Contribution ID: **279** Type: **not specified**

Linux and DRTM on Arm

Wednesday, September 22, 2021 8:30 AM (30 minutes)

A specification for Dynamic Root of Trust for Measurement (DRTM) on the Arm architecture will be available Fall 2021. DRTM allows a system in a potentially unknown or untrusted state to boot an OS or hypervisor into a known and trusted state.

This topic will present an overview of DRTM on Arm to provide context, followed by discussion around several topics that have implications for the Linux kernel:

- questions around the handoff from the dynamic launch to the Linux kernel
- the problem of UEFI RT services in the context of DRTM and Linux
- questions around supporting dynamic TPM localities on Arm systems

I agree to abide by the anti-harassment policy

I agree

Primary author: YODER, Stuart (Arm)

Presenter: YODER, Stuart (Arm)

Session Classification: System Boot and Security MC

Track Classification: System Boot and Security MC