Confidential Compute solutions in Arm® ecosystem
Confidential Compute solutions in Arm® ecosystem

Sridhar Valluru
Director Product Management
Arm®
Confidential Compute: Threats Addressed

- Protect code/data from higher privileged software (e.g., host, hypervisor, hardware agents) and administrators
- Strong isolation technologies to support multi-tenancy
- Encrypt memory to prevent physical access and cold boot attacks
- Encrypt multiple confidential regions with different keys
- Protect payload on IO links from interposer cards and physical probes
- Securely and uniquely bind device functions to confidential processes
## Arm v8.4-A Architecture for Security

### Architecture Features in Arm v8.4-A

<table>
<thead>
<tr>
<th>TrustZone®</th>
<th>Virtualization</th>
<th>S-EL2 Virtualization</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Protected from Host OS/Hypervisor</td>
<td>- Can be used to protect from host primary OS kernel</td>
<td>- Complementary to first two</td>
</tr>
<tr>
<td>- Platform security use cases for SIP + OEM</td>
<td>- Standard OS development</td>
<td>- Improves modularity and isolation in TrustZone®</td>
</tr>
<tr>
<td>- Specific tool chains/Trusted OS</td>
<td>- Limited only by available memory</td>
<td></td>
</tr>
<tr>
<td>- Limited resource</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Security State / PA Space

<table>
<thead>
<tr>
<th></th>
<th>Non-Secure PA</th>
<th>Secure PA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Secure</td>
<td>Allow</td>
<td>Block</td>
</tr>
<tr>
<td>Secure</td>
<td>Allow</td>
<td>Allow</td>
</tr>
</tbody>
</table>

### EL0, EL1, EL2, EL3

- **EL0**: VM1
  - Non-secure: App, App
  - Secure: TOS, Secure Service
- **EL1**: OS Kernel
- **EL2**: Hypervisor
- **EL3**: Monitor

TrustZone® protects from Host OS/Hypervisor and platform security use cases for SIP + OEM. It is specific to tool chains and Trusted OS and has limited resources. Virtualization can be used to protect from the host primary OS kernel, standard OS development, and limited only by available memory. S-EL2 virtualization is complementary to the first two and improves modularity and isolation in TrustZone®.
Arm v9+ Architecture for Security: RME

Architecture to protect application code and data

- TrustZone® 2 world to RME 4 worlds
  - Secure → Secure & Root
  - Non-Secure → Non-Secure & Realm
- Realm space is isolated from Secure & Non-Secure
  - Access violations results in page faults
- RME is implemented in hardware and firmware
  - Open source RMM and Monitor code
  - Resource allocation managed by hypervisor
  - Access management by Monitor code
- No change in programming model
  - Realm an extension of Non-Secure
  - Interrupt model remains the same

<table>
<thead>
<tr>
<th>Security State / PA Space</th>
<th>Non-Secure PA</th>
<th>Secure PA</th>
<th>Realm PA</th>
<th>Root PA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Secure</td>
<td>Allow</td>
<td>Block</td>
<td>Block</td>
<td>Block</td>
</tr>
<tr>
<td>Secure</td>
<td>Allow</td>
<td>Allow</td>
<td>Block</td>
<td>Block</td>
</tr>
<tr>
<td>Realm</td>
<td>Allow</td>
<td>Block</td>
<td>Allow</td>
<td>Block</td>
</tr>
<tr>
<td>Root</td>
<td>Allow</td>
<td>Allow</td>
<td>Allow</td>
<td>Allow</td>
</tr>
</tbody>
</table>
Confidential Compute TCB

Trust needs to extend to any component where code/data reside

- Memory controllers
  - Separate keys for worlds
  - Fresh Keys for individual Realms

- IO (CXL and PCIe) Controllers
  - Enable device assignment
  - Security support defined by SIG/Consortium
Attestation
For end user confidence in platform

- Hardware Enforced Security (HES) for Arm Confidential Compute Architecture
  - Initiates and measures AP Boot
  - Key generation and management
  - Collect measurements for the system

- Provides on-demand Attestation reports
  - Separate from cloud provider attestation

Platform and Realm Measurement:
Attestation reports used by end user to establish platform trust before running applications
Arm Confidential Compute Resources

https://www.arm.com/armccca

https://developer.arm.com/armccca

Contact: armccca@arm.com
Call to Action
Need for a subgroup to address common industry Confidential Compute issues

- Device attestation report standardization and verification
- Standardization of device isolation granularity
  Security context is same or smaller than Virtualization context
- Life cycle and supply chain management
- Independent device security certification
Visit Arm @ OCP 2021

Booth (B11)
• Demos: Arm SystemReady Certified Hardware
  • Arm SystemReady, SR – ServerReady:
    • Ampere Altra ‘Mt Jade’ Platform (Wiwynn)
  • Arm SystemReady, ES – Embedded Server:
    • Hawkeye Tech HK-6010
    • SolidRun Macchiatobin
  • Arm SystemReady, IR – IoT:
    • Raspberry Pi

Talks
• Wed, Nov 10 @ 8:35am Room 211A-D
  Cost Modeling Analysis for Heterogeneous Integration of Chiplets, Javier DeLaCruz (Arm), Mudasir Ahmad (Google), Anu Ramamurthy (Microchip Technology)
• Wed, Nov 10 @ 10:00am Room 220C
  Confidential Compute Solutions in Arm Ecosystem, Sridhar Valluru (Arm)
• Wed, Nov 10 @ 1:00pm Room 210C
  Introduction to Open System Firmware (OSF) at OCP, Dong Wei (Arm), Ryan O’Leary (Google), Anjaneya “Reddy” Chagam (Intel)
• Wed, Nov 10 @ 2:30pm Room 210BF
  Arm and Ampere support for Standards-based OpenSource Firmware, Samer El-Haj-Mahmoud (Arm), Peter Pouliot (Ampere)
Thank you!