Junjie Shen

Address: 1013 Verano Pl, Irvine, CA 92617
Email: junjies1@uci.edu
Mobile: +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, Vulnerability Discovery, Adversarial Machine Learning.
GPA: 4.0/4.0

2014–2015 | **M.S. in Computer Engineering, North Carolina State University, Raleigh, NC**
Advisor: **Prof. Huiyang Zhou**
GPA: 4.0/4.0

2009–2013 | **B.E. in Communication Engineering, Hangzhou Dianzi University, Hangzhou, China**
GPA: 3.3/4.0

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.

Selected Projects

2018–present **Security analysis of Multi-Sensor Fusion (MSF) based Localization in Autonomous Vehicles**
Performed the first security analysis on the state-of-the-art MSF-based localization algorithm in Autonomous Vehicle. Discovered a security vulnerability in the MSF design, and proposed an attack, which can successfully deviation the vehicle by 2 meters in 10 seconds using GPS spoofing.
Skills Involved: Binary Analysis, Cause Analysis, Optimization

2018–present **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 the state-of-the-art 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

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. *arXiv preprint arXiv:1905.11026*, 2019

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 *2019 USENIX Annual Technical Conference (USENIX ATC '19)*, 2019

2019 Gongjin Sun, Junjie Shen, and Alex Veidenbaum. Combining Prefetch Control and Cache Partitioning to Improve Multicore Performance. In *IPDPS '19*. IEEE, 2019

2018 Yonghua Mao, Junjie Shen, and Xiaolin Gui. A Study on Deep Belief Net for Branch Prediction. *IEEE Access*, 2018

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 *FDTC '17*. IEEE, 2017

Workshops and Posters

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 *NDSS Poster Session*, 2019. **Distinguished Poster Presentation Award**
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. **Selected as contributed talk**

Talk

Sept 25, 2017	**CAMFAS: A compiler approach to mitigate fault attacks via enhanced SIMDization** In Fault Diagnosis and Tolerance in Cryptography workshop, Taipei, Taiwan

Skills

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