Contribution ID: **100** Type: **not specified**

BPF LSM (Updates + Progress)

Tuesday, 25 August 2020 09:45 (45 minutes)

The BPF LSM or Kernel Runtime Security Instrumentation (KRSI) aims to provide an extensible LSM by allowing privileged users to attach eBPF programs to security hooks to dynamically implement MAC and Audit Policies.

KRSI was introduced in LSS-US 2019 and has since then had multiple interesting updates and triggered some meaningful discussions. The talk provides an update on:

- Progress in the mainline kernel, the ongoing discussions, and a recap of the interesting discussions that were resolved.
- New infrastructure merged into BPF to support the BPF LSM use-case.
- Some optimisations that can improve the performance characteristics of the currently existing LSM framework which would not only benefit KRSI but also all other LSMs.

The talk showcases how the design has evolved over time and what trade-offs were considered and what's upcoming after the initial patches are merged.

I agree to abide by the anti-harassment policy

I agree

Primary author: SINGH, KP (Google)

Presenter: SINGH, KP (Google)

Session Classification: Networking and BPF Summit

Track Classification: Networking & BPF Summit