CHAOWEI XIAO

3944 BBB, 2260 Hayward St,
University of Michigan,
Ann Arbor, MI 48105
Homepage: `http://www-personal.umich.edu/~xiaocw/`

Email: chaoweixiao11@gmail.edu
Tel: (+1)734-239-2561

RESEARCH INTERESTS

Adversarial Machine Learning

EDUCATION

University of Michigan, Ann Arbor, USA — 09/2015-present
PhD student in Computer Science and Engineering.
- Advisor: Prof. Mingyan Liu.

Tsinghua University, Beijing, China — 08/2011-07/2015
B.S. in Computer Software. Advisor: Prof. Yunhao Liu.
B.S. in Economics, School of Economic and Management.

University of California, Berkeley, USA — 10/2017-05/2018
Visiting Student in Computer Science and Engineering.
- Advisor : Prof. Dawn Song and Prof. Bo Li

HONORS & AWARDS

Student Travel Award (ICLR, USENIX Security)	2018
Rackham Travel Grant	2018
Best Paper Award in MobiCom 2014, Maui, Hawaii	2014
First Prize in the 32nd Tsinghua Great Challenge Cup.	2014
Intel Chinese Outstanding Student Scholarship	2014
National Innovation and Entrepreneurship Training Program	2013,2014
Tecent Chinese Outstanding Student Scholarship	2013
First Class Scholarship for Overall Excellence	2014,2013,2012

CONFERENCE PAPERS

- **Chaowei Xiao**, Ruizhi Deng, Bo Li, Fisher Yu, Mingyan Liu, Dawn Song. *Characterize Adversarial Examples Based on Spatial Consistency Information for Semantic Segmentation.* ECCV 2018.

- **Chaowei Xiao***, Jun-Yan Zhu*, Bo Li, Warren He, Mingyan Liu, Dawn Song. *Spatially Transformed Adversarial Examples.* ICLR 2018.

- **Chaowei Xiao**, Bo Li, Jun-Yan Zhu, Warren He, Mingyan Liu, Dawn Song. *Generating Adversarial Examples with Adversarial Networks.* IJCAI 2018.

- **Chaowei Xiao**, Armin Sarabi, Yang Liu, Bo Li, Tudor Dumitra, Mingyan Liu. *From Behavior Similarity to Symptom Similarity: Using Community Detection for Early Discovery of Software Exploits.* Usenix Security 18.

- Kevin Eykholt*, Ivan Evtimov*, Earlence Fernandes, Bo Li, Amir Rahmati, **Chaowei Xiao**, Atul Prakash, Tadayoshi Kohno, Dawn Song. *Robust Physical-World Attacks on Machine Learning Models.* CVPR 2018.

- Armin Sarabi, Ziyun Zhu, **Chaowei Xiao**, Mingyan Liu, Tudor Dumitras. *Patch Me If You Can: A Study on the effects of Individual User Behavior on the End-Host Vulnerability State.* Passive and Active Measurement conference (PAM) 2017.

- Chenshu Wu, Zheng Yang, **Chaowei Xiao**, Chaofan Yang, Yunhao Liu and Mingyan Liu.
  Static Power of Mobile Devices: Self-updating Radio Maps for Wireless Indoor Localization. IEEE International Conference on Computer Communications (INFOCOM) 2015. (Acceptance Rate: 19% (316/1640))

- Lei Yang, Yekui Chen, Xiangyang Li, **Chaowei Xiao**, Mo Li and Yunhao Liu.
  Tagoram: Real-time Tracking of Mobile RFID Tags to High Precision Using COTS Devices. ACM International Conference on Mobile Computing and Networking (MobiCom) 2014. **BEST PAPER AWARD (1/220)**

WORKING PAPERS

- **Chaowei Xiao**, Xinlei Pan, Warren He, Bo Li, Jian Peng, Mingjie Sun, Jinfeng Yi, Mingyan Liu, Dawn Song.
  Characterizing Vulnerabilities of Deep Reinforcement Learning. Under submission at ICML 2019.

- Dawei Yang*, **Chaowei Xiao***, Bo Li, Jia Deng, Mingyan Liu.
  Realistic Adversarial Examples in 3D Meshes . Under submission at CVPR 2019.

- **Chaowei Xiao**, Ruizhi Deng, Bo Li,Taesung Lee, Benjamin Edwards, Jinfeng Yi, Ian Molloy, Mingyan Liu, Dawn Song.
  Characterizing Adversarial Frames in Videos Based on Temporal Information. Under submission at CVPR 2019

- **Chaowei Xiao**, Zhenbang Wang, Yulong Cao, Dawei Yang, Jin Fang, Ruigang Yang, Mingyan Liu, Bo Li.
  Adversarial Attacks Against LIDAR. Under submission at CVPR 2019

- Aria Rezaei, **Chaowei Xiao**, Bo Li, Jie Gao
  *Protecting Sensitive Hidden Attributes in IoT Data by Generative Adversarial Networks.*Under Submission at Mobisys 19. https://arxiv.org/abs/1812.10193

- 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.* Under Submission at CCS 19

- Liang Tong, Bo Li, Chen Hajaj, **Chaowei Xiao**, Yevgeniy Vorobeychik.
  Hardening Classifiers against Evasion: the Good, the Bad, and the Ugly. Major reversion at USENIX Security 19.

- Mingjie Sun, Jian Tang, Huichen Li, Bo Li, **Chaowei Xiao**, Yao Chen, Dawn Song *Data Poisoning Attack against Unsupervised Node Embedding Methods.*

Under Submission at KDD 19.https://arxiv.org/abs/1810.12881

JOURNAL PAPER

- Chenshu Wu, Zheng Yang,**Chaowei Xiao**.
  Automatic Radio Map Adaptation for Indoor Localization using Smartphones.
  IEEE Transactions on Mobile Computing (IEEE TMC) 2017.

WORKSHOP PAPER

- Kevin Eykholt*, Ivan Evtimov*, Earlence Fernandes, Bo Li, Amir Rahmati, **Chaowei Xiao**, Atul Prakash, Tadayoshi Kohno, Dawn Song.
  *Robust Physical-World Attacks on Deep Learning Visual Classification.*CV-COPS 2018

RESEARCH POSITION EXPERIENCE

Industry

Research intern, IBM Waston Research Lab, New York, USA. 06/2018-08/2018
Research intern, JD.com, Santa Clara, USA. 06/2017-08/2017
Research intern, SENSETIME Inc, Beijing, China. 01/2015-06/2015
Consulter, GUANGZHOU SECURITY INC, Guangzhou, China 05/2015-06/2015

Academia

Research Intern, Advised by Prof. Dawn Song, Computer Science and Engineering, University of California, Berkeley. 09/2017-present
Research Assistant, Advised by Prof. Mingyan Liu, Computer Science and Engineering, University of Michigan, Ann Arbor. 08/2015-present
Research Intern, Advised by Prof. Lionel Ni.M, Computer Science and Engineering, HongKong University of Science and Technology. 07/2014-09/2014
Research Intern, Advised by Prof. Yunhao Liu, School of Software, Tsinghua University 08/2013-06/2015