Bihe Zhao

PhD candidate, CISPA
Saarbrücken, Germany

☎ +49-681870832632
✉ bihe.zhao@cispa.de
🌐 Personal Website
🎓 Google Scholar

Education

•**Beihang University (BUAA)** *09/2021–01/2024*
***Master** in Cyber Science and Technology* Score: 93.05/100 Rank: 6/49
– Major Courses: Matrix Theory (99/100), Cyber Security (97/100), Algorithm Design and Analysis (96/100)

•**Beihang University (BUAA)** *09/2017–06/2021*
***Bachelor** in Cyber Science and Technology* Score: 91.20/100 Rank: 5/50
– Major Courses: Information Theory and Encoding (99/100), Natural Language Processing (95/100)

•**University of Illinois at Urbana-Champaign (UIUC)** *07/2018–08/2018*
***Visiting Student** at Global Education and Training Program for Accounting and Finance* GPA: 4.0/4.0

Publications

1. **Zhao B**, Guan Z, Jing J, Zhang Y, Leng X, Bian S. SEEKER: Semi-Supervised Public Knowledge Transfer for Query-Efficient Model Extraction.
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. **Zhao B***, Guan Z*, Bian S. PointSteal: Opening the Black-box of Point Cloud Models.
4. Guan Z, Zhang L, Huang B, **Zhao B**, Bian S. Adaptive Hyperparameter Optimization for Black-box Adversarial Attack[J]. International Journal of Information Security.
5. 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 Assistant at Agency for Science, Technology and Research (A*STAR)** *07/2023-present*
Advised by Prof. Qing Guo
– Proposed a neural radiance field (NeRF) editing scheme that enables drag-style operations on the NeRF scene under user specification.
– Implemented the project with Pytorch.

•**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

•**Semi-Supervised Public Knowledge Transfer for Query-Efficient Model Extraction** *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 semantic consistency based self-supervised 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.

•**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.
- Accepted by IEEE Signal Processing Letters, open source at GitHub.

•**Drag-style Manipulation on Neural Radiance Field** *07/2023-present*

Advised by Prof. Qing Guo

- Proposed a neural radiance field (NeRF) editing scheme that propagates drag-style manipulation from a single image to novel views.
- Designed a geometric matching algorithm to enhance multi-view consistency for the edited NeRF scene.
- Propose a generative model with a multi-view consistency constraint and a multi-view joint optimization scheme to edit the NeRF scene.

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

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.

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

Advised by Longfei Zheng and Prof. Song Bian

- 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 Swapping Detection based on Video Watermarking and PUF** *01/2019-08/2019*

- First Prize, 12th National College Student Information Security Competition (top 3%).
- 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

•Excellent Graduate of Beijing (top 3%)	*11/2023*
•Ant Group Student Innovation Support Program (top 7%)	*10/2022*
•Excellent Graduate of Beihang University (top 5%)	*06/2021*
•Outstanding Student Leader of Beihang University (top 4%)	*11/2019*
•First Prize, Academic Excellence Award (top 5%)	*10/2019*
•First Prize, 12th National College Student Information Security Competition (top 3%)	*08/2019*
•Excellent Student of Beihang University (top 5%)	*06/2019*

Teaching & Mentoring Activities

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

Professional Skills

Programming Languages: Python, C, Java
Tools: MATLAB, Wireshark, MySQL, Latex
AI Frameworks: Pytorch, TensorFlow, nltk
English: TOEFL:105 (R30+L28+S23+W24)
GRE: Verbal 160, Quantitative 167, AW 3.5