WON PARK

(408) 438-8066
won.park19@gmail.com
https://wonpark.io

EDUCATION

University of Michigan, Ann Arbor | Ann Arbor, MI GPA: 3.98
PhD candidate in Computer Science Sep 2018- 2023 (exp)

University of Michigan, Ann Arbor | Ann Arbor, MI Awarded Dec 2020

MS in Computer Science

University of California, Berkeley| Berkeley, CA
BA in Computer Science Aug 2014 - May 2018

RESEARCH EXPERIENCE

Graduate Student Research Assistant (University of Michigan, Ann Arbor) 2018-present

- PI: Z. Morley Mao

Undergraduate Research Assistant (University of California, Berkeley) 2016-2018

- PI: David Wagner

INDUSTRY EXPERIENCE

Data Science Intern at **Ericsson** May 2021 – Present
Researching anomaly detection and distributed ML techniques for application in cellular networks

Machine Learning Lead Engineer at **CloudAEye** Oct 2020 - Present
Early employee responsible for writing machine learning models used to deliver core intelligent cloud operations

Cyber Security Intern at **Sandia National Laboratories** May 2015- Nov 2016
Albuquerque, NM

CONFERENCE PUBLICATIONS

Yi Zeng*, **Won Park***, Z. Morley Mao, Ruoxi Jia. "Rethinking the Backdoor Attacks' Triggers: A Frequency Perspective". International Conference on Computer Vision (ICCV) 2021 (Under Review)

Won Park, Nan Liu, Qi Alfred Chen, Z. Morley Mao. "Sensor Adversarial Traits: Analyzing Robustness of 3D Object Detection Sensor Fusion Models". IEEE International Conference on Image Processing (ICIP) 2021

Yulong Cao, Chaowei Xiao, Benjamin Cyr, Yimeng Zhou, **Won Park**, Sara Rampazzi, Qi Alfred Chen, Kevin Fu. Z. Morley Mao. "Adversarial Sensor Attack on LIDAR-based Perception in Autonomous Driving". 26th ACM Conference on Computer and Communications Security (CCS), 2019.

Steven Chen*, **Won Park*,** Joanna Yang*, David Wagner. "Inferring Phone Location". 14th International Conference on Wireless and Mobile Computing, 2018.

* Indicates equal contribution

WORKSHOP PUBLICATIONS

Michael McCoyd**, Won Park,** Steven Chen, Neil Shah, Ryan Roggenkemper, Minjune Hwang, Jason Liu, David Wagner. "Minority Reports Defense: Defending Against Adversarial Patches". Workshop of Security in Machine Learning and its Application**, 2020 (Best Paper)**

Won Park, Qi Alfred Chen, Z Morley Mao. "Crafting Adversarial Examples on 3D Object Detection Sensor Fusion Models". CVPR Workshop on Adversarial Machine Learning in Computer Vision, 2020

Yulong Cao, Chaowei Xiao, Benjamin Cyr, Yimeng Zhou, **Won Park**, Sara Rampazzi, Qi Alfred Chen, Kevin Fu. Z. Morley Mao. "Adversarial Sensor Attack on LIDAR-based Perception in Autonomous Driving". CVPR Workshop on Adversarial Machine Learning in Real-World Computer Vision Systems, 2019.

PRESENTATIONS

"Analyzing Defense of Sensor Fusion Models Against Adversarial Examples", 2019 Michigan Engineering Research Symposium. Ann Arbor, MI, 2019

"Defending Against Adversarial Images on Deep Neural Nets" RSA Security Conference. San Francisco, CA, 2018

"The Emerging Cyber-Physical Threat: A Data-Driven Analysis of Major Cyber-Physical Attacks from Around the World" 84th MORS Symposium. Quantico, VA, 2016

TEACHING EXPERIENCE

Private Tutoring

Lumiere Mentor June 2021 – Present
Private tutor assisting high school student in ML research

Private Tutor Feb 2021 - Present
Present Tutoring in introduction to programming in Java, data structures + algorithms

Teaching Assistant UC Berkeley

Spring 2017 CS 188. Introduction to Artificial Intelligence

Fall 2017 CS 168: Introduction to the Internet

Spring 2018 CS 161: Computer Security (Head TA)

Academic Tutor UC Berkeley

Fall 2016 CS 61C: Great Ideas in Computer Architecture

Fall 2016 CS 188. Introduction to Artificial Intelligence

HONORS AND AWARDS

2020 University of Michigan Nam Center Graduate Fellow

2018 RSA Conference Scholar

"Outstanding Research Award" for Computer Science at UC Berkeley

PROFESSIONAL ACTIVITIES

Program Committee

2021 ICML Workshop on Socially Responsible Machine Learning
2021 CVPR Workshop on Adversarial Machine Learning in Real-World Computer Vision Systems
2021 ICLR Workshop on Security and Safety in Machine Learning Systems
2020 ECCV Workshop on Adversarial Robustness in the Real World
2020 IEEE Symposium on Security and Privacy, Poster Committee
2020 IEEE Symposium on Security and Privacy, Shadow Committee

OUTREACH AND SERVICE

Michigan of Engineering Grad Vlogger (5 out of 70+ candidates)

Co-chair for 2021 University of Michigan Engineering Symposium

Eta Kappa Nu Photography Chair **2019**

UMich CSEG Tea Chair and Social Chair 2019-Present

CSE Health and Wellness Co-Founder 2019- Present

Group to promote mental wellness and support for CSE graduate students