BRIAN JAY TANG

Computer Science Researcher - AI for Security & Privacy

CONTACT

+1 630-880-3691

bjaytang@umich.edu

https://www.bjaytang.com

FULL CV

github.com/byron123t

linkedin.com/in/bjaytang

Google Scholar

SKILLS

Python 7+ yrs

Security 6+ yrs

Privacy 4+ yrs

Computer Vision 4+ yrs

JavaScript 4+ yrs

HCI 3+ yrs

NLP and LLMs 2+ yrs

Flight Experience < 1 yr

SELECTED AWARDS/GRANTS

Defense University Research Instrumentation Program (DURIP, $300k)

Securing Cyber-Physical System Communication and Control

College of Engineering Fellowship ($90k)

University of Michigan 1st year PhD Fellowship Recipient

Patent: Real-Time Protection For Mobile Devices From Shoulder Surfing

U.S. Pat. App. No. 63/468,650-Conf. #8672

EDUCATION

Ph. D. - Computer Science & Engineering — **2021 - ongoing**
University of Michigan - Ann Arbor, MI (USA)

B.S. - Computer Sciences — **2017 - 2020**
University of Wisconsin - Madison, WI (USA)

WORK EXPERIENCE

Graduate Research Assistant — **Sep '21 - ongoing**
University of Michigan, Ann Arbor (MI)

Researching and creating systems that enhance user privacy. Designing AI systems to protect online data privacy, smartphone data, vehicle data, etc.

Undergraduate Research Assistant — **Sep '18 - Aug '21**
University of Wisconsin, Madison (WI)

Researched security, privacy, and fairness properties of ML systems such as face recognition, image recognition, NLP, and social robots.

Software Engineering Intern — **May '19 - Aug '19**
Roblox, San Mateo (CA)

Developed enhancements and features for Roblox Studio's script editor.

Software Engineering Intern — **May '18 - Aug '18**
Optum UHG, Eden Prairie (MN)

Developed data visualization tools for analyzing security vulnerabilities.

SELECTED PUBLICATIONS

"It LIED To Me": Implications of Injecting Personalized Advertising into Large Language Model Chatbots — **Submission**
ACM CHI Conference on Human Factors in Computing Systems (2025), *Acc Rate: 25%*

Eye-Shield Real-Time Protection of Mobile Device Screen Information from Shoulder Surfing — **Publication**
32nd USENIX Security Symposium (2023), *Acc Rate: 17%*

Detection of Inconsistencies in Privacy Practices of Browser Extensions — **Publication**
44th IEEE Symposium on Security and Privacy (2023), *Acc Rate: 13%*

Fairness Properties of Face Recognition and Obfuscation Systems — **Publication**
32nd USENIX Security Symposium (2023), *Acc Rate: 17%*

Confidant: A Privacy Controller for Social Robots — **Publication**
17th ACM/IEEE International Conference on Human-Robot Interaction (2022), *Acc Rate: 26%*

Face-Off: Adversarial Face Obfuscation — **Publication**
21st Symposium of Privacy Enhancing Technologies (2021), *Acc Rate: 22%*