Contribution ID: **113** Type: **not specified**

Testing Intel TDX functionality with new set of self tests

Tuesday, September 13, 2022 12:50 PM (20 minutes)

The new TDX architecture makes changes to the hardware and the host and guest software stacks.
All of these components are being developed simultaneously and are constantly changing. As the host kernel changes, we need a system to test its functionality which is independent from the guest enlightenment changes and doesn't rely on a fully functional system which doesn't exist yet.

We propose a new extension to the selftest framework for running simple code as a TD guest to test various functionality of the TDX hardware and host kernel support.

This framework has been in use by Google for several months and allows us to test memory access interactions between host and guest and allow testing of the Guest-Hypervisor Communication Interface (GHCI). It allowed us to uncover issues in the early development stages of TDX and surface requirements which are not always clear from the SPEC.

The framework was originally proposed in "[RFC PATCH 0/4] TDX KVM selftests"and we intend to send out an updated patch series based on Intel's latest RFC V6 patch to TDX and include additional tests.

I agree to abide by the anti-harassment policy

Yes

Primary author: SHAHAR, Sagi (Google)

Co-authors: Mr AFRANJI, Ryan (Google); AKTAS, Erdem (Google)

Presenter: SHAHAR, Sagi (Google)

Session Classification: Confidential Computing MC

Track Classification: LPC Microconference: Confidential Computing MC