Bo Hui

Email : bo.hui@jhu.edu

Education

Johns Hopkins University Maryland, United States
Doctorate of Science in Computer and information (GPA: 3.97/4.0) *Jan. 2021 – Now*

Johns Hopkins University Maryland, United States
Master of Science in Security Informatics (GPA: 3.84/4.0) *Sep. 2019 – Dec.2020*

Shandong University Shandong, China
Bachelor of Engineering in Software Engineering (GPA: 4.36/5.0) *Sep. 2015 – June 2019*

Experience

Sr. Data Scientist, Intern - Cybersecurity Mar. 2024 – Aug. 2024
Advisor: Dr. Yan Zhai *Visa Inc.*

Research Assistant Mar. 2020 – Now
Advisor: Prof. Yinzhi Cao, Prof. Philippe Burilina, Prof. Neil Gong *Johns Hopkins University*

Course Assistant Feb. 2020 – May 2020
EN.650.656(1): Computer Forensics *Johns Hopkins University*

Publication

Practical Blind Membership Inference Attack via Differential Comparisons
Bo Hui*, Yuchen Yang*, Haolin Yuan*, Philippe Burlina, Neil Gong, Yinzhi Cao. *: equally contributed
In the Proceedings of Network & Distributed System Security Symposium (NDSS), 2021

Addressing Heterogeneity in Federated Learning via Distributional Transformation
Haolin Yuan*, **Bo Hui***, Yuchen Yang*, Philippe Burlina, Neil Gong, Yinzhi Cao. *:equally contributed
In the Proceedings of European Conference on Computer Vision (ECCV), 2022

PrivateFL: Accurate, Differentially Private Federated Learning via Personalized Data Transformation
Yuchen Yang*, **Bo Hui***, Haolin Yuan*, Neil Gong, Yinzhi Cao. *:equally contributed
In the Proceedings of USENIX Security Symposium, 2023

SneakyPrompt: Jailbreaking Text-to-image Generative Models
Yuchen Yang, **Bo Hui**, Haolin Yuan, Neil Gong, Yinzhi Cao.
To appear in the Proceedings of the IEEE Symposium on Security and Privacy (Oakland), 2024.

PLeak: Prompt Leaking Attacks against Large Language Model Applications
Bo Hui, Haolin Yuan, Neil Gong, Philippe Burlina, Yinzhi Cao
To appear in the Proceedings of The ACM Conference on Computer and Communications Security (CCS), 2024.

Projects

Master Dissertation Mar. 2020 – Aug. 2020

- Proposed BlindMI, a novel Membership Inference attack via differential comparison
- Implemented a prototype of BLINDMI including BLINDMI-DIFF and BLINDMI-1CLASS
- Improved attack performance and defeated state-of-art defenses

Undergraduate Dissertation Dec. 2018 – May 2019

- Based on Reinforcement Learning, DQN to implement the Gobang Platform
- Started with a neural network that knows nothing about Gobang and played against with itself, combining robust search algorithms and deep neural network
- Using a simple GUI frame to show the process of self-playing and playing with a human

Automatic Movie Trailer based on Deep Learning Apr. 2017 – May 2018

- Developed a movie trailer generation system using algorithms of Convolution Neural Network and LSTM on the platform of Caffe
- Programmed using WPF framework to implement front end used for users to upload a movie and wait for a while to get a trailer with the desired style and length