Liam Fowl

✉ Email: lfowl@umd.edu
☎ Cell Phone: +1(443)845-9206

EDUCATION

PhD in Mathematics Sept 2016 - Expected: Spring 2022
University of Maryland, College Park, MD, USA
Advised by Professor Tom Goldstein (CS) and Professor Wojtek Czaja (Math).
GPA: 4.0/4.0

BS in Mathematics Sept 2012 - May 2016
University of Maryland, College Park, MD, USA
High honors in Mathematics, with a minor in Physics.
GPA: 3.9/4.0

EXPERIENCE

University of Maryland September 2016 - Present
Graduate Research/Teaching Assistant

- Developed state-of-the-art indiscriminate, targeted, and backdoor data poisoning attacks for deep neural networks.
- Developed state-of-the-art attacks on privacy in federated learning.
- Courses taught include: Calculus 1, 2, and 3 as well as Statistics, and Introduction to Machine Learning.

National Institute of Health May 2017 - January 2018
Researcher

- Developed analytic methods for extraction of coefficients in bi-exponential decay models.
- Implemented computational method for extraction of coefficients and improved performance over non-linear least squares method.

RESEARCH INTERESTS

My research has primarily focused on robustness and security of deep learning models. Specifically, I have published research on adversarial robustness, data poisoning attacks on deep networks, and, more recently, privacy attacks against both language and vision models trained in a federated learning setting.

Keywords: Deep Learning, Adversarial Machine Learning, Machine Learning. Security, Computer Vision, NLP, Language Models, Federated Learning, Mathematical Machine Learning.

PROJECTS AND PUBLICATIONS

New Projects

[1] **Fowl*, L.**, Geiping*, J., Reich, S., Wen, Y., Goldblum, M., & Goldstein, T. *Decepticons: Corrupted Transformers Breach Privacy in Federated Learning for Language Models.* https://arxiv.org/abs/2201.12675. Under review.

[2] Wen*, Y., Geiping*, J., **Fowl*, L.**, Goldblum, M., & Goldstein, T. *Fishing for User Data in Large-Batch Federated Learning via Gradient Magnification.* https://arxiv.org/abs/2202.00580. Under review.

[3] Souri, H*, **Fowl*, L.**, Chellappa, R., Goldblum, M., & Goldstein, T. *Sleeper Agent: Scalable Hidden Trigger Backdoors for Neural Networks Trained from Scratch.* https://arxiv.org/abs/2106.08970. Under review.

[4] Geiping, J., **Fowl, L.**, Somepalli, G., Goldblum, M., Moeller, M., & Goldstein, T. (2020). *What Doesn't Kill You Makes You Robust(er): Adversarial Training against Poisons and Backdoors.* https://arxiv.org/abs/2102.13624. Under review.

[5] Somepalli, G., **Fowl, L.**, Bansal, A., Yeh-Chiang, P., Dar, Y., Baraniuk, R., Goldblum, M., Goldstein, T. *Can You Learn the Same Model Twice? Investigating Reproducibility and Double Descent from the Decision Boundary Perspective.* Under review.

Selected Publications

[6] **Fowl*, L.**, Geiping*, J., Czaja, W., Goldblum, M., & Goldstein, T. *Robbing the FED: Directly Obtaining Private Data in Federated Learning with Modified Models.* Accepted for Publication in the International Conference on Learning Representations **(ICLR)** 2022.

[7] **Fowl*, L.**, Goldblum*, M., Chiang, P., Geiping, J., Czaja, W., & Goldstein, T. *Adversarial Examples Make Strong Poisons!* Advances in Neural Information Processing Systems **(NeurIPS)**, 2021.

[8] Geiping*, J., **Fowl*, L.**, Huang, W. R., Czaja, W., Taylor, G., Moeller, M., & Goldstein, T. *Witches' Brew: Industrial Scale Data Poisoning via Gradient Matching.* International Conference on Learning Representations **(ICLR)**, 2021.

[9] Goldblum*, M., **Fowl*, L**., & Goldstein, T. *Adversarially robust few-shot learning: A meta-learning approach.* Advances in Neural Information Processing Systems **(NeurIPS)**, 2020.

[10] Goldblum*, M., **Fowl*, L.**, Feizi, S., & Goldstein, T. *Adversarially robust distillation.* In Proceedings of the **AAAI** Conference on Artificial Intelligence 2020.

[11] Goldblum, M., Reich*, S., **Fowl*, L.**, Ni*, R., Cherepanova*, V., & Goldstein, T. *Unraveling meta-learning: Understanding feature representations for few-shot tasks.* In International Conference on Machine Learning **(ICML)** 2020.

[12] Huang*, W. R., Geiping*, J., **Fowl, L.**, Taylor, G., & Goldstein, T. (2020). *Metapoison: Practical general-purpose clean-label data poisoning.* Advances in Neural Information Processing Systems **(NeurIPS)**, 2021.

[13] Borgnia*, E., Cherepanova*, V., **Fowl*, L.**, Ghiasi*, A., Geiping*, J., Goldblum*, M., ... & Gupta*, A. *Strong Data Augmentation Sanitizes Poisoning and Backdoor Attacks Without an Accuracy Tradeoff.* In IEEE International Conference on Acoustics, Speech and Signal Processing **(ICASSP)** 2021.

[14] Abdelkader*, A., Curry*, M. J., **Fowl*, L.**, Goldstein*, T., Schwarzschild*, A., Shu*, M., ... & Zhu*, C. *Headless Horseman: Adversarial Attacks on Transfer Learning Models.* In IEEE International Conference on Acoustics, Speech and Signal Processing **(ICASSP)** *(Spotlight)* 2020.

Preprints and Workshop Publications

[15] **Fowl*, L.**, Goldblum*, M., Gupta, A., Sharaf, A., & Goldstein, T. (2020). *Random Network Distillation as a Diversity Metric for Both Image and Text Generation.* In **NeurIPS** 2020 Workshop on Dataset Curation.

[16] **Fowl*, L.**, Chiang*, P., Goldblum*, M., Geiping, J., Bansal, A., Czaja, W., & Goldstein, T. *Preventing Unauthorized Use of Proprietary Data: Poisoning for Secure Dataset Release.* In **NeurIPS** 2020 Workshop on Dataset Curation.

[17] Huang, W. R., Emam, Z., Goldblum, M., **Fowl, L.**, Terry, J. K., Huang, F., & Goldstein, T. *Understanding generalization through visualizations.* arXiv:1906.03291.

[18] Peri, N., Gupta, N., Huang, W. R., **Fowl, L.**, Zhu, C., Feizi, S., ... & Dickerson, J. P. *Deep k-nn defense against clean-label data poisoning attacks.* In European Conference on Computer Vision **(ECCV)**AROW workshop.

COMMUNITY INVOLVEMENT

Reviewer - ICLR: 2020, 2021, NeurIPS: 2020, 2021, CVPR: 2021	Sept 2020-Present
Organizer Deep Learning Research Interaction Team (RIT) at UMD	Sept 2018 - Present
Organizer and Student Liaison - Norbert Wiener Center Seminar	Sept 2018 - Present
Organizer - UMD Data Science Day	Mar 2019
Volunteer - Girls Excelling in Math and Science (GEMS)	Sept 2016 - Jun 2018
Tutor - Northwestern High School (Prince George's County MD)	Sept 2015 - Jun 2018
Mentor - Directed Reading Program at UMD	Sept 2016 - Jun 2018

AWARDS

Banneker-Key Scholarship - Most prestigious full scholarship given to top 1% of incoming students at UMD.

Aziz Mathematics Scholarship - Given once per year to the top undergraduate student in Mathematics.

Outstanding Senior Award - Given at the end of each year to the top graduating senior in Mathematics each year.

Award for Excellence in Teaching - Given to graduate students who have demonstrated excellent teaching abilities.

Wiley Dissertation Fellowship - Fellowship given to a select few graduate students for dissertation writing.