Contribution ID: **134** Type: **not specified**

Pixie's eBPF Protocol Tracer

Thursday 23 September 2021 10:20 (40 minutes)

We present Pixie's protocol tracer, which uses eBPF to provide instant observability into application messaging without requiring code instrumentation. Pixie's protocol tracer uses eBPF kprobes on networking-related system calls to capture communication data, which it then parses into protocol messages. The messages are inserted into structured data tables that are easily queried by application developers to help them gain insight into their application behavior.

We contrast our syscall tracing approach against other approaches (e.g. libpcap and uprobes), and discuss pros and cons. We share what worked well with our approach, and also the challenges we faced, including eBPF-related challenges of tracing syscalls that have a multitude of usage patterns.

Finally, we discuss the limitations of kprobe based tracing, in particular with respect to stateful protocols like HTTP/2 and encrypted connections like those that use TLS. We describe our complementary approach that uses eBPF uprobes on user-space libraries to capture the data in these scenarios.

We hope the technical details presented here will be of value to the eBPF community, and we are eager to hear from the eBPF community about potential improvements and suggestions for future directions.

I agree to abide by the anti-harassment policy

I agree

Primary authors: AZIZI, Omid (Pixie Labs); ZHAO, Yaxiong (Pixie Labs); CHENG, Ryan (Pixie Labs); STEVENSON, John P (Pixie Labs); ASGAR, Zain (Pixie Labs)

Presenters: AZIZI, Omid (Pixie Labs); ZHAO, Yaxiong (Pixie Labs); CHENG, Ryan (Pixie Labs); STEVENSON, John P (Pixie Labs); ASGAR, Zain (Pixie Labs)

Session Classification: BPF & Networking Summit

Track Classification: Networking & BPF Summit (Closed)