IPM

"سخنرانی های علمی"

پژوهشگاه دانشهای بنیادی

پژوهشکده علوم
کامپیوتر

TRRespass: Exploiting the Many Sides of Target Row Refresh

دکتر کاوه رضوی

استادیار دانشگاه ETH Zurich

Abstract

After a plethora of high-profile RowHammer attacks, CPU and DRAM vendors scrambled to deliver what was meant to be the definitive hardware solution against the RowHammer problem: Target Row Refresh (TRR). A common belief among practitioners is that, for the latest generation of DDR4 systems that are protected by TRR, RowHammer is no longer an issue in practice. However, in reality, very little is known about TRR. How does TRR exactly prevent RowHammer? Which parts of a system are responsible for operating the TRR mechanism? Does TRR completely solve the RowHammer problem or does it have weaknesses?

In this paper, we demystify the inner workings of TRR and debunk its security guarantees. We show that what is advertised as a single mitigation mechanism is actually a series of different solutions coalesced under the umbrella term Target Row Refresh. We inspect and disclose, via a deep analysis, different existing TRR solutions and demonstrate that modern implementations operate entirely inside DRAM chips. Despite the difficulties of analyzing in-DRAM mitigations, we describe novel techniques for gaining insights into the operation of these mitigation mechanisms. These insights allow us to build TRRespass, a scalable black-box RowHammer fuzzer that we evaluate on 42 recent DDR4 modules.

TRRespass shows that even the latest generation DDR4 chips with in-DRAM TRR, immune to all known RowHammer attacks, are often still vulnerable to new TRR-aware variants of RowHammer that we develop. In particular, TRRespass finds that, on present-day DDR4 modules, RowHammer is still possible when many aggressor rows are used (as many as 19 in some cases), with a method we generally refer to as Many-sided RowHammer. Overall, our analysis shows that 13 out of the 42 modules from all three major DRAM vendors (i.e., Samsung, Micron, and Hynix) are vulnerable to our TRR-aware RowHammer access patterns, and thus one can still mount existing state-of-the-art system-level RowHammer attacks. In addition to DDR4, we also experiment with LPDDR4(X) chips and show that they are susceptible to RowHammer bit flips too. Our results provide concrete evidence that the pursuit of better RowHammer mitigations must continue.

Bio: Kaveh Razavi is an assistant professor in the Department of Information Technology and Electrical Engineering at ETH Zurich where he leads the COMSEC group. His research interests are in the area of systems security and more broadly, computer systems. He regularly publishes at top systems and security venues (e.g., S&P, USENIX Security, SOSP/OSDI, etc.) and his research has won a prestigious VENI personal grant as well as industry and academic awards including multiple Pwnies, best practical paper award at S&P 2019 and best paper award at S&P 2020 among others.

زمان : دوشنبه ۹۹/۳/۱۹ – ساعت ۱٤:۰۰

*****شرکت برای عموم علاقه مندان آزاد است*****