Liuwan Zhu

PhD Candidate · Department of Electrical & Computer Engineering

Old Dominion University, 5115 Hampton Blvd, Norfolk, VA 23529

+1 757-335-8193 | lzhu001@odu.edu | https://lzhu.netlify.app

Interests

- Machine Learning for Cybersecurity, especially in the computer system and cyber-physical systems
- Robustness and Security of Deep Learning Systems
- Vision-Language Multi-modal Deep Learning

Education

Old Dominion University *Norfolk, VA, USA*

PhD, Electrical & Computer Engineering *Expected in May 2023*

- Advisor: Dr. Hongyi Wu

Hunan University *Changsha, Hunan, CHINA*

BS, Computer Science *2017*

Professional Experiences

Graduate Research and Teaching Assistants

Department of Electrical & Computer Engineering, Old Dominion University *2017-2023*

Publications

L. Zhu, R. Ning, J. Li, C. Xin, and H. Wu, "Most and Least Retrievable Images in Visual-Language Query Systems", in *Proceedings of European Conference on Computer Vision* (ECCV), 2022.

L. Zhu, R. Ning, C. Xin, and H. Wu, "CLEAR: Clean-up Trigger-Free Backdoor in Neural Networks", in *Proceedings of IEEE International Conference on Computer Vision* (ICCV), 2021.

L. Zhu, R. Ning, C. Wang, C. Xin, and H. Wu, "GangSweep: Sweep out Neural Backdoors by GAN", in *Proceedings of ACM International Conference on Multimedia* (MM), Seattle, WA, October 12-16 , 2020.

R. Ning, C. Wang, C. Xin, J. Li, **L. Zhu**, and H. Wu, "CapJack: Capture In-Browser Crypto-jacking by Deep Capsule Network through Behavioral Analysis", in *Proceedings of IEEE International Conference on Computer Communications* (INFOCOM), Paris, France, April 29-May 2, 2019. **(Best In-session Presentation Award**).

W. Purwanto, Y. He, J. Ossom, Q. Zhang, **L. Zhu**, K. Arcaute, M. Sosonkina and H. Wu, "DeapSECURE Computational Training for Cybersecurity Students: Improvements, Mid-Stage Evaluation, and Lessons Learned." In *Journal of Computational Science Education*, 12(2), 3-10, 2021

L. Zhu, R. Ning, J. Li, C. Xin, and H. Wu, "SEER: Backdoor Detection for Vision-Language Models through Searching Target Text and Image Trigger Jointly", submitted to *IEEE International Joint Conference on Artificial Intelligence (IJCAI)*, 2023

Proposals

As the main student contributor, I helped my advisor to write the following grant proposals on multiple research tasks.

Title: TrustAI: enhancing human confidence and trust in AI models

- Funded by Commonwealth Cyber Initiative(CCI)
- During: 12/2022 - 12/2023

- Total Award: $60,000
- Wrote proposal: curriculum development and workforce training, including secure and safe AI Workshop and NSA GenCyber Summer Camps.

Title: Facilitate the Convergence of the Next-gen AI and Wireless

- Funded by InterDigital Communications, Inc.
- During: 01/2023 - 01/2024
- Total Award: $100,000
- Wrote proposal: Next-gen AI for Wireless Network.

Title: Backdoor Detection, Mitigation, and Prevention in Deep Learning Models

- Funded by National Security Agency(NSA)
- During: 2022-2024
- Total Award: $500,000
- Worked together with advisor to investigate, design neural backdoor detection algorithms, conduct experiments and write proposals.

Teaching Experiences

GenCyber Summer Camp(Funded by NSA) (Instructor) *2019-2022*

- Led instructors to create lessons and hands-on labs, including wireless security, cyber attack and defenses, and AI security.
- More than **200** K-12 students and teachers completed the camp.

DeapSECURE(Data Enabled Advanced Training Platform for Cybersecurity Research and Education) Workshop Series(Funded by NSF CyberTraining) (Instructor) *2019-2021*

- Created six lessons and hands-on labs (in total 24 hours) covering usage of High-Performance Computing(HPC), parallel computing, cryptography for privacy-preserving computation, big data and machine learning and so on.
- More than **150** undergraduate and graduate students completed the training.

CYSE635. AI Security and Privacy (Guest Lecturer) *Fall 2021*

- Taught the backdoor attack and corresponding defenses in deep learning.

CYSE301. Cybersecurity Techniques and Operations (Teaching Assistant) *Spring 2023*

ECE355. Introduction to Networks and Data Communications (Teaching Assistant) *Fall 2018*

Activity and Services

Reviewers: IEEE Transaction of Mobile Computing; IEEE / CVF Computer Vision and Pattern Recognition Conference 2023
Volunteer: IEEE International Conference on Computer Communications (INFOCOM) 2020