

# BLAINE HOAK

Ph.D. Student, 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. Computer Sciences 📅 Aug 2022 – present  
**University of Wisconsin-Madison**
- Advisor: Dr. Patrick McDaniel
- Ph.D. Computer Science and Engineering<sup>1</sup> 📅 Aug 2020 – July 2022  
**Pennsylvania State University**
- Advisor: Dr. Patrick McDaniel
- Bachelor of Science, Biomedical Engineering 📅 Jan 2017 – May 2020  
**Pennsylvania State University**
- Specialization: Medical Imaging and Devices

## PUBLICATIONS

### 👥 Conference Proceedings

- Hadi Abdullah, Blaine Hoak, Ke Wang, Yizhen Wang, Sunpreet Arora, and Yiwei Cai. “Is Memorization Actually Necessary for Generalization?” In: *In submission*. Nov. 2023.
- Blaine Hoak, Ryan Sheatsley, Eric Pauley, and Patrick McDaniel. “The Space of Adversarial Strategies”. In: *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim, CA: USENIX Association, Aug. 2023, pp. 3745–3761. ISBN: 978-1-939133-37-3. URL: <https://www.usenix.org/conference/usenixsecurity23/presentation/sheatsley>.
- Eric Pauley, Ryan Sheatsley, Blaine Hoak, Quinn Burke, Yohan Beugin, and Patrick McDaniel. “Measuring and Mitigating the Risk of IP Reuse on Public Clouds”. In: *IEEE Symposium on Security and Privacy (S&P)*. Apr. 2022. URL: <https://www.computer.org/csdl/proceedings-article/sp/2022/131600b523/1CI07rpcgSs>.
- Yohan Beugin, Quinn Burke, Blaine Hoak, Ryan Sheatsley, Eric Pauley, Gang Tan, Syed Raful Hussain, and Patrick McDaniel. “Building a Privacy-Preserving Smart Camera System”. In: *Proceedings on Privacy Enhancing Technologies*. Jan. 2022. DOI: [10.2478/popets-2022-0034](https://doi.org/10.2478/popets-2022-0034).
- 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*. Association for Computing Machinery, 2021. URL: <https://doi.org/10.1145/3460120.3484570>.

## INVITED TALKS

- Machine Learning in Security 📅 Nov 2023  
**CS 642 - University of Wisconsin-Madison**
- 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**

## EXPERIENCE

- Ph.D. Research Intern - Trustworthy AI 📅 May 2024 – Aug 2024  
**Visa** 📍 Atlanta, GA
- Ph.D. Research Intern - Trustworthy AI 📅 May 2023 – Aug 2023  
**Visa** 📍 Atlanta, GA
- Graduate Research Assistant 📅 Aug 2022 – present  
**Madison Security & Privacy (MadS&P) Laboratory** 📍 University of Wisconsin-Madison

<sup>1</sup>Degree incomplete, transferred to University of Wisconsin-Madison with advisor.

Graduate Research Assistant  
**Systems and Internet Infrastructure Laboratory**

📅 Aug 2020 – Jul 2022  
📍 Pennsylvania State University

Undergraduate Research Assistant  
**Systems and Internet Infrastructure Laboratory**

📅 Jan 2020 – Jul 2020  
📍 Pennsylvania State University

Engineering Co-Op  
**BK Medical**

📅 May 2019 – Dec 2019  
📍 State College, PA

Engineering Intern  
**Summit Radiation Safety Services**

📅 Oct 2018 – May 2019  
📍 Boalsburg, PA

Undergraduate Research Assistant  
**Artificial Heart and Cardiovascular Fluid Dynamics Laboratory**

📅 May 2018 – Oct 2018  
📍 Pennsylvania State University

## LEADERSHIP AND TEACHING

---

Guest Lecturer  
**CS 642 - Intro to Information Security**

📅 Fall 2023  
📍 University of Wisconsin-Madison

Teaching Assistant  
**CMPSC297 - Intro to C Programming**

📅 Fall 2021  
📍 Pennsylvania State University

Guided Study Group Leader  
**Women in Engineering Program**

📅 Jan 2019 – May 2020  
📍 Pennsylvania State University

Vice President  
**Nittany Chemical Society**

📅 May 2019 – May 2020  
📍 Pennsylvania State University

Learning Assistant  
**Chem112 - General Chemistry II**

📅 Spring 2018  
📍 Pennsylvania State University

## OUTREACH ACTIVITIES

---

Mentor  
**Chronic Health Allies Mentorship Program (CHAMP)**

📅 Aug 2022 - present  
📍 University of Wisconsin-Madison

Lead Organizer  
**Queer in Security & Privacy Social Hours**

📅 May 2022 - present

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

Volunteer  
**Girls Who Code**

📅 Spring 2022  
📍 Pennsylvania State University

Creator and Volunteer  
**EECS Girl's Summer Camp**

📅 Summer 2021 & 2022  
📍 Pennsylvania State University

## REVIEWING AND INVOLVEMENT

---

Area Chair

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

Program Committee

- IEEE Symposium on Security and Privacy (IEEE S&P) - 2024
- IEEE Symposium on Security and Privacy (IEEE S&P), Posters - 2024
- Conference on Neural Information Processing Systems (NeurIPS) - 2023
- 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

## **Grant Involvement**

- National Science Foundation - Center for Trustworthy Machine Learning (CTML)
- Multidisciplinary University Research Initiative - Cybersecurity Assurance for Teams of Computers and Humans (CATCH MURI)
- Army Research Laboratory - Collaborative Research Alliance (CRA)