Contribution ID: **143**

Type: **not specified**

A Ridiculously Short Intro into Device Attestation

Thursday 27 August 2020 09:35 (20 minutes)

A Ridiculously Short Intro into Device Attestation

Dimitar Tomov, Design First, ES
Ian Oliver, Nokia Bell Labs, FI

Very practical look at how to use a TPM and perform device attestation. A system can have trusted qualities instead of being 100% trusted. Cross-referencing different types of attestation data can provide evidence for trusted qualities. The decision of whether a device is trusted is not responsibility of the attestor and verifier - these just gather and check the evidence. Example use cases of Time Attestation.

Intro

Use of Trusted Platform Modules (TPM), Measured Boot and [Remote] Attestation can provide significant security benefits to, arguably, the most sensitive and critical parts of a system, particularly the firmware and initial boot. However, the verification of attestation claims can be daunting and complex.

In this presentation, we briefly describe what measurements are and can be take, how these are reported by a TPM. What the TPM attest structures contain and how this information can be better understood in terms of device identity, configuration parameters, temporal aspects etc.

We conclude with a short demonstration(example as presentation platform allows) of attestation of trustable devices (servers, IoT, etc) focussing on certain temporal and device identity aspects.

I agree to abide by the anti-harassment policy

I agree

Primary authors: Mr TOMOV, Dimitar (DesignFirst); Mr OLIVER, Ian (Nokia Bell Labs)

Presenters: Mr TOMOV, Dimitar (DesignFirst); Mr OLIVER, Ian (Nokia Bell Labs)

Session Classification: System Boot and Security MC

Track Classification: System Boot and Security MC