

# Kyle Domico

PH.D. STUDENT · COMPUTER SCIENCES

1205 University Avenue, Room 4576, Madison, WI 53706, USA

✉ domico@cs.wisc.edu | 🏠 kyledomico.com | 📱 kyledomico | 📺 kyle-domico-4562771b6

## Research Experience

---

### MadS&P - Security and Privacy Research Group at UW-Madison

Madison, WI, USA

RESEARCH ASSISTANT

2023 - Present

- Analyzing the threat landscape of AI systems through reinforcement learning.
- Developing reinforcement learning-based defenses to detect malicious behavior in AI services.
- Collaborating on projects in cloud security and trustworthy machine learning.

### Systems and Internet Infrastructure Security Laboratory

University Park, PA, USA

UNDERGRADUATE RESEARCH ASSISTANT

2021 - 2023

- Designed a machine learning pipeline to predict geomagnetic storms from images of the Sun.
- Collaborated on projects in systems and cloud security.

## Education

---

### University of Wisconsin-Madison

Madison, WI, USA

PH.D. IN COMPUTER SCIENCES

2023 - Present

- Researching the trustworthiness of machine learning systems through reinforcement learning.
- Advisor: Prof. Patrick McDaniel
- Doctoral Minor: Statistics

### University of Wisconsin-Madison

Madison, WI, USA

M.S. IN COMPUTER SCIENCES

2023 - 2025

- Thesis: *Generalist Adversarial Policies in Black-Box Settings*
- Advisor: Prof. Patrick McDaniel
- Thesis Committee: Prof. Patrick McDaniel, Prof. Josiah Hanna, Prof. Rahul Chatterjee

### The Pennsylvania State University

University Park, PA, USA

B.S. IN COMPUTER SCIENCE

2020 - 2023

- Minor: Mathematics
- Rank: *Cum Laude*

## Publications

---

### CONFERENCES

- 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.
- Kunyang Li, **Kyle Domico**, Jean-Charles Noiro Ferrand, Patrick McDaniel. "The Efficacy of Transformer-Based Adversarial Attacks in Security Domains". In: *MILCOM 2023 - Workshop on Artificial Intelligence for Cyber (MILCOM 2023 - Workshop on AI for Cyber)*. Nov. 2023.
- **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.

### PREPRINTS

- **Kyle Domico**, Jean-Charles Noiro Ferrand, Ryan Sheatsley, Eric Pauley, Josiah Hanna, and Patrick McDaniel. "Adversarial Agents: Black-Box Evasion Attacks with Reinforcement Learning". arXiv: 2503.01734 [cs.CR]. Mar. 2025. URL: <https://arxiv.org/abs/2503.01734>.

### THESES

- **Kyle Domico**. "Generalist Adversarial Policies in Black-Box Settings". University of Wisconsin-Madison. Aug. 2024.

## Honors & Awards

---

- 2023 **UW-Madison Computer Sciences Department Scholarship**, University of Wisconsin-Madison
- 2020 **Alpha Fire Company Scholarship**, State College Alpha Fire Company
- 2020 **Centre County Sports Hall of Fame Scholarship**, Centre County Sports Hall of Fame

## Engagement and Public Speaking

---

- *Adversarial Agents: Black-Box Evasion Attacks with Reinforcement Learning*. UW-Madison New CS Graduate Student Welcome Weekend (Poster Presenter). Mar. 2025.
- *Machine Learning Security*. UW-Madison CS 642: Introduction to Information Security (Guest Lecture). Nov. 2024.
- *Generalist Adversarial Policies in Black-Box Settings*. UW-Madison Reinforcement Learning Reading Group. Oct. 2024.
- *A Machine Learning and Computer Vision Approach to Geomagnetic Storm Forecasting*. 2022 Machine Learning in Heliophysics Conference (Poster Presenter). Mar. 2022.
- *A Machine Learning and Computer Vision Approach to Geomagnetic Storm Forecasting*. Penn State Institute for Computational and Data Sciences (ICDS) Symposium. Oct. 2021.

## Professional Activities

---

### TEACHING EXPERIENCE

Fall 2024 **CS 642 — Introduction to Information Security**, Course Design and Guest Lecturer

*UW-Madison*

### REVIEWING COMMITTEES

- 2025-26 **IEEE Symposium on Security and Privacy (IEEE S&P)**, Artifact Evaluator, External Reviewer
- 2026 **Proceedings on Privacy Enhancing Technologies Symposium (PoPETS)**, Artifact Evaluator
- 2026 **Association for the Advancement of Artificial Intelligence (AAAI)**, Reviewer
- 2025 **International Conference on Learning Representations (ICLR)**, External Reviewer
- 2024 **ACM Conference on Computer and Communications Security (ACM CCS)**, External Reviewer

### OTHER SERVICE

- 2025 **UW-Madison New CS Graduate Student Welcome Weekend 2025**, Poster Presenter and Open Lab Volunteer
- 2025 **NSF Research Experiences for Undergraduates (REU)**, Undergraduate Student Mentor

## Skills

---

### COMPUTING SKILLS

**Programming** Python, C, Java, HTML, LaTeX

**OS** MacOS, GNU/Linux (Ubuntu), Windows

**Python Libraries** ML/AI (Pytorch, scikit-learn, stablebaselines3), Data (Pandas, sci-py), Visualization (Seaborn)

### INTERDISCIPLINARY SKILLS

**Research** Experimental Design, Project Management, Problem Solving, Writing, Data Analysis, Statistics

**Soft Skills** Leadership, Public Speaking, Communication

### LANGUAGES

**English** Fluent

**German** Intermediate