Erweiterte Security für LPWAN-Geräte

Security-Grundlagen für Entwickler

Jürgen Messerer, bbv Software Services AG

In unserem digitalen Zeitalter sind wir überall von Vernetzung umgeben. Jeder und alles tauscht sich untereinander aus. Ein sehr wichtiger Bestandteil dieser digitalen Vernetzung ist das IoT mit zahllosen Anwendungsfällen. Jedoch lässt sich nicht jeder Anwendungsfall mit einer einzigen Technologie realisieren. Für IoT-Geräte steht eine Vielfalt von diversen Wireless-Lösungen zur Verfügung. Um die geeignetsten Technologien auszuwählen, müssen verschiedene Kriterien. wie z.B. Reichweite, Datenrate, Security und Lizenzmodell, berücksichtigt werden. Eine Technologie, die diese Kriterien berücksichtigt und dabei unkompliziert und vielseitig einsetzbar ist, ist das Low-Power Wide Area Network, kurz LPWAN. LPWAN verfügt über eine hohe Batterielebensdauer bei großer Abdeckung und niedriger Durchsatzrate. Doch wie sieht es mit Security aus? Erleben wir wieder das Gleiche wie bei anderen IoT-Geräten, wo die Security nur spärlich oder gar nicht umgesetzt wurde?

In diesem Artikel wird gezeigt, worauf geachtet werden muss, damit die LPWAN-Geräte von morgen nicht sofort als Bots von nicht autorisierten Personen umkonfiguriert werden.

Einführung

Sicherheit (engl. Security) bedeutet, dass man sich in einem Zustand befindet, der praktisch frei von Bedrohungen und Gefahren ist. Doch je komplexer ein System ist, desto schwieriger bis unmöglich wird es, diesen Zustand zu erreichen. Das Gebiet der Computertechnik ist solch ein komplexes System, das sich zudem noch ständig weiterentwickelt. Weil immer häufiger Schutzmaßnahmen umgangen oder gebrochen werden, muss von Anfang an ein Sicherheitskonzept zur Wahrung der Vertraulichkeit, Verfügbarkeit und der Integrität erstellt werden. Dabei müssen auch zukünftige Sicherheitsangriffe in Betracht gezogen werden, die gegenwärtig noch nicht einmal bekannt sind. Security darf nie als Option angesehen werden! Auch ist es sehr unpraktikabel, Security im Nachhinein nachzurüsten, weil dadurch die Herstellungskosten exponentiell ansteigen würden.

Security Audit/Beurteilung

Es ist wichtig, durch gezielte Fragen einen Überblick über die Sicherheit eines Produkts zu erhalten. Anhand der folgenden vereinfachten Fragen kann schon einiges über das Sicherheitskonzept eines Gerätes gesagt werden.

Physical Assessment

- Ist das Gerät gegen nicht autorisierten Zugriff geschützt?
- Sind die Schnittstellen geschützt?

*Access Control Assessmen*t

- Wer hat alles Zugriff auf das Gerät und mit welcher Zutrittsberechtigung?
- Wird der Zugriff geloggt?

Vulnerability Assessment

- Welche Software läuft auf dem Gerät und welches sind bekannte Schwachstellen?
- Wie werden wir über Sicherheitsprobleme benachrichtigt?

*Network Security Assessmen*t

- Werden die Daten an den autorisierten Server gesendet?
- Wie wird die Identität des Servers verifiziert?
- Werden die Daten verschlüsselt übertragen?
- Sind andere Netzwerk-Services geschützt?

Software Update Process Assessment

- Wie werden Softwarefehler beseitigt und wie werden Updates sicher verteilt?
- Wie wird sichergestellt, dass keine fremde Software auf den Geräten läuft?
- Ist das erhaltene Software-Update von einer vertrauenswürdigen Quelle empfangen worden?
- Ist die Integrität des Updates nicht kompromittiert worden?

Key Management Assessment

- Wie und wo werden die Schlüssel gespeichert?
- Wie sieht der Lebenszyklus der Schlüssel aus?

Sicherheitsschwächen in LPWAN-Implementierungen
Sehen wir uns das bei einem stromsparenden Gerät wie einem LPWAN-Gerät an, das batteriebetrieben ist und nur über eine geringe Rechenleistung und geringen Speicher verfügt. LPWAN-Protokolle und deren Implementierungen, wie LoRaWAN, Sigfox, Weightless-P, RPMA und NB-IoT, verfügen über gewisse Sicherheitseigenschaften, die nur einen kleinen Teil des zuvor aufgelisteten Assessments abdecken. Im Großen und Ganzen kann man sagen, dass alle Protokolle ein Verschlüsseln und Entschlüsseln der Daten mit Hilfe von AES, sprich symmetrischen Schlüsseln, verwenden. Doch leider werden in den Referenzimplementierungen diese Schlüssel statisch in den Geräten hinterlegt. Es gibt keine Möglichkeit, diese Schlüssel bei Bedarf zu ersetzen. Die einzige Möglichkeit besteht darin, die Schlüssel physikalisch abzulösen. Eine weitere Sicherheitsschwäche liegt in der Unmöglichkeit, ein Software-Update über die Luft zu verteilen. Häufig wird aus Kostengründen auch auf das Speichern der Schlüssel in einem sicheren Speicher verzichtet. Wie können nun diese Schwächen der LPWAN Security behoben werden?

- Sicheres Speichern der symmetrischen Schlüssel
- Symmetrische Schlüssel der LPWAN-Geräte updaten
- Sicheres Software-Update über die Luft

Security by Design
Sicherheit fängt schon beim Hardware-Design an. Die Schlüssel müssen in einem sicheren Memorybereich gespeichert werden. Um dies zu erreichen, ist es von Vorteil, einen Sicherheits-Chip einzusetzen. Die Firma Microchip, ehemals Atmel, besitzt eine ganze Serie solcher Sicherheits-Chips, die jeder für sich ein ganz bestimmtes Sicherheitssegment abdecken. Sicherheits-Speicher-Chips wie der AT88SCxxxx eignen sich hervorragend für das sichere Speichern der symmetrischen Schlüssel und liegen mit 50Cent/1000Stk in einem kostengünstigen Preissegment. Aber wie sieht es mit dem Schlüsselupdate über die Luft aus?

Um ein Schlüsselupdate über einen nicht sicheren Kanal wie über die Luft zu ermöglichen, werden weitere Sicherheitsmechanismen benötigt. Zum Glück sind solche Sicherheitsmechanismen schon seit mehr als 20 Jahren bekannt. Damit die symmetrischen Schlüssel sicher durch die Luft ausgetauscht werden können, muss ein sicherer Kanal aufgebaut werden. Dazu wird seit Jahren das Diffie-Hellman-Verfahren angewendet, welches auf asymmetrischen Schlüsseln basiert. Im Gegensatz zu der Verschlüsselung mit symmetrischen Schlüsseln ist das asymmetrische Verschlüsseln rechenintensiver und verbraucht dadurch auch mehr Energie. Daher wird für batteriebetriebene Geräte eine abgewandelte Form des Diffie-Hellman-Verfahrens angewendet: das sogenannte Elliptic-Curve-Diffie-Hellman-Verfahren (ECDH), welches auf elliptischen Kurven basiert und dadurch weniger rechenintensiv und stromsparender ist. Mit diesem Verfahren ist erst einmal nur der Austausch gesichert, aber nicht, ob der Sender wirklich der ist, dem wir vertrauen.

Zum Glück gibt es auch hier ein Verfahren, das sich schon seit Jahren bewährt hat. Der sogenannte Elliptic Curve Digital Signature Algorithm (ECDSA), der eine abgewandelte

Form des herkömmlichen Digital Signature Algorithm darstellt. Durch diese beiden Verfahren, ECDH und ECDSA, ist ein sicherer Schlüsselaustausch über die Luft gewährleistet. Auch hier bietet Microchip eine kostengünstige Lösung an, den ATECC508A Crypto Authentication Chip. Dieser Chip bietet neben dem sicheren Speichern der Schlüssel zusätzlich ein einfach zu benutzendes Interface für den Schlüsselaustausch mittels ECDH und ECDSA. Ein mögliches Hardware-Design könnte wie folgt aussehen:

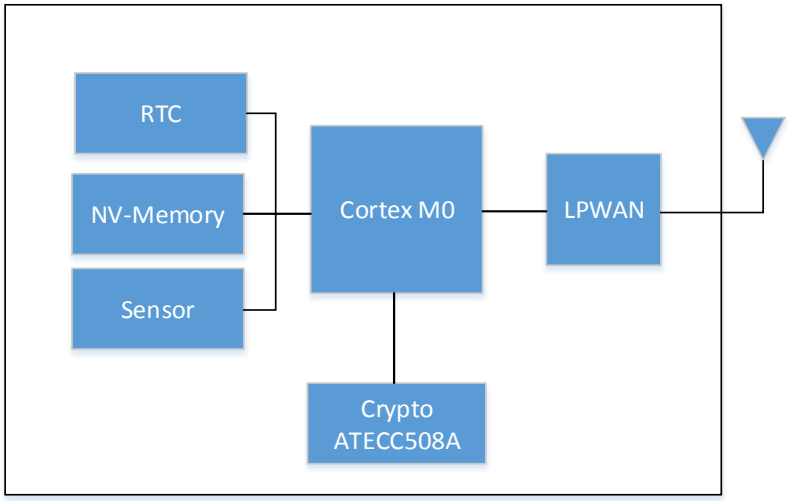

Abb. 1: Blockdiagramm eines LPWAN-Gerätes

Mit Hilfe von ECDH und ECDSA ließe sich auch ein sicheres Software-Update über die Luft realisieren. In gewissen Implementierungen wird nur ein eingeschränkter Downlink angeboten. Sollte dies der Fall sein, muss überprüft werden, ob ein Schlüsselupdate überhaupt möglich ist und damit die Sicherheitsanforderungen erfüllt werden. Weiter existiert in den meisten LPWAN-Protokollen kein Broadcast an alle. Organisationen wie die LoRa-Alliance haben diese Schwächen erkannt und erweitern die Protokollspezifikation um genau diese Eigenschaft.

Zusammenfassung/Fazit

Die LPWAN-Protokolle und deren Implementierungen sind aus Security-Sicht unzureichend. Mit Hilfe eines dedizierten Crypto-Chips, wie dem ATECC508a der Firma Microchip, ist es möglich, Funktionen wie ECDH und ECDSA auf solchen LPWAN-Geräten und deren Implementierungen nachzurüsten. Dadurch wird die Sicherheit dieser Geräte deutlich erhöht.

Autor
Jürgen Messerer arbeitet bei der bbv Software Services AG als Embedded Software Architekt. Seine Schwerpunkte liegen in kleinen wie in großen Embedded-Systemen sowie in der Applikationsentwicklung mit C++ und Qt5.

Kontakt
Internet: www.bbv.ch
E-Mail: juergen.messerer@bbv.ch