Junjie Shen

Address: 541 Oakside Ave Apt. D, Redwood City, CA 94063
Email: junjies1@uci.edu, Phone: +1 (919) 279-5935
Homepage: https://junjieshen.com/

Education

2016–2022 **Ph.D. in Computer Science, University of California, Irvine, CA**
Advisor: **Prof. Qi Alfred Chen**
Research Interests: Autonomous Driving Security, AI/ML Security.

2014–2015 **M.S. in Computer Engineering, North Carolina State University, Raleigh, NC**

2009–2013 **B.E. in Communication Engineering, Hangzhou Dianzi University, China**

Selected Projects

2019–2021 **Security of Deep Learning based Automated Lane Centering under Physical-World Attack**
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 attack can successfully cause a production-grade ALC system, *OpenPilot*, to drive off lane boundaries within as short as 0.95 seconds.
Skills Involved: Adversarial Machine Learning, LGSVL Autonomous Driving Simulator, OpenPilot

2018–2020 **Security of Multi-Sensor Fusion based Localization in Autonomous Vehicles**
Performed the first security analysis on the state-of-the-art Multi-Sensor Fusion (MSF) based localization algorithm in Autonomous Vehicle. Discovered a security vulnerability in the MSF design that enables the attacker to take over the localization via GPS spoofing. Our proposed attack method can deviate the vehicle to drive off-road or on the wrong-way with 97% and 91.3% success rates, respectively.
Skills Involved: Binary Analysis, Cause Analysis, Optimization, Baidu Apollo

2018–2019 **Vulnerability Discovery in Open-Source Autonomous Vehicle Systems**
Wrote fuzzing tests for open-source Autonomous Vehicle systems such as Baidu Apollo and Autoware to find software vulnerabilities. Identify the limitations of existing fuzzers.
Skills Involved: Dynamic Analysis, Cause Analysis

2017 **Compiler Assisted Simultaneous Fault and Side-Channel Attack Mitigation**
Proposed a compiler-based mitigation technique to automatically strengthen vulnerable program against fault and side-channel attacks. Results showed that it can fully mitigate power side-channel attacks, and achieves 99.47% fault coverage on average.
Skills Involved: Intel Pin, LLVM, Correlation Power Analysis

Publications

Summary: **7** in top-tier conferences across various areas, 6 of them focus on Autonomous Driving Security.

- Security (NDSS'22, USENIX Security'21, USENIX Security'20), machine learning (ICLR'20), software engineering (ICSE'20), systems (ATC'19), transportation systems (IV'21)

Conference/Journal Publications

(* denotes equal contributions; top-tier conferences are highlighted in **bold**)

NDSS'22	Ziwen Wan, **Junjie Shen**, Jalen Chuang, Xin Xia, Joshua Garcia, Jiaqi Ma, and Qi Alfred Chen. Systematic Discovery of Denial-of-Service Vulnerability in Autonomous Driving Planning under Physical-World Attacks. In *Network and Distributed System Security (NDSS) Symposium*, 2022
TRB'22	Zhen Yang, Jun Ying, **Junjie Shen**, Yiheng Feng, Qi Alfred Chen, Z Morley Mao, and Henry X Liu. Anomaly Detection in Localization Module of Autonomous Vehicles Using Learning from Demonstration. *Transportation Research Board Annual Meeting*, 2022
USENIX Security'21	**Junjie Shen***, Takami Sato*, Ningfei Wang, Yunhan Jack Jia, Xue Lin, and Qi Alfred Chen. Dirty Road Can Attack: Security of Deep Learning based Automated Lane Centering under Physical-World Attack. In *USENIX Security Symposium (USENIX Security)*, 2021. (*Acceptance rate 18.7% = 246/1316*)
IV'21	Ruochen Jiao, Hengyi Liang, Takami Sato, **Junjie Shen**, Qi Alfred Chen, and Qi Zhu. End-to-end Uncertainty-based Mitigation of Adversarial Attacks to Automated Lane Centering. In *32nd IEEE Intelligent Vehicles Symposium (IV)*, 2021
USENIX Security'20	**Junjie Shen**, Jun Yeon Won, Zeyuan Chen, and Qi Alfred Chen. Drift with Devil: Security of Multi-Sensor Fusion based Localization in High-Level Autonomous Driving under GPS Spoofing. In *USENIX Security Symposium (USENIX Security)*, 2020. (*Acceptance rate 16.1% = 157/977*)
ICLR'20	Yunhan Jia*, Yantao Lu*, **Junjie Shen**, Qi Alfred Chen, Hao Chen, Zhenyu Zhong, and Tao Wei. Fooling Detection Alone is Not Enough: Adversarial Attack against Multiple Object Tracking. In *International Conference on Learning Representations (ICLR)*, 2020. (*Acceptance rate 26.5% = 687/2594*)
ICSE'20	Joshua Garcia, Yang Feng, **Junjie Shen**, Sumaya Almanee, Yuan Xia, and Qi Alfred Chen. A Comprehensive Study of Autonomous Vehicle Bugs. In *ACM/IEEE International Conference on Software Engineering (ICSE)*, 2020. (*Acceptance rate 23.5% = 129/550*)
ATC'19	Vikram Narayanan, Abhiram Balasubramanian, Charlie Jacobsen, Sarah Spall, Scott Bauer, Michael Quigley, Aftab Hussain, Abdullah Younis, **Junjie Shen**, Moinak Bhattacharyya, and Anton Burtsev. LXDs: Towards Isolation of Kernel Subsystems. In *USENIX Annual Technical Conference (USENIX ATC)*, 2019. (*Acceptance rate 19.9% = 71/356*)
IPDPS'19	Gongjin Sun, **Junjie Shen**, and Alex Veidenbaum. Combining Prefetch Control and Cache Partitioning to Improve Multicore Performance. In *IEEE International Parallel & Distributed Processing Symposium (IPDPS)*. IEEE, 2019. (*Acceptance rate 27.7% = 103/372*)
LCPC'18	**Junjie Shen**, Zhi Chen, Nahid Farhady Ghalaty, Rosario Cammarota, Alex Nicolau, and Alex Veidenbaum. New Opportunities for Compilers in Computer Security. In *Languages and Compilers for Parallel Computing (LCPC)*. Springer, 2018
IEEE Access 2018	Yonghua Mao, **Junjie Shen**, and Xiaolin Gui. A Study on Deep Belief Net for Branch Prediction. *IEEE Access*, 2018
FDTC'17	Zhi Chen, **Junjie Shen**, Alex Nicolau, Alex Veidenbaum, Nahid Farhady Ghalaty, and Rosario Cammarota. CAMFAS: A Compiler Approach to Mitigate Fault Attacks Via Enhanced SIMDization. In *Fault Diagnosis and Tolerance in Cryptography*. IEEE, 2017

Workshops/Posters

AutoSec 2021	Kanglan Tang, **Junjie Shen**, and Qi Alfred Chen. Fooling Perception via Location: A Case of Region-of-Interest Attacks on Traffic Light Detection in Autonomous Driving. In *Third International Workshop on Automotive and Autonomous Vehicle Security (AutoSec)*, 2021
AutoSec 2021	**Junjie Shen***, Takami Sato*, Ningfei Wang, Yunhan Jack Jia, Xue Lin, and Qi Alfred Chen. WIP: Deployability Improvement, Stealthiness User Study, and Safety Impact Assessment on Real Vehicle for Dirty Road Patch Attack. In *Third International Workshop on Automotive and Autonomous Vehicle Security (AutoSec)*, 2021
AutoSec 2021	Hengyi Liang*, Ruochen Jiao*, Takami Sato, **Junjie Shen**, Qi Alfred Chen, and Qi Zhu. WIP: End-to-End Analysis of Adversarial Attacks to Automated Lane Centering Systems. In *Third International Workshop on Automotive and Autonomous Vehicle Security (AutoSec)*, 2021. **Best Short Paper Award**
NDSS Poster 2020	**Junjie Shen***, Takami Sato*, Ningfei Wang, Yunhan Jack Jia, Xue Lin, and Qi Alfred Chen. Poster: Security of Deep Learning based Lane Keeping Assistance System under Physical-World Adversarial Attack. In *Network and Distributed System Security Symposium (NDSS)*, 2020. **Best Technical Poster Award**
NDSS Poster 2019	**Junjie Shen**, Jun Yeon Won, Shinan Liu, Qi Alfred Chen, and Alexander Veidenbaum. Poster: Security Analysis of Multi-Sensor Fusion based Localization in Autonomous Vehicles. In *Network and Distributed System Security Symposium (NDSS)*, 2019. **Distinguished Poster Presentation Award**
CVPR Workshop 2019	Yunhan Jia*, Yantao Lu*, **Junjie Shen**, Qi Alfred Chen, Zhenyu Zhong, and Tao Wei. Fooling Detection Alone is Not Enough: First Adversarial Attack against Multiple Object Tracking. In *CVPR Adversarial Machine Learning in Real-World Computer Vision Systems Workshop*, 2019. **Oral Presentation**

Academic Services

Organizer	Autonomous Driving CTF at DEF CON 29 (AutoDriving CTF), Las Vegas, NV, Aug 2021
Web Chair	IEEE Workshop on the Internet of Safe Things (SafeThings), 2021
Reviewer	International Conference on Learning Representations (ICLR), 2021, 2022, 2023
Reviewer	Neural Information Processing Systems (NeurIPS), 2022
PC Member	DYnamic and Novel Advances in Machine Learning and Intelligent Cyber Security workshop (DYNAMICS), 2020
Reviewer	International Conference on Machine Learning (ICML), 2020
Reviewer	ACM Transactions on Cyber-Physical Systems (TCPS), 2020
Reviewer	International Journal of Parallel Programming (IJPP), 2016, 2018

Mentoring and Teaching Experience

Mentoring

12/19–03/21	Kanglan Tang (UCI B.S., now M.S. at UC Berkeley): **Chancellors Award for Excellence in Undergraduate Research**, **NDSS'21 Student Travel Grant**, Publication: AutoSec'21 (**1st author**)
09/19–07/20	Zeyuan Chen (UCI B.S., now M.S. at CMU): Publication: USENIX Security'20
07/18–07/19	Jun Yeon Won (UCI M.S., now Ph.D. at OSU): **NDSS'19 Distinguished Poster Presentation Award**, Publication: USENIX Security'20

Teaching Assistant

UCI	Principles in System Design, Principles of Operating Systems, Data Structure Implementation and Analysis, Parallel and Distributed Computing
NCSU	Introduction to Computer Systems, Architecture of Parallel Computers

Awards

Oct 2021	**The Beall Family Foundation Graduate Student Entrepreneur Award in Computer Science**, UC Irvine
June 2021	**Graduate Dean's Dissertation Fellowship**, UC Irvine
Feb 2021	**Best Short Paper Award** for "*End-to-End Analysis of Adversarial Attacks to Automated Lane Centering Systems*" at AutoSec 2021 (highest-scored short paper)
Sept 2020	**Champion**, The first Autonomous Driving CTF hosted by Baidu Security (top 1/24 teams)
Feb 2020	**Best Technical Poster Award** for "*Security of Deep Learning based Lane Keeping Assistance System under Physical-World Adversarial Attack*" at ISOC NDSS 2020 (top 1/30)
Feb 2019	**Distinguished Poster Presentation Award** for "*Security Analysis of Multi-Sensor Fusion based Localization in Autonomous Vehicles*" at ISOC NDSS 2019 (top 2/36)
2019–2021	**Student Travel Grants**, USENIX Security'20, USENIX Security'21, IEEE S&P'21

Work Experience

03/21–12/21	**Security Research Intern at Baidu Research, Sunnyvale, CA.** *Mentors:* **Dr. Zhisheng Hu**, **Dr. Shengjian Guo**, and **Prof. Kang Li** Organize the AutoDriving CTF on behalf of the $\mathrm{AS}^2\mathrm{Guard}$ Group at UC Irvine. Jobs include drafting DEF CON contest proposal, designing Autonomous Driving CTF challenges, deploying evaluation servers, managing and hosting the CTF at DEF CON 29 in Las Vegas. *Over 100 teams participated in the AutoDriving CTF worldwide.*
06/17–09/17	**CPU Performance Modeling Intern at Qualcomm, Raleigh, NC.** *Mentors:* **Dr. Arthur Perais** and **Dr. Luke Yen** Developed tool to extract and break down instruction critical path in microarchitectural simulator. Identified several memory accessing and control flow bottlenecks in Qualcomm's ARM-based server CPU microarchiecture design. *Received a rating of superb in the intern performance review.*
05/15–08/15	**Research Intern at AMD Research, Beijing, China.** *Mentor:* **Dr. Guoqing Chen** Characterized DNN workloads on AMD GPUs by exhaustively searching the GPU design space, e.g., computing units, GPU frequency, memory bandwidth, cache size, etc.
03/12–10/12	**Software Engineering Intern at Uniview Technologies, Zhejiang, China** Developed Linux device driver for video encoders and decoders.

Skills

Programming	C/C++, Python, Shell Script, Verilog HDL
Tools	LibFuzzer, Intel Pin, IDA Pro, Keras, TensorFlow, GDB
Platforms	Baidu Apollo, Autoware, OpenPilot, ROS, CyberRT, LGSVL Simulator, CARLA Simulator, Unity, LLVM, Linux Kernel