draft-ietf-6tisch-minimal-security

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

• Status: Ready for WGLC

• Published -05 with
  • Implementation feedback
  • Resolved last remaining known issues
  • Review by Thomas Watteyne

• Goal of the presentation
  • Quick summary of updates since -04
  • Discuss WGLC
Change #1: Join traffic tagging

• Unauthenticated traffic from pledges forwarded in the mesh
• May cause intermediate 6TiSCH routers to request additional link capacity
  • e.g. Minimal Scheduling Function (draft-chang-6tisch-msf-01)
• Opens the network to the resource exhaustion attack vector
• Resolution:
  • Tag IP packets from pledges at Join Proxy before forwarding them
  • Use DiffServ Code Point to identify join traffic (RFC2597)
  • AF43 code point for Join Request, AF42 for (authenticated) join response
  • Out-of-scope how an SF reacts to this traffic, recommendation provided
  • Normative reference on RFC2597
Change #2: How does JRC know which network a pledge is trying to join?

• Use case: JRC **not** co-located with 6LBR, managing multiple 6TiSCH networks

• When Join Request arrives, JRC needs to identify the network the pledge is attempting to join in order to hand out the correct link-layer keys

• Resolution:
  • Define Join Request payload: CBOR array with a single “network_identifier” element
  • Join Request maps to a CoAP POST, so can carry payload
Change #3: Editorial 1/2

- Goals: clarify terminology, allow future specs to override identifiers
- Resolution:
  - Terminology section
    - List the terms extensively used, definitions in draft-ietf-6tisch-terminology
    - Stress the difference between “join process” and “join protocol”
  - Added a separate “Identifiers” section
    - Purpose is to use generic terms for “network identifier” and “pledge identifier”, mapping to PAN ID and EUI-64 by default, but allowing future specs to override it
    - The identifiers are used in the protocol
    - As this requires “standardization” text, the Terminology section is not the best fit
Change #3: Editorial 2/2

• Goal: Precise standardization scope of the document
• Resolution:
  • Configuration of:
    • 802.15.4 layer (e.g. link-layer security requirements)
    • IP layer (neighbor cache management, join traffic tagging)
    • Application layer (how to configure OSCORE context, use of Stateless-Proxy CoAP option)
  • Definition of the 6TiSCH Join Protocol (6JP)
    • Message mapping to CoAP
    • Payload formats (use of CBOR, examples in CBOR data definition language)
    • Semantics
  • Definition of Stateless-Proxy CoAP option
  • Separate sections in the document for each
Next steps

• Another plugtest in June 2018 in Paris
• Ready for WGLC
  • Coordinate with CORE on Stateless-Proxy
  • Normative reference on OSCORE, which is under IESG review