Linux Plumbers Conference 2022

Contribution ID: **104** Type: **not specified**

Remote Attestation of IoT devices using a discrete TPM 2.0

Monday, 12 September 2022 12:20 (35 minutes)

There are billions of networked IoT devices and most of them are vulnerable to remote attacks. We are developing a remote attestation solution for IoT devices based on Arm called EnactTrust. The project started with PoC for a car manufacturer in 2021.

Today, we have an open-source agent at GitHub[1] that performs attestation. The EnactTrust agent leverages a discrete TPM 2.0 module and has some unique IoT features like attestation of the TPM's GPIO for safety-critical embedded systems.

Currently, we are working on integrating our open-source agent with Arm's open-source Trusted Firmware implementation. We are targeting both TF-A and TF-M.

Our goal is to demonstrate bootloader attestation using EnactTrust. Bootloader candidates are TrenchBoot, Tboot, and U-Boot. Especially interesting is the case of U-Boot since it does not have the same level of security capabilities as TrenchBoot and Tboot.

EnactTrust consists of an agent application (running on the device) and a connection to a private or public cloud[2]. We believe that the security of ARM-based IoT devices can be greatly improved using attestation.

[1] https://github.com/EnactTrust/enact
[2] https://a3s.enacttrust.com

I agree to abide by the anti-harassment policy

Yes

Primary authors: Mr TOMOV, Dimitar (TPM.dev); Mr KALCHEV, Svetlozar (EnactTrust)

Presenters: Mr TOMOV, Dimitar (TPM.dev); Mr KALCHEV, Svetlozar (EnactTrust)

Session Classification: System Boot and Security MC

Track Classification: LPC Microconference: System Boot and Security MC