Wenjie Qu
Email: wen_jie_qu@outlook.com Website: https://quwenjie.github.io/

EDUCATION

Huazhong University of Science and Technology Wuhan, China
B.E. in Automation (ECE), Honor Class *2019.9-2023.6(Expected)*
GPA: 3.88/4.0, Rank: 1/27, China National Scholarship 2020 (Top 0.2% nationwide)

RESEARCH INTEREST

Various topics at the intersection of Security and Privacy, Systems, Machine Learning:

- Applied Cryptography
- Machine Learning Security& Privacy
- AI for Security, Software Engineering, System

PUBLICATIONS

[1] **W. Qu***, Y. Li*, B. Wang. "A Certified Radius-Guided Attack Framework to Image Segmentation Models" in *Network and Distributed System Security (**NDSS**), 2023*, Under Review

[2] **W. Qu**, J. Jia, N. Gong. "REaaS: Enabling Adversarially Robust Downstream Classifiers via Robust Encoder as a Service" in *Network and Distributed System Security (**NDSS**), 2023*, Under Review

[3] J. Wang, **W. Qu**, Y. Rong, C. Zhang, H. Qiu, Q. Li, Z. Li. "MPass: Bypassing Learning-based Static Malware Detectors" in *AAAI Conference on Artificial Intelligence (**AAAI**), 2023*, Under Review

[4] J. Jia*, **W. Qu***, and N. Gong. "MultiGuard: Provably Robust Multi-label Classification against Adversarial Examples" in *Advances in Neural Information Processing Systems (**NeurIPS**), 2022*

[5] H. Wang*, **W. Qu***, G. Katz, W. Zhu, Z. Gao, H. Qiu, J. Zhuge, and C. Zhang. "jTrans: Jump-Aware Transformer for Binary Code Similarity Detection" in *International Symposium on Software Testing and Analysis (**ISSTA**), 2022*

[6] H. Liu*, J. Jia*, **W. Qu**, and N. Gong. "EncoderMI: Membership Inference against Pre-trained Encoders in Contrastive Learning" in *ACM Conference on Computer and Communications Security (**CCS**), 2021*

RESEARCH EXPERIENCE

CoLink: A Programming Framework for Decentralized Data Science
Research Intern at University of California, Berkeley *April 2022-Present*
Advisor: **Prof. Dawn Song**

- Served as a core contributor to open source project CoLink, a programming framework that can greatly simplify the deployment of decentralized data science solutions.
- Implemented CoLink SDK python interface, based on gRPC services, basis for most CoLink-based machine learning applications.
- Designed and implemented an ML-MPC framework based on CoLink, containing protocols that enable users to perform general privacy-preserving data collaboration tasks. This framework supports horizontal, vertical, and hybrid distributed machine learning scenarios. It uses a highly flexible json structure, enabling users to freely define and specify their task and dataset without writing any code. With negligible manual modification, users can perform different tasks on the same dataset.

jTrans: Jump-Aware Transformer for Binary Code Similarity Detection[5]
Research Intern at Tsinghua University *July 2021-January 2022*
Advisor: **Prof. Chao Zhang**

- Proposed a novel neural network architecture for binary function similarity detection, encoding control flow information into the transformer.
- Proved through attention weights how our mechanism delivered the jump target information.
- Released the currently largest binary dataset to the community as a benchmark.
- Outperformed state-of-the-art binary similarity detection methods by 30.5%.

REaaS: Enabling Adversarially Robust Downstream Classifiers via Robust Encoder as a Service[2]
Research Intern at Duke University *June 2021-November 2022*
Advisor: **Prof. Neil Gong**

- Proposed a novel method for encoder cloud service which enables a client to build a provably robust downstream classifier while reducing the number of queries to the encoder by orders.
- Proposed a novel pre-training method to enhance the robustness of the encoder based on a spectral-norm regularization term.
- Achieved much better provable robustness for the clients' downstream classifiers when the cloud server pre-trains the encoder via our spectral-norm regularized training method.

MultiGuard: Provably Robust Multi-label Classification against Adversarial Examples [4]
Research Intern at Duke University *February 2021-May 2021*
Advisor: **Prof. Neil Gong**

- Proposed the first provable defense algorithm against adversarial examples on multi-label classification task.
- Derived a lower bound of intersection size between the set of labels predicted by our MultiGuard and ground truth labels, by a variant of Neyman-Pearson Lemma.
- Outperformed previous work by 7% on certified top-k precision and 15% on certified top-k recall.

A Certified Radius-Guided Attack Framework to Image Segmentation Models [1]
Research Intern at Illinois Institute of Technology *August 2020-January 2021*
Advisor: **Prof. Binghui Wang**

- Designed an attack framework against image segmentation models leveraging the properties of certified radius derived by randomized smoothing.
- Proposed the first blackbox attack to image segmentation models via gradient estimation based on bandits.
- Outperformed state-of-the-art PGD attack by 13% relatively.

ACADEMIC SERVICE

External Reviewer

- International Conference on Machine Learning (ICML), 2022

HONORS & AWARDS

- Science and Technical Innovation Scholarship 2022
- Huawei Scholarship (The only undergraduate in the department) 2022
- Autodriving CTF, DEFCON 29, 4th/89 2021
- **National Scholarship (Highest honor awarded by Ministry of Education)** 2020
- Outstanding Undergraduate of Academic Performance (Highest honor for HUST undergraduates, top 1%) 2020
- Merit Student (1/30) 2020
- Bronze Medal, National Olympiad in Informatics Winter Camp 2018
- First Prize, National Olympiad in Informatics in Provinces 2017