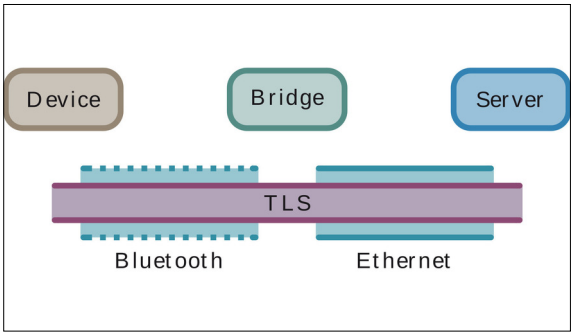
Pascal Stump

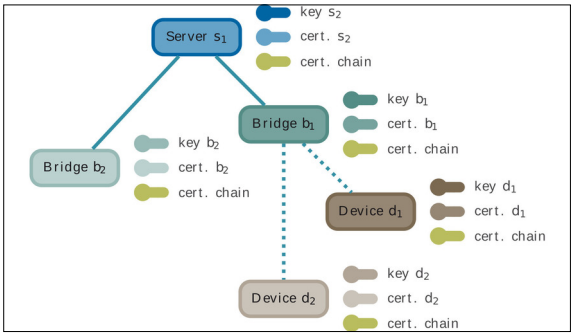
Graduate Candidate	Pascal Stump
Examiner	Prof. Reto Bonderer
Co-Examiner	Urs Reidt, Hamilton Bonaduz AG, Bonaduz, GR
Subject Area	Sensor, Actuator and Communication Systems
Project Partner	Biovotion AG, Zurich, ZH

Embedded Security

Resource-optimized security on an embedded microcontroller



The three participants are connected over Bluetooth/Ethernet with an uninterrupted end-to-end message encryption.



All participants do have their own private key and certificate. The certificate chain is the only common trust source.

Introduction: Biovotion is a digital health company, located in Zurich. They are developing wearable physiological monitoring, offering integrated solutions with connected hardware, analytics and monitoring services. Biovotion works together with leading experts toward a “hospital on the arm” platform. The Everion device is such a platform, measuring different vital signs. This device is worn at the upper arm. At the moment the measured data are sent over Bluetooth low energy to a phone, which forwards them to the cloud. In a future product the measurement device should connect to a bridge device, which forwards the data to a cloud server. Because of this, a new security architecture is required.
The goal of this master thesis is to get an understanding of the needed features/abilities of cryptography implemented into an embedded system and to give Biovotion a suggestion for a new security concept. The concept should be able to authenticate the message sender and includes message encryption and verification.

Procedure / Result: At first, an introduction into the topic of applied cryptography was done. A special attention was set into the key deployment. A widely used solution to this problem is TLS (Transport Layer Security). Then, the cryptography support of some microcontrollers was looked up. At last, a development board with additional shields was chosen as a test system to implement a MQTT service with underlying TLS encryption. This system should show the TLS capability of embedded systems.

Result: TLS is used in the concept suggestion. In the first figure, the three participants are shown with the uninterrupted end-to-end encryption between device and server. The second figure shows the key deployment in the concept. All participants do have the CA (certificate authority) certificate chain, which is used to verify the participants' own certificate. With this, no participant knows the private keys of any other participant. Therefore, if one participant gets hacked the entire system security stays intact.
The practicality of a TLS implementation on embedded system was tested with the development board. In this not optimized version, the additional flash requirements for TLS are ~170 kB, which makes it possible to include it into a Cortex-M4F. The additional data transferred with TLS are < 3.8 kB during handshake (at communications start) and 63 bytes while transferring data (mostly encryption/verification algorithm dependent not TLS specific). These measurements show that an implementation of TLS into embedded systems is possible and useful.