Dzung V. Pham

Contact Information	Security and Privacy Lab (Rm. 226) Computer Science Building 140 Governors Drive, Amherst, MA 01003, USA	*Mobile:* +1 (413) 629-9759 *E-mail:* dzungvpham@gmail.com *Website:* `dzungvpham.github.io`

Research Interests

My research focus is at the intersection of security, privacy, and AI/ML algorithms and systems. Currently, I am investigating how to leverage and improve the reasoning capability of on-device large language models to provide privacy protection for users.

Keywords: security and privacy, machine learning, federated learning, differential privacy, large language models, the web.

Education

University of Massachusetts Amherst **2022 - Present**

MS/PhD in Computer Science (GPA: 4.00)
Advisor: Prof. Amir Houmansadr.
Research Group: The Secure, Private Internet Research Group (`SPIN`).

Williams College **2016 - 2020**

B.A. in Computer Science & in Statistics (with Honors) (GPA: 3.90)
Thesis: *Exploring Variable Importance with Stacked Models.* Advisor: Prof. Richard D. De Veaux.
Honors: Magna cum laude, Sigma Xi, Phi Beta Kappa, Mu Sigma Rho.
Awards: Recipient of the 2019 Ward Prize for Best Project in Computer Science.

Publications

Dzung Pham, Jade Sheffey, Chau Minh Pham, Amir Houmansadr, "ProxyGPT: Enabling Anonymous Queries in AI Chatbots with (Un)Trustworthy Browser Proxies." `https://arxiv.org/abs/2407.08792`. Preprint, under review.

Dzung Pham, Shreyas Kulkarni, Amir Houmansadr. "RAIFLE: Reconstruction Attacks on Interaction-based Federated Learning with Adversarial Data Manipulation." In *Network and Distributed System Security (NDSS) Symposium,* 2025. `https://arxiv.org/abs/2310.19163`.

Quan Do, Kiersten Campbell, Emmie Hine, Dzung Pham, Alex Taylor, Iris Howley, Daniel Barowy. "Evaluating ProDirect Manipulation in Hour of Code." In *Proceedings of the 2019 ACM SIGPLAN SPLASH-E Symposium (SPLASH-E '19).* `dl.acm.org/doi/10.1145/3358711.3361623`.

Industry Experiences

Meta Platforms (Facebook), Inc.,

Software Engineer – Machine Learning **2020 - 2022**

- Trained and deployed a wide variety of ML models to identify and prevent fraud, scams, and harassment on Facebook Marketplace.
- Built and maintained scalable and reliable ML backend infrastructure to support the integrity of Marketplace for billions of daily interactions.

Software Engineer Intern **Summer 2018 & 2019**

- Built two internal tools to support software release engineers with managing version releases and debugging software build failures.
- Trained and deployed a ranking ML model to help Facebook employees discover internal job opportunities based on their career history, skills and preferences.

Undergraduate Research Experiences

Exploring Variable Importance with Stacked Models - Senior Thesis **2019 - 2020**
Evaluated the robustness of variable importance measures calculated from stacked models compared to individual models and found that the ensemble diversity can impact robustness.
Advisor: Prof. Richard De Veaux. `https://doi.org/10.36934/t2020-099`.

Fall Detection - Winter Research Project **2019**
Designed and trained a two-stream convolutional neural network with transfer learning from MobileNetV2 to detect people falling in video input using Keras, TensorFlow, and OpenCV, and Motion History Image. The project won the 2019 Ward Prize for Best Project in Computer Science.
Advisor: Prof. Duane Bailey. `github.com/dzungvpham/fall-detection-two-stream-cnn`.

SWELL - Research Assistant **2018 - 2019**
Designed and implemented major parts of the SWELL graphical programming language, including the parser, interpreter, and programming user interface. Taught the language to 5th-grade students at Williamstown Elementary School and evaluated its effectiveness in teaching beginners coding.
Advisor: Prof. Dan Barowy. `http://swell-lang.org/index.html`.

Teaching & Mentorship Experiences

PhD Mentor - UMass Center for Data Science **2024 - Present**
Currently mentoring a group of UMass Computer Science Master's students in collaboration with industry researchers from Google Research and Meta's FAIR Lab on evaluating the privacy property of zero-th order machine learning algorithms via membership inference attacks.

Teaching Assistant - University of Massachusetts Amherst **2022 - Present**
Courses: Intro to Computer and Network Security, Programming Methodology, Web Programming

Teaching Assistant - Williams College **2017 - 2020**
Courses: Statistical Learning & Data Mining, Regression & Forecasting, Principles of Programming Languages, Algorithm Design & Analysis, Computer Organization, Data Structures & Advanced Programming, Introduction to Computer Science.

Talks

Guest Lecture - UMass First Year Seminar: Exploring Modern Computing **2024**
Large Language Models and User Privacy

Computer Science Colloquium - Williams College **2023**
On the Challenges of Building Privacy-preserving Chatbot Services

Services

Reviewer: The WebConf 2025, IMC 2025

Computer Science Student Advisory Committee - Williams College **2018 - 2019**
Organized the first mock tech interview program in the Computer Science department at Williams College to help fellow students apply for software engineering jobs in the tech industry.