

Jacob M. Springer

500 College Ave, Swarthmore, PA 19081

✉ jacmspringer@gmail.com

📞 Jacob M. Springer

🌐 jakespringer

🔗 sprin.xyz

EDUCATION

Swarthmore College

BA, Mathematics and Computer Science, GPA 3.86

Swarthmore, PA

August 2017 – December 2021

RELEVANT SKILLS & CLASSWORK

Python • C/C++ • Java • CUDA • TensorFlow • Keras • PyTorch • Algorithms • Deep Learning
• Neuromorphic Computing • Linear Algebra • Calculus • Probability • Neurobiology • Robotics

WORK EXPERIENCE

Los Alamos National Laboratory

Researcher in Machine Learning & Computational Neuroscience

Los Alamos, NM

June 2018 – Present

- Advised by Dr. Garrett T. Kenyon
- Demonstrated that classifiers based on biologically-plausible machine learning models (deep sparse coding) are robust to certain types of adversarial attacks
- Explored applications of biologically-plausible machine learning in video compression
- Investigated the limits of deep learning with respect to the lottery ticket hypothesis
- Discovered a relationship between semantically meaningless non-robust features and more interpretable robust features that helps to explain the non-robust component of neural networks
- Developed highly transferable targeted adversarial examples based on universal features

MIT CSAIL

Researcher in Machine Learning

Cambridge, MA

June 2020 – August 2020

- Advised by Dr. Una-May O'Reilly
- Developed a novel and highly efficient gradient-free black-box adversarial attack targeting neural models of source code

Portland State University

Researcher in Computer Security Education

Portland, OR

June 2017 – August 2017

- Advised by Professor Wu-chang Feng
- Developed a collection of scaffolded capture-the-flag and an associated curriculum to teach symbolic execution in CS 492/592: Malware Reverse Engineering at Portland State University
- The capture-the-flag challenges have been released as an open-source project

CDK Global

Software Development Intern

Portland, OR

June 2016 – August 2016

- Worked in a team on an internal project to develop a Chrome extension in JavaScript to provide useful widgets for developers
- Used JavaScript to develop the frontend to a project to index internal data to be searchable using Elasticsearch as a week-long hackathon project

Autodesk

Software Development Intern

Portland, OR

June 2015 – August 2015

- Worked in a team to continue the development of Autodesk's Synthesis project a robot simulator for the FIRST Robotics Challenge
- Developed a platform in C++ (and analogous Java bindings) to emulate code on a simulated robot

PUBLICATIONS & MANUSCRIPTS

- Jones, Haydn T*; **Springer, Jacob M***; Moore, Juston; Kenyon, Garrett T. Representation Similarity in Robust Neural Networks. In progress. (Co-first author.)
- **Springer, Jacob M**; Mitchell, Melanie; Kenyon, Garrett T. A Little Robustness Goes a Long Way: Leveraging Universal Features for Targeted Transfer Attacks. Advances in Neural Information Processing Systems (NeurIPS). 2021.
- **Springer, Jacob M**; Mitchell, Melanie; Kenyon, Garrett T. Uncovering Universal Features: How Adversarial Training Improves Adversarial Transferability. ICML 2021 Workshop on Adversarial Machine Learning. 2021. (Shorter version of above.)
- **Springer, Jacob M**; Mitchell, Melanie; Kenyon, Garrett T. Adversarial Perturbations Are Not So Weird: Entanglement of Robust and Non-Robust Features in Neural Network Classifiers. Preprint. 2021.
- **Springer, Jacob M**; Reinstadler, Bryn Marie; O'Reilly, Una-May. STRATA: Simple, Gradient-Free Attacks for Models of Code. 3rd Workshop on Adversarial Learning Methods for Machine Learning and Data Mining @ KDD. 2021.
- **Springer, Jacob M**; Kenyon, Garrett T. It's Hard for Neural Networks To Learn the Game of Life. International Joint Conference on Neural Networks (IJCNN). 2021.
- Wang, Daniel A; Strauss, Charles MS; **Springer, Jacob M**; Thresher, Austin; Pritchard, Howard; Kenyon, Garrett T. Sparse MP4. IEEE Southwest Symposium on Image Analysis and Interpretation (SSIAI). 2020.
- **Springer, Jacob M**; Strauss, Charles S; Thresher, Austin M; Kim, Edward; Kenyon, Garrett T. Classifiers based on deep sparse coding architectures are robust to deep learning transferable examples. Preprint. 2018.
- **Springer, Jacob M**; Feng, Wu-chang. Teaching with Angr: A Symbolic Execution Curriculum and CTF. USENIX Workshop on Advances in Security Education (ASE). 2018.

AWARDS & ACHIEVEMENTS

- Barry M. Goldwater Scholarship, 2020
- Finalist, National Merit Scholarship, 2017

NOTABLE PROJECTS

- Angr-y CTF, a collection of capture-the-flag challenges for teaching symbolic execution using the Angr symbolic execution library, github.com/jakespringer/angr_ctf (400+ stars, 80+ forks)
- Swarthmore College Robotics Club (SRC), founded and run a robotics team to build a robot to compete in the Micromouse competition; competition was canceled due to COVID-19