Process level network security monitoring and enforcement with eBPF

SSTIC 2020

Guillaume Fournier
Security Engineer
github.com/gui774ume
gui774ume.fournier@gmail.com
I. Problem

II. eBPF: a new technology

III. Proposal

IV. Demo

- Cutting egress is hard (filtering ports / protocols is not enough)
  - IP based solutions
  - DNS based solutions
- Applying networking rules is hard
  - Granularity
  - Kubernetes (rules propagation & pods scheduling)

Provide a network access control solution, at the process level, in a Kubernetes environment
I. Problem

II. eBPF: a new technology

III. Proposal

IV. Demo

Network Security Probe architecture

Pod 1   Pod 2   Pod 3   Pod 4

Security Profiles (ETCD)

Network Security Probe

Kernel
eBPF

K8s Node

Internet

SSTIC 2020 - Guillaume Fournier
I. Problem

II. eBPF: a new technology

III. Proposal

IV. Demo

- Cutting egress is hard (filtering ports / protocols is not enough)
  - IP based solutions
  - DNS based solutions
  ➔ Snoops on DNS requests to enforce IPs

- Applying networking rules is hard
  - Granularity
  - Kubernetes (rules propagation & pods scheduling)
  ➔ Per workload and per process rules
I. Problem  II. eBPF: a new technology  III. Proposal  IV. Demo

- Differences with Cilium
  - Process level monitoring & enforcement
  - Non-intrusive design
  - In-kernel DNS parsing
  - Attacks detection & prevention
  - Includes host protection
In-kernel overhead: Average round trip time per domain (over 5000 A record queries / domain)
I. Problem  

II. eBPF: a new technology  

III. Proposal  

IV. Demo  

Demo 1: security profiles configuration and update  

Demo 2: RCE exploitation  

pastebin.com
Thanks

Source code:
https://github.com/gui774ume/network-security-probe

guillaume@datadoghq.com