Securing Containers

Djob Mvondo

ESIR 2021/2022

Containers

- Fast instantiating times
- Portable via DockerFiles
- Supported by major Cloud providers
- Several runtimes and orchestrators

--- Poor isolation

Track syscalls to filter malicious ones

- Proposed by gVisor (https://gvisor.dev)
- Proposed in 2018 by Google
- However, it incurs overhead for I/O intensive applications

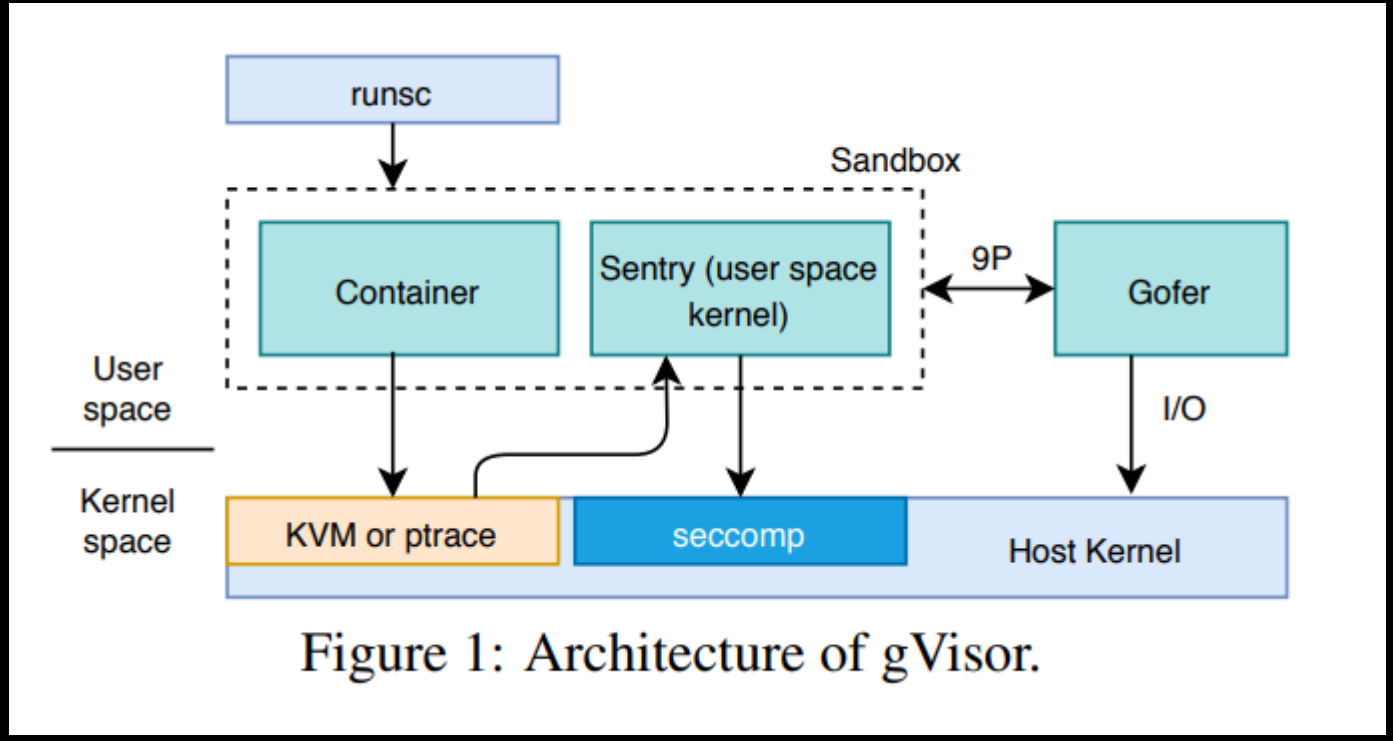


Figure 1: Architecture of gVisor.

Li, Guoqing, et al. "Comparative Performance Study of Lightweight Hypervisors Used in Container Environment." *CLOSER*. 2021.

Young, Ethan G., et al. "The True Cost of Containing: A {gVisor} Case Study." *11th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 19)*. 2019.

Run containers in VMs

- Proposed by KataContainers (https://katacontainers.io/)
- Proposed in 2017 by Intel

Previous Intel Clear Containers

- Good balance between security and boot time.
- Lacks support for SELinux and has network issues

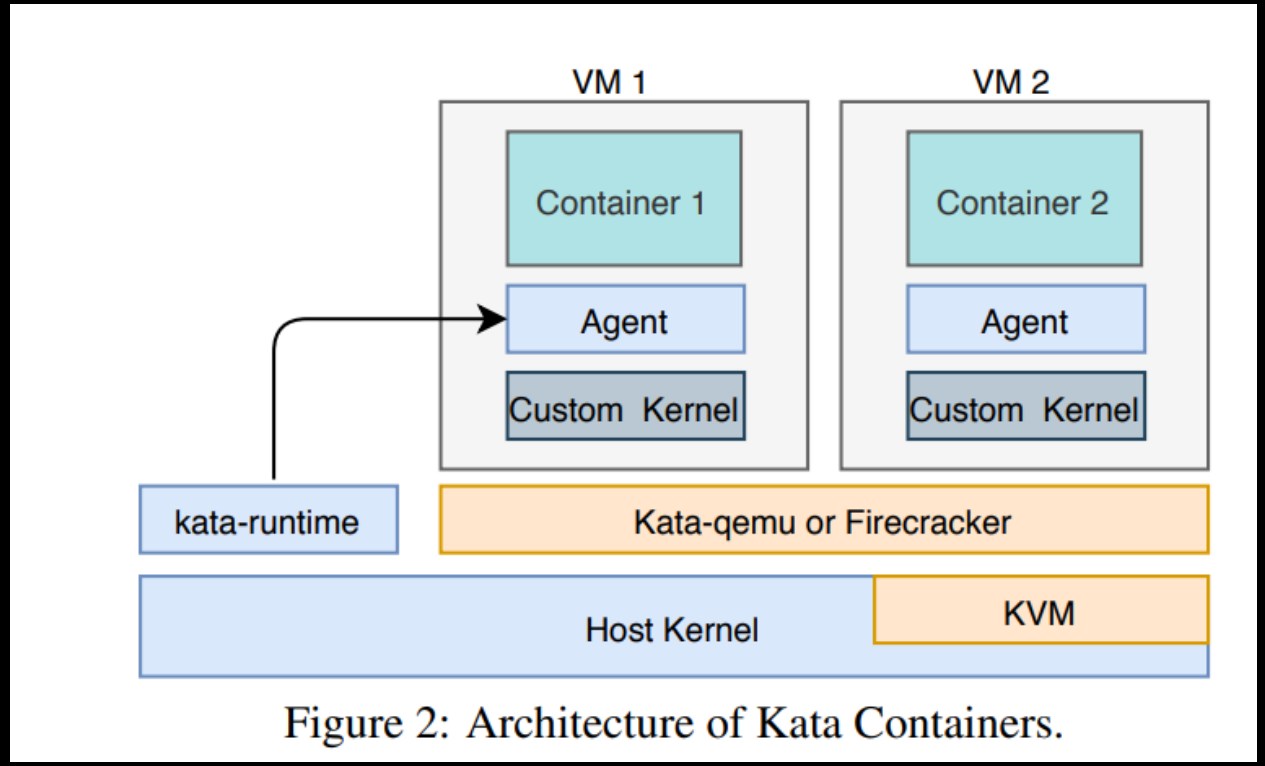
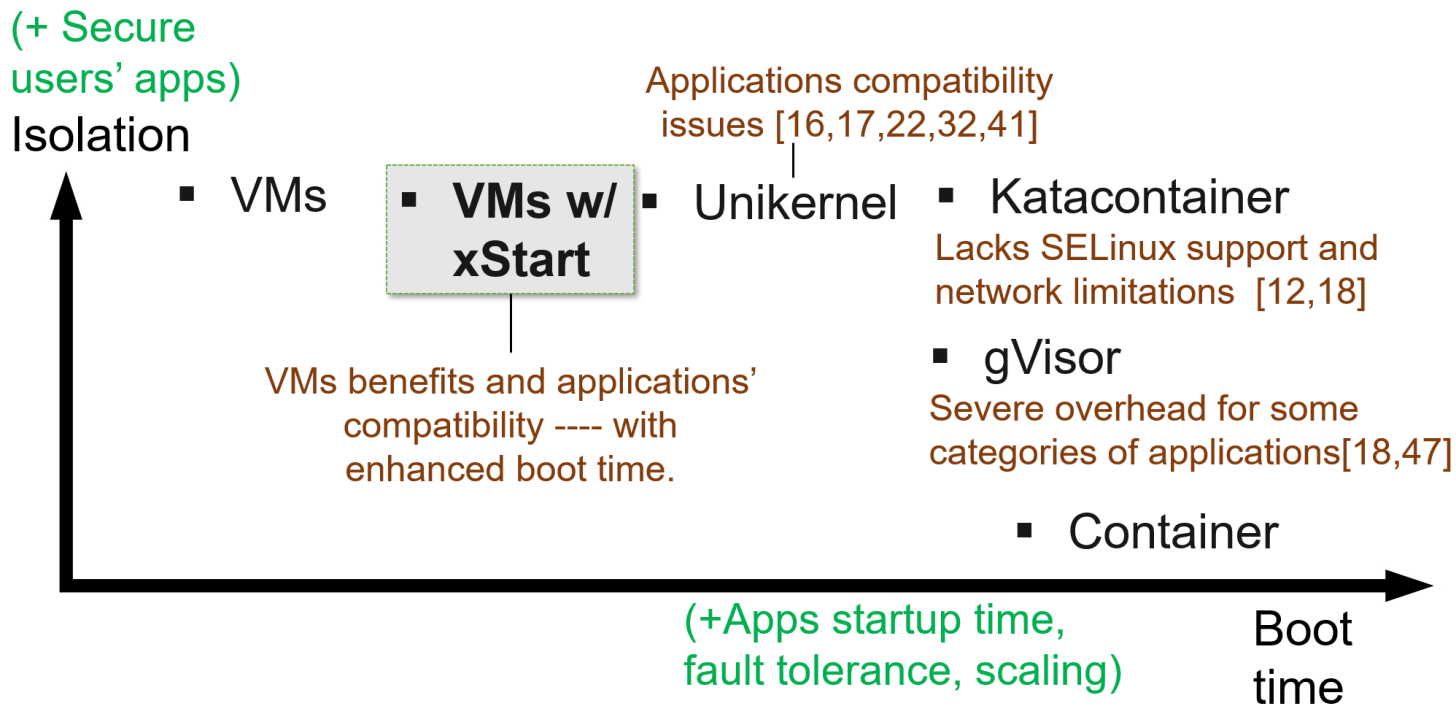


Figure 2: Architecture of Kata Containers.

Li, Guoqing, et al. "Comparative Performance Study of Lightweight Hypervisors Used in Container Environment." *CLOSER*. 2021.

Overall

- Several works to improve the Cloud
- Ongoing research works
- Beware of your usecases



There is room for improvement ☺