Infineon Security Partner Network

infineon

Security Partner Preferred

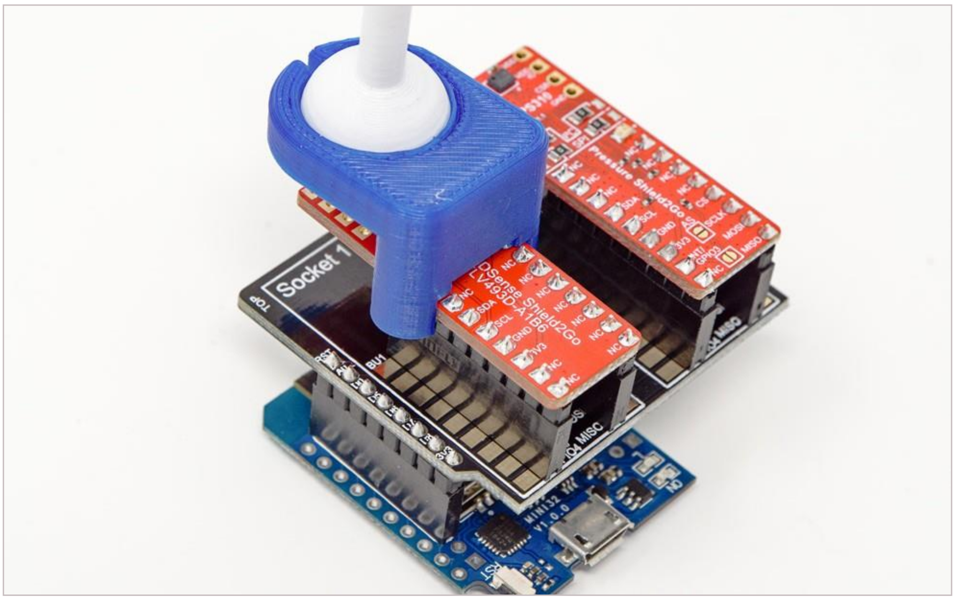
CHIP GLOBE

lighting the chip world

Partner Use Case

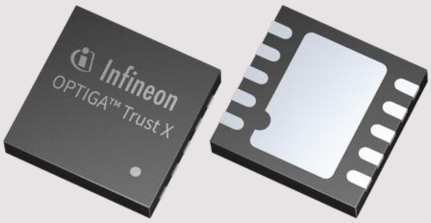
Providing security of a motion control device

Security made easy by Infineon and ChipGlobe - experience how “Sniffing” and a “Man in the middle” attack works on unprotected hardware in comparison to protected hardware. Understand why hardware based security is key and easy to implement at the same time.



Products

OPTIGA™ Trust X



www.infineon.com/ispn

Use case

Application context and security requirements

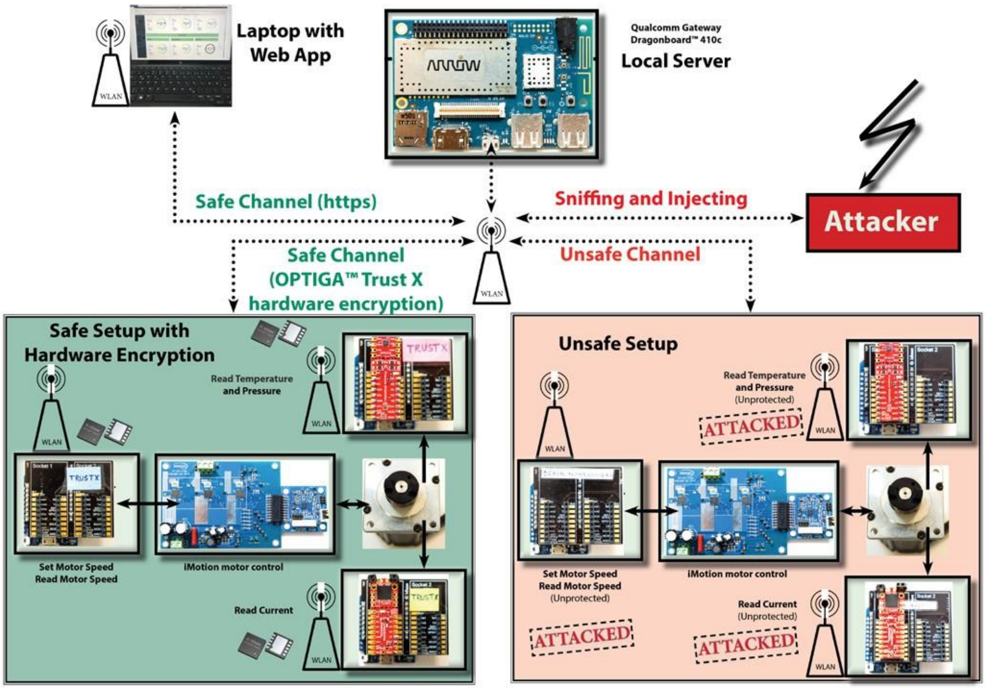
Sensors, transmission of data to a server or a cloud and data harvesting become standard in today's IoT world. Data breaches happen more often and this endangers customers´ IP and data, endangers their business cases and harms their corporate image. Therefore securing data is key.

Challenge

In many IoT applications adequate security solutions are missing. In these cases attackers have an easy game to attack and manipulate valuable data - which raises the question, if the received data is still valid. Companies have to ask themselves, if their existing security measures are the right ones? Why use software security in IoT when hardware based security and hardware encryption offer many advantages besides speed and unambiguous identification.

Implementation

We implemented two pieces of identical hardware. One with OPTIGA™ Trust X in order to add hardware based security, the other one without security measures. We used standard components of ChipGlobe's Sensor Boxes, Infineon iMOTION™ Controller, Infineon's Shield2Go Dual Adapter for WEMOS D1 mini, ESP32 Controller and Infineon Sensor Boards. The communication runs via WIFI. The local gateway is a Snapdragon™ 400 series processor board. It is the central data collector, that has a rule engine implemented and that communicates with a laptop which is hosting the dashboard. This laptop connects to the gateway and controls as well as displays the data on a dashboard. Finally, two electrical motors are driven by the electronics.



Benefits for the user

- Users can experience how hardware encryption protects data between sensor and cloud cannot be manipulated in a meaningful way.
- Sniffing with Wireshark makes it visible why unencrypted data is open for manipulation and why in return encrypted data is protected.
- Users see the value of implementing hardware encryption with OPTIGA™ Trust X.
- Users can see that using standard prototyping components from Infineon and ChipGlobe can help to build a demonstrator as a "proof of concept" vehicle.

Solution

The demonstrator setup consists of a central iMOTION™ motor controller that drives the electrical motor. The control signals come from a staggered device consisting of a Shield2Go Dual Adapter with a ESP32 microcontroller acting as a communication device (COM-Device). The communication to set and read the motor speed runs via a Universal Asynchronous Receiver Transmitter (UART) interface between the motor control and the first COM-Device. The second COM-Device has an additional staggered current sensor that reads the motor current and the communication runs through a Serial Peripheral Interface (SPI) interface. The third COM-Device reads the motor temperature using a staggered temperature sensor and the communication runs through an Inter-integrated Circuit (I2C) interface.

All three COM-Devices communicate through WIFI with the local server that acts as a central data harvesting device and as a rule engine to control the motor operation. It allows secured communication to a dashboard.

The secured hardware setup consist of three Shield2Go Dual Adapters with Infineon's OPTIGA™ Trust X. The unsecured hardware setup has no hardware encryption device implemented.

The unsecured setup uses an unsafe channel communication. The data is visible in a readable ASCII format.
With the next step we are simulating a "man in the middle attack". In order to achieve this attack we use the following three tools on a PC (attacker PC):

1. WireShark
2. Python script (written by ChipGlobe to mock the sensor information)
3. Ettercap

How does it work?

By using WireShark it is possible to see the traffic in the network. We can see that the secured connection is encrypted and not readable. The unsecured connection is open and we can watch the data being transmitted between sender and receiver. This information is used to recreate the data packets which are consisting sensor information on the attacker PC by using the python tool.

Ettercap is the third mentioned tool, which does the "sniffing". In Ettercap we are scanning for all hosts and choose the target IPs.

We enable the Address Resolution Protocol (ARP) poisoning by using Ettercap. The goal of the attack is to associate the attacker PC's MAC address with the IP address of the server, so that any traffic, which is supposed to reach the server, is sent to the attacker instead.

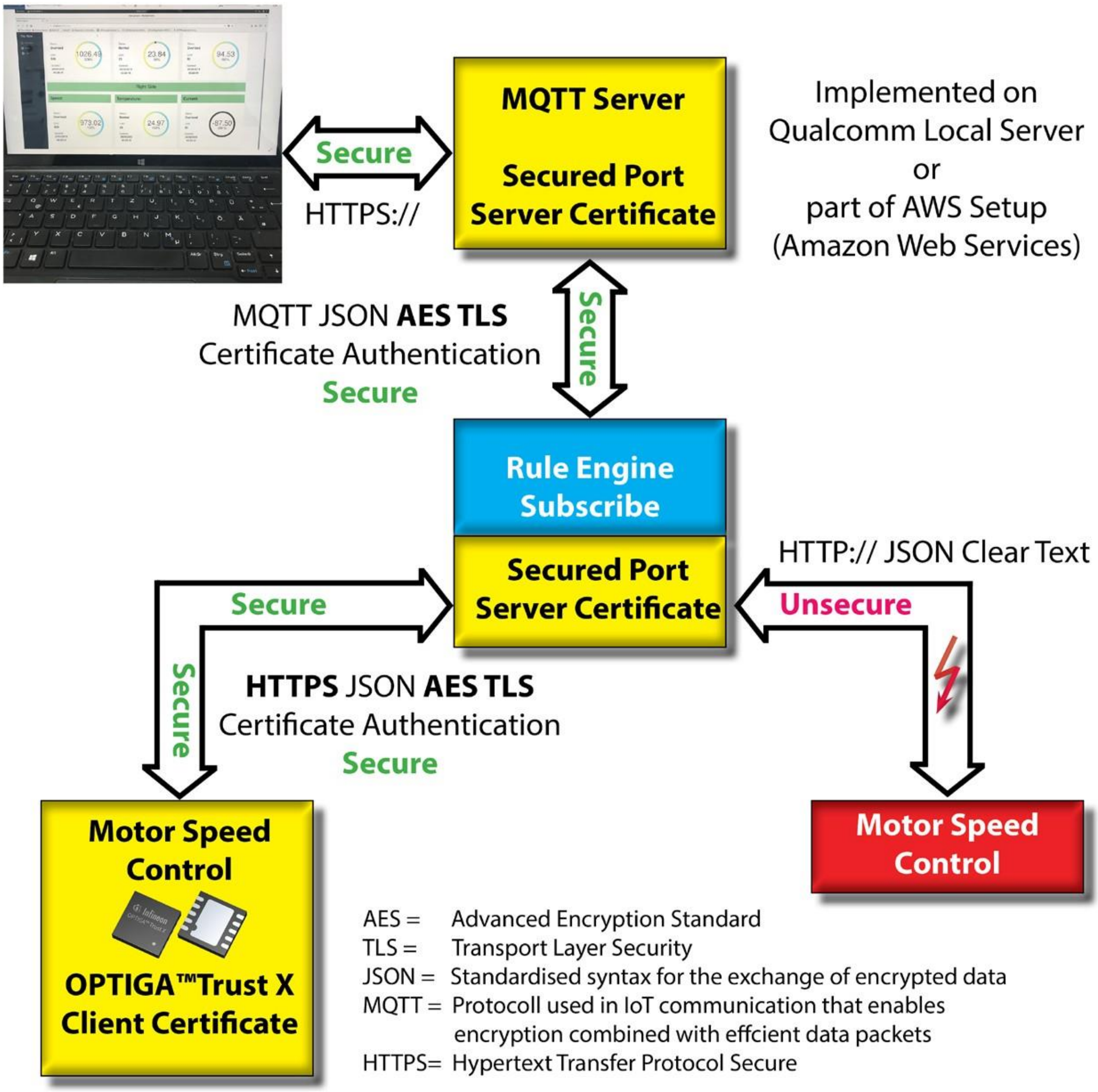
Then we do a Domain Name System (DNS) spoofing by using Ettercap. Ettercap does the sniffing and the traffic from the sensor IP is sent to the attacker PC. The result is the server will not receive any communication from sensor.
After this we run our script which will start sending the dummy sensor information to server. This way the attacker PC mocks itself as a sensor and sends false information to server.

With the help of above mentioned tools and steps, we achieve a "man in the middle attack" using our PC as an attacker. By using hardware based security not only the connection to the local server, but also the data transfer directly to and from the cloud (e.g. Amazon Web Services (AWS)) is set up in a safe way.

Solution

Main benefits of the Infineon product

- The use of an OPTIGA™ Trust X hardware encryption solution is faster and requires less microcontroller resources than a software solution.
- Each OPTIGA™ Trust X protected hardware has a unique serial number and can be used for secured provisioning and remote hardware identification (secured update processes).
- Hardware protected devices are protected from being copied, because each OPTIGA™ Trust X has a securely stored unique key. Unauthorized exchange of hardware can thereby be detected.



Secure

HTTPS://

MQTT Server

Secured Port
Server Certificate

Implemented on
Qualcomm Local Server
or
part of AWS Setup
(Amazon Web Services)

MQTT JSON **AES TLS**
Certificate Authentication
Secure

Secure

Rule Engine
Subscribe

Secured Port
Server Certificate

HTTP:// JSON Clear Text
Unsecure

Secure

Secure

HTTPS JSON **AES TLS**
Certificate Authentication
Secure

Motor Speed
Control

OPTIGA™Trust X
Client Certificate

Motor Speed
Control

AES = Advanced Encryption Standard
TLS = Transport Layer Security
JSON = Standardised syntax for the exchange of encrypted data
MQTT = Protocoll used in IoT communication that enables encryption combined with effcient data packets
HTTPS= Hypertext Transfer Protocol Secure

Partner Use Case

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.

ChipGlobe

ChipGlobe delivers IoT solutions, turnkey designs and consulting in the context of Infineon sensors and combining it with OPTIGA™ Trust X hardware encryption solutions.

ChipGlobe offers IoT developments including sensors, secure data transfer, solutions based on OPTIGA™ Trust X and Infineon OPTIGA™ TPM products, PCBs, assembly, utilization of several processor boards, test hardware and test software, cloud integration, system integration, application software, application development, GUI design, firmware design and verification, driver development and documentation.

ChipGlobe focuses on Automotive, Wireless, Networking, Security, Smart Secure Home and IoT market segments with a team of 80+ experts in design centers in Munich, Dresden, Belgrade, Singapore and Ho Chi Minh City.

ChipGlobe’s contribution to the Infineon Security Partner Network

ChipGlobe cooperates with Infineon as an Infineon Design House for more than 15 years and contributes to the ISPN partnership with:

- upgrade/redesign of hardware with OPTIGA™ TPM as well as OPTIGA™ Trust X solutions
- implementing secured connections from Infineon sensors to cloud
- designing and building sensor boards fitting to embedded systems
- designing and production of sensor boxes for prototyping solutions (proof of concept)
- bridging different prototyping worlds

The solutions relate to Infineon sensors and Infineon security products as well as Shield2Go based prototyping solutions. ChipGlobe supports ISPN with customized and turnkey IoT solutions in hardware and software.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 10 / 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 ANYTIME.

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.