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*

Selected Research Experience

- **Security of Multi-Sensor Fusion based Perception in Autonomous Vehicles** — University of California, Irvine
  Graduate Student Researcher, ASGuard Research Group (Prof. Qi Alfred Chen) — *Sep 2019 - now*
  - **Description**: Explored the vulnerabilities of Multi-Sensor Fusion (MSF) -based perception in autonomous driving (AD). We demonstrated our attacks on production-grade AD system Baidu Apollo and simulator LGSVL in MLSys 2020. The full paper was submitted to 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.
- **Interpretable Deep Learning under Fire** — University of California, Irvine / Lehigh University, USA
  Research Assistant, ALPS lab (Prof. Ting Wang) — *Sep 2018 - Sep 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.
- **Code De-anonymization** — Lehigh University, USA
  Research Assistant, ALPS lab (Prof. Ting Wang) — *Mar 2018 - Jul 2018*
  - **Description**: Developed SUNDAE, a novel code de-anonymization framework which integrates both static and dynamic stylometry analysis. The paper was accepted by the 11th ACM Workshop on Artificial Intelligence and Security and we won the **best paper award**.
  - **Contribution**: Extracted static and dynamic features (ignored by previous works) of Python source codes. Designed a stylometry matcher based on Siamese Network, which contributes to predicting the similarity of source codes from different programmers. Our approach outperformed the state-of-art methods by a margin of 45.65%.

- **UniGL: Preventing WebGL-based Browser Fingerprinting** Lehigh University, USA
  Research Assistant, SEC lab (Prof. Yinzhi Cao) *Oct 2017 - Jul 2018*
  - **Description**: Developed UNIGL to rewrite OpenGL shading language (GLSL). Uniformized WebGL rendering on different browsers to defend against WebGL-based browser fingerprinting. The paper was accepted by USENIX Security 2019.
  - **Contribution**: Converted the vertex shader to a JavaScript program and execute it. Redefined floating-point operations in fragment shader via integer simulation. Developed a website which connected with back-end MySQL database to collect rendering results and machines hardware features (e.g., DataURL, Agent).

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) *Demonstration: 3D Adversarial Object against MSF-based Perception in Autonomous Driving*
Yulong Cao*, **Ningfei Wang***, 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

2) *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

3) *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.