

# Liuwan Zhu

ASSISTANT PROFESSOR · DEPARTMENT OF ELECTRICAL & COMPUTER ENGINEERING

University of Hawai'i at Mānoa, Honolulu, HI

✉ liuwan@hawaii.edu | 🏠 <https://lzhu.netlify.app>

## Interests

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

## Education

### Old Dominion University

PHD, ELECTRICAL & COMPUTER ENGINEERING

Norfolk, VA, USA

2017-2023

### Hunan University

BS, COMPUTER SCIENCE

Changsha, Hunan, CHINA

2013-2017

## Work Experiences

### Assistant Professor

DEPARTMENT OF ELECTRICAL & COMPUTER ENGINEERING, UNIVERSITY OF HAWAI'I AT MĀNOA

Start at Aug 2023

### 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 *the Annual AAAI Conference on Artificial Intelligence*, 2024

## Proposals

### Title: A Holistic Evaluation Framework for Multi-Modal AI Security and Trustworthiness on Federated IoT

- Funded by Commonwealth Cyber Initiative(CCI)
- During: 2023-2024

- Total Award: \$50,000
- Senior Personnel

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

---

<b>EE/ICS660. Computer Architecture (Instructor)</b>	<i>Fall 2023</i>
<b>GenCyber Summer Camp(Funded by NSA) (Instructor)</b>	<i>2019-2022</i>
<b>DeapSECURE(Data Enabled Advanced Training Platform for Cybersecurity Research and Education) Workshop Series(Funded by NSF CyberTraining) (Instructor)</b>	<i>2019-2021</i>
<b>CYSE635. AI Security and Privacy (Guest Lecturer)</b>	<i>Fall 2021</i>
<b>CYSE301. Cybersecurity Techniques and Operations (Student Mentor)</b>	<i>Spring 2023</i>
<b>ECE355. Introduction to Networks and Data Communications (Teaching Assistant)</b>	<i>Fall 2018</i>

## Activity and Services

---

Reviewers: IEEE Transaction of Mobile Computing(TMC); Pervasive and Mobile Computing Journal (PMC); IEEE CVPR 2023; ACM MultiMedia 2023

Volunteer: IEEE International Conference on Computer Communications (INFOCOM) 2020 Faculty Mentor: NSF REU sites at School of Cybersecurity, ODU, 2023