

# Zane Weissman

Cybersecurity || Microarchitectural Security || FPGA || Embedded Computing  
488 Plantation St, Worcester MA 01602  
+1-510-407-1958 | zweissman@wpi.edu | www.zaneweissman.net

I am a Ph.D. researcher at Worcester Polytechnic Institute studying microarchitectural security threats to modern cloud systems. I have published two papers presenting new threats posed by FPGAs in the cloud, and I have substantial experience with embedded systems. I am currently looking for positions in cybersecurity, computer architecture, FPGA implementation, or embedded systems design.

## Education

### Worcester Polytechnic Institute (WPI)

Worcester, MA

Ph.D. in Electrical and Computer Engineering

- *Research assistant under supervision of Prof. Berk Sunar*
- *Teaching assistant for graduate and undergraduate classes*

2019 - Present

M.S. in Electrical and Computer Engineering

2017-2019

B.S. *cum laude* in Electrical and Computer Engineering

2015-2019

## Skills and Knowledge

- Programming and Math**
- **C/C++, Assembly** (x86, ARM, SIMD), Matlab, Python, R, (System)Verilog, LaTeX, Bash
  - **Embedded systems programming** including RTOS, task scheduling, interrupts, semaphores and data sharing, timers and clocks, serial interfaces, ADCs and DACs, digital I/O
  - **Linux development** including kernel driver development and kernel image compilation
  - **Private and public key cryptography** including RSA, AES, ECDSA; security protocols including Diffie-Helman key exchange, SSL/TLS, WEP, WPA
  - **Machine learning** including DNN, CNN, SVM, decision tree and random forest, KNN, regression, bootstrap aggregating, dimensionality reduction and feature extraction

- Electronics and Design**
- **Microarchitectural design** including inclusive and non-inclusive cache organization, pipelines, branch prediction, parallelism, out of order execution and Tomasulo's algorithm
  - **Microarchitectural vulnerabilities** including Spectre and Meltdown/MDS-class speculative execution vulnerabilities, cache timing side-channel techniques, and common defenses and countermeasures in software, firmware, and hardware
  - **Digital and analog circuits**, VLSI design, function generators and oscilloscopes, soldering, serial and parallel interfaces, discrete, continuous, and probabilistic signals

**Software tools** GNU Toolchain, Git, Eclipse, TI Code Composer Studio, Xilinx Vivado, Intel Quartus, Synopsys Design Compiler, QEMU, libvirt, Linux distributions based on Debian, Red Hat, and Arch

## Experience

Worcester, MA

### Ph.D., Vernam Cybersecurity Lab

Jan 2019-Present

Research assistant under supervision of Prof. Berk Sunar

### Jackhammer: a powerful and stealthy Rowhammer implementation for FPGAs

- Designed Jackhammer, an FPGA implementation of a **Rowhammer** attack that causes twice as many hardware faults as a comparable CPU-based attack.
- Reverse-engineered the memory and cache subsystems of two **heterogeneous** FPGA-CPU compute

platforms based on the PCIe-based Intel Arria 10 GX FPGA.

- Discovered a fault-injection vulnerability in WolfSSL's RSA library and demonstrated a practical attack with Jackhammer with 25-200% performance gains over CPU-based Rowhammer exploits.

#### **IOTLB-SC: a new side-channel cache attack against PCIe memory address translation hardware**

- Hypothesized and proved the existence of IOTLB-SC, a side-channel vulnerability in IOTLBs, the translation caches of the hardware units that perform peripheral-to-CPU memory address translation.
- Developed a kernel driver to manipulate the IOTLB and assist with debugging the side-channel.
- Used a custom FPGA function to collect traces from a network card using the IOTLB-SC side-channel.
- Analyzed the threats that IOTLB-SC poses to hardware functions, device drivers, and applications, and proposed countermeasures for applications, cloud infrastructure, and memory translation hardware.

#### **Microarchitectural security analysis of AWS Firecracker virtual machines**

- Analyzed security model of AWS's Firecracker MicroVM designed for serverless cloud platforms.
- Tested Firecracker's defenses against MDS and Spectre microarchitectural attacks.
- Found variants of each that pose significant threats to cloud platforms using Firecracker for isolation, even using a recommended system setup with common microarchitectural defenses in place.
- Provided additional system and application security recommendations for Firecracker-based platforms.

Worcester, MA      **WPI Capstone Project**

Aug 2018-May 2019      Modular Electronic Skateboard

- Designed onboard software for a smart, modular electronic skateboard: implemented motor control systems and data logging on remote database.
- Collaborated with hardware and database designers to ensure system interoperability.
- Presented work in a technical report, a poster, and a short presentation.

Worcester, MA      **Battle of the Rockets**

Jan 2016-April 2017      Leader of Lander Design Team

- Managed 5 students designing and building an autonomous lander. Led development of system software and electronics. Oversaw design and manufacture of mechanical systems.
- Lander was launched from a rocket at a height of over 1000 feet and awarded 2<sup>nd</sup> place in competition.

Newark, CA      **Softiron Inc.**


June 2016-Aug 2016      Assembly and Testing Intern


- Tested server motherboards, RAM, and other components.
- Assembled and packed server units for shipment.
- Managed parts inventory, wrote scripts to print labels, and assisted with other odd jobs.

## **Publications**


"Microarchitectural Vulnerabilities Introduced, Exploited, and Accelerated by Heterogeneous FPGA-CPU Platforms," in Security of FPGA-Accelerated Cloud Computing Environments, edited by J. Szefer and R. Tessier, Springer, forthcoming.

Microarchitectural Security of AWS Firecracker VMM for Serverless Cloud Platforms, under review.

IOTLB-SC: An Accelerator-Independent Leakage Source in Modern Cloud Systems, ACM ASIA CCS, 2023, forthcoming. 

JackHammer: Efficient Rowhammer on Heterogeneous FPGA-CPU Platforms, IACR TCHES, 2020, Issue 3 

## **Conferences**

hardwear.io 2020, JackHammer: Rowhammer and Cache Attacks on Heterogeneous FPGA-CPU Platforms, D. Moghimi, T. Tiemann, and [Z. Weissman](#). 

Cryptographic Hardware and Embedded Systems (CHES) 2020, JackHammer: Efficient Rowhammer on Heterogeneous FPGA-CPU Platforms, [Z. Weissman](#), T. Tiemann. 