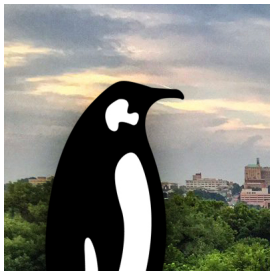

Contribution ID: **193** Type: **not specified**

Sysarmor: Meta's eBPF Security Detection and Enforcement Tool

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

Sysarmor is a security daemon used to detect possible threats, and enforce security rules at Meta. Sysarmor is deployed to higher threat environments, such as: collocated hosts, Meta Network Appliances, development servers, Meta cloud gaming, and public cloud (AWS/GCP). Sysarmor has over 40 BPF based detections, including areas such as: networking, privilege escalation, hardware attacks, rootkits, unknown executables, container creation, and container escape.

The main differentiator between sysarmor and similar BPF based security tools is that sysarmor evaluates its rules inside the bpf program, instead of dispatching events to userspace logic. This allows sysarmor to use BPF-LSM to enforce these rules if desired. Sysarmor rules can make use of process information or container information, as well as hook-specific arguments to make a decision as to whether or not an action is allowed.

The talk will provide an overview Sysarmor, and some of the hooks used, then will discuss several challenging areas the Sysarmor team has worked on:

1. Efficiently and accurately gathering process information such as executable filename and using it for filtering events.
2. Gathering container information such as ids and image ids, and associating that information with kernel information such as namespace ids.
3. Using uprobes in system executables effectively, and associating information from system logs with BPF events.
4. Using BPF iterators to recreate context after a service restart.

Primary authors: WISEHART, Liam (Meta); GNANASHANMUGAM, Shankaran (Meta)

Presenters: WISEHART, Liam (Meta); GNANASHANMUGAM, Shankaran (Meta)

Session Classification: eBPF & Networking

Track Classification: eBPF & Networking Track