draft-ietf-6tisch-minimal-security

Mališa Vučinić, Inria
Jonathan Simon, Analog Devices
Kris Pister, UC Berkeley
Michael Richardson, Sandelman Software Works
Status

• News
  • draft-ietf-6tisch-minimal-security-03
  • Published on June 15th 2017
  • Implementation with PSKs in OpenWSN completed, Contiki ongoing
  • Summary of updates in -03
Communication Overview

- **Pledge**: fe80::EUI-JP, fe80::EUI-P
- **Join Proxy**: L2 insecure
- **Join Registrar/Coordinator**: bbbb::JRC, bbbb::EUI-JP
- **L2 secure**
Update #1: Security Handshake

- Optional with PSKs
- Mandatory with asymmetric keys
Update #2: How pledge learns JRC address

• Join Proxy (JP) statelessly forwards to JRC
• How JP knows the address of JRC?
  • Learns at join time when it acted as a pledge
  • Join Response now contains the address
  • Omitted if JRC is co-located with DAG root, implied from DODAG ID
  • Assumption: DAG root pre-configured with the address
Update #3: Mandatory to Implement Algorithms

- AEAD algorithm:
  - AES_CCM_16_64_128 from COSE
  - 8 byte authentication tag
  - Corresponds to 802.15.4 CCM* in nonce length

- Hash:
  - SHA-256

- Asymmetric:
  - P-256 Elliptic Curve (secp256r1)
  - ECDSA with SHA-256 signature algorithm
Implementation Status

• In OpenWSN ecosystem with Pre-Shared Keys:
  • draft-ietf-core-object-security-03 in Python
  • draft-ietf-6tisch-minimal-security-03 in Python (JRC)
  • draft-ietf-core-object-security-03 in C
  • draft-ietf-6tisch-minimal-security-03 in C (Pledge and Join Proxy)

• In Contiki:
  • draft-ietf-core-object-security-03
  • draft-ietf-6tisch-minimal-security-03 (ongoing)
  • draft-selander-ace-cose-ecdhe-07 (ongoing)
Implementation Experience

• Issue #1: Problems to fit Join Response in 127 bytes with multiple hops
  • Bottleneck is the link from DAG root to first hop
  • Due to the source routing header, there is a limit on max depth of the network without fragmentation

• Issue #2: Policy by which JP should accept insecure L2 frames from pledges
  • Additional clarifications in the document needed on hooks to lower layers
Issue #1: Packet size

Source Routing Header

Token length set to 0

Object-Security option

Stateless-Proxy option

EUI-64 of Pledge

Content-Format removed

26 + 1 + 1 + 8
Issue #1: Packet size

- Join Response without short and JRC’s address

- 26 bytes to encode key (16 bytes) and key ID (1 byte)
- Uses CBOR + COSE structures
- Can be optimized with compressed COSE approach like used in OSCOAP
Issue #2: Join Proxy Policy

• Proposal: Provide a mechanism to accept insecure L2 packets at JP only upon a trigger (i.e. DAG root button press)

• Needed signal that join is allowed in EB
  • One option to use draft-richardson-6tisch-join-enhanced-beacon
  • Another option to reserve 0xFF of Join Metric in EBs to signal that node will NOT accept insecure L2 frames
    • Upon a trigger, fill Join Metric with the value according to RFC8180 (calculated from the DAG rank)
Conclusion

• PSK variant stable and implementation ready
• Settled down for EDHOC roles in the asymmetric variant, yet to implement
• Implementations of PSK variant available
• Will publish -04 with implementation experience before WGLC
• Reviews welcome