Tingwei Zhang

✉ tz6rz@virginia.edu 🏠 https://Tingwei-Zhang.github.io Tingwei-Zhang

🏛 Security Research Group at UVA

ACADEMIC QUALIFICATIONS

College of Arts and Sciences, University of Virginia (UVA), *Charlottesville, VA, USA*
B.A. in Computer Science with Minor in Statistics *Aug. 2020 – May. 2023 (Expected)*
Distinguished Majors Program in Computer Science

Research Interest: Security of Machine Learning

RESEARCH EXPERIENCE

SoK: What Have We Learned About Black-box Attacks Against Classifiers?
Supervisors: Prof. David Evans and Prof. Yuan Tian, UVA *Jun. 2022- Dec. 2022*

- Our team designed a comprehensive platform to facilitate reproducing existing black-box attacks against image and malware classifiers and proposed a general taxonomy of attacks based on the applicable scenarios in practice.
- I implemented 30+ black-box attacks (50,000+ lines of source code) of image domain on our platform. I designed and conducted experiments to evaluate them under the same criteria.
- I designed new attacks that significantly outperform existing attacks by summarizing the progress and trends in attacks and leveraging the insights from extensive experiments.
- Submitted the paper to 44th IEEE Symposium on Security and Privacy in December 2022.

Black-box Attack in Partial Auxiliary Information Setting
Supervisor: Prof. Yuan Tian, UVA *Oct. 2021 - Jun. 2022*

- Our team designed a black-box transfer attack with a self-supervised auxiliary model. Our method relaxes the assumption that the auxiliary and target models are built on the same training dataset in existing transferred attacks.
- I developed several popular self-supervised models, such as auto-encoders and contrastive learning. With an ensemble of masked auto-encoders, the number of queries was reduced by 86% and 11% in comparison to the naive black-box attack on MNIST and CIFAR10 datasets.

Machine Learning for Virginia Project (ML4VA)
Supervisor: Prof. Rich Nguyen *Sep. 2021 - Dec. 2021*

- Working with two students, I built a recommender system for electric and hybrid vehicles based on a user's desired features (price, size, model, etc.) using self-supervised machine learning models (see video), and won the third place for ML4VA EXPO over 40+ groups.
- I was in charge of collecting and analyzing the data, building and testing different models, and implementing a simple user interface.

ACADEMIC ACTIVITIES

IEEE / CVF Computer Vision and Pattern Recognition Conference (CVPR)
Attended in person CVPR'2022, New Orleans, Louisiana, USA (Self-funded) *Jun. 19 - 24, 2022*

International ACM SIGIR Conference on Research and Development in Information Retrieval
Attended in person SIGIR'2022, Madrid, Spain (Self-funded) *Jul. 11 - 15, 2022*

TEACHING ASSISTANT

CS4102: Algorithms, TA
Taught by Prof. Thomas B. Horton, UVA *Jan. - Jun. 2022*

- Held three-hour office hours per week for answering questions of homework and graded exams.
- Completed the course TA Practicum - Computer Science (CS2910, Taught by Prof. Nathan Brunelle), which is only open to Teaching Assistants in the CS department.

CS4774: Machine Learning, TA
Taught by Prof. Rich Nguyen, UVA *Aug. - Dec. 2022*

- Helped in the classroom when conducting in-class activities, held three-hour office hours per week for answering homework questions, and graded exams.

AWARDS & HONORS

Dean's List of Distinguished Students, College of Arts & Sciences, UVA
Awarded to students who demonstrate academic excellence for one semester *Fall 2021 and Spring 2022*

Euclid Mathematics Contest
Distinction (Ranked in top twenty-five percent of contestants, International ranking) *2019*

Canadian Senior Mathematics Contest (CSMC)
Distinction (Ranked in top twenty-five percent of contestants, International ranking) *2019*

21st ANNUAL High School Mathematical Contest in Modeling (HiMCM)
Honorable Nomination *2018*

Canadian Open Mathematics Challenge (COMC)
Bronze Award (National ranking) *2018*

SKILLS & INTERESTS

Technical Skills: Project experience in Python (PyTorch & TensorFlow), Java, C/C++, and R

Interests: Basketball (Caption of high school basketball team), Movies, Erhu - Chinese two-stringed fiddle (a member of V Major Chinese Arts Performing Troupe at UVA), and Traveling

Last updated Dec. 1, 2022