Contribution ID: **151** Type: **not specified**

Kernel Runtime Security Instrumentation (KRSI)

Wednesday, September 11, 2019 6:00 PM (20 minutes)

Existing Linux Security Modules can only be extended by modifying and rebuilding the kernel, making it difficult to react to new threats. The Kernel Runtime Security Instrumentation project (KRSI) (prototype code) aims to help this by providing an LSM that allows eBPF programs to be added to security hooks.

The talk discusses the need for such an LSM (with representative use cases) and compares it to some existing alternatives, such as Landlock, a separate custom LSM, kprobes+eBPF etc. The second half of the talk outlines the proposed design and interfaces, and includes a live demo.

KRSI is an LSM that:

- Allows the attachment of eBPF programs to security hooks.
- Provides a good ecosystem of safe eBPF helper functions specifically written with security and auditing features in mind.

This enables the development of a new class of userspace security products that:

- Reduce the overhead of building and updating the kernel/LSM when a new security vulnerability is discovered.
- Allows the system owners to choose the format in which the data is audit logged. Provide flexibility w.r.t granularity of auditing needed and add new auditing without needing to re-build or update the LSM/Kernel (in contrast to the existing audit framework)

The intended audience for this talk would be:

- Security-focused kernel engineers
- Engineers building user-space security products on Linux.
- Security Engineers and Admins who care about the time required to deploy security software to detect and prevent a new class of malicious activity.

I agree to abide by the anti-harassment policy

Yes

Primary author: Mr SINGH, KP

Presenter: Mr SINGH, KP

Session Classification: BPF MC