Project Cassini
Infrastructure Line of Business
Q4, 2019
Context

• Intelligent infrastructure connecting a world of 1T endpoints to the Cloud – *the AI Edge* – is being built
• Diversity across Silicon, platform & application worlds fosters innovative solutions at the AI Edge, but...
• Deploying a cloud-native software stack at the infrastructure edge remains a significant challenge
Project Cassini

Goal
Ensuring a cloud-native experience across a diverse and secure edge ecosystem

Collaborate with Arm to

Define  Platform Standards & Reference Systems
Adopt  PSA extended for a secure Infrastructure Edge
Enable  Cloud-native Software stacks for the Edge
Platform Standards – Background

- The Infrastructure edge hosts a diverse array of platforms
  Traditional-embedded, fixed-function gateways
  General purpose compute with heterogenous accelerators

- Mature firmware + OS ecosystems co-exist
  Embedded / RTOS, U-Boot, Commercial BIOS
  Standard / Enterprise OS, Hypervisor, Bare-metal solutions

Platform standards at the AI Edge influenced by

- **Deployment** model → High-touch, per-system management vs. 3rd party-ready
- **Functional** model → **MUD**-based vs. general purpose compute
- **Management** model → System management & security updates – remote vs. local
Platform Standards – SBSA / SBBR

- Arm supports standards versus specific implementations
- Recommendations and guidelines uniformly apply to all platforms from the Infrastructure Edge to the Cloud / Datacenter

For all platforms expected to host 3rd party Commercial OSes, Hypervisors, or other bare-metal solutions → SBSA / SBBR
  Examples:- Red Hat, Windows, VMware ESXi,…

SBSA / SBBR
  Minimum Hardware requirements → SBSA
  Minimum Firmware requirements → SBBR
  Arm provides → Certification Program (ServerReady) + Compliance Test Suites (ACS)
Platform Standards – EBBR

Platform characteristics
Traditional/Embedded with varying degrees of per-platform engineering enablement, support & maintenance

For such Platforms that host a vertically-integrated stack derived from community distributions (Yocto/Linux, BSD or other), EBBR minimizes custom engineering effort on the Firmware-OS interface

Moving towards EBBR
1. Leverage UEFI by merging BSP to mainline U-Boot
2. Check EBBR-readiness with community-managed open-source tool from Arm (WIP)

Under consideration
- Android, Coreboot + LinuxBoot
Reference list of SBSA/SBBR platforms

For the latest on SBSA/SBBR platforms and partners, please go (here)
Platform Standards - Summary

1. Arm recommends **SBSA/SBBR** as the de-facto standard for all platforms esp., in cases where 3\textsuperscript{rd} party & managed software – OS, Hypervisors, etc. – are expected to run

2. When SBSA/SBBR is not feasible, esp. where vertically integrated OS stacks are enabled and managed, Arm recommends **EBBR**-compliance to reduce custom engineering efforts and to allow community distros to support Arm platforms
Security for the Infrastructure Edge

Background

- At the AI Edge, implementations for **Root of Trust (RoT)** & **RoT Service APIs** are heavily fragmented, between endpoints, edge, cloud, test and development environments, and across processor architectures and platforms
  - RoT examples: TPM, HSM, Secure Element, ...
  - RoT service API examples: PKCS11, TPM2.0, ...

Solution

**PSA** (Platform Security Architecture) solves fragmentation through architecture, reference SW and certification with market traction in the constrained IoT space

Project Cassini extends PSA to the infrastructure edge
PSA for constrained IoT devices

The open device security framework, with independent testing

**PSA: enabling right-sized device security**

---

**STAGE 1**

Analyzer
Threat modelling

**STAGE 2**

Architect
Hardware and firmware architecture specs

**STAGE 3**

Implement
Hardware and software

**STAGE 4**

Certify
Independently testing SoCs, devices and OSes

Unlocking digital transformation
# PSA extensions for the Infrastructure Edge

<table>
<thead>
<tr>
<th>PSA for M-profile (constrained IoT) deliverable</th>
<th>PSA for Infrastructure Edge deliverable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat models</td>
<td>New Threat Model and Security Analysis (TMSA) for the Edge</td>
</tr>
<tr>
<td>Firmware Framework-M</td>
<td>Firmware Framework-A</td>
</tr>
<tr>
<td>Trusted Boot and Firmware Update</td>
<td>Same</td>
</tr>
<tr>
<td>PSA APIs (Crypto, Attestation, Secure Storage)</td>
<td>Same</td>
</tr>
<tr>
<td></td>
<td>A new open-source security microservice: <a href="https://bit.ly/311Pb3Q">PARSEC</a></td>
</tr>
<tr>
<td>Trusted Firmware-M</td>
<td>Trusted Firmware-A</td>
</tr>
<tr>
<td></td>
<td>New features being added to support the needs of infrastructure</td>
</tr>
<tr>
<td>Certification scheme</td>
<td>In progress – Working to understand market need</td>
</tr>
<tr>
<td></td>
<td>New SBSG – Server Base Security Guide</td>
</tr>
</tbody>
</table>

Security for the Infrastructure Edge – PARSEC

The gap between Secure Hardware & Cloud native software worlds

- Key benefit of cloud native ➔ software abstracts the platform
  - Once software is packaged (e.g. as a container), can be deployed anywhere
- But the best security is rooted in hardware..
- Plumbing hardware directly into cloud native stacks, weakens ‘run anywhere’ benefits

PARSEC
Provides applications, access to security services in a Project Cassini platform

- Architecture neutral
- Reference implementation available in PSA software
- Originally developed in collaboration with Docker
- Currently independently hosted as open source with plans to seed to a community project
End-to-End Integrated Hardware Backed Platform Security

PARSEC Collaboration with Docker

Docker Enterprise for IoT

DOCKER DESKTOP → TEST → POLICY → STAGING → PRODUCTION → DEVICES

Software
TPM

Software

Azure HSM
AWS CloudHSM
GCP vTPM
Software

TrustZone
Secure Element
(TPM, proprietary)
Software

PARSEC Backends

© 2019 Arm Limited
Cloud Native stack for the AI Edge
The AI Edge Technology Stack

Flexible Edge Deployment Profiles
- Cloud / Hyperscaler
- Enterprise
- Telco / MNO

Hybrid/Cloud Data Center ecosystem

Device ecosystem

Crypto services (device edge)

Crypto services (infrastructure edge)

Arm PSA

IDE
Code-once, deploy-anywhere

RUNTIME SECURITY SERVICES
- Edge Runtime
- Network Services
- Network Prediction
- SQL/NoSQL Data Engines
- Analytics
- Filter / React / Store

OS/ Container / Hypervisor

Hardware Acceleration

Arm Neoverse Platform

Root of Trust

Code-once, deploy-anywhere
Engaging on Project Cassini

- Enable standards-based edge & gateway platforms
- Integrate PSA / PARSEC APIs into Software runtimes
- Establish joint value propositions through end-to-end demos

Partner with Arm on PoCs to project-cassini@arm.com
Thank You
Danke
Merci
谢谢
ありがとうございます
Gracias
Kiitos
감사합니다
धन्यवाद
شكرًا
tωδή