Zürcher Hochschule
für Angewandte Wissenschaften

School of Engineering
InES Institute of Embedded Systems

Secure Firmware Updates for Internet of Things

Vernetzte IoT-Systeme sind ein stark wachsender Bereich im Technologiesektor. Die Netzwerke werden immer grösser und leistungsfähiger, wodurch auch der benötigte Unterhalt steigt. Damit ein grosses IoT-Netzwerk wirtschaftlich bleibt, müssen die Endgeräte ohne physische Interaktion kabellos aktualisiert werden können. Die Sicherheit spielt dabei eine zentrale Rolle. IoT-Geräte sollen keinen Schwachpunkt im Netzwerk darstellen oder als Einfallstor für Cyberangriffe dienen.

Ziel dieser Arbeit ist das Erstellen eines funktionsfähigen Prototyps als Demonstrator, mit welchem ein sicheres, kabelloses Update von IoT-Geräten gezeigt werden kann. Neben einer Demonstration der Grundanforderungen sollen weiterführende Tests Aufschluss über Dauer und Energieverbrauch des Updatevorgangs geben.

Als «Proof of Concept» wird ein kleines IoT-Testnetzwerk aufgebaut. Die verwendeten IoT-Endgeräte kommunizieren über das IEEE 802.15.4 (WPAN) Low-Power Wireless Protokoll. Die verschlüsselte Kommunikation sowie der sichere Update-Download erfolgen über das IoT-Protokoll «Thread».

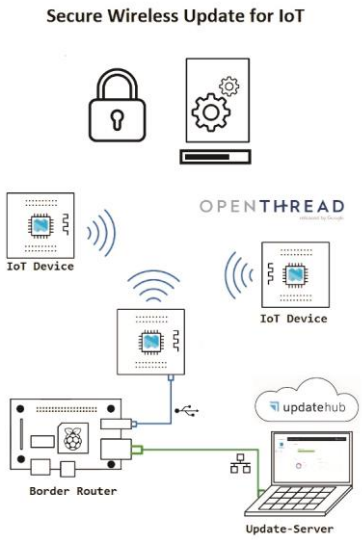
Die sichere Installation der Updates wird mittels digitaler Signaturen und einem sicheren Bootloader gewährleistet. Der Code des Bootloaders wird angepasst, sodass dieser zur Kontrolle der Signatur zusätzlich zu Software-Algorithmen die Hardwareunterstützung eines Secure Elements (NXP SE050) nutzen kann. Das gesamte System wird so ausgelegt, dass die Anforderungen aus RFC9019 (SUIT) an eine sichere Update-Infrastruktur für IoT-Geräte erreicht werden können.

Die Ergebnisse zeigen, dass die programmierte Software sowie das aufgebaute Netzwerk inklusive Update-Kontrollinfrastruktur die Anforderungen erfüllen. Die Software-Updates können mit Verfahren signiert und überprüft werden, welche dem aktuellen Stand der Technik entsprechen. Das Starten von nicht autorisierter Software wird durch den sicheren Bootloader erfolgreich verhindert.

Software-Updates können problemlos und skalierbar für mehrere Geräte gestartet werden. Die Datenübertragung im IEEE 802.15.4. Wireless-Netzwerk funktioniert reibungslos und Update-Downloads können in nützlicher Frist getätigt werden. Für batteriebetriebene IoT-Geräte ist der Energieverbrauch eines Updatevorgangs jedoch nicht unerheblich und muss bei der Planung eines ausgedehnten Netzwerks beachtet werden. Auch der erhöhte Speicherbedarf der Firmware durch den sicheren Bootloader sowie die Wireless-Update-Applikation muss beachtet werden.

Diplomierende
Lukas Eugster
Simon Stuck

Dozierende
Simon Künzli
Andreas Rüst



Darstellung des im Rahmen der Bachelorthesis erstellten Demonstrations-Netzwerks. Mehrere Microcontroller (IoT Devices) können kabellos über ein Thread-Netzwerk (IEEE 802.15.4) aktualisiert werden. Ein RaspberryPi4 dient dabei als Border-Router zwischen Thread-Netz und LAN. An einem Update-Server mit Webinterface können Updates gestartet und verwaltet werden. Die Sicherheit wird durch einen Secure Bootloader garantiert, welcher digitale Signaturen der Firmware überprüft. Zur Sicherung der Schlüssel werden diese auf einer speziellen Hardware mit sicherem Schlüsselspeicher abgelegt. [5] [15] [21]