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

- **Applied Scientist Intern** Amazon
  Search Relevance Team – Mentor: Yupin Huang and Han Cheng *Jun. 2023 – Sept. 2023*
  - **Work Content**: Explored the potential vulnerabilities (e.g., adversarial example) of the DNN models (e.g., search, feature extraction, and ranking models) in Amazon. Developed mitigation (i.e., improved model robustness) for the vulnerabilities.
  - **Skill Involved**: natural language processing (e.g., transformer, BERT), adversarial machine learning.
- **Machine Learning Intern** Cheetah Mobile, China
  Machine Learning Department *Mar. 2017 - Jun. 2017*
  - **Work Content**: Optimized the “Cheetah Keyboard”, an input method for Cheetah Mobile, with deep learning (e.g., CNN and LSTM) and re-constructing the *Trie*.
  - **Skill Involved**: Machine learning algorithms (e.g., Ngram, CNN and LSTM), natural language processing.

SELECTED RESEARCH EXPERIENCE

- **Physical-World Adversarial Attack in Autonomous Driving** University of California, Irvine
  Graduate Student Researcher, AS^{2}Guard Research Group (Prof. Qi Alfred Chen) *2021 - now*
  - **Description**: Discovered new physical-world vulnerabilities in autonomous driving (AD) systems. Our paper was just accepted by ICCV 2023 (a top-tier computer vision conference).
- **Security of Multi-Sensor Fusion-based Perception in Autonomous Driving** University of California, Irvine
  Graduate Student Researcher, AS^{2}Guard Research Group (Prof. Qi Alfred Chen) *2019 - 2021*
  - **Description**: Explored the vulnerabilities of Multi-Sensor Fusion (MSF) -based perception in AD. Demonstrated that our attacks can fool the MSF-based AD perception and lead the targeted AD vehicle crash into the obstacles on industry-grade full-stack AD system Baidu Apollo. Our paper was accepted by *IEEE S&P 2021* (a top-tier computer security conference).
  - **Skill Involved**: Adversarial machine learning, object detection, differentiable rendering, LGSVL AD simulator, 3D printing.
- **Security of DNN-based Automated Lane Centering in Autonomous Driving** University of California, Irvine
  Graduate Student Researcher, AS^{2}Guard Research Group (Prof. Qi Alfred Chen) *2019 - 2021*
  - **Description**: Designed the first systematic approach to attack production-grade Automated Lane Centering (ALC) in level-2 AD systems. Proposed an adversarial dirty road patch generation method, which involves vehicle motion, physical world realizability, and stealthiness. Our paper was accepted by *USENIX Security 2021* (a top-tier computer security conference).
  - **Skill Involved**: Adversarial machine learning, lane detection, LGSVL AD simulator, OpenPilot, vehicle motion model.
- **Interpretable Deep Learning under Fire** University of California, Irvine / Lehigh University
  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). Our paper was accepted by *USENIX Security 2020.*
  - **Skill Involved**: Adversarial machine learning, model interpretation (saliency map), optimization.

- **UniGL: Preventing WebGL-based Browser Fingerprinting** Lehigh University, USA
  Research Assistant, SEC lab (Prof. Yinzhi Cao) *2017 - 2019*
  - **Description**: Developed UniGL to rewrite OpenGL shading language (GLSL). Uniformized WebGL rendering on different browsers to defend against WebGL-based browser fingerprinting. Our paper was accepted by *USENIX Security 2019*.
  - **Skill Involved**: Browser fingerprinting, WebGL, web assembly (WASM), MySQL, GLSL.

Publication (* denotes equal contributions)

Summary

- Total Citations: 372, h-index: 8, i10-index: 8 (Google Scholar, as of July 2023)
- 4 in commonly-recognized top-tier security conferences (IEEE Security & Privacy, USENIX Security, ACM CCS, NDSS)

Preprint

1) Junjie Shen, **Ningfei Wang**, Ziwen Wan, Yunpeng Luo, Takami Sato, Zhisheng Hu, Xinyang Zhang, Shengjian Guo, Zhenyu Zhong, Kang Li, Ziming Zhao, Chunming Qiao, Qi Alfred Chen, *SoK: On the Semantic AI Security in Autonomous Driving*, arXiv:2203.05314 2022

Conference & Workshop Publications

(Top-tier conferences are highlighted in **bold**)

1) [VehicleSec'23] Chen Ma, **Ningfei Wang**, Alfred Chen, Chao Shen, *WIP: Towards the Practicality of the Adversarial Attack on Object Tracking in Autonomous Driving*, Inaugural Symposium on Vehicle Security and Privacy 2023
2) [AutoSec'22] Yunpeng Luo, **Ningfei Wang**, Bo Yu, Shaoshan Liu, Qi Alfred Chen, *WIP: Infrastructure-Aided Defense for Autonomous Driving Systems: Opportunities and Challenges*, The 4th International Workshop on Automotive and Autonomous Vehicle Security 2022
3) **[IEEE S&P'21]** Yulong Cao*, **Ningfei Wang***, Chaowei Xiao*, Dawei Yang*, Jin Fang, Ruigang Yang, Qi Alfred Chen, Mingyan Liu, Bo Li, *Invisible for both Camera and LiDAR: Security of Multi-Sensor Fusion based Perception in Autonomous Driving Under Physical-World Attacks*, The 42nd IEEE Symposium on Security and Privacy 2021 (acceptance rate 12.0% = 117/972)
4) **[USENIX Security'21]** Takami Sato*, Junjie Shen*, **Ningfei Wang**, Yunhan Jack Jia, Xue Lin, Qi Alfred Chen, *Dirty Road Can Attack: Security of Deep Learning based Automated Lane Centering under Physical-World Adversarial Attack*, The 30th USENIX Security Symposium 2021 (acceptance rate 18.7% = 246/1316)
5) [AutoSec'21] Takami Sato*, Junjie Shen*, **Ningfei Wang**, Yunhan Jack Jia, Xue Lin, Qi Alfred Chen, *WIP: Deployability Improvement, Stealthiness User Study, and Safety Impact Assessment on Real Vehicle for Dirty Road Patch Attack*, The 3rd International Workshop on Automotive and Autonomous Vehicle Security 2021
6) **[USENIX Security'20]** Xinyang Zhang, **Ningfei Wang**, Hua Shen, Shouling Ji, Xiapu Luo, Ting Wang, *Interpretable Deep Learning under Fire*, The 29th USENIX Security Symposium 2020 (acceptance rate 16.1% = 157/977)
7) **[USENIX Security'19]** Shujiang Wu, Song Li, Yinzhi Cao, **Ningfei Wang**, *Rendered Private: Making GLSL Execution Uniform to Prevent WebGL-based Browser Fingerprinting*, The 28th USENIX Security Symposium 2019 (acceptance rate 16.2% = 113/697)
8) [AISec'18] **Ningfei Wang**, Shouling Ji, Ting Wang *Integration of Static and Dynamic Code Stylometry Analysis for Programmer De-anonymization*, ACM Workshop on Artificial Intelligence and Security 2018, **Best Paper Award**

Poster Publications

1) **Ningfei Wang**, Yunpeng Luo, Takami Sato, Kaidi Xu, Qi Alfred Chen, *Poster: On the System-Level Effectiveness of Physical Object-Hiding Adversarial Attack in Autonomous Driving*, The ACM Conference on Computer and Communications Security (CCS) 2022
2) Takami Sato*, Junjie Shen*, **Ningfei Wang**, Yunhan Jack Jia, Xue Lin, Qi Alfred Chen, *Poster: Security of Deep Learning based Lane Keeping Assistance System under Physical-World Adversarial Attack*, Network and Distributed System Security Symposium (NDSS) Poster session 2020, **Best Technical Poster Award**

Academic Services

Program Committee

- USENIX Security 2023 (AE): 32nd USENIX Security Symposium Artifact Evaluation (AE)
- KDD 2023: 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining
- IJCAI 2023: 32nd International Joint Conference on Artificial Intelligence

Reviewer

- NeurIPS 2023: Thirty-seventh Conference on Neural Information Processing Systems
- ICML 2023: Fortieth International Conference on Machine Learning
- ICLR 2023: Eleventh International Conference on Learning Representations
- NeurIPS 2022: Thirty-sixth Conference on Neural Information Processing Systems
- TDSC 2022: IEEE Transactions on Dependable and Secure Computing
- JSS 2022: The Journal of Systems & Software
- TOPS 2022: ACM Transactions on Privacy and Security

Organizer

- Autonomous Driving CTF at DEF CON 30 (AutoDriving CTF), Las Vegas, NV, 2022

Research Impacts

Industry Discussions & Responses

- Triggered over 30 Autonomous Driving (AD) companies such as Tesla, GM, Volkswagen, Baidu, Zoox, Hyundai, Bosch, TuSimple, Lyft, Nuro, Toyota, etc. to start investigating our newly-discovered security vulnerabilities in AD perception algorithms; some scheduled the meeting to discuss potential impacts.

Selected Honors & Awards

- **UCI ECPS Fellowship** 2023
- **Chancellor's Graduate Student Award for Undergraduate Mentorship** 2023
- **UCI ICS Innovation Fellowship** 2023
- **IEEE S&P 2022, VehicleSec 2023 student travel grant** 2022, 2023
- **USENIX Security 2021, NDSS 2022 student travel grant (virtual)** 2021, 2022
- **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

- **Teaching assistant (TA), CS134: Computer and Network Security** Sept. 2022 – Dec. 2022
  Instructor: Prof. Qi Alfred Chen
- **Teaching assistant (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