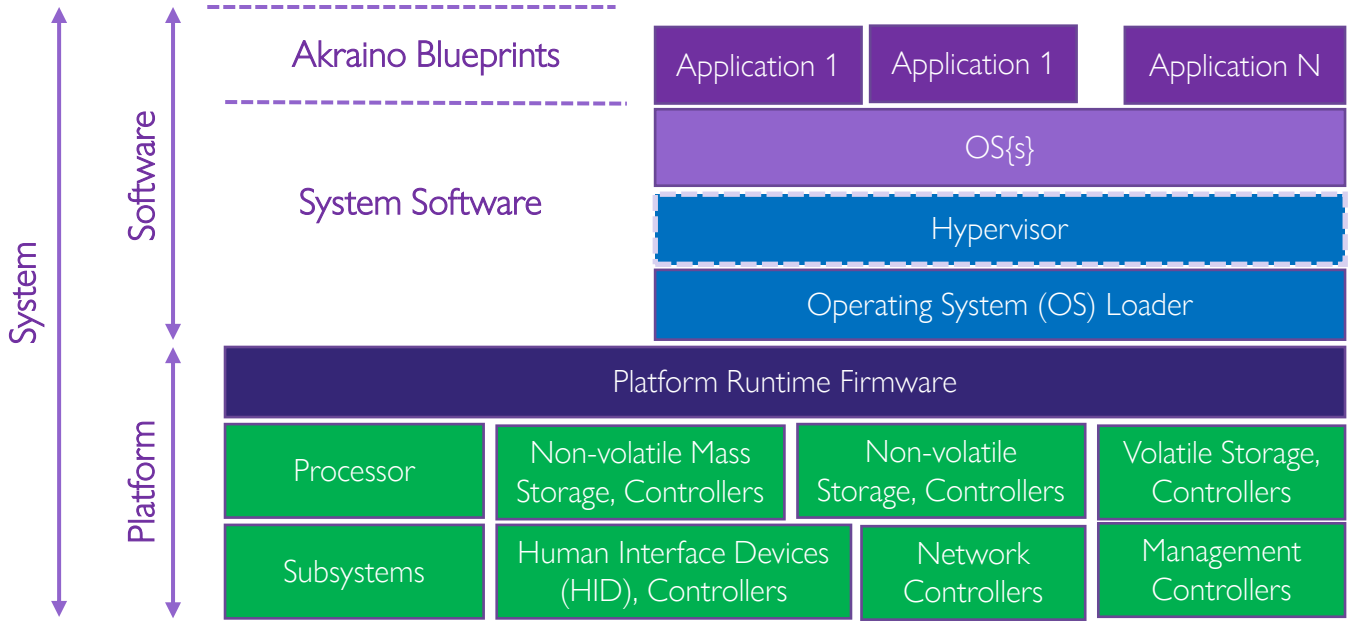
Akraino Platform Security Overview

December 2020

Daniil Egranov, Arm

Akraino System Components Overview



Security of Akraino execution environment (or System) consists both Platform and Software security:

- Containerized environment security (Akraino Blueprints)
- System software security (OS loader, Hypervisor and OS{s})
- Firmware Security
- Platform Devices Security

Akraino Platform Security Objectives

- Maintain the integrity of the platform layer and provide a safe execution environment for Akraino software stack.
- Define secure boot environments based on the platform Root-of-Trust.
- Secure attesting the platform's state of integrity.
- Protection of key assets in the platform:
  - Platform critical data (platform Id, encryption keys, configuration data, etc.).
  - Mutable firmware components.
- Secure platform firmware update.
- Protection platform runtime environment and data.
- Provide a secure interface for the Akraino software stack to the platform firmware runtime services and devices (TPM, TEE, etc.).

AKRAINO

Akraino Platform Security Goals

- **Unique identification.** Devices shall be uniquely identifiable.
- **Security lifecycle.** Devices shall support a security lifecycle. The device states shall be attestable and may impact access to data that is bound to the device.
- **Attestation.** Devices shall be securely attestable.
- **Software authorization.** Devices shall ensure that only authorized software is executed. Secure boot and secure loading processes are necessary to prevent unauthorized software from being executed.
- **Secure update.** Devices shall support secure update of software, or platform critical data like hardware configuration.
- **Anti-rollback.** Devices shall prevent unauthorized rollback of updates
- **Isolation.** Devices shall support isolation. Isolation of trusted services from one another and from less trusted services is essential to protect confidentiality and integrity of that service.
- **Interaction.** Devices shall support interaction over isolation boundaries. The interfaces must not be used to compromise confidentiality and integrity of the device
- **Device binding of stored data.** All devices shall support unique binding of stored sensitive data to the device.
- **Cryptographic and trusted services.** All devices shall support a minimum set of trusted services and cryptographic operations that are necessary to support other security goals.

Akraino Security Platform Abstraction

Platform Abstraction Interface should be available for the Akraino blueprints for securely accessing the platform's runtime services and secure devices.

PARSEC is the **P**latform **A**bst**R**action for **SEC**urity, an open-source initiative to provide a common API to hardware security and cryptographic services in a platform-agnostic way. This abstraction layer keeps workloads decoupled from physical platform details, enabling cloud-native delivery flows within the data center and at the edge.

PARSEC provides the following:

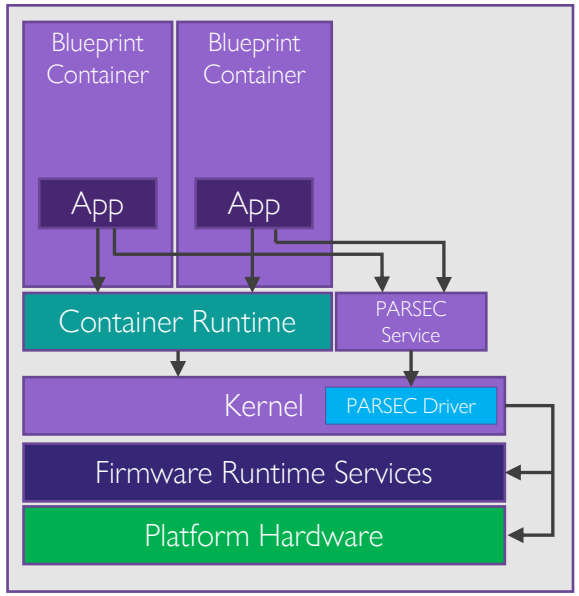
- **Abstraction** – a common API that is truly agnostic and based on modern cryptographic principles
- **Mediation** – security as a microservice, brokering access to the hardware and providing isolated key stores in a multi-tenant environment
- **Ergonomics** – a client library ecosystem that brings the API to the fingertips of developers in any programming language: "easy to consume, hard to get wrong"
- **Openness** – an open-source project inviting contributions to enhance the ecosystem both within the service and among its client libraries

https://github.com/parallaxsecond/parsec

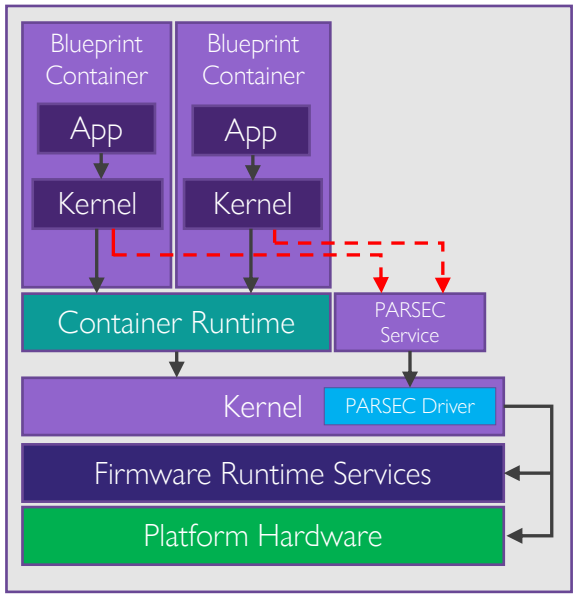
AKRAINO

Akraino Blueprints in Native Host Environment With PARSEC

Blueprint Containers on Host System

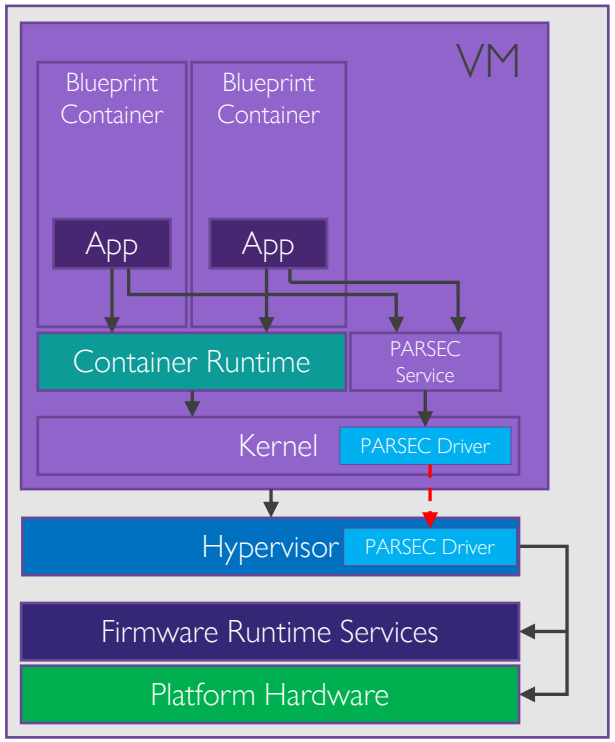


Blueprint Containers on Host System with Kernel in Container

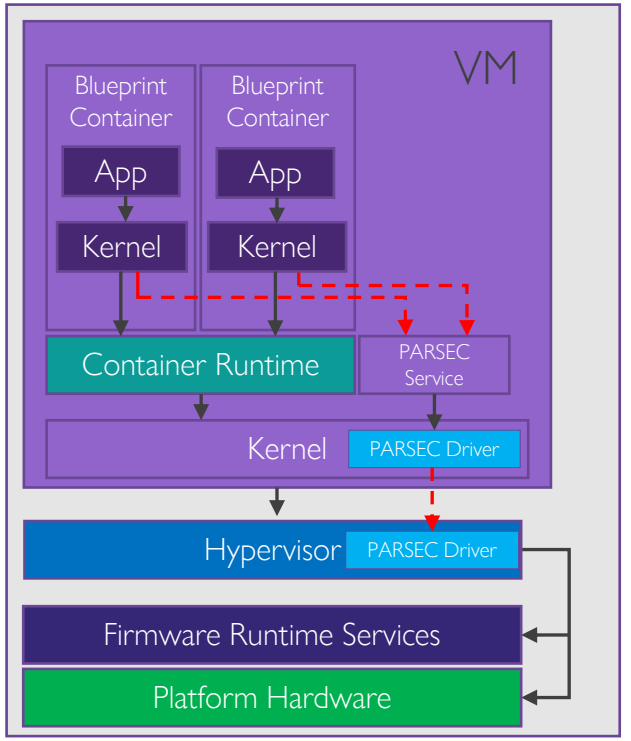


Akraino Blueprints in VM Environment with PARSEC

Blueprint Containers in Virtual Machine



Blueprint Containers in Virtual Machine with Kernel in Container



AKRAINO

Questions