Internet Engineering Task Force (IETF)
Request for Comments: 7983
Updates: 5764
Category: Standards Track
ISSN: 2070-1721

M. Petit-Huguenin
Impedance Mismatch
G. Salgueiro
Cisco Systems

September 2016

Multiplexing Scheme Updates for Secure Real-time Transport Protocol (SRTP) Extension for Datagram Transport Layer Security (DTLS)

Abstract

This document defines how Datagram Transport Layer Security (DTLS), Real-time Transport Protocol (RTP), RTP Control Protocol (RTCP), Session Traversal Utilities for NAT (STUN), Traversal Using Relays around NAT (TURN), and ZRTP packets are multiplexed on a single receiving socket. It overrides the guidance from RFC 5764 ("SRTP Extension for DTLS"), which suffered from four issues described and fixed in this document.

This document updates RFC 5764.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7983.

Table of Contents

1. Introduction

Section 5.1.2 of "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)" [RFC5764] defines a scheme for a Real-time Transport Protocol (RTP) [RFC3550] receiver to demultiplex DTLS [RFC6347], Session Traversal Utilities for NAT (STUN) [RFC5389], and Secure Real-time Transport Protocol (SRTP) / Secure Real-time Transport Control Protocol (SRTCP) [RFC3711] packets that are arriving on the RTP port. Unfortunately, this demultiplexing scheme has created problematic issues:

1. It implicitly allocated codepoints for new STUN methods without an IANA registry reflecting these new allocations.

2. It did not take into account the fact that ZRTP [RFC6189] also needs to be demultiplexed with the other packet types explicitly mentioned in Section 5.1.2 of RFC 5764.

3. It implicitly allocated codepoints for new Transport Layer Security (TLS) ContentTypes without an IANA registry reflecting these new allocations.

4. It did not take into account the fact that the Traversal Using Relays around NAT (TURN) usage of STUN can create TURN channels that also need to be demultiplexed with the other packet types explicitly mentioned in Section 5.1.2 of RFC 5764.

Having overlapping ranges between different IANA registries becomes an issue when a new codepoint is allocated in one of these registries without carefully analyzing the impact it could have on the other registries when that codepoint is demultiplexed. Among other downsides of the bad design of the demultiplexing algorithm detailed in [RFC5764], it creates a requirement for coordination between codepoint assignments where none should exist, and that is organizationally and socially undesirable. However, RFC 5764 has been widely deployed, so there must be an awareness of this issue and how it must be dealt with. Thus, even if the feature related to a codepoint is not initially thought to be useful in the context of demultiplexing, the respective IANA registry expert should at least raise a flag when the allocated codepoint irrevocably prevents multiplexing.

The first goal of this document is to make sure that future allocations in any of the affected protocols are done with the full knowledge of their impact on multiplexing. This is achieved by updating [RFC5764], which includes modifying the IANA registries with instructions for coordination between the protocols at risk.

A second goal is to permit the addition of new protocols to the list of existing multiplexed protocols in a manner that does not break existing implementations.

At the time of this writing, the flaws in the demultiplexing scheme were unavoidably inherited by other documents, such as [RFC7345] and [SDP-BUNDLE]. So in addition, these and any other affected documents will need to be corrected with the updates this document provides.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Implicit Allocation of Codepoints for New STUN Methods

The demultiplexing scheme in [RFC5764] states that the receiver can identify the packet type by looking at the first byte. If the value of this first byte is 0 or 1, the packet is identified to be STUN. The problem with this implicit allocation is that it restricts the codepoints for STUN methods (as described in Section 18.1 of [RFC5389]) to values between 0x000 and 0x07F, which in turn reduces the number of possible STUN method codepoints assigned by IETF Review (i.e., the range 0x000 - 0x7FF) from 2048 to only 128 and eliminates the possibility of having STUN method codepoints assigned by Designated Expert (i.e., the range 0x800 - 0xFFF).

To preserve the Designated Expert range, this document allocates the values 2 and 3 to also identify STUN methods.

The IANA Registry for STUN methods has been modified to mark the codepoints from 0x100 to 0xFFF as Reserved. These codepoints can still be allocated, but require IETF Review with a document that will properly evaluate the risk of an assignment overlapping with other registries.

In addition, this document also updates the IANA registry such that the STUN method codepoints assigned in the 0x080-0x0FF range are also assigned via Designated Expert. The "STUN Methods" registry has been changed as follows:

OLD:

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

NEW:

0x000-0x07F	IETF Review
0x080-0x0FF	Designated Expert
0x100-0xFFF	Reserved

4. Multiplexing of ZRTP

ZRTP [RFC6189] is a protocol for media path Diffie-Hellman exchange to agree on a session key and parameters for establishing unicast SRTP sessions for Voice over IP (VoIP) applications. The ZRTP protocol is media path keying because it is multiplexed on the same port as RTP and does not require support in the signaling protocol.

In order to prevent future documents from assigning values from the unused range to a new protocol, this document modifies the [RFC5764] demultiplexing algorithm to properly account for ZRTP [RFC6189] by allocating the values from 16 to 19 for this purpose.

5. Implicit Allocation of New Codepoints for TLS ContentTypes

The demultiplexing scheme in [RFC5764] dictates that if the value of the first byte is between 20 and 63 (inclusive), then the packet is identified to be DTLS. For DTLS 1.0 [RFC4347] and DTLS 1.2 [RFC6347], that first byte corresponds to the TLS ContentType field. Considerations must be taken into account when assigning additional ContentTypes in the codepoint ranges 0 to 19 and 64 to 255, so this does not prevent demultiplexing when this functionality is desirable. Note that [RFC5764] describes a narrow use of DTLS that works as long as the specific DTLS version used abides by the restrictions on the demultiplexing byte (the ones that this document imposes on the "TLS ContentType Registry"). Any extension or revision to DTLS that causes it to no longer meet these constraints should consider what values may occur in the first byte of the DTLS message and what impact it would have on the multiplexing that [RFC5764] describes.

With respect to TLS packet identification, this document explicitly adds a warning to the codepoints from 0 to 19 and from 64 to 255 indicating that allocations in these ranges require coordination, as described in this document. The "TLS ContentType Registry" has been changed as follows:

OLD:

0-19	Unassigned
20	change_cipher_spec
21	alert
22	handshake
23	application_data
24	heartbeat
25-255	Unassigned

NEW:

0-19	Unassigned (Requires coordination; see RFC 7983)
20	change_cipher_spec
21	alert
22	handshake
23	application_data
24	heartbeat
25-63	Unassigned
64-255	Unassigned (Requires coordination; see RFC 7983)

6. Multiplexing of TURN Channels

When used with Interactive Connectivity Establishment (ICE) [RFC5245], an implementation of RFC 5764 can receive packets on the same socket from three different paths, as shown in Figure 1:

1. Directly from the source

2. Through a NAT

3. Relayed by a TURN server

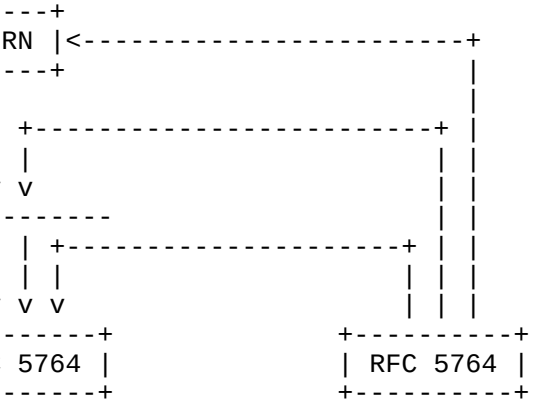

Figure 1: Packet Reception by an Implementation of RFC 5764

Even if the ICE algorithm succeeded in selecting a non-relayed path, it is still possible to receive data from the TURN server. For instance, when ICE is used with aggressive nomination, the media path can quickly change until it stabilizes. Also, freeing ICE candidates is optional, so the TURN server can restart forwarding STUN connectivity checks during an ICE restart.

TURN channels are an optimization where data packets are exchanged with a 4-byte prefix instead of the standard 36-byte STUN overhead (see Section 2.5 of [RFC5766]). The problem is that the 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 and 127 (inclusive). If the TURN server was instructed to send data over a TURN channel, then the demultiplexing scheme specified in RFC 5764 will reject these packets. Current implementations violate RFC 5764 for values 64 to 127 (inclusive) and they instead parse packets with such values as TURN.

In order to prevent future documents from assigning values from the unused range to a new protocol, this document modifies the demultiplexing algorithm in RFC 5764 to properly account for TURN channels by allocating the values from 64 to 79 for this purpose. This modification restricts the TURN channel space to a more limited set of possible channels when the TURN client does the channel binding request in combination with the demultiplexing scheme described in [RFC5764].

7. Updates to RFC 5764

This document updates the text in Section 5.1.2 of [RFC5764] as follows:

OLD TEXT

The process for demultiplexing a packet is as follows. The receiver looks at the first byte of the packet. If the value of this byte is 0 or 1, then the packet is STUN. If the value is in between 128 and 191 (inclusive), then the packet is RTP (or RTCP, if both RTCP and RTP are being multiplexed over the same destination port). If the value is between 20 and 63 (inclusive), the packet is DTLS. This process is summarized in Figure 3.

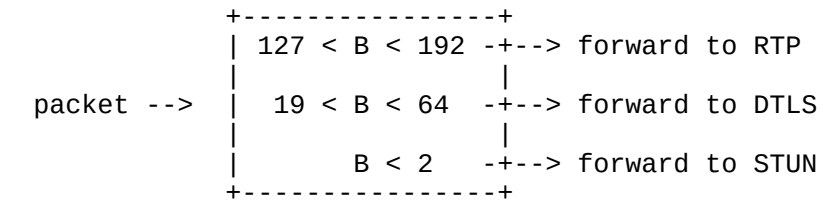

Figure 3: The DTLS-SRTP receiver's packet demultiplexing algorithm. Here the field B denotes the leading byte of the packet.

END OLD TEXT

NEW TEXT

The process for demultiplexing a packet is as follows. The receiver looks at the first byte of the packet. If the value of this byte is in between 0 and 3 (inclusive), then the packet is STUN. If the value is between 16 and 19 (inclusive), then the packet is ZRTP. If the value is between 20 and 63 (inclusive), then the packet is DTLS. If the value is between 64 and 79 (inclusive), then the packet is TURN Channel. If the value is in between 128 and 191 (inclusive), then the packet is RTP (or RTCP, if both RTCP and RTP are being multiplexed over the same destination port). If the value does not match any known range, then the packet MUST be dropped and an alert MAY be logged. This process is summarized in Figure 3.

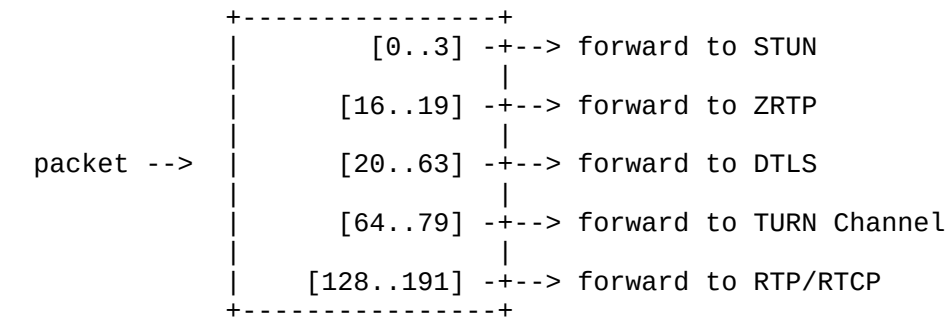

Figure 3: The DTLS-SRTP receiver's packet demultiplexing algorithm.

END NEW TEXT

8. Security Considerations

This document updates existing IANA registries and adds a new range for TURN channels in the demultiplexing algorithm.

These modifications do not introduce any specific security considerations beyond those detailed in [RFC5764].

9. IANA Considerations

9.1. STUN Methods

This specification contains the registration information for reserved STUN Methods codepoints, as explained in Section 3 and in accordance with the procedures defined in Section 18.1 of [RFC5389].

Value: 0x100-0xFFF

Name: Reserved (For DTLS-SRTP multiplexing collision avoidance, see RFC 7983. Cannot be made available for assignment without IETF Review.)

Reference: RFC 5764, RFC 7983

This specification also reassigns the ranges in the STUN Methods Registry as follows:

Range: 0x000-0x07F

Registration Procedures: IETF Review

Range: 0x080-0x0FF

Registration Procedures: Designated Expert

9.2. TLS ContentType

This specification contains the registration information for reserved TLS ContentType codepoints, as explained in Section 5 and in accordance with the procedures defined in Section 12 of [RFC5246].

Value: 0-19

Description: Unassigned (Requires coordination; see RFC 7983)

DTLS-OK: N/A

Reference: RFC 5764, RFC 7983

Value: 64-255

Description: Unassigned (Requires coordination; see RFC 7983)

DTLS-OK: N/A

Reference: RFC 5764, RFC 7983

9.3. Traversal Using Relays around NAT (TURN) Channel Numbers

This specification contains the registration information for reserved codepoints in the "Traversal Using Relays around NAT (TURN) Channel Numbers" registry, as explained in Section 6 and in accordance with the procedures defined in Section 18 of [RFC5766].

Value: 0x5000-0xFFFF

Name: Reserved (For DTLS-SRTP multiplexing collision avoidance, see RFC 7983.)

Reference: RFC 7983

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, DOI 10.17487/RFC3550, July 2003, <http://www.rfc-editor.org/info/rfc3550>.

[RFC3711] Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, DOI 10.17487/RFC3711, March 2004, <http://www.rfc-editor.org/info/rfc3711>.

[RFC5245] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", RFC 5245, DOI 10.17487/RFC5245, April 2010, <http://www.rfc-editor.org/info/rfc5245>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <http://www.rfc-editor.org/info/rfc5246>.

[RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT (STUN)", RFC 5389, DOI 10.17487/RFC5389, October 2008, <http://www.rfc-editor.org/info/rfc5389>.

[RFC5764] McGrew, D. and E. Rescorla, "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)", RFC 5764, DOI 10.17487/RFC5764, May 2010, <http://www.rfc-editor.org/info/rfc5764>.

[RFC5766] Mahy, R., Matthews, P., and J. Rosenberg, "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)", RFC 5766, DOI 10.17487/RFC5766, April 2010, <http://www.rfc-editor.org/info/rfc5766>.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347, January 2012, <http://www.rfc-editor.org/info/rfc6347>.

10.2. Informative References

[RFC4347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security", RFC 4347, DOI 10.17487/RFC4347, April 2006, <http://www.rfc-editor.org/info/rfc4347>.

[RFC6189] Zimmermann, P., Johnston, A., Ed., and J. Callas, "ZRTP: Media Path Key Agreement for Unicast Secure RTP", RFC 6189, DOI 10.17487/RFC6189, April 2011, <http://www.rfc-editor.org/info/rfc6189>.

[RFC7345] Holmberg, C., Sedlacek, I., and G. Salgueiro, "UDP Transport Layer (UDPTL) over Datagram Transport Layer Security (DTLS)", RFC 7345, DOI 10.17487/RFC7345, August 2014, <http://www.rfc-editor.org/info/rfc7345>.

[SDP-BUNDLE] Holmberg, C., Alvestrand, H., and C. Jennings, "Negotiating Media Multiplexing Using the Session Description Protocol (SDP)", Work in Progress, draft-ietf-mmusic-sdp-bundle-negotiation-32, August 2016.

Acknowledgements

The implicit STUN Method codepoint allocations problem was first reported by Martin Thomson in the RTCWEB mailing list and discussed further with Magnus Westerlund.

Thanks to Simon Perreault, Colton Shields, Cullen Jennings, Colin Perkins, Magnus Westerlund, Paul Jones, Jonathan Lennox, Varun Singh, Justin Uberti, Joseph Salowey, Martin Thomson, Ben Campbell, Stephen Farrell, Alan Johnston, Mehmet Ersue, Matt Miller, Spencer Dawkins, Joel Halpern, and Paul Kyzivat for the comments, suggestions, and questions that helped improve this document.

Authors' Addresses

Marc Petit-Huguenin
Impedance Mismatch

Email: marc@petit-huguenin.org

Gonzalo Salgueiro
Cisco Systems
7200-12 Kit Creek Road
Research Triangle Park, NC 27709
United States of America

Email: gsalguei@cisco.com