NETCONF over TLS

Jürgen Schönwälder
Jacobs University Bremen

draft-ietf-netconf-rfc5539bis-05

Status and Issues

- Implementation effort end of March 2014 (thanks to Vaibhav Bajpai and Radek Krejčí)
- Issues reported on the mailing list in April
- Ongoing discussions of what belongs into which document
- Some of the issues on the following slides may end up being addressed in other documents

hostname verification and NATs

- How to handle TLS certificate hostname verification when multiple hosts are behind a NAT? The NMS should have some kind of pre-defined knowledge, that the hostname is correct (expected for the certificate). Maybe this can be mentioned more explicitly in the NETCONF over TLS text.
- Proposal #1: Have explicit text for call home certificate checking and regular certificate checking. (But then I note that also the NMS can be behind a NAT.)
- Proposal #2: Deal with this in the Security Considerations by providing advice that certificates should include other unique identifiers in cases of NATs.
- Proposal #3: Better explain that what is expected is a check against the 'expected' hostname (not the name obtained from a usually not trust-worthy DNS lookup).

strictness of certificate verification

- What shall be the strictness of the TLS certificate mutual verification?
  - a) validate the peer certificate against a trusted CA chain
  - b) validate using a) and check if peer certificate is locally known (e.g. hash configured)
- Proposal: This should be configurable in the NETCONF server data model and it should be possible to use self-signed certificates through proper configuration.

client side configuration of call-home?

- Do we need to document NETCONF client-side configuration for NETCONF call home? Do we need to configure how the client should/must verify the server certificates?
- Proposal: unclear

mandatory cipher suites

- The CIPHER suites for TLS v1.2 are mandated by Section 9 of RFC 5246. Do we need to mention them in this document?
- Proposal: Remove the following text:

  which is TLS_RSA_WITH_AES_128_CBC_SHA. This document is assumed to apply to future versions of TLS; in which case, the mandatory-to- implement cipher suite for the implemented version MUST be supported.

required authentication schemes

- [Section 2.4]:

  Implementations MAY optionally support TLS certificate-based authentication [RFC5246].
- For non-constrained systems, it may make sense to require (MUST) certificate-based authentication.
- Meta question: Do we have to cater for constrained systems (this is why we have PSK authentication) or is a RESTCONF/CoAP approach not anyway the better solution to deal with constrained devices?
- Proposal: Require certificate-based authentication (MUST), remove PSK authentication from all relevant documents.

resolve hostname check contradiction

- Resolve the following contracdiction:

  [Section 2.4.1]: "the NETCONF client MUST check its understanding of the NETCONF server hostname against the server's identity" [...] "If the NETCONF client has external information as to the expected identity of the NETCONF server, the hostname check MAY be omitted.”

- Proposal:

  If NC client has external information [...], the hostname check may not be performed. Otherwise, the NC client MUST check its understanding...

messages received after <close-session>

- [Section 2.3]

  The NETCONF server MUST NOT process any NETCONF messages received after the <close-session> operation.

- RFC 6241 section 7.8 already says:

  Any NETCONF requests received after a <close-session> request will be ignored.

- Proposal: Remove the text from section 2.3

client and server clarification

- Change section titles to be more explicit:
  - 2.1.1 Client to Server
    2.1.1 NETCONF Client to NETCONF Server
  - 2.1.2 Server to Client (Call Home)
    2.1.2 NETCONF Server to NETCONF Client
- Unclear whether there really is an ambiguity since the context is rather clear
- Proposal: Leave as is (but may change anyway if the document structure changes)