TEACHING STATEMENT

Fnu Suya

A teacher's core responsibility is to facilitate learning and effectively impart knowledge. This requires foundational elements such as deep knowledge of the subject, well-prepared materials, and engaging examples. These are basic yet essential aspects of teaching. Building upon this foundation, my teaching philosophy strongly emphasizes *understanding each student's background* and *uniquely and continuously tailoring my teaching approach* to meet their individual learning styles and needs. This approach, grounded in the belief that there is no one-size-fits-all solution in education, has shown promise in enhancing student learning and success [1, 2]. I am enthusiastic about the opportunity to teach both undergraduate and graduate courses, with a particular focus on machine learning, cybersecurity, and the broader ethical and societal implications of technology.

1 Teaching Experiences

During my doctoral studies at Arizona State University (ASU) and the University of Virginia (UVa), I took on multiple roles, including as a teaching assistant for various undergraduate and graduate courses, and giving a guest lecture on adversarial examples in a mobile security class. These roles highlighted the importance of tailoring teaching strategies to students' diverse backgrounds and educational needs.

Undergraduate teaching. In an introductory C++ programming lab session designed for first-year non-CS majors at ASU, I encountered a unique challenge: the course material was somewhat ahead of the lab sessions, leading to a gap in the students' immediate recall of relevant content. This was particularly evident as the students, coming from non-CS majors like business and economics, might not prioritize programming. To address this, I restructured the lab sessions to start with a brief 10-15 minute overview of the pertinent content before students began working on coding problems. This adjustment allowed for a more effective learning environment, as evidenced by the increased efficiency in the class and the heartfelt thank-you emails I received at the end of the semester.

Graduate teaching. My role as a teaching assistant for a graduate-level Game Theory course at ASU presented me with an opportunity to engage deeply with PhD students who had a sufficient mathematical background. I deviated from traditional lecturing methods with slides, choosing instead to conduct interactive whiteboard sessions. This hands-on approach allowed for a more thorough exploration of mathematical concepts in game theory. It encouraged active student participation, where they contributed to theorem derivations and discussions, thereby significantly enhancing their engagement and comprehension. While delivering a guest lecture on adversarial examples in a mobile security class at UVa, I crafted my own lecture slides, including visualizations to capture the students' interest, and delved deeper into the technical aspects while ensuring comprehensibility. In particular, when explaining why deep learning models are vulnerable to adversarial examples, instead of showing the formula commonly found in research papers, I used logistic regression as an example and showed, with concrete numbers, how adding a small perturbation in every dimension of the image (the ℓ_∞-attack in adversarial example literature) can lead to completely flipped model prediction in binary classification. This explanation helped better illuminate why machine learning models can be susceptible to adversarial examples.

2 Mentoring Experience

Teaching extends beyond classroom instruction, with student mentoring and advising forming critical components of a professor's role. It is essential to adjust mentoring strategies based on each student's background, knowledge level and personal goals. I am committed to listening to students, understanding their unique situations, and providing direction and feedback that fosters their development as independent researchers.

Adjust styles based on seniority. Throughout my PhD and postdoctoral experiences, I have had the opportunity to mentor a diverse group of senior undergraduate and both junior and senior PhD students. My mentoring approach

varies depending on the student's level and their knowledge background. At UVa, I worked with senior undergraduate students who had limited prior research experience. I helped them identify promising research problems and provided concrete tasks towards completing research papers. My involvement was hands-on, involving detailed discussions and problem-solving, such as debugging code implementations. This approach ensured that their research progressed in a promising direction and led to exciting results: the students who worked with me over extended periods successfully published papers [3, 4], including one that won the best paper award [3], and secured positions to pursue PhDs at different universities. For example, Evan Rose, the lead author of Rose et al. [3], is now pursuing a PhD at Northeastern, and Tingwei Zhang, the co-author of Suya et al. [4], is pursuing a PhD at Cornell. When mentoring senior PhD students, such as Yulong Tian from Nanjing University, my style shifted to providing high-level guidance, such as designing research agendas and offering strategic solutions to technical challenges. In paper writing, I played a significant role, ensuring the paper delivers a compelling and coherent story. Our collaborative efforts resulted in two papers accepted to top-tier journal [5] and conference [6].

Adjust styles based on backgrounds and foster independent thinking. I also tailor my mentoring to their unique backgrounds. Since my postdoc at the University of Maryland, College Park, I've been mentoring two first-year PhD students with different expertise on a project on leveraging machine learning for malware detection. For the student with a strong background in machine learning, I suggested engaging with advanced models for malware detection. Conversely, for the student with system-level experience, I recommended delving into case studies on malware behavior, aiming to gain a deeper understanding of the limitations and failures of current machine learning models. This personalized approach maximizes each student's strengths and learning opportunities. While I believe in a hands-on approach for junior students, I also understand the importance of fostering independent thinking. For instance, when students seek advice on whether a particular experiment should be run, I encourage them to articulate their goals and assess alignment with our research objectives, stepping in with my reasoning when necessary. I was happily surprised with some of their smart ideas during this process. This balance of guidance and independence is crucial for growing research skills.

Provide critical feedback and support wellness. As an advisor, my aim is to provide critical feedback throughout the research journey. Research comes with inherent challenges, including the unpredictability of the review process, limited external feedback, and peer pressures, all of which can adversely affect students' mental health and impede the quality of their work. I deeply empathize with their anxieties, having faced similar doubts myself, particularly during significant personal life changes. These experiences have highlighted the importance of supportive advisors, for which I have been fortunate. I am committed to offering the same level of encouragement and guidance to my students, encouraging them to focus on their personal growth. I will ensure they receive the necessary external validation to build confidence in their achievements and develop into strong, capable researchers for the future.

References

[1] Hanna Dumont and Douglas D Ready. On the promise of personalized learning for educational equity. *Npj science of learning*, 8(1):26, 2023.

[2] John F Pane, Elizabeth D Steiner, Matthew D Baird, and Laura S Hamilton. Continued progress: Promising evidence on personalized learning. *Rand Corporation*, 2015.

[3] Evan Rose, Fnu Suya, and David Evans. Poisoning attacks and subpopulation susceptibility. In *Workshop on Visualization for AI Explainability (VISxAI)*, 2022.

[4] Fnu Suya, Anshuman Suri, Tingwei Zhang, Jingtao Hong, Yuan Tian, and David Evans. Sok: Pitfalls in evaluating black-box attacks. *arXiv preprint arXiv:2310.17534*, 2023.

[5] Yulong Tian, Fnu Suya, Fengyuan Xu, and David Evans. Stealthy backdoors as compression artifacts. *IEEE Transactions on Information Forensics and Security*, 2021.

[6] Yulong Tian, Fnu Suya, Anshuman Suri, Fengyuan Xu, and David Evans. Manipulating transfer learning for property inference. In *IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2023.