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

CV Last Updated: 2022-04-09
https://www.linkedin.com/in/btang12/
https://github.com/byron123t
https://scholar.google.com/citations?user=pgkhBk8AAAAJ&hl=en
🔗 https://www.bjaytang.com/

EDUCATION

PhD Student | ***Computer Science and Engineering*** — Fall 2021 – Present
University of Michigan - Ann Arbor — GPA: 4.00

Bachelor of Science | ***Major: Computer Science*** — Fall 2017 – Winter 2020
University of Wisconsin - Madison — GPA: 3.53

RESEARCH INTERESTS

Security and Privacy: Usable Privacy, Web Privacy, Face Recognition Privacy, Social Privacy
Machine Learning: Adversarial Machine Learning, Computer Vision, Natural Language Processing
Human-Computer Interaction: Usable Privacy, Human-Robot Interaction

WORK EXPERIENCE

Graduate Research Assistant — Fall 2021 – Present
University of Michigan

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

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

Software Engineering Intern — Summer 2019
Roblox Corporation

Software Engineering Intern — Summer 2017
Optum, UHG

RESEARCH PROJECTS

Confidant: A Privacy Controller for Social Robots[4] — Fall 2021
University of Michigan | *17th ACM/IEEE International Conference on Human-Robot Interaction* — 24.8% AR

Toxicity Detection and Mitigation on Social Networking Platforms — Fall 2021
University of Michigan | *Course Project*

DJGRAD: Sparse Gradients Protocol for Distributed Assisted Learning in CAVs — Fall 2021
University of Michigan | *Course Project*

Fairness Properties of Face Recognition and Obfuscation Systems[3] — Summer 2021
University of Wisconsin - Madison | ***Submitted:*** *USENIX Security 2022*

Face-Off: Adversarial Face Obfuscation[1] — Summer 2020
University of Wisconsin - Madison | *21st Symposium of Privacy Enhancing Technologies* — 19.0% AR

Scaling Properties of Interval Bound Propagation — Spring 2020
University of Wisconsin - Madison | *Course Project*

Rearchitecting Classification Frameworks For Increased Robustness[2] — Spring 2019
University of Wisconsin - Madison | *arXiv Preprint*

PERSONAL PROJECTS

Algorithmic Trading Framework — Summer 2019
https://github.com/ramasrirama99/AlgoTradeFramework

Transcend UW Website | ***https://www.transcenduw.com/*** — Spring 2018
University of Wisconsin - Madison | *Transcend UW*

Service

PoPETS Spring 2021
External/Sub Reviewer

USENIX Security Spring 2020
External/Sub Reviewer

Presentations and Talks

Confidant: A Privacy Controller for Social Robots[4] Mar 2022
University of Michigan | *ACM/IEEE International Conference on Human-Robot Interaction*

Face-Off: Adversarial Face Obfuscation[1] Jan 2021
University of Wisconsin - Madison | *VMWare - NSF: Data Privacy and Edge Computing*

Face-Off: Adversarial Face Obfuscation[1] July 2021
The Internet | *Proceedings on Privacy Enhancing Technologies Symposium*

Honors and Awards

CVS Health Foundation Program Fall 2017
Scholarship for outstanding children of CVS employees

Qualcomm Innovation Fellowship (Nominee) Spring 2021
Selected abstract on autonomous vehicle domain adaptation

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

Skills

Languages: English (Native), Chinese Mandarin (Spoken-Only), Japanese (N5), French (A2)
Programming: Python, C++, JavaScript, SQL, HTML
Software Development: GitHub, Perforce, Qt, NginX, Flask, Squish, Flutter, Firebase
Machine Learning: TensorFlow, PyTorch, Pandas, NumPy, D3.js
Hobbies & Interests: Reading, Investing, Gaming, Anime, Skateboarding, Meditation

References

Kassem Fawaz kfawaz@wisc.edu
Assistant Professor | ECE Department | University of Wisconsin - Madison (608) 890-0529

Somesh Jha jha@cs.wisc.edu
Professor | CS Department | University of Wisconsin - Madison (608)-262-9519

Kang G. Shin kgshin@umich.edu
Professor | EECS Department | University of Michigan - Ann Arbor (734) 763-0391

Publications—Preprints—Journals

[1] Varun Chandrasekaran et al. "Face-Off: Adversarial Face Obfuscation". In: *21st Privacy Enhancing Technologies Symposium*. 2021. URL: https://arxiv.org/abs/2003.08861.

[2] Varun Chandrasekaran et al. "Rearchitecting Classification Frameworks For Increased Robustness". In: (2020). arXiv: 1905.10900. URL: https://arxiv.org/abs/1905.10900.

[3] Harrison Rosenberg et al. "Fairness Properties of Face Recognition and Obfuscation Systems". In: (2021). arXiv: 2108.02707. URL: https://arxiv.org/abs/2108.02707.

[4] Brian Tang et al. "Confidant: A Privacy Controller for Social Robots". In: *17th ACM/IEEE International Conference on Human-Robot Interaction*. 2022.