Junjie Shen

Address: 1013 Verano Pl, Irvine, CA 92617
Email: junjies1@uci.edu, Phone: +1 (919) 279-5935
Homepage: https://junjieshen.com/

Education

2016–present | **Ph.D. in Computer Science, University of California, Irvine, CA**
Advisor: **Prof. Qi Alfred Chen**
Research Interests: Cyber-Physical Systems Security, Adversarial Machine Learning, Vulnerability Discovery.

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–present | **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

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

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 mitigates power side-channel attacks, and achieves 99.47% fault coverage on average.
Skills Involved: Intel Pin, LLVM, Correlation Power Analysis

Conference and Journal Publications

(* denotes equal contributions)

2020	Takami Sato*, **Junjie Shen***, Ningfei Wang, Yunhan Jack Jia, Xue Lin, and Qi Alfred Chen. Hold Tight and Never Let Go: Security of Deep Learning based Automated Lane Centering under Physical-World Attack. *Under submission*, 2020
USENIX Security 2020	**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. *USENIX Security Symposium (USENIX Security) (**top-tier conference in Security**)*, 2020. (*Winter quarter acceptance rate 13.0% = 62/477*)
ICLR 2020	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) (**top-tier conference in Machine Learning**)*, 2020. (*Acceptance rate 26.5% = 687/2594*)
ICSE 2020	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) (**top-tier conference in Software Engineering**)*, 2020. (*Acceptance rate 23.5% = 129/550*)
ATC 2019	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) (**top-tier conference in Operating Systems**)*, 2019. (*Acceptance rate 19.9% = 71/356*)
IPDPS 2019	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 2018	**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 2017	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 (FDTC)*. IEEE, 2017

Workshops and Posters

NDSS Poster 2020	Takami Sato*, **Junjie Shen***, 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**

Talks

Aug 13, 2020	**Drift with Devil: Security of Multi-Sensor Fusion based Localization in High-Level Autonomous Driving under GPS Spoofing** USENIX Security Symposium 2020
Nov 27, 2019	**FusionRipper: Security of Multi-Sensor Fusion based Localization in Autonomous Driving under GPS Spoofing** Advancement to Ph.D. Candidacy Talk, UC Irvine, CA
Sept 25, 2017	**CAMFAS: A compiler approach to mitigate fault attacks via enhanced SIMDization** In Fault Diagnosis and Tolerance in Cryptography workshop, Taipei, Taiwan

Academic Services

Reviewer	ACM Transactions on Cyber-Physical Systems (TCPS), 2020
Reviewer	International Conference on Machine Learning (ICML), 2020
Reviewer	IEEE Access, 2019
Reviewer	International Journal of Parallel Programming (IJPP), 2016, 2018

Awards

Aug 2020	**Student Grant**, USENIX Security Symposium 2020
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)
July 2019	**Student Travel Grant**, UC Irvine

Work Experience

Summer 2017	**CPU Performance Modeling Intern at Qualcomm, Raleigh, NC.** *Mentors:* **Dr. Arthur Perais** and **Dr. Luke Yen** Developed a tool to extract and break down instruction critical path in microarchitectural simulator. Helped identify 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.**
Summer 2015	**Research Intern at AMD Research, Beijing, China.** *Mentor:* **Dr. Guoqing Chen** Characterized Convolutional Neural Network workloads on AMD GPUs. Exhaustively searched the GPU design space by adjusting computing units, GPU frequency, memory bandwidth, and cache size.
Summer 2012	**Software Engineering Intern at Uniview Technologies, Zhejiang, China** Developed Linux device driver for video encoders and decoders.

Skills

Programming Languages	C/C++, Python, Shell Script, Verilog HDL
Tools	LibFuzzer, Intel Pin, IDA Pro, GDB, Gem5
Platforms	LLVM, Baidu Apollo Autonomous Driving Platform, Autoware, OpenPilot, LGSVL Simulator, Linux Kernel