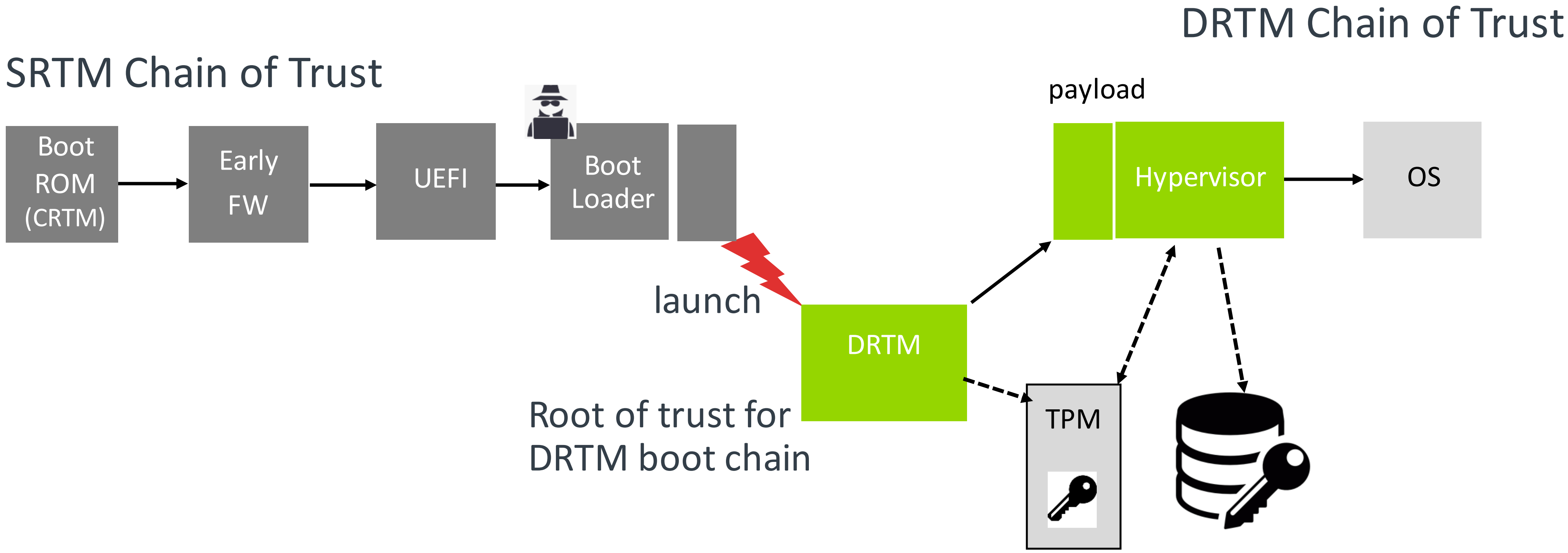
DRTM support in TF-A

30 June 2022

DRTM

- 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



TF-A

- Initial upstream support patches under review https://review.trustedfirmware.org/q/topic:%22mb%252Fdrtm-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/kJxWgelNGSh9h2ulaBnNVPtoqhyGRrgK7bp-oMu4jlMxNjU2NTkzMTA1MDI3Ojk6YW5vbnltb3VzOmpvYi90Zi1hLWJ1aWxkZXIvMTA3ODYzMS9hcnRpZmFjdA==/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

Function	Description	Support	Limitations
DRTM_VERSION	Version of the DRTM implementation	Yes	
DRTM_FEATURES	To determine the supported DRTM capabilities of the platform	Yes	
DRTM_DYNAMIC_LAUNCH	Initiated DRTM dynamic launch	Yes	
DRTM_UNPROTECT_MEMORY	Removes the memory protection put in place by the dynamic launch	Partial	Region based protection is not supported
DRTM_CLOSE_LOCALITY	Close a locality in the physical TPM.	No	No physical TPM supported
DRTM_GET_ERROR	Returns error code from the previous DRTM dynamic launch	Yes	
DRTM_SET_ERROR	Set the Dynamic launch error code	Yes	
DRTM_SET_TCB_HASH	Record the hashes of the TCB components	No	
DRTM_LOCK_TCB_HASH	Lock the TCB component hashes	No	

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

Asante

Merci

감사합니다

धन्यवाद

Kiitos

شكرًا

ধন্যবাদ

תודה