Contribution ID: **295**

Type: **not specified**

Closing the BPF map permission loophole

Wednesday 14 September 2022 11:00 (30 minutes)

While working on github.com/cloudflare/tubular we discovered that it's possible for a program with CAP_BPF to circumvent file permissions of BPF map fds, effectively making it impossible to enforce read-only access. In our case, a process exporting metrics from maps can't be prevented from also being able to modify those maps.
I will outline how permissions, map flags like BPF_F_RDONLY and map freezing interact and explain how current semantics fall short. I'll also propose a possible solution which changes how the verifier tracks the mutability of map values.

I agree to abide by the anti-harassment policy

Yes

Primary author: BAUER, Lorenz

Presenter: BAUER, Lorenz

Session Classification: eBPF & Networking

Track Classification: eBPF & Networking Track