Zeyan Liu

https://github.com/liuzey

Email: liuzey97@gmail.com

EDUCATION

The University of Kansas — Aug 2019 - present
Ph.D. in Computer Science
- Instructor: Dr. Bo Luo, Dr. Fengjun Li
- GPA: 3.80/4.00

Wuhan University — Sep 2015 - June 2019
B.S. in Mathematics & Applied Mathematics

PUBLICATIONS

- **Zeyan Liu**, Fengjun Li, Zhu Li, and Bo Luo. LoneNeuron: a Highly-effective Feature-domain Neural Trojan using Invisible and Polymorphic Watermarks. In ACM SIGSAC Conference on Computer and Communications Security (CCS), Los Angeles, CA, USA, 2022.

- **Zeyan Liu**, Fengjun Li, Jingqiang Lin, Zhu Li, and Bo Luo. Hide and Seek: on the Stealthiness of Attacks against Deep Learning Systems. In European Symposium on Research in Computer Security (ESORICS), Copenhagen, Denmark, 2022.

- Aozhuo Sun, Jingqiang Lin, Wei Wang, Fengjun Li, Bingyu Li, Qiongxiao Wang, and **Zeyan Liu**. Certificate Transparency Revisited: The Public Inspections on Third-party Monitors. Under review at ACM CCS 2023.

HONORS AND AWARDS

- **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

SERVICES AND PRESENTATION

- **Reviewer**: ICASSP 22-23, ICIP 22-23
- **External Reviewer**: STM 2022
- **Organizing Committee**: EAI AC3 2022
- **Presentation**: CANSec 2022, KU ISRS 2023

EMPLOYMENT EXPERIENCE

EECS, The University of Kansas — Spring & Fall 2021 - 2022
Graduate Teaching Assistant
- Courses: EECS 210 Discrete Structures, EECS 647 Intro Database System.

I2S, The University of Kansas — Fall 2019 - Summer 2022
Graduate Research Assistant
- Research focus: Adversarial machine learning.

PROJECT EXPERIENCE

Model Poisoning against Deep Neural Networks — 2020.8 - 2022.7
- Conducted a survey on real-world vulnerabilities and feasibility of attacks in MLaaS.
- Designed a trojan attack which reached 100% ASR and bypassed 96% human inspectors.
- Demonstrated robustness against nine sota defenses, including data cleansing and explanations.

Stealthiness Study of Adversarial and Backdoor Attacks — 2020.8 - 2022.4
- Implemented twenty state-of-art deep learning attacks on six image datasets.
- Evaluated attack images using 24 metrics of image quality and similarity.
- Compared and connected numerical and experimental implications using correlations.

Machine Learning Solutions for Security Applications — 2020.2 - present
- Designed a real-world adversarial attack against face authentication systems using infrared.
- Scaled up the efficiency of DNN validations in secure MPC with FHE.
- Explained inconsistency of TLS/HTTPS server certificates with SVM and RandomForest.

Keystroke Inference using Sequence Learning — 2019.8 - 2020.2
- Improved side-channel ASR on smartwatch sensor data using HMM and LSTM.

SKILLS SUMMARY

- **Languages & Software**: Python, Java, SQL, MATLAB
- **Frameworks**: PyTorch, TensorFlow, Keras