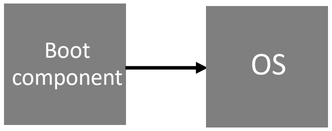
Linux & DRTM on Arm

September 2021

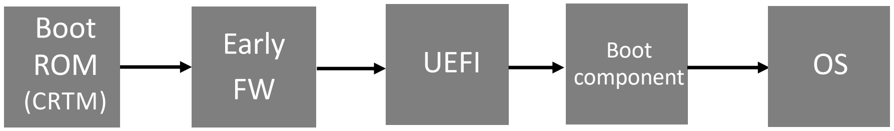
Agenda

- DRTM on Arm Overview
- Handoff from DRTM launch to Linux
- UEFI Runtime Services
- Interface from kernel TPM driver to TPM

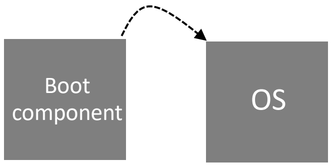
DRTM (Dynamic Root of Trust for Measurement)



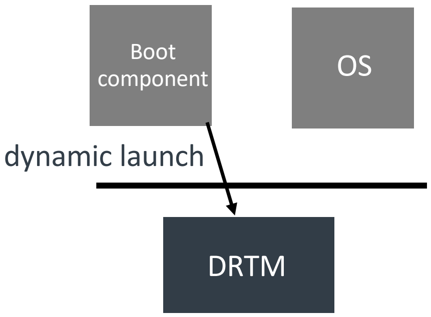
DRTM (Dynamic Root of Trust for Measurement)



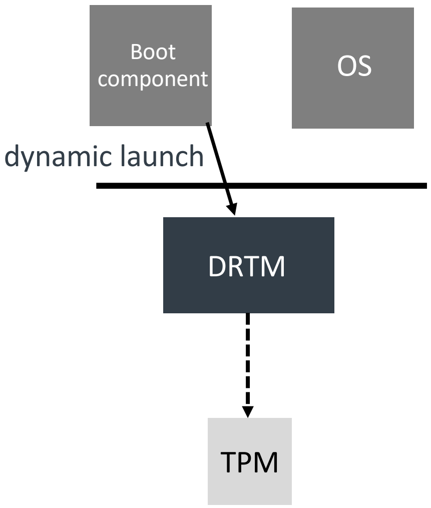
DRTM (Dynamic Root of Trust for Measurement)



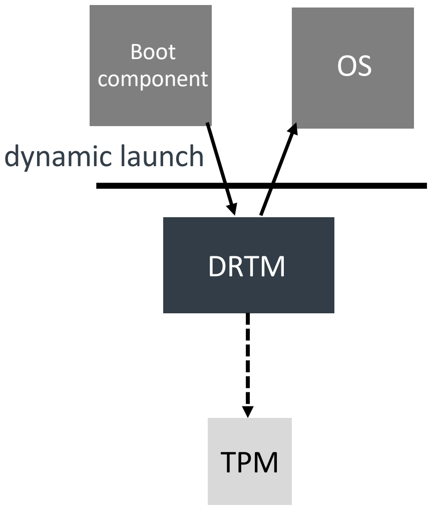
DRTM (Dynamic Root of Trust for Measurement)



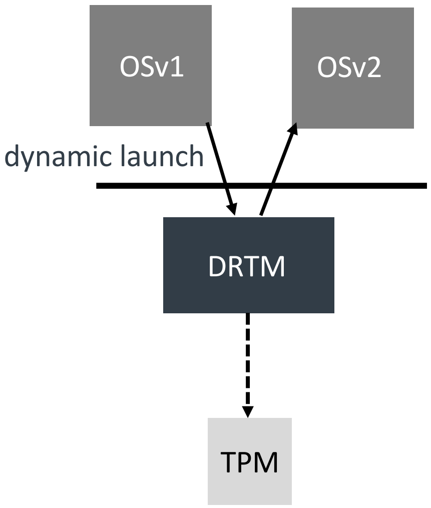
DRTM (Dynamic Root of Trust for Measurement)



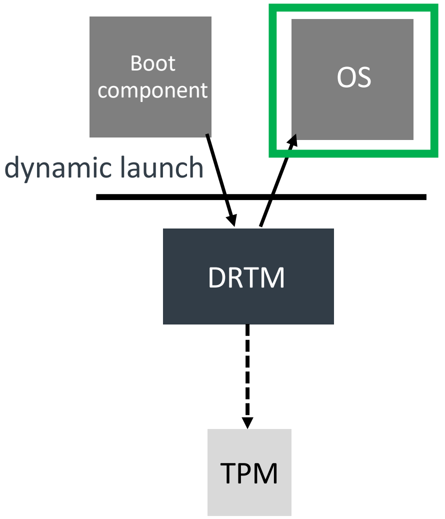
DRTM (Dynamic Root of Trust for Measurement)



DRTM (Dynamic Root of Trust for Measurement)



DRTM (Dynamic Root of Trust for Measurement)

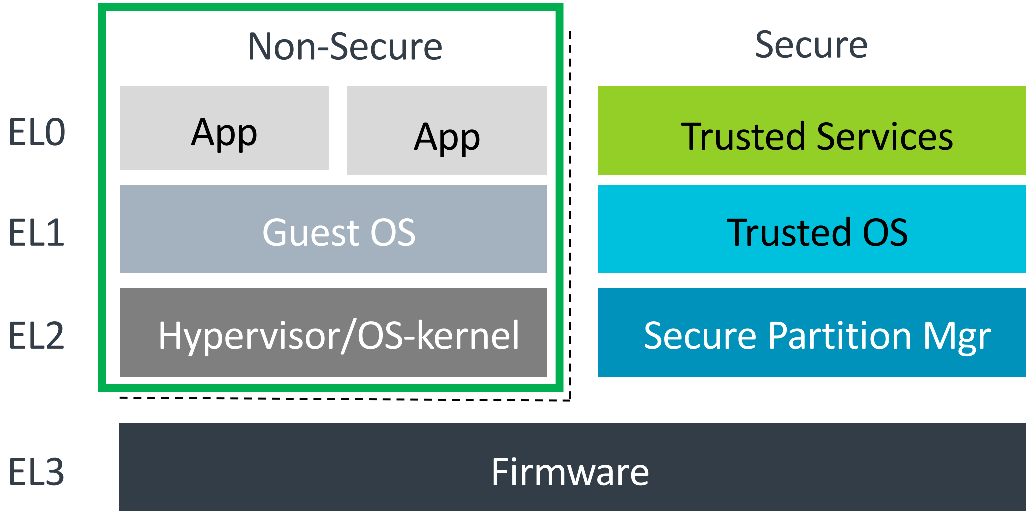


Security guarantee

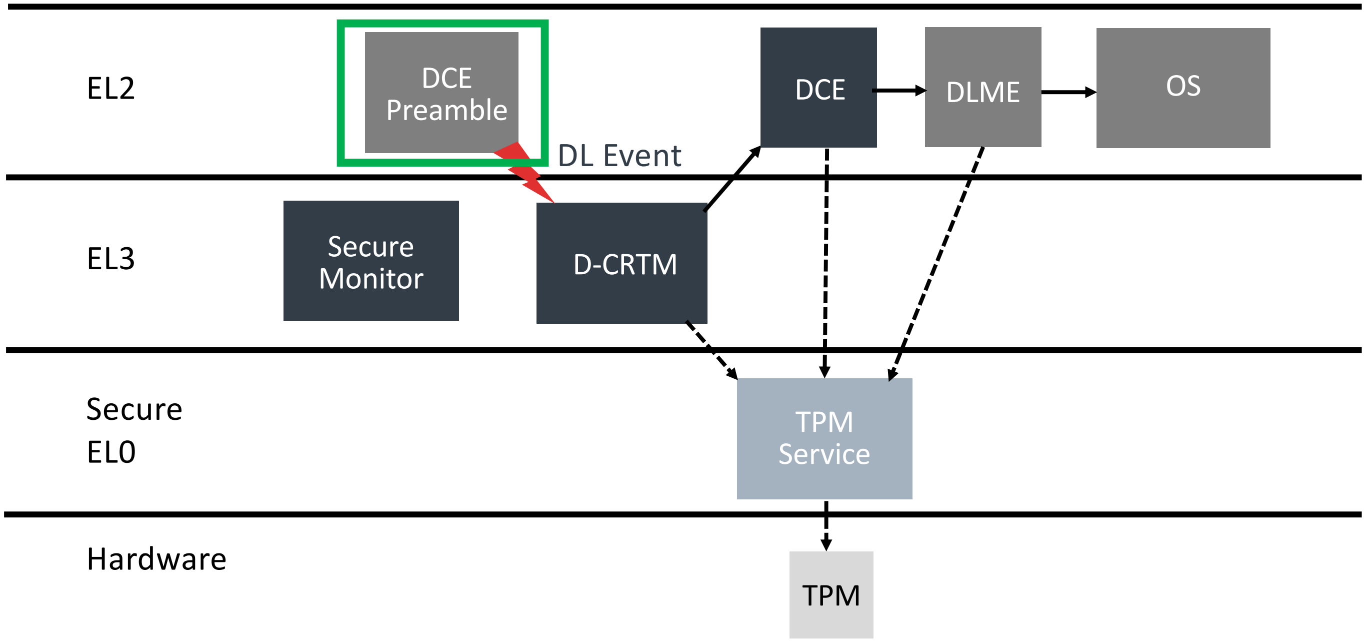
- Trustworthy measurement of target image
- Target image begins in a safe state
  - Single thread of execution
  - Interrupts disabled
  - DMA protections in place
  - Trustworthy memory map and security ACPI tables available

Scope of DRTM on Arm

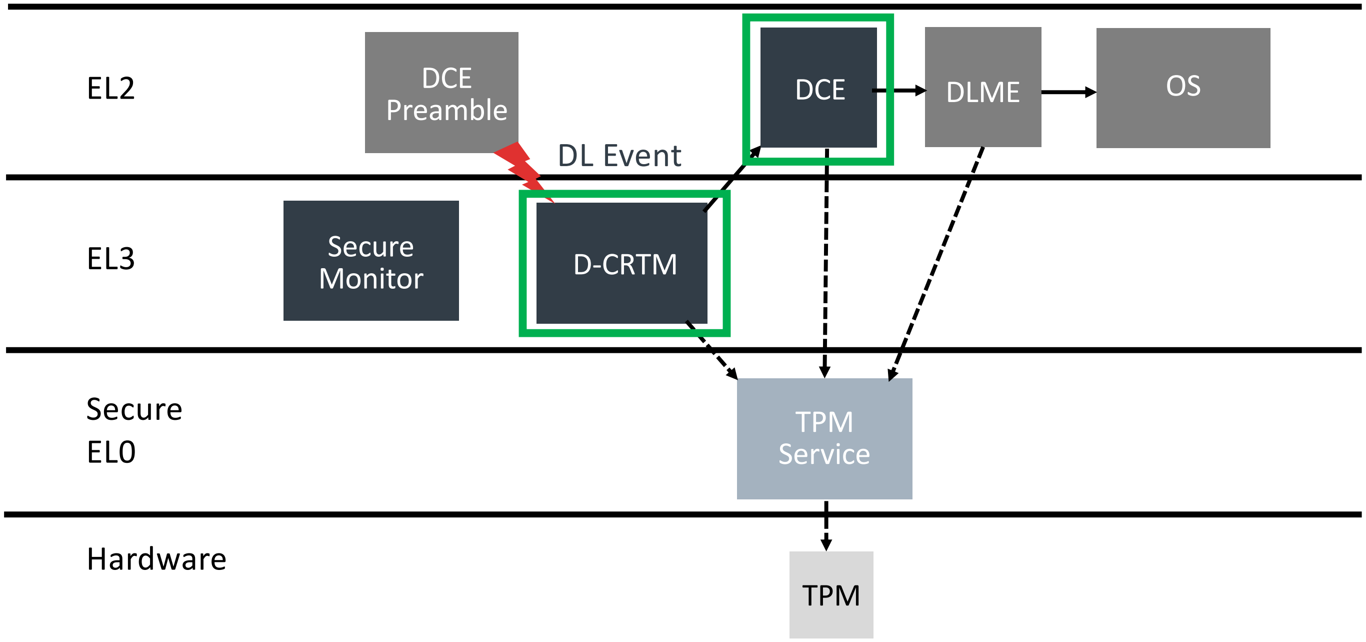
- The scope of the restarted DRTM chain-of-trust is the non-secure side of the machine



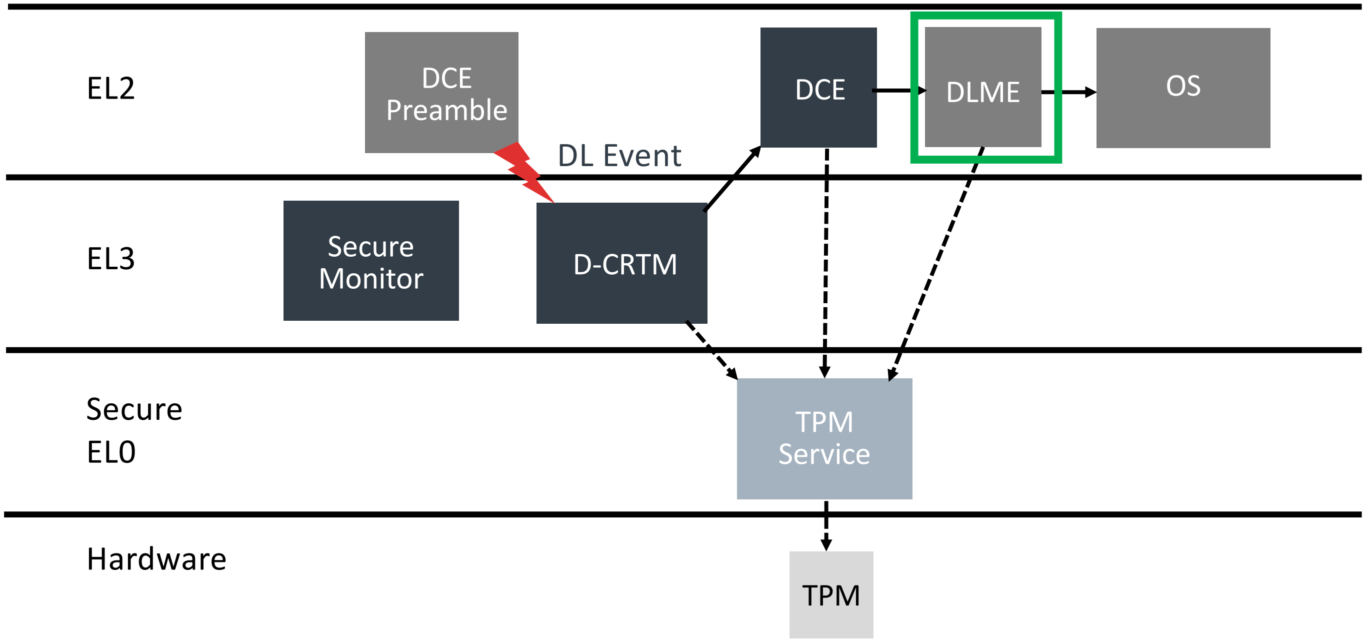
DRTM on Arm (firmware based)



DRTM on Arm (firmware based)

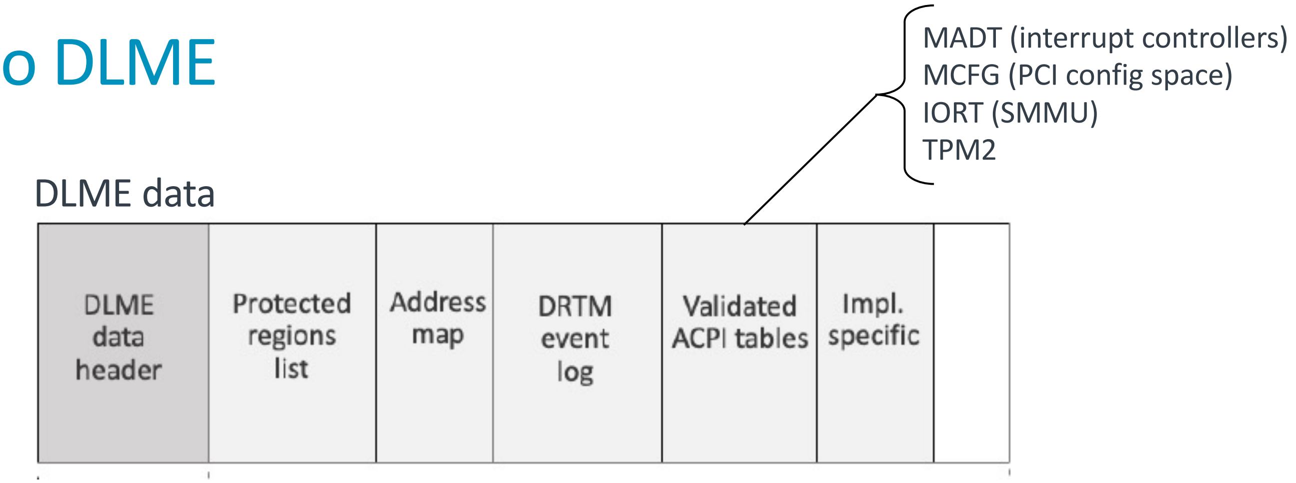


DRTM on Arm (firmware based)



arm

Handoff to DLME



DLME data

DLME data header	Protected regions list	Address map	DRTM event log	Validated ACPI tables	Impl. specific	

MADT (interrupt controllers)
MCFG (PCI config space)
IORT (SMMU)
TPM2

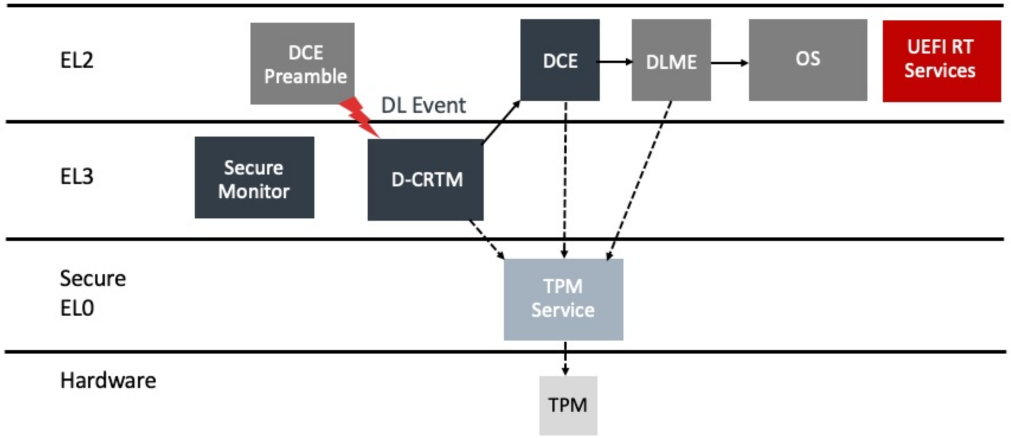
For security critical data, DRTM provides validated tables to allow the DLME to defend itself.

What data does Linux/TrenchBoot need?

Anything missing?

UEFI RT Services

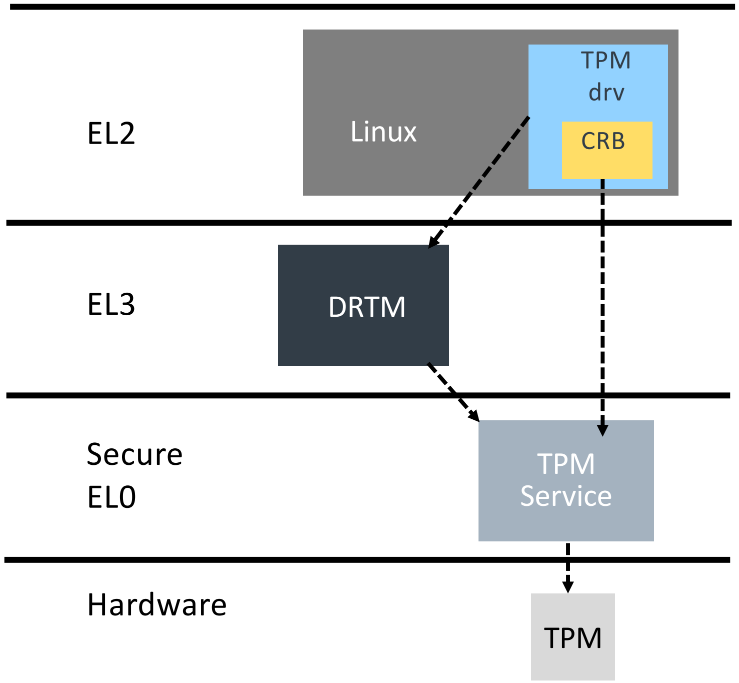
“EFI runtime services are driving a hole as big as barn through DRTM.”



This is an issue that is not architecture specific.

Does ACPI PRM (Platform Runtime Mechanism) help?

Interface from kernel TPM driver to TPM



- Command Respons Buffer is in normal memory. Definition in TCG Mobile CRB spec. Needs to be extended to encompass localities.
- Allocation of CRB buffer-- Is there an issue with the kernel driver allocating the buffer and registering with TPM service?