Lucas Hsiung

ljhsiun2 | lucas-hsiung | ljhsiung.com | lucas.j.hsiung@gmail.com

Professional Experience

Security and Verification Infrastructure Engineer - Nuvia/Qualcomm Aug 2020 - present

- Responsible for verifying multiple security features for Qualcomm's Oryon CPU (Trng, Pointer Auth, Performance Counters, Speculative Behavior).
- Creating end-to-end testplans across multiple blocks of a CPU for security features, and defining methodologies to aid designers in writing more secure code. Verified mitigations against current suite of side-channel attacks and made a general mitigation plan for detecting potential attacks.
- Writing linter rules to automate detecting various SystemVerilog bugs to ensure proper coding (such as completing FSM cases, ensuring boundary conditions, proper parameters)
- Within infrastructure, creating debug analysis tools such as scripts for instruction pipeline tracing and waveform data mining. Also managing simulation and regression performance, such as rewriting slow Verilog, analyzing simulator workload, and separating testbenches for large models, improving performance by up to 50%.

Security and Design Verification Engineer - SiFive Jul 2019 - Aug 2020

- Creating testplans for specific security IP blocks and building models to detect security violations
- Worked closely with the architecture team to create security properties/specifications for side-channel behavior

Undergraduate Researcher, Chris Fletcher Jan 2018 - May 2019

- Assisting in designing hardware features to mitigate security vulnerabilities with low area and performance cost. Evaluated design using benchmarks for publication
- Analyzing modern processors for various side-channel vectors e.g. cache attacks

Security Consultant Intern - Cisco Summer 2018

- Conducted on-site evaluation of companies' cybersecurity. Provided reports and presentations for external clients' records
- Conducted penetration tests on binaries, embedded devices, etc. Includes network analysis, web applications, and some policy evaluation for clients

Web Application Security Penetration Tester - TransUnion Summer 2017

- Responsible for carrying out internal reviews of Javascript and .NET codebases for security vulnerabilities. Gave monthly reviews to director on categories of bugs and risks.
- Helped design company-wide security policies and execute enforcement of said policy, such as launching fully automated internal phishing campaigns.

Projects

Elliptic Curve Cryptography on FPGA Source code

- SystemVerilog crypto accelerator implementing ElGamal's and ECDSA
- Performance and security optimizations such as Tonneli-Shanks, Barrett's reduction, constant time, etc.

Top 5 Participant at HAC@DAC2020 Event and Github Work

- Developed end-to-end exploits and comprehensive bug reports for hardware security competition
- Created miniature linter to analyze security bugs within RTL (out of bounds memory, improper reglock)

Education

University of Illinois **May 2019**

- B.S., Computer Engineering (3.29/4.0)

Publications

Fletcher, Jiyong Yu; Lucas Hsiung; Mohamad El Hajj; Christopher W. (2019). "Data Oblivious ISA Extensions for Side Channel-Resistant and High Performance Computing". In: *NDSS*, URL: https://eprint.iacr.org/2018/808.pdf.

Finalist, CSAW Applied Research Competition 2019
IEEE Micro Top Picks 2020

Teaching

ECE411, Computer Organization and Design Teaching Assistant, Spring 2019

- First semester launching revamped curriculum taught in RISC-V
- Created benchmarks to evaluate students' performance of designs. Also created tests for catching edge-case bugs in designs.

Skills

Technical Skills	C/C++, Assembly, SystemVerilog, Cryptography, ChipWhisperer, Metasploit, Reverse Engineering, Debugging, Scripting
Soft Skills	Testplanning, Diagram Design, Presentation ability, Prototyping

Related Coursework

Processor Design	- A (ECE411)	Applied Cryptography - A (ECE498AM)
FPGA Programming	- B+ (ECE385)	Operating Systems - A- (ECE391)
Computer Security	- A (CS461)	Security Laboratory - A (CS460)
Data Structures	- A (CS225)	