Contribution ID: **296** Type: **not specified**

Seamless transparent encryption with BPF and Cilium

Tuesday, 10 September 2019 17:00 (45 minutes)

Providing encryption in dynamic environments where nodes are added and removed on-the-fly and services spin-up and are then torn-down frequently, such as Kubernetes, has numerous challenges. Cilium, an open source software package for providing and transparently securing network connectivity, leverages BPF and the Linux encryption capabilities to provide L3/L7 encryption and authentication at the node and service layers. Giving users the ability to apply encryption either to entire nodes or on specified services. Once configured through a high level feature flag (–enable-encrypt-l3, –enable-encrypt-l7) the management is transparent to the user. Cilium will manage and ensure traffic is encrypted allowing for auditing of encrypted/unencrypted flows via a monitoring interface to ensure compliance.

In this talk we will show how Cilium accomplishes this in the Linux datapath and control plane. As well as discuss how Cilium with Linux and BPF fits into the evolving encryption standards and frameworks such as IPsec, mTLS, Secure Production Identity Framework For Everyone (SPIFFE), and Istio. Looking forward we propose a set of extensions to the Linux kernel, specifically to the BPF infrastructure, to ease the adoption and improve the efficiency of these protocols. Specifically, we will look at a series of BPF helpers, possible hardware support, scaling to thousands of nodes, and transparently enforcing policy on encrypted sessions.

Finally to show this is not mere slide-ware we will show a demo Cilium implementing transparent encryption.

I agree to abide by the anti-harassment policy

Yes

I confirm that I am already registered for LPC 2019

Primary author: Mr FASTABEND, John (Isovalent)

Presenter: Mr FASTABEND, John (Isovalent)

Session Classification: Networking Summit Track