Shijia Wei
shijiawei@utexas.edu (512)-200-5393
https://0x161e-swei.github.io/ Google Scholar

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

Education

- **The University of Texas at Austin** Austin, TX
  Ph.D. in Electrical and Computer Engineering, Dept. of ECE *Jan 2024 (Expected)*
  MSE in Electrical and Computer Engineering, Dept. of ECE. *May 2019*
  Architecture, Computer Systems, and Embedded Systems track (ACSES/CAEP)
  GPA: 3.83; 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: 3.98 *June 2016*

Selected Publications

[4] *"Revisiting Browser Performance Benchmarking from an Architectural Perspective"*, Y. Zhu, **S. Wei**, M. Tiwari, in **IEEE CAL**.
[3] *"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, 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**.
[1] *"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 Research Assistant at Spark Research Lab, UT Austin** September 2016 - Present, Austin, TX
  - **Silo**: Understanding the isolation of security domains at the app-layer (Chromium site-isolation, Cloud function isolation).
    - System and hardware performance characterization using TopDown microarchitectural analysis on isolating 100s of domains.
  - **Triton**: Secure multi-tenant ML-inference accelerators with software-defined threat models.
    - Reduced secure accelerator performance overhead from over 95% to less than 5% by tailoring threat models at deployment time.
  - **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 and memory contention attacks.
    - Cyclone detects cache attacks (e.g. Prime+Probe) and speculation-driven attacks (e.g. Spectre) with up to 1000× lower false positive rate relative to using best-known prior work (that tracks 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 (Spectre, Rowhammer) in embedded systems [1].
    - Design and implement ML (LSTM, CNN) based anomaly detectors on power-traces to detect evasive 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 Microsoft Azure** May 2022 - Aug. 2022, Remote
  - **Advancing Hardware Root-of-Trust for Confidential Computing in Heterogeneous Systems with FPGAs**:
    - Performed software and hardware threat-modeling, requirements analysis for trusted-component measurement and attestation.
    - Designed and implemented proof-of-concept RISC-V cores to evaluate cost and performance trade-offs.
- **Research Intern at Facebook AI Research** May 2020 - Dec. 2020, Remote
  - **Partition-Boundary Optimization for Enclave Applications**: using LLVM-based static and dynamic program analysis
    - Developed a boundary optimization tool with detailed performance characterization of SGX overhead in TLB and cache.
- **Co-op Engineer at AMD Research** May 2017 - August 2017, Austin, TX
  - **Patented Processor Power Model**: Instruction-level power model using AMD Instruction-Based-Sampling (IBS)
- **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

Teaching and Services

- **Reviewer**: IEEE MICRO (2019, 2022), IEEE TACO (2019, 2020), IEEE TVLSI (2020), ACM ToPS (2021)
- **Artifact Evaluation Committee**: MICRO'21, ASPLOS'22, USENIX Security'22
- **Organizer**: *ISCA'19 Tutorial: Side and Covert Channels: Attacks and Defenses*
- **Guest Lecturer**: *Information System Security* 2019, *Computer Architecture* 2019, *Security* 2022
- **Volunteer**: VLDB 2014, HPCA/CGO/PPoPP 2017
- **Teaching Assistant (UT Austin)**: *Real-Time Bluetooth Networks (edX)* 2016; *Introduction to Embedded Systems* 2017
- **Teaching Assistant (ZJU)**: *Computer Organization* 2014, *Introduction to Computing Systems* 2015