
Education

- 2017 - 2021 **Massachusetts Institute of Technology (MIT)**, Cambridge, MA
B.S. in Computer Science and Engineering, B.S. in Mathematics, Minor in Economics
GPA: 5.0/5.0
Relevant Coursework: Machine Learning, Advances in Computer Vision, Computational Cognitive Science, Cryptography & Cryptanalysis, Algorithms, Information Theory
- 2014 - 2017 **Garnet Valley High School**, Garnet Valley, PA
Class Rank: 1 (out of 410)

Experience

- Jun 2021 - Present **Google**, Security & Anti-Abuse Research Team
Software Engineer II, advised by Elie Bursztein
- o Robust and Scalable NLP-based Protections
 - Building adversarially robust, efficient, and scalable NLP models and text embeddings using deep similarity learning [1, 2]. These models currently protect many products (Gmail, YouTube, Google Workspace, Google Drive, and Google Forms) from abusive content such as malware, phishing and spam campaigns.
 - o Machine Learning for Security Applications
 - Developing deep learning models for security use cases, including client-side malicious URL detection for end-to-end encrypted environments, defenses against PDF malware and phishing attacks, breached password detection, and side channel attacks on cryptographic hardware [3].
 - Leveraging large language models (LLMs) to build novel solutions to long-standing security and privacy problems, e.g. synthetic data generation and code deobfuscation.
 - o Security and Reliability of LLMs
 - Conducting research on the trustworthiness, robustness, and security vulnerabilities of LLMs, including on-device content safety protections (Google I/O 2023 demo) and hallucination detection.
- Sep 2020 - Jun 2021 **University of Pennsylvania**, Department of Neuroscience
Research Assistant, advised by Prof. Wenqin Luo
- o Designed the convolutional recurrent neural network (CRNN) used for Scratch-AID, a deep learning-based tool which can automatically identify and quantify mouse scratching behavioral patterns from raw video footage. Paper published in journal (eLife) [4].
 - o Investigated the neurobiological relationship between behavioral states and breathing patterns using clustering techniques; built a classifier capable of distinguishing between 9 different behavioral states in rodents using breathing recordings. Paper published in journal (iScience) [5].
- Jun 2020 - Aug 2020 **Google**, Security & Anti-Abuse Research Team
Software Engineer Intern, advised by Elie Bursztein
- o Built a deep-learning model training framework for security research, which supported state-of-the-art model training techniques including hyperparameter tuning, semi-supervised labeling, and transfer learning.
 - o Designed and wrote a TensorFlow/Keras package which automates searching for and applying the best data augmentation policies during model training.

- Sep 2019 - Dec 2019 **MIT CSAIL**, Medical Vision Group
Research Assistant, advised by Prof. Polina Golland
- o Built an ML model for automatically quantifying the severity of pulmonary edema from patients' x-ray images and radiology reports, helping to improve clinicians' abilities to provide more accurate and personalized treatment plans for heart failure patients.
- Jun 2019 - Aug 2019 **Microsoft**, Edge Browser Experiences Team
Software Engineer Intern
- o Designed and added the quick-access Favorites toolbar button and drop-down menu in Microsoft Edge. This feature was shipped to all users.
- Sep 2017 - Jun 2018 **MIT**, Department of Economics
Research Assistant, advised by Prof. Daron Acemoglu
- o Investigated historical trends of technological change and innovation using statistical methods applied to U.S. agriculture data and economic records.

Papers

- [1] **M. Zhang**, O. Vallis, A. Bumin, T. Vakharia, and E. Bursztein. "RetSim: Resilient Text Similarity." *Under Submission*, 2023.
- [2] E. Bursztein, **M. Zhang**, O. Vallis, X. Jia, and A. Kurakin. "RETVec: Resilient and Efficient Text Vectorizer." *Under Submission*, 2023. [arXiv:2302.09207](https://arxiv.org/abs/2302.09207).
- [3] E. Bursztein, L. Invernizzi, K. Král, D. Moghimi, J.M. Picod, and **M. Zhang**. "Generic Attacks against Cryptographic Hardware through Long-Range Deep Learning." *Under Submission*, 2023. [arXiv:2306.07249](https://arxiv.org/abs/2306.07249).
- [4] H. Yu, J. Xiong, A. Y. Ye, S. L. Cranfill, T. Cannonier, M. Gautam, **M. Zhang**, R. Bilal, J. Park, Y. Xue, V. Polam, Z. Vujovic, D. Dai, W. Ong, J. Ip, A. Hsieh, N. Mimouni, A. Lozada, M. Sosale, A. Ahn, M. Ma, L. Ding, J. Arsuaga, and W. Luo. "Scratch-AID: A Deep-learning Based System for Automatic Detection of Mouse Scratching Behavior with High Accuracy." *eLife* Vol. 11:e84042, 2022. [doi:10.7554/eLife.84042](https://doi.org/10.7554/eLife.84042).
- [5] E. Janke, **M. Zhang**, S. Ryu, J. Bhattarai, M. R. Schreck, A. H. Moberly, W. Luo, L. Ding, D. W. Wesson, and M. Ma. "Machine Learning-based Clustering and Classification of Mouse Behaviors via Respiratory Patterns." *iScience* Vol. 25 (12):105625, 2022. [doi:10.1016/j.isci.2022.105625](https://doi.org/10.1016/j.isci.2022.105625).

Honors

- 2020 Tau Beta Pi (TBP) Honor Society
- 2020 Eta Kappa Nu (HKN) Honor Society
- 2020 MIT Undergraduate Research and Innovation Scholar
- 2019 2x ITA Scholar-Athlete Award
- 2017 National Merit Scholarship Winner
- 2017 National AP Scholar

Activities

- 2022 - Present **Google Intern Host**
Hosted/co-hosted two Research Scientist interns and two SWE interns at Google
- 2020 - 2021 **MIT HKN Tutor for EECS**
Tutor for 6.009 Fundamentals of Programming and 6.006 Introduction to Algorithms
- 2019 - 2020 **MIT xFair Committee**
Organizational committee for xFair, MIT's largest student-run career fair and tech expo
- 2017 - 2019 **MIT Varsity Tennis Team**
2x NCAA Elite 8; 2x ITA Scholar-Athlete Award; 2x NEWMAC First Team All-Conference