Boyang (Edward) Zhang — CV

boyang.zhang@cispa.de • boz083.github.io

last update: February 20, 2023

Education

CISPA Helmholtz Center for Information Security — **Saarbrücken, Germany**
Ph.D. , Computer Science, Advisor: Yang Zhang — *12/2021 - present*

University of California, San Diego — **San Diego, USA**
M.S. , Electrical Engineering (Machine Learning and Data Science) — *9/2017 - 6/2019*

Bowdoin College — **Brunswick, USA**
B.A. , Physics High Honor, German (minor) — *8/2013 - 5/2017*

Research Interests

- Trustworthy Machine Learning (Privacy, Security, and Safety)
- Computer Vision

Publication

Conference

[1] **Boyang Zhang** and Xinlei He and Yun Shen and Tianhao Wang and Yang Zhang. A Plot is Worth a Thousand Words: Model Information Stealing Attacks via Scientific Plots. In *USENIX Security Symposium (USENIX Security)*. USENIX, 2023.

Teaching

Teaching Assistant — **Seminar: Privacy of Machine Learning**
October 2022 - February 2023, Saarland University

Teaching Assistant — **Advanced Lecture: Machine Learning Privacy**
May 2022 - September 2022, Saarland University

Teaching Assistant — **Seminar: Data-driven Understanding of the Disinformation Epidemic**
May 2022 - September 2022, Saarland University

Skills

Programming Languages
Python, Java, JavaScript, HTML, CSS, SQL, MATLAB

Tools and Libraries
PyTorch, TensorFlow, Keras, scikit-learn, OpenCV, NumPy, Pandas, Flask, Spring Boot

Languages

English - Fluent; Mandarin - Native; German - Basic (B1)

Additional Experience

Super Models for Global Health **Berkeley, USA**
Research Assistant – Single Payers with Machine Learning *3/2021 - 11/2021*
Advisor: James G. Kahn

- Evaluate machine learning algorithms' advantages in dealing with complex health insurance claims data including elimination of prior causal models, predicting non-linear interactions between features, reducing project design/hypothesis test time, and assisting feature selection/engineering for inference
- Integrate machine learning algorithms (Random Forest, SVM, DNN, GBM) into existing projects using simulated claims data (DE-SynPUF) to evaluate single payer healthcare system's potential impact on HSR

C&B Tech **San Diego, USA**
Software Engineer – Machine Learning *7/2019 - 11/2020*

- Developed image-based defect detection machine learning models for manufacturers in multiple industries (PCBs, LED panels), reaching human inspection's accuracy and efficiency (TensorFlow, Keras)
- Implemented feature extractions in PCB project to reduce deep learning model's workload by 40% and allow quick adjustment to different requirements from various manufacturers (scikit-learn, OpenCV)

Bowdoin College, Department of Physics **Brunswick, USA**
Honors Project – High Frequency Ultrasonic Propagation in Silicon *8/2016 - 5/2017*
Advisor: Madeleine Msall

- Imaged the anisotropic propagation of ultrasonic wave in different solids, to help providing information for calibrating dark matter detector schemes (CRESST, super-CDMS)
- Developed algorithms for simulating wave propagation in solids with known elastic constants
- Analyzed correlations between different parameters of the excitation pulse with the wave propagation
- Awarded department prize Noel C. Little Prize in Experimental Physics