Brian Jay Tang

☎ +1 630-880-3691
✉ byron123t@gmail.com
✉ bjaytang@umich.edu

CV Last Updated: 2024-03-25
https://www.linkedin.com/in/bjaytang/
https://github.com/byron123t
https://scholar.google.com/citations?user=pgkhBk8AAAAJ&hl=en
https://www.bjaytang.com/

Education

PhD Candidate | ***Computer Science and Engineering*** — Fall 2021 – Present
University of Michigan - Ann Arbor — Advised by Kang G. Shin

Bachelor of Science | ***Major: Computer Science*** — Fall 2017 – Winter 2020
University of Wisconsin - Madison — Advised by Kassem Fawaz, Varun Chandrasekaran

Research Interests

Thesis: Protecting Privacy and Autonomy in the Era of Large Language Models
Software Systems: Mobile Computing, Real-Time Systems, Cyber-Physical Systems, Compound AI Systems
Security and Privacy: Usable Privacy, Web Privacy, Face Recognition Privacy, Social Privacy, Mobile Privacy
Artificial Intelligence: Natural Language Processing, Adversarial ML, Computer Vision, Cognitive Architectures

Skills

Programming: Python (Expert), JavaScript (Familiar), HTML (Familiar), SQL (Proficient), C++ (Proficient)
Software Development: GitHub, Perforce, Qt, NginX, Flask, Squish, AWS, Redis
Machine Learning: TensorFlow, PyTorch, Pandas, NumPy, D3.js, HuggingFace
Languages: English (Native), Chinese Mandarin (Spoken-Only), Japanese (Weak), French (Weak)
Hobbies & Interests: Reading, Drumming, Gaming, Anime, Meditation, Hiking, Camping, Flight Sim

Work Experience

Co-Founder — Fall 2023 – Present
PocketEngineer LLC

- Developed an automation prototype that parses technical specs sheets and manuals.
- Designed system to transcribe sales calls and generate product suggestions and technical details.

Graduate Research Assistant — Fall 2021 – Present
University of Michigan

- Applying AI techniques to protect user privacy in cyber-physical systems and platforms.
- Created a real-time software privacy film to protect against screen snooping on smartphones.
- Developed various web automation tools and document parsers for auditing data collection activities.

Research Intern — Spring 2021 – Fall 2021
University of Wisconsin - Madison

- Researched fairness properties of face recognition systems.
- Created a controller for social robots to preserve conversational privacy.

Undergraduate Research Assistant — Fall 2018 – Spring 2021
University of Wisconsin - Madison

- Explored using physical invariants from LiDAR to improve ML classifier robustness against adversarial attacks.
- Developed an anti face recognition system using adversarial attacks to protect online photo privacy.

Software Engineering Intern — Summer 2019
Roblox Corporation

- Created core features for Roblox Studio's script editor in a test-driven development setting.
- Developed integrated JavaScript Squish tests for evaluating expected behavior of new UI features.

Software Engineering Intern — Summer 2018
Optum, UHG

- Designed and developed data visualization application aggregating 50+ million records from security databases.
- Presented project to audience of Optum's executives, directors, security analysts, and interns.

Publications and Preprints

[1] **Brian Tang**, Noah T. Curran, Florian Schaub, and Kang G. Shin. “Embedding Advertising in LLM Chatbots: Risks and Ethical Considerations”. In: *In Preparation: ACM CHI Conference on Human Factors in Computing Systems*. 2025.

[2] **Brian Tang**, Duc Bui, and Kang G. Shin. “Navigating Cookie Compliance Across the Globe”. In: *Under Submission: Privacy Enhancing Technologies Symposium*. 2024.

[3] **Brian Tang** and Kang G. Shin. “Steward: Natural Language Web Automation”. In: *Under Submission: The 30th Symposium on Operating Systems Principles*. 2024.

[4] Noah T. Curran, Minkyoung Cho, Ryan Feng, Liangkai Liu, **Brian Jay Tang**, Kang G. Shin, Pedram MohajerAnsari, and Mert D. Pesé. “Short: Achieving the Safety and Security of the End-to-End AV Pipeline”. In: *Under Submission: ESCAR USA*. 2024.

[5] **Brian Tang** and Kang G. Shin. “Eye-Shield: Real-Time Protection of Mobile Device Screen Information from Shoulder Surfing”. In: *32nd USENIX Security Symposium*. 2023. URL: https://rtcl.eecs.umich.edu/rtclweb/assets/publications/2023/usenix23-tang.pdf.

[6] Duc Bui, **Brian Tang**, and Kang G. Shin. “Detection of Inconsistencies in Privacy Practices of Browser Extensions”. In: *44th IEEE Symposium on Security and Privacy*. 2023. URL: https://www.bjaytang.com/pdfs/ExtPrivA.pdf.

[7] Harrison Rosenberg, **Brian Tang**, Kassem Fawaz, and Somesh Jha. “Fairness Properties of Face Recognition and Obfuscation Systems”. In: *32nd USENIX Security Symposium*. 2023. URL: https://arxiv.org/abs/2108.02707.

[8] **Brian Tang**, Dakota Sullivan, Bengisu Cagiltay, Varun Chandrasekaran, Kassem Fawaz, and Bilge Mutlu. “Confidant: A Privacy Controller for Social Robots”. In: *17th ACM/IEEE International Conference on Human-Robot Interaction*. 2022. URL: https://arxiv.org/abs/2201.02712.

[9] Duc Bui, **Brian Tang**, and Kang G. Shin. “Do Opt-Outs Really Opt Me Out”. In: *29th ACM Conference on Computer and Communications Security*. 2022. URL: https://dl.acm.org/doi/10.1145/3548606.3560574.

[10] Varun Chandrasekaran, Chuhan Gao, **Brian Tang**, Kassem Fawaz, Somesh Jha, and Suman Banerjee. “Face-Off: Adversarial Face Obfuscation”. In: *21st Privacy Enhancing Technologies Symposium*. 2021. URL: https://arxiv.org/abs/2003.08861.

[11] Varun Chandrasekaran, **Brian Tang**, Nicolas Papernot, Kassem Fawaz, Somesh Jha, and Xi Wu. “Rearchitecting Classification Frameworks For Increased Robustness”. In: (2020). URL: https://arxiv.org/abs/1905.10900.

Honors and Awards

3 Minute Thesis Competition (*Finalist*) Fall 2023
Recovering Privacy and Autonomy in the Era of Large Language Models

College of Engineering Fellowship Fall 2021
University of Michigan 1st year PhD fellowship

Qualcomm Innovation Fellowship (*Selected Abstract*) Spring 2021
Autonomous Vehicle Domain Adaptation

CVS Health Foundation Program Fall 2017
Scholarship (Outstanding Children of CVS Employees)

Patents

Real-Time Protection For Mobile Devices From Shoulder Surfing[5] Spring 2023
U.S. Pat. App. No. 63/468,650-Conf. #8672 Filed

Grant Proposal Experience

Securing Interactions between Driver and Vehicle Using Batteries Summer 2023
National Science Foundation (NSF) Cloud Credits (Cloudbank) Granted, $16k

Securing Cyber-Physical System Communication and Control Spring 2023
Defense University Research Instrumentation Program (DURIP) Granted, $300k

Service

External/Sub Reviewer Spring 2020 - Fall 2023
USENIX Security 2021, PoPETS 2022, NeurIPS 2023, CHI 2024

Poster Committee Member Spring 2024
IEEE S&P 2024

Presentations and Talks

Steward: Natural Language Web Automation[3] Mar 2024
Ann Arbor, MI | *SECRIT Security Reading Group*

Recovering Privacy and Autonomy in the Presence of Language Models Sept 2023
Ann Arbor, MI | *3 Minute Thesis Finalist Competition (Engineering Graduate Symposium)*

Eye-Shield: Real-Time Protection of Mobile Device Screen Information from Shoulder Surfing[5] Aug 2023
Anaheim, CA | *USENIX Security Symposium*

Confidant: A Privacy Controller for Social Robots[8] Mar 2022
The Internet | *ACM/IEEE International Conference on Human-Robot Interaction*

Face-Off: Adversarial Face Obfuscation[10] Jan 2021
The Internet | *VMWare - NSF: Data Privacy and Edge Computing*

Face-Off: Adversarial Face Obfuscation[10] July 2021
The Internet | *Proceedings on Privacy Enhancing Technologies Symposium*