DTLS as Transport for STUN

draft-petithuguenin-tram-stun-dtls

IETF-89

London, March 5, 2014

Marc Petit-Huguenin, Gonzalo Salgueiro

Overview

- This draft specifies the usage of DTLS as a transport protocol for STUN.
- DTLS offers necessary security and a more optimal transport for RTC.
- Provides guidance on how to use DTLS with the current STUN Usages and makes modifications to STUN/TURN URI &TURN resolution mechanism (to allow DTLS).

Open Issues (#1)

- Currently the draft states:

  STUN over DTLS MUST, at a minimum, support TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

  What is the recommendation these days?

Open Issues (#2)

- Currently the draft states:

  Any STUN request or indication without the magic cookie over DTLS MUST MUST always trigger an error when receiving a request from Classic STUN.

- This a departure from RFC 5389, which does not explicitly state what to do in that case. *Is this the right decision?*

Open Issues (#3)

- Currently the draft states:

  Future STUN usages MUST take into account DTLS as a transport and discuss its applicability.

- RFC 5389 omitted to say that transport applicability MUST be discussed.

  Is this a reasonable addition?

Open Issues (#4)

- Currently the draft states:

  The <host> value MUST be used when using the rules in Section 7.2.2 of [RFC5389] to verify the server identity.

- Now we have STUN/TURN URI & can use domain name to verify server identity.
  What if an IP address is used in the URI? Should we reject it?

Next Steps

- Other issues?
- Need additional reviews
- For milestone:

  Send draft adding DTLS as a transport for STUN/TURN to IESG

- Adopt as WG document to satisfy this?