draft-ietf-6tisch-minimal-security

• Authors: Mališa Vučinić (Ed.)
  Jonathan Simon
  Kris Pister
  Michael Richardson
Status

- Published -10 after Prague and -11 after shepherd’s review
- Shipped to AD
- Goal of the presentation
  - Summary of changes in -10 and -11
  - Discuss ASN replay attack
Updates in -10

• Failure handling after Göran Selander’s 2\textsuperscript{nd} WGLC review
  • Expanded Section 8.3.3.
  • RECOMMEND usage of OSCORE Appendix B.2 to renegotiate context ID

- Procedure defined in RFC8613 (OSCORE)

- JRC failure event
  - PSKs preserved
  - Seq numbers lost

- Force rejoin out-of-band
  - e.g. restart 6LBR

- Join Request (kid\_context = EUI-64)
- 4.01 Unauthorized (kid\_context = R2)
- Join Request (kid\_context = R2 || R3)
- Join Response
Updates in -10

- CoJP Error handling
  - Christian Amssus’ comment on the ML
- Redefined CBOR parameters
- CoAP request now carries self-contained CBOR object describing the error
- Malformed and Unsupported parameters

- Editorial: Rekeying process is now a separate section

```plaintext
Unsupported_Configuration = [
    + parameter : Unsupported_Parameter
]

Unsupported_Parameter = {
    code : int,
    parameter_label : int,
    parameter_addinfo : nil / any
}
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unsupported</td>
<td>0</td>
<td>The indicated setting is not supported by the networking stack implementation.</td>
<td>[[this document]]</td>
</tr>
<tr>
<td>Malformed</td>
<td>1</td>
<td>The indicated parameter value is malformed.</td>
<td>[[this document]]</td>
</tr>
</tbody>
</table>
Updates in -11

• Pascal Thubert’s shepherd review
• Update RFC6775 reference to RFC8505
• Editorial:
  • Elaborate on SHOULDs in Section 6.1.2 on setting DSCP code points
  • Nits
Latest discussions on the ML
Background:
L2 nonce in IEEE 802.15.4 TSCH

8-byte globally unique EUI-64

Absolute slot number
Local notion of time

Locally unique 2-byte address
Background:
Distribution of ASN in IEEE 802.15.4 TSCH and 6TiSCH

Wait for at most MAX_EB_DELAY to find NUM_NEIGHBORS_TO_WAIT

Store EB,
Store ASN and start counting slots

Pledge

Advertising node

Advertising node

EB (ASN=X, join metric=Y)

EB (ASN=X+n1, join metric = Y+k1)

EB (ASN=X+n3, join metric=Y)
Background:
Distribution of ASN in IEEE 802.15.4 TSCH and 6TiSCH

Wait for at most MAX_EB_DELAY to find NUM_NEIGHBORS_TO_WAIT

Store EB, Store ASN and start counting slots

EB (ASN=X, join metric=Y)

Join Request
Join Response

ASN used for communication purposes but not for crypto
ASN replay attack

Pledge → Attacker → JP

EB (ASN=23) → EB (ASN=115) → EB (ASN=23)

Join Request (no L2 sec) → Join Request (no L2 sec)

Join Response (no L2 sec) → Join Response (no L2 sec)

EB (ASN=23) MIC check validates

First frame after joining (ASN=55)

6TiSCH - IETF 105 - Montreal
ASN replay attack

6TiSCH - IETF 105 - Montreal

Pledge
Attacker
JP
JRC

EB (ASN=23)
EB (ASN=23)
EB (ASN=115)
EB (ASN=115)

Join Request (no L2 sec)
Join Request (no L2 sec)
Join Response (no L2 sec)
Join Response (no L2 sec)

EB (ASN=23) MIC check validates

First frame after joining (ASN=55)

L2 nonce reuse if:
- Short address given to pledge was reassigned
- Pledge joining for nth time and previously sent frames secured under ASN=55
Proposed resolution

1. Discard L2 verification
2. Decrypt & verify OSCORE
3. Get the L2 keys
4. Verify L2 MIC and on success, declare ASN as valid

Cryptographically bound
Guarantee that response is no
older than the request

Pledge

EB (ASN=23)

EB (ASN=115)

Join Request (no L2 sec)

JRC

Join Request

Join Response

Authenticate at L2 using the data key

Join Response

6TiSCH - IETF 105 - Montreal
Proposed resolution - Caveats

• Reception of the Join Response at Pledge
  • Security processing at L2 fails due to the missing key
  • Use 802.15.4 *promiscuous* mode during the join process at the pledge
  • Will pass the frame to the upper layer in any case

• L2 ACK of the Join Response

  - Sec processing FAIL
  - Send unencrypted Enh-Ack

  - Process Enh-Ack
  - Sec processing SUCCESS due to secExempt set for the pledge
TSCH and CCM security proofs

• *CCM* security proofs apply if nonce contains the security level
• Not the case with TSCH nonce (see Slide 7)
• Security proofs of *CCM* still apply
• Limitation is that a single key can only be used with fixed-length authentication tags

**Proposed resolution:**
Implementations MUST use different link-layer keys when using different authentication tag (MIC) lengths, as using the same key with different authentication tag lengths might be unsafe. For example, this prohibits the usage of the same key for both MIC-32 and MIC-64 levels. See Annex B.4.3 of {{IEEE802.15.4}} for more information.
Conclusion

• Shipped to AD already
• Note on ASN replay attack resolution needed
• Publish in -12