Container Security

Hackathon - 8
Puneet, Arun

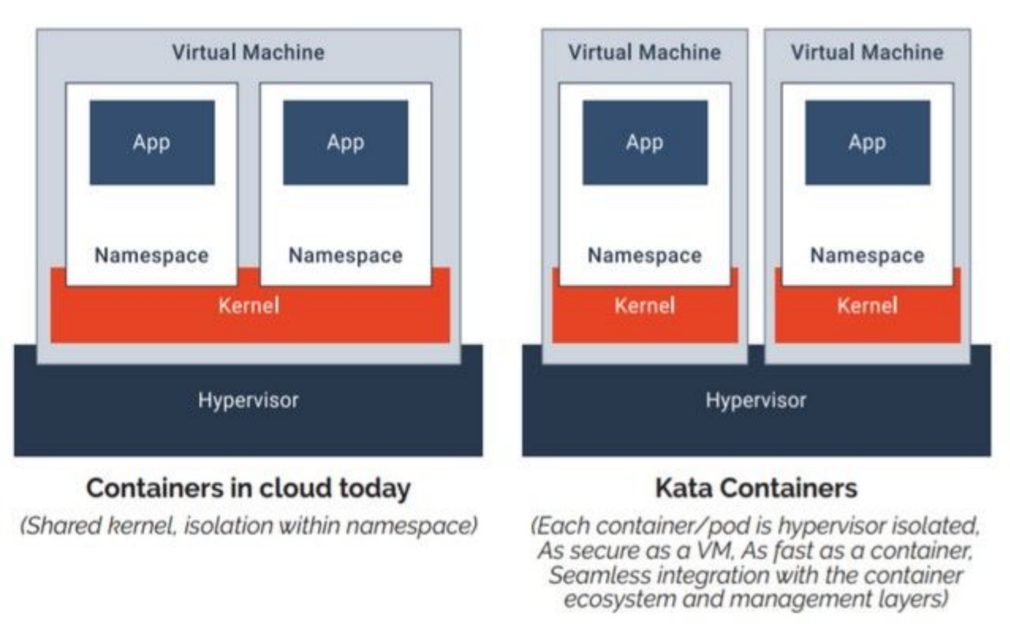
Why?

- Us : Multi-tenancy requirements to run our customer accounts

- Customers: Administrative control over user workloads. Added security over network isolation & micro-segmentation

Kata Containers

- Container isolation
- No shared kernel



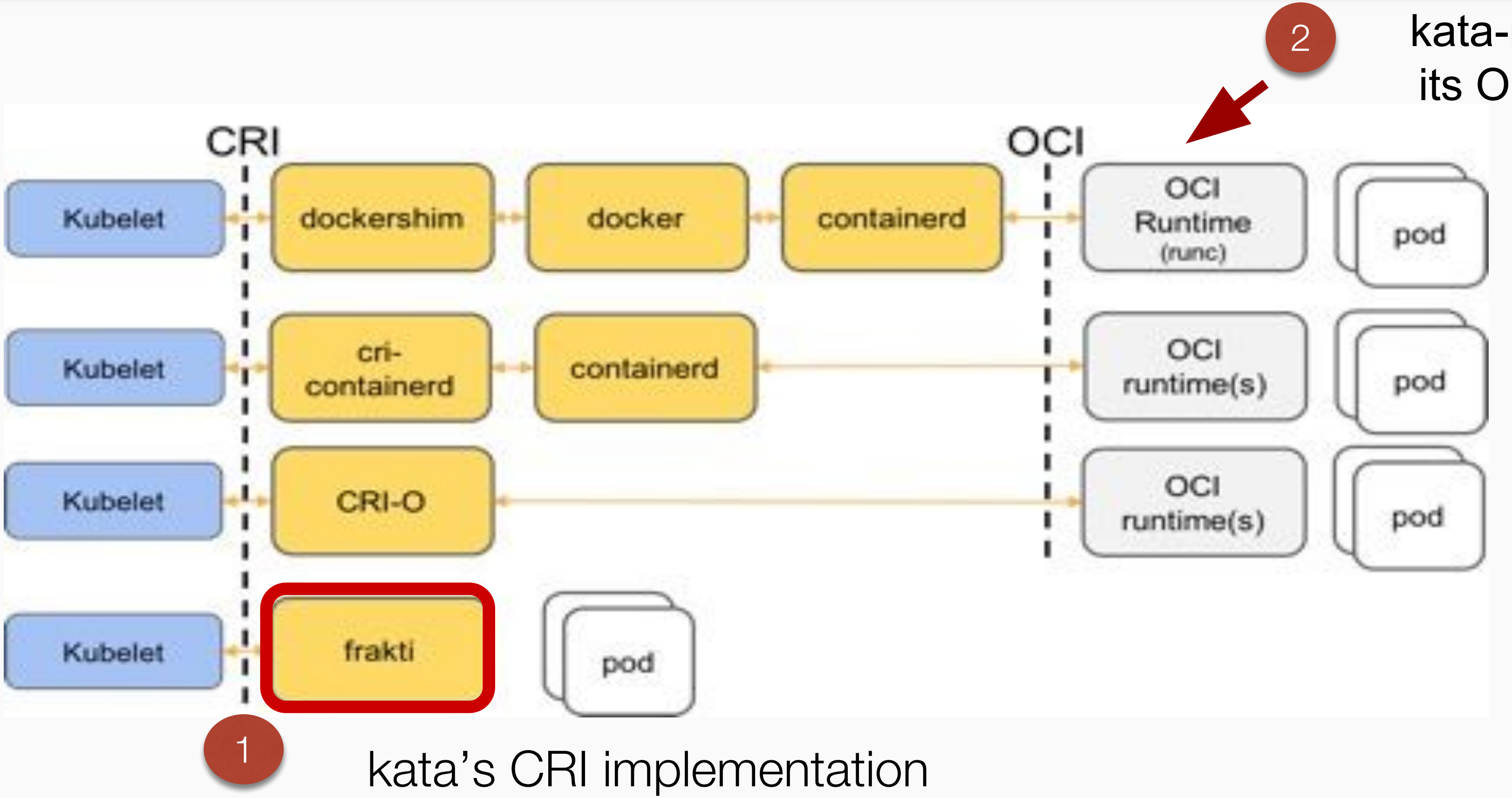
Containers in cloud today

(Shared kernel, isolation within namespace)

Kata Containers

(Each container/pod is hypervisor isolated. As secure as a VM. As fast as a container. Seamless integration with the container ecosystem and management layers)

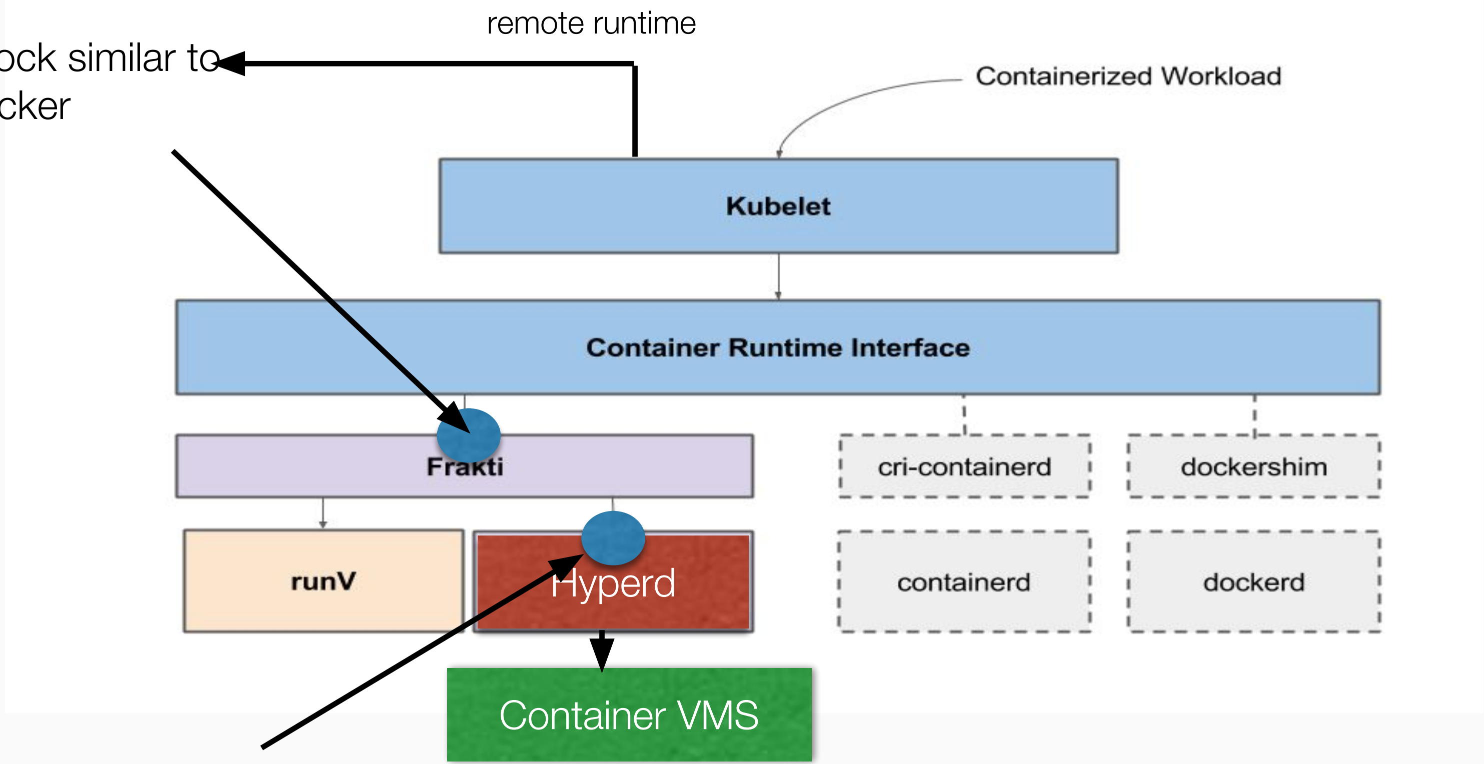
Kata Containers



kata-runtime
its OCI impl

kata's CRI implementation

Kata Containers



Kubelet is told to use this remote runtime

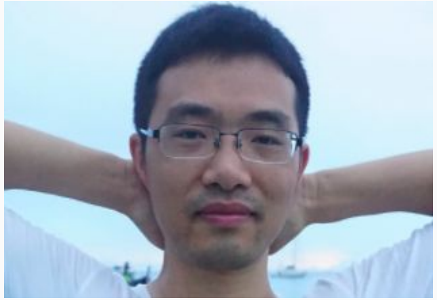
listens on sock similar to docker

listens on host:port

Thanks

katacontainers.slack.com

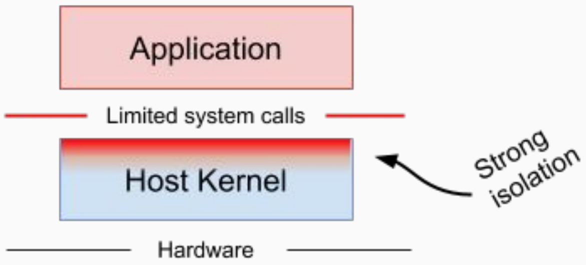
Harry



Peng

- Helped through multiple issues
  - Version mismatch (even updated the release!)
  - Invalid artifacts..
  - Guided on how to build various components from source

gVisor



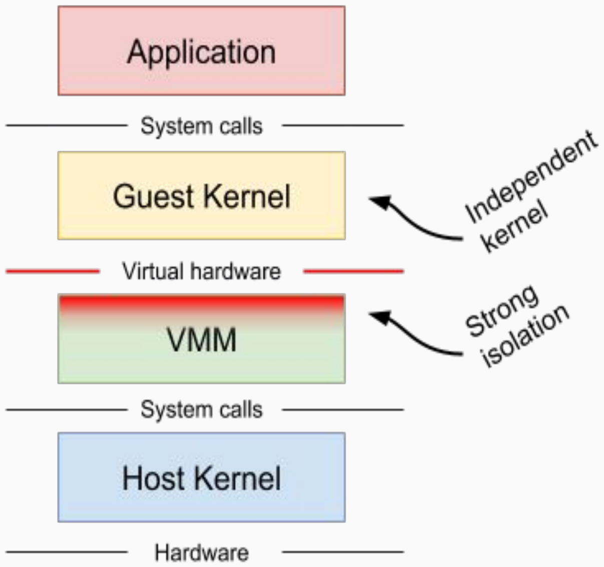
Application

Limited system calls

Host Kernel

Strong isolation

Hardware



Application

System calls

Guest Kernel

Independent kernel

Virtual hardware

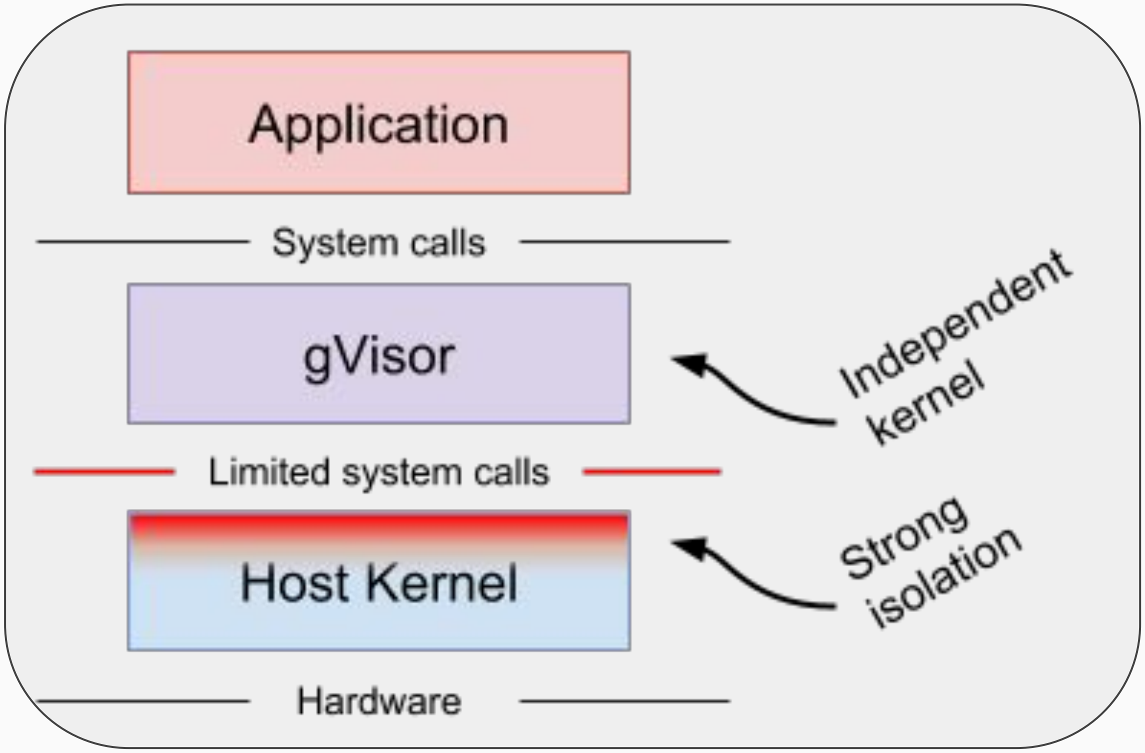
VMM

Strong isolation

System calls

Host Kernel

Hardware



Application

System calls

gVisor

Independent kernel

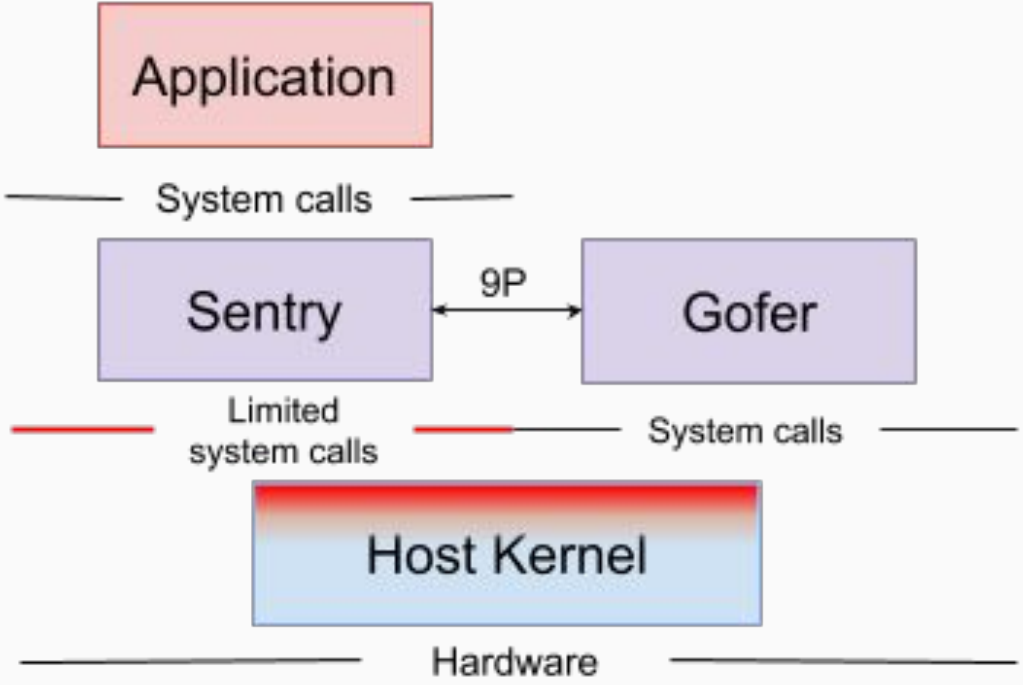
Limited system calls

Host Kernel

Strong isolation

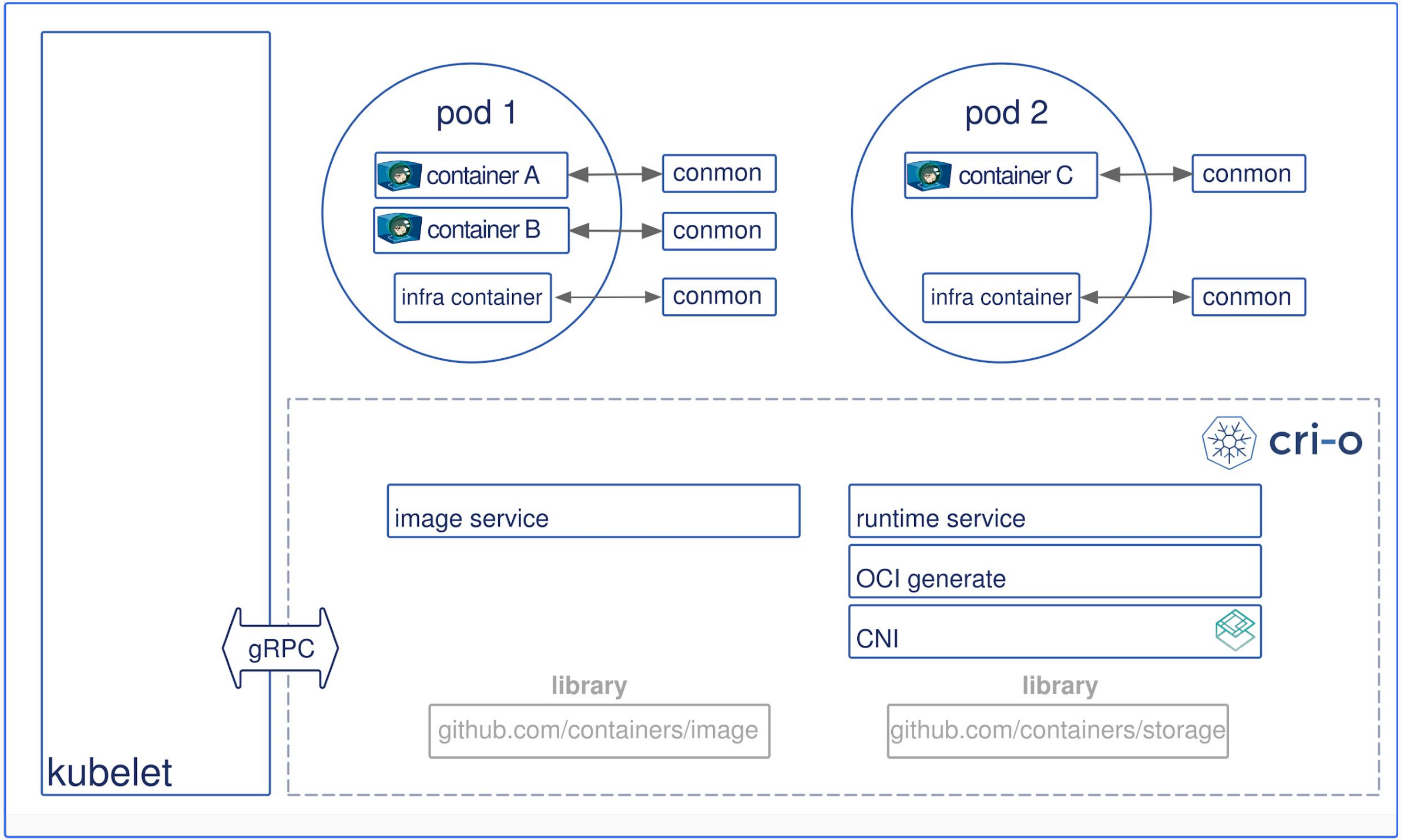
Hardware

gVisor



- User space kernel implementation
- Each container is sandboxed by this user space kernel
- Uses cri-o to integrate wi k8s

cri-o


pod 1
container A
container B
infra container
conmon
conmon
conmon
pod 2
container C
infra container
conmon
conmon
cri-o
image service
runtime service
OCI generate
CNI
gRPC
library
github.com/containers/image
library
github.com/containers/storage
kubelet

Demo

Resources

- Notes: https://docs.google.com/document/d/1hJkjDFVlAm1f6gcM4WWW4ldTxP4XGhnnRTn-XoEf4tU/edit?usp=sharing
- gVisor: https://github.com/google/gvisor#kubernetes-support-experimental
- Kata: https://github.com/kata-containers
- CRI-O: https://github.com/kubernetes-incubator/cri-o
- Kelsey Hightower (K8s the hard way with CRI-O & runsc): https://github.com/kelseyhightower/kubernetes-the-hard-way/blob/master/docs/09-bootstrapping-kubernetes-workers.md
- https://katacontainers.io/posts/why-kata-containers-doesnt-replace-kubernetes/
- https://medium.com/cri-o/intel-clear-containers-and-cri-o-70824fb51811
- https://kubernetes.io/blog/2017/11/containerd-container-runtime-options-kubernetes/
- https://github.com/kubernetes/frakti/blob/master/docs/deploy.md