Security Partner

insight

Partner Use Case

Server side management system for multiple IoT terminals in industrial systems

This system utilizes the technology of the Trusted Computing Group (TCG) as a time-to-market solution based on open standards to flexibly adopt multiple Internet of Things (IoT) devices into a system. The demonstration is showcased at TCG Japan Regional Forum office.

Products

OPTIGA™ TPM

Security Partner

Use case

Application context and security requirement

In industrial systems, multiple devices from multiple vendors are managed under the same network environment. Insight's server side management system for multiple IoT terminals in industrial systems, utilizing the technology of the Trusted Computing Group (TCG) such as TPM 2.0 (Trusted Platform Module), in-house TPM Software Stack (TSS - TPM 2.0 Library), measurement based secured boot, and Opal, is provided to customers as a turn-key solution to realize time-to-market based on open standards to flexibly adopt multiple IoT devices into the system.

Challenge

Once this industrial system is connected to an external network (internet), the network is exposed to threats from all over the world, providing security for the overall network and enabling management of all devices is essential to protecting the system from such threats.

Implementation

This system uses a server to verify the integrity of the endpoint so that the endpoint can use it securely. The endpoint won't run the required application unless server verification is complete. The server performs its own integrity verification. Opal drive can be used to help protect data in the case of disk theft.

Benefits for the user:

Users can use the following mechanisms

› Endpoints can be used securely at any time
› Confirm the health state of the endpoint by looking at the status LED
› Check the security of the server itself, and protect files from theft of the disk

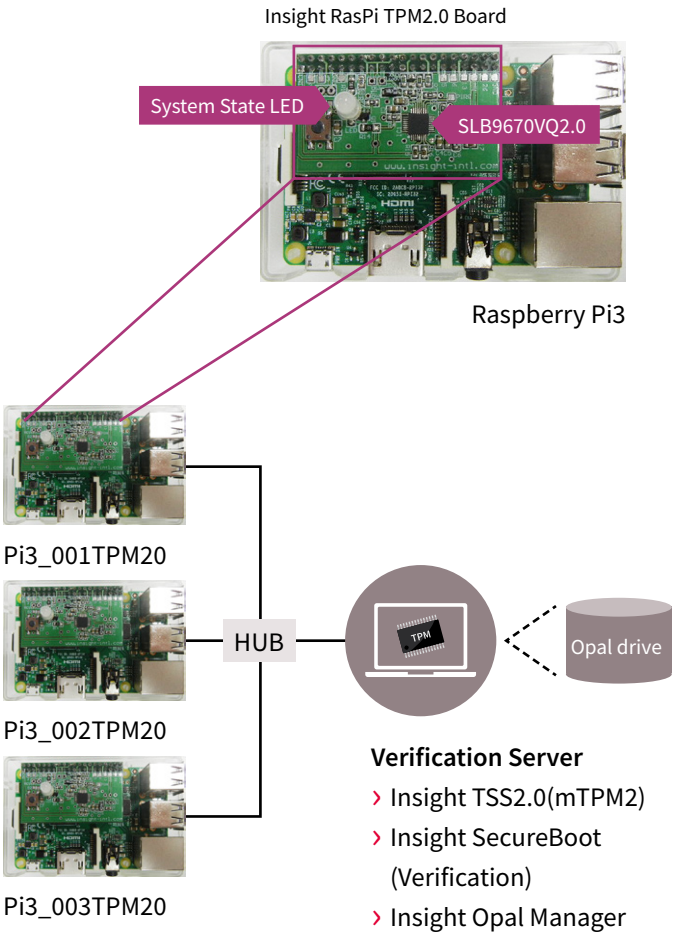
Infineon Security Partner

Solution

This system can perform cryptographic functionality in the secured environment by using the Trusted Computing Group's Root of Trust technology. Functional requirements require TCG compliant TPM 2.0, Opal drives, and the software to operate them.

In this system, Infineon's OPTIGA™ TPM SLB 9670 (TPM version 2.0) plays a very important security role. Millions of PCs and embedded devices around the world are protected from a vast variety of cyber security threats with the OPTIGA™ TPM.

2017 TCG JRF TPM2.0 Demo System



Insight RasPi TPM2.0 Board

- Supports Raspberry Pi2 and Pi3
- Working on Linux
- Insight TSS2.0(mTPM2)
- Insight SecureBoot(based on Hash)

Verification Server

- Insight TSS2.0(mTPM2)
- Insight SecureBoot (Verification)
- Insight Opal Manager

1. Boot up each Raspberry Pi3
2. Start Hash measurement with Insight SecureBoot
3. Verify PCR values(SLB9670) with White list on Server using Insight SecureBoot verification
4. If matching, then indicate with GREEN LED on Pi3, If not matching then indicate with RED blinking on Pi3. Also if data is tampered with, start Recovery Engine by Insight SecureBoot, then recover "Correct Files" from Opal drive
5. After the Pi3 boot has completed successfully, start Enc/Dec and sign with the TPM using Insight TSS2.0(mTPM2)

Security Partner

Solution

Features of Infineon's OPTIGA™ TPM SLB 9670 2.0

› TCG, EAL, FIPS 140-2 and many certifications already acquired
› Storing measured values of files when the endpoint boots up
› Encryption / decryption, Random number generation, all with the latest cryptographic engines.

The software features a measurement-based secured boot, TPM 2.0 library and Opal Manager provided by Insight.

Features of Insight TPM 2.0 Library

› HMAC calculation function installed
› Supports session (decryption, encryption, auditing) functionality
› Extensive combination tests have been conducted

In addition, Insight offers TAW (TPM Access Wrapper) which is designed for ease-of-use development of TPM application utilizing encryption / decryption and key duplication.

Mechanism

The mechanism of this operation is achieved by using secured boot software to measure the endpoint file with a hash (SHA 256) when the endpoint is booted up. The measurement result is stored in the Infineon OPTIGA™ TPM. The stored value is compared and verified with the whitelist in the server, and if there is no problem the endpoint performs normal operation. At the same time, you can check the health status of the endpoint by looking at the status LED. As for the safety of the server, the server itself also performs a measurement-based secured boot. The server has a TCG Opal drive which is installed to provide protection against the theft of the disk and also the file can be encrypted and protected. The Opal uses the range area which is a security function to store the file and to prevent file theft from the network.

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.

Insight

Insight International is developing TCG (Trusted Computing Group) related software for Trusted Platform Modules (TPM). They offer a TCG Software Stack for TPM 1.2 & 2.0 and secured boot software based on measurement and Opal Management software. Insight has over 10 years of experience serving the TPM demands of the markets. Insight is also focusing on the embedded market for MFPs (Multi-Function Printer), POS (Point of Sales), Network terminals, and many more applications.

Insight works closely with leaders in the industry to provide high performance software that our customers can use to make their products more affordable and to be able to support the latest industry standards.

In 1984 the company opened its headquarters in Tokyo, Japan. In 2009, Insight International shipped its first Insight TSS for TPM1.2 to a MFP vendor. In 2017 Insight International released and shipped Insight TSS for TPM2.0, and Insight has plans to soon supply worldwide customers.

Insight's contribution to the Infineon Security Partner Network

Insight International offers design house services to their customers, and has the capabilities to offer solutions and consultations on their product security needs. Insight has developed a server side management system for IoT terminals in industrial systems and provides this to customers as a turn-key solution to realize time-to-market based on open standards. With this customers can flexibly adopt multiple IoT devices into the system by working with other cutting edge partners.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 07 / 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.