XI LI

she/her/hers | 814-777-6667 | W346, Westgate Building, University Park, PA, 16802
xili.cs.psu@gmail.com ◇ lixi1994.github.io

RESEARCH INTERESTS AND VISION

My research focuses on **machine learning security**, with specific studies on the data poisoning attacks and defenses. My research vision is centered on developing **trustworthy and reliable AI systems**, supporting advancement of technology and solving social challenges.

EDUCATION

The Pennsylvania State University — State College, PA
Ph.D. Candidate in Computer Science and Engineering — Aug. 2018 - July 2024 (expected)
Advisor: Dr. George Kesidis and Dr. David Miller
M.S. in Computer Science and Engineering — Aug. 2016 - July 2018

The Southeast University — Nanjing, China
B.E. in Electrical Engineering — Aug. 2012 - June 2016

PUBLICATIONS

- **X. Li**, J. Wang. *Position Paper: Assessing Robustness, Privacy, and Fairness in Federated Learning Integrated with Foundation Models*. under review.
- **X. Li**, D. J. Miller, G. Kesidis. *CEPA: Consensus Embedded Perturbation for Agnostic Detection and Inversion of Backdoors*. under review.
- **X. Li**, C. Wu, J. Wang. *Vulnerabilities of Foundation Model Integrated Federated Learning Systems Under Adversarial Threats*. under review.
- **X. Li**, D. J. Miller, Z. Xiang, G. Kesidis. *BIC-based Mixture Model Defense against Data Poisoning Attacks on Classifiers: A Comprehensive Study*. IEEE Transactions on Knowledge and Data Engineering (TKDE), 2024.
- **X. Li**, C. Wu, J. Wang. *Unveiling Backdoor Risks Brought by Foundation Models in Heterogeneous Federated Learning*. The Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD), 2024.
- **X. Li**, S. Wang, R. Huang, M. Gowda, G. Kesidis. *Temporal-Distributed Backdoor Attack Against Video Based Action Recognition*. AAAI, 2024.
- **X. Li**, S. Wang, C. Wu, H. Zhou, J. Wang. *Backdoor Threats from Compromised Foundation Models to Federated Learning*. FL@FM-NeurIPS'23.
- **X. Li**, D. J. Miller, Z. Xiang, G. Kesidis. *A BIC-based Mixture Model Defense against Data Poisoning Attacks on Classifiers*. IEEE International Workshop on Machine Learning for Signal Processing (MLSP), 2023.
- **X. Li**, Z. Xiang, D. J. Miller, G. Kesidis. *Backdoor Mitigation by Correcting Distribution of Neural Activation*. under review of Neurocomputing.
- **X. Li**, D. J. Miller, Z. Xiang, G. Kesidis. *Test-Time Detection of Backdoor Triggers of Poisoned Deep Neural Networks*. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), 2022.
- Z. Xiang, D. J. Miller, S. Chen, **X. Li**, G. Kesidis. *Detecting Backdoor Attacks Against Point Cloud Classifiers*. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), 2022.
- Z. Xiang, D. J. Miller, S. Chen, **X. Li**, G. Kesidis. *A Backdoor Attack against 3D Point Cloud Classifiers*. ICCV, 2021.

TEACHING EXPERIENCE

- **Teaching Assistant** — 2021 Spring
  CMPSC465 Data Structures and Algorithms
  Instructor: Prof. Chunhao Wang and Prof. Paul Medvedev.
- **Teaching Assistant** — 2019 Fall - 2024 Spring
  CMPSC/MATH 451 Numerical Computations
  Instructor: Prof. Jesse Barlow, Prof. George Kesidis, and Prof. Kamesh Madduri.

- **Teaching Assistant** 2018 Fall
  CMPEN/EE 455 Digital Image Processing I
  Instructor: Prof. William Higgins

PROFESSIONAL SERVICE

Conference Program Committee:

- SIAM International Conference on Data Mining (SDM), 2024

Conference Reviewer:

- IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), 2022-2024
- SIGKDD Conference on Knowledge Discovery and Data Mining (KDD), 2023, 2024
- IEEE/CVF Computer Vision and Pattern Recognition Conference (CVPR), 2024

Journal Reviewer:

- Computers and Security (C&S), 2024
- IEEE Transactions on Circuits and Systems for Video Technology (TCSVT), 2024

Student Volunteer:

- Conference on Neural Information Processing Systems (NeurIPS), 2023