Kyle Domico

PhD Student and Research Assistant

+1 (814) 933-4303 domico@cs.wisc.edu kyle-domico kyledomico kyledomico.com

Summary

I am a PhD Student in the School of Computer, Data, and Information Sciences at the University of Wisconsin-Madison. I am a research assistant in the MadS&P computer security group and advised by Dr. Patrick McDaniel. My research interests lie at the intersection of computer security and reinforcement learning. In current work, I'm evaluating the efficacy of adversaries using reinforcement learning algorithms to craft adversarial samples on machine learning models.

Education

Ph.D. Computer Sciences | University of Wisconsin-Madison — Sep 2023 - *Present*

- Adviser: Dr. Patrick McDaniel
- Doctoral Minor: Statistics

M.S. Computer Sciences | University of Wisconsin-Madison — Sep 2023 - May 2025

- Adviser: Dr. Patrick McDaniel
- Thesis Title: "Generalist Adversarial Policies in Black-Box Settings"
- Thesis Committee: Prof. Patrick McDaniel, Prof. Josiah Hanna, Prof. Rahul Chatterjee

B.S. Computer Science | Pennsylvania State University — Aug 2020 - May 2023

- GPA: 3.86 (Cum Laude)
- Minor: Mathematics

Research Experience

Research Assistant | University of Wisconsin-Madison — July 2023 - *Present*
Madison Security and Privacy Laboratory — Madison, WI

Undergraduate Research Assistant | Pennsylvania State University — February 2021 - May 2023
Systems and Internet Infrastructure Security Laboratory — University Park, PA

Publications

- Eric Pauley, **Kyle Domico**, Blaine Hoak, Ryan Sheatsley, Quinn Burke, Yohan Beugin, Engin Kirda, Patrick McDaniel. "Secure IP Address Allocation at Cloud Scale". In: *Network and Distributed Systems Security Symposium (NDSS 2025)*. Feb. 2025.
- **Kyle Domico**. "Generalist Adversarial Policies in Black-Box Settings". M.S. Thesis. University of Wisconsin-Madison. Aug. 2024.
- Kunyang Li, **Kyle Domico**, Jean-Charles Noirot Ferrand, Patrick McDaniel. "The Efficacy of Transformer-Based Adversarial Attacks in Security Domains". In: *Workshop on Artificial Intelligence for Cyber (MILCOM 2023)*. Nov. 2023. URL: https://arxiv.org/abs/2310.11597
- Eric Pauley, **Kyle Domico**, Blaine Hoak, Ryan Sheatsley, Quinn Burke, Yohan Beugin, Patrick McDaniel. "EIPSIM: Modeling Secure IP Address Allocation at Cloud Scale". *ArXiv Preprint*. Oct. 2022. URL: https://arxiv.org/abs/2210.14999
- **Kyle Domico**, Ryan Sheatsley, Yohan Beugin, Quinn Burke, Patrick McDaniel. "A Machine Learning and Computer Vision Approach to Geomagnetic Storm Forecasting". In: *2nd Machine Learning in Heliophysics Conference (ML-HELIO 2022)*. Mar. 2022. URL: https://arxiv.org/abs/2204.05780

Invited Talks and Presentations

A Machine Learning and Computer Vision Approach to Geomagnetic Storm Forecasting — March 2022
ML-Helio 2022 Poster Session — Boulder, CO (Hybrid)

A Machine Learning and Computer Vision Approach to Geomagnetic Storm Forecasting — October 2021
Penn State ICDS Symposium 2021 — University Park, PA

Generalist Adversarial Policies in Black-Box Settings October 2024
UW-Madison Reinforcement Learning Reading Group Madison, WI

Guest Lecture: Machine Learning Security November 2024
UW-Madison CS642: Introduction to Information Security Madison, WI

Achievements & Certifications

- **Alpha Fire Company Scholarship** May 2020
- **Centre County Sports Hall of Fame Scholarship** May 2020
- **UW-Madison Computer Sciences Department Scholarship** September 2023