Security Partner

MIXED MODE

Partner Use Case

Secured boot for ARM processor platforms

Securely boot an ARM processor platform into a trusted state with Infineon's OPTIGA™ TPM

Products

OPTIGA™ TPM

Security Partner

Use case

Application context and security requirement

Due to the wide and ever-growing application of embedded systems in security critical areas like automotive and industrial markets, the protection of such systems' integrity and a reliable mode of operation is paramount. But how can we verify a correct system state and supply a reliable chain of trust for this task?

Challenge

Embedded systems must provide a reliable mode of operation and protect the integrity of the system, thus verifying a correct and trusted system state. Unfortunately, with such systems a wide range of potential blind spots exist. To achieve a trusted system state a secure boot mechanism can be implemented. However, this requires an entity which offers secured storage and the reporting of security relevant metrics. All these assets have to be accessible at boot time - securely storing and verifying all relevant platform metrics and thus forming the root for a chain of trust.

Implementation

In order to achieve a root of trust and further benefit from secured storage and reporting of security related platform metrics, a dedicated Trusted Platform Module (TPM) was incorporated into the ARM processor platform. Infineon's OPTIGA™ TPM, compliant with TPM 1.2 Rev. 116, is capable of operating as a root of trust and fulfilling our task's requirements.

To achieve this, the bootloader was enhanced to securely store and verify relevant system metrics directly on the TPM with the chip's platform configuration registers (PCR). These PCRs include platform metrics like boot configurations and state transitions, and are further extended by hashes of environment variables, console input and the kernel image. The following verification only succeeds if these extended PCRs conform with the trusted PCR values, thus certifying the platform's integrity and a correct system state.

User benefits

- Easy integration of a root of trust by incorporating a dedicated OPTIGA™ TPM chip which provides all functionalities to perform a secured boot process.
- Secured boot process based on the verification of security relevant metrics, configurations and the kernel image.
- Provides Certificate Signing Requests using Simple Certificate Enrollment Protocol (SCEP), Enrollment over Secured Transport (EST), and Online Certificate Status Protocol (OCSP)
- Full integration with public and private Certificate Authorities

The boot verification is not restricted to environment variables or a kernel image. Virtually every component of a platform can easily be integrated into the PCRs and further serve as indicator for a trusted system state.

Security Partner

Solution

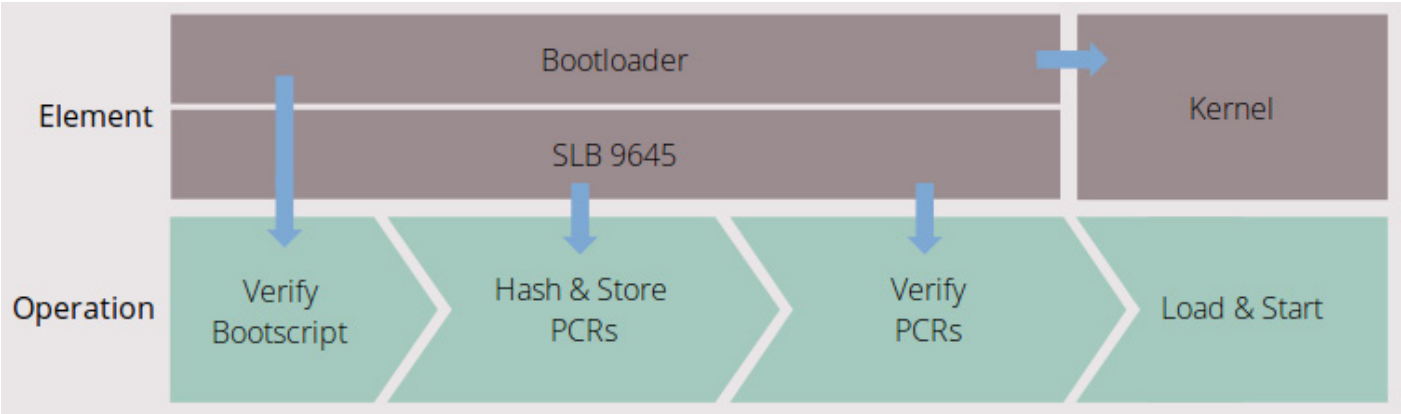
As embedded systems are often deeply integrated in complex systems, an important goal of the solution was to incorporate the required modifications in a minimal and flexible manner. As a result, the addition of a TPM chip on the ARM processor platform was the most straightforward approach to enable secured boot.

Mixed Mode GmbH analyzed the requirements for this approach and developed a solution for the task of securely booting an ARM processor platform. Different attack vectors, as well as securing the integrity of different parts of the system like environment variables and the kernel image had to be taken into account. The OPTIGA™ TPM was incorporated into the embedded system, featuring secured storage and cryptographic functionalities, as well as the reporting of security relevant metrics. All TPM related operations like storing and extending the PCRs, as well as verifying their values, are performed directly on the TPM. The enhancement of the bootloader and the adaption of the TPM chip to the Linux kernel and device tree, as well as the associated implementations have been performed by Mixed Mode GmbH.

This solution enables a chain of trust by observing a platform's boot process and provides extensive protection of a platform's integrity, as well as safeguarding against a wide range of attacks such as fault attacks or a tampered kernel. Simultaneously, the incorporation of the TPM chip and the enhancement of the bootloader and the Linux kernel requires minimal modifications and offers high compatibility to existing systems.

Main benefits of the Infineon product

The Infineon OPTIGA™ TPM is a compliant chip which incorporates the secured storage of security relevant platform metrics and additional system parameters. In combination with the verification of these parameters, the OPTIGA™ TPM forms the root of the secured boot operation in order to enable and check a trusted system state.



Security Partner

Partner

Partners from the Infineon Security Partner Network help you secure your devices and applications: understand which threats can undermine your business, propose solutions that will protect your business, build and implement such security solutions and, when relevant manage their operation. They have been selected by Infineon on the basis of their system security competence and ability to design and deliver strong and trustworthy security solutions. Their activities are diverse and include security consulting, security solution provision, electronic design, systems integration and trust services management. For some, offers are off-the-shelf; while for others, offers are custom-built.

Mixed Mode GmbH

Mixed Mode GmbH is a SME, founded in 1994 in Gräfelfing near Munich, where it is still located to this day. It has about 85 employees in Research and Development. Mixed Mode is a part of the PIXEL group which provides their customers with IT & Embedded Engineering & Consulting services and achieved a turnover of 11M€ in 2016.

Mixed Mode is specialized in consulting and developing embedded systems solutions, and has amassed its competence in a number of ambitious projects in a range of sectors including industrial, automotive & transport, telecommunication, aerospace, semiconductor and medical. Its fields of activity consist of the whole systems engineering workflow starting from requirements analyses, up to and including integration in the customer's environment, for both hard- and software. Mixed Mode's workflows are ISO 9001 certificated, ensuring comprehensive quality management in each project phase.

Mixed Mode GmbH contribution to the Infineon Security Partner Network

Mixed Mode offers expertise in the following fields:

› Embedded Security › Test & Quality › Internet of Things › Professional User Interfaces › Embedded Linux

With about 15 years of experience in projects within security applications, Mixed Mode has worked on the development of cash handling solutions, point-of-sales terminals and security tools, the validation of cryptographic algorithms and have consulted on security software development.

Mixed Mode has been active in security research projects for the last ten years, both as a member of the project-consortia and as a subcontractor for Infineon (e.g. TPM & SLE-Chipcard applications).

Mixed Mode operates in the following industries – Industrial, Automotive & Transport, Telecommunication, Aerospace, Semiconductor, Medical, Energy & Facility Systems – and provides "Time & Material" and "working package" oriented project support as well as supporting customer projects in Embedded & Software Engineering and Consulting (for trainings offerings see Mixed Mode's "Expert Session" Catalogue).

Mixed Mode has experience implementing the following Infineon products into security projects: SLI 97, SLE 97, AURIX™ 1st Generation HSM, OPTIGA™ TPM 1.2, OPTIGA™ TPM 2.0.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 05 / 2017

Additional information

For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices please contact your nearest Infineon Technologies office (www.infineon.com).

Please note!

THIS DOCUMENT IS FOR INFORMATION PURPOSES ONLY AND ANY INFORMATION GIVEN HEREIN SHALL IN NO EVENT BE REGARDED AS A WARRANTY, GUARANTEE OR DESCRIPTION OF ANY FUNCTIONALITY, CONDITIONS AND/OR QUALITY OF OUR PRODUCTS OR ANY SUITABILITY FOR A PARTICULAR PURPOSE. WITH REGARD TO THE TECHNICAL SPECIFICATIONS OF OUR PRODUCTS, WE KINDLY ASK YOU TO REFER TO THE RELEVANT PRODUCT DATA SHEETS PROVIDED BY US. OUR CUSTOMERS AND THEIR TECHNICAL DEPARTMENTS ARE REQUIRED TO EVALUATE THE SUITABILITY OF OUR PRODUCTS FOR THE INTENDED APPLICATION.

WE RESERVE THE RIGHT TO CHANGE THIS DOCUMENT AND/OR THE INFORMATION GIVEN HEREIN AT ANY TIME.

Warnings

Due to technical requirements, our products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life endangering applications, including but not limited to medical, nuclear, military, life critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.