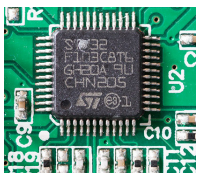
Projekt NAMIB

Network Access Makes IoT Better

Olaf Bergmann, Ute Bormann, Carsten Bormann

Hintergrund



Das Konzept *Internet of Things* (IoT) ist in den Vorstandsetagen, zunehmend auch in den Supermarktregalen angekommen. Die Verfügbarkeit extrem kostengünstiger Mikrocontrollerplattformen mit Leistungen, die noch vor ein paar Jahrzehnten als Entwicklungsrechner ausgereicht hätten, ermöglicht zusammen mit effizienter Produktionstechnik einen qualitativen Sprung. In den nächsten Jahren und Jahrzehnten sollen Milliardenumsätze mit IoT-Systemen erwirtschaftet werden.

Kleine, intelligente, und vor allem mit dem Netz verbundene Geräte mit Sensoren und Aktoren finden zunehmend Verbreitung, um auf Umgebungsbedingungen besser eingehen und sie besser steuern zu können, nicht zuletzt auch, um Energie und andere Ressourcen zu sparen.

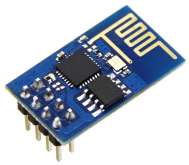
Aber was genau tun diese kleinen Geräte eigentlich? Hat der Hersteller wirklich nur die beworbene Funktion realisiert oder hat das Gerät noch einen Zweitjob als Spion? Und läuft überhaupt noch die Firmware des Herstellers, oder hat ein Angreifer (“Hacker”) schon längst das Gerät übernommen und verfolgt finstere Ziele? Es gehört schon einiger Mut (oder einige Naivität) dazu, ein Gerät zu kaufen und ihm ungeprüft Zugriff auf persönliche Bereiche und gleichzeitig uneingeschränkten Zugang zum Internet zu geben. Vertrauen in einen Hersteller haben zu können ist hier gut, Kontrolle aber wahrscheinlich besser.

Um die gewünschte Vertrauenswürdigkeit von IoT-Geräten herzustellen, müssen einerseits die Geräte und ihre Sicherheitsfunktionen diese auch verdienen. Andererseits muss die Infrastruktur, in die die Geräte eingebracht werden, ihren Beitrag leisten. Klassische „Firewalls“ bringen hier nur begrenzten Gewinn, denn die Angriffe kommen im Zweifelsfall ja von innen! Die Geräte müssen der Infrastruktur also nachweisen, dass die von ihnen abgewickelte Kommunikation auch im Sinne ihrer Nutzer ist.

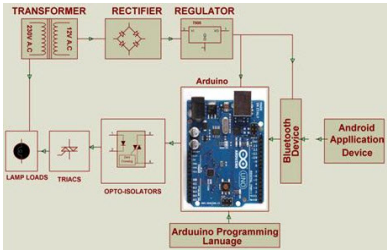
Auf der Geräteseite wurden in den nach Wüsten und ihren Bewohnern benannten Projekten der AGRN in den vergangenen Jahren Bausteine entwickelt, die einfache abgesicherte IoT-Anwendungen auf Basis gängiger Mikrocontroller-Plattformen ermöglichen. Damit ist ein vergleichsweise einfacher Einstieg auf Basis moderner IoT-Plattformen (ARM Cortex M oder ESP als Hardware, RIOT als Betriebssystem) möglich. Der meist geringe Speicherplatz, das erforderliche strikte Energiemanagement und die eingeschränkten Benutzungsschnittstellen in diesem Segment stellen besondere Anforderungen an die Entwicklung.

Auf der Infrastrukturseite gab es in diesen Projekten auch schon einzelne Ansätze, die auf der Basis von SDN-Techniken (*Software-Defined Networks*) kontrollierte Kommunikationskanäle für die erwünschten Funktionen der IoT-Geräte zur Verfügung gestellt haben. Linux-basierte Netzkomponenten und vor allem OpenWRT als Softwarepaket für Heimrouter und -WLAN-Komponenten bieten hier eine gute Grundlage für weitere Entwicklungen.

Projektziel



Ziel des Projektes ist es, zu den genannten Problembereichen unter Nutzung des Standes der Technik praktische Fortschritte zu entwickeln und zu demonstrieren. Es entsteht Open-Source-Software und -Dokumentation, oft auf der Grundlage von (oder als Zusatz zu) bestehender Open-Source-Software, insbesondere RIOT und OpenWRT. Die Ergebnisse sollen dazu geeignet sein, in den Heimumgebungen der Teilnehmer zum Einsatz zu kommen und die Vertrauenswürdigkeit beim dortigen Einsatz von IoT-Hard- und Software verbessern helfen. Die einzelnen Projektziele werden zu Beginn des Wintersemesters 2020/21 in einem Vorbereitungskurs und einem Projektwochenende konkretisiert; dabei sind über die konkreten Vorstellungen der Betreuenden hinaus Vorschläge der Teilnehmenden hochgradig erwünscht.



Der Fokus von NAMIB liegt auf System- und Entwicklungssoftware, aber die Nutzer müssen auch damit umgehen können: Offensichtlich benötigen auch IoT-Geräte eine Schnittstelle zu ihren Nutzern. Dabei verfügen die Geräte selbst oft über wenig Interaktionsmöglichkeiten; weitere Geräte wie Smartphones (Android und/oder iOS) oder „Zentralen“ mit Webschnittstellen fungieren als große Brüder. Mit diesen muss aber auch erst einmal ein sicherheitstechnisches Vertrauensverhältnis hergestellt werden, und vor allem muss eine Stehlampe erst einmal wissen, welcher Lichtschalter sie überhaupt ein- und ausschaltet.

Unter Nutzung und Ausbau dieser Ideen werden wir Entwicklungsszenarien für Anwendungen im Web of Things (WoT) entwickeln, dokumentieren, und auch veröffentlichen. Neben WoT-Anwendungen im allgemeinen geht es dabei insbesondere auch um „Smart Energy“ und „Home Automation“. Das Ergebnis ist ein Open-Source-System mit Betriebssystem-, Vernetzungs- und Entwicklungskomponenten für diesen Zweck, einschließlich eines oder mehrerer Demonstratoren.

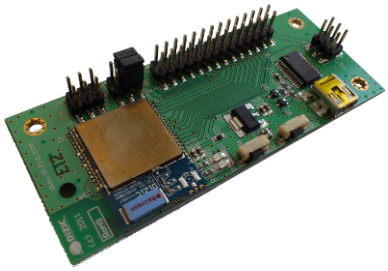
Zwei einander ähnliche Szenarien könnten bei der genaueren Entwicklung der Projektziele inspirieren: In beiden Fällen setzt ein Nutzer einen personalisierten, IoT-smarten Wecker ein, der auch in einem temporär genutzten Hotelzimmer seine volle Funktion entfalten soll. Im einen Fall bringt der Nutzer den Wecker mit, und dieser soll dann im Hotelzimmer natürlich die dort vorhandene IoT-Infrastruktur (Sensoren; Einfluss auf Raumtemperatur, Lüftung, Beleuchtung, Gardinen) voll nutzen können. Im anderen Fall ist genau so ein Wecker im Hotelzimmer schon vorhanden, muss aber noch in die Lage versetzt werden, mit den persönlichen Sensoren des Nutzers zu kommunizieren und dessen persönliche Präferenzen umzusetzen. In beiden Fällen sollen die Datenspuren nach Beendigung des Aufenthalts minimiert werden. Offensichtlich geht es hier nicht nur darum, den Netzzugang und die Kommunikationskanäle zu autorisieren, sondern auch um die Autorisierung und Konfiguration der Anwendungen.

Vorgehensweise

Die Vorgehensweise ist agil, iterativ, und ergebnisorientiert. Wird eine mögliche Aktivität durch das Projekt als zielführend bewertet, nimmt sich ein kleines Teilprojektteam des Themas an und produziert in mehreren Iterationen Ergebnisse („release early, release often“). Die globale Projektplanung strukturieren wir so, dass bereits nach wenigen Monaten ein nachhaltiges Ergebnis vorliegt; darauf können dann weitere Iterationen zur Verbesserung der Qualität und des Funktionsumfangs aufsetzen.

Um das Rad nicht neu zu erfinden, setzen wir auf Open-Source-Projekte wie RIOT und OpenWRT auf. Das soll keine Einbahnstraße sein: Zu Beginn des Projektes werden wir uns darauf einigen, wie die erzielten Ergebnisse wiederum der Open-Source-Welt zugute kommen können (z.B. auch durch Auswahl geeigneter Lizenzen wie GPL, BSD, CC).

Als IoT-Hardware kommen z.B. Arduino-, ESP- und STM32-(ARM-)-Umgebungen zum Einsatz, für die Infrastruktur OpenWRT-fähige Router. Zum Entwickeln nehmen wir natürlich unsere Laptops, aber auch Smartphones (Android, gegebenenfalls auch iOS).



NAMIB arbeitet mit Systemen, die im Dreieck Hardware, Software, Benutzungsschnittstellen agieren. Eine gewisse Bereitschaft zum „Basteln“ bis hin zu Fertigkeiten wie Löten, 3D-Modelle erarbeiten etc. ist bei der Erstellung von Prototypen hilfreich. Die Arbeit mit Betriebssystemen wie RIOT erfordert auch ein gewisses Interesse für maschinennahes Denken. Andererseits benötigen wir auch klassische Web-Anwendungen und GUIs. Manches wird in C (Router, Sensorknoten), C++, C-Varianten (Objective-C für iOS, oder auch Swift) oder Java (Android) entwickelt werden, anderes in Sprachen wie Python (Skripte), Ruby oder JavaScript (Web-Anwendungen). Besonderes Interesse liegt auch auf der Sprache *Rust* für speichersichere IoT-Anwendungen sowie auf Methoden, *mobilen Code* auf sehr kleine Geräte zu bringen. Die Projektbeteiligten werden Gelegenheit haben, ihre jeweiligen Aktivitäten auf einen Teilbereich dieser Themenvielfalt zu fokussieren.

Das Projektmanagement wird durch die Studierenden organisiert, z.B. durch rollierende/überlappende Wahl eines PM-Teams. Jede Teilnehmerin/jeder Teilnehmer ist aber auch selbst verantwortlich für die durch sie/ihn erzielten Fortschritte; dies wird durch regelmäßige Selbstbewertung und Bewertungsgespräche mit den Betreuern bekräftigt.

Projektbetreuung

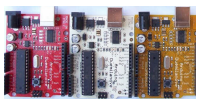
Das Projekt wird betreut aus der Arbeitsgruppe Rechnernetze:

- Dr. Olaf Bergmann
- Prof. Dr. Ute Bormann
- Prof. Dr. Carsten Bormann

Studiengänge und Laufzeiten

Das Projekt NAMIB ist als Bachelor-Projekt für das WS 2020/2021 und SS 2021 für Bachelor-Studierende der Informatik und des Systems Engineering angelegt. Ein Master-Projekt für die Profile *SQ* und *DMI* ist im Anschluss geplant.

SQ: IoT-Systeme sind immer auch sicherheitskritisch. Weder wollen wir uns von ihnen überwachen lassen, noch wollen wir Fremden Zugriff auf unsere Fernseher, Lichtschalter und Türschlösser geben. Daher lohnt sich ein Blick auf die Sicherheit dieser Systeme. Diese beschränkt sich nicht nur auf die Absicherung der Kommunikation gegen Angriffe von außen, sondern umfasst auch die Sicherheit gegen Programmierfehler, die zu Fehlfunktionen oder Systemausfällen führen können.



DMI: Die entwickelten Benutzungsschnittstellen für die Entwickler (aber auch möglicherweise Anwender) sollen nicht nur *benutzbar* sein, sondern schlicht auch Spaß machen. Die entwickelten Systeme werden also auch nach gestalterischen Aspekten bewertet. Dabei spielen nicht nur mobile Apps und Web-Clients eine Rolle, sondern auch die beschränkten Ein-/Ausgabe-Schnittstellen der eingebetteten Systeme. Wie kommuniziere ich am besten mit einer Stehlampe?