Pranav Kumar

First Year Graduate Student
Department of Electrical and Computer Engineering
The University of Texas at Austin

Web: pranavk2.github.io
E-mail: pranavkumar@utexas.edu
Phone: 1-737-346-1748

RESEARCH INTERESTS

Computer Architecture, Machine Learning and Security

EDUCATION

- **The University of Texas at Austin** Expected: May 2019
  Masters in Electrical and Computer Engineering – **Cumulative GPA: 4.0**
  Advisor: Prof. Mohit Tiwari
  Research Topics: Machine learning centric security.
- **Indian Institute of Technology Kanpur, India** – **9.0/10** (**9.3/10** in major) 2017
  Bachelor in Electrical Engineering and *Minor* in Computer Systems
- **Class XII** - Indian School Certificate (ISC) - **95.2%** 2012

RESEARCH at SPARK Lab (UT Austin)

- **Detecting Advanced Malware as Instruction and Microarchitectural Anomalies** Fall 2017
  Mentored by Prof. Mohit Tiwari, Dept. of ECE, UT Austin [Report] [Slides]
  - Aim was to design and evaluate Hardware-based Malware Detectors (HMDs) against a broad class of advanced malware.
  - Intelligently iterated through and chose a set of hardware performance counters that modeled program execution precisely, a bag-of-words feature extraction algorithm and an XGBoost classifier as the design for our HMD.
  - Tested it against memory exploits, side channels, covert channels and microarchitectural timing channels on x86 systems with good results. Exploits like code-reuse attacks, ransomware and flush+flush cache attack were not detected.
  - Thus, explained the shortcomings of current systems and subsequently the need and proposed design for a RISC-V based solution.
  - Work done was presented at **CFAR** (Center for Future Architectures Research) Annual Research Review 2017 at the University of Michigan, Ann Arbor; has been **submitted to ISCA 2018** and was presented at the 7^{th} **RISC-V Workshop** in Milpitas CA.

- **An Architecture for Configurable Anomaly Detection**
  Mentored by Prof. Mohit Tiwari, Dept. of ECE, UT Austin Ongoing
  - To detect hardware-based attacks, embedding security primitives into the architecture.
  - Implementing programmable local detectors (histogram, n-gram) at various microarchitectural components and global detector (RFC, SVM) as a microcontroller (to reduce false positives). Optimizing with respect to run-time performance overheads.
  - Forming a database of side channel attacks to evaluate against; ported Spectre to RISC-V.

PROJECTS

- **FPGA Implementation of an 8-bit Microprocessor & Audio Monitoring System** Fall 2016
  Mentored by Prof. S. Qureshi, Electrical Engineering, IIT Kanpur [Code] [Report] [Slides]
  - Implemented an 8-bit microprocessor on FPGA (Xilinx Virtex-II Pro using Verilog).
  - Developed a sound monitoring system using the on-board ADC.

- **Machine Learning Projects** Machine Learning [Reports], Fall 2017
  - Projects on PCA applied on MNIST dataset, ICA for sound source separation, learning human movement with gaussian processes, implementing pacman via reinforcement learning and CNN applied on MNIST.

- **Cryptography, Software and System Security** HW/SW Security labs [Reports], Fall 2017
  - Projects on RSA & AES implementation (with 128-bit arithmetic) as an accelerator on RISC-V ISA sim, software security SEED labs, differential power analysis to obtain AES key, side channel attack on mysql queries and web server access control using SELinux.

- **Instrumenting Benchmarks & Pipelining MIPS** Computer Architecture labs, Spring 2017
  - Worked with the instrumentation tool PIN to analyze different instructions in SPEC 2006.

– Subsequently implemented direction predictors for conditional branches and target predictors for indirect calls. Finally, pipelined the MIPS simulator.

- **Software and Web Security** MIT-6.858 based labs, Spring 2017
  – Found vulnerabilities in web application server code like buffer overflows; subsequently wrote stack smashing and return-to-libc exploits and fixed the bugs.
  – Mounted cross-site scripting, cross-site request forgery and side channel attacks on zoobar; subsequently fixed these browser vulnerabilities and implemented privilege separation.

- **Image Inpainting: Exemplar-based Object Removal from Images** Fall 2016
  Class Project under Prof. Tanaya Guha, Electrical Engineering, IIT Kanpur [Report] [Slides]
  – Implemented Criminisi et al's algorithm and proposed a novel adaptive regularizer and an improved criterion for patch selection on top of it.
  – Achieved better results than the SOTA, adjudged as the **Best Project** for the course and **accepted to SIGNAL 2017**.

- **Extension of NachOS** Operating Systems labs, Fall 2016
  – Implemented system calls (fork, join, exec, yield, sleep, exit), scheduling (FIFO, SJF, Round Robin, Unix) and page replacement (FIFO, LRU, LRU-clock) algorithms on NachOS.

- **Computer Vision: 3D Display and User Interface** Winter 2014
  Mentored by Prof. K.S. Venkatesh, Electrical Engineering, IIT Kanpur [Slides]
  – Built a desktop application for e-commerce websites to exhibit a 3D view of their products.
  – The application provided a real-time 3D experience by displaying the perspective view to the user.
  – Selected among the top 6 projects at the **Ericsson Innovation Awards** and awarded INR 25000.
  – Featured by Mint, Silicon India, Storypick, Networked India and OnlineShop4Me.

- **An Improved CMOS Design for a Full Adder Circuit** Fall 2016
  Class Project under Prof. S. Qureshi, Electrical Engineering, IIT Kanpur [Report] [Slides]
  – Proposed an improved full adder design employing CMOS logic and implemented it on Mentor Graphics. The circuit functioned with lesser number of transistors and lower power consumption.

PRESENTATIONS

- ***7th RISC-V Workshop (Milpitas, CA) Nov'17*** – Poster on *Detecting Advanced Malware as Instruction and Microarchitectural Anomalies.*
- ***C-FAR Research Review (University of Michigan) Aug'17*** – Poster on *Hardware-based Malware Detection on x86 Systems.*
- ***3rd Annual SARC Technology Forum (Samsung Austin Research Center) Oct'17*** – Poster on *Hardware-based Malware Detection on x86 Systems.*

INTERNSHIPS

- ***New York University*** – **Design of a 10 GHz Class-A Power Amplifier using a Gallium Nitride Radio-Frequency Device Model** Summer 2016
  Mentored by Prof. Shaloo Rakheja, Dept. of ECE, New York University [Slides]
  – Used the MIT Virtual-Source GaN RF model to design single-stage 2.14 GHz and 2-stage 10 GHz (SHF Microwave Spectrum) Class-A Power Amplifiers.
  – Studied the performance impact of technological parameters and further optimized accordingly.

- ***New York University*** – **An improved Virtual-source based transport model for quasi-ballistic transistors, MIT Virtual Source Model (MVS-2.0)** Summer 2015
  Mentored by Prof. Shaloo Rakheja, Dept. of ECE, New York University
  – Implemented a revised model of the MIT Virtual Source Model in Verilog-A which took into account the dependence of carrier injection velocity on concentration, the VS charge on the non-equilibrium channel transport conditions and non-linearity of access resistances (now deployed on nanohub-U).

AWARDS AND ACHIEVEMENTS

- **Academic Excellence Award** by IIT Kanpur for outstanding academic performance.
- Travel grant to **Aalborg University Copenhagen** by the Danish Embassy for the Workshop in Innovation and Entrepreneurship (WOFIE) 2016 [Slides].
- **Summer Research Fellow 2016** by the Indian Academy of Sciences.
- **Ericsson Innovation Award-2015** by Ericsson, conferred to top 6 projects in India.
- **All India Rank (AIR) 1** in the Indian Railway Engineering Entrance Exam.
- **Indra Dhanush Scholarship** for excellence in academics and strong leadership skills.

- **All India Rank 520 (top 0.04 percentile)** in **IIT-JEE 2013** among 1.4 million candidates.
- **Intl. Rank 24** in the **International Mathematics Olympiad**, **128** in the **National Science Olympiad** and **201** in the **National Cyber Olympiad**, conducted by Science Olympiad Foundation.
- **Special Mention** in the 24hr Google Developer's Fest 2013 for making a shopping website, BookMyTee.

RELEVANT COURSES

- **Computer Systems**: Computer Organization, Computer Architecture, Operating Systems, Computer Systems Security, Security at HW/SW Interface, Performance Evaluation & Benchmarking*, Microarchitecture*, Programming for Performance*
- **Mathematics and Algorithms**: Machine Learning, Data Structures and Algorithms, Probability, Calculus, Linear Algebra, Information Theory, Fundamentals of Computing
- **Others**: Software Architectures*

* - ongoing courses

TECHNICAL SKILL SET

- **Programming Languages**: C, C++, Java, Python, Verilog, x86 Assembly
- **Softwares and Other Tools**: Xilinx ISE, Keysight ADS, Cadence, ModelSim, Mentor Graphics, GDB, MATLAB, LaTeX, Tensorflow, Git, PAPI, perf, PINTool
- **Development Platforms**: dsPIC, Xilinx Spartan and Virtex FPGAs

TEACHING/MENTORING EXPERIENCE

- **Project Mentor**: Mentored a junior undergraduate during Summer 2017 at NYU in the area of semiconductor device physics and RF circuit design.
- **Academic Mentor, Introduction to Electrodynamics**: Took remedial classes for the course, Introduction to Electrodynamics, and individually mentored academically deficient students.
- **Student Guide, Counselling Service**: Organized the Orientation Programme for the freshmen batch of 800 and specifically guided six students emotionally and academically.