Implemented an image classification model that runs in a Trusted Execution Environment (Occlum).

Research Interests

My research interests focus on network security, protocol security, web security, and LLM for Security. I'm particularly interested in discovering and mitigating new security vulnerabilities in widely-used Internet protocols and systems, such as HTTP protocol, and CDN system.

Selected Awards

- 2nd Prize Scholarship (Fuzhou University) 2024
- Best Paper Award, 2024 2nd International Conference on Big Data and Privacy Computing 2024
- Bug Bounty Award ($200), Discovery of Alibaba CDN vulnerabilities 2023
- 3rd Place of TEE Track in 2022 World Privacy-Preserving Computing Competition (WPPCC) 2022
- 2nd Prize Scholarship (Fuzhou University) 2022
- 2nd Prize Scholarship (Fujian Agriculture and Forestry University) 2020
- 1st Place of China Undergraduate Mathematical Contest in Modeling (CUMCM), Fujian Province 2020
- 3rd Prize Scholarship (Fujian Agriculture and Forestry University) 2019