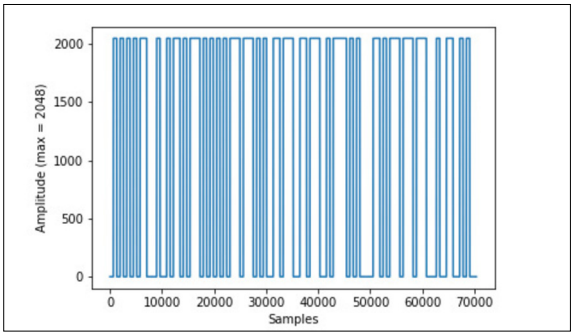
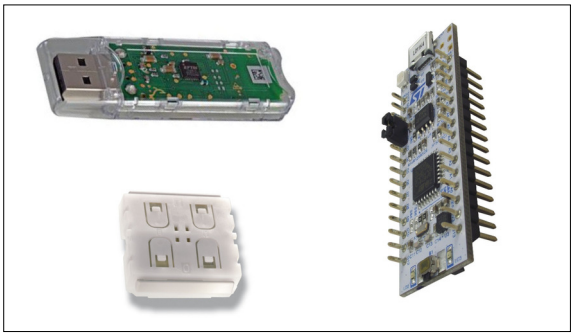
Heinz
Hofmann

Diplomand	Heinz Hofmann
Examinator	Prof. Reto Bonderer
Experte	Reidt Urs, Hamilton Medical AG, Bonaduz, GR
Themengebiet	Sensor, Actuator and Communication Systems
Projektpartner	Compass Security AG, Rapperswil-Jona, SG

Cryptographically Secure IoT System



Erzeugtes rohes enOcean-Frame. Wenn dieses über 868.3MHz Funk versendet wird, imitiert es damit einen enOcean-Sensor.



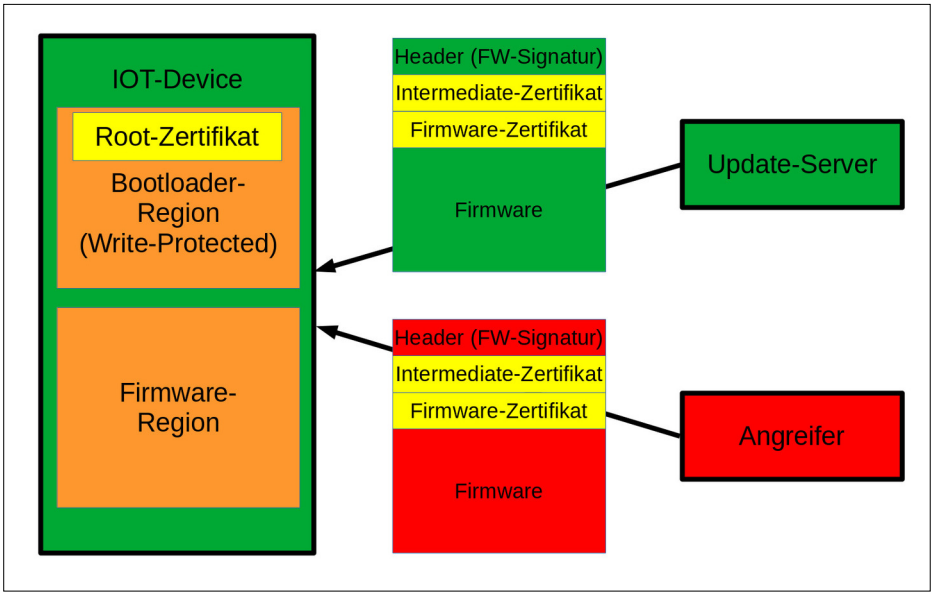
Verwendete Hardware: enOcean-Empfänger (links oben), enOcean-Button (links unten), ST-Microcontroller (rechts)

Ausgangslage:

- enOcean ist ein proprietäres Funkprotokoll. Dieses erlaubt es, mit extrem wenig Energie Funksignale zu versenden. Im Jahr 2013 wurde dieses Protokoll kryptografisch erweitert. Dieses Protokoll soll auf Schwachstellen, welche potentielle Hacker ausnutzen könnten, untersucht werden.
- Embedded Systems werden immer öfters als so genannte IoT-Devices ans Internet angeschlossen. Dabei werden zu oft Aspekte der Informationssicherheit vernachlässigt. Dies macht solche Devices zu leichten Zielen für Hacker. Es gilt herauszufinden, was alles beachtet werden sollte, um solche Systeme so sicher wie möglich zu machen. Ein besonderer Fokus wird dabei auf das sichere Booten und Updaten von entsprechenden Devices gelegt. Zudem soll die Security möglichst wenig Ressourcen belegen.

Ergebnis:

- Die Verschlüsselung von enOcean ist für die Anwender optional. Dies resultiert darin, dass kaum jemand das enOcean-Protokoll in verschlüsselter Form verwendet. In dieser Arbeit wurde ein Programm entwickelt, welches es erlaubt, unverschlüsselte enOcean-Meldungen eins zu eins oder in abgeänderter Form nachzubilden. Damit können enOcean-Systeme in der Praxis erfolgreich angegriffen und getäuscht werden.
- Die Untersuchungen ergeben, dass aktuell ein Zusammenspiel von Hardware-Sicherheitsmechanismen, TLS und einem guten Secure-Bootloader nötig ist, um ein möglichst sicheres System zu erzeugen. Ein bereits vorhandenes Secure-Boot-Secure-Firmware-Update Modul (SBSFU von ST-Microelectronics) wurde um die Verwendung von X509-Zertifikaten erweitert. Dadurch kann gezeigt werden, dass IoT-Systeme ähnlich kryptografisch sicher und flexibel implementiert werden können wie herkömmliche IT-Systeme.



Szenario, bei dem der Bootloader aufgrund des Root-Zertifikats kryptografisch eindeutig unterscheiden kann, ob das Firmwareupdate vom Update-Server oder von einem Angreifer kommt.