Chaowei Xiao

NVIDIA Research

2216 Stone Rd, Ann Arbor, MI, 48105
734-2392-561
xiaocw@umich.edu
www-personal.umich.edu/~xiaocw/
Google Scholar: citations 2300+

Research Interests

Trustworthy Machine Learning, Security & Privacy, Internet of Things & Cyberphysical System

Education

2015.8- 2020.8 **University of Michigan, Ann Arbor**.
Ph.D. in Computer Science, EECS.
Advisor: Prof. Mingyan Liu.

2011.8- 2015.7 **Tsinghua University**.
B.S. in Computer Software. Advisor: Prof. Yunhao Liu.
B.S. in Economics, School of Economic and Management.

2017.9- 2018.6 **University of California, Berkeley**.
Visiting Student in Computer Science.
Advisor: Prof. Dawn Song.

Employments

2021.8- **Arizona State University**.
Incoming Assistant Professor

2020.9- **NVIDIA Research, Santa Clara**.
Research Scientist.

2020.6- 2020.9 **University of Michigan**.
Research Fellow.

Honors & Awards

2018 Student Travel Award (ICLR, USENIX Security)
2018,2019 Rackham Travel Grant
2014 **Best Paper Award in MobiCom 2014**, Maui, Hawaii
2014 First Prize in the 32nd Tsinghua Great Challenge Cup
2014 Intel Chinese Outstanding Student Scholarship
2013,2014 National Innovation and Entrepreneurship Training Program
2013 Tencent Chinese Outstanding Student Scholarship
2012-2014 First Class Scholarship for Overall Excellence

Publications (* indicates equal contributions.)

[1] Huan Zhang, Hongge Chen, **Chaowei Xiao**, Bo Li, Mingyan Liu, Duane Boning, Cho-Jui Hsieh. *Robust Deep Reinforcement Learning against Adversarial Perturbations on State Observations*. In NeurIPS 2020 (**Spotlight**).

[2] Haonan Qiu*, **Chaowei Xiao***, Lei Yang*, Xinchen Yan, Honglak Lee, Bo Li. *SemanticAdv: Generating Adversarial Examples via Attribute-conditional Image Editing*. In ECCV 2020.

[3] Huan Zhang, Hongge Chen, **Chaowei Xiao**, Sven Gowal, Robert Stanforth, Bo Li, Duane Boning, Cho-Jui Hsieh. *Towards Stable and Efficient Training of Verifiably Robust Neural Networks*. In ICLR 2020.

[4] **Chaowei Xiao***, Dawei Yang*, Bo Li, Jia Deng, Mingyan Liu. *Realistic Adversarial Examples in 3D Meshes*. In CVPR 2019 (**Oral Presentation**).

[5] **Chaowei Xiao**, Ruizhi Deng, Bo Li, Taesung Lee, Benjamin Edwards, Jinfeng Yi, Dawn Song, Mingyan Liu, Ian Molloy. *Characterizing Adversarial Frames in Videos Based on Temporal Information*. In ICCV 2019.

[6] 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*. In CCS 2019.

[7] Liang Tong, Bo Li, Chen Hajaj, **Chaowei Xiao**, Ning Zhang, Yevgeniy Vorobeychik. *Improving Robustness of ML Classifiers against Realizable Evasion Attacks Using Conserved Features*. In USENIX Security 2019.

[8] Kin Sum Liu, **Chaowei Xiao**, Bo Li, Jie Gao. *Performing Co-Membership Attacks Against Deep Generative Models*. In ICDM 2019.

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

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

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

[12] **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*. In Usenix Security 2018.

[13] 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*. In CVPR 2018.

[14] Chenshu Wu, Zheng Yang, **Chaowei Xiao**. *Automatic Radio Map Adaptation for Indoor Localization using Smartphones*. In TMC 2017.

[15] 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*. In PAM 2017.

[16] Chenshu Wu, Zheng Yang, **Chaowei Xiao**, Chaofan Yang, Yunhao Liu, Mingyan Liu. *Static Power of Mobile Devices: Self-updating Radio Maps for Wireless Indoor Localization*. In INFOCOM 2015.

[17] 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*. In MobiCom 2014 (**Best Paper Award**).

Workshop Papers

[18] Yulong Cao*, Ningfei Wang*, **Chaowei Xiao***, Dawei Yang*, Jin Fang, Ruigang Yang, Qi Alfred Chen, Mingyan Liu, Bo Li. *Demonstration: 3D Adversarial Object against MSF-based Perception in Autonomous Driving*. In MLSys 2020 Demonstration Track.

[19] **Chaowei Xiao***, Xinlei Pan*, Warren He, Bo Li, Jian Peng, Mingjie Sun, Jinfeng Yi, Mingyan Liu, Dawn Song. *Characterizing Vulnerabilities of Deep Reinforcement Learning*. In ICML SPML 2019.

[20] Yulong Cao*, **Chaowei Xiao***, Dawei Yang*, Jin Fang, Ruigang Yang, Mingyan Liu, Bo Li. *Adversarial Objects for LiDAR-Based Autonomous Driving Systems*. In CVPR AMLCV 2019 (**Contributed Talk**).

[21] Aria Rezaei, **Chaowei Xiao**, Bo Li, Jie Gao. *Protecting Sensitive Hidden Attributes in IoT Data by Generative Adversarial Networks*. In ICML SPML 2019.

[22] Ruoxi Jia, Bo Li, **Chaowei Xiao**, Dawn Song. *Delving into Bootstrapping for Differential Privacy*. In ICML SPML 2019.

[23] 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*. In CVPR CV-COPS 2018.

Preprints

[24] Yulong Cao*, **Chaowei Xiao***, Dawei Yang*, Jin Fang, Ruigang Yang, Mingyan Liu, Bo Li. *Adversarial Objects for LiDAR-Based Autonomous Driving Systems*. https://arxiv.org/abs/1907.05418

[25] **Chaowei Xiao**, Mingjie Sun, Han Liu, Mingyan Liu, Bo Li. *Shape Features Improve General Model Robustness*. Under Submission.

[26] Mingjie Sun, Jian Tang, Huichen Li, Bo Li, **Chaowei Xiao**, Yao Chen, Dawn Song. *Data Poisoning Attack against Unsupervised Node Embedding Methods*. https://arxiv.org/abs/1810.12881

[27] **Chaowei Xiao***,Haonan Qiu*, Wenbo Guo, Gang Wang,Xinyu Xing, Mingyan Liu , Bo Li . *PaintMal: Inpainting Network Based Malware Evasion Generation*.

Selected Press

2019 Exhibition of "Physical Stop Sign" in London Science Museum.

2019 Analytics. Elon Musk Might Be Right. New Research Exposes Vulnerabilities In LiDAR-based Autonomous Vehicle.

2019 Synced. Researchers Fool LiDAR with 3D-Printed Adversarial Objects.

2017 Wired. Security News This Week: A Whole New Way to Confuse Self-Driving Cars.

2017 Fortune. Researchers Show How Simple Stickers Could Trick Self-Driving Cars

2017 SPECTRUM. Slight Street Sign Modifications Can Completely Fool Machine Learning Algorithms.

2017 Yahoo News. Researchers demonstrate the limits of driverless car technology.

2017 Telegraph. Graffiti on stop signs could trick driverless cars into driving dangerously.

Talks

Machine Learning in Adversarial Environment.

2020/3 Google Brain.

2020/3 Facebook AI Research.

2020/3 Nvidia Research.

2020/3 Uber ATG Research.

2020/3 Amazon AWS.

2020/2 Visa Research.

2020/2 Ant Finance.

2020/2 ByteDance.

Machine Learning : the Good, the Bad, and the Ugly.

2019/9 Microsoft Research, Redmond.

2019/3 Amazon Graduate Research Symposium, Seattle.

2019/2 University of Michigan, Ann Arbor.

2018/6 Baiduxlab, Sunnyvale.

Adversarial Objects for Lidar-Based Autonomous Driving System.

2019/8 Microsoft Security Workshop, Redmond.

2019/6 CVPR workshop on Adversarial Machine Learning in Real-World Computer Vision Systems, Long Beach.

Characterizing Adversarial Frames in Videos Based on Temporal Information.

2018/8 IBM Watson Research Lab.

Research Experience

Industry

2019 Microsoft Research, Redmond, USA. Research Intern at Deep Learning Group.

2018 IBM Watson Research Lab, New York, USA. Research Intern at IBM Research AI group.

2017 JD.com, Santa Clara, USA. Research Intern at JD AI and BIGDATA.

2015 SenseTime Inc, Beijing, China. Research Intern.

Academia

2017-2018 University of California, Berkeley. Advised by Prof. Dawn Song.

2014 HongKong University of Science and Technology. Advised by Prof. Lionel Ni.M.

2013-2015 Tsinghua University. Advised by Prof. Yunhao Liu.

Academia Service

Workshop/Tutorial

2020 Guest Editor for Frontiers in AI.

2019 Organzier, CVPR 2019 Adversarial Machine Learning in Real-World Computer Vision Systems.

Conference (and Journal) Program Committee/Reviewer

NeurIPS, ICML, CVPR, ICCV, ECCV, WACV, AAAI, IJCAI, GlobalSIP, USENIX Security, ASE, IJCV, TPAMI, TDSC.

Teaching & Mentoring Experience

Teaching

2019 Guest Lecturer, CS 598: Special Topics on Adversarial Machine Learning, UIUC.

2015 Teaching Assistant, Computer Network, Tsinghua University.

- Responsibilities including teaching discussion sections, creating homework and exams, and holding the office hours.

Mentoring

2018 Yulong Cao (UMich Ph.D.): Investigated and explored the spoofing attacks of Light Detection and Ranging (LiDAR) on autonomous driving system; Contributed to the physical attacks on autonomous driving system. We co-authored the ACM CCS'19 paper.

2016-2018 Ruizhi Deng (UMich B.S, SFU M.S and now SFU Ph.D.): Contributed to the spatial consistency analysis of Semantic Segmentation against adversarial attacks and the temporal consistency analysis of videos against adversarial attacks. We co-authored the ACM ECCV'18 paper and ICCV' 19 paper.

2018 Mingjie Sun (Tsinghua B.S, now CMU Ph.D.):Investigated and explored the graph poisoning attacks.

2019 Kaizhao Liang (UIUC B.S, now applying Ph.D.): Investigated the effectiveness of Interval Bound Propagation (IBP) for Training Verifiably RNN Robust Models.

2019 Max Wolff (Viewpoint school): Investigated attacks on Face verification system.

References

Mingyan Liu (mingyan@umich.edu), Peter and Evelyn Fuss Chair of Electrical and Computer Engineering, University of Michigan, Ann Arbor.

Dawn Song (dawnsong.letters@gmail.com), Professor, University of California, Berkeley.

Yunhao Liu (yunhao@cse.msu.edu), Professor, Michigan State University

Jia Deng (jiadeng@princeton.edu), Assistant Professor, Princeton University