Han Liu

h.liu1@wustl.edu
https://masterendless.github.io/
han-liu-539176239
https://github.com/MasterEndless

Education

2021-Now **Washington University in St. Louis**, St. Louis, U.S.
Ph.D. in Computer Science & Engineering. Advisor: Prof. Ning Zhang
Research Area: Trustworthy Machine Learning (Security/Privacy).

2016-2020 **University of Glasgow**, Glasgow, U.K.
B.Eng. in Electrical & Electronic Engineering
GPA: 20.2/22 (92.62/100). Graduated with First-Class Honor Degree

2016-2020 **University of Electronic Science and Technology of China**, Chengdu, China
B.Eng. in Communication Engineering
GPA: 89.2/100. Outstanding Graduates Honor

Professional Experience

2020-2021 **Tencent**, Shenzhen, China
Research Engineer in Machine Learning for Recommendation Systems.
- Designing and implementing the recommendation algorithms in WeSing Apps.
- Maintaining three application entrances with daily active users (DAU) up to 1500w.

Research Experience

2020-Now **Washington University in St. Louis**, St. Louis, U.S.
Research Assistant. Advised by Prof. Ning Zhang.
Topic: Security and Privacy of Machine Learning.

2019 Summer **Rutgers University**, New Brunswick, U.S.
Research Intern. Advised by Prof. Bo Yuan.
Topic: Efficient Deep Learning Algorithm Design.

Research Interests

Current research focuses on Adversarial Machine Learning, Cyber-Physical Security, and Privacy-Preserving Machine Learning

Publications

(∗ indicates equal contribution.)

CVPR 2023 **RIATIG: Reliable and Imperceptible Adversarial Text-to-Image Generation with Natural Prompts**
Han Liu, Yuhao Wu, Shixuan Zhai, Bo Yuan, and Ning Zhang. In IEEE / CVF Computer Vision and Pattern Recognition Conference (CVPR), 2023.

CVPR 2023 **SlowLiDAR: Increasing the Latency of LiDAR-Based Detection Using Adversarial Examples**
Han Liu, Yuhao Wu, Zhiyuan Yu, Yevgeniy Vorobeychik, and Ning Zhang. In IEEE / CVF Computer Vision and Pattern Recognition Conference (CVPR), 2023.

DAC 2023 **IP Protection in TinyML**
Jinwen Wang*, Yuhao Wu*, **Han Liu**, Bo Yuan, Roger Chamberlain, and Ning Zhang. In ACM/IEEE Design Automation Conference (DAC), 2023.

CCS 2022 **When Evil Calls: Targeted Adversarial Voice over IP Network**
Han Liu, Zhiyuan Yu, Mingming Zha, XiaoFeng Wang, William Yeoh, Yevgeniy Vorobeychik, and Ning Zhang. In ACM Conference on Computer and Communications Security (CCS), 2022.

RTSS 2022 **PolyRhythm: Adaptive Tuning of a Multi-Channel Attack Template for Timing Interference**
Ao Li*, Marion Sudvarg*, **Han Liu**, Zhiyuan Yu, Chris Gill, and Ning Zhang. In IEEE Real-Time Systems Symposium (RTSS), 2022.

IROS 2022 **From Timing Variations to Performance Degradation: Understanding and Mitigating the Impact of Software Execution Timing in SLAM**
Ao Li, **Han Liu**, Jinwen Wang, and Ning Zhang. In IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), 2022.

Awards

2021 **Student Grant Awarded by CCS conference committee**

2019 **National Scholarship Awarded by Ministry of Education of China**

2018 **First Prize in Undergraduate Biomedical Engineering Innovation Design Competition (only 6 teams in China)**

Service

2021-Now **Reviewer**, *IEEE/ACM Transactions on Networking*
Sub-Reviewer, *DAC, EuroS&P, WACV*

Skills

Programming Languages, *Python, Go, PostgreSQL, C++, C, Matlab*
Deep Learning, *PyTorch, TensorFlow*

Teaching

2022 **CSE 433S: Introduction to Computer Security**, *CSE*, WashU

2020 **Communication Principles and Systems**, *CE*, UESTC

2019 **Engineering Career Skills**, *CE*, UESTC