Contribution ID: **73** Type: **not specified**

Confidential Computing with Secure Execution (IBM Z)

Tuesday 21 September 2021 09:20 (20 minutes)

As confidential computing gains traction, several technologies that are based on a secure hypervisor are emerging.
Besides SEV (AMD), PEF (Power), and TDX (Intel), IBM Z's *Secure Execution* enables running a guest that even an administrator cannot look into or tamper with.
At the same time, it becomes desirable to run an OCI container workload in a secure context.

The *Kata Containers* runtime is based on VMs and thus, Secure Execution can be leveraged.
Initially, Kata had the goal of protecting the host from malicious guests, but the vice versa approach is now being discussed and worked on, with some patches landed, but other patches required in adjacent projects like containerd.

I work in IBM's Linux on Z department, enabling Kata on the IBM Z and LinuxONE platform, including Secure Execution.
I propose a talk where first, a general overview of Secure Execution is given: what the threat and security models are and how a user would go about running a protected workload.
This helps the audience learn about a confidential computing solution that is distinct from discussed x86 approaches, in that images to be launched in Secure Execution are encrypted and can only be decrypted in a secure context, as opposed to x86 firmware attestation approaches.
It is then described how Secure Execution maps to the challenges in confidential computing including Kata and Kubernetes, concerning the need to control and provide certain resources from the host.

Note: Samuel Ortiz of Apple has also proposed to speak about general confidential computing challenges in Kata in this microconference.
Even though I will introduce Kata and confidential computing so that the talk makes sense on its own, it is probably better if I speak after him.

I agree to abide by the anti-harassment policy

I agree

Primary author: NAUCKE, Jakob (IBM Corp.)

Presenter: NAUCKE, Jakob (IBM Corp.)

Session Classification: Confidential Computing MC

Track Classification: Confidential Computing MC