Contribution ID: **141** Type: **not specified**

Towards truly portable eBPF

Friday, September 24, 2021 7:00 AM (40 minutes)

As eBPF is getting more popular and mainstream, one of the challenges of making it accessible to more users is how to distribute eBPF powered applications. Unlike simpler applications which involves shipping a binary or a container image, with eBPF we usually need to compile the program for the target kernel. This is a hurdle in adoption by both users and vendors. The CO-RE (Compile Once - Run Everywhere) initiative improved this by introducing a way to ship a compiled artifact, which will work on any supporting distribution. But what is a supporting distribution and what about unsupported distributions? How can we make eBPF CO-RE widely usable in the real world of enterprise users? In this talk we will answer these questions by introducing CO-RE and BTF mechanics, and how to leverage them in a concrete scenario in our project Tracee.

I agree to abide by the anti-harassment policy

I agree

Primary authors: SHAKURY, Itay (Aqua Security); TINOCO, Rafael David (Aqua Security)

Presenters: SHAKURY, Itay (Aqua Security); TINOCO, Rafael David (Aqua Security)

Session Classification: BPF & Networking Summit

Track Classification: Networking & BPF Summit (Closed)