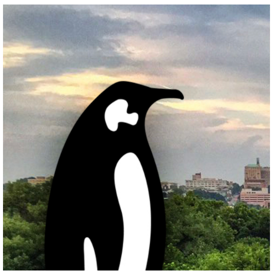

Contribution ID: **184**

Type: **not specified**

Extending Non-Repudiable Logs with eBPF

Monday, 13 November 2023 16:30 (30 minutes)

The Linux kernel uses non-repudiable logging to attest to system integrity. Non-repudiation ensures that the validity of the log cannot be disputed, even in the presence of an untrusted actor. We present an extensible interface for user-defined programs to leverage TPM-based non-repudiable logging of any kernel data accessible to eBPF programs. With the large variety eBPF hook locations, our approach allows system integrity to be verified with greater granularity than previously possible. We have used this technique to measure and store container image digests when they are run to verify and attest container integrity. The variety of use cases present an exciting future for eBPF in security and trust.

Primary author: BLANCHARD, Avery (Duke University)

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

Presenters: BLANCHARD, Avery (Duke University); ALMASI, George (IBM)

Session Classification: eBPF & Networking

Track Classification: eBPF & Networking Track