Identity Aware Threat Detection and Network Monitoring by using eBPF

eBPF Summit

Natalia Reka Ivanko, Isovalent

October 28, 2020

Introduction

- Wide variety of eBPF use cases (logging, CPU over overhead)

- Today:
  - Network Monitoring and Threat Detection
- Use Cases:
  - Monitor suspicious inbound/outbound connections

  - External connections to suspicious IP (outbound)
  - Unauthorized traffic from the Internet (inbound)
  - Workloads accessing the K8s API server

Problem

- Traditional network-layer tools are based on IPs and ports
- K8s workloads are containerized
- IPs are dynamically changing all the time, not meaningful anymore

One of the solutions

- eBPF + Cilium
- Export the data to Splunk
- Define signatures

Egress flows to suspicious external IP

- Monitor certain workloads for outbound connections

- Example:
  - Compromised pod with a Monero miner
- Alert fields:
  - Source (namespace, pod, labels)
  - NetworkPolicyDecision
    (FORWARDED, DROPPED)
  - DestinationDNS

Unauthorized connections from the Internet

- Monitor and audit application
- Unexpected / unauthorized connections to workloads

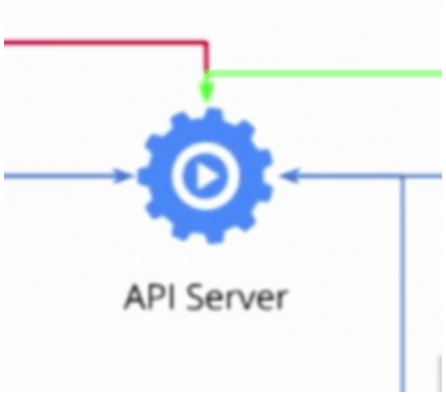
- Example:
  - Exposing a Kubernetes service unintentionally (e.g: Guestbook FE)
- Alert fields:
  - Destination (K8s labels)
  - NetworkPolicyDecisions

    (FORWARDED, DROPPED)

Workloads accessing the K8s API server

- Detect unauthorized, malicious traffic

- Example:
  - Already existing vulnerability and a compromised pod
  - Stolen token
- Alert fields:
  - Source (namespace, pod, labels)
  - NetworkPolicyDecision
    (FORWARDED, DROPPED)



eBPF

Q&A on the Slack channel :)