NETCONF over TLS

M. Badra, A. Luchuk, J. Schoenwaelder

(RFC 5539bis)

draft-ietf-netconf-rfc5539bis-06

Motivation

- Alternate transport for platforms that do not support SSH; e.g., embedded systems
- Define a standards-based mechanism for generating NETCONF usernames
- Alignment with new NC framing in SSH

Changes since RFC 5539bis-05

- Removed all call-home related text
- Removed redundant text as discussed at the Toronto IETF meeting
- Textual clarifications
- Revised to include comments from draft reviewers

Open Issues

- WG chairs posted two open issues to the list
- Deadline was set to 2014-11-08
- Comments received from these contributors:
  - QW = Qin Wu <bill.wu@huawei.com>
  - VB = Vaibhav Bajapi <v.bajpai@jacobs-university.de>
  - LB = Liubing (Leo) <leo.liubing@huawei.com>
  - TP = Tom Petch <ietfc@btconnect.com>
  - KW = Kent Watsen <kwatsen@juniper.net>
  - AL = Alan Luchuk <luchuk@snmp.com>

Issue #1

- Should RFC 5539bis be limited to X.509 certificates or should it be more generic to cover other (future) authentication schemes as well?
- QW: Prefer a single NC over TLS document, mutual X.509 should be optional
- VB: Separate documents may be easier to develop
- LB: No strong feeling, may be more practical to limit scope to X.509
- KW: Prefers to limit scope to X.509 authentication
- AL: Limit scope to X.509 authentication

Issue #2

- Should RFC 5539bis detail the algorithm to extract a NETCONF username from a X.509 certificate?

- QW: Prefer to have the algorithm defined in RFC5539bis
- LB: Prefer to have the algorithm defined in RFC5539bis
- TP: <JS is confused by his messages - I am not sure what TP prefers, chairs please investigate>
- KW: Prefer RFC5539bis to be self-contained, unclear where the username algorithm should go

Strawman Proposal

- Limit scope to mutual X.509 authentication
- Describe the algorithm how to extract a username in RFC 3559bis (essentially providing a high-level summary of the essential parts of the description clause of snmpTlstmCertToTSNTable in RFC 6353)

Remaining Work

- Modify document as needed to reflect WG consensus on questions on previous slide
- TP suggests to have the text more clearly structured along the following three steps:
  - certificate validation (should be short, largely covered by a reference to RFC 5280)
  - checking whether the presented certificate matches the expectations
  - deriving the username form the certificate