Demonstration Overview

Securing IOT with trusted computing

Trusted computing technologies supported: TPM and TNC

This demonstration shows a deployment of IoT sensors and actuators (such as those found in a Smart Building) managed by a cloud-based application that is remote to the sensors (such as the Building Management application). The server and the IoT devices are connected over the public Internet, using an OpenSSL connection. Mutual authentication and integrity checks of devices and systems is required at session start.

Trusted Computing technology is applied in this case by using open standards to extend OpenSSL authentication. Instead of single factor authentication, using certificates only, the enhanced OpenSSL authentication process shown here requires both a certificate and an integrity report, both of which are protected by a Trusted Platform Module (TPM) on each device. Servers and gateways perform local validation of the integrity reports. If both identity and integrity are validated, a secure session for data exchange is started. IoT devices validate the SSL certificate from the gateway in conventional, single factor OpenSSL authentication.

Several security threats are addressed by these protections. Fake servers, gateways, and sensors are detected and blocked by always performing mutual authentication. Infected components are similarly detected and blocked by checking integrity reports. Rooting these checks in a TPM prevents malware from stealing credentials or falsifying an integrity report. The security of the IoT system is grounded in hardware, ensuring uptime and maximizing reliability.

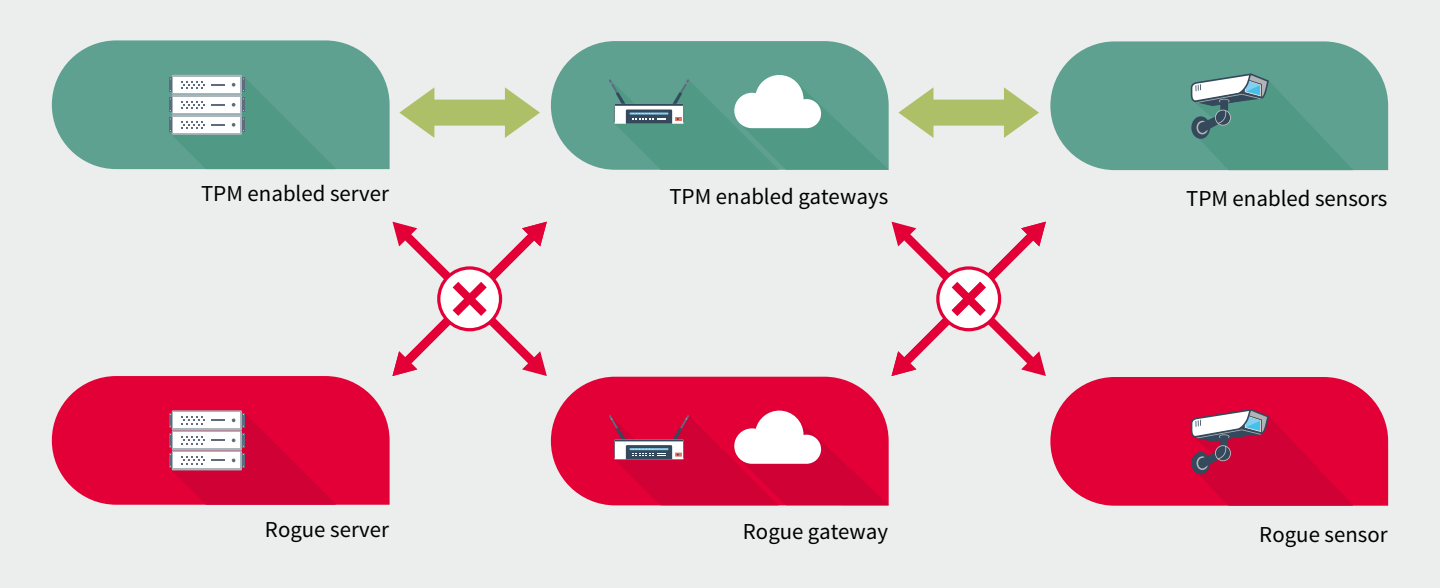
The demo includes an extensive GUI showing activity logs, credentials provided at session start and other logged information relevant to session start and device status.
The security chips in this demo are Infineon SLB9645 TPM chips, based on the TPM standards created by the Trusted Computing Group (TCG). The industrial router in the demo is a Cisco CGR1120 which implements TCG's TPM and TNC standards. The IoT device is a Raspberry Pi with an Infineon TPM daughterboard. The TNC software is an open source implementation by the Technical University of Rapperswil, Switzerland (HSR Rapperswil). The OpenSSL software is open source. The IoT devices and gateways may later come from a mix of vendors, due to the open nature of the protocols.

More Info

For more information on this demo and on IoT security, contact Steve Hanna at steve.hanna@infineon.com

Securing IOT with trusted computing

Trusted computing technologies supported: TPM and TNC



Our partners:

CISCO

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

Published by
Infineon Technologies AG
El Segundo, California

Order Number: xxxxxx-xxx
Date: 05 / 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.