Lowell, Ma
Linkedin

Andrew Adiletta

(978) 735 9666
ajadiletta@wpi.edu

Embedded security engineer and PhD researcher specializing in microarchitectural security for AI and advanced computing platforms. Adept at fault injection, side-channel analysis, and hardware security, I combine a deep understanding of secure system design with cutting-edge research in AI/LLM hardware defenses. I am seeking a Research Scientist role where I can drive innovations in security and privacy for next-generation AI systems.

Work Experience

Senior Embedded Security Researcher — **MITRE** — **Aug. 2023 - Present**
Project Lead – Fault Injection Studies — Bedford, Ma — Secret Clearance

- Investigated protections for Rowhammer and DVFS-FI on modern platforms
- Accelerated discovery, characterization, actuation, and demonstration of Rowhammer and DVFS-FI
- Shared results with Gov. stakeholders on cutting edge hardware security research

Pre-silicon Validation Engineer — **Intel** — **2019-22 (22 months)**
Fault Tolerant Validation Utility — Hudson Ma

- Expanded graph-based validation checker, improving runtime and resource efficiency
- Produced internal white paper on benefits of graph-based validation, leading to widespread adoption
- Implemented validation for various power systems related flows for SoC servers

Publications

Spill The Beans: Exploiting CPU Cache Side Channels to Leak Tokens from LLMs

- Discovered novel side channel targeting LLMs via a CPU cache sidechannel
- Enabled by CUDA GPU cache coherency protocols with the CPU cache, allows Flush+Reload token leakage
- Paper: https://arxiv.org/pdf/2505.00817

LeapFrog: The Rowhammer Instruction Skip Attack (EuroS&P, 2025)

- Developed Rowhammer gadget called LeapFrog, enables control flow subversion, TLS & OpenSSL attacks
- Presented findings at Hardwear.io in Santa Clara, California (2024)
- Paper: https://arxiv.org/abs/2404.07878

Mayhem: Targeted Corruption of Register and Stack Variables (AsiaCCS, 2024)

- Groundbreaking attack on stack, register variables using Rowhammer (SUDO, OpenSSH, OpenSSL)
- Bypassed stack Address Space Layout Randomization (ASLR) in the Linux kernel
- Presented "Mayhem: Targeted Corruption of Register and Stack Variables" at AsiaCCS 2024 in Singapore
- Paper: https://arxiv.org/abs/2309.02545

Don't Knock! Rowhammer at the Backdoor of DNN Models (DSN, 2023)

- Coauthored paper on backdoor injection attacks on machine learning algorithms using fault injection
- Presented "Don't Knock! Rowhammer at the Backdoor of DNN Models" at DSN conf in Porto, Portugal
- Paper: https://arxiv.org/abs/2110.07683

Education and Certifications

- **PhD ECE (GPA 4.0),** Vernan Lab - Worcester Polytechnic Institute — **2021-(Exp. Fall 2025)**
- **MS ECE (GPA 4.0),** Vernan Lab **-** Worcester Polytechnic Institute — **2021-2023**
- **BS ECE (GPA 4.0),** Worcester Polytechnic Institute (Dearborn Scholar, WPI Presidential Scholar) — **2019-2022**

Technologies & Interests

- Technologies: Literature to Practice Proficiency, Remote Fault Injection/Side Channel Expert
- Interests: Underwater hockey, Guitar/Piano, hiking, running, weight-lifting, cooking