Pranav Kumar

pranavk2.github.io
pranavkumar@utexas.edu
Mob: (737) 346-1748

Education

- **University of Texas at Austin** — Austin, TX
  M.S. in ECE (Architecture, Computer Systems and Embedded Systems track); GPA: 4.00 — *July 2017 – May 2019*
- **Indian Institute of Technology Kanpur** — Kanpur, India
  B.Tech. in Electrical Engineering, Minor in Computer Systems; GPA: 9.0/10.0 (Major: 9.3) — *July 2013 – May 2017*

Skills

- **Languages**: C, C++, Java, Python, Verilog, x86/ARM assembly, SystemC
- **Software and Tools**: gem5, MATLAB, Tensorflow, git, PAPI, perf, PinTool, McPAT, Vivado HLS, ModelSim, Spice

Internship

- **ARM Research** — Austin, TX
  Manager: Dr. Prakash Ramrakhyani — *May 2018 – Aug 2018*
  - **Cache-Based Side-Channel Attack Mitigations**: Proposed two new techniques: *Context-Aware Cache Management* and *Cryptic Cache Architecture* for defending against same or different-core cache-based timing side channel attacks like Prime-Probe and Flush-Reload. Evaluated trade-offs between cache performance and security.

Experience and Projects

- **Spark Research Lab, UT Austin** — Austin, TX
  Graduate Research Assistant, Advisor: Prof. Mohit Tiwari — *July 2017 – present*
  - **Contention in Function-as-a-Service (FaaS) Systems**: Benchmarked AWS Lambda for various network, OS and compute (INT and FP) latencies and determined on an OpenFaaS-based system locally if contention between lambdas could be a performance bottleneck.
  - **Performance Counters Based Software Anomaly Detection**: Designed a machine learning based anomaly detector that models microarchitectural attacks as behavioral anomalies in terms of security-critical performance counters. Showed how these detectors can easily break via adversarial examples. Work presented at **CFAR**[1], **SARC**[2] and **Western Digital**[3].
  - **Hardware-Based Malware Detection**: Implemented a mechanism to detect side and covert-channel attacks in the microarchitecture via *trusted* and *untrusted* label propagation and subsequently locally detecting label contention on L1/LLC/BPred/MemBus and physical memory addresses. Additionally, a global detector reduced false positives.
  - **Database of Side-Channel Attacks on gem5**: For evaluation of such a hardware mechanism, implemented covert-channel attacks through caches, memory bus, branch predictor and also ported Rowhammer, Spectre attacks to AArch64 on gem5. Implemented two versions: standalone attacks and attacks leaking sensitive information from privacy-critical apps.
- **Architecture, Systems and Security**:
  - **Architecture**: Implemented exclusive caches in ChampSim, implemented and evaluated different branch predictors and a 4-stage pipeline in MIPS simulator, implemented a simple in-order 8-bit microprocessor in Verilog on FPGA.
  - **Performance Evaluation & Benchmarking**: Instrumented and evaluated workloads (SPEC2017, LLL etc.) using PINTool and performance monitoring counters, evaluated localities in them via RAW, WAW, WAR distributions, used gem5+McPAT with MiBench embedded benchmarks to evaluate trade-offs in performance, power and energy.
  - **System-on-Chip Design**: Identified bottleneck for Darknet execution on ARM: GEMM execution, isolated it into a SystemC-modeled hardware module and accessed it via HAL, synthesized the GEMM accelerator.
  - **Operating Systems**: Implemented system calls, scheduling and page replacement algorithms on NachOS.
  - **Security**: Implemented RSA, AES accelerators on RISC-V core; found buffer overflow vulnerabilities, wrote stack-smashing and return-2-libc exploits, mounted side-channel attack on MySQL queries and DPA attack to obtain AES key.
- **Machine Learning and Image Processing**:
  - **Machine Learning**: Projects on PCA, ICA, learning human movement using Gaussian processes, implementing Pac-Man via reinforcement learning and CNN applied on MNIST.
  - **3D Display**: Real-time 3D viewing based on face posture on your laptop. **Top 5 at Ericsson Innovation Awards**.

Courses

* ongoing

- **Computer Systems**: Computer Architecture, Comp Arch: User-System Interplay*, HW-SW Security, Performance Evaluation and Benchmarking, SOC Design*, Operating Systems, Microarchitecture, Digital Electronics, Analog/Digital VLSI Circuits
- **Mathematics and Algorithms**: Probability and Statistics, Machine Learning, Data Structures and Algorithms

Leadership Positions

• **Head TA**, Fall 2018 - Security at the Hardware-Software Interface (graduate security course) • **President**, UT Graduate ECE Student Association • **ECE Department Representative**, UT Graduate Engineering Council

[1] Center for Future Architectures Research, University of Michigan, Ann Arbor
[2] Samsung Austin Research Center
[3] 7th RISC-V Workshop, Milpitas CA