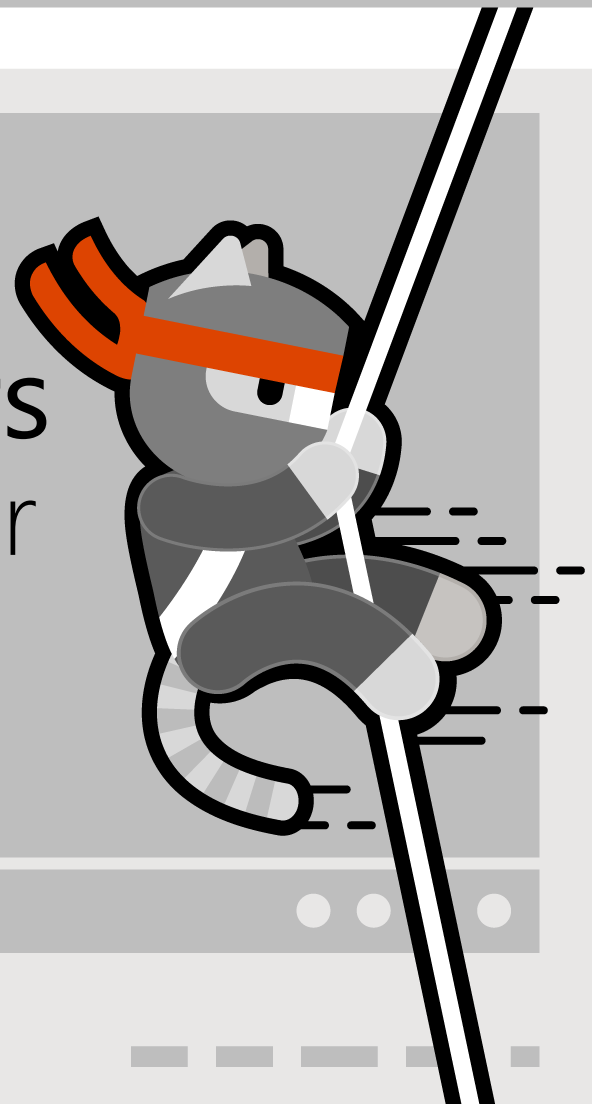
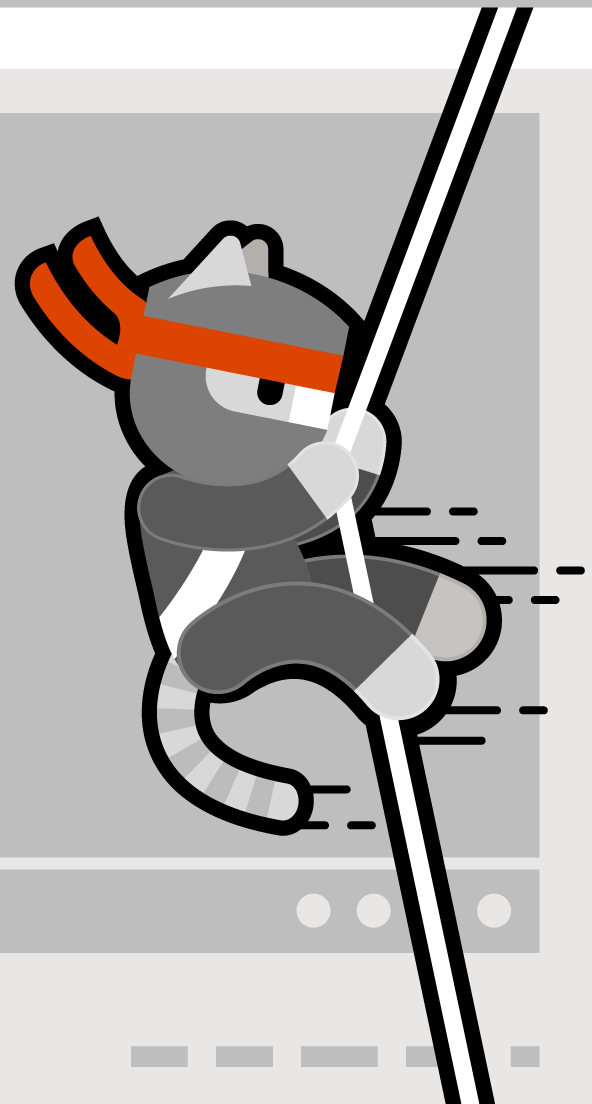
Hacking Containers

Applications & Docker



Eng Teong Cheah

Microsoft MVP



Applications

Containers have slowly taken the place of virtual machines in many environments

There is a tradeoff currently between containers and virtual machines – one that we can easily exploit.

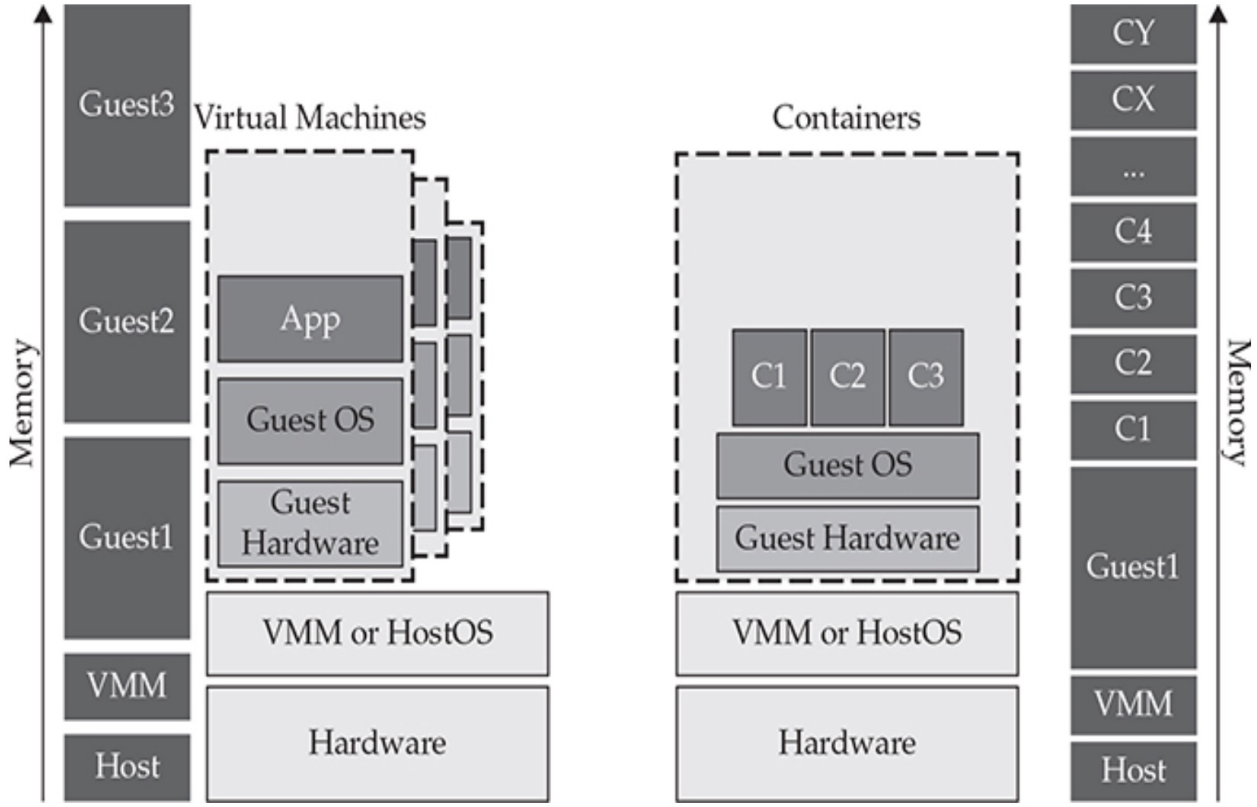
Virtual machines bring a layer of security into the application by virtualizing the hardware layers.

This abstraction means that an operating system kernel, drivers, memory management, and file system must be provided each time a virtual machine is created.

Applications

Containers are different; they bring over the userland binaries and share the operating system kernel, drivers, and memory structures.

The demarcation or isolation is at the container group and namespaces layer.



What Is Docker?

Docker is not a Container Runtime Interface (CRI).

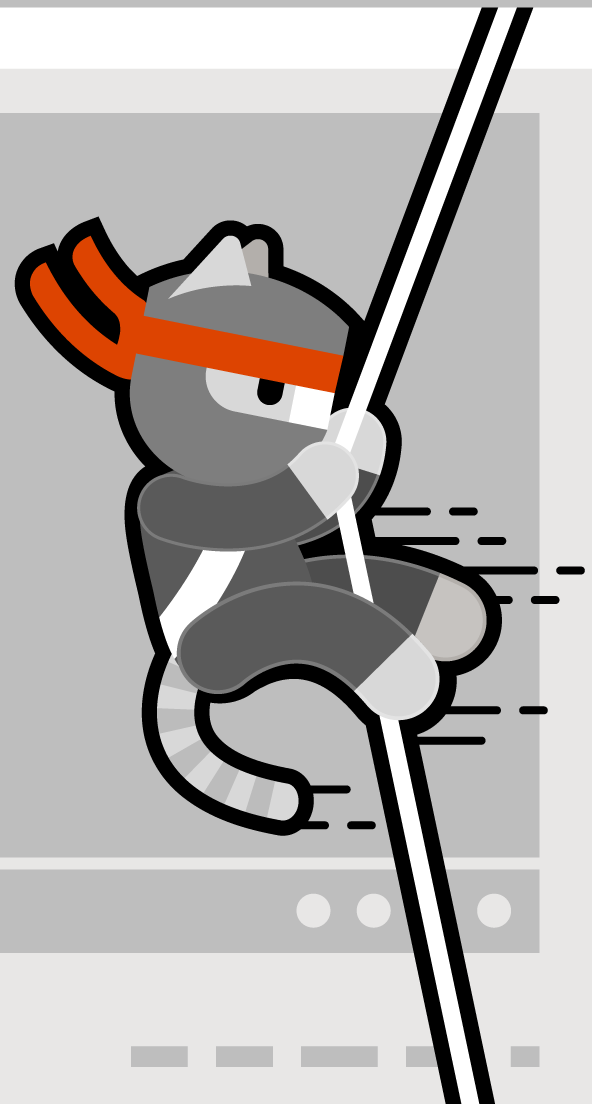
Docker open-sourced its container runtime interface knowns as ContainerD.

The Docker daemon usually runs in a Linux socket, but not always.

Seaching on popular Internet search tools will yield many open and exposed Docker daemons.

In essence, Docker ends up being a wrapper command or an API layer that orchestrator that allows an administrator to orchestrate multiple containers on the same box.

Demo
Looking for Docker Daemons



References

Gray Hat Hacking, Sixth Edition