PEIYU XIONG

MASTER OF APPLIED SCIENCE

◊ gbxpeiyu@gmail.com
◊ 6047825801
◊ Vancouver, BC Canada
◊ Linkedin.com/in/peiyu-gabriella-xiong-349a82b1

MASc in Electrical and Computer Engineering. Research focused on Adversarial Robustness of Machine Learning applications / ML-based Android malware detection. Passionate about Artificial Intelligence, Machine Learning and Visualization.

Skills

MACHINE LEARNING / STATISTICAL ANALYSIS
Python
PyTorch
Pandas
Scikit-learn
Numpy
SciPy
MatplotLib
Julia
MATLAB
Mathematica

DATA VISUALIZATION
D3.js JavaScript
React Framework
Django Framework

GENERAL PROGRAMMING
Python
Scala
Java
C++

Education

University of British Columbia — Sept. 2019 to Dec. 2022
MASc Electrical and Computer Engineering 2022

University of British Columbia — Sept. 2013 to May 2019
BASc Engineering Physics 2019
Graduated with Distinction

Publication

Surveying the Effects of Data on Adversarial Robustness — Jan. 2022 to Dec. 2022
- Lead a research project to identify the impact of training data on the adversarial robustness of ML model through systematic review of literature published in top-ranked conferences and journals.
- Organized collected literature based on the properties of data identified (e.g., dimensionality, distribution), and analyzed the gaps in existing research.

On the Benign Features in Malware Detection — May 2022 to Sep. 2022
- Collaborated with other research students to design defense techniques against adversarial attacks for ML- based Android malware detectors.
- Demonstrated the effectiveness of proposed technique on the Android malware datasets (improved the robustness by 30% under Blackbox attacks, and by 60% under moderate Gray-box attacks).

Projects

Monotonic Classification for Adversarial Robustness — Sept. 2020 to Jan. 2022
- Designed a monotonic classification-based approach to improve ML models' adversarial robustness.
- Implemented training procedure for monotonic classifiers using PyTorch, and 3 different one-sided feature selection approaches using Scikit-learn.
- Validated the effectiveness of proposed approach on Android malware datasets.

Visualization of Android App Dataset for ML Model — Sept. 2020 to Dec. 2020
- Designed and developed program to visualize and interactively analyze android app datasets.
- Implemented the front-end of the system using D3.js with React Framework, and python with Django framework as back-end.

Employment

Visier Inc. — Vancouver, BC
Software Development (Backend) — May 2018 to Dec. 2018
- Implemented new features in Scala to support visualization of hierarchical data in large scale.
- Implemented data screening process to de-identify and sanitize data prior to data analysis.
- Wrote integration tests to evaluate both the correctness and performance of implemented features.

Laser Zentrum Hannover e.V. — Hannover, Germany
Research Assistant — May 2016 to Dec. 2016
- Wrote Mathematica programs to visualize the modification process of the surface topology of ceramic during Laser Micro-machining.
- Designed a dust suction box to reduce the residual particles from laser micro-machining by 80% through optimizing the structural design using SOLIDWORKS ANSYS CFX/Fluent simulation.
- Wrote image processing program to automatically analyze the density of microstructures on machined surface in micro-meter scale images.
- Assisted in investigating and developing techniques for Laser micro-machining on alumina to create anti- reflective surface structure.

Physics and Astronomy department of UBC — Vancouver, BC
Demonstration Equipment Management Assistant — Jan. 2015 to Apr. 2015
- Managed demonstration equipment for UBC physics and astronomy courses: repaired Mal-functioned equipment, assisted in demonstrations and developed new demonstrations.
- Updated and maintained UBC's Physics Department demonstration website in HTML.