Network Device Interpretation # 21

Using garbled messages to test TLS implementation

Status: ☒ *Active* ☐ *Inactive*

Date: *30-Jun-2016*

Type of Document: ☒ *Technical Decision* ☐ *Technical Recommendation*

Approved by: ☒ *Network iTC Interpretations Team* ☐ *Network iTC*

Affected Document(s): *ND SD V1.0*

Affected Section(s): *sections 2.2.13.3, 2.2.15.3*

Superseded Interpretation(s): *None*

Issue:

There are two tests for TLS (one for TOE as client (section 2.2.13.3, line 225) and one for server (section 2.2.15.3, line 255)) that requires sending of garbled messages:
Client: Send a garbled message from the Server after the Server has issued the ChangeCipherSpec message and verify that the client denies the connection.
Server: Send a garbled message from the client after the client has issued the ChangeCipherSpec message and verify that the Server denies the connection.
The question I have is:
When should the garbled message be sent? I am assuming it is before TLS connection is setup. If that is the case, is the expectation that the evaluator craft a separate (garbled) packet to be sent right after ChangeCipherSpec message? This would be the only way to perform this test since in most cases ChangeCipherSpec and Finished messages are sent together and tunnel is set-up right after that.
Also what is the intention of this test? Does anyone know what does this test help accomplish/verify?

Resolution:

As part of completing negotiation of the TLS tunnel, a Finished message is sent (after ChangeCipherSpec) which contains a hash of the previous messages exchanged. The tunnel should be set up only if this hash is correctly verified. By sending a garbled message (before Finished message is sent) it can be verified that the TLS implementation waits for Finished message and verifies the hash before sending data. So for the purpose of this test the garbled messaged shall be sent before the Finished message is sent.

Rationale:

None

Further Action:

None

Action by Network iTC:

None