IPsec in Constrained Environments

INSIDE Security
Tero Kivinen
kivinen@iki.fi

Constrained Environments

- Small devices
  - Energy requirements
  - CPU constraints
  - Memory constraints (both RAM and Flash)
- Sensor, Actuator, Smart Object, Smart Device etc.

LWIG Terminology

- Draft-ietf-lwig-terminology gives 3 classes:

Name	Data size (RAM)	Code size (Flash)
Class 0, C0	<< 10 KiB	<< 100 KiB
Class 1, C1	~ 10KiB	~ 100 KiB
Class 2, C2	~ 50KiB	~ 250 KiB

- The devices usually do not have usable UI, might only have single button, or not even that.

Security

- Those small devices do require security
  - They can be in life critical devices, like fire alarms
  - They can be security critical devices, like theft alarms, door openers
  - They can be automation devices, like temperature sensors, thermostats, light switches, etc.
- Currently the security is mostly decided by the vendor, and nobody knows how good it is.

Security Solutions

- Lots of security is only on the link layer
  - 802.15.4 has link encryption, but no key management.
- Vendor proprietary solutions
  - Can use shared keys or even vendor secret group keys.
- Some devices uses TLS or DTLS
- IPsec is also one possibility

IPsec and IEEE 802.15.9

- IEEE 802.15.9 Task group is defining key management for IEEE 802.15.4
  - 802.15.4 do have link encryption AES-CCM*
  - No key management, it is upper layer problem
  - 802.15.9 will define how to wrap existing key management protocols to 802.15.4 frames
    - IKEv2, HIP, PANA, 802.1X, SAE, etc
  - If using IKEv2 for KMP for the link layer, and AES-CCM for link encryption, it would allow using IKEv2 + IPsec for end to end security

Other Internet of Things uses

- Smart Energy and Smart Grid
  - They already use or can use IPsec to protect data

Why use IPsec

- If you remove optional feature it is small
- If you need some optional features, they are already there
  - Rekey, different authentication methods, dead peer detection, multiple SAs etc.
- Can protect any kind of data (UDP, TCP, IP)
- Kernel/usermode split is not that big problem in small devices
- Works well with sleeping nodes