5 Palermo St.
Cambridge, MA 02141

Jonah O'Brien Weiss

https://jonahobw.github.io

(774) 312 1209
jgow98@gmail.com

SUMMARY

Results-driven Research Engineer with a Master's in Computer Systems Engineering and expertise in deep learning, computer vision, and applied AI research. Proven ability to translate state-of-the-art research into shippable products, fine-tune cutting-edge models and deliver tangible solutions for complex challenges.

EDUCATION

University of Massachusetts Amherst Graduation May 2023
Master of Science in Computer Systems Engineering GPA: 3.96

- Thesis: *A Model Extraction Attack on Deep Neural Networks Running on GPUs.*
- Gave a research presentation and won 2nd Place in poster competition at New England Hardware Security Day.
- Departmental Three Minute Thesis winner for presenting my research to a nontechnical audience.

University of Massachusetts Amherst – Commonwealth Honors College May 2021
Bachelor of Science in Computer Systems Engineering, Minor in Philosophy GPA: 3.90

- Thesis: *Towards Mitigating Adversarial Attacks on Neural Networks via Hybrid Neural Network Decision Tree Architecture*

EXPERIENCE

Research Engineer, Computer Vision/Image Processing, *The MathWorks, Natick, MA* August 2023-Current

- Performed literature surveys and implemented state-of-the-art research into computer vision products.
- Fine-tuned a multimodal embedding model for use in industrial anomaly classification and segmentation tasks.
- Investigated compression methods for physics-informed neural networks on edge devices.
- Shipped 5 image metrology tools with proprietary snap-to-edge functionality for automated measurements.
- Implemented industry standard template-matching algorithms from expired Cognex PATMAX patent.
- Validated performance of a new loss function for a 3D pose estimation model and designed an interface for it.
- Trained and coached colleagues and customers on deep learning in MATLAB, PyTorch, and TensorFlow.

Robotics Software Engineering Intern, *Amazon Robotics, Westborough, MA* May 2022-August 2022

- Designed, architected, and implemented C++ software for a semi-autonomous, mobile manipulation robot.
- Wrote synchronized perception (OpenCV), motion planning, and control orchestration microservices in C++.
- Collaborated with mechanical and electrical engineers as part of a small research group.
- Ran live robot demos for Amazon Robotics Leadership and external stakeholders.

Data Science Intern, *Tesla, Palo Alto, CA* May 2021-August 2021

- Led the Energy Reliability team's transition to a proprietary hardware test automation framework in Python.
- Debugged multi-threaded Python programs to optimize framework's performance for long-running tests.
- Completed ad-hoc data analyses on Tesla's fleet telemetry using Python and Spark for various stakeholders.

Security Engineering Intern, *Dell Technologies, Hopkinton, MA* June 2020-August 2020

- Developed a cryptographically secure supply-chain component verification solution for Dell storage platforms.
- Built a RESTful service using Python, Flask, SwaggerUI, and MongoDB as a proof of concept.

PAPERS/PROJECTS

Kim, Dong Hyub, Jonah O'Brien Weiss, and Sandip Kundu. **"Extracting DNN Architectures via Runtime Profiling on Mobile GPUs."** IEEE Journal on Emerging and Selected Topics in Circuits and Systems (2024).

Weiss, Jonah O'Brien, Tiago Alves, and Sandip Kundu. **"EZClone: Improving DNN Model Extraction Attack via Shape Distillation from GPU Execution Profiles."** arXiv preprint arXiv:2304.03388 (2023).

Weiss, Jonah O'Brien, Tiago Alves, and Sandip Kundu**. "Hardening DNNs against Transfer Attacks during Network Compression using Greedy Adversarial Pruning."** IEEE 4th International Conference on Artificial Intelligence Circuits and Systems. (2022).

EXPERIENCED IN

Python, C, C++, MATLAB, Git, PyTorch, TensorFlow, Pandas, OpenCV, Point Cloud Library, Docker, Linux, AWS.