Security Partner Preferred

Partner Use Case

TPM 2.0 Protected IIoT Security Gateway for Industrial Control Systems

Lanner

To secure millions of Industrial Internet of Things (IIoT) endpoints, controllers and gateways in complex environments, a comprehensive IIoT edge security platform should be equipped with hardware root of trust on each device, gateway and controller, with a mutual authentication between device and gateway as well as with a secured communication overlays design.

Products

OPTIGA™ TPM

Use case

Application context and security requirements

Secured, mutual authentication—where two entities (device and service) must prove their identity to each other in order to build up trust and help to protect against malicious attacks. As a critical position in Operational Technology (OT) network topology, it is required to build a security gateway empowered with a set of encrypted platform identities, which is unique for every shipped device. The identity of the security gateway is not allowed to be modified permanently.

Several issues have been addressed towards current unsecure IIoT adoption that includes:

› Insecure interface
› Insufficient authentication/authorization
› Lack of transport encryption/integrity verification

Implementation

Encrypted Platform Identity API

To allow the authentication process being executed, Lanner Electronics provides a set of easy-to-use Application Programming Interfaces (APIs) to enable application developers to secure the communication and protect every piece of code implemented on the computing space.

With the newly launched TPM 2.0 architecture, a better secured hardware level of trust is given. In Lanner IIoT Security Gateway, you can also find TPM Software Stack 2.0 (TSS 2.0) compliant APIs which allows you to seal your keys in Non-Volatile Random-Access Memory (NVRAM), measure your code by Platform Configuration Register (PCR) and utilizing the cryptographic algorithms involving symmetric cryptography and asymmetric cryptography.

Benefits for the user

Lanner's IIoT Security Gateway provides a set of solid designed and validated APIs to make sure that:

› software code execution is being measured
› data-at-rest is protected
› data-in-transit is encrypted
› confidential data is being sealed

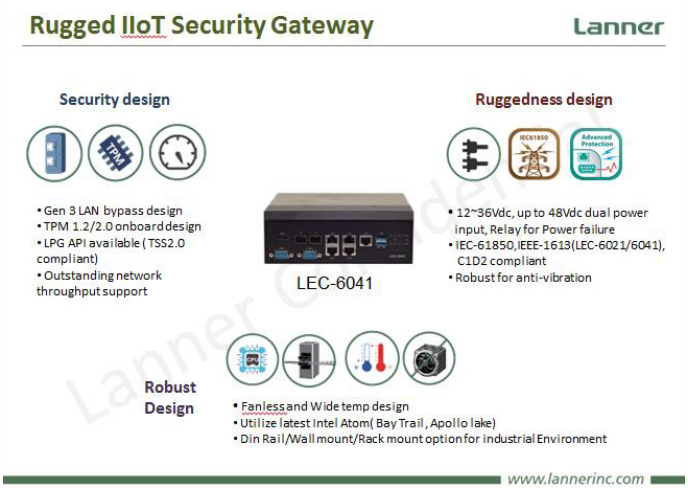
Solution

In the domain of Edge Computing and Industrial IoT the physical threat environment is quite different than in a traditional Information Technology (IT) environment. Being able to secure this at scale is a key requirement we see from our customers. The Infineon OPTIGA™ TPM offers three key features to fulfill this requirement:

1. The ability to generate Elliptic Curve Cryptography (ECC) key pairs using the TPM (ECC is more efficient in key length for the 20-year design lifetime we require for Edge Computing).
2. Storing the ECC private key in the TPM to protect the strong device identity from being compromised or cloned.
3. The ability to use the PCRs for measured boot, which in our scalable approach involves sending the measurements to the EV controller* for analysis across the population of devices.

Functional requirements include TPM on device for hardware root of trust, secured/measured boot, secured key pair generation, secured storage of private keys and root certificates. The solution offers device factory-configured with trusted root Certificate Authority (CA) certificates, configuration check summed and signed by trusted certificates, cloud-managed access controls and two-factor authentication. The included Infineon security products will be OPTIGA™ TPM and TPM 2.0 APIs.

* The EV-controller is Lanner's single plane of glass providing control, visibility and protection at scale for the Edge gateways. It's the user interface to manage all the devices. For example it gives the customer the ability to have zero-touch deployments with instant provision of edge gateways and device-, operating system- or application updates.



Main benefits of the Infineon product

The Infineon OPTIGA™ TPM 2.0 provides hardware root of trust security for IoT and Edge customers, adding zero touch deployment and cloud managed access control for simplified management and scale.

Security Partner Preferred

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.

Lanner Electronics Inc.
Lanner Electronics Inc. (TAIEX 6245) is a world-leading hardware provider in design, engineering, and manufacturing services for advanced network appliances and rugged industrial computers. Lanner provides reliable and customizable computing platforms with high quality and performance. Today, Lanner has a large and dynamic manpower of over 1100 well-experienced employees worldwide with the headquarters in Taipei, Taiwan and subsidiaries in the US, Canada, and China.

Lanner creates customized network appliance for client applications with managed manufacturing process thanks to our in-house design and manufacturing services, covering color of chassis, height, modular or fixed port, BIOS, IPMI, acceleration cards, special certification and additional I/O interface. Lanner's building block design concept can fulfill all your requirements.

Lanner Electronics Inc. contribution to the Infineon Security Partner Network
TPM 2.0 is not limited to addressing the need to have dedicated hardware security on the motherboard but using the processor more and relying more on the firmware, where making libraries available will enable the options that apply to the platform we are using.

With the OPTIGA™ TPM from Infineon, Lanner now can add an extra layer of security to the data. TPM 2.0 along with Lanner LAN Bypass technology available in Lanner network appliances and industrial PCs can offer robust hardware level cyber-hardening at low power consumption. TPM 2.0 enabled crypto security in Lanner hardware is especially important for vertical markets, like network security, uCPE/vCPE for SD-WAN, transportation and industrial cyber security.

Lanner is one of the major hardware solutions companies, focusing on building highly customizable network security appliances for software partners in ISPN.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 08 / 2019

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.