Lingzhi Wang

lexuswang.github.io linkedin.com/in/lingzhi-wang-lexus lingzhiwang2025@u.northwestern.edu

Education

Northwestern University — Evanston, United States
Ph.D Computer Science(Advisor: Prof. Yan Chen) — *May 2021-present*

Tsinghua University — Beijing, China
B.E Electronic Information Science and Technology — *Aug 2016-June 2020*
B.Ec Economics (double major) — *May 2017-June 2020*

Coursework

Courses: Object-Oriented Programming, Data Structures & Algorithms, Embedded Systems, Discrete Math, Linear Algebra, Calculus, Physics, Probability & Statistics, Machine Learning, Artificial Intelligence
Awards: Comprehensive Scholar with Distinction

Research Interest

My research is centered around system security and cyberattacks, with a focus on developing and optimizing Endpoint Detection and Response (EDR) systems and Host Intrusion Detection Systems (HIDS) systems to detect and defend against Advanced Persistent Threats (APT). My research involves behavior analysis of software, AI security, and the development of the Knowledge Base to enhance our understanding of cyberattack techniques to improve system security and protect against evolving threats in the digital space.

Publications

1. Shen, X., Li, Z., Burleigh, G., **Wang, L.**, Chen, Y. "Decoding the MITRE Engenuity ATT&CK Enterprise Evaluation: An Analysis of EDR Performance in Real-World Environments". In Proceedings of the 19th ACM Asia Conference on Computer and Communications Security (AsiaCCS'24). [paper][code]

2. **Wang, L.**, Zhao, N., Chen, J., Li, P., Zhang, W., Sui, K. "Root-cause metric location for microservice systems via log anomaly detection." 2020 IEEE international conference on web services (ICWS'20). IEEE, 2020. [paper]

Working Papers

1. **Wang, L.**, Shen, X., Li, W., Li, Z., Sekar, R., Liu, H., & Chen, Y. "Incorporating Gradients to Rules: Towards Lightweight, Adaptive Provenance-based Intrusion Detection" [arxiv][code]

2. **Wang, L.**, Wang, J., Jung, K., Thiagarajan, K., Wei, E., Shen, X., Chen, Y., & Li, Z. "From Sands to Mansions: Enabling Automatic Full-Life-Cycle Cyberattack Construction with LLM" [arxiv]

3. Li, Z., Wei, Y., Shen, X., **Wang, L.**, Chen, Y., Xu, H., ... & Zhang, F. "Marlin: Knowledge-Driven Analysis of Provenance Graphs for Efficient and Robust Detection of Cyber Attacks" [arxiv]

Ongoing Projects

Automated Cyber Attack Construction using LLM | *Northwestern University* — Jan. 2023-Present
- Uses a large language model for in-depth understanding and automated generation of advanced cyber-attacks.
- Reduces human labor in red team emulation through a newly developed system.
- Marks the first initiative to automate cyber-attack construction using a large language model.

Intelligent System Intrusion Detection System | *Northwestern University* — Dec. 2023 – Present
- Improved existing provenance-based host intrusion detection system using transformers and graph neural network.
- Our system can reduce the overhead running the real-time detection and get a more accurate detector using less training data.

Experience

Northwestern University | *Teaching Assistant* Sept. 2021 – Present
CS450: Internet Security, CS396: Intro to the Data Science Pipeline, DE200: Foundations of Data Science, CS217: Data Management and Information Processing, CS212: Mathematical Foundation to Computer Science

Tencent | *Research Intern* May 2020 – Aug. 2020
Work on data mining using the map data from users' smartphones.

Bizseers | *Research Intern* Mar. 2019 – Jan. 2020
Proposed a novel framework of failure localization and root-cause diagnosis using system logs and key performance indicators collected from large distributed systems, such as servers and databases in banks or E-commerce companies.

Tsinghua University | *Research Assistant* Nov. 2018 – Jun. 2019
Constructed a weighted graph of app behavior based on deep learning and graphic modeling to analyze app-using data collected by a software company in Finland, including app usage data from more than 8,000 users in 7 years, with over 20 million records.

Skills

Languages: C/C++, Python, Java, SQL, Matlab LaTeX
Tools: Git/GitHub, Unix Shell, Webpack, VS Code, IntelliJ CLion/PyCharm/IDEA, Metasploit, PyTorch, TensorFlow

Services

External Reviewer: IEEE S&P 2024, IEEE S&P 2025