_Q8OIj.png _Q8OIj.bb _Q8OIj.png height

Contribution ID: **171** Type: **not specified**

In-kernel protocol aware filtering

Thursday, 15 November 2018 14:00 (20 minutes)

Deep packet inspection seems to be a largely unexplored area of BPF use cases. The 4096 instruction limit and the lack of loops make such implementations non-straightforward for many protocols. Using XDP and socket filters, at Red Sift, we implemented DNS and TLS handshake detection to provide better monitoring for our clusters. We learned that while the protocol implementation is not necessarily straightforward, the BPF VM provides a reasonably safe environment for DPI-style parsing. When coupled with our Rust userspace implementation, it can provide information and functionality that previously would have required userspace intercepting proxies or middleboxes, at a comparable performance to iptables-style packet filters. Further work is needed to explore how we can turn this into a more comprehensive, active component, mainly due to the BPF VM restrictions around 4096 instruction programs.

I agree to abide by the anti-harassment policy

Presenter: PARKANYI, Peter (Red Sift)

Session Classification: BPF MC