# Hao Zhang

Personal Webpage:
https://superhenry2333.github.io

Phone: (+86) 15821930565
Email: zhanghaovs120@sjtu.edu.cn

## Education

B.S. Information Security, ShanghaiJiaoTong University, 2015-2019. GPA: 3.75/4.3 (88.1/100)

## Research Interest

Security Machine learning, Adversarial examples

## Research Experiences

### *0.1 Security machine learning research supervised by Ping Yi, Shanghai Jiao Tong University(2018/3-2018/5)*

Designed a cross training method to train a robust classification model, and successfully boost the robustness of the models to transfered adversarial examples.

When adversarial examples were detected, we used proposed "Inverse gradient recovery" method to recover the example so that it could be classified correctly. We find the proposed method can recover 93% adversarial examples generated by CW and 76% adversarial examples generated by FGSM.

### *0.2 Software security and reverse engineering research in Tencent (2018/7-2018/9)*

Reversed a decompile plugin of IDA. Tried to divide its C++ code into architecture independent code and architecture relative code, so that we could easily develop plugins supporting more architectures.

Took part in Defcon CTF the highest specification hacking competition, and won the fourth place.

### *0.3 Meta learning supervised by Hongyuan Zha, Georgia Institute of Technology (2019/6-2019/9)*

Construct a meta learning GAN with meta-learning method like MAML, Relational Network and MTL.

Addressed the few shot problem in ranking with neuSort and MAML.

### *0.4 Research on recommender system in ThinkLab in SJTU supervised by Junchi Yan(2018/10-2019/05)*

Improve the performance of our recommendation algorithm in few-shot scenario with meta learning method and considered each user as a task.

Extracted neighbor features of users with CNN and used popularity based negative sampling. Imporved the recommendation performance by over 10% compared with the state-of-the-art methods like NCF and eALS.

# Selected Projects

### *0.5 Attention based object detector*

Designed a new IOU combining attention and GIOU.

Implemented an object detector based on the new IOU. Put the new IOU into the loss function to boost the performance of the detector.

Use the proposed detector to count the number of birds in videos.

### *0.6 Music player based on recognize emotion*

Developed an android music player that can recognize human emotion and play music that is suitable for the emotion

Implement an emotion recognition model based on CNN and ran the model on a server.

The player take a photo of the user's face and send it to the server. The server recognize the user's emotion and send it to the player.

# Publications

Chao Chen, **Hao Zhang**, Dongsheng Li etc. Synergizing Local and Global Models for Matrix Approximation, *CIKM 2019*, accepted

Chao Chen, **Hao Zhang**, Junchi Yan etc. Probabilistic Meta-learner for Few-Shot Collaborative Filtering, *AAAI 2019*, submitted

# Patents

**Hao Zhang**, Ping Yi, Jiashang Hu etc. A cross-training method to enhance the robustness of deep learning model

**Hao Zhang**, Ping Yi, Jiashang Hu etc. A method of adversarial example detection based on the distance from the example to the decision boundary

**Hao Zhang**, Ping Yi, Jiashang Hu etc. Inverse gradient method for adversarial example recovery

# Prizes

First Prize in National college student information security contest (top3%), 2018

Honorable Mentioned in Mathematical Contest in Modeling, 2017

Academic Excellence Scholarship in SJTU, 2019