Shijia Wei
shijiawei@utexas.edu (512)-200-5393
https://0x161e-swei.github.io/ 3463 Lake Austin Blvd. APT E, Austin, TX 78703

A PhD student working at the intersection between security, systems, and computer architecture.

Education

- **The University of Texas at Austin** Austin, TX
  Ph.D. in Architecture, Computer Systems, and Embedded Systems (ACSES), Dept. of ECE *Dec 2022 (Expected)*
  MSE in Electrical and Computer Engineering, Dept. of ECE. GPA: 3.83/4.0 *May 2019*
  Related Courses: Security at the Hardware Software Interface, Distributed Systems, Computer Architecture, Parallelism and Locality, Prediction Mechanisms in Comp. Arch., Performance Evaluation and Benchmarking
- **Zhejiang University** Zhejiang, China
  B.Eng. in Computer Science, Chu kochen Honors College. GPA: 3.82/4.0. *June 2016*

Publications

[1] *"Morpheus II: A RISC-V Security Extension for Protecting Vulnerable Software and Hardware"*, A. Harris, T. Verma, **S. Wei**, A. Kisil, M. T. Aga, V. Bertacco, B. Kasikci, M. Tiwari, T. Austin, to appear in **HOST 2021**.

[2] *"Cyclone: Detecting Contention-Based Cache Information Leaks Through Cyclic Interference"*, A. Harris*, **S. Wei***, P. Sahu, P. Kumar, T. Austin, M. Tiwari (*=co-primary authors), in **MICRO 2019**.

[3] *"Using Power-Anomalies to Counter Evasive Micro-Architectural Attacks in Embedded Systems"*, **S. Wei**, A. Aysu, M. Orshansky, A. Gerstlauer, M. Tiwari, in **HOST 2019**, Best Paper Finalist.

Experience

- **Graduate Researcher at Spark Research Lab, UT Austin** August 2016 - Present, Austin, TX
  - **Silo**: Understanding the isolation of security domains at the app-layer (Chromium site-isolation, Cloud function isolation).
    - Characterized system and hardware impact for process-level isolation for tens and hundreds of security domains.
  - **Terminator**: Leaking secrets from termination-timing channel for privacy sensitive database, browser, and graph programs.
    - Break state-of-the-art predictive mitigation with statistical analysis on programs beyond cryptographic kernels.
  - **Cyclone**: Micro-architecture enhancement to detect micro-architectural information leaks through cyclic interference [2].
    - *Cycles of directional interference* between security domains is fundamental to both resource contention (prime+probe family) and memory contention (flush/evict+reload) attacks.
    - Cyclone detects cache attacks (e.g. Prime+Probe) and speculation-driven attacks (e.g. Spectre) with orders of magnitude lower false positive rate relative to using best-known prior work (that track performance counters or contention alone).
    - Enhanced Linux kernel and WebKit to isolate JS origins; Evaluated Cyclone with Gem5 OoO full system simulator.
  - **Power-Anomaly**: Detecting evasive micro-architectural attacks in embedded systems as power anomalies [3].
    - Design and implement ML detectors(e.g. LSTM) on power-traces to detect evasive Spectre and Rowhammer attacks.
  - **Lean Stack**: Programmable accelerator to offload application-layer routing and functions for serverless applications
    - Implemented using Chisel on an x86-FPGA server, and evaluated on Memcached, ELK Stack.
- **Research Intern at Facebook AI Research** May 2020 - Dec. 2020, Remote
  - **Automatic Optimizing Partition Scheme for Enclave Applications**:
    - Developed LLVM-based static program analysis and threat modeling for Augment Reality algorithms.
    - Developed a tool that searches optimal partition boundary based on static program analysis and dynamic profiling.
    - Built performance characterization of SGX overhead regarding TLB and cache pressure.
- **Co-op Engineer at AMD Research** May 2017 - August 2017, Austin, TX
  - **Instruction-level Power Model for Data-center Processors (Patent pending)**:
    - Developed a power model that decouples instruction baseline energy from power consumed by micro-architectural events.
    - Developed a parallel tool that automates annotation of hot code path for AMD Instruction-Based-Sampling (IBS) Toolkit.
- **Undergrad Researcher at DASlab, Harvard University** September 2015 - May 2016, Cambridge, MA
  - **Workload-Aware Column-Store**: Heuristic based range partitioning for column-store data systems

Selected Class Projects

- **Memcache-SGXd**: Evaluated different porting schemes (e.g. SCONE, code partitioning, etc.) to secure Memcached in SGX on Azure for various threat models. Evaluated optimization schemes like dedicated syscall threads and reducing boundary crossing.
- **I-Cache Replacement Policy**: Designed and developed an I-cache replacement policy based on run-time basic block signatures, improving Cloud workload performance for Node.js applications—**I-Cache miss rate (MPKI) reduced by up to** 7×.
- **Performance Evaluation between FPGA and GPU**: Performance study using, Cuda, OpenCL for GPU and FPGA, on embarrassingly parallel applications like matrix-multiplication, bloom filter, and single-source-shortest-path.
- **Remote Attacks on ARM**: Implemented successful Rowhammer, AnC, and Spectre in JavaScript.

Skills

Languages C/C++, Python, Bash, Go, x86/ARM Assembly, SQL, Java, Verilog
Tools Gem5, LLVM, PINTool, AMD IBS, PAPI, Perftools, VTune, Git, Kubernetes