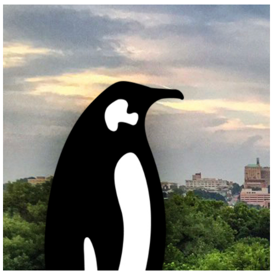

Contribution ID: **191** Type: **not specified**

Shrinking The Elephant - A Confidential Computing Attestation Sequel

Tuesday 14 November 2023 15:00 (20 minutes)

At the 2022 confidential computing LPC microconference, we talked about the elephant in the confidential computing room: guest attestation and verification. We showed how opaque, fragmented and closed this essential piece of the confidential computing puzzle is, adding one more hurdle to this technology adoption.

During the past year, the Confidential Containers project worked on putting the elephant on a diet, and here we will first talk about how we are building the first-ever fully open source attestation service. We'd also like to use this microconference as an opportunity to introduce the new and unresolved attestation challenges that we uncovered during that journey, to a wider confidential computing audience.

We will start by describing the Attestation Service and Key Broker Service (KBS) projects that form the backbone of the open source and vendor agnostic attestation service framework that we built during the last months. We'll talk about the public facing interface of that framework, the KBS API and protocol, and will show how that simple HTTPS based interface supports different attestation models without being bound to vendor specific formats or data. We'll also mention how the verification backend of the Attestation Service already supports all major CoCo vendor attestation format evidences by abstracting attestation verification operations through a simple plugin interface.

The next part of the presentation will go through the known and remaining issues we'll have to address in the short term: Converging the attestation results format and plugging the attestation service with the rest of the software supply chain for consuming trustable attestation reference values and policies, for example. As with any technological exploration, one challenge only leads to the next one and the last section of this presentation will focus on introducing the new, longer term problems that we are facing. Integrating the asynchronous, SoC vendor-independent, trusted device attestation flow with the guest one might be the biggest one.

Primary author: ORTIZ, Samuel

Presenter: ORTIZ, Samuel

Session Classification: Confidential Computing MC

Track Classification: LPC Microconference: Confidential Computing MC