Trusted Substrate

Ilias Apalodimas

Aug 09, 2023

CONTENTS

Note: Trusted Substrate is part of Linaro Trusted Reference Stack. The full documentation has moved here

Trusted Substrate is a meta-layer in OpenEmbedded aimed towards board makers who want to produce an Arm System-Ready compliant firmware and ensure a consistent behavior, tamper protection and common features across platforms. In a nutshell TrustedSubstrate is building firmware for devices which verifies the running software hasn't been tampered with. It does so by utilizing a well known set of standards.

- **UEFI secure boot enabled by default**

  UEFI Secure Boot is a verification mechanism for ensuring that code launched by a computer's UEFI firmware is trusted. It is designed to protect a system against malicious code being loaded and executed early in the boot process, before the operating system has been loaded.

- **Measured boot. With a discrete or firmware TPM**

  Measured Boot is a method where each of the software layers in the boot sequence of the device , measures the next layer in the execution order, and extends the value in a designated TPM PCR. Measured boot further validates the boot process beyond Secure Boot.

- **Dual banked firmware updates with rollback and bricking protection**

  Dual banked firmware updates provides protection to the firmware update mechanism and shield the device against bricking as well as rollback attacks.