Lingzhi Wang

lingzhiwang.me 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 focuses on applying advanced machine learning and artificial intelligence techniques to strengthen both cyber offense and defense, as well as to optimize cloud architectures. Specifically, I explore the following questions: 1) How can cutting-edge AI methods be integrated into the development of practical security and network systems such as Security Operation Centers (SOCs), Extended Detection and Response (XDR) systems, and serverless applications (FaaS)? 2) How can we model human knowledge and reasoning processes to carry out complex offensive cybersecurity tasks such as penetration testing and red teaming? 3) With LLMs, how can we represent, learn, and apply abstract knowledge in practical cybersecurity systems, as well as other industrial areas?

Publications

1. Shen, X., **Wang, L.**, Li, Z., Chen, Y., Zhao, W., Sun, D., Wang, J., & Ruan, W. "PentestAgent: Incorporating LLM Agents to Automated Penetration Testing". To appear in Proceedings of the 20th ACM Asia Conference on Computer and Communications Security (AsiaCCS'25) [arxiv][code]

2. **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". In Proceedings of the 32nd Network and Distributed System Security Symposium 2025 (NDSS'25) [arxiv][code]

3. 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]

4. **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]

Papers Under Review

1. **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]

2. Wang, J., **Wang, L.**, Yu, H., Shen, X., & Chen, Y. "Paris: A Practical, Adaptive Trace-Fetching and Real-Time Malicious Behavior Detection System" [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 Penetration Testing using LLM | *Northwestern University* Nov. 2024 – Present

- Uses a large language model for unstructured cyberattack knowledge summarization and planning problem definition.
- Addresses the challenges of using traditional AI planning and the Planning Domain Definition Language (PDDL) in penetration testing, such as managing uncertainty, handling partial observability, etc.
- Reduces human labor and domain expertise needed in manual penetration testing.

Next-generation Provenance-based Intrusion Detection System | *Northwestern University* Dec. 2024 – Present

- Addresses challenges of generating adaptive and fine-grained rules in existing provenance-based host intrusion detection systems using generative AI.
- Reduces the overhead running the real-time detection and builds a more accurate detector using less training data.
- Incorporates new data log sources (e.g. call stack traces) to mitigate novel threats such as the fileless attack.

Talks

1. **Conference Talk**: *"Incorporating Gradients to Rules: Towards Lightweight, Adaptive Provenance-based Intrusion Detection"*
   NDSS Symposium, San Diego, CA, February 25, 2025.

Experience

SRI International (SRI) | *Research Intern* exp Jun. 2025 – Aug. 2025
Applications of machine learning in serverless computer environments, with specific emphasis on performance and graph analytics.

Northwestern University | *Teaching Assistant* Sept. 2021 – Present
CS450: Internet Security, CS396/CS326: 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

Reviewer: IEEE Security & Privacy
Artifact Committee Member: USENIX Security 2025, ACM CCS 2025
External Reviewer: NDSS 2026, IEEE S&P 2025, IEEE S&P 2024