DRTM Overview
Measured Boot – Static Root of Trust

SRTM Chain of Trust

Boot ROM (CRTM) → Early FW → UEFI → Boot Loader → Hypervisor → OS

TPM
Measured Boot – Static Root of Trust

SRTM Chain of Trust

Boot ROM (CRTM) → Early FW → UEFI → Boot Loader → Hypervisor → OS

TPM

OS

UEFI

Boot Loader

Hypervisor

Early FW

Boot ROM (CRTM)
Measured Boot – Static Root of Trust

SRTM Chain of Trust

Boot ROM (CRTM) → Early FW → UEFI → Boot Loader → Hypervisor → OS

Arbitrarily extensible (a “gap” in the trust chain)

TPM
Dynamic Root of Trust for Measurement

SRTM Chain of Trust

Boot ROM (CRTM) → Early FW → UEFI → Boot Loader → DRTM

Root of trust for DRTM boot chain

DRTM Chain of Trust

payload

Hypervisor → OS

TPM

launch
DRTM launch can be done on running system

DRTM Chain of Trust

launch

payload

DRTM

Hypervisor

OS

OS

TPM

payload

DRTM

Hypervisor

OS

TPM

payload

DRTM

Hypervisor

OS

TPM

Security Guarantee

Security guarantee
• Trustworthy measurement of payload and critical system state
• Target image begins in a safe state
  • Single thread of execution
  • Interrupts disabled
  • DMA protections in place
• Trustworthy memory map and security ACPI tables available

DRTM Chain of Trust

- payload
- Hypervisor
- OS
- DRTM
- TPM
- Key

DRTM

TPM

Key
Arm Privilege Levels

EL0  Non-Secure  EL1  Guest OS  EL2  Hypervisor/OS-kernel  EL3  Firmware

Secure

Trusted Services

Trusted OS

Secure Partition Mgr
Scope of DRTM on Arm

- The scope of the restarted DRTM chain-of-trust is the non-secure side of the machine.
DRTM on Arm – firmware backed

EL2

DCE Preamble

DLME

runtime

LAUNCH

EL3

DRTM impl.

TPM
DRTM on Arm – hardware backed

- EL2
- DCE Preamble
- LAUNCH
- EL3
- Security co-processor
- TPM
- DLME
- D-CRTM
- DCE
- runtime
DRTM parameters
• Launch features
• DLME addr/size
• DLME image start offset
• DLME entry point offset
• DLME image size
• DLME data offset
• Mem protect table addr/size

LAUNCH SMC call
DRTM support in TF-A
TF-A

- DRTM PoC Branch hosted on trustedfirmware.org [topics/arm-drtm-poc](topics/arm-drtm-poc)
- Based on v2.5 release
- Initial upstream support planned around mid of this year
  - Experimental
  - FVP platform
  - QEMU support depends on interests and support from maintainers
Implementation details

• Firmware backed implementation
• D-CRTM and DCE components are both part of EL3, DCE guarded against build macro to decouple it from EL3 in future
• EL3 makes sure pre-condition to launch DLME is met by ensuring
  • Single PE execution
  • NS Interrupts disabled
  • SMMU v3 driver to abort all NS pending transactions and disable SMMU before launching DLME to achieve complete DMA protection
• DRTM standard services (SMC details on next slide)
• DRTM co-exist with trusted boot
• DRTM parameter parsing support
Contd...

- Crypto support for hash calculation of various DRTM components
- Event Log driver support
  - To record the hash measurements of various DRTM components
  - Attach it to DLME data
- Platform hooks for
  - Retrieve the address map and attach it to DLME data
  - Retrieve base address and number of SMMU to engage DMA protection
  - To read/write DRTM errors to Non-volatile memory
- CI configuration with pre-built DRTM application (DCE preamble + DLME)
## SMC Support

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Support</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>DRTM_VERSION</td>
<td>Version of the DRTM implementation</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>DRTM_FEATURES</td>
<td>To determine the supported DRTM capabilities of the platform</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>DRTM_DYNAMIC_LAUNCH</td>
<td>Initiated DRTM dynamic launch</td>
<td>Partial</td>
<td>1. Measure various image/data components (partial)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. Engage DMA protection (partial)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3. Prepare DLME data (partial)</td>
</tr>
<tr>
<td>DRTM_UNPROTECT_MEMORY</td>
<td>Removes the memory protection put in place by the dynamic launch</td>
<td>Partial</td>
<td>Region based protection is not supported</td>
</tr>
<tr>
<td>DRTM_CLOSE_LOCALITY</td>
<td>Close a locality in the physical TPM.</td>
<td>No</td>
<td>No physical TPM supported</td>
</tr>
<tr>
<td>DRTM_GET_ERROR</td>
<td>Returns error code from the previous DRTM dynamic launch</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>DRTM_SET_ERROR</td>
<td>Set the Dynamic launch error code</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>DRTM_SET_TCB_HASH</td>
<td>Record the hashes of the TCB components</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>DRTM_LOCK_TCB_HASH</td>
<td>Lock the TCB component hashes</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
Limitations in first delivery

- Targeted only for 2 world system
- Assumptions
  - There is no secure payload running which can impact DRTM
  - No request to power on secondary cores
- Complete DMA protection, no region-based protection yet
- Separate event log driver for SRTM(measured boot) and DRTM
- Disabling SDEI events
  - It's responsibility of DCE preamble to make call to disable SDEI events (by using SDEI_PRIVATE_RESET & SDEI_SHARED_RESET)
  - Once it is done, EL3 can check that SDEI events are disabled before launching DLME
Thank You
Danke
Gracias
Grazie
谢谢
ありがとう
ありがとう
Asante
Merci
감사합니다
धन्यवाद
Kiitos
شكرًا
ধন্যবাদ
תודה