Low Power Wide Area Networks security

Sophia-Antipolis, December 9, 2015
Pierre Girard, Security Solution Expert
Introduction

- LPWAN technologies are booming

- Main drivers
  - Low cost
  - Low power consumption

- High trust level needs to be maintained
Why trust in IoT?

- Management of sensitive devices
  - Valve, pump, door, engine, ...

- Management of sensitive transactions
  - Energy: (not) producing, (not) consuming, storing ...
  - X as a Service: cleaning, manufacturing, flying ...

- Management of sensitive data
  - Location / presence, behavior / consumption patterns, ...
IoT will redefine your business model …

… and you want to protect it!
Main security requirements

- Device / network mutual authentication
- End-to-end applicative level security
<table>
<thead>
<tr>
<th>Requirements</th>
<th>WAN</th>
<th>LPWAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mutual auth.</td>
<td>![Key] + AKA</td>
<td>Too costly</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Too much power</td>
</tr>
<tr>
<td>E2E sec.</td>
<td>![Key] ![Certificate] + TLS</td>
<td>Too costly</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Too much power</td>
</tr>
</tbody>
</table>
The LoRaWAN security example
LoRaWAN device (class A) communication
LoRa architecture
LoRa security

Each device is provisioned with a unique AES 128 key: AppKey.
LoRa security: network connection

A cryptogram (MIC) is computed with AppKey
LoRa security: network connection

A cryptogram (MIC) is also computed with AppKey

Joint accept (…, MIC)

Devices  Gateways  LoRa network server  Application servers
Not a classic challenge / response scheme

- Saves a round trip
- But nonce is generated by the device to be authenticated
- Server-side has to check for replays
LoRa security: network connection

Two session keys are derived: AppSKey and NwkSKey
LoRa security: network connection

NwkSkey is used for network layer security
LoRa security: network connection

**AppSkey** is used for application layer end to end security
LoRaWAN frame content for payloads

<table>
<thead>
<tr>
<th>DevAddr</th>
<th>FCnt</th>
<th>Payload</th>
<th>MIC</th>
</tr>
</thead>
</table>

Encrypted with

Compute MIC with
How to provision the keys?
Problem statement for secure key provisioning

- How to provision the devices / servers without Secure Elements?
- As the same key (AppKey) is used to derive both the network key (NwkSKey) and the applicative key (AppSkey), the network operator and its customers have a conflict of interest:
  - if the network operator knows the device key AppKey, it will be able to compute the AppSkey and thus intercept the applicative data;
  - if the application provider knows the device key AppKey, it will be able to compute the NwkSKey and thus clone devices.

A Trusted Third party is needed!
Introduction of a Trusted Third Party
Device provisioning

AppKey generation

Trusted Third Party

Device manufacturers
Device claiming

Claim device DevEUI

Trusted Third Party

Device manufacturers
Network connection

Trusted Third Party

Joint request (…, MIC)

Device manufacturers
Network connection

Joint request (…, MIC)

Trusted Third Party

Device manufacturers

Network connection diagram with key elements connected to trusted third party, including joint request and device manufacturers.
Network connection

Joint accept (…, MIC)

Trusted Third Party

Device manufacturers
Network connection

Trusted Third Party

Joint accept(..., MIC)

Device manufacturers
Key derivation

Trusted Third Party

Device manufacturers
Key distribution

Trusted Third Party

Device manufacturers
Secure communication with TLS
Conclusion

- LPWAN drivers are low cost and low power
- Trust is needed, more than ever!
- A new trust infrastructure is required
Thanks for your attention