Chaowei Xiao

University of Michigan, Ann Arbor

3944 BBB, Ann Arbor, MI, 48105
☎ 734-2392-561
✉ xiaocw@umich.edu
`www-personal.umich.edu/~xiaocw/`
Google Scholar: citations 1000+, h-index 10

Research Interests

Adversarial Machine Learning, Data Driven Security

Education

2015- **University of Michigan, Ann Arbor**.
Ph.D. Candidate in Computer Science, EECS.
Advisor: Prof. Mingyan Liu.

2011-2015 **Tsinghua University**.
B.S. in Computer Software. Advisor: Prof. Yunhao Liu.
B.S. in Economics, School of Economic and Management.

2017-2018 **University of California, Berkeley**.
Visiting Student in Computer Science.
Advisor: Prof. Dawn Song and Prof. Bo Li.

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

[2] **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*. To appear at ICCV 2019.

[3] 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*. To appear at CCS 2019.

[4] 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.

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

[6] **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.

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

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

[9] **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.

[10] 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.

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

[12] 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.

[13] 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.

[14] 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

[15] **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.

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

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

[18] 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.

Working Papers

[19] 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

[20] Haonan Qiu*, **Chaowei Xiao***, Lei Yang*, Xinchen Yan, Honglak Lee, Bo Li. *SemanticAdv: Generating Adversarial Examplesvia Attribute-conditional Image Editing*. https://arxiv.org/abs/1906.07927

[21] Huan Zhang, Hongge Chen, **Chaowei Xiao**, Bo Li, Duane Boning, Cho-Jui Hsieh. *Towards Stable and Efficient Training of Verifiably Robust Neural Networks*. https://arxiv.org/abs/1906.06316

[22] **Chaowei Xiao**, Mingjie Sun, Han Liu, Mingyan Liu, Bo Li. *Shape Features Improve General Model Robustness*. Under Submission at ICLR 2020.

Selected Press

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.

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

2017 Wired. Security News This Week: A Whole New Way to Confuse 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.

2017 Engadget. You can confuse self-driving cars by altering street signs.

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 Guangzhou Security Inc, Guangzhou, China. Consultant at TMT group.

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.

Engineer Experience

2015-2015 **SENSETIME Inc**, *Software Engineer/Research Engineer*.

- Proposed and implemented the first version of face liveness detection system.
- This system has shown to many large companies such as Tencent, JD.COM, etc and has received the investment.

2013-2014 **YIKEWANG (An Online Education Platform)**, *Software Engineer*.

- Designed and implemented the online Question-Answer system on wechat platform.
- This system has drawn 1000+ students into registration.

SKILLS

Python, Pytorch, Tensorflow, C++/C, Java, Django, HTML, CCS, Javascript, etc.