psd

The Story of RowHammer

WHEN

October 6th, 2022

1:30pm - 2:30pm

WHERE

John Crerar Library - Room 390

Onur Mutlu, Professor, ETH Zurich

We will examine the RowHammer problem in DRAM, which is the first example of how a circuit-level failure mechanism in Dynamic Random Access Memory (DRAM) can cause a practical and widespread system security vulnerability. RowHammer is the phenomenon that repeatedly accessing a row in a modern DRAM chip predictably causes errors in physically-adjacent rows. It is caused by a hardware failure mechanism called read disturb errors, a manifestation of circuit-level cell-to-cell interference in a scaled memory technology. Building on our initial fundamental work that appeared at ISCA 2014, Google Project Zero demonstrated that this hardware phenomenon can be exploited by user-level programs to gain kernel privileges. Many other works demonstrated other attacks exploiting RowHammer, including remote takeover of a server vulnerable to RowHammer and takeover of a mobile device by a malicious user-level application. Unfortunately, the RowHammer problem still plagues cutting-edge DRAM chips, DDR4 and beyond. Based on our recent characterization studies of more than 1500 DRAM chips from six technology generations that appeared at ISCA 2020 and MICRO 2021, we will show that RowHammer at the circuit level is getting much worse, newer DRAM chips are much more vulnerable to RowHammer than older ones, and existing mitigation techniques do not work well. We will also show that existing proprietary mitigation techniques employed in DDR4 DRAM chips, which are advertised to be Rowhammer-free, can be bypassed via many-sided hammering (also known as TRRespass & Uncovering TRR). Throughout the talk, we will analyze the properties of the RowHammer problem, examine circuit/device scaling characteristics, and discuss solution ideas. We will also discuss what other problems may be lurking in DRAM and other types of memory, e.g., NAND flash, Phase Change Memory and other emerging memory technologies, which can potentially threaten the foundations of reliable and secure systems, as the memory technologies scale to higher densities. We will conclude by describing and advocating a principled approach to memory reliability and security research that can enable us to better anticipate and prevent such vulnerabilities.

computerscience.uchicago.edu

THE UNIVERSITY OF CHICAGO | DEPARTMENT OF COMPUTER SCIENCE