DRTM support in TF-A
Dynamic Root of Trust for Measurement (DRTM) begins a new chain of trust by measuring and executing a protected payload.

DRTM is useful in case of number of components in boot-chain grows.

Reduce the attack surface and the risk of executing un-trusted code compromising the security.

No dependency on previous chain of trust
Dynamic Root of Trust for Measurement

SRTM Chain of Trust

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

DRTM Chain of Trust

Launch

payload

Root of trust for DRTM boot chain

DRTM → Hypervisor → OS

TPM
TF-A

- Initial upstream support patches under review [https://review.trustedfirmware.org/q/topic:%22mb%2522Fdrtm-preparatory-patches%22+(status:open%20OR%20status:merged)]
- Currently marked as experimental
- Supported on FVP, QEMU next.
- Steps to reproduce [https://ci-builds.trustedfirmware.org/static-files/kJxWgeIhN9h2ula8nNVPtoqhyGRrgK7bp-oMu4jiMxNiU2NTKzMTA1MDI3Ojk6YW5vbnJt3VzOmpvYi90Zi1hLWJ1aWxkZXIvMTA3ODYzMS9hcnRpZmFjdA==/artefacts/debug/build/html/design_documents/drtm_poc.html]
- CI configuration with pre-built DRTM application
- Platform Porting guidelines
Implementation details

- Firmware backed implementation
- D-CRTM and DCE components are both part of EL3
- 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
- Generate/pass DLME data during its launch
Contd...

• Crypto support for hash calculation of various DRTM components
• Single Event Log driver support for both SRTM(measured boot) and DRTM
• Platform hooks for
  • Retrieve the address map and attach it to DLME data
  • Retrieve base address and number of SMMU to engage DMA protection
  • Ensure no SDEI event registered
  • Retrieve the TPM features
  • DMA protected regions
# 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>Yes</td>
<td></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>
Future work

- Getting feedback from reviewers
- Getting patches merged upstream
- Support for QEMU?
- Helping new platform ports?
- TFTF tests
- Detailed design document
- Threat model
  - Implement missing SMC and Platform hooks
  - Finish off to-do items marked inline
  - Start discussion on moving event log/TPM to FFA complaint secure partition
Thank You
Danke
Gracias
Grazie
谢谢
ありがとう
ありがとう
Asante
Merci
감사합니다
धन्यवाद
 شكرا
धन्यवाद
হাদি