Contribution ID: **316** Type: **not specified**

Do we need CAP_BPF_ADMIN?

Wednesday, September 11, 2019 4:07 PM (23 minutes)

Currently, most BPF functionality requires CAP_SYS_ADMIN or CAP_NET_ADMIN. However, in many cases, CAP_SYS_ADMIN/CAP_NET_ADMIN gives the user more than enough permissions. For example, tracing users need to load BPF programs and access BPF maps, so they need CAP_SYS_ADMIN. However, they don't need to modify the system, so CAP_SYS_ADMIN adds significant risk.

To better control BPF functionality, this is time to think about CAP_BPF_ADMIN (or even multiple CAP_BPF_*s). In this BPF MC, we would like to discuss whether we need CAP_BPF_ADMIN, and what CAP_BPF_ADMIN would look like. We will present survey of major BPF use cases, and identify use cases that may benefit from a new CAP. Then, we will discuss which syscalls/commands should be gated by the new CAP. We expect constructive discussions between the BPF folks and security folks.

I agree to abide by the anti-harassment policy

Yes

I confirm that I am already registered for LPC 2019

Primary author: LIU, Song

Presenter: LIU, Song

Session Classification: BPF MC