Archit Agarwal

+1-858-518-4733 | architagarwal256@gmail.com | linkedin.com/in/archit-agarwal-0/ | Google Scholar

Education

University of California, San Diego — San Diego, California
PhD in Computer Science and Engineering under Dr. Dean Tullsen — *Sep 2023 - Present*

- Grade Point Average (GPA): **3.95/4.0**
- Recipient of **Jacob School of Engineering Fellowship** for top PhD applicants

Birla Institute of Technology and Science, Pilani — Goa, India
Bachelor of Engineering in Electronics and Communication — *Aug 2017 – May 2021*

- Cumulative Grade Points Average (CGPA): **9.65/10**
- Recipient of **Full Merit Scholarship** in all 8 semesters (Top 1% of batch by GPA)

Publications

- **ASPLOS '24**: H. Yavarzadeh, **A. Agarwal**, M. Christman, C. Garman, D. Genkin, A. Kwong, D. Moghimi, D. Stefan, M. Taram, D. Tullsen, "Pathfinder: High-Resolution Control-Flow Attacks Exploiting the Conditional Branch Predictor", In Proceedings of the 29th ACM International Conference on Architectural Support for Programming Languages and Operating Systems, San Diego, CA, USA, 2024
- **DAC '24**: A. Hajiabadi, **A. Agarwal**, A. Diavastos, T.Carlson, "Levioso: Efficient Compiler-Informed Secure Speculation", 2024 61st ACM/IEEE Design Automation Conference, San Francisco, CA, USA, 2024
- **IJPEDS '23**: A. Nair, G. Patil, **A. Agarwal**, A. Pai, B. Raveendran & S. Punnekkat "CAMP: A Hierarchical Cache Architecture for Multi-core Mixed Criticality Processors", International Journal of Parallel, Emergent and Distributed Systems, 2023

Experience

University of California, San Diego — San Diego, USA
PhD Student under Dr. Dean Tullsen — *Sep 2023 - Present*

- Developed a new speculative attack that utilizes the Intel Conditional Branch Predictor to leak the complete dynamic control flow of a victim function and further poison its execution to leak secret values *(ASPLOS '24)*
- Currently proposing and designing an efficient and secure architecture-agnostic branch predictor unit for use in modern server-grade processors

National University of Singapore — Singapore
Research Engineer under Dr. Trevor Carlson — *June 2021 - June 2023*

- Proposed a hardware-software co-design framework for efficient and configurable mitigation strategies against speculative attacks, improving the performance and efficacy of current and future countermeasures *(DAC '24)*
- Built the proposed framework on top of the Gem5 Hardware Simulator for performance and security analysis
- Integrated the proposed framework with existing state-of-the-art mitigations to allow for a comprehensive yet configurable protection scope including the proposed new attack as well as future attacks
- Reduced the average performance overhead of state-of-the-art mitigation solutions by 2.7x-3.9x (SPEC'06 Suite)

Cisco Systems — Bengaluru, India
Hardware Engineering Intern — *Aug 2020 – Dec 2020*

- Developed a Real Time Traffic Generator for TLS 1.2 and 1.3 encryption protocols using Wireshark and Python
- Developed a Custom Packet Generator for multiple internet protocols using Scapy and TCPDump
- Created the verification environment for an AES-XTS Encryption Engine using SVerilog and OpenSSL

Birla Institute of Technology and Science, Pilani — Goa, India
Research Assistant under Dr. Pravin Mane and Dr. Biju Raveendran — *Jan 2019 – May 2021*

- Project 1: Proposed a 3-Tier Criticality Aware Cache Architecture to increase the probability of high criticality tasks meeting their worst case execution time in mixed-criticality multi-core real-time automotive systems. The proposal utilized a mix of static and weighted dynamic cache partitioning techniques *(IJPEDS '23)*
- Project 2: Proposed an optimized recursion multiplier design bringing down layers of addition in design by 33 percent. Achieved a delay improvement of over 30 percent compared to exact multiplication techniques while retaining a relative error of under 0.01 percent and a state-of-the-art average hamming distance

Technical Skills

Languages: C, C++, Python, Assembly, MATLAB, Verilog
Softwares/Tools: Gem5 Simulator, Intel SGX, Wireshark, Cadence Genus Synthesis Solution, Xilinx ISE, Git