Bihe · Zhao

Beijing, China 100000 • (+86)130-1256-3808 • bihezhao@buaa.edu.cn

EDUCATION

Beijing University of Aeronautics and Astronautics Beijing, China 09/2017-01/2024

Bachelor of **Information Security** GPA:3.8

Master of **Cyber Space and Technology** GPA:3.8

University of Illinois at Urbana-Champaign Champaign, Illinois 07/2018-08/2018

Global Education and Training Program for Accounting & Finance GPA:4.0

PROFESSIONAL SKILLS AND LANGUAGE

Programming Languages: Python, C, Java

Tools: MATLAB, Wireshark, MySQL, Latex

Computer Science: Data Structures and Program Design, Operating System, Computer Networks, Database System Concepts, Machine Learning, Natural Language Processing

AI Frameworks and Libraries: Pytorch, TensorFlow, nltk

English: TOEFL:109 (R30+L30+S25+W24)

GRE: Verbal 160, Quantitative 167, AW 3.5

PUBLICATIONS

Zhao B, Guan Z, Zhang Y, Leng X, Bian S. SEEKER: Query-Efficient Model Extraction via Semi-Supervised Public Knowledge Transfer. Under Review.

Deng X*, ***Zhao B****, Guan Z, Xu M. A New Finding and Unified Framework for Fake Image Detection[J]. IEEE Signal Processing Letters, 2023.

Zhang Y, Liu J, Guan Z, ***Zhao B***, Leng X, Bian S. ARMOR: Differential Model Distribution for Adversarially Robust Federated Learning[J]. Electronics, 2023, 12(4): 842.

Guan Z, Zhang L, Huang B, ***Zhao B***, Bian S. Adaptive Hyperparameter Optimization for Black-box Adversarial Attack. Under Review at .IJIS.

PROFESSIONAL EXPERIENCE

Model Security Research Internship at SenseTime Technology 01/2022-now

- Proposed a query-efficient model extraction attack based on public datasets that outperforms state-of-the-art model extraction attacks by a large margin.
- Designed an augmentation invariant unsupervised training scheme to effectively extract information from public datasets.
- Proposed an aggregated query generator based on multi-input autoencoder to craft information-extracting queries.
- Implemented with Pytorch, will be open source.

Backend Development Internship at ByteDance Technology 08/2020-02/2021

- Assisted in the development of data annotation and management platform.
- Developed and improved an alarm center that has more than 20,000 rules to detect unusual data traffic.
- Wrote more than 5,000 lines of code with Go.

PROJECT EXPERIENCE

Feature Reconstruction Attack in Split Learning 10/2022-now

- Developing a feature reconstruction attack against vertical split learning to recover the private datasets of the clients.
- Supported by Ant Group.

COMPETITIONS

Face shifting Detection based on Video Watermarking and PUF 01/2019-08/2019

- First Prize, 12th National College Student Information Security Contest (top 8%)
- Utilized OpenCV to apply video watermarking based on DCT (Discrete Cosine Transform).
- Detected face shifting operation via NCC (Normalized Cross-Correlation) analysis of two watermark images extracted from videos before and after face shifting.
- Used Raspberry Pi to extract PUF (Physical Unclonable Function) information from SRAM to verify the video watermarking.
- Implemented a pipeline from video collection to video/image processing.

AWARDS

First Prize, 12th National College Student Information Security Contest (top 8%) 08/2019

Excellent Student of Beijing University of Aeronautics and Astronautics (top 5%) 06/2019

First Prize, Academic Excellence Award (top 5%) 10/2019

Outstanding Leader of Beijing University of Aeronautics and Astronautics (top 4%) 12/2018

Second Prize, National English Competition for College Students (top 2%) 05/2019

EXTRACURRICULAR ACTIVITIES

Student President in Cyber Science and Technology Department 09/2018-06/2021

Volunteer Work: New Year's Party of Cyber Science and Technology Department, College Basketball Game 08/2018-11/2022