PRATEEK SAHU

(737) 207-2578 ⋄ prateeks@utexas.edu
https://www.linkedin.com/in/sahuprateek/ ⋄ https://prateeksahu.github.io

EDUCATION

University of Texas at Austin *August 2017 - Present*
Ph.D., Computer Architecture. GPA: 3.79/4
Indian Institute of Technology, Kanpur *July 2011 - May 2015*
Bachelor of engineering, Electrical. GPA: 8.2/10

PUBLICATIONS

Behnia, M., **Sahu, P.**, Paccagnella, R., Yu, J., Zhao, Z., Zou, X., Unterluggauer, T., Torrellas, J., Rozas, C., Morrison, A., Mckeen, F., Liu, F., Gabor, R., Fletcher, C.W., Basak, A., Alameldeen, A. (2020, July). *Speculative Interference Attacks: Breaking Invisible Speculation Schemes* arXiv 2007.11818. [pdf]

Harris, A., Wei, S., **Sahu, P.**, Kumar, P., Austin, T., Tiwari, M. (2019, October). *Cyclone: Detecting Contention-Based Cache Information Leaks Through Cyclic Interference.* In Proceedings of the 52nd Annual IEEE/ACM International Symposium on Microarchitecture (pp. 57-72). ACM. [pdf]

WORK EXPERIENCE

Interests: Architecture, Systems & processor security, Hardware/Software for performance & efficiency

SPARK Reasearch Lab, University of Texas at Austin
Graduate Research Assistant, Advised by Prof. Mohit Tiwari *Spring 2018 - Present*

- **Cyclone: Detecting Contention-Based Cache Information Leaks Through Cyclic Interference.**
  - Micro-architectural malware detector based on resource contention
  - Novel property of contention direction across security labels
  - Evaluate against cache based side and covert channels like prime-probe and spectre
  - Evaluation of system based on ARM v8 ISA in gem5 full system simulation
- **Speculative Interference Attacks: Breaking Invisible Speculation Schemes**
  - Speculative attack vectors which exploits younger instruction affecting older instruction latency
  - Undermines current state-of-the-art defense mechanisms
  - Proof-of-concept attacks on caches.
- **Systems design and security in micro-service architectures**
  - Performance evaluation of current architectures for micro-service type workloads
  - Architectural implications of data-plane proxies and service-mesh designs
  - Security impacts of FaaS/serverless platforms in cloud environment
- **QoS and efficiency for serverless computing platforms**
  - Identify bottlenecks and opportunities in a serverless platform for better runtime resource orchestration
  - Explore bump-in-the-wire FPGA accelerator solutions to improve latency of microservices

Intel Labs, Intel Corp.
Graduate Technical Intern *June 2020 - Nov 2020*

- **Secure Accelerator Design**: Design of secure data offload to Accelerators
  - System design for remote attestation
  - Proof of concept designs for key provisioning and secure data offload

Qualcomm Technologies Inc.
Engineering Intern *May 2019 - July 2019*

- **Hexagon QDSP Design**: Design and Verification of QDSP6 Control Unit
  - Architectural design for SMT in QDSP6 Control Unit and implications
  - Formal verification of existing RTL design to find hardware scheduler bugs

VMware India Software Pvt. Ltd
Member of Technical Staff *July 2015- June 2017*

- **Cloud Management**: Private cloud resource and cost monitoring tool using utilization statistics
  - Containerized micro-services for efficient and scalable application design
  - Invention Disclosure Form(IDF) filed for system health monitoring tool using vSphere metrics

SELECT COURSE PROJECTS

Verilog system design for 32-bit x86 ISA *Microarchitecture Course, Dr. Y. Patt*
CPU design of a pipelined machine with memory & branch predictor for subset of x86 ISA. [Report]
Intelligent instruction duplication for side-channel defence *Security Course, Dr. M. Tiwari*
Compiler solution for duplication of instructions which work on dummy data. [Report]
Low-power real-time object recognition SoC design *SoC Design, Dr. A. Gerstlauer*
FPGA design and implementation of GEMM module of YOLO model. [Report]

RELEVANT COURSES

Computer Architecture | Operating Systems | Security in HW/SW Systems | Micro-architecture

SKILLS

Languages	C, C++, Java, Verilog, Python, Bash, x86/ARM Assembly
Software & Tools	gem5, Docker, Kubernetes, qemu, Vivado HLS, Matlab, Synopsis Verdi