Zeyan Liu

CSE Department
University of Louisville
Duthie Center 220, Louisville, Kentucky 40292

Email: zeyan.liu@louisville.edu
Web: https://liuzey.com

RESEARCH INTERESTS

- **Security in AI/ML**: AI system security, generative AI security, human factors in AI security
- **Responsible AI**: AI disinformation and misusage, privacy-preserving ML
- **AI for Cybersecurity**: network security

WORK EXPERIENCE

University of Louisville, Computer Science and Engineering Department, Louisville, KY, USA
Tenure-track Assistant Professor, August 2024 - Now

Visa Inc., Cyber Analytics & AI Innovations, Ashburn, VA, USA
Cybersecurity Research Scientist Intern, May 2023 - August 2023

EDUCATION

The University of Kansas, Lawrence, KS, USA
Ph.D., Computer Science, 2024
- Advisor: Prof. Bo Luo, Prof. Fengjun Li

Wuhan University, Wuhan, Hubei, China
B.S., Mathematics and Applied Mathematics, 2019

PUBLICATIONS

Conference Papers (My student mentorees are underlined.)

1. Yuying Li, **Zeyan Liu**, Junyi Zhao, Liangqin Ren, Fengjun Li, Jiebo Luo, Bo Luo, "The Adversarial AI-Art: Understanding, Generation, Detection, and Benchmarking", *European Symposium on Research in Computer Security (**ESORICS**)*, Springer, 2024.
2. Ye Wang, **Zeyan Liu**, Bo Luo, Rongqing Hui, Fengjun Li, "The Invisible Polyjuice Potion: an Effective Physical Adversarial Attack against Face Recognition", *ACM SIGSAC Conference on Computer and Communications Security (**CCS**)*, ACM, 2024.
3. **Zeyan Liu**, Zijun Yao, Fengjun Li, Bo Luo, "On the Detectability of ChatGPT Content: Benchmarking, Methodology, and Evaluation through the Lens of Academic Writing", *ACM SIGSAC Conference on Computer and Communications Security (**CCS**)*, ACM, 2024.
4. Aozhuo Sun, Jingqiang Lin, Wei Wang, **Zeyan Liu**, Bingyu Li, Shushang Wen, Qiongxiao Wang, Fengjun Li, "Certificate Transparency Revisited: The Public Inspections on Third-party Monitors", *31st ISOC Network and Distributed System Security Symposium (**NDSS**)*, The Internet Society, 2024.
5. Liangqin Ren, **Zeyan Liu**, Fengjun Li, Kaitai Liang, Zhu Li, Bo Luo, "PrivDNN: A Secure Multi-Party Computation Framework for Deep Learning using Partial DNN Encryption", *Privacy Enhancing Technologies Symposium (**PETS**)*, self-pub, 2024.
6. **Zeyan Liu**, Fengjun Li, Zhu Li, Bo Luo, "LoneNeuron: a Highly-effective Feature-domain Neural Trojan using Invisible and Polymorphic Watermarks", *ACM SIGSAC Conference on Computer and Communications Security (**CCS**)*, ACM, 2022.
7. **Zeyan Liu**, Fengjun Li, Jingqiang Lin, Zhu Li, Bo Luo, "Hide and Seek: on the Stealthiness of Attacks against Deep Learning Systems", *European Symposium on Research in Computer Security (**ESORICS**)*, Springer, 2022.

TEACHING EXPERIENCE

University of Louisville

- Instructor, CSE 502 Data Structures, Spring 2025

The University of Kansas

- Teaching Assistant, EECS 447 Introduction to Database Systems LEC, Spring 2023
- Teaching Assistant, EECS 210 Discrete Structures LEC, Fall 2022
- Teaching Assistant, EECS 647 Introduction to Database Systems LEC, Spring 2022
- Teaching Assistant, EECS 210 Discrete Structures LEC, Fall 2021
- Instructor, EECS 210 Discrete Structures DIS, Fall 2021
- Teaching Assistant, EECS 647 Introduction to Database Systems LEC, Spring 2021

MENTORING

- Liangqin Ren, Ph.D. Student, The University of Kansas, 09/2021-present
  Mentored Project: Multi-party Computation Framework with Partial DNN Encryption (PETS'24)
- Yuying Li, MS Student, The University of Kansas, 08/2023-present
  Mentored Project: Benchmarking Text-to-Image Generation Models (ESORICS'24)
- Junyi Zhao, Undergraduate Student, The University of Kansas, 10/2021-present (Now MS student at KU)

HONORS & AWARDS

- Doctorate Dissertation Defense - Pass with Honors, The University of Kansas, 2024
- EECS Robb Award, The University of Kansas, 2022
- ACM CCS Travel Grant Award, 2022
- Graduate Scholarly Presentation Travel Award, The University of Kansas, 2022
- CANSec Travel Grant Award, 2022
- Honors Graduate (Top 10%), Wuhan University, 2019
- Outstanding Scholarship, Wuhan University, 2018
- Freshman Scholarship (Top 10%), Wuhan University, 2015

PROFESSIONAL SERVICES & TALKS

Organizing Committee

- EAI International Conference on Applied Cryptography in Computer and Communications (EAI AC3), 2022

Journal Reviewer

- IEEE Transactions on Image Processing (TIP)
- IEEE Transactions on Emerging Topics in Computing (TETC)
- IEEE Transactions on Dependable and Secure Computing (TDSC)
- ACM Transactions on Internet of Things (TIOT)
- Artificial Intelligence Review
- Data Science and Engineering
- Frontiers in Research Metrics and Analytics

Conference Program Committee

- Financial Cryptography and Data Security (FC), 2025
- International Conference on Mining Software Repositories (MSR), 2025

Nominated Conference Reviewer

- International Conference on Learning Representations (ICLR), 2025
- International Conference on Artificial Intelligence and Statistics (AISTATS), 2025
- ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD), 2025
- International Joint Conference on Neural Networks (IJCNN), Area Chair, 2025
- ACM The Web Conference (WWW), 2024-2025
- ACM Conference on Computer Supported Cooperative Work (CSCW), 2024
- Annual Conference on Neural Information Processing Systems (NeurIPS), 2024
- IEEE International Conference on Acoustics, Speech, & Signal Processing (ICASSP), 2022-2024
- IEEE International Conference on Image Processing (ICIP), 2022-2025

Workshop Paper Reviewer

- NeurIPS Workshop on Women in Machine Learning, 2024
- NeurIPS Workshop on Mathematical Reasoning and AI, 2024
- NeurIPS Workshop on Pluralistic Alignment, 2024
- NeurIPS Workshop on Fusing Neuroscience and AI for Intelligent Solutions, 2024
- NeurIPS Workshop on Behavioral ML, 2024
- EMNLP Workshop on Multilingual Representation Learning, 2024
- ICML Workshop on LLMs and Cognition, 2024
- Women in Computer Vision Workshop (WiCV), 2024-2025
- Robust, Out-of-Distribution And Multi-Modal models Workshop for Autonomous Driving at ECCV, 2024
- MICCAI Workshop on Fairness of AI in Medical Imaging, 2024
- International Workshop on Security and Trust Management (STM) at ESORICS, 2022

Conference Artifact Evaluation Program Committee

- USENIX Security Symposium (USENIX SEC), 2025
- ACM SIGSAC Conference on Computer and Communications Security (CCS), 2024
- ACM Symposium on Operating Systems Principles (SOSP), 2024
- ACM Special Interest Group on Management of Data (SIGMOD), 2024
- USENIX Symposium on Operating Systems Design and Implementation (OSDI), 2024
- USENIX Annual Technical Conference (USENIX ATC), 2024
- USENIX WOOT Conference on Offensive Technologies (WOOT), 2024
- IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2024
- European Conference on Object-Oriented Programming (ECOOP), 2024
- IEEE International Symposium on Software Reliability Engineering (ISSRE), 2023-2024

Volunteering

- EAI International Conference on Security and Privacy in Communication Networks (SecureComm), The University of Kansas, 2022
- GenCyber Camp, The University of Kansas, 2021-2022

Talks

- ”On the Security of Modern AI: Backdoors, Robustness, and Detectability”, CSE/PhD Seminar, University of Louisville, 2024
- ”LoneNeuron: a Highly-effective Feature-domain Neural Trojan using Invisible and Polymorphic Watermarks”, I2S Student Research Symposium, The University of Kansas, 2023

- ”LoneNeuron: a Highly-effective Feature-domain Neural Trojan using Invisible and Polymorphic Watermarks”, GEA Research Symposium, The University of Kansas, 2023
- ”LoneNeuron: a Highly-effective Feature-domain Neural Trojan using Invisible and Polymorphic Watermarks”, 15th Central Area Networking and Security Workshop (CANSec), Wichita State University, 2022