Contribution ID: **84** Type: **not specified**

ASI: Efficiently Mitigating Speculative Execution Attacks with Address Space Isolation

Thursday, 27 August 2020 08:10 (20 minutes)

Speculative execution attacks, such as L1TF, MDS, LVI pose significant security risk to hypervisors and VMs. A complete mitigation for these attacks requires very frequent flushing of buffers (e.g., L1D cache) and halting of sibling cores. The performance cost of such mitigations is unacceptable in realistic scenarios. We are developing a high-performance security-enhancing mechanism to defeat speculative attack which we dub Address Space Isolation (ASI). In essence, ASI is an alternative way to manage virtual memory for hypervisors, providing very strong security guarantees at a minimal performance cost. In the talk, we will discuss the motivation for this technique as well as initial results we have.

I agree to abide by the anti-harassment policy

I agree

Primary author: Dr WEISSE, Ofir (Google)

Presenter: Dr WEISSE, Ofir (Google)

Session Classification: System Boot and Security MC

Track Classification: System Boot and Security MC