JIAHAO YU

ABOUT

Shanghai Jiaotong University(SJTU)
Major in ECE, Zhiyuan Honor Progarm
Advisor: Haojin Zhu, Liyao Xiang
Homepage
email:yujiahao@sjtu.edu.cn

RESEARCH INTERESTS

Machine Learning, Deep Learning
Privacy and Security

PUBLICATION

MSTrojan: Backdoor Attacks in Federated Learning with First-Order Triggers(under review for TMC)
Jiahao Yu, Liyao Xiang, Yuxin Lin, Shuchen Cai, Quanshi Zhang

Privacy Threats in Robust Model Inversion Attack(on revision for PPAI21)
Jiahao Yu, Liyao Xiang, Yuxin Lin, Weiting Li, Quanshi Zhang, Baochun Li

Voiceprint Mimicry Attack Towards Speaker Verification System in Smart Home(INFOCOM20)
Lei Zhang, Yan Meng, **Jiahao Yu**, Chong Xiang, Brandon Folk, Haojin Zhu

Matrix Gaussian Mechanism for Differentially-Private Learning(under review for INFOCOM21)
Jungang Yang, **Jiahao Yu**, Ruidong Chen, Weiting Li, Liyao Xiang, Xinbing Wang, Baochun Li

Invisible Backdoor Attacks Against Deep Neural Networks
Shaofeng Li, Benjamin Zi Hao Zhao, **Jiahao Yu**, Minhui Xue, Dali Kaafar, Haojin Zhu

EXPERIENCE

Shanghai Jiaotong University (Sep.2017-Jun.2021)

UIUC Summer research advised by Prof. Bo Li (Jul.2020-present)
Research Interest: Adversarial style transfer for NLP

MSRA Research Intern (Jul.2020-present)
Research Interest: Enhance adversarial robustness of malware detector

AWARDS

Zhiyuan Honor Rewards
1st place for Zhiyuan Scholar Program

PERSONAL SKILLS

Programming: C/C++,Python,Matlab,LaTeX,PowerShell
Software: Pytorch,Keras,Tensorflow,Echart