Xiangmin Shen
Email: Xiangmin.Shen@hofstra.edu
Website: shensecurity.com

RESEARCH INTERESTS

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

PROFESSIONAL EXPERIENCE

Hofstra University, Hempstead, NY

Tenure-Track Assistant Professor, Department of Computer Science Sept 2025 – present

EDUCATION

Northwestern University, Evanston, IL

Ph.D. in Computer Science Sept 2019 - Sept 2025

Thesis: *Beyond Evaluation: Towards Automated and Explainable Red Teaming*

Advisor: Yan Chen. Thesis Committee: Xinyu Xing, Han Liu, Zhenkai Liang

Northwestern University, Evanston, IL

M.S. in Computer Science Sept 2019 - June 2025

Northwestern University, Evanston, IL

B.S. in Computer Science and Applied Mathematics Sept 2015 - June 2019

PUBLICATION

Conference Publications

[C6] Qizhi Cai, Lingzhi Wang, Yao Zhu, Zhipeng Chen, **Xiangmin Shen**, Zhenyuan Li
Building Next-Generation Datasets for Provenance-Based Intrusion Detection
In Proceedings of Workshop on Attack Provenance, Reasoning, and Investigation for Security in the Monitored Environment (PRISM) 2026

[C5] Jiahui Wang, **Xiangmin Shen**, Zhengkai Wang, Zhenyuan Li
The Case for LLM-Enhanced Backward Tracking
In Proceedings of Workshop on Attack Provenance, Reasoning, and Investigation for Security in the Monitored Environment (PRISM) 2026

[C4] 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.
In Proceedings of 24th International Conference on Applied Cryptography and Network Security (*ACNS ‘26*).

[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] Lingzhi Wang*, **Xiangmin Shen***, 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*).

Journal Publications

[J1] Zhenyuan Li, Lingzhi Wang, Zhengkai Wang, **Xiangmin Shen**, Haitao Xu, Yan Chen, Shouling Ji
Incorporating Gradients to Rules: towards Online, Adaptive Provenance-based Intrusion Detection.
IEEE Transactions on Dependable and Secure Computing (2025).

Refereed Poster

[P3] Yangyang Wei, **Xiangmin Shen**, Yijie Xu, Zhenyuan Li
Poster: Abstracting and Tracking Semantic Flow among Agents for Threat Detection
In Network and Distributed System Security Symposium 2026 (*NDSS '26*).

[P2] Mingxiang Shi, **Xiangmin Shen**, Yuqiao Gu, Zhipeng Chen, Lingzhi Wang, Yi Jiang, Zhenyuan Li
Poster: Reconstructing the Provenance of Android
In Network and Distributed System Security Symposium 2026 (*NDSS '26*).

[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

[W2] Lingzhi Wang, Xinyi Shi, Ziyu Li, Yi Jiang, Shiyu Tan, Yuhao Jiang, Junjie Cheng, Wenyuan Cheng, **Xiangmin Shen**, Zhenyuan Li, Yan Chen
When Agents Need a Plan: Advancing Automated Penetration Testing through Code Assistant Systems and Classical Planning.
Under submission.

[W1] Xiangmin Shen, Wenyuan Cheng, Yan Chen, Zhenyuan Li, Yuqiao Gu, Lingzhi Wang, Wencheng Zhao, Dawei Sun, Jiashui Wang
AEAS: Actionable Exploit Assessment System.
Under submission.

AWARDS AND GRANTS

Hofstra Interdisciplinary Undergraduate Research Community Grant, Spring 2026 (*$4,000*)
NDSS Symposium Student Fellowship, 2025
Northwestern Conference Travel Grant, 2023
Northwestern Undergraduate Research Summer Grant, 2017
Northwestern Undergraduate Research Academic Year Grant, 2017

INVITED & CONFERENCE TALKS

"THE BEAUTY OF TRUST: BUILDING INTELLIGENT AND SECURE SYSTEMS"
Hofstra's fifth annual Presidential Symposium, Hofstra University, Hempstead, NY, September 2025

TEACHING AND MENTORSHIP EXPERIENCE

Research Mentorship @ Hofstra

- Joseph Falco (Undergraduate @ Hofstra University)

Teaching @ Hofstra

- CSC 015: Fundamentals of Computer Science I: Problem Solving and Program Design (2025 Fall, 2026 Spring)
- CSC 017: Fundamentals of Computer Science III: Advanced Data Structures and Object-Oriented Programming (2025 Fall, 2026 Spring)

Research Mentorship @ Northwestern

- 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 [W3], [W2] and [P1]
- Shiyu Tan (Master student @ Zhejiang University): paper co-author [W3]

Teaching Assistant @ Northwestern

- 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

- NDSS 2026 Workshop PRISM
- USENIX Security 2025 Artifact Evaluation
- ACM CCS 2025 Artifact Evaluation
- NDSS 2026 Artifact Evaluation

Reviewer

- IEEE Transactions on Dependable and Secure Computing, 2026
- Computer Networks Journal, 2025
- NeurIPS 2025 Workshop BERT2S
- 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