

Jiahao Yu

✉ jiahaoyu04@gmail.com • 🌐 sherdencooper.github.io/

Education

Northwestern University

Ph.D., Computer Science

- Advisor: Prof. Xinyu Xing

Evanston, United States

Sep. 2021 – Now

Shanghai Jiao Tong University

B.S., School of Electronic Information and Electrical Engineering

- Advisor: Prof. Haojin Zhu; Prof. Liyao Xiang

Shanghai, China

Sep. 2017 – July 2021

Research Interests

My research interests lie primarily in secure machine learning and reinforcement learning.

Publications

AIRS: Explanation for Deep Reinforcement Learning based Security Applications

- Jiahao Yu, Wenbo Guo, Qi Qin, Gang Wang, Ting Wang, Xinyu Xing
- In Proceedings of the 2023 USENIX Security 2023

Matrix Gaussian Mechanism for Differentially-Private Learning

- Jungang Yang, Liyao Xiang, Jiahao Yu, Xinbing Wang, Bin Guo, Bin Guo, Zhetao Li, Baochun Li
- In IEEE Transactions on Mobile Computing 2021

Speedup robust graph structure learning with low-rank information

- Hui Xu, Liyao Xiang, Jiahao Yu, Anqi Cao, Xinbing Wang
- In Proceedings of the 30th ACM International Conference on Information & Knowledge Management 2021

Voiceprint Mimicry Attack Towards Speaker Verification System in Smart Home

- Lei Zhang, Yan Meng, Jiahao Yu, Chong Xiang, Brandon Folk, Haojin Zhu
- In Proceedings of IEEE INFOCOM 2020

Invisible backdoor attacks against deep neural networks

- Shaofeng Li, Benjamin Zi Hao Zhao, Jiahao Yu, and Minhui Xue, Dali Kaafar, Haojin Zhu
- <https://arxiv.org/abs/1909.02742v1>

Working Experiences

Adversarial Attack against PowerShell Malware Detector

MSRA

- Research Intern
- Advisor: Dr. Bin Zhu

Beijing, China

Aug. 2020 – Mar. 2021