Jiahao Yu

✉ jiahaoyu04@gmail.com • 🌍 https://sherdencooper.github.io/

Education

Northwestern University **Evanston, United States**
Ph.D., Computer Science *Sep. 2021 – Now*

- Advisor: Prof. Xinyu Xing

Shanghai Jiao Tong University **Shanghai, China**
B.S, School of Electronic Information and Electrical Engineering *Sep. 2017 – July 2021*

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

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

Voiceprint Mimicry Attack Towards Speaker Verification System in Smart Home

- Lei Zhang, Yan Meng, **Jiahao Yu**, Chong Xiang, Brandon Folk, Haojin Zhu
- In IEEE INFOCOM 2020-IEEE Conference on Computer Communications 2020

Invisible backdoor attacks against deep neural networks

- Shaofeng Li, Benjamin Zi Hao Zhao, **Jiahao Yu**, and Minhui Xue, Dali Kaafar, Haojin Zhu
- arXiv:1909.02742v1

Working Experiences

Adversarial Attack against PowerShell Malware Detector **Beijing, China**
MSRA *Aug. 2020 – Mar. 2021*

- Research Intern
- Advisor: Dr. Bin Zhu