Yun-Yun Tsai

alice103000004@gmail.com (+886)973-798-908

RESEARCH INTERESTS

I'm a master student and research assistant in National Tsing Hua University. My research focuses on Artificial Intelligence Security, adversarial machine learning toward the robustness of deep neural networks, including attack, defense and robust evaluation. I'm currently working with Dr. Tsung-Yi Ho and Dr. Pin-Yu Chen from IBM research.

EDUCATION

National Tsing Hua University Hsinchu, Taiwan
M.S. in Computer Science Department Sep. 2018 – Jun. 2020

- Advisor: Dr. Tsung-Yi Ho
- Overall GPA: 4.18 / 4.3

National Tsing Hua University Hsinchu, Taiwan
B.S. in Computer Science Department Sep. 2014 – Jun. 2018

- Last 60 GPA: 3.89 / 4.3

PUBLICATIONS

- **Yun-Yun Tsai**, Pin-Yu Chen, Tsung-Yi Ho, "Transfer Learning without Knowing, Reprogramming black box machine learning model with scarce data and limited resources." in Proceeding of International Conference on Machine Learning (ICML), 2020.
- **Yun-Yun Tsai**, Pin-Yu Chen, Tsung-Yi Ho, "Adversarial Machine Learning for Social Good: Reprogramming black box machine learning model with scarce data and limited resources." Advances in Neural Information Processing Systems (NeurIPS) NewInML Workshop, Poster, 2019.
- Honggang Yu, Kaichen Yang, Teng Zhang, **Yun-Yun Tsai**, Tsung-Yi Ho, Yier Jin, "CloudLeak: Large-Scale Deep Learning Models Stealing Through Adversarial Examples." in Proceeding of Network and Distributed System Security Symposium (NDSS), 2020.
- Ta-Wei Huang, **Yun-Yun Tsai**, Chung-Wei Lin, Tsung-Yi Ho, "Vehicle Sequence Reordering with Cooperative Adaptive Cruise Control." In Proceeding of Design, Automation & Test in Europe Conference & Exhibition (DATE), 2019.

WORKING EXPERIENCES

Graduate Research Assistant July. 2020 – present
Advisor: Dr. Tsung-Yi Ho THETA Lab, NTHU, Hsinchu

- Focus on the research about federated learning system and sophisticated adversarial attack.

Visiting Scholar Mar. 2019 – Aug. 2019
Advisor: Dr. Yier Jin HSL at University of Florida (UF), Gainesville, Florida

- Focus on model retrieving attack on large-scale Deep Learning Model.

Software Engineer Intern Jul. 2017 – Jun. 2018
Microsoft Azure IoT Team Taipei, Taiwan

- Built POC (covers Smart City/Retail/Home/Manufacturing) leveraging Azure IoT Cloud services to demonstrate IoT solutions to 10+ technical business partners.

Microsoft 2017 Coding Angel, R&D Leader

- Designed/Created Azure Machine Learning hands-on materials with Microsoft MVPs and delivered the workshop in coding angel event to 100+ college STEM female students.

PROFESSTIONAL Skills AND ACTIVITIES

Invited talk at CYBERSEC - Aug. 20. 2020

- Giving a keynote about "CloudLeak: DNN Model Extractions from Commercial MLaaS Platforms" at CYBERSEC Taiwan 2020, one of the largest cybersecurity conference and exhibition in the Asia Pacific Region.

Programming Languages

- C/C++, Python, Verilog, etc.
- Package: Deep Learning Framework (ex: Tensorflow, Pytorch), Scikit-Learn, Keras, etc.

Certification

- Microsoft Professional Program Certificate in Data Science

English Skill

- Toefl: 99 (R 25, L 25, S 23, W 26)

EXTRACURRICULAR ACTIVITIES

First stand of Viola in National Tsing Hua University Orchestra Sep.2014 – June. 2018

- Have 10+ years training and performing experiences

Student Association of Computer Science Department in NTHU

- Student Association Leaders Section Sep. 2016 – Jul. 2017
- Computer Science Camp Leaders Section Jul. 2016 / Jul. 2017