Securing Sidecar Containers in a Zero Trust Kubernetes Cluster

Aarni Halinen

Department of Computer Science
Aalto University

May 23, 2023

Supervisor: Prof. Mario Di Francesco
Advisor: M.Sc. (Tech.) José Luis Martin Navarro
Advisor: M.Sc. (Tech.) Jacopo Bufalino

Zero Trust Architecture

- A

Containers

- Linux namespaces
- Container breakout

Kubernetes

- Industry standard container orchestrator

Kubernetes Control Plane

- TODO: Add image

Container Network Interface (CNI)

- Kubernetes has no built-in component that provides connectivity and reachability for Pods $\Rightarrow$ CNI plugins
- Plugins may differ in architecture significantly
- Calico and Cilium are powerful CNIs that work with IPTables and eBPF

Network policies

- Default Kubernetes resouce, allows creationg of Ingress and Egress rules for Pods
- Rules are applied to Pod's default NIC by the CNI plugin
- Does not affect intra-Pod communication via loopback device

Pod Security Admission control

- G

Sidecar pattern

- H

Sidecar pattern issues

- Containers within a Pod share namespace $\Rightarrow$ same PSA rules
- Same NetworkPolicy for all containers in a Pod $\Rightarrow$ all containers have same Egress policy
- No isolation on loopback device

Network Isolation Solution 1: IPTables or eBPF

- Add IPTables rules to sidecar after Pod is deployed
- Containers share IP address $\Rightarrow$ need to use IPTables owner-module (user-id, similarly to Envoy proxy) to apply rules only for the sidecar

Network Isolation Solution 2: Split containers to own namespace

- Own Pods $\Rightarrow$ NPs can be used to restrict communication
- Own Kubernetes namespaces $\Rightarrow$ own PSA rules
- Not sidecar anymore (no loopback connectivity, deployed to different Nodes...)
- Prevent scheduling on different Nodes with Node and Pod affinity

Multus

- CNI plugin that allows multiple NICs per Pod
- Uses other CNI plugins for implementation the NICs
- Allows creation of another network segment between Pods

Solution 2+: Re-routing loopback to Multus NIC

- Requires kernel flag to be set: net.ipv4.conf.all.route_localnet=1
- DNAT rule on IPTables in sufficient but eBPF solution is also possible
- Open source Network Policy implementation for Multus network exists
- Combined with affinity, sidecar is deployed on same Node and communicates via loopback!

Refining the solutions

- Use a custom CNI plugin or controller loop to modify Pod network namespaces, however no available implementations yet exist
- All solutions are somewhat hacky and unstable, including Multus network with policies

Extra security

- Tetragon for observability?
- Service meshes?

Re-cap

- Kubernetes does not support Zero Trust Architecture
- Custom CNIs and controllers can be used to build ZTA to Pod network namespace

References

- N