Ningfei Wang

Address: 418 ICS1, University of California Irvine, Irvine, CA, 92617
Email: ningfei.wang@uci.edu | Tel: 1-610-653-3849 | Website: http://me.ningfei.org

Summary

Focus on Machine Learning (ML) and Deep Learning (DL), including their robustness/security, application (e.g., computer vision, perception), and interpretation, especially in the context of Autonomous Driving (AD) and robotics systems.

Education

- **University of California, Irvine** California, USA
  Ph.D. in Computer Science – Advisor: Qi Alfred Chen *Sept. 2019 – Present*
- **Lehigh University** Pennsylvania, USA
  M.S. in Computer Science *Aug. 2017 – May. 2019*
- **Beijing University of Posts and Telecommunications (BUPT)** Beijing, China
  B.E. in Information Engineering *Aug. 2013 – Jun. 2017*

Work Experience

- **Machine Learning Intern** Cheetah Mobile, China
  Machine Learning Department *Mar 2017 - Jun 2017*
  - **Work Content**: Learned the algorithms of Deep Learning (e.g., Convolutional Neural Network and Recurrent Neural Networks). Accomplish LSTM algorithms. Optimized the Cheetah's input method by re-constructing the *Trie*.
  - **Skill Involved**: Machine learning algorithms(e.g., CNN, RNN, and LSTM), natural language processing

Selected Research Experience

- **Physical-World Adversarial Attack in Autonomous Driving** University of California, Irvine
  Graduate Student Researcher, ASGuard Research Group (Prof. Qi Alfred Chen) *2021 - now*
  - **Description**: Discovering new physical-world vulnerabilities in AD systems with adversarial attack. Submitted a paper to ICLR 2023.
- **Security of Multi-Sensor Fusion based Perception in Autonomous Vehicles** University of California, Irvine
  Graduate Student Researcher, ASGuard Research Group (Prof. Qi Alfred Chen) *2019 - 2021*
  - **Description**: Explored the vulnerabilities of Multi-Sensor Fusion (MSF) -based perception in autonomous driving (AD). We demonstrated our attacks can fool the MSF-based AD perception and lead the targeted AD vehicle crash into the obstacles on production-grade AD system Baidu Apollo and simulator LGSVL. Our paper was accepted by IEEE S&P 2021.
  - **Contribution**: Designed an optimization-based approach to physically attack MSF-based perception, i.e., both camera- and LiDAR-based perception, in AD systems by generating printable adversarial 3D objects. Performed comprehensive evaluations on our attack including the effectiveness, stealthiness, robustness, transferability, and physical-world realizability. Performed our attack on production-grade AD system Baidu Apollo and simulator LGSVL to demonstrate the end-to-end attack impacts.
- **Security of DNN-based Automated Lane Centering under Physical-World Attack** University of California, Irvine
  Graduate Student Researcher, ASGuard Research Group (Prof. Qi Alfred Chen) *2019 - 2021*
  - **Description**: Designed the first systematic approach to attack real-world DNN-based Automated Lane Centering (ALC) systems. Proposed an adversarial dirty road patch generation method, which considers the vehicle motion, physical-world realizability, and stealthiness. Our paper was accepted by USENIX Security 2021
  - **Contribution**: Designed an optimization-based approach to physically attack DNN-based ALC system in AD systems by generating dirty road patch. Performed comprehensive evaluations and demonstrated the attack impacts in real world.
- **Interpretable Deep Learning under Fire** University of California, Irvine / Lehigh University, USA
  Research Assistant, ALPS lab (Prof. Ting Wang) *2018 - 2019*
  - **Description**: Provided a broad class of attacks that generate adversarial inputs, which not only mislead target DNN models but also deceive their coupled interpretation models (saliency map models). The paper was accepted by USENIX Security 2020.
  - **Contribution**: Converted Caffe model and TensorFlow model into PyTorch and trained DNN (Resnet and Densenet) on ImageNet. Generated adversarial examples and their saliency map. Evaluated the success rate of the attacks and distances of saliency map between adversarial and benign examples. Proposed and explored a potential countermeasure.

Publication (* denotes equal contributions)

Conference and Journal Publications

1) *Invisible for both Camera and LiDAR: Security of Multi-Sensor Fusion based Perception in Autonomous Driving Under Physical-World Attacks*
Ningfei Wang*, Yulong Cao*, Chaowei Xiao*, Dawei Yang*, Jin Fang, Ruigang Yang, Qi Alfred Chen, Mingyan Liu, Bo Li
The 42nd IEEE Symposium on Security and Privacy in 2021 (IEEE S&P 2021)

2) *Security of Deep Learning based Automated Lane Centering under Physical-World Adversarial Attack*
Takami Sato*, Junjie Shen*, **Ningfei Wang**, Yunhan Jack Jia, Xue Lin, Qi Alfred Chen
The 30th USENIX Security Symposium in 2021

3) *Interpretable Deep Learning under Fire*
Xinyang Zhang, **Ningfei Wang**, Hua Shen, Shouling Ji, Xiapu Luo, Ting Wang
The 29th USENIX Security Symposium in 2020 (acceptance rate 16.3% = 158/972)

4) *Rendered Private: Making GLSL Execution Uniform to Prevent WebGL-based Browser Fingerprinting*
Shujiang Wu, Song Li, Yinzhi Cao, **Ningfei Wang**
The 28th USENIX Security Symposium in 2019 (acceptance rate 16.2% = 113/697)

Workshop and Poster Publications

1) *Poster: On the System-Level Effectiveness of Physical Object-Hiding Adversarial Attack in Autonomous Driving*
Ningfei Wang, Yunpeng Luo, Takami Sato, Kaidi Xu, Qi Alfred Chen
The ACM Conference on Computer and Communications Security (CCS 2022)

2) *WIP: Infrastructure-Aided Defense for Autonomous Driving Systems: Opportunities and Challenges*
Yunpeng Luo, **Ningfei Wang**, Bo Yu, Shaoshan Liu, Qi Alfred Chen
The 4th International Workshop on Automotive and Autonomous Vehicle Security (AutoSec 2022)

3) *WIP: Deployability Improvement, Stealthiness User Study, and Safety Impact Assessment on Real Vehicle for Dirty Road Patch Attack*
Takami Sato*, Junjie Shen*, **Ningfei Wang**, Yunhan Jack Jia, Xue Lin, Qi Alfred Chen
The 3rd International Workshop on Automotive and Autonomous Vehicle Security (AutoSec 2021)

4) *Demonstration: 3D Adversarial Object against MSF-based Perception in Autonomous Driving*
Ningfei Wang*, Yulong Cao*, Chaowei Xiao*, Dawei Yang*, Jin Fang, Ruigang Yang, Qi Alfred Chen, Mingyan Liu, Bo Li
The 3rd Conference on Machine Learning and Systems (MLSys 2020) Demonstration Track

5) *Poster: Security of Deep Learning based Lane Keeping Assistance System under Physical-World Adversarial Attack*
Takami Sato*, Junjie Shen*, **Ningfei Wang**, Yunhan Jack Jia, Xue Lin, Qi Alfred Chen
Network and Distributed System Security Symposium (NDSS 2020) Poster session.
Best Technical Poster Award

6) *Integration of Static and Dynamic Code Stylometry Analysis for Programmer De-anonymization*
Ningfei Wang, Shouling Ji, Ting Wang
The 11th ACM Workshop on Artificial Intelligence and Security (AISec 2018).
Best Paper Award

Academic Services

- **Program Committee**, 32nd USENIX Security Symposium (USENIX Security 2023) Artifact Evaluation (AE) 2022
- **Organizer**, Autonomous Driving CTF at DEF CON 30 (AutoDriving CTF), Las Vegas, NV 2022
- **Reviewer**, Thirty-sixth Conference on Neural Information Processing Systems (NeurIPS 2022) 2022
- **Reviewer**, The Journal of Systems & Software 2022
- **Reviewer**, ACM Transactions on Privacy and Security 2022

Selected Honors & Awards

- **The Beall Family Foundation Graduate Student Entrepreneur Award in Computer Science** 2021
- **Champion (top 1/24),** Baidu AutoDriving CTF (BCTF) 2020
- **Best Technical Poster Award (top 1/30),** Network and Distributed System Security Symposium (NDSS 2020), Poster session 2020
- **Dean's Fellowship (top 10/100+),** UCI CS Department Dean's Fellowship for AY 19/20 2019–2020
- **Dean's Award,** UCI CS Department Dean's Award 2019–2020
- **Best Paper Award (top 1/9),** The 11th ACM Workshop on Artificial Intelligence and Security (AISec 2018) 2018

Teaching

- **Discussion Session during TA, CS134: Computer and Network Security** Sept. 2021 – Dec. 2021
  Instructor: Prof. Qi Alfred Chen
- **Guest Lecturer, CS134: Computer and Network Security** Nov. 2019
  Instructor: Prof. Qi Alfred Chen
  - Guest lecture on Machine Learning Security at UC, Irvine.

Skills

- **Programming Language:** Python, C/C++, JavaScript, Matlab, R
- **Framework:** PyTorch, MySQL, Keras, Scikit-Learn, OpenCV, OpenMP