BLAINE HOAK

Ph.D. Candidate, Computer Sciences

@ bhoak@cs.wisc.edu https://hoak.me https://github.com/blainehoak
in https://www.linkedin.com/in/blaine-hoak-97270b158/ @blaine_hoak

EDUCATION

Ph.D. in Computer Sciences — May 2026 (expected)
University of Wisconsin–Madison
- Advised by Prof. Patrick McDaniel, research area in AI Security

B.S. in Biomedical Engineering — May 2020
Pennsylvania State University
- Specialization in Medical Imaging and Devices

EXPERIENCE

Assistant Professor — Jul 2026 - present
Department of Computer Science — University of Texas at Dallas

Graduate Research Assistant — Aug 2022 - May 2026
Madison Security & Privacy (MadS&P) Laboratory — University of Wisconsin-Madison

Ph.D. Research Intern - Trustworthy AI — May 2023 - Aug 2023
Visa — Atlanta, GA

Graduate Research Assistant — Aug 2020 - Jul 2022
Systems and Internet Infrastructure Laboratory — Pennsylvania State University

Undergraduate Research Assistant — Jan 2020 - Jul 2020
Systems and Internet Infrastructure Laboratory — Pennsylvania State University

Engineering Co-Op — May 2019 - Dec 2019
BK Medical — State College, PA

Engineering Intern — Oct 2018 - May 2019
Summit Radiation Safety Services — Boalsburg, PA

Undergraduate Research Assistant — May 2018 - Oct 2018
Artificial Heart and Cardiovascular Fluid Dynamics Laboratory — Pennsylvania State University

AWARDS

MIT EECS Rising Star Award — 2025
Massachusetts Institute of Technology

Notable Reviewer Award — 2025
USENIX Security

Top Reviewers Award — 2024
ACM CCS

Best Capstone Project — 2020
Pennsylvania State University

INVITED TALKS

Visionary AI: Innovation, Risk, and Responsibility — Mar 2026
Badgers in Tech — University of Wisconsin-Madison

Uncovering the Mechanisms of AI Model Failures — Mar 2026
Clemson University — Clemson, SC

Uncovering the Mechanisms of AI Model Failures — Feb 2026
University of Tennessee at Knoxville — Knoxville, TN

Uncovering the Mechanisms of AI Model Failures — Feb 2026

Max Planck Institute for Security and Privacy — Bochum, Germany

Uncovering the Mechanisms of AI Model Failures — Feb 2026
University of Texas at Dallas — Dallas, TX

Uncovering the Mechanisms of AI Model Failures — Jan 2026
Rutgers University — Camden, NJ

Uncovering the Mechanisms of AI Model Failures — Dec 2025
University of Arizona — Tucson, AZ

Uncovering the Mechanisms of AI Model Failures — Oct 2025
Max Planck Institute for Security and Privacy — Bochum, Germany

Uncovering the Mechanisms of AI Model Failures — Oct 2025
PurSec Group Seminar, Purdue University — Purdue University

Harnessing CHTC to Uncover ML Vulnerabilities — May 2025
Open Science Grid School — University of Wisconsin-Madison

Adversarial Attacks — May 2024
SecureAI Program — Loyola University

AI's Impact on the Future of Work — March 2024
Microsoft — Chicago, IL

Machine Learning in Security — Nov 2023
CS 642 - University of Wisconsin-Madison — Madison, WI

Trust, Expectations, and Failures in AI — Mar 2023
The UW Now Livestream

The Space of Adversarial Strategies — Oct 2022
Collaborative Research Alliance (CRA) Webinar

The Space of Adversarial Strategies — May 2022
CATCH MURI Review — Melbourne, Australia

LEADERSHIP AND TEACHING

Guest Lecturer — Fall 2023
CS 642 - Intro to Information Security — University of Wisconsin-Madison

Teaching Assistant — Fall 2021
CMPSC 297 - Intro to C Programming — Pennsylvania State University

Teaching Assistant — Spring 2020
CMPSC 311 - Intro to Systems Programming — Pennsylvania State University

Teaching Facilitator — Spring 2019, Fall 2020, Spring 2020
MATH 256 - Ordinary and Partial Differential Equations — Pennsylvania State University

Guided Study Group Leader — Jan 2019 – May 2020
Women in Engineering Program — Pennsylvania State University

Vice President — May 2019 – May 2020
Nittany Chemical Society — Pennsylvania State University

Learning Assistant — Spring 2018
Chem112 - General Chemistry II — Pennsylvania State University

OUTREACH ACTIVITIES

Lead Organizer — May 2022 – present
Queer in Security & Privacy Social Hours

- Symposium on Computer and Communications Security (CCS) 2022
- IEEE Symposium on Security & Privacy (IEEE S&P) 2022

Mentor
Chronic Health Allies Mentorship Program (CHAMP)
Aug 2022 – Aug 2023
University of Wisconsin-Madison

Volunteer
Girls Who Code
Spring 2022
Pennsylvania State University

Creator and Volunteer
EECS Girl's Summer Camp
Summer 2021 & 2022
Pennsylvania State University

DEPARTMENTAL SERVICE

Lead Organizer
MadS&P Seminar
May 2024 – Sep 2025
University of Wisconsin-Madison

Panelist
Doing Research & Finding an Advisor
Nov 2024
University of Wisconsin-Madison

PROFESSIONAL SERVICE

Area Chair
- International Conference on Learning Representations (ICLR), Tiny Papers Track - 2023

Session Chair
- USENIX Security Symposium - 2025

Program Committee
- USENIX Security Symposium - 2025, 2026
- ACM Conference on Computer and Communications Security (CCS) - 2025, 2026
- IEEE Symposium on Security and Privacy (IEEE S&P) - 2024, 2025
- IEEE Symposium on Security and Privacy (IEEE S&P), Posters - 2024
- ACM Workshop on Artificial Intelligence and Security (AISec) - 2025
- Conference on Neural Information Processing Systems (NeurIPS) - 2023, 2025, 2026
- International Conference on Learning Representations (ICLR) - 2024
- International Conference on Learning Representations (ICLR), Tiny Papers Track - 2023
- IEEE Conference on Secure and Trustworthy Machine Learning (SaTML) - 2023, 2024

External Reviewer
- USENIX Security Symposium - 2023
- IEEE Symposium on Security and Privacy (IEEE S&P) - 2022
- ACM Conference on Computer and Communications Security (CCS) - 2022
- ACM Conference on Mobile Computing and Networking (MobiCom) - 2021
- IEEE Computer Security Foundations Symposium (CSF) - 2021

PUBLICATIONS

Conference Proceedings

- **Blaine Hoak** and Patrick McDaniel. "On Synthetic Texture Datasets: Challenges, Creation, and Curation". In: *European Conference on Artificial Intelligence (ECAI)*. July 2025. URL: http://arxiv.org/abs/2409.10297.
- Kunyang Li, Jean-Charles Noirot Ferrand, Ryan Sheatsley, **Blaine Hoak**, Yohan Beugin, Eric Pauley, and Patrick McDaniel. "On the Robustness Tradeoff in Fine-Tuning". In: *IEEE/CVF International Conference on Computer Vision (ICCV)*. Oct. 2025. URL: https://arxiv.org/abs/2503.14836.
- **Blaine Hoak**, Ryan Sheatsley, and Patrick McDaniel. "Err on the Side of Texture: Texture Bias on Real Data". In: *2025 IEEE Conference on Secure and Trustworthy Machine Learning (SaTML)*. IEEE Computer Society, Apr. 2025. DOI: 10.1109/SaTML64287.2025.00042.
- Eric Pauley, Kyle Domico, **Blaine Hoak**, Ryan Sheatsley, Quinn Burke, Yohan Beugin, Engin Kirda, and Patrick McDaniel. "Secure IP Address Allocation at Cloud Scale". In: *2025 Network and Distributed Systems Security Symposium (NDSS)*. San Diego, CA: Internet Society, Feb. 2025. URL: https://arxiv.org/abs/2210.14999.
- **Blaine Hoak** and Patrick McDaniel. "Explorations in Texture Learning". In: *ICLR 2024, Tiny Papers Track*. Mar. 2024. URL: http://arxiv.org/abs/2403.09543.
- **Blaine Hoak**, Ryan Sheatsley, Eric Pauley, and Patrick McDaniel. "The Space of Adversarial Strategies". In: *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Aug. 2023. URL: https://www.usenix.org/conference/usenixsecurity23/presentation/sheatsley.

- Yohan Beugin, Quinn Burke, **Blaine Hoak**, Ryan Sheatsley, Eric Pauley, Gang Tan, Syed Rafiul Hussain, and Patrick McDaniel. “Building a Privacy-Preserving Smart Camera System”. In: *Proceedings on Privacy Enhancing Technologies Symposium (PETS)*. July 2022. URL: https://arxiv.org/abs/2201.09338.
- Eric Pauley, Ryan Sheatsley, **Blaine Hoak**, Quinn Burke, Yohan Beugin, and Patrick McDaniel. “Measuring and Mitigating the Risk of IP Reuse on Public Clouds”. English. In: *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, May 2022. URL: https://arxiv.org/abs/2204.05122.
- Ryan Sheatsley, **Blaine Hoak**, Eric Pauley, Yohan Beugin, Michael J. Weisman, and Patrick McDaniel. “On the Robustness of Domain Constraints”. In: *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. CCS ’21. Association for Computing Machinery, Nov. 2021. DOI: 10.1145/3460120.3484570.

Journals

- Quinn Burke, Yohan Beugin, **Blaine Hoak**, Rachel King, Eric Pauley, Ryan Sheatsley, Mingli Yu, Ting He, Thomas La Porta, and Patrick McDaniel. “Securing Cloud File Systems with Trusted Execution”. In: *IEEE Transactions on Dependable and Secure Computing (TDSC)* (Sept. 2024). DOI: 10.1109/TDSC.2024.3474423.

Workshops

- **Blaine Hoak**, Kunyang Li, and Patrick McDaniel. “Alignment and Adversarial Robustness: Are More Human-Like Models More Secure?” In: *International Workshop on Security and Privacy-Preserving AI/ML (SPAIML) 2025*. July 2025. URL: https://arxiv.org/abs/2502.12377.
- Rachel King, Quinn Burke, Yohan Beugin, **Blaine Hoak**, Kunyang Li, Eric Pauley, Ryan Sheatsley, and Patrick McDaniel. “ParTEETor: A System for Partial Deployments of TEEs within Tor”. In: *Proceedings of the 23rd Workshop on Privacy in the Electronic Society (WPES)*. Salt Lake City, UT, USA: ACM, Oct. 2024. URL: https://dl.acm.org/doi/10.1145/3689943.3696203.

In Submission

- **Blaine Hoak**, Kunyang Li, Kyle Domico, and Patrick McDaniel. “Robustness Under Texture Transformations: Exploiting Natural Texture Backdoors in Vision Models”. In: *Under review*. Under review, Aug. 2025.
- Hadi Abdullah, **Blaine Hoak**, Ke Wang, Yizhen Wang, Sunpreet Arora, and Yiwei Cai. “Is Memorization Actually Necessary for Generalization?” In: *Under review*. Jan. 2024. URL: https://openreview.net/forum?id=lf8QQ2KMgv.

Tech Reports

- Yohan Beugin, Quinn Burke, **Blaine Hoak**, Ryan Sheatsley, Eric Pauley, Gang Tan, Syed Rafiul Hussain, and Patrick McDaniel. *Privacy-Preserving Protocols for Smart Cameras and Other IoT Devices*. 2022. arXiv: 2208.09776 [cs.CR].
- Alban Héon, Ryan Sheatsley, Quinn Burke, **Blaine Hoak**, Eric Pauley, Yohan Beugin, and Patrick McDaniel. *Systematic Evaluation of Geolocation Privacy Mechanisms*. 2023. arXiv: 2309.06263 [cs.CR].