Contribution ID: **143** Type: **not specified**

Attack vector controls for speculation mitigations

Friday, 20 September 2024 15:20 (20 minutes)

There are currently more than a dozen command line options related to x86 CPU speculation bugs, and it takes a security expert to understand them all and when they can be safely disabled. This talk will discuss a recent RFC that proposes simpler “attack vector”based controls which would allow admins to select a set of mitigation options based on how the system is being used. For instance, if the system only runs trusted VMs, then guest-to-host mitigations should be disabled. The goal is to make it easier to select appropriate and consistent mitigation options, and potentially recover lost performance.

Primary author: KAPLAN, David (AMD)

Presenter: KAPLAN, David (AMD)

Session Classification: x86 MC

Track Classification: x86 Microconference