Dokumenttyp: Konferenzbeitrag

Autor(en) des Beitrags: Hristozov, Stefan and Heyszl, Johann and Wagner, Steffen and Sigl, Georg

Titel des Beitrags: Practical Runtime Attestation for Tiny IoT Devices

Abstract: One of the main challenges in IoT security is to assure the integrity of the firmware running on a constrained low-cost device. A solution to this challenge could be provided by a security service called attestation, where the device generates an evidence about its firmware which is attested by a remote verifier. How attestation evidence can be generated at boot time on a tiny microcontroller was investigated in earlier work and also specified by the TCG’s DICE specification. It is, however, challenging to generate such attestation evidence during runtime, where the device usually is prone to powerful attacks. Previous contributions have attempted to solve this by using custom hardware extensions of the CPU architecture. We, however, present a method based on DICE to securely generate attestation evidence at runtime using only standard CPU features like MPU, privileged/unprivileged levels of execution and the required by DICE boot ROM and lock mechanism. Precisely, we use the MPU and privilege levels to effectively isolate the attestation firmware and secrets from the remaining application. As a result, our method can immediately be applied to a broad range of popular
we provide a proof of concept implementation for the Cortex-M4-based STM32L476 microcontroller.

Stichworte:
IoT

Dewey Dezimalklassifikation (Liste):
620 Ingenieurwissenschaften

Kongress- / Buchtitel:
NDSS Workshop on Decentralized IoT Security and Standards (DISS) 2018, San Diego, CA, USA

Kongress / Zusatzinformationen:
San Diego, CA, USA

Jahr:
2018

Quartal:
1. Quartal

Jahr / Monat:
2018-02

Monat:
Feb

Print-ISBN:
1-891562-51-7

Volltext / DOI:
http://doi.org/10.14722/diss.2018.23011

WWW:
https://www.ndss-symposium.org/ndss2018/

CC-Lizenz:
by, http://creativecommons.org/licenses/by/4.0

Occurences:
- Einrichtungen > Fakultäten > Fakultät für Elektrotechnik und Informationstechnik > Lehrstühle und Professuren > Sicherheit in der Informationstechnik (Prof. Sigl) > 2018

entries: