Xiangmin Shen
Xiangminshen2019@u.northwestern.edu
(224) 714 - 9896

EDUCATION

Northwestern University, Evanston, IL
Ph.D. in Computer Science — June 2025 (anticipated)

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

PUBLICATION

Shen, Xiangmin, et al. "Decoding the MITRE Engenuity ATT&CK Enterprise Evaluation: An Analysis of EDR Performance in Real-World Environments." To appear in **AsiaCCS 2024**.

PROJECTS

Automated Pentesting Agent — Jan. 2024 – present

- Develop an automated penetration testing agent leveraging GPT and RAG techniques.

Intrusion Detection with Streaming Provenance Graph Alignment — Sept. 2023 – present

- Developed a lightweight tag-based streaming provenance graph alignment system.
- Demonstrated high throughput while maintaining detection accuracy.

Adaptive Configuration Learning in PIDS — Sept. 2021 – present

- Developed a tag-based PIDS capable of automatically adapting to diverse environments.
- Reduce false alarms by over 90% (11.49x) on average compared with the baseline without hurting the detection capability.

MITRE ATT&CK Evaluation Analysis — July 2021 – Dec. 2023

- Designed a whole-graph analysis method, which utilizes additional control flow and data flow information to measure the performance of EDR systems.
- Analyzed MITRE evaluation's results over multiple years from various aspects, including detection coverage, detection confidence, detection modifier, data source, compatibility, etc.

Provenance-based Intrusion Detection System — June 2018 – Sept. 2021

- Developed a real-time provenance-based APT detection system that detected all attacks with low false positive alarm volume in DARPA Transparent Computing Engagement 5
- Designed and tuned policies to improve detection performance.

EXPERIENCE

Northwestern University Lab for Internet and Security Technology, Evanston, IL
Position: Research Assistant — June 2018 – present

- Research Mentor for undergraduate and master students.
- Server Manager for five servers accessed by hundreds of users.
- External reviewer for AsiaCCS 2022, IEEE S&P 2024

Northwestern University Electrical Engineering & Computer Science Department, Evanston, IL
Position: Teaching Assistant — September 2019 – present

- CS 354: Computer System Security
- CS 212: Mathematical Foundations of Computer Science
- CS 211: Fundamentals of Computer Programming II
- CS 111: Fundamentals of Computer Programming I