Bowei Tian

boweitian@whu.edu.cn | +86-13677130812

EDUCATION

Wuhan University, Wuhan, CHN 09/2020-06/2024

Bachelor of Engineering in **Information Securities**, expected in June 2024

- Cumulative GPA: **3.9/4.0**; Average Score: **91.3/100**
- Scholarship: Second Class Scholarship (06/2023)

PUBLICATION

- Meng Xue, Yuyang Zeng, Shengkang Gu, Qian Zhang, **Bowei Tian**, and Changzheng Chen. SDE: Early Screening for Dry Eye Disease with Wireless Signals, *The 2023 ACM International Joint Conference on Pervasive and Ubiquitous Computing(Ubicomp/IMWUT) 2023*
- Patent: Adversarial Sample Defense Methods and Devices based on Model Inversion Methods

RESEARCH EXPERIENCE

Network Information System Security & Privacy (NIS&P) Lab, Wuhan University 04/2022-Present

Researcher, **Backdoor on Transformers** 10/2022-Present

- Intended to limit the scope of trigger to raise the stealthiness of backdoor in transformers and manipulate the attention mechanism called "Attention diffusion" to improve attack elasticity
- Created Python codes based on PyTorch/TensorFlow/Colab to realize scope limitation and attention diffusion
- Achieved high stealthiness and efficiency, surpassing the baselines in Vision Transformers and NLP based transformers by 25%+
- Planning to submit a paper to *ACM Conference on Computer and Communications Security (CCS)* in May 2023

Research Assistant for Prof. Qian Wang, **Dry Eye Disease Detection** 01/2023-03/2023

- Proposed to use radar, a more convenient, contactless and ubiquitous way, to detect Screening dry eye disease
- Analyzed the structure of focal loss based Transformer model in Colab to detect dry eye disease
- Ran various kind of ablation studies, reorganizing codes and implementing functions such as data enhancement, dataset splitting, model fine-tuning
- Submitted a paper titled SDE: Early Screening for Dry Eye Disease with Wireless Signals to The 29th Annual International Conference on Mobile Computing and Networking (Mobicom) as a co-author

Research Assistant for Prof. Qian Wang, **Model Inversion Defense** 04/2022-10/2022

- Utilized Python to design API for several large scale databases (including ImageNet, CIFAR-10, and GTSRB) to prepare for later model training
- Established and analyzed codes of GAN model raised in the latest model inversion paper MIRROR (NDSS'22)
- Developed a program with 4000+ lines of Python code to realize a stealthy and robust Backdoor on Transformer
- Produced a patent named *Adversarial Sample Defense Methods and Devices based on Model Inversion Methods*

SELECTED PROJECTS

Game Development: Pac-Man 07/2021

- Designed a role play game that allows users to play against the ghost (AI) and eat as many beans as possible in a maze
- Utilized C programming language and A* algorithm to traverse all the location of the maze to avoid the ghost and set direction for movement to eat beans
- Achieved a high score that defeated 90%+ rivals

SKILLS

- Programming Language: C/C++, Python, MATLAB