



Constrained Join Protocol for 6TiSCH

was: Minimal Security Framework for 6TiSCH

draft-ietf-6tisch-minimal-security

Presenter: Mališa Vučinić

Authors: Mališa Vučinić, Jonathan Simon, Kris Pister, Michael Richardson

Status

- Currently in -13
- IESG reviews received
- Goal of the presentation
 - Summary of changes in -12 and -13
 - Discuss issues raised during IESG reviews

Changes in -12 and -13

- Fixed Issue #60 (-12): Text prohibiting mixing of different levels of auth tags
- Fixed Issue #61 (-12): New subsection on ASN replay attack
- Fixed Issue #62 (-13): Mandatory support for extended tokens at JRC
- OPSDIR review by Linda Dunbar
 - +In case of device re-commissioning to a new owner, the PSK MUST be changed.
 - Nits
- SECDIR review by Hilarie Orman
 - Clarifications and nits

IESG reviews received

- Alvaro Retina
 - NO OBJECTION with comment
- Roman Danyliw
 - NO OBJECTION with comment
- Éric Vyncke
 - NO OBJECTION with comment
- Barry Leiba
 - DISCUSS
 - cleared
- Mirja Kühlewind
 - DISCUSS
- Adam Roach
 - DISCUSS
- Benjamin Kaduk
 - DISCUSS

Open Issues: Well-known URI for CoJP

Adam Roach and Benjamin Kaduk

- 6tisch.arpa and /j
 - We register a well-known host name 6tisch.arpa
 - JRC exposes /j during joining phase, joined nodes expose /j for parameter updates
 - Parameter Update Message did not use to carry « 6tisch.arpa » hostname
 - Makes every node a server at /j
 - Should it be under /.well-known ?
 - 11 additional bytes!

Proposed resolution: Specify that »6tisch.arpa « must also be carried in Parameter Update Message making 6tisch.arpa/j isolated from other uses

Open Issues: Parameter Update Response redundant

<https://bitbucket.org/6tisch/draft-ietf-6tisch-minimal-security/issues/72/remove-parameter-update-response-message>

Mirja Kühlewind

- Parameter Update Response message
 - Parameter Update Message is CoAP CON
 - Payload of Parameter Update Response is empty
 - Why keep it?

Proposed resolution: Remove Parameter Update Response message from the protocol

Open Issues: Traffic analysis of CoJP messages



<https://bitbucket.org/6tisch/draft-ietf-6tisch-minimal-security/issues/71/analyse-how-traffic-analysis-can-be-made>

Benjamin Kaduk

There are some seriously low-hanging fruit for traffic analysis with some of these messages, e.g., any OSCORE request with 'kid' of "JRC" is going to be a parameter update, at present. If someone wanted to throw out some chaff and muddle up this traffic analysis, what options are available to them?

Open Issues: Use of secExempt

<https://bitbucket.org/6tisch/draft-ietf-6tisch-minimal-security/issues/67/discuss-how-secexempt-should-be-used>

Benjamin Kaduk

I think we may need to say more about how a JP knows that "secExempt" is in effect (see comment in Section 5), since that affects a critical piece of the security posture of the network.

- We have join_rate parameter available at each joined node
- If set to 0, joining is disabled
- JRC can at any time update the join_rate at a JP to enable joining

Proposed resolution: Discuss that secExempt should be configured in response to a non-zero join_rate. Allow other means for secExempt to be configured, such as local button press.

Open Issues: CoJP_MAX_JOIN_ATTEMPT use inconsistent



https://bitbucket.org/6tisch/draft-ietf-6tisch-minimal-security/issues/65/use-of-cojp_max_join_attempt-is

Benjamin Kaduk

The string COJP_MAX_JOIN_ATTEMPTS appears only twice in the text, once in Section 8.3.1 and again in the table in Section 8.5. The former text leaves me confused as to what counts as a "join attempt" for this purpose, and in particular how it differs from the MAX_RETRANSMIT timer mentioned in the previous sentence.

- COJP_MAX_JOIN_ATTEMPTS is a remnant from the time Join Request was a NON message
- Now, we rely on CoAP to declare failure to the application upon MAX_RETRANSMIT

Proposed resolution: Remove the use of COJP_MAX_JOIN_ATTEMPTS from text

Open Issues: parameter_addinfo underspecified

https://bitbucket.org/6tisch/draft-ietf-6tisch-minimal-security/issues/64/parameter-add_info-is-underspecified

Benjamin Kaduk

The "parameter_addinfo" field in Unsupported_Parameter (Section 8.4.5) feels underspecified to me. The inline text says that only a subset of the link-layer key set from the Configuration could be included here, but how is that formally specified?

- The idea was that any key compliant with Link_Layer_Key struct can be included
- More text needed.

Proposed resolution: Discuss that the value of the parameter must be compliant with the structs defined in the document.

Open Issues: Indicate label validity for each message



https://bitbucket.org/6tisch/draft-ietf-6tisch-minimal-security/issues/64/parameter-add_info-is-underspecified

Benjamin Kaduk

It feels a little unusual to have a consolidate registry for CoJP parameters that are used as map labels across different messages, without some indication of which map labels are valid in which messages.

- CDDL fragments indicate which labels are valid in which CoJP objects
- CoJP objects can be carried by different messages
 - E.g. Configuration object carried by Join Response or Parameter Update

Proposed resolution: Add a paragraph reiterating and summarizing CDDL

Next steps

- Incorporate resolutions of open issues
- Publish -14