Contribution ID: **274** Type: **not specified**

Mitigating speculative execution attacks with ASI - follow up

Tuesday, September 13, 2022 10:30 AM (30 minutes)

In this talk we will argue the case for adopting ASI in upstream Linux.

Speculative execution attacks, such as L1TF, MDS, LVI, (and many others) pose significant security risks to hypervisors and VMs, from neighboring malicious VMs. The sheer number of proposed patches/fixes is quite high, each with its own non-trivial impact on performance. A complete mitigation for these attacks requires very frequent flushing of several buffers (L1D cache, load/store buffers, branch predictors, etc. etc.) and halting of sibling cores. The performance cost of deploying these mitigations is unacceptable in realistic scenarios.

Two years ago, we presented Address Space Isolation (ASI) - a high-performance security-enhancing mechanism to defeat these speculative attacks. We published a working proof of concept in https://lkml.org/lkml/2022/2/23/14. ASI, in essence, 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 what new vulnerabilities have been discovered since our previous presentation, what are the existing approaches, and their estimated costs. We will then present our performance estimation of ASI, and argue that ASI can mitigate most of the speculative attacks as is, or by a small modification to ASI, at an acceptable cost.

I agree to abide by the anti-harassment policy

Yes

Primary authors: SHAHID, Junaid (Google); WEISSE, Ofir (Google)

Presenters: SHAHID, Junaid (Google); WEISSE, Ofir (Google)

Session Classification: linux/arch MC

Track Classification: LPC Microconference: linux/arch MC