

# Shawn Shan

✉ shawnshan@uchicago.edu  
🌐 www.shawnshan.com

EDUCATION	<b>University of Chicago</b> <i>PhD Candidate, Computer Science</i> <i>Advised by Prof. Ben Y. Zhao and Prof. Heather Zheng</i>	2020 - Current
	<b>University of Chicago</b> <i>Master of Science, Computer Science</i>	2020 - 2022
	<b>University of Chicago</b> <i>Bachelor of Science, Computer Science with honors</i>	2016 - 2020
APPOINTMENTS	<b>Dartmouth College</b> <i>Assistant Professor of Computer Science</i>	July 2026 (Incoming)
HONORS AND AWARDS	• MIT Technology Review - Innovator of the Year	2024
	• MIT Technology Review - 35 Under 35	2024
	• Forbes - 30 Under 30	2024
	• Siebel Scholarship	2024
	• CCS Distinguished Paper Award	2024
	• TIME Magazine Best Inventions Special Mention	2023
	• USENIX Internet Defense Prize	2023
	• USENIX Security Distinguished Paper Award	2023
	• Chicago Innovation Award	2023
	• Eckhardt Graduate Scholarship	2020
	• Liew Family Research Fellowship	2018
PUBLICATIONS	[1] S. Wu, R. Bhaskar, A. Ha, <b>S. Shan</b> , H. Zheng, BY. Zhao. On the Feasibility of Poisoning Text-to-Image AI Models via Adversarial Mislabeling. <i>ACM Conference on Computer and Communications Security (CCS)</i> 2025.	
	[2] E. Liu, E. Luo, <b>S. Shan</b> , G. Voelker, BY. Zhao, S. Savage. Awareness, Agency and Efficacy in Protecting Content Creators From AI Crawlers. <i>ACM Internet Measurement Conference (IMC)</i> 2025.	
	[3] W. Ding, CY. Li, <b>S. Shan</b> , BY. Zhao, H. Zheng. Understanding Implosion in Text-to-Image Generative Models. <i>ACM Conference on Computer and Communications Security (CCS)</i> 2024.	
	[4] A. Ha, J. Passananti, R. Bhaskar, <b>S. Shan</b> , R. Southen, H. Zheng, BY. Zhao. Organic or Diffused: Can We Distinguish Human Art from AI-generated Images? <i>ACM Conference on Computer and Communications Security (CCS)</i> 2024.	
	<b>Distinguished Paper Award</b>	

[5] **S. Shan**, W Ding, J Passananti, H. Zheng, BY. Zhao. Nightshade: Prompt-Specific Poisoning Attacks on Text-to-Image Generative Models. *IEEE Symposium on Security and Privacy (Oakland)* 2024.

[6] **S. Shan**, J. Cryan, E. Wenger, H. Zheng, R. Hanocka, BY. Zhao. Glaze: Protecting Artists from Style Mimicry by Text-to-Image Models. *USENIX Security Symposium (USENIX Security)* 2023.

**Distinguished Paper Award, Internet Defense Prize**

[7] E. Wenger, **S. Shan**, H. Zheng, BY. Zhao. SoK: Anti-Facial Recognition Technology. *IEEE Symposium on Security and Privacy (Oakland)* 2023.

[8] **S. Shan**, W. Ding, E. Wenger, H. Zheng, BY. Zhao. Post-breach Recovery: Protection against White-box Adversarial Examples for Leaked DNN Models. *ACM Conference on Computer and Communications Security (CCS)* 2022.

[9] **S. Shan**, A.N. Bhagoji, H. Zheng, BY. Zhao. Poison Forensics: Traceback of Data Poisoning Attacks in Neural Networks. *USENIX Security Symposium (USENIX Security)* 2022.

[10] H. Li, **S. Shan**, E. Wenger, J. Zhang, H. Zheng, BY. Zhao. Blacklight: Scalable Defense for Neural Networks against Query-Based Black-Box Attacks. *USENIX Security Symposium (USENIX Security)* 2022.

[11] **S. Shan**, A. Bhagoji, H. Zheng, and B. Zhao. Patch-based Defenses against Web Fingerprinting Attacks. *ACM Workshop on Artificial Intelligence and Security (AISec)* 2021.

[12] T. Xu, G. Goossen, H.K. Cevahir, S. Khodeir, Y. Jin, F. Li, **S. Shan**, S. Patel, D. Freeman, P. Pearce. Deep Entity Classification: Abusive Account Detection for Online Social Networks. *USENIX Security Symposium (USENIX Security)* 2021.

[13] **S. Shan**, E. Wenger, B. Wang, B. Li, H. Zheng, B. Zhao. Gotta Catch 'Em All: Using Concealed Trapdoors to Detect Adversarial Attacks on Neural Networks. *ACM Conference on Computer and Communications Security (CCS)* 2020.

[14] **S. Shan**, E. Wenger, J. Zhang, H. Li, H. Zheng, B. Zhao. Fawkes: Protecting Personal Privacy against Unauthorized Deep Learning Models. *USENIX Security Symposium (USENIX Security)* 2020.

[15] B. Wang, Y. Yao, **S. Shan**, H. Li, B. Viswanath, H. Zheng, B. Zhao. Neural Cleanse: Identifying and Mitigating Backdoor Attacks in Neural Networks. *IEEE Symposium on Security and Privacy (Oakland)* 2019.

[16] B. Weinshel, M. Wei, M. Mondal, E. Choi, **S. Shan**, C. Dolin, M. Mazurek, B. Ur. Oh, the Places You've Been! User Reactions to Longitudinal Transparency About Third-Party Web Tracking and Inferencing. *ACM Conference on Computer and Communications Security (CCS)* 2019.

[17] C. Dolin, B. Weinshel, **S. Shan**, C. Hahn, E. Choi, M. Mazurek, B. Ur. Unpacking Perceptions of Data-Driven Inferences Underlying Online Targeting and Personalization. *ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)* 2018.

**ACADEMIC  
SERVICE****Reviewing**

PC, <i>USENIX Security Symposium</i>	2025,2026
PC, <i>ACM Conference on Computer and Communications Security (CCS)</i>	2025
PC, <i>AdvML Frontiers at NeurIPS</i>	2024
PC, <i>Privacy Enhancing Technologies Symposium (PETS)</i>	2023, 2024
PC, <i>ACM Workshop on Artificial Intelligence and Security (AISec)</i>	2022
Reviewer, <i>Neural Information Processing Systems (NeurIPS)</i>	2022, 2023
Reviewer, <i>Computer Vision and Pattern Recognition (CVPR)</i>	2022, 2023, 2024
Reviewer, <i>European Conference on Computer Vision (ECCV)</i>	2022

**Organizing/Chairing**

Organizer, BANDS Workshop at ICLR	2023
Session Chair, USENIX Security	2023

**TEACHING &  
MENTORING****Teaching**

Guest Lecture, AI and Entertainment Industry, Southwestern University Law School	2024
Guest Lecture, Introduction to Computer Security, University of Chicago	2024
Teaching Assistant, Networks and Distributed Systems, University of Chicago	2022

**Mentoring**

Josephine Passananti	B.S. Computer Science, UChicago > Ph.D, UChicago	2023-24
August Deer	B.S. Computer Science, UChicago	2024
Anna Yoo Jeong Ha	Ph.D, UChicago	2023-24
Stanley Wu	Ph.D, UChicago	2023-24
Ronik Bhaskar	B.S. Computer Science, UChicago > Ph.D, UChicago	2023-24
Jiayun Zhang	Summer Intern > Ph.D, UCSD	2020
Max Bronckers	B.S. Computer Science, UChicago > M.S. Cambridge	2021

**MEDIA  
COVERAGE  
(SELECTED)**

Innovator of the Year: Shawn Shan builds tools to fight back against exploitative AI	2024
Melissa Heikkilä, <i>MIT Technology Review</i>	
This Tool Could Protect Artists From A.I.-Generated Art That Steals Their Style	2023
Kashmir Hill, <i>The New York Times</i>	
This New Data Poisoning Tool Lets Artists Fight Back against Generative AI	2023
Melissa Heikkilä, <i>MIT Technology Review</i>	
These New Tools Could Help Protect Our Pictures from AI	2023
Melissa Heikkilä, <i>MIT Technology Review</i>	
New Tools Help Artists Fight AI by Directly Disrupting the Systems	2023
Chloe Veltman, <i>NPR</i>	
New Tool ‘Poisons’ AI Data To Shield Artists Against Having Their Work Stolen	2023
Leslie Katz, <i>Forbes</i>	
This Tool Could Protect Your Photos From Facial Recognition	2020

Kashmir Hill, *The New York Times*

Full list of media coverage can be found at [www.shawnshan.com/press.html](http://www.shawnshan.com/press.html)

**INVITED  
TALKS**

<b>Medientage München (Munich Media Days)</b> , Keynote <i>One of the largest media conferences in Europe with over 5,000 attendees</i>	Oct 2024
<b>Grantmakers in the Arts Conference (GIA)</b> , Panel <i>The annual conferences of GIA, an arts funding organization with over 40,000 members.</i>	Oct 2024
<b>Center for Intellectual Property x Innovation Policy (CIP2)</b> , Panel <i>A roundtable bringing together legal scholars and technologists to explore AI and copyright.</i>	Jul 2024
<b>Solarpunk Conference</b> , Invited Talk <i>An one-day virtual artist event.</i>	Jun 2024
<b>NPR Cool Science</b> , Invited Talk <i>A NPR science radio show.</i>	Apr 2024
<b>British Screen Forum Annual Conference</b> , Invited Talk <i>An annual conferences in London for ~100 senior executives from the UK screen industries.</i>	Nov 2023
<b>Artly World Nonprofit</b> , Invited Talk <i>A 501(c)(3) nonprofit supporting young aspiring artists.</i>	Sep 2023
<b>Copyright Alliance</b> , Invited Talk <i>The largest copyright organization in US representing over 2 millions creators.</i>	Aug 2023
<b>National Association of Voice Actors: NAVA</b> , Invited Talk <i>A leading association of U.S. voice actors.</i>	Jun 2023
<b>Concept Art Association</b> , Invited Talk <i>A leading association of concept artists.</i>	May 2023
<b>Privacy and Security in ML Seminars</b> , Invited Talk <i>A seminar hosted by UCL and CISPA.</i>	Mar 2023