IEC/IEEE 60802
NETCONF over TLS 1.2 or TLS 1.3?

Stephan Kehrer, Hirschmann Automation and Control GmbH

July 2023

Current state

- Currently IEC/IEEE 60802 D2.0 mandates the following:
  - Support of NETCONF over TLS (IETF RFC 7589) → TLS 1.2 in the conformance clause (5.5.4)
  - The usage of TLS 1.2 in 6.3.2.1.2:
    "TLS shall be used for NETCONF/YANG according to the following profile:
    a) TLS protocol version 1.2 according to IETF RFC 5246 shall be used with mutual authentication."
  - The use of specific cipher suites that go beyond the cipher suites mandated by RFC 5246.
- The topic of TLS 1.3 has been previously discussed[1].
- The discussion was brought up again based on a comment (#397) against IEC/IEEE 60802/D2.0.
  - While the initial disposition was to reject the comment and stay with NETCONF over TLS 1.2, further investigation of the topic brought up a few points that may be worth considering and might reopen the discussion.

[1] https://www.ieee802.org/1/files/public/docs2022/60802-Pfaff-et-al-Afterthoughts-for-D13-14-Security-0722-v01.pdf

What is the issue?

- In the view of the presenter, The usage of NETCONF over TLS 1.2 is problematic for the following reasons:
  - TLS 1.3 is the current state-of-the-art protocol version. It…
    - is defined in RFC 8446,
    - was published August 2018,
    - **obsoletes** RFC 5077, **RFC 5246**, RFC 6961.
  - NIST requires support of TLS 1.3 everywhere, without exception, from January 2024[1].
  - IETF is discussing to deprecate TLS 1.2[2].
  - IETF is working on NETCONF over TLS 1.3[3].

Mandating the implementation and use of the outdated TLS 1.2 protocol may cause acceptance issues from a security perspective!

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf
[2] https://datatracker.ietf.org/meeting/116/materials/slides-116-tls-tls-12-deprecation-discussion-00
[3] https://datatracker.ietf.org/doc/draft-ietf-netconf-over-tls13/

Taking a closer look…

- The reference to IETF RFC 5246 in 6.3.2.1.2 is problematic as RFC 5246 has been obsoleted by RFC 8446 in August 2018
  - A comment (#323) against IEC/IEEE 60802/D2.0 pointed out another place in the draft that referenced an obsolete RFC, requesting to update the reference to the current RFC. This comment was accepted.
    → **The reference in 6.3.2.1.2 should be updated to point to the current RFC 8446**.
    - This might result in further updates to the sections in IEC/IEEE 60802 that mandate specific cipher suites.

Taking a closer look…

- Referencing TLS 1.3, and more specifically NETCONF over TLS 1.3, seems to be a minor update to IEC/IEEE 60802 in the opinion of the presenter for the following reasons:
  - Draft status of the document:
    - **IEC/IEEE 60802 currently refers to other draft documents**, expecting that they will be published by the time IEC/IEEE 6082 is finished.
    - The NETCONF over TLS 1.3 draft is not a very large or complicated document
    - It is reasonable to assume that the document may soon become a proposed standard:
      - Current draft will expire on September 11, 2023
      - According to https://datatracker.ietf.org/wg/netconf/documents/ the state of the draft is “I-D Exists, WG Consensus: Waiting for Write-Up”.
      - This, together with the small document size, seems to indicate that the document will most likely be available as standard before IEC/IEEE 60802 is published.

Taking a closer look…

- Referencing TLS 1.3, and more specifically NETCONF over TLS 1.3, seems to be a minor update to IEC/IEEE 60802 in the opinion of the presenter for the following reasons *(continued)*:
  - The NETCONF over TLS 1.3 draft…
    - states that the implementation **must** support TLS 1.2 and **should** support TLS 1.3,
    - states that TLS 1.3 **must** be preferred, if it is implemented,
    - explicitly states that 0-RTT (round-trip time) data **must not** be used for NETCONF
    - specifies mandatory cipher suites different from the ones currently mandated for TLS 1.2.
  - The phrasing in the NETCONF over TLS 1.3 draft effectively achieves what the presenter thinks IEC/IEEE 60802 should aim for:
    mandate at least TLS 1.2 but strongly advise to use TLS 1.3.
  - This wording also should allow existing equipment, supporting TLS 1.2, to remain compliant to IEC/IEEE 60802.
  - Specifying the use of NETCONF over TLS 1.3 by referencing the IETF draft (and hopefully standard by the time IEC/IEEE 60802 is published) would help to address the issues pointed out on slide 3.

Suggested way forward

- Change IEC/IEEE 60802 to refer to NETCONF over TLS in 5.5.4

- Update 6.3.2.1.2 to state
  “TLS shall be used for NETCONF/YANG according to the following profile:
  a) TLS protocol version 1.3 according to IETF RFC 8446 shall be used with mutual authentication.”

- Update mandatory cipher suites and add additional mandatory cipher suites as required in both places.

Thank you!

Discussion and Questions?