Contribution ID: **239** Type: **not specified**

BPF packet capture helpers, libbpf interfaces

Monday 9 September 2019 10:45 (45 minutes)

Packet capture is useful from a general debugging standpoint, and is useful in particular in debugging BPF programs that do packet processing. For general debugging, being able to initiate arbitrary packet capture from kprobes and tracepoints is highly valuable (e.g. what do the packets that reach kfree_skb() - representing error codepaths - look like?). Arbitrary packet capture is distinct from the traditional concept of pre-defined hooks, and gives much more flexibility in probing system behaviour. For packet-processing BPF programs, packet capture can be useful for doing things such as debugging checksum errors. The intent of this proposal is to help drive discussion around how to ease use of such features in BPF programs, namely:

- should additional BPF helper(s) be provided to format packet data suitable for libpcap interpretation?
- should libbpf provide interfaces for retrieving packet capture data?
- should interfaces be provided for pushing filters?

Note that while there has been some work in this area already, such as

https://new.blog.cloudflare.com/xdpcap/

...it seems like such efforts would be made much simpler if APIs were provided.

I agree to abide by the anti-harassment policy

Yes

I confirm that I am already registered for LPC 2019

Primary author: MAGUIRE, Alan (Oracle)

Presenter: MAGUIRE, Alan (Oracle)

Session Classification: Networking Summit Track