

Ningfei Wang

Address: 3243 Donald Bren Hall, University of California Irvine, Irvine, CA, 92617
Email: ningfei.wang@uci.edu | Tel: 1-610-653-3849 | Website: <http://me.ningfei.org>

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

PROFESSIONAL EXPERIENCES

- **Graduate Student Researcher (GSR)** UC, Irvine
ASGuard Research Group - Advisor: Qi Alfred Chen Sept. 2019 – Present
- **Research Assistant (RA)** Lehigh University
APLS lab - Advisor: Ting Wang Sept. 2018 – Jun. 2019
- **Research Assistant (RA)** Lehigh University
SEC lab - Advisor: Yinzhi Cao Mar. 2018 – Aug. 2018
- **Research Assistant (RA)** Lehigh University
WiNS lab - Advisor: Mooi Choo Chuah Sept. 2017 – Dec. 2017
- **Machine Learning Engineer (Intern)** Cheetah Mobile
Machine Learning department Feb. 2017 – Jun. 2017
- **Research Assistant (RA)** Tsinghua University
Department of Automation - Advisor: Xiangyang Ji Feb. 2016 – Aug. 2016

PUBLICATION (* INDECATES EQUAL CONTRIBUTIONS)

Conference and Journal Publications

- 1) *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)
- 2) *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) *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 and Qi Alfred Chen
The 3rd International Workshop on Automotive and Autonomous Vehicle Security (AutoSec 2021)
- 2) *Demo: Security of Camera-based Perception for Autonomous Driving under Adversarial Attack*
Christopher DiPalma, **Ningfei Wang**, Takami Sato, Qi Alfred Chen
The 3rd International Workshop on Automotive and Autonomous Vehicle Security (AutoSec 2021)
- 3) *Demo: Security of Deep Learning based Automated Lane Centering under Physical-World Attack*
Takami Sato*, Junjie Shen*, **Ningfei Wang**, Yunhan Jack Jia, Xue Lin and 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 and 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

HONORS & AWARDS

- **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
- **Second Place (top 2/11)**, the Game of Go on The BUPT Mind Sports Games 2016
- **Second Prize in Beijing Region**, National College Students' Innovative Projects 2016
- **Second Prize (top 17.6% = 256/1454)**, Contemporary Undergraduate Mathematical Contest in Modeling 2015

TALKS

- **Integration of Static and Dynamic Code Stylometry Analysis for Programmer De-anonymization** Oct. 2018
Talk at AISec 2018

TEACHING

- **Guest Lecturer, CS134: Computer and Network Security** Nov. 2019
Instructor: Prof. Qi Alfred Chen
 - Guest lecture on Machine Learning Security at UC, Irvine.