Smart-Grids mit Hardware-Security-Modulen sichern

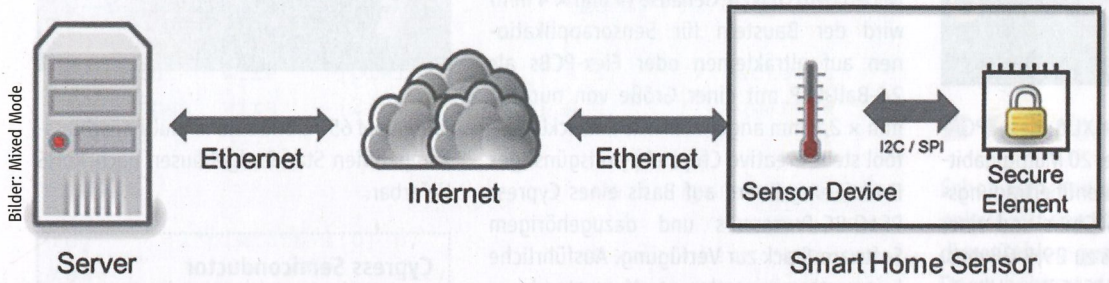

Bild 1: Anbindung eines HSMs an einen Smart-Home-Sensor. Das externe HSM wird über einen vom HSM unterstützten Bus am Mikrocontroller angeschlossen. Das HSM kann dazu verwendet werden, schützenswerte Informationen wie Schlüssel und Zertifikate abzulegen und eine sichere Verbindung zu einem Server aufzubauen.

Je mehr die Welt vernetzt ist, umso mehr steigt auch die Gefahr durch Cyberangriffe. Um Anwendungen gegen Cyberangriffe zu schützen, müssen die Daten und Kommunikationswege verschlüsselt werden. Hier kommen meist in Software umgesetzte Kryptographie-Algorithmen zum Einsatz. Diese schützen nicht immer vor Angriffen direkt am Gerät. Es gibt aber auch hier Wege, durch eine Turn-Key-Solution diese Informationen zu schützen.

Rouven Braden
Security Engineer bei Mixed Mode

Durch die ortlaufende Vernetzung unserer Welt im Smart Home sowie in der Industrie steigt auch stetig das Risiko von Angriffen aus dem Internet. Während Geräte wie Computer und Laptops mit Sicherheitsupdates und Sicherheitssoftware versorgt werden, werden IoT-Geräte noch stark vernachlässigt. Dass die Sicherung von IoT-Geräten und -Verbindungen essenziell wichtig ist, zeigen Vorfälle in der Vergangenheit, wie Mirai, eine Schadsoftware, die nicht gesicherte IoT-Geräte manipuliert und sie für DDoS-Angriffe nutzt. So wurde Anfang 2016 der Internetzugriff in Liberia zeitweise unterbrochen. Jedoch hört es bei Angriffen auf die Internetinfrastruktur nicht auf.

Durch die Verbreitung von IoT-Geräten in sensiblen Bereichen wie Gesundheitswesen (Medizintechnik) und Verkehr (Connected Car) können Cyberangriffe hier nicht nur zu finanziellen Schäden führen, sondern auch zu Schäden an Leib und Leben. Eindrückliches Beispiel hierfür waren in der jüngeren Vergangenheit die Fälle von Angriffen durch Ransomware auf die IT von Krankenhäusern.

Security durch reine Softwarelösungen genügt nicht

Damit Daten in Kommunikationsnetzwerken sicher übertragen werden und sie nicht von Unberechtigten gelesen oder sogar manipuliert werden können, müssen Verbindungen abgesichert werden. Jedoch sind nicht nur die Verbindungen zwischen Geräten gefährdet, sondern die Geräte selbst auch. Zur Realisierung dieser geforderten Sicherheit gibt es mittlerweile verschiedene Ansätze. Zum einen können softwarebasierte Kryptografie-Algorithmen verwendet werden, zum anderen sind Hardware-Security-Module (HSMs) eine Möglichkeit.

Eine rein softwarebasierte Lösung birgt allerdings die Gefahr, dass die Manipulation direkt am Gerät weiterhin möglich ist. Der Angreifer kann mittels moderner Angriffstechniken Teile des Speichers auslesen beziehungsweise Softwaremanipulationen durchführen. HSMs bieten die Möglichkeit, die Geräte auch vor sol-

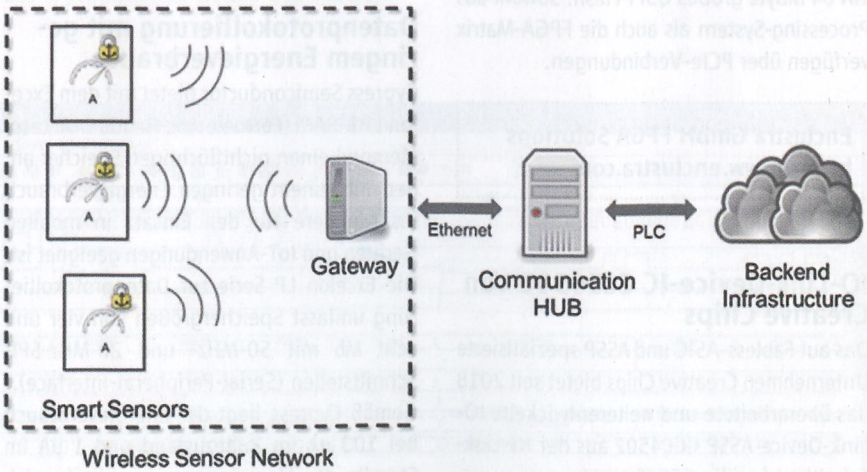

Bild 2: Smart-Grid-Kommunikationsinfrastruktur im Forschungsprojekt CONNECT. Im Wireless-Sensor-Network wird der Stromverbrauch der einzelnen Verbraucher ermittelt und über eine verschlüsselten Verbindung an das Gateway gesendet. Das Gateway dient dazu, das Sensornetzwerk zu konfigurieren und die empfangenen Daten an den Communication HUB weiterzuleiten. Der Communication-HUB verarbeitet die Daten und sendet sie über ein Power-Line-Communication-Interface an die Backend-Infrastruktur.

chen direkten Zugriffen abzuschirmen. Sie haben die Eigenschaft, dass sie einen Manipulationsschutz besitzen, der sie vor Hardwareangriffen schützt. Direkte Manipulationen an der Hardware werden erkannt, worauf sich das HSM sperrt und das Auslesen des internen Speichers verhindert (*Bild 1*).

Um diese Manipulationen zu erkennen, werden diverse Sensoren in das HSM mit eingebaut, um zum Beispiel Druckänderungen, Lichtänderungen, extreme Temperaturänderungen oder Röntgenstrahlung zu detektieren. Somit können empfindliche Daten wie Schlüssel und Zertifikate in dem HSM sicher gespeichert werden. HSMs bieten überdies den Vorteil, dass sie speziell für Kryptografie-Algorithmen entwickelt werden.

Die kryptografischen Funktionen werden schneller ausgeführt als auf einem Anwendungs-Mikrocontroller. Lediglich die Anbindung über einen Bus kann die Geschwindigkeit begrenzen.

Um bestehende Systeme um HSMs zu erweitern, bieten sich Elemente an, die über SPI oder I²C angebunden werden. Durch diese Möglichkeit muss der Mikrocontroller des Systems nicht getauscht, sondern lediglich um das externe Element erweitert werden. Voraussetzung dafür ist jedoch, dass die Anwendungssoftware angepasst wird und das System mit der neuen Firmware aktualisiert wird. Bei der Neuentwicklung eines Systems sollte ein HSM direkt in der Designphase mit eingeplant werden (Security by design).

Security in Energienetzwerken

Im Rahmen des EU-Forschungsprojekts CONNECT (http://www.connect-ecsel.eu), an dem die Firma Mixed Mode als Mitglied des Infineon Security Circle Partner Network beteiligt war, wurde der OPTIGA Trust X als HSM zur Absicherung eines Smart-Grids genutzt (*Bild 2*). Die Wandlung des Energienetzes vom reinen Verteilnetz hin zum Smart-Grid ist ein unverzichtbarer Schritt, um die Klimaschutzziele zu erreichen und den Bedarf an fossilen Energieträgern deutlich zu reduzieren. Wesentliche Elemente dieses Wandels sind die Erweiterung des Energieversorgungsnetzwerks zur Zustandserfassung in Echtzeit, sichere Kommunikationsverfahren für den Austausch von Zustands-, Kontroll- und Steuerungsdaten sowie die effiziente Wandlung elektrischer Energie zur Verknüpfung von Verbrauchern, Speichern und Energiequellen.

Ein zentrales Thema dabei ist die sichere drahtlose und drahtgebundene Kommunikation für den Austausch der obengenannten Daten zwischen den beteiligten Sensoren und Aktoren in einer Liegenschaft sowie mit einer dahinterliegenden Backend-Infrastruktur, bestehend aus den Kommunikations-Netzwerkstrukturen vom Sensor beziehungsweise Aktor über zentrale Kommunikationsknoten zum Verbraucher und zum Versorger.

Security-Anforderungen betreffen in erster Linie:

- eingebettete, energieeffiziente Systeme,
- das Smart-Grid selbst sowie die
- drahtlose Vernetzung intelligenter Sensorknoten im Anwendungsfall des Wireless-Sensor-Network.

Abfangen und Manipulation der Daten im drahtlosen Sensornetzwerk muss zwischen den Sensorknoten und dem Gateway als neuralgischer Strecke verhindert werden. Diese Aufgabe übernimmt der OPTIGA Trust X, der etwaige Manipulationen der Hardware erkennt und verhindert, sowie als sichere Ablage für Schlüssel und Zertifikate dient. Die Kommunikation zwischen dem Gateway und dem Energienetz wird durch einen Communication-Hub umgesetzt, der auf einer Linux-Plattform basiert, deren Security ihrerseits durch ein HSM der Firma NXP gewährleistet ist. Die Sensordaten werden verschlüsselt vom Gateway über den Communication-Hub in das Energienetz eingespeist, wobei die Schlüssel selbst eben auf den HSM und damit für Angreifer unerreichbar liegen.

Der im drahtlosen Sensornetz eingesetzte OPTIGA Trust X von Infineon ist nach Common Criteria EAL6+ (high) zertifiziert und somit der geeignetste Sicherheitscontroller dieser Firma. Er unterstützt ECC256, AES128 sowie SHA-256 und besitzt vier Speicherplätze für Schlüssel sowie zwei für Trust-Anchor-Zertifikate. Als Turn-Key-Lösung bietet er die Möglichkeit, mit wenig Aufwand eine sichere Verbindung über TLS/DTLS aufzubauen.

Einsatz des HSM mit RIOT

Der Sicherheitscontroller wird in Verbindung mit dem Betriebssystem RIOT eingesetzt (*Bild 3*), das eigens für IoT-Geräte entwickelt wurde. Durch seine Modularität ist es mit verschiedenen Mikrocontrollern und Peripheriegeräten einsetzbar und lässt

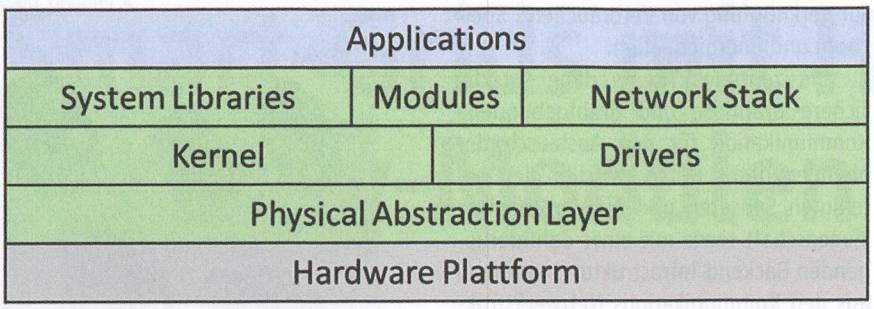

Bild 3: Standardstruktur des Betriebssystems RIOT mit Kernel, Treibern, Modulen und Netzwerkstack.

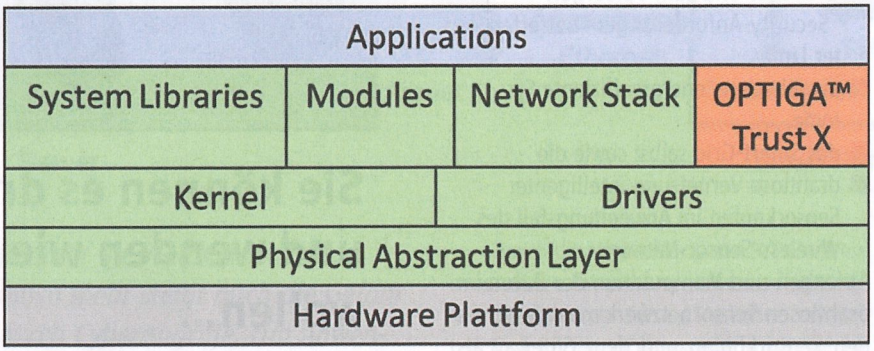

Bild 4: Um die OPTIGA-Trust-X-Funktionen erweiterte Struktur des Betriebssystems RIOT.

sich durch neue Komponenten relativ problemlos erweitern.

Zur Nutzung des HSM wurde die von Infineon gelieferte Bibliothek als neues Modul eingebunden. Die Controllersoftware arbeitet direkt mit den I²C- und Ethernet-Treibern. Somit ist kein weiteres Handling der Daten durch die Anwendung nötig. Lediglich Änderungen am Physical-Abstraction-Layer (PAL) der OPTIGA-Library mussten vorgenommen werden. Infineon hat die PAL-Funktionen auf ihre Demonstration angepasst ausgeliefert. Hier mussten die Treiber-Funktionen gegen die von RIOT vorgegebenen ausgetauscht werden. Des Weiteren wurden die OPTIGA-Library Funktionen in der Anwendung eingesetzt, um die Kryptographie-Algorithmen des HSM zu nutzen (*Bild 4*).

Als Verschlüsselungstechnik wird DTLS verwendet, da es eine verbindungslose gesicherte Kommunikation auf Basis von UDP ermöglicht (*Bild 5*). Die Sensorknoten und das Gateway erhalten ihre Schlüsselpaare und Zertifikate basierend auf der gleichen Root of Trust. Die Schlüssel, Zertifikate und die Root of Trust werden bei der ersten Inbetriebnahme durch den Administrator auf dem Secure-Element abgelegt. Somit ist gewährleistet, dass nur durch den Administrator zugelassene Geräte im Netzwerk kommunizieren können. Als Ergebnis ist die Kommunikation im gesamten drahtlosen Netzwerk geschützt und ein Mitlesen oder Manipulieren der Daten ist nicht möglich.

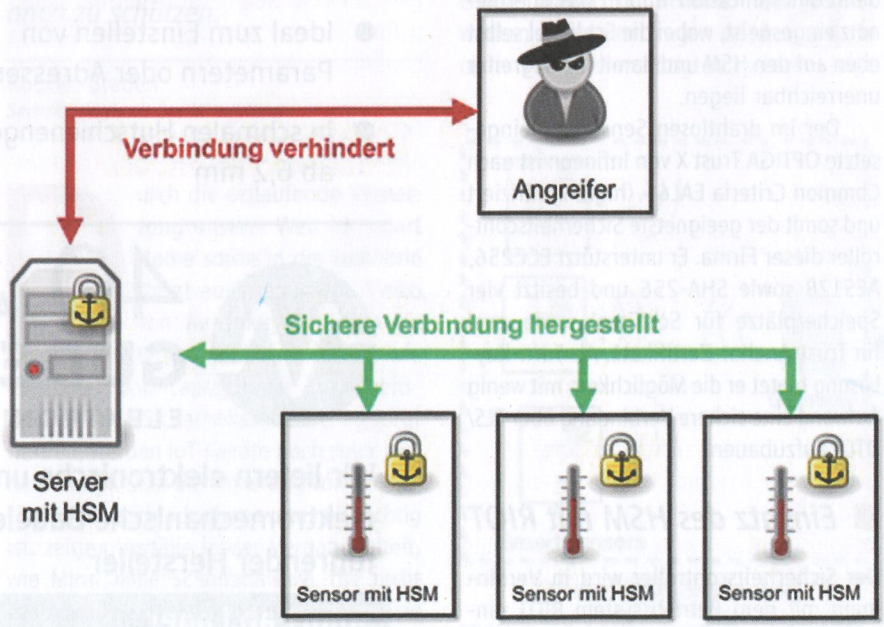

Bild 5: Funktionsweise einer DTLS-Verbindung. Der Server authentifiziert sich gegenüber dem Sensor mit seinem Zertifikat. Der Sensor kann über einen auf dem HSM abgelegten Trust-Anchor die Gültigkeit des Zertifikats überprüfen. Optional kann sich der Sensor auch gegenüber dem Server authentifizieren. Daraufhin wird ein gemeinsamer Schlüssel ausgehandelt, der für die weitere sichere Kommunikation verwendet wird.

Was bleibt zu tun?

Das bisher Beschriebene stellt den ersten Ansatz zur Sicherung von Daten und Geräten dar. Bei Tests und Evaluierungen ergab sich eine Schwachstelle im Bereich der Anbindung des HSM: Ein potentieller Angreifer kann Informationen aus dem SPI beziehungsweise I²C-Bus auslesen. Wenn die Daten dort nicht verschlüsselt übertragen werden, könnte er sie sogar im Klartext mitlesen. Deswegen muss die Sicherheit des Busses gewährleistet werden. Hierzu muss ein Schlüssel auf dem Mikrocontroller abgelegt werden, wobei der Mikrocontroller mit einem Speicherbereich ausgerüstet sein muss, der nach dem Programmieren über keine Schnittstelle mehr ausgelesen beziehungsweise geändert werden kann. Eine solche Lösung muss auch vom HSM unterstützt werden und wird zurzeit durch Infineon in einem neuen HSM integriert.

Wesentlich vorteilhafter wäre ein Mikrocontroller mit eingebautem HSM, das den gesamten Controller gegen Manipulationen schützt. Der Nachteil neben höheren Kosten besteht darin, dass solche Mikrocontroller meist nur schwer in bestehenden Systemen nachzurüsten sind, wenn überhaupt. Absicherung von Daten und Geräten ist stets ein Abwägen von Kosten und Nutzen. Jedoch ist eines klar: IoT-Geräte müssen vor Angriffen geschützt werden. (fr)