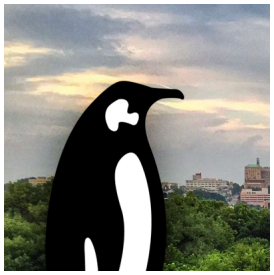

Contribution ID: **302** Type: **not specified**

Application network security and observability in an encrypted future

Tuesday, 14 November 2023 12:00 (30 minutes)

Application security and observability systems provide useful insight into L7 application networking. These systems promise nice looking service maps showing all your GRPC connections and how all the network services interact. They snoop DNS traffic providing the key insights of IP to DNS name mappings in a world where IPs are increasingly dynamic and meaningless from an identity perspective. From observability security policies can be built and applied pushing least privilege principles into the application networking.

However, this tooling is on a collision course with TLS1.3 (encrypted SNI), encrypted DNS and HTTPS. Faced with losing the valuable insights folks have proposed moving observability into the encryption library with uprobes or application modifications. Alternatively, to keep the threat models required when applications are not trusted users have proposed proxy logic and complex certificate management systems. We've even seen proposals to steal the SSH keys from the pod directly through the filesystem. Often security architects cringe.

Linux has all the building blocks to build a better model though. In this talk we discuss the threat models we believe a security or reliable observability platform needs to meet. Then show how we might build this system using kTLS and BPF. We will discuss current limitations and propose improvements to make the system more seamless and easier to use. As well as provide performance benchmarks. The hope here is to show by extending the operating system with BPF we can chart a course to transparent encryption and keep the security tooling working.

Primary author: FASTABEND, John (Isovalent)

Presenter: FASTABEND, John (Isovalent)

Session Classification: eBPF & Networking

Track Classification: eBPF & Networking Track