Multiplexing Scheme Updates for SRTP Extension for DTLS

draft-petithuguenin-avtcore-rfc5764-mux-fixes

IETF-90

Toronto, July 23, 2014

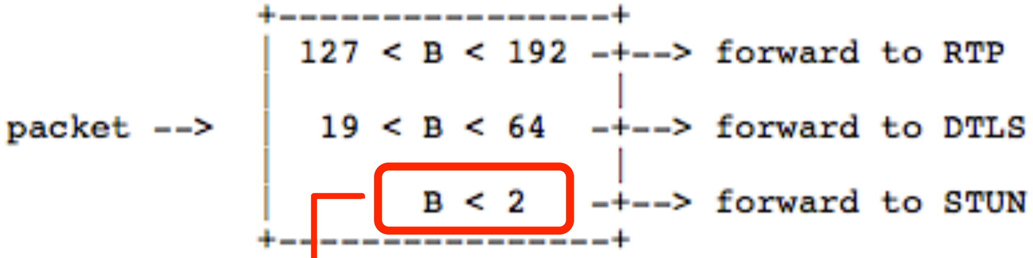
Marc Petit-Huguenin, Gonzalo Salgueiro

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

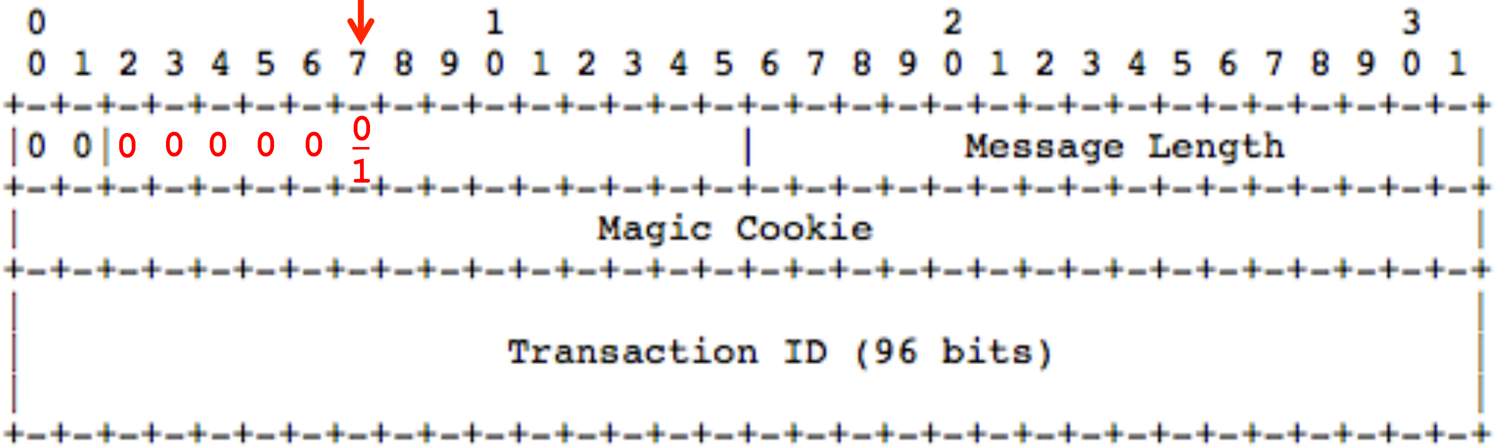
Problem 1: STUN Methods



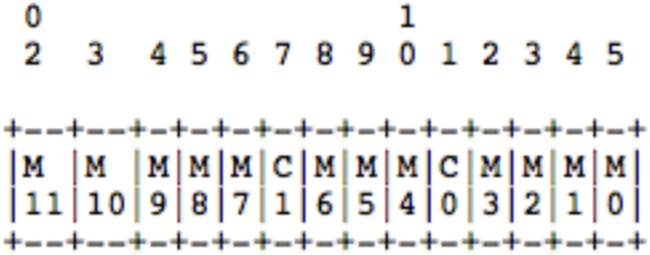
```
                +----------------+
                | 127 < B < 192 -+--> forward to RTP
                |                |
    packet -->  |  19 < B < 64  -+--> forward to DTLS
                |                |
                |       B < 2   -+--> forward to STUN
                +----------------+
```

Current packet identification scheme: if first byte is 0 or 1, the packet is STUN

Restricts STUN methods to values 0x000 – 0x07F



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0 0|0 0 0 0 0 0                |         Message Length        |
+-+-+-+-+-+-+-+1+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Magic Cookie                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                     Transaction ID (96 bits)                  |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```



```
 0                 1
 2  3  4 5 6 7 8 9 0 1 2 3 4 5

+--+--+-+-+-+-+-+-+-+-+-+-+-+-+
|M |M |M|M|M|C|M|M|M|C|M|M|M|M|
|11|10|9|8|7|1|6|5|4|0|3|2|1|0|
+--+--+-+-+-+-+-+-+-+-+-+-+-+-+
```

Range

Min:	MMMMMCMMMCMMMM 0b0000000000000000	**method = 0x000** class = 0b00
Max:	MMMMMCMMMCMMMM 0b0000000111111111	**method = 0x07F** class = 0b11

Proposed Solution

- Update RFC 5764 packet identification algorithm to expand range assigned to STUN from 0-1 to 0-19 (values 2-19 currently unused)
- Proposed changes to the STUN Method Registry is:

OLD:

0x000-0x7FF	IETF Review
0x800-0xFFF	Designated Expert

NEW:

0x000-0x27F	IETF Review
0x280-0x4FF	Designated Expert
0x500-0xFFF	Reserved

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
Description: Reserved
DTLS-OK: N/A
Reference: RFC5764, RFCXXXX

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

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 3: TURN Channels

- RFC 5764 demultiplexing scheme does not define what to do with packets received over a TURN channel since these packets will start with a first byte whose value will be between 64-127
- These packets would be rejected by current scheme
- Current implementations violate RFC 5764 for values 64-127 and they instead parse packets with such values as TURN

Proposed Solution

- Modify the RFC 5764 demultiplexing algorithm to properly account for TURN channels and prevent future documents from assigning values from the unused range to a new protocol
- Proposed changes to the TURN Channel Number Registry is:

Value: 0x8000-0xFFFF

Name: Reserved

Reference: RFCXXXX

Next Steps

- RFC 5764 updates will be discussed in AVTCORE
- Coordinated effort of 3 different WGs (TRAM, TLS, AVTCORE)
- Do we create a WG milestone for updating the STUN Methods Registry?
- Can we adopt as WG doc to satisfy this?