Ningfei Wang

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

Research Interests

My research predominantly focuses on the safety-critical Cyber-Physical Systems (CPS) security, such as Autonomous Driving (AD)/robotics system security, and Machine Learning (ML)/Artificial Intelligence (AI) security.

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 *Sept. 2013 – Jun. 2017*

Professional Experiences

- **Graduate Student Researcher (GSR)** UC, Irvine
  AS^{2}Guard Research Group - Advisor: Prof. Qi Alfred Chen *Sept. 2019 – Present*
- **Applied Scientist Intern** Amazon
  Search Relevance Team – Mentor: Yupin Huang and Han Cheng *Jun. 2023 – Sept. 2023*
- **Teaching Assistant (TA)** UC, Irvine
  CS 134 Computer and Network Security - Instructor: Prof. Qi Alfred Chen *Sept. 2022 – Dec. 2022 & Sept. 2021 – Dec. 2021*
- **Research Assistant (RA)** Lehigh University
  APLS lab - Advisor: Prof. Ting Wang *Sept. 2018 – Jun. 2019*
- **Research Assistant (RA)** Lehigh University
  SEC lab - Advisor: Prof. Yinzhi Cao *Mar. 2018 – Aug. 2018*
- **Research Assistant (RA)** Lehigh University
  WiNS lab - Advisor: Prof. Mooi Choo Chuah *Sept. 2017 – Dec. 2017*
- **Research Assistant (RA)** Tsinghua University
  Department of Automation - Advisor: Prof. Xiangyang Ji *Feb. 2016 - Aug. 2016*

Publication (* denotes equal contributions)

Summary

- Total Citations: 466, h-index: 9, i10-index: 9 (Google Scholar, as of Nov. 18, 2023)
- 4 in top-tier security conferences (IEEE Security & Privacy, USENIX Security)
- 1 in top-tier computer vision conferences (ICCV)

Preprint

1) Takami Sato*, Justin Yue*, Nanze Chen*, **Ningfei Wang**, Qi Alfred Chen, *Intriguing Properties of Diffusion Models: A Large-Scale Dataset for Evaluating Natural Attack Capability in Text-to-Image Generative Models*, arXiv:2308.15692 2023
2) 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) [DAC'23] Xiangguo Liu, Yunpeng Luo, Anthony Goeckner, Trishna Chakraborty, Ruochen Jiao, **Ningfei Wang**, Yixuan Wang, Takami Sato, Qi Alfred Chen, Qi Zhu, *Waving the Double-Edged Sword: Building Resilient CAVs with Edge and Cloud Computing*, The 60th ACM/IEEE Design Automation Conference

2) [**ICCV'23**] **Ningfei Wang**, Yunpeng Luo, Takami Sato, Kaidi Xu, Alfred Chen, *Does Physical Adversarial Example Really Matter to Autonomous Driving? Towards System-Level Effect of Adversarial Object Evasion Attack*, International Conference on Computer Vision 2023 (acceptance rate 26.1% = 2160/8260)

3) [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

4) [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

5) **[IEEE S&P'21] Ningfei Wang***, Yulong Cao*, 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)

6) **[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)

7) [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

8) **[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)

9) **[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)

10) [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**

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

3) 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

- MSN: International Conference on Mobility, Sensing and Networking, 2023
- USENIX Security (AE): USENIX Security Symposium Artifact Evaluation (AE), 2023
- KDD: ACM SIGKDD Conference on Knowledge Discovery and Data Mining, 2023
- IJCAI: International Joint Conference on Artificial Intelligence, 2023

Reviewer

- ICLR: International Conference on Learning Representations, 2023, 2024

- SecureComm: International Conference on Security and Privacy in Communication Networks, 2023
- NeurIPS: Conference on Neural Information Processing Systems, 2022, 2023
- ICML: International Conference on Machine Learning, 2023
- TDSC: IEEE Transactions on Dependable and Secure Computing, 2022
- JSS: The Journal of Systems & Software, 2022
- TOPS: ACM Transactions on Privacy and Security, 2022

Selected External Reviewer

- IEEE S&P: IEEE Symposium on Security and Privacy, 2024
- USENIX Security: USENIX Security Symposium, 2021, 2022, 2023, 2024
- ACM CCS: ACM Conference on Computer and Communications Security, 2021, 2023
- NDSS: The Network and Distributed System Security Symposium, 2022, 2023
- ACSAC: Annual Computer Security Applications Conference, 2020, 2022
- AsiaCCS: ACM ASIA Conference on Computer and Communications Security, 2021

Organizer

- Autonomous Driving CTF at DEF CON 30, 31 (AutoDriving CTF), Las Vegas, NV, 2022, 2023

Volunteer

- Inaugural Symposium on Vehicle Security and Privacy (VehicleSec), 2023

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

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

- **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.

- **Research advising and mentoring (Total: 8 M.S., 9 B.S.)**
  - Chen Ma (M.S. from Xi'an Jiaotong University, 2022/01–Present). Publications: VehicleSec'23 (1st author).
  - Rong Mu (B.S. from UCI, 2022/02–Present). Award: ICS Outstanding Contribution to Research Undergraduate Award, Funding supported by The Undergraduate Research Opportunities Program (UROP).
  - Nanze Chen (B.S. from UCI, 2022/09–Present). Award: ICS Outstanding Contribution to Research Undergraduate.
  - Christopher Joseph Dipalma (B.S. from UCI, 2019/09–2021/09). Publications: AutoSec'21 Demo (1st author), SafeThings'21 Demo (1st author)
  - Other advised students: Pallavi Garg (M.S. from UCI, 2023/02–2023/06), Nitesh Gupta (M.S. from UCI, 2023/02–2023/06), Shubham Bhanudas Abhale (M.S. from UCI, 2023/02–2023/06), Aditya Sanjay Dikshit (M.S. from UCI, 2023/02–2023/06), Yiwen Zhu (M.S. from UCI, 2022/09–2023/06), Chaoran Yuan (M.S. from UCI, 2022/09–2023/06), Zhiqi Xu (M.S. from UCI, 2022/09–2023/06), Chi Zhang (B.S. from UCI, 2023/02–Present), Justin Yue (B.S. from UCI, 2021/05–Present), Han Wang (B.S. from UCI, 2021/05–2022/06), Jiahao Chen (B.S. from UCI, 2021/05–2022/06), Kanglan Tang (B.S. from UCI, 2020/4–2021/04), Zeyuan Chen (B.S. from UCI, 2019/09–2021/05)

TALKS

- **Security of Multi-Sensor Fusion based Perception in Autonomous Driving Under Physical-World Attacks**
  - Security Seminar in University of California, Irvine, 2021 (Virtual)
  - The 42nd IEEE Symposium on Security and Privacy (IEEE S&P), 2021 (Virtual)
- **Towards Robustness Analysis of E-Commerce Ranking System**
  - Amazon A9 Search Relevance Team, 2023