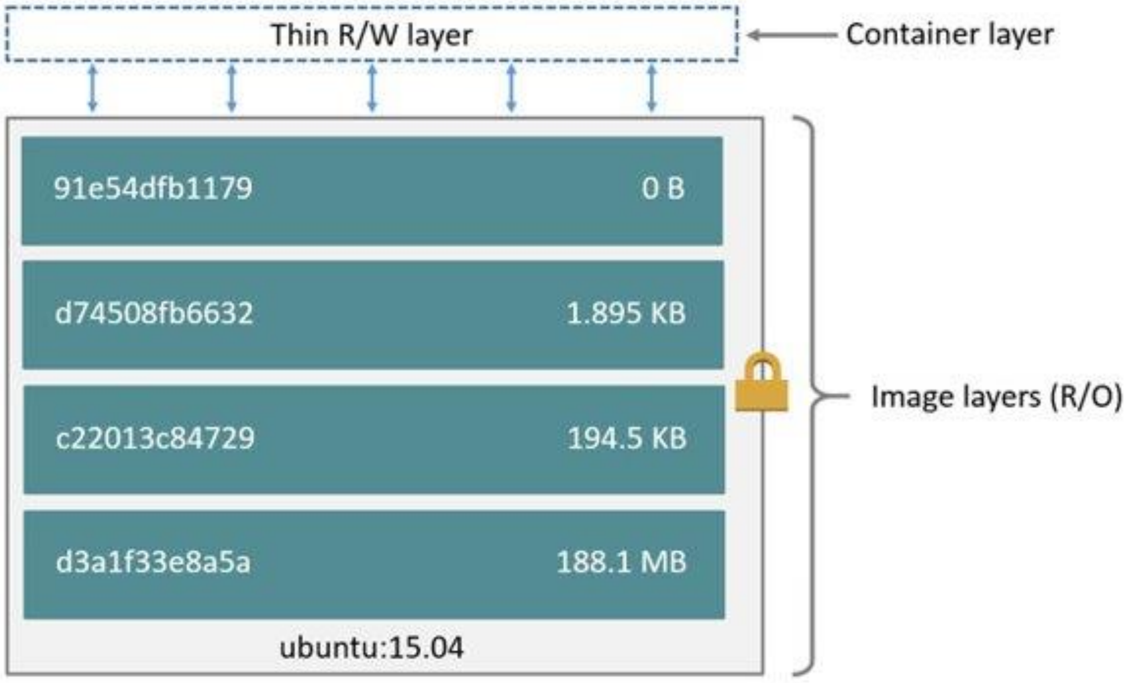
DORNERWORKS

Improving Embedded DevOps with seL4 VMM

Containers

Packaging of software execution code along with required OS libraries and dependencies inside a lightweight executable called a container that can be used reliably across multiple environments.

- Containers are built from images
  - Images built from read-only layers
  - Layers can be shared across images
  - When deployed (as a container) top-most layer mounted as rd/wt
- Managed and configured by a container runtime software
  - Docker set the standard in 2013
  - Kubernetes, OpenShift, Podman



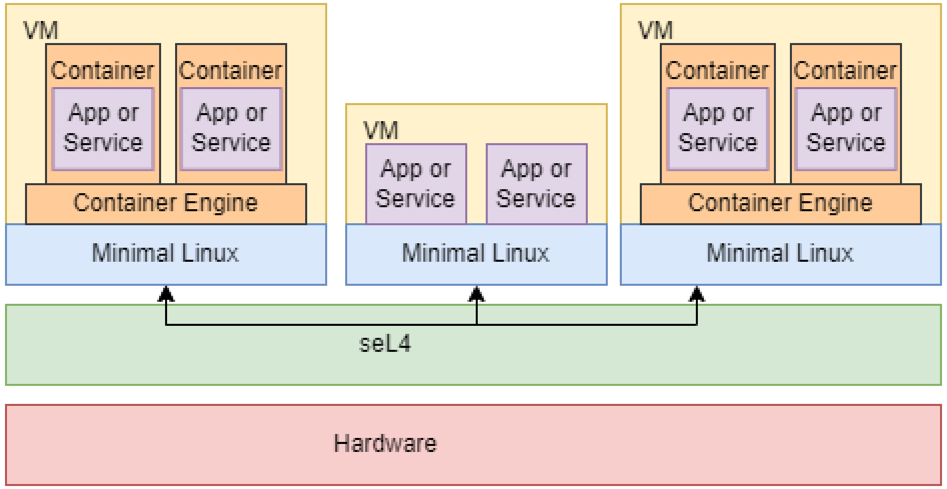
Container
(based on ubuntu:15.04 image)

Containers for Embedded DevSecOps

- Containers benefit Embedded DevSecOps
  - Improved Deployment/Portability
  - Local Testing and prototyping
  - Near native performance
  - Large databases of container images (building blocks)
  - More secure isolation than apps as processes
- However, Isolation is not as secure as a hypervisor

Embedded DevSecOps for Mixed-Criticality Systems

- Running an OS with containers does not provide strong enough isolation for Mixed-Criticality Systems
- In these cases, you want to use a hypervisor to get the necessary security guarantees
- Containers and seL4 virtualization provides the best of both worlds
    - Strong isolation between criticality levels
    - DevOps improvements from containers
        - Prototyping/Testing/Deploying
- DornerWorks has a prebuilt Linux VM that supports containers



Future Plans

Reduce memory usage

- Current build uses 1 GB to support ramdisk with container engine
  - Before container images!
- Optimize current image
- Alternatives:
  - LinuxKit

Containers directly on seL4

- Still get strong isolation benefits of seL4
- Should also reduce memory usage
- ▼ Large undertaking

Investigate Unikernels

- Provides similar benefits of containers
- Each app gets built with the unikernel and just the libs/stacks it needs
- Each unikernel deployed as its own VM

Discussion Ideas

- DevSecOps Needs from community
- Thoughts on where to go
- Unikernel adoption

References

- http://gvsets.ndia-mich.org/documents/CGS/2022/Containeriztion%20in%20Embedded%20Trusted%20Computing.pdf
- https://trustedcomputingcoe.org/__static/4ef7dd6c50293b00ecf3656d703f2549/10_-1-_luhui_enablingsel-4-containerstosupportlegacyapplications.pdf