Security Partner

Partner Use Case

Secure remote firmware updates and ECU integrity protection

Fraunhofer SIT

Protecting Remote Firmware Updates and system data protection in control units using the latest TPM 2.0 technology.

Product

OPTIGA™ TPM

Fraunhofer SIT

Infineon Security Partner

Use case

Application context and security requirement

Automotive Electronic Control Units (ECUs) and other embedded or IoT devices store high amounts of security-critical data on the devices' flash storage. For example modern automotive ECUs, such as the head unit, central gateway and telematic units, store vehicle data, user data or remote firmware updates which will be deployed to other ECUs in the vehicle. In this use case the security-critical data and the firmware update process are protected against a variety of threats with the latest OPTIGA™ TPM 2.0 technology, modern cryptographic algorithms and verification of the platform integrity of the ECU.

Challenge

The automotive industry and other embedded or IoT markets face more and more intense threats on devices and the security-critical data in these devices. The visibility of such attacks is magnified through press and public articles. The security of such devices can be significantly increased through the use of the OPTIGA™ TPM 2.0 for the data encryption in the device as well as the protection of the system integrity during the boot process. The TPM is used as a trust anchor which stores critical data such as cryptographic keys for data protection and verification values for the firmware update process. Many challenges in the firmware update process are addressed in the use case, enabling security mechanisms to verify the current firmware and provide a protected transition to a new regular firmware in the update process. This protects against malicious firmware updates which may be inserted by an attacker. There is also a protection against a downgrade attack, so that an attacker can't use the firmware update process to replace the current firmware with an outdated firmware image.

Implementation

Fraunhofer SIT has been collaborating in the Trusted Computing Group (TCG) for more than eight years and became one of the first providers of a TPM 2.0 software stack for the OPTIGA™ TPM. This knowledge and software was applied in the use case of an infotainment system; which was presented with a demonstrator on the Cebit 2016 and Embedded World 2016. This demonstration integrates the essential security concept and shows the implementation of the latest TPM 2.0 functionalities on a typical infotainment system. When the owner of the infotainment ECU chooses a firmware release the TPM protects the update process and validates the firmware in the boot process of the device. The technology is already in line to be licensed for two industrial applications and the researchers are en route to a finished automotive product.

User benefits

› Ready to use application of TPM 2.0 for data protection in the device and the firmware update process
› Innovative security mechanism for the firmware update process using device integrity to protect against malicious updates
› Availble source code and demonstration for a currently available infotainment system

Fraunhofer SIT

Infineon Security Partner

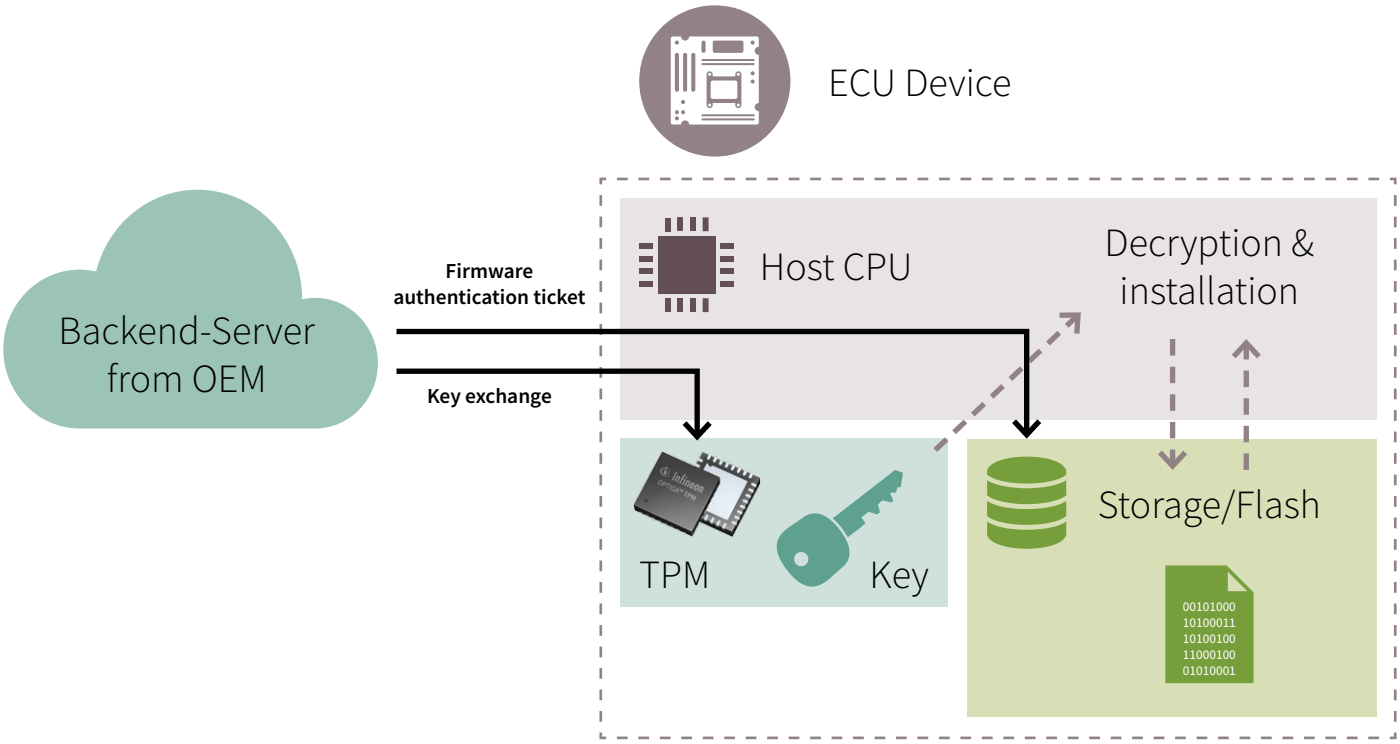
Solution

This solution is implemented as a prototypical extension to a typical In-Vehicle Infotainment (IVI) head unit operating system without interfering with its original functionalities. The solution can easily be adapted to other In-Vehicle Infotainment systems. It extends the IVI by encrypting the device data with a cryptographic process so that the data is protected against threats. The key for the encryption is stored inside the Infineon OPTIGA™ TPM 2.0 using the Fraunhofer SIT TPM Software Stack 2.0 (SIT-TSS2), which protects the key from malicious use and cloning.

Furthermore, a boot protection mechanism is integrated which verifies the current firmware in the device. If the verification is successful, the boot process continues and makes protected data available to the infotainment system.

Given the increasing interconnectivity of modern automotive systems and the large number of security weaknesses detected in recent years, automotive ECU security needs to be reconsidered. This includes specifically the protection of Original Equipment Manufacturers (OEMs) and user data and the update of ECU firmware in a timely and frequent manner. The proof of concept solution for local data protection was implemented using the available Fraunhofer SIT-TSS2 and a typical IVI system with a built-in Infineon OPTIGA™ TPM 2.0. This demonstrates the feasibility of such optimized security solutions based on off-the-shelf solutions that fulfill the security needs of the future.

Since this solution is based on features of typical Linux distributions, the software and the security concept with the TPM 2.0 can be adapted easily to other systems such as industrial control devices or any other IoT device.



Main benefits of the Infineon product

The Infineon OPTIGA™ TPM 2.0 acts as a secure environment for storing keys inside the chip. The advantage is the high level of security with the TCG certification and the functional compliance to the TCG specification. This enables seamless integration and application of the OPTIGATM TPM in to the scenario.

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.

Fraunhofer SIT

The Fraunhofer Institute for Secure Information Technology SIT is the leading expert for IT Security and privacy protection and develops solutions for immediate use, tailored to the customer's needs. The institute deals with the central security challenges in industry, administration and society. Over 180 highly qualified employees covering all areas of IT security work on current topics and challenges of cyber security research.

Fraunhofer SIT supports its partners in the conception of new IT systems, in the protection of existing IT infrastructures and in the development of new prducts and services. Furthermore the institute gives advise in important IT security questions and is involved in national and internatioal standardization.

Fraunhofer SIT is a driving force in the international IT security area and is part of the Centers for Research in Security and Privacy (CRISP) in Darmstadt, the biggest research center for cyber security in Germany.

Fraunhofer SIT's contribution to the Infineon Security Partner Network

Fraunhofer SIT has a long-standing history in standardization and application of Trusted Computing technologies. This includes the design of innovative solutions for identity, integrity and data protection incorporating the Infineon OPTIGA™ TPM.

The focus lies on the collaboration with partners to leverage the advanced security features of TPMs in their products to their full potential. These security solutions may be targeted at any application domain including but not limited to automotive, industrial control systems and critical infrastructures.

With all its expertise in the field of Trusted Computing technologies Fraunhofer SIT offers consultancy, licensing and development support for TPM based applications as well as an implementation of a TPM Software Stack 2.0.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 10 / 2016

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.