LoRaWAN™

LoRaWAN™ SECURITY

FULL END–TO–END ENCRYPTION FOR IoT APPLICATION PROVIDERS

A WHITE PAPER PREPARED FOR THE LoRa ALLIANCE™

BY GEMALTO, ACTILITY AND SEMTECH

February 2017

LoRa Alliance™
Wide Area Networks for IoT

INTRODUCTION

LoRaWAN™ is a Low Power Wide Area Network (LPWAN) protocol that supports low-cost, mobile, and secure bi-directional communication for Internet of Things (IoT), machine-to-machine (M2M), smart city, and industrial applications. The LoRaWAN protocol is optimized for low power consumption and is designed to support large networks with millions of devices. Innovative LoRaWAN features include support for redundant operation, geolocation, low-cost, and low-power applications. Devices can even run on energy harvesting technologies enabling the mobility and ease of use of IoT.

As security is a fundamental need in all of the aforementioned applications, it has been designed into the LoRaWAN specification from the very beginning. However, the topic of security encompasses multiple properties and, in particular, the cryptographic mechanisms used to implement security in LoRaWAN deserve careful explanation. This whitepaper aims to present the security of the current LoRaWAN specification. First, we will present the security properties embodied in the LoRaWAN specifications, then details of its implementation and finally some explanations about LoRaWAN security design.

PROPERTIES OF LoRaWAN™ SECURITY

LoRaWAN security is designed to fit the general LoRaWAN design criteria: low power consumption, low implementation complexity, low cost and high scalability. As devices are deployed in the field for long periods of time (years), security must be future-proof. The LoRaWAN security design adheres to state-of-the-art principles: use of standard, well-vetted algorithms, and end-to-end security. Later, we describe the fundamental properties that are supported in LoRaWAN security: mutual authentication, integrity protection and confidentiality.

Mutual authentication is established between a LoRaWAN end-device and the LoRaWAN network as part of the network join procedure. This ensures that only genuine and authorized devices will be joined to genuine and authentic networks.

LoRaWAN MAC and application messaging are origin authenticated, integrity protected, replay protected, and encrypted. This protection, combined with mutual authentication, ensures that network traffic has not been altered, is coming from a legitimate device, is not comprehensible to eavesdroppers and has not been captured and replayed by rogue actors.

LoRaWAN security further implements end-to-end encryption for application payloads exchanged between the end-devices and application servers. LoRaWAN is one of the few IoT networks implementing end-to-end encryption. In some traditional cellular networks, the traffic is encrypted over the air interface, but it is transported as plain text in the operator's core network. Consequently, end users are burdened by selecting, deploying and managing an additional security layer (generally implemented by some type of VPN or application layer encryption security such as TLS).

This approach is not suited in LPWANs where over-the-top security layers add considerable additional power consumption, complexity and cost.

SECURITY IMPLEMENTATION

The security mechanisms mentioned previously rely on the well-tested and standardized AES[1] cryptographic algorithms. These algorithms have been analysed by the cryptographic community for many years, are NIST approved and widely adopted as a best security practice for constrained nodes and networks. LoRaWAN security uses the AES cryptographic primitive combined with several modes of operation: CMAC[2] for integrity protection and CTR[3] for encryption. Each LoRaWAN device is personalized with a unique 128 bit AES key (called AppKey) and a globally unique identifier (EUI-64-based DevEUI), both of which are used during the device authentication process. Allocation of EUI-64 identifiers require the assignor to have an Organizationally Unique Identifier (OUI) from the IEEE Registration Authority. Similarly, LoRaWAN networks are identified by a 24-bit globally unique identifier assigned by the LoRa Alliance™.

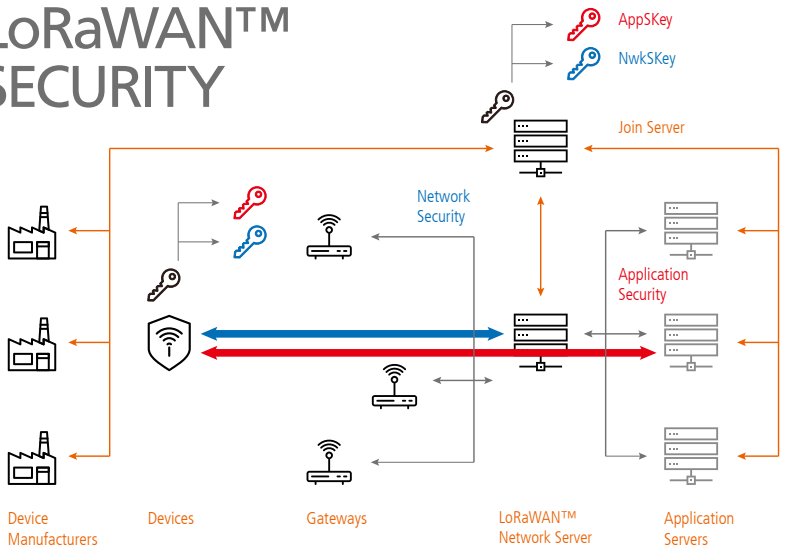
SECURING APPLICATION PAYLOADS

LoRaWAN™ application payloads are always encrypted end-to-end between the end-device and the application server. Integrity protection is provided in a hop-by-hop nature: one hop over the air through the integrity protection provided by LoRaWAN protocol and the other hop between the network and application server by using secure transport solutions such as HTTPS and VPNs.

MUTUAL AUTHENTICATION

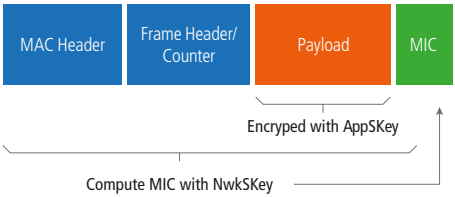
The Over-the-Air Activation (a.k.a. Join Procedure) proves that both the end device and the network have the knowledge of the AppKey. This proof is made by computing an AES-CMAC[4] (using the AppKey) on the device's join request and by the backend receiver. Two session keys are then derived, one for providing integrity protection and encryption of the LoRaWAN MAC commands and application payload (the NwkSKey), and one for end-to-end encryption of application payload (the AppSKey). The NwkSKey is distributed to the LoRaWAN network in order to prove/verify the packets authenticity and integrity. The AppSKey is distributed to the application server in order to encrypt/decrypt the application payload. AppKey and AppSKey can be hidden from the network operator so that it is not able to decrypt the application payloads.

LoRaWAN™ SECURITY



DATA INTEGRITY AND CONFIDENTIALITY PROTECTION

All LoRaWAN traffic is protected using the two session keys. Each payload is encrypted by AES-CTR and carries a frame counter (to avoid packet replay) and a Message Integrity Code (MIC) computed with AES-CMAC (to avoid packet tampering). See beside the structure of a LoRaWAN packet and its protection:



SECURITY FACTS AND FALLACIES

PHYSICAL SECURITY OF A LoRaWAN™ DEVICE

AppKey and the derived session keys are persistently stored on a LoRa Alliance™ device and their protection depends on the device physical security. If the device is subject to physical threats, keys can be protected in tamper resistant storage (a.k.a. Secure Element), where they will be extremely difficult to extract.

CRYPTOGRAPHY

Some sources claim that LoRaWAN™ cryptography only uses XOR and not AES. In fact, as already mentioned, AES is used in the standardised CTR mode which makes use of XOR crypto operations (as many other modes like CBC[5]). This strengthens the AES algorithm by using a unique AES key for each block cipher.

SESSION KEY DISTRIBUTION

As AppSKey and NwkSKey are generated from the same AppKey, one could argue that if the LoRaWAN operator has the AppKey, it is able to derive the AppSKey and hence to decrypt the traffic. In order to avoid this situation, the server managing the AppKey storage, mutual authentication and key derivation can be run by an entity outside the control of the operator. In order to give operators additional flexibility, a future release of the LoRaWAN specification (1.1) defines two independent master keys: one for the network (NwkKey) and one for the applications (AppKey).

BACKEND INTERFACES SECURITY

The backend interfaces involve control and data signaling among network and application servers. HTTPS and VPN technologies are used for securing the communication among these critical infrastructure elements, much the same way done in any other telecom systems.

IMPLEMENTATION AND DEPLOYMENT SECURITY

The LoRa Alliance works towards ensuring its protocol and architecture specifications are secure, while recognizing that the overall security of the solution also depends on the specific implementation and deployment. Implementation security issues need to be taken up by the relevant manufacturers and deployment issues need to be taken up by the relevant network operators. These two types of issues are not specific to the LoRaWAN technology and usually equally applicable to any radio technology implemented on the same platforms/networks.

AS SHOWN IN THIS PAPER, THE LoRaWAN™ SPECIFICATION HAS BEEN DESIGNED FROM THE ONSET WITH SECURITY AS AN ESSENTIAL ASPECT, PROVIDING STATE-OF-THE-ART SECURITY PROPERTIES FOR THE NEED OF HIGHLY-SCALABLE LOW POWER IOT NETWORKS. UNLIKE MANY OTHER IOT TECHNOLOGIES, IT ALREADY OFFERS DEDICATED END-TO-END ENCRYPTION TO APPLICATION PROVIDERS.

LoRa Alliance™

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

[1] AES - Advanced Encryption Standard. It is a public encryption algorithm based on symmetric secret keys, allowing message encryption and authentication. [2] CMAC - Cipher-based Message Authentication Code. [3] CTR - Counter Mode Encryption. It is a mode of operation of AES algorithm relying on a counter to encrypt streams of data. [4] AES-CMAC - Cipher-based Message Authentication Code using AES encryption algorithm to provide message integrity and authenticity. [5] CBC is a mode of operation of AES algorithm relying on an initialization vector and the previous data block to encrypt streams of data.