Soda Hall, UC Berkeley
Berkeley, CA 94709
510-423-2880
chawins@berkeley.edu
https://chawins.github.io/

Chawin Sitawarin

PhD Student, EECS Department at UC Berkeley
Interested in Machine Learning and Computer Security

Education

2018–present **PhD in Computer Science**, *UC Berkeley*, Berkeley CA.
Advisor: Professor David Wagner | GPA 3.86

2014–2018 **BSE in Electrical Engineering (High Honor)**, *Princeton University*, Princeton NJ.
Cumulative GPA: 3.90, Departmental GPA: 3.95 | Certificate in Applications of Computing

Research Interests

- Robustness of Machine Learning
- Interpretable Machine Learning
- Adversarial Examples
- Security and Privacy of Data-Driven Applications

Publications

2022 **Demystifying the Adversarial Robustness of Random Transformation Defenses**, *C. Sitawarin, Z. Golan-Strieb, D. Wagner*, ICML 2022 (Short Talk) and AAAI-22 AdvML Workshop (Best Paper), workshop, code.

2021 **Adversarial Examples for k-Nearest Neighbor Classifiers Based on Higher-Order Voronoi Diagrams**, *C. Sitawarin, E. M. Kornaropoulos, D. Song, D. Wagner*, NeurIPS 2021 (Poster), paper, code.

2021 **Improving the Accuracy-Robustness Trade-Off for Dual-Domain Adversarial Training**, *C. Sitawarin, A. Sridhar, D. Wagner*, Workshop on Uncertainty & Robustness in Deep Learning (ICML 2021), paper, code.

2021 **Mitigating Adversarial Training Instability with Batch Normalization**, *A. Sridhar, C. Sitawarin, D. Wagner*, Workshop on Security and Safety in Machine Learning Systems (ICLR 2021), paper.

2021 **SAT: Improving Adversarial Training via Curriculum-Based Loss Smoothing**, *C. Sitawarin, S. Chakraborty, D. Wagner*, AISec 2021 (co-located with CCS), paper.

2020 **Minimum-Norm Adversarial Examples on k-NN and k-NN-Based Models**, *C. Sitawarin, D. Wagner*, Deep Learning and Security Workshop 2020 (IEEE S&P 2020), paper.

2019 **Analyzing the Robustness of Open-World Machine Learning**, *V. Sehwag, A. N. Bhagoji, L. Song, C. Sitawarin, D. Cullina, M. Chiang, and P. Mittal*, AISec 2019 (co-located with CCS), paper.

2019 **Defending Against Adversarial Examples with K-Nearest Neighbor**, *C. Sitawarin, D. Wagner*, Preprint, arXiv:1906.09525.

2018 **On the Robustness of Deep k-Nearest Neighbors**, *C. Sitawarin, D. Wagner*, Deep Learning and Security Workshop 2019 (co-located with IEEE S&P), paper.

2018 **Not All Pixels are Born Equal: An Analysis of Evasion Attacks under Locality Constraints**, *V. Sehwag, C. Sitawarin, A. N. Bhagoji, A. Mosenia, M. Chiang, P. Mittal*, CCS 2018 Poster, paper.

2018 **Enhancing Robustness of Classifiers Against Adversarial Examples**, Undergraduate Thesis, Advisor: Professor Peter Ramadge.

2018 **DARTS: Deceiving Autonomous Cars with Toxic Signs**, *C. Sitawarin, A. N. Bhagoji, A. Mosenia, M. Chiang, P. Mittal*, Preprint, arXiv:1802.06430.

2018 **Rogue signs: Deceiving traffic sign recognition with malicious ads and logos**, *C. Sitawarin, A. N. Bhagoji, A. Mosenia, M. Chiang, P. Mittal*, DLS Workshop 2018 (co-located with IEEE S&P), paper.

2018 **Enhancing Robustness of Machine Learning System via Data Transformations**, *A. N. Bhagoji, D. Cullina, C. Sitawarin, P. Mittal*, CISS 2018, paper.

2018 **Inverse-designed photonic fibers and metasurfaces for nonlinear frequency conversion [Invited]**, *C. Sitawarin, Z. Lin, W. Jin and A. W. Rodriguez*, Photonics Research Vol. 6, Issue 5, pp. B82-B89, paper.

2017 **Beyond Grand Theft Auto V for Training, Testing and Enhancing Deep Learning in Self Driving Cars**, *M. A. Martinez, C. Sitawarin, K. Finch, L. Meincke, A. Yablonski, A. Kornhauser*, Preprint, arXiv:1712.01397.

2016 **Inverse-designed nonlinear nanophotonic structures: Enhanced frequency conversion at the nano scale**, *Z. Lin, C. Sitawarin, M. Lončar, A. W. Rodriguez*, Conference on Lasers and Electro-Optics (CLEO) 2016, paper.

Other Experiences

Summer 2021 **Google**, *Sunnyvale*, Research Intern.
Hosted by Ali Zand and David Tao.

Fall 2021 - Spring 2022 **Google**, *Remote*, Student researcher (part-time).
Developed threat model and appropriate evaluation for adversarial robustness in new and practical settings (e.g., dynamic models, black-box model recovery). Mentored by Nicholas Carlini.

Summer 2021 **Nokia Bell Labs**, *Remote*, Summer research intern.
Investigated relationships between causality and robustness in machine learning, focusing on leveraging causal relationship to improve robustness and generalization to unseen attacks/corruptions. Mentored by Anwar Walid.

Fall 2020 **EECS Department, UC Berkeley**, *Berkeley CA*, Graduate student instructor.
Part of the content development team for CS189/289A: Introduction to Machine Learning. Created homework problems and materials for the discussion sections and taught discussion sections.

Summer 2019 **IBM Research**, *Yorktown Heights NY*, Summer research intern.
Studied the effectiveness of existing defenses against adversarial examples from a perspective of concentration bound and improved adversarial training through optimization techniques. Mentored by Supriyo Chakraborty.

Summer 2016 **Hong Kong Applied Science and Technology Research Institute (ASTRI)**, *Hong Kong*, Summer intern in IC Digital Design team.
Implemented image processing module written in C and Matlab using Vivado High-Level Synthesis tool, and evaluated its efficiency compared to human-written RTL code.

Awards & Honors

2021 **BAIR-Microsoft Commons Project** *Research grant*

2021 **Center for Long-Term Cybersecurity (CLTC)** *Research grant*

2018 **Phi Beta Kappa** *Academic Honor Society*

2018 **Sigma Xi** *Scientific Research Honor Society*

2017 **The P. Michael Lion III Fund** *Summer research funding for Princeton engineering students*

2016 **Tau Beta Pi** *Engineering Honor Society*

2016 **Shapiro Prize for Academic Excellence** *Academic award at Princeton University*

2013 **King's Scholarship** *Prestigious scholarship awarded by Thai government for pursuing a bachelor's degree*

Activities and Services

2022 **ICML**, *Reviewer*.

2019–present **DARE: Diversifying Access to Research in Engineering**, *Mentor*, I have mentored multiple students from DARE, a program that promotes diversity in EECS undergraduate research.

2018–2020 **CSGSA**, *Treasurer*, Computer Science Graduate Student Assembly at UC Berkeley.

2018–2019 **Security Seminar**, *Organizer*, Organize a biweekly lunch seminar on security and privacy at UC Berkeley, hosting outside speakers from both industry and academia.

2016–2017 **THAIgers**, *Co-President*, Princeton Thai Student Association.