FAKTEN UND MISSVERSTÄNDNISSE ZUM THEMA SICHERHEIT

PHYSISCHE SICHERHEIT BEI LoRaWAN®-GERÄTEN

Der AppKey-Schlüssel und die abgeleiteten Sitzungsschlüssel sind im nichtflüchtigen Speicher eines LoRaWAN-Gerätes abgelegt. Ihr Schutz ist daher davon abhängig, wie der Zugriff auf diesen Speicher geschützt ist. Bei möglicher physischer Gefahr kann ein vor Manipulation sicherer Speicher (Secure Element) eingesetzt werden, der das Auslesen der Schlüssel extrem erschwert.

KRYPTOGRAPHIE

Einige Quellen behaupten, LoRaWAN nutze nur eine XOR-Verknüpfung statt AES.[1] Tatsächlich nutzt LoRaWAN, wie bereits erwähnt, das standardisierte AES-CTR-Verfahren, das wie andere AES-Verfahren (z.B. CBC[5]) die XOR-Verknüpfung nutzt. Dies verstärkt die AES-Verschlüsselung, da für jeden Datenblock ein einmaliger Schlüssel verwendet wird.

SCHLÜSSELVERTEILUNG

Da der AppSKey und der NwkSKey vom selben AppKey abgeleitet werden, könnte man argumentieren, dass der Netzwerkbetreiber, wenn er im Besitz des AppKey sein sollte, auch den AppSKey berechnen und den Datenverkehr entschlüsseln könne. Um dies zu vermeiden, kann die Speicherung des AppKey-Schlüssels und die Ableitung der Sitzungsschlüssel auf einem vom Netzwerkserver getrennten System durchgeführt werden.
Um Netzwerkbetreibern noch mehr Flexibilität zu geben, gibt es ab der LoRaWAN-Version 1. zudem zwei getrennte Hauptschlüssel: den NwkKey für den Netzwerkbetreiber und den AppKey für die Anwendung.

SICHERHEIT DER BACKEND-SCHNITTSTELLEN

Die Backend-Schnittstellen beinhalten die Kommunikation zwischen Netzwerkserver und Anwendungsserver. Es werden HTTPS und VPN-Technologien eingesetzt, um wie in anderen Telekommunikationssystemen die sichere Kommunikation zwischen diesen kritischen Infrastruktur-Elementen zu garantieren.

IMPLEMENTIERUNGS- UND BETRIEBSSICHERHEIT

Die LoRa Alliance arbeitet stetig daran, die Sicherheit der LoRaWAN Protokoll- und Architekturspezifikationen weiterzuentwickeln. Trotzdem muss darauf hingewiesen werden, dass die Gesamtsicherheit auch von der konkreten Implementierung und dem Betrieb abhängt.
Implementierungsprobleme liegen in der Verantwortung des jeweiligen Herstellers und Betriebsprobleme im Verantwortungsbereich des jeweiligen Netzwerkbetreibers.
Diese beiden Problemfelder sind nicht LoRaWAN-spezifisch und betreffen auch jede andere Funktechnologie, wenn sie auf denselben Plattformen bzw. Netzwerken betrieben wird.

WIE DIESES WHITE PAPER ZEIGT, WURDE LoRaWAN VON ANFANG AN MIT SICHERHEIT ALS ESSENTIELLEM ASPEKT ENTWORFEN, UM DEN ANFORDERUNGEN VON MODERNEN, SICHEREN, HOCH SKALIERBAREN UND ENERGIEEFFIZIENTEN IOT-NETZWERKEN GERECHT ZU WERDEN.
LoRaWAN BIETET IM GEGENSATZ ZU VIELEN ANDEREN IOT-TECHNOLOGIEN BEREITS EINE ENDE-ZU-ENDE-VERSCHLÜSSELUNG.

LoRa Alliance™

LoRaWAN® Specification, v1.0.2, July 2016
LoRa Alliance™: **www.lora-alliance.org**
marcom@lora-alliance.com

[1] AES – Advanced Encryption Standard. AES ist ein standardisierter Algorithmus zur Verschlüsselung und Authentifizierung auf Basis symmetrischer Schlüssel. [2] CMAC - Cipher-based Message Authentication Code. [3] CTR - Counter Mode Encryption. Einsatzmodus des AES-Verfahrens, das einen Nachrichtenzähler nutzt, um Datenströme blockweise zu verschlüsseln. [4] AES-CMAC - Cipher-based Message Authentication Code ist ein Einsatzmodus des AES-Verfahrens, der Datenintegrität und Datenauthentizität sicherstellt. [5] CBC ist ein Einsatzmodus des AES-Verfahrens, der einen Initialisierungsvektor und den vorangegangenen Datenblock nutzt, um Datenströme zu verschlüsseln.

LoRaWAN®

LoRaWAN® SICHERHEIT

VOLLSTÄNDIGE ENDE–ZU–ENDE VERSCHLÜSSELUNG FÜR IOT-ANWENDUNGSANBIETER

LoRa Alliance™

EINE VERÖFFENTLICHUNG ERSTELLT FÜR DIE LoRa ALLIANCE™
von GEMALTO, ACTILITY UND SEMTECH
Februar 2017

INS DEUTSCHE ÜBERSETZT
von DIGIMONDO, LORIOT, MINOL ZENNER GROUP UND TELENT
Mai 2019

EINLEITUNG

LoRaWAN® ist ein Verbindungsprotokoll für energiesparende Weitverkehrsnetze (Low Power Wide Area Networks - LPWAN), das kostengünstige, mobile, sichere und bidirektionale Kommunikation für das Internet der Dinge (IoT), Maschine-zu-Maschine-Kommunikation (M2M), Smart City und industrielle Anwendungen unterstützt. Das LoRaWAN-Protokoll ist für niedrigen Energieverbrauch optimiert und wurde entworfen, um große Netzwerke mit Millionen von Endgeräten zu ermöglichen. Die innovativen Eigenschaften von LoRaWAN unterstützen redundante Betriebsmodi, Geolokation sowie kosten- und energieeffiziente Anwendungen. Endgeräte können sogar über „Energy Harvesting"-Technologien (Energiegewinnung aus der Umgebung) betrieben werden, die besonders einfache, anwenderfreundliche und mobile IoT-Applikationen ermöglichen. Sicherheit und verschlüsselte Übertragung sind fundamentale Voraussetzungen für IoT-Applikationen. Deshalb wurde dieser Aspekt von Anfang an bei der Konzeption der LoRaWAN-Spezifikation priorisiert. Das komplexe Thema Sicherheit muss auf verschiedensten Stufen berücksichtigt werden – insbesondere beim verwendeten kryptographischen Verfahren.
Dieses White Paper dokumentiert die Sicherheitsmechanismen, welche in der LoRaWAN-Spezifikation festgelegt sind. Im Detail werden die Implementierung von Sicherheitsaspekten sowie das LoRaWAN-Sicherheitskonzept beleuchtet.

EIGENSCHAFTEN DER LoRaWAN-SICHERHEITSMECHANISMEN

Die LoRaWAN-Sicherheitsmechanismen wurden speziell nach den Kriterien von LoRaWAN entworfen: Energieeffizienz, geringe Implementierungskomplexität, Kosteneffizienz und hohe Skalierbarkeit. Da die Endgeräte in einem sehr langen Zeitraum zum Einsatz kommen, müssen die Sicherheitsmechanismen zukunftssicher sein. Die LoRaWAN-Sicherheitsmechanismen nutzen dem aktuellen Stand der Technik entsprechende, standardisierte und felderprobte Ende-zu-Ende-Verschlüsselungsalgorithmen.
Im Folgenden werden die fundamentalen Eigenschaften, welche die Sicherheit bei LoRaWAN gewährleisten, beschrieben: gegenseitige Authentifizierung, Datenintegrität und Geheimhaltung.
Die gegenseitige Authentifizierung von LoRaWAN-Endgerät und LoRaWAN-Netzwerkserver wird im Zuge der Netzwerkanmeldung sichergestellt (Join-Prozedur). Dadurch wird gewährleistet, dass nur echte und authentische Geräte an ebensolchen Netzwerken angemeldet werden können.
Bei Nachrichten, welche über LoRaWAN-MAC-Layer und den LoRaWAN-Application-Layer gesendet werden, werden die Herkunft authentifiziert, die Integrität geschützt, Replay-Attacken verhindert und Inhaltsdaten verschlüsselt. Diese Sicherheitsmechanismen, kombiniert mit der gegenseitigen Authentifizierung, stellen sicher, dass der Netzwerkverkehr nicht von Dritten verändert wurde, von einem legitimen Endgerät kommt, für Lauscher nicht verwendbar ist und nicht von Dritten aufgezeichnet und erneut gesendet werden kann.
Zusätzlich wird bei LoRaWAN die Kommunikation zwischen Netzwerkservern und Anwendungsservern verschlüsselt. LoRaWAN ist eines der wenigen IoT-Protokolle, das Ende-zu-Ende-Verschlüsselung sicherstellt. In einigen Mobilfunknetzen sind die Nachrichten nur über Funk verschlüsselt und werden ab der Basisstation im Netzwerk des Providers unverschlüsselt übertragen. Dies führt dazu, dass der Anwender sich selber um eine zusätzliche Verschlüsselungsebene kümmern muss (meist wird dies über eine Art VPN oder Anwendungs-Schichtverschlüsselung wie TLS realisiert). Diese zusätzliche Verschlüsselungsschicht eignet sich nicht für LoRaWAN, da sie erhöhten Energieverbrauch, Komplexität und zusätzliche Kosten verursacht.

IMPLEMENTIERUNG DER SICHERHEITSMECHANISMEN

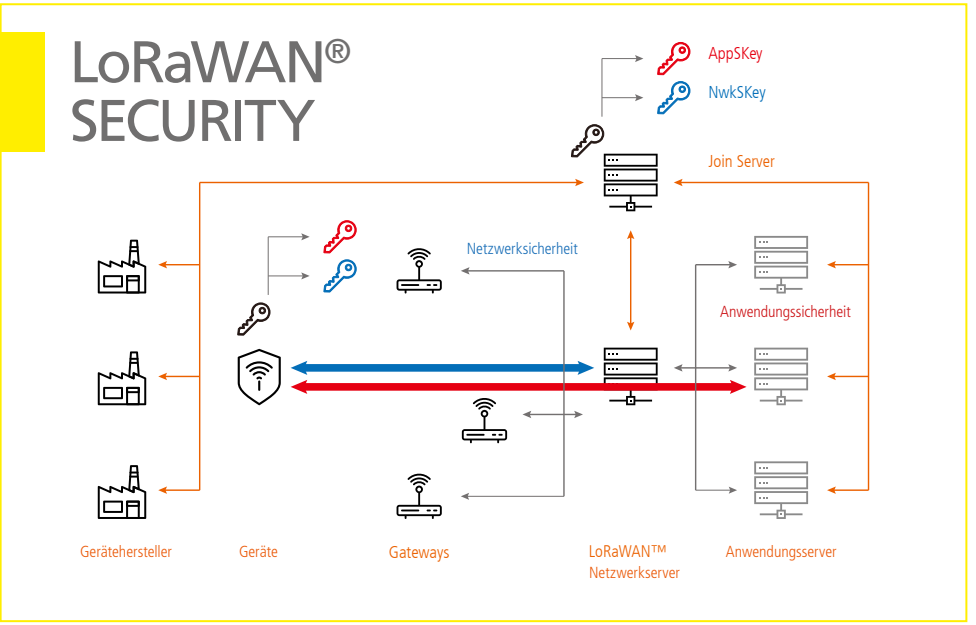
Die zuvor genannten Sicherheitsmechanismen basieren auf den bewährten und standardisierten kryptographischen AES-Algorithmen. Diese Algorithmen werden seit vielen Jahren von der kryptographischen Gemeinschaft analysiert, sind NIST-zugelassen und gelten allgemein als beste Sicherheitspraxis für resourcenlimitierte Geräte und Netzwerke. LoRaWAN verwendet das kryptographische AES-Verfahren in Kombination mit mehreren Betriebsarten: CMAC[2] für Integritätsschutz und CTR[3] für Verschlüsselung. Jedes LoRaWAN-Gerät ist mit einem eindeutigen 128-Bit-AES-Schlüssel (AppKey genannt) und einer global eindeutigen Kennung (EUI-64-basierte DevEUI) personalisiert, die beide während der Geräteauthentifizierung verwendet werden. Die Zuweisung von EUI-64 Identifikatoren erfordert, dass der Zuweiser über einen Organizationally Unique Identifier (OUI) der IEEE-Registrierungsbehörde verfügt. Ebenso werden LoRaWAN-Netzwerke durch eine global eindeutige 24-Bit-Kennung identifiziert, die durch die LoRa Alliance™ vergeben wird.

SCHUTZ DER ANWENDUNGSDATEN

LoRaWAN®-Anwendungsdaten sind immer Ende-zu-Ende vom Gerät bis zum Anwendungsserver verschlüsselt. Die Integrität wird schrittweise sichergestellt: Zunächst vom Endgerät bis zum Netzwerkserver über die LoRaWAN-Sicherheitsmechanismen, dann vom Netzwerkserver zum Anwendungsserver über eine sichere Transportschicht, z.B. HTTPS oder VPN.

GEGENSEITIGE AUTHENTIFIZIERUNG

Im Rahmen der sogenannten Over-the-Air-Aktivierung (auch Join-Prozedur genannt) findet eine Authentifizierung zwischen Endgerät und Netzwerkserver statt. Dafür wird der AppKey verwenden, der auf beiden Seiten bekannt sein muss. Die Authentifizierung erfolgt über eine AES-CMAC[4]-Berechnung mit dem AppKey auf dem Gerät und auf dem empfangenden Netzwerkserver. Anschließend werden zwei Sitzungsschlüssel abgeleitet: Ein Schlüssel zur Integritätsprüfung und Verschlüsselung von MAC-Befehlen (NwkSKey) und ein Schlüssel zur Ende-zu-Ende-Verschlüsselung (AppSKey) des Payloads. Der NwkSKey wird dem Netzwerkserver mitgeteilt, damit dieser die Integrität und Authentizität der Nachrichten prüfen kann. Der AppSKey wird auf dem Anwendungsserver zur Ver- und Entschlüsselung verwendet. AppKey und AppSKey müssen dem Netzbetreiber nicht mitgeteilt werden, so dass dieser nicht in der Lage ist, die Anwendungsdaten zu entschlüsseln.



DATENINTEGRITÄT UND GEHEIMHALTUNG

Der komplette Datenverkehr von LoRaWAN wird mit zwei Sitzungsschlüsseln geschützt. Jedes Nutzdatenpaket (Payload) wird über AES-CTR verschlüsselt und um eine Nachrichtennummer (Frame Counter) sowie einen „Message Integrity Code" (MIC) ergänzt. Der MIC wird mit AES-CMAC berechnet, um eine Manipulation der Daten auszuschließen. In dieser Skizze wird die Struktur eines LoRaWAN-Paketes dargestellt: