Contribution ID: **423** Type: **not specified**

Ultraviolet: A Code Integrity Model for Minimal Container Hosts

We're seeing increased adoption of boot security technologies in Linux and utilization of platform root-of-rust mechanisms. There's also been significant progress in open community efforts around image-based systems, where typically the root partition and/or the usr partition are implemented as signed DM-Verity volumes.

We'd like to demonstrate how to extend the integrity chain from boot to the OS in the general case, using Integrity Police Enforcement (IPE), DM-Verity, mandatory access control, and a mostly immutable filesystem layout. This is a policy-driven approach to code integrity, drawing upon our experiences with special-purpose hyperscale systems, but aimed at more generalized scenarios and broader community adoption.

We'll utilize ParticleOS (systemd's "customizable immutable distribution") as the base for the Ultraviolet model, extending it with emerging features (like script execution control) to provide an end-to-end measured and attestable code integrity system. We'll discuss technical challenges in adapting existing workloads to image-based systems and propose some ideas for solving them–ideally without overlays and other hacks.

The intention is to share both an architectural model and a reference implementation, firstly so others can benefit from what we've learned, and secondly to foster discussions about how we can work together on raising the security bar in the broader ecosystem.

References:

1. Ultraviolet Linux: https://github.com/uv-linux
2. Integrity Policy Enforcement (IPE): https://microsoft.github.io/ipe/
3. ParticleOS: https://github.com/systemd/particleos

Primary author: MORRIS, James

Presenter: MORRIS, James

Session Classification: System Boot and Security MC

Track Classification: System Boot and Security MC