Bihe Zhao

Master, Beihang University
Beijing, China

+86-13012563808
bihezhao@buaa.edu.cn
Personal Website
GitHub Profile
Google Scholar

Education

•Beihang University (BUAA) *09/2021–01/2024*
***Master** in Cyber Security and Technology* GPA: 3.8/4.0

•Beihang University (BUAA) *09/2017–06/2021*
***Bachelor** in Cyber Security and Technology* GPA: 3.8/4.0

•University of Illinois at Urbana-Champaign (UIUC) *09/2021–01/2024*
***Visiting Student** at Global Education and Training Program for Accounting & Finance* GPA: 4.0/4.0

Publications

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

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

3. 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.

Professional Experience

•Research Intern at SenseTime Technology *01/2022-04/2023*
Advised by Xianglun Leng and Ningyi Xu
- Proposed a query-efficient model extraction attack based on public datasets that outperforms state-of-the-art model extraction attacks by a large margin.
- Revealed an observation for face forgery detection and designed a unified detection framework based on the finding.
- Implemented both projects with Pytorch.

•Software Engineer Intern at ByteDance Technology *08/2020-02/2021*
Advised by Hao Tang
- 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.

Research Experience

•Query-Efficient Model Extraction via Semi-Supervised Public Knowledge Transfer *04/2022-03/2023*
Advised by Prof. Song Bian and Prof. Zhenyu Guan
- Proposed a two-stage query-efficient model extraction framework that consists of a offline pre-training stage and a online querying stage.
- Designed an augmentation invariant unsupervised training scheme to effectively extract information from publicly available datasets.
- Proposed an aggregated query generator based on multi-input autoencoder to craft information-extracting queries.
- Implemented the attack that achieves 50× query-efficiency compared to state-of-the-art model extraction attacks.
- Implemented the attack with Pytorch, will be open source.
- Under review at ICCV 2023.

•A New Finding and Unified Framework for Fake Image Detection *01/2022-01/2023*
Advised by Prof. Xin Deng and Prof. Zhenyu Guan
- Revealed an important observation that GAN generated faces possess stronger non-local self-similarity property than real faces.
- Proposed a non-local attention based fake face detection network based on the above observation, which outperforms state-of-the-art fake face detection networks across six datasets.
- Designed a non-local feature extraction module that can be combined with different fake image detection networks and improve their detection accuracy.
- Implemented the framework with Pytorch, open source at GitHub.
- Accepted by IEEE Signal Processing Letters.

•**Model Extraction against black-box 3D Point Cloud Models via Single-view Reconstruction** *11/2022-now*

Advised by Prof. Song Bian and Prof. Zhenyu Guan

– Proposed the first model extraction attack against 3D point cloud classifiers.
– Designing a query generator based on single-view 3D reconstructon, which can produce 3D point clouds from 2D public datasets.
– Implementing the attack with Pytorch, will be open-source.
– Will be submitted to NIPS 2023.

•**Feature Reconstruction Attack against Vertical Split Learning** *10/2022-now*

Advised by Longfei Zheng and Prof. Zhenyu Guan

– Developing a feature reconstruction attack against vertical split learning that recovers the private datasets of the clients.
– Designing a two-stage feature reconstruction framework that consists of a bottom model completion stage and a model inversion stage.
– Supported by Ant Group Student Innovation Support Program.

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

•Ant Group Student Innovation Support Program (top 20%) *10/2022*
•Excellent Graduate of Beihang University (top 20%) *06/2021*
•First Prize, Academic Excellence Award (top 5%) *10/2019*
•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*
•Second Prize, National English Competition for College Students *05/2019*
•Outstanding Leader of Beijing University of Aeronautics and Astronautics (top 4%) *12/2018*

Teaching & Mentoring Activities

•**Teaching Assistant** of The Secret of Cryptology, Beihang University *09/2022-01/2023*
•**Mentor** for National College Student Information Security Contest, First Prize *03/2022-08/2022*
•**Mentor** for undergraduate researcher *12/2021-05/2022*
•**Teaching Assistant** of The Secret of Cryptology, Beihang University *09/2021-01/2022*

Professional Skills

Programming Languages: Python, C, Java
Tools: MATLAB, Wireshark, MySQL, Latex
Courses: Data Structures and Program Design, Operating System, Computer Networks, Database System Concepts, Machine Learning, Natural Language Processing
AI Frameworks: Pytorch, TensorFlow, nltk
English: TOEFL:109 (R30+L30+S25+W24)
GRE: Verbal 160, Quantitative 167, AW 3.5

Extracurricular Activities

•**Student President** in Cyber Science and Technology Department, Beihang University *09/2018-06/2021*
•**Volunteer** at New Year Gala of Cyber Science and Technology Department *11/2022*
•**Volunteer** at College Basketball Game *08/2018*