Secure container in IoT segment – Extend KATA to ACRN IoT hypervisor

Yu Wang, Intel SSP
PART1: ACRN Overview
PART2: Introducing Container to IoT
PART3: Why KATA Container
PART4: Extend KATA to ACRN
ACRN™ is a Big Little Hypervisor for IoT Development

ACRN™ is a flexible, lightweight reference hypervisor, built with real-time and safety-criticality in mind, optimized to streamline embedded development through an open source platform.
ACRN Focus

- Small Footprint
- Built for IoT
- Adaptability
- Built for Real-Time
- Safety Criticality
- Truly Open Source
Virtualization User Cases for IoT

- In-Vehicle-Infotainment
- Robotics
- Precision instrument
- Industrial
Why introducing container to IoT?

- Container technology is easy deployment, provide consistent behavior on any supported hardware platforms.

- More and more various of workloads need to be execute into single IoT embedded system, container technology provides isolation to avoid influence.

- Container image is built up from a serial of layers, can easy derives new features base on the mature container images. Accelerate the development of IoT production iteration with easy maintenance and upgradability.
# Container vs Virtual Machine

<table>
<thead>
<tr>
<th></th>
<th>Virtual Machine</th>
<th>Container</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heavyweight</td>
<td>Lightweight</td>
<td></td>
</tr>
<tr>
<td>Limited performance</td>
<td>Native performance</td>
<td></td>
</tr>
<tr>
<td>Startup time in minute</td>
<td>Startup time in seconds</td>
<td></td>
</tr>
<tr>
<td>Allocates required memory</td>
<td>Requires less memory space</td>
<td></td>
</tr>
<tr>
<td>Hardware-level virtualization</td>
<td>OS virtualization</td>
<td></td>
</tr>
<tr>
<td>Fully isolated and hence more secure</td>
<td>Process-level isolation, possibly less secure</td>
<td></td>
</tr>
</tbody>
</table>

*Container is not secure!!*
Kata provides a lightweight VM and individual kernel for additional isolation.

Utilize the hardware virtualization technology to provide more secure isolation.

Isolation by namespaces, cgroups with shared kernel

Additional isolation with a lightweight VM and individual kernels
What are included in KATA?

**Kata-runtime**: A OCI compatible runtime.

**Kata-shim**: A CRI friendly shim.

**Kata-proxy**: A multiplex to route between kata-shim/kata-runtime and kata-agent.

**Kata-agent**: A process running in the VM as a supervisor for managing containers and processes running with those containers.
KATA+ACRN = secure container for IoT

- Hardware node
- Consolidated Workloads
  - Real time workload
  - FuSa workload
  - Container workload
Acrn is a type-1 hypervisor. All Kata container’s VM will share the same service VM.

Per Kata VM be launched by separated acrn-dm in service VM for providing mediator supports.

The guest VM executes the Kata provided highly performance optimized kernel and rootfs.
Acrn device model exports two PCI virtio console devices to guest VM, and provides UNIX domain socket interfaces for Kata host side services.

The Acrn guest VM is created by kata-runtime who will spawn the kata-proxy.

kata-proxy will connect to kata-agent over virtio consoles.

kata-proxy will offer access to the VM kata-agent to multiple kata-shim and kata-runtime clients associated with the VM.
Acrn device model exports two PCI virtio console devices to guest VM, and provides UNIX domain socket interfaces for Kata host side services.

The Acrn guest VM is created by kata-runtime who will spawn the kata-proxy.

kata-proxy will connect to kata-agent over virtio consoles.

kata-proxy will offer access to the VM kata-agent to multiple kata-shim and kata-runtime clients associated with the VM.
How to extend KATA to ACRN?

- Kata-runtime heavily utilizes the virtcontainer which provides a generic, runtime-specification agnostic, hardware-virtualized containers library.
- The virtcontainer abstracts the operations for the sandbox and container on different hypervisor solution. Adds a new hypervisor operation instance for Acrn.
Call for Participation

https://projectacrn.github.io/index.html
https://projectacrn.org

Joining ACRN Community Today!!!
Questions?