Contribution ID: **126** Type: **not specified**

BPF security auditing at Google

Friday, September 24, 2021 8:40 AM (40 minutes)

We'll discuss some recent and ongoing work we've been doing to audit Google's Linux systems with eBPF. We'll look at a case study of the problems we've solved for logging process lifecycles, and then look at the challenges we're facing to make these systems as reliable and maintainable as possible. The topics we'll cover include:

- A brief overview of the BPF LSM
- Why and how we ended up adding atomics to eBPF
- Why we implemented task-local BPF storage
- How we push large data blobs through the BPF ringbuffer (and how we'd like to improve it)
- Why we wish we didn't have to attach to so many fexit hooks (and what we'd like to do about it)

I agree to abide by the anti-harassment policy

I agree

Primary authors: JACKMAN, Brendan (Google); SINGH, KP (Google)

Presenters: JACKMAN, Brendan (Google); SINGH, KP (Google)

Session Classification: BPF & Networking Summit

Track Classification: Networking & BPF Summit (Closed)