LoRaWAN Security

Alper Yegin

Director of Standards and Advanced Technology Development, Actility
Technical Committee Co-chair and Vice-Chair, LoRa Alliance
Is LoRaWAN secure?
How are the LoRaWAN protocol/networks secured?
General Wireless Security

<table>
<thead>
<tr>
<th>Threats</th>
<th>Remedies (tools)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized access</td>
<td>Mutual end-point authentication</td>
</tr>
<tr>
<td>Spoofing</td>
<td>Data origin authentication</td>
</tr>
<tr>
<td></td>
<td>Replay protection</td>
</tr>
<tr>
<td>Modification</td>
<td>Integrity protection</td>
</tr>
<tr>
<td>Eavesdropping</td>
<td>Encryption</td>
</tr>
</tbody>
</table>

... using cryptographic algorithms with strong keys
Mutual End-point Authentication

Using Advanced Encryption Standard (AES) with 128-bit symmetric keys and algorithms

AppKey is random and per-device root key (cryptographic isolation)

DevEUI: Device Extended Unique Identifier
JoinEUI: Join server Extended Unique identifier (replaces AppEUI in earlier specs)
Note -- Depicting LoRaWAN 1.0.x for brevity
Mutual End-point Authentication

Using Advanced Encryption Standard (AES) with 128-bit symmetric keys and algorithms

AppKey is random and per-device root key (cryptographic isolation)

AS: Application Server
JS: Join Server
NS: Network Server
GW: Gateway

LoRaWAN Join/Activation Procedure
Session Key Generation and Delivery

LoRaWAN Join/Activation Procedure

Device

GW

NS

JS

Application

Network

AS

AppSKey
DevEUI

NwkSKey
DevAddr,DevEUI

AES-128 symmetric session keys
Data Origin Authentication, Integrity and Replay Protection

Uplink/downlink frame transmission

MIC: Message Integrity Code
Payload Encryption + Data Origin Auth, Integrity/Replay Protection

**MIC:** Message Integrity Code
AES-CCM*: AES Counter with Cipher Block Chaining Message Authentication Code, * is for encryption-only variation defined in Zigbee standard
LoRaWAN End-to-end (Transport) Security

Device <-> LoRaWAN security <-> Backend security (IPsec, TLS, firewall, etc.) <-> AS

Note 1 – “Integrity protection” represents “data origin authentication, integrity & replay protection”

Note 2 – Supports encryption of MAC commands between the device and the NS

Note 3 – Application-layer end-to-end integrity protection is left to the apps as an option
LoRaWAN End-to-end (Transport) Security

Communication protocol design.
Overall/Complete Security

Communication protocol design, implementation, deployment.

Application security, Device HW/SW platform security, Infra platform security.
Network-agnostic Provisioning

Device manufacturer

DevEUI
JoinEUI
AppKey

Device

Network1

Network2

Network3

GWs

NSs

JS

DevEUI
JoinEUI
AppKey
Deployment Flexibility

Various options for where the JS of a Device can be hosted
Hardware Security

Device manufacturer

SE (Secure Element)  Device

GW  NS

HSM (Hardware Security Module)

JS
OTAA vs ABP

OTAA (Over-the-Air Activation) dynamically generates session keys from root keys.

ABP (Activation by Personalization) devices are provisioned with session keys for a pre-selected network.

Prefer OTAA because:
- ABP device can only work with a single network in its whole life
- ABP device cannot rekey sessions
LoRaWAN 1.1 Improvements

- Additional replay protection
- Separation of security realms
- Enhanced key management

- 32bit FCnt, disallow ABP FCnt reset, no DL retransmit, UL MIC bound to TxDr/TxCh, counter-based Join nonce values, Ack frame MIC uses Acked FCnt
- Distinct root keys and FCntDown for App and Nwk, UL MIC check in "stateful" visited network
- Richer key hierarchy with purpose-built session keys, re-keying w/o resetting data session
LoRaWAN 1.1 Improvements

- Additional replay protection
- Separation of security realms
- Enhanced key management

Applied to LoRaWAN 1.0.x: “Technical Recommendations for Preventing State Synchronization Issues around LoRaWAN™ 1.0.x Join Procedure”

- 32bit FCnt, disallow ABP FCnt reset, no DL retransmit, UL MIC bound to TxDr/TxCh, counter-based Join nonce values. Ack frame MIC uses Aced FCnt
- Distinct root keys and FCntDown for App and Nwk, UL MIC check in "stateful" visited network
- Richer key hierarchy with purpose-built session keys, re-keying w/o resetting data session

lora-alliance.org/resource-hub/technical-recommendations-preventing-state-synchronization-issues-around-lorawan-10x

Copyright ©Actility
Firmware Update over the Air (FUOTA)

Security for FUOTA

Signed firmware

Integrity-protected multicast delivery (using group key)

Integrity-protected unicast commands (using device key)

FUOTA for Security

Update device with software/firmware (security) patches in the field
DOs and DONTs

- Pick secret keys randomly and per-device, deliver and store securely
- Don’t use arbitrary DevEUIs (respect IEEE OUIs)
- Don’t use arbitrary DevAddrs (respect LoRa Alliance NetID/NwkID allocations)
- Don’t use arbitrary JoinEUI/AppEUI (must point to a real JS with legitimate IEEE OUI)
- Use trusted OS/ HW security for sensitive apps
- Ensure end-to-end, whole-stack system security

- Contribute to Technical Committee
  - Finding issues & proposing solutions
  - On-going work
    - QR code for facilitating device provisioning
    - Over-the-air device personalization

OUI: Organizationally Unique Identifier
• Leading LoRaWAN system vendor
  • Over half of national public networks globally powered by ThingPark platform
• Most comprehensive product/service portfolio
• LoRa Alliance leadership
  • Founding member, Alliance Vice-chair, Board Member, Technical Committee Co-chair, Developer Community WG Chair, and active across all groups
• Developer network
  • 1000+ registered members
• B2B marketplace
  • 150+ sellers
ThingPark and Security

ThingPark Activation

Device Manufacturers
SE Partners

AEP

DX Decoders
DX Engines
DX Connectors

HSM Partners

ThingPark Enterprise
Large Manufacturers
Vertical players
Enterprise networks

ThingPark Wireless
Public Service Provider Networks

ThingPark Market

Actility

ThingPark Activation webinar: www.youtube.com/watch?v=mZgTr5VZiuI
Roaming/ThingPark Exchange webinar: www.youtube.com/watch?v=lWP6VV1CKEq
Questions?

www.actility.com