Contribution ID: **27** Type: **not specified**

Kernel Address Space Isolation

Wednesday, August 26, 2020 7:00 AM (45 minutes)

First investigations about Kernel Address Space Isolation (ASI) were presented at LPC last year as a way to mitigate some cpu hyper-threading data leaks possible with speculative execution attacks (like L1 Terminal Fault (L1TF) and Microarchitectural Data Sampling (MDS)). In particular, Kernel Address Space Isolation aims to provide a separate kernel address space for KVM when running virtual machines, in order to protect against a malicious guest VM attacking the host kernel using speculative execution attacks.

https://www.linuxplumbersconf.org/event/4/contributions/277/

At that time, a first proposal for implementing KVM Address Space Isolation was available. Since then, new proposals have been submitted. The implementation have become much more robust and it now provides a more generic framework which can be used to implement KVM ASI but also Kernel Page Table Isolation (KPTI).

Currently, RFC version 4 of Kernel Address Space Isolation is available. The proposal is divided into three parts:

- Part I: ASI Infrastructure and PTI
 https://lore.kernel.org/lkml/20200504144939.11318-1-alexandre.chartre@oracle.com/
- Part II: Decorated Page-Table
 https://lore.kernel.org/lkml/20200504145810.11882-1-alexandre.chartre@oracle.com/
- Part III: ASI Test Driver and CLI
 https://lore.kernel.org/lkml/20200504150235.12171-1-alexandre.chartre@oracle.com/

This presentation will show progress and evolution of the Kernel Address Space Isolation project, detail the kernel ASI framework and how it is used to implement KPTI and KVM ASI. It also looks forward to discuss possible way to integrate the project upstream, concerns about making changes in some of the nastiest corners of the x86, and kernel page table management improvement, in particular page table creation and population.

I agree to abide by the anti-harassment policy

I agree

Primary author: CHARTRE, Alexandre (Oracle)

Presenter: CHARTRE, Alexandre (Oracle)

Session Classification: LPC Refereed Track

Track Classification: LPC Refereed Track (Closed)