Title:

Learning to Trust DRAM in the Era of Worsening Rowhammer Vulnerability

Abstract:

In recent years, DRAM Rowhammer attacks have emerged as a potent threat to system integrity. Due to this vulnerability, rapid activations of a DRAM row can induce bit-flips in neighboring rows due to charge leakage. Using such attacks, an adversary can tamper critical data and even escalate to kernel level privilege. Moreover, the vulnerability of DRAM to such attacks is worsening with technology scaling: DDR3, DDR4, and DDR5 memories have been shown vulnerable, and the number of DRAM accesses needed to induce such bit-flips has reduced, by >30x in the last decade, to just around 5000 activations currently.

This talk will cover our recent works to mitigate this Rowhammer vulnerability. (1) We will first cover memory-controller based defenses **(RRS - ASPLOS'22** and **SRS - HPCA'23 Best Paper Award**), which propose new mitigation mechanisms that randomize the mapping of DRAM addresses to physical rows, to break the spatial correlation between hammered aggressor rows and victim rows. These aggressor-focused mitigations are resilient to emerging attacks such as Half-Double, which break existing victim mitigations. (2) We will next cover integrity-protection for critical data-structures like Page-Tables (**PTGuard – DSN'23**), which prevent exploitation of systems, even if a Rowhammer attack is successful in defeating existing mitigations. (3) Finally, we will discuss how this issue can be mitigated fundamentally with in-DRAM mitigations (**PrIDE – ISCA'24**), by designing a probabilistic in-DRAM tracker whose security is independent of attacker access patterns. These solutions protect the DRAM at low overhead even as the Rowhammer threshold (accesses required to induce bit-flips) drops by an order of magnitude to sub-500 in the next few generations, allowing us to regain trust in DRAM in the era of worsening Rowhammer vulnerability.

Bio:

Gururaj Saileshwar is an Assistant Professor at the University of Toronto, Department of Computer Science. His research is at the intersection of computer architecture and systems security, with interests in micro-architectural side-channel attacks, DRAM Rowhammer attacks, and Confidential Computing. His research has been awarded an IEEE HPCA 2023 Best Paper Award, an IEEE Micro Top Picks 2019 Honorable Mention, and his 2022 PhD dissertation has been recognized with an IEEE HOST Best PhD Dissertation

Award, an IEEE TCCA / ACM SIGARCH Best Dissertation Award (Honorable Mention), and ACM SIGMICRO Dissertation Award (Honorable Mention).