Xiangmin Shen
Email: Xiangminshen2019@u.northwestern.edu
Website: nbshenxm.github.io

RESEARCH INTERESTS

I am broadly interested in system security and security measurement. My current research focuses on enhancing system security by applying AI techniques in defense and offense.

EDUCATION

Northwestern University, Evanston, IL
Ph.D. in Computer Science — Sept 2019 - June 2025 (anticipated)
Advisor: Yan Chen

Northwestern University, Evanston, IL
Bachelor of Science in Computer Science and Applied Mathematics — Sept 2015 - June 2019

PUBLICATION

Conference Publications

[C3] Xiangmin Shen, Lingzhi Wang, Zhenyuan Li, Yan Chen, Wencheng Zhao, Dawei Sun, Jiashui Wang
PentestAgent: Incorporating LLM Agents to Automated Penetration Testing.
In Proceedings of 20th ACM ASIA Conference on Computer and Communications Security (*AsiaCCS '25*).

[C2] Xiangmin Shen*, Lingzhi Wang*, Weijian Li, Zhenyuan Li, R.Sekar, Han Liu, Yan Chen
Incorporating Gradients to Rules: Towards Lightweight, Adaptive Provenance-based Intrusion Detection.
In Proceedings of Network and Distributed System Security Symposium 2025 (*NDSS '25*).

[C1] Xiangmin Shen, Zhenyuan Li, Graham Burleigh, Lingzhi Wang, and Yan Chen
Decoding the MITRE Engenuity ATT&CK Enterprise Evaluation: An Analysis of EDR Performance in Real-World Environments.
In Proceedings of 19th ACM ASIA Conference on Computer and Communications Security (*AsiaCCS '24*).

Refereed Poster

[P1] Xiangmin Shen, Wenyuan Cheng, Yan Chen, Zhenyuan Li, Wencheng Zhao, Dawei Sun
Poster: LLM-Driven Automated Exploit Assessment for Penetration Testing
In Network and Distributed System Security Symposium 2025 (*NDSS '25*).

Working Papers

[W5] Xiangmin Shen, Wenyuan Cheng, Wencheng Zhao, Dawei Sun, Yan Chen, Jiashui Wang, Lingzhi Wang, Zhenyuan Li
EEAS: An Automatic and Explainable Vulnerability Assessment System.
Under submission.

[W4] Zhenyuan Li, **Xiangmin Shen**, Yangyang Wei, Lingzhi Wang, Zhengkai Wang, Yan Chen, Shouling Ji
Efficient and Robust Cyber Attack Detection via Streaming Provenance Graph Alignment
Under submission.

[W3] Zhenyuan Li, Yangyang Wei, **Xiangmin Shen**, Lingzhi Wang, Yan Chen, Haitao Xu, Shouling Ji, Fan Zhang

TAGS: Real-time Intrusion Detection with Tag-Propagation-based Provenance Graph Alignment on Streaming Events.
Under submission.

[W2] Lingzhi Wang, Zhenyuan Li, Yi Jiang, Zhengkai Wang, **Xiangmin Shen**, Wei Ruan, Yan Chen
From Sands to Mansions: Enabling Automatic Full-Life-Cycle Cyberattack Construction with LLM.
Under submission.

[W1] Jian Wang, Lingzhi Wang, Husheng Yu, **Xiangmin Shen**, Yan Chen
PARIS: A Practical, Adaptive Trace-Fetching and Real-Time Malicious Behavior Detection System.
Under submission.

AWARDS AND GRANTS

NDSS Symposium Student Fellowship, 2025
Northwestern Conference Travel Grant, 2023
Northwestern Undergraduate Research Summer Grant, 2017
Northwestern Undergraduate Research Academic Year Grant, 2017

TEACHING AND MENTORSHIP EXPERIENCE

Research Mentor

- Graham Burleigh (Undergraduate @ Northwestern University): paper co-author [C1], awarded Northwestern Undergraduate Research Summer Grant, 2021
- Wenyuan Cheng (PhD student @ Zhejiang University): paper co-author [W5] and [P1]
- Shiyu Tan (Master student @ Zhejiang University): paper co-author

Teaching Assistant

- CS 450: Internet Security (2020 Winter, 2021 Winter, 2023 Winter, 2024 Winter, 2025 Winter)
- CS 355: Digital Forensics and Incident Response (2025 Spring)
- CS 354: Computer System Security (2021 Winter, 2023 Winter, 2024 Winter, 2025 Winter)
- CS 213: Intro to Computer Systems (2024 Spring)
- CS 212: Mathematical Foundations of Computer Science (2021 Spring)
- CS 211: Fundamentals of Computer Programming II (2021 Fall, 2022 Winter, 2022 Spring, 2022 Fall, 2023 Spring, 2023 Fall)
- CS 111: Fundamentals of Computer Programming I (2020 Fall, 2024 Fall)

SERVICE

Program Committee Member

- USENIX Security 2025 Artifact Evaluation
- ACM CCS 2025 Artifact Evaluation

Reviewer

- Computer Networks
- ICLR 2025 Workshop XAI4Science
- International Conference on Electrical, Computer and Energy Technologies 2025
- IEEE Internet of Things Journal, 2024

Shadow Reviewer

- Network and Distributed System Security Symposium 2026
- IEEE Symposium on Security and Privacy (Oakland) 2024, 2025
- ACM AsiaCCS 2022