Christiana Marchese

Claremont, CA
cemb2020@mymail.pomona.edu
+1 (240) 855-9357

Personal Website
Github
LinkedIn

Education

Pomona College, Claremont, CA — May 2024
Bachelor of Arts Computer Science; GPA: 3.94/4.00

Yonsei University, Seoul, South Korea — August 2022-December 2022
CIEE Arts and Sciences Program Study Abroad Program

Research Interests

My research interests lie at the intersection of cybersecurity and machine learning (ML), the security of ML systems and the use of ML – as well as other methods – towards approaching broader problems in application, network, and systems security. In my current work, I investigate the security weaknesses of ML systems and methods for improving robustness through both training and test-time defenses.

Current Projects

Senior Thesis: Securing Federated Learning Against Post-Breach Evasion Attacks
Advisors: Dr. Eleanor Birrell and Dr. Anthony Clark

Autonomous Robotics and Complex Systems Lab: Adversarial Training for Sim-to-Real Transfer
Advisor: Dr. Anthony Clark

Publications and Project Writeups

Implementing and Evaluating the Probability Weighted Word Saliency Algorithm as a Method of Adversarial Example Generation for Deep Neural Networks — May 2023
NLP Final Class Project

- Implemented the Probability Weighted Word Saliency (PWWS) algorithm and evaluated its effectiveness in adversarial example generation for sentiment analysis models (Github)

Investigating Neural Network Architectures, Techniques, and Datasets for Autonomous Navigation in Simulation — December 2021
2021 IEEE Symposium Series on Computational Intelligence Conference

- Co-wrote and published research paper on analyzing different neural network architectures and data collection techniques for agent navigation in simulated environments (PDF)

Predicting Mental Health Outcomes with Deep Learning — July 2021
2021 ACM Practice and Experience in Advanced Research Computing (PEARC) Conference

- Created and presented research poster based on XSEDE Empower Program work (PDF)

Research Experience

Research Assistant, Autonomous Robotics and Complex Systems (ARCS) Lab May 2021-Present

Adversarial Training for Sim-to-Real Transfer Project

- Researching methods to overcome the reality gap between the simulation learning and real-life performance in order to develop more safe, robust mobile robots
- Implementing adversarial example generation algorithms for the adversarial training of computer vision models

Investigating Neural Network Architectures, Techniques, and Datasets for Autonomous Navigation Project

- Researched neural networks that retain different degrees of state for simulated navigation (Github)
- Built custom datasets and modified convolutional neural network architectures to create hybrid-input CNNs and ConvLSTMs, for computer vision navigation tasks (Pytorch and FastAI)
- Wrote automation scripts to streamline the training and inference of custom neural networks
- Conducted literature reviews and wrote lab learning material, library documentation, and publications

Cybersecurity Intern, AT&T June 2023-August 2023

ML-Driven Fraud Detection Project with the Research and Innovation in Security Engineering Team

- Developed Machine Learning models for sim swap fraud detection across call logs to streamline the confirmation of fraud cases with the Research and Innovation in Security Engineering Team (FastAI)
- Researched and implemented word-based and phrase-based sentiment identification algorithms for the text highlighting of words commonly associated with fraud cases
- Work now deployed in AT&T's internal fraud detection app that attempts to confirm or deny thousands of customer fraud cases every day

CVE Analysis Project with the Application Vulnerability Team

- Created mechanized reports in order to assess the impact of repeated vulnerabilities (CVEs) across the application landscape and inform targeted remediation efforts
- Web scraped CVE data and processed internal vulnerability data (Beautifulsoup, PySpark, DataBricks)
- Collaborated with the AI Tiger group to brainstorm AI-driven solutions for vulnerability remediation efforts

Research Apprentice, NSF XSEDE Empower Program January 2021-May 2021

Predicting Mental Health Outcomes with Deep Learning Project

- Researched the use of deep learning for community assessment of mental health, using US Census Bureau data, CDC data, TACC's Stampede2 supercomputer, and geospatial analysis
- Developed and compared the performances of a linear regression model, a multilayer perceptron, and a convolutional neural network that all predict the risk level of California counties for suicide based on community features (Sklearn, Pytorch)

High-Performance Computing Support, Pomona College August 2020-May 2021

Observing Trends in Technical Skill Demand Project

- Researched market trends in skill demand with Pomona Economics professors, using topic modeling
- Processed and visualized data in Python and R

Teaching Experience

Computer Systems – Teaching Assistant, Pomona College August 2023-Present

English Conversation – Teacher (Volunteer), Liberty in North Korea August 2022-December 2022

Introduction to Computer Science – Teaching Assistant, Pomona College January 2021-May 2021

Industry Work Experience

Meta University Engineering Intern – Android, Meta Platforms Inc. May 2022-August 2022

- Created a fully functional Android social media app from scratch: SurfStop (Java)
- Implemented a weather API, a Parse backend running on top of MongoDB, data offline persistence (Room ORM), ephemeral timeline posting through database auto-purging using ParseCloud job executions (JavaScript) and an AlarmManager (Java), etc.
- Deployed custom in-app beach state image classifier with web-scraped image data (Keras) (Model's Github)

Skills

Technical: Proficient in Python, Java; Experienced in Deep Learning (TensorFlow/Keras, Pytorch, Fastai), Federated Learning (TensorFlow Federated), Adversarial Machine Learning, Natural Language Processing, Computer Vision, Android Mobile Development, Jupyter Notebook, C, Git, Linux, DataBricks, Data Processing and Visualization, CAD, soldering

Language: English (native), Korean (intermediate, conversational), Spanish (elementary)

Honors

Academic: Marshall Scholarship Finalist, Pomona College Scholar (Top 20% of class), SCIAC All-Academic Team, National AP Scholar

Athletic (Water Polo): Division 1 All CIF-SS Third Team Selection, CIF-SS Jim Staunton Champions for Character Award, All-Trinity League First Team Selection, 2019 CIF-SS Division 1 Regional State Champion

Extracurricular Activities

Surf Club, Spotlight Musical Theatre, Greenroom Theatre, Korean Student Association, Association for Computing Machinery-Women