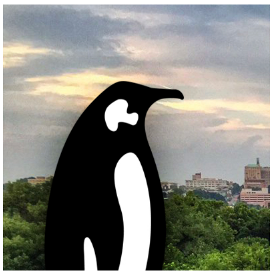
Linux Plumbers Conference 2023



Contribution ID: **185** Type: **not specified**

In Containers We Trust? Building Trust in Containerized Environments

Monday, 13 November 2023 15:30 (30 minutes)

Building trust in containerized environments requires the measurement and attestation of individual containers. The Linux Integrity Measurement Architecture ("IMA") collects and stores file integrity measurements in a non-repudiable log. These measurements are used during remote attestation to verify system integrity and extend trust from the kernel to measured files. File measurements cannot, however, be used to attest individual container integrity because they are not differentiated by namespace. We present a mechanism to measure container integrity, without requiring changes to the host operating system. Using loadable kernel extensions and existing IMA infrastructure, we measure images at container creation and namespace container file integrity measurements throughout runtime.

Primary author: BLANCHARD, Avery (Duke University)

Co-authors: ALMASI, George (Ibm); FRANKE, Hubertus (IBM Research); BOTTOMLEY, James (IBM)

Presenter: BLANCHARD, Avery (Duke University)

Session Classification: Containers and checkpoint/restore MC

Track Classification: LPC Microconference: Containers and checkpoint/restore MC