Linux Plumbers Conference 2022

Contribution ID: **93** Type: **not specified**

Upstream & Guest Distro support for Confidential Compute

Tuesday 13 September 2022 10:00 (20 minutes)

Confidential compute is developing fast. However, at Google we are facing challenges regarding the maintenance and support of guest distros. In particular, we're finding it difficult to maintain an efficient way of communicating with different distros and hard to test, validate, and merge fixes into guest distros.

Backporting fixes
Customers do not always run the guest with the latest kernels. In fact, the majority of our distros are still based on 5.4/5.10 kernels. Thus, bug fixes on the guest side usually require backporting the patches into the stable branches. Unfortunately, our backporting attempts got rejected several times because confidential compute is considered a new feature. Since the patches were considered to be new features instead of bug fixes, they were unable to be merged into stable branches. Ultimately, by working with each of our supported distros individually, we got our patches backported. This approach not only created unnecessary work on both our end and each distros'end but also significantly delayed the time a patch got backported and merged in distros.

With the upcoming guest patches for Intel TDX and AMD SEV-SNP, we hope we can find a better way of maintaining guest-related confidential compute patch backporting, whether it is for supporting new or existing confidential compute features.

Guest Distro testing and verification
With upcoming launch for AMD SEV-SNP and Intel TDX, we are starting to support multiple types of confidential compute. For each offering, we will support several different guest distros. It is becoming harder to keep track on what confidential compute technology each guest distro version supports.

In addition to tracking supportability, we are also facing challenges on testing and verification of newly published images. It would be great if we can work on a common validation test suite for confidential compute to make sure new guest distros are indeed qualified before releasing them.

I agree to abide by the anti-harassment policy

Yes

Primary author: GAO, Jianxiong

Presenter: GAO, Jianxiong

Session Classification: Confidential Computing MC

Track Classification: LPC Microconference: Confidential Computing MC