Multiplexing Scheme Updates for SRTP Extension for DTLS

draft-petithuguenin-avtcore-rfc5764-mux-fixes

IETF-90

Toronto, July 24, 2014

Marc Petit-Huguenin, Gonzalo Salgueiro

IETF

Overview

- Identifies 3 issues with multiplexing scheme defined in RFC 5764 Section 5.1.2

1. Implicit allocation of codepoints for new STUN methods with no IANA registry
2. Implicit allocation of codepoints for new TLS ContentTypes with no IANA registry
3. Didn't account for TURN usage of STUN can create TURN channels that also need demuxing with other explicitly mentioned packet types

Problem 2: TLS ContentTypes

- RFC 5764 demultiplexing scheme dictates that if the value of the first byte is between 20 and 63 (inclusive), then the packet is identified to be DTLS
- This restricts the TLS ContentType codepoints to this range
- By extension this implicitly allocates ContentType codepoints 0-19 and 64-255

Proposed Solution

- Explicitly reserves the TLS ContentType codepoints from 0-19 and from 64-255 so they are not inadvertently assigned in the future
- Proposed changes to TLS ContentType Registry is:

Value: 0-19	Value: 64-255
Description: Reserved	Description: Reserved
DTLS-OK: N/A	DTLS-OK: N/A
Reference: RFC5764, RFCXXXX	Reference: RFC5764, RFCXXXX

Next Steps

- RFC 5764 updates will be discussed in AVTCORE
- Coordinated effort of 3 different WGs (TRAM, TLS, AVTCORE)
- Need TLS WG expert review