TRAM
Internet-Draft
Updates: 5928, 7065 (if approved)
Intended status: Standards Track
Expires: August 4, 2014

M. Petit-Huguenin
Jive Communications
G. Salgueiro
Cisco Systems

January 31, 2014

Datagram Transport Layer Security (DTLS) as Transport for Traversal Using Relays around NAT (TURN) draft-petithuguenin-tram-turn-dtls-00

Abstract

This document specifies the usage of Datagram Transport Layer Security (DTLS) [RFC6347] as a transport protocol between a Traversal Using Relays around NAT (TURN) [RFC5766] client and a TURN server. It also specifies modifications to the TURN URIs [RFC7065] and to the TURN resolution mechanism [RFC5928] to facilitate the resolution of TURN URIs into the IP address and port of TURN servers supporting DTLS as a transport protocol.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 4, 2014.

Copyright Notice

Table of Contents

1. Introduction

TURN [RFC5766] defines Transport Layer Security (TLS) over TCP (simply referred to as TLS [RFC5246]) as the transport for TURN due to additional security advantages it offers over plain UDP or TCP transport. But TLS-over-TCP is not an optimal transport when TURN is used for its originally intended purpose, which is to support multimedia sessions. This sub-optimality primarily stems from the added latency incurred by the TCP-based head-of-line (HOL) blocking problem coupled with additional TLS buffering (for integrity checks). This is a well documented and understood transport limitation for secure real-time communications.

TLS-over-UDP (referred to as DTLS [RFC6347]) offers the same security advantages as TLS-over-TCP, but without the undesirable latency concerns.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] when they appear in ALL CAPS. When these words are not in ALL CAPS (such as "must" or "Must"), they have their usual English meanings, and are not to be interpreted as RFC 2119 key words.

3. DTLS as Transport for TURN

TURN [RFC5766] defines three combinations of transports/allocations: UDP/UDP, TCP/UDP and TLS/UDP. This document adds DTLS/UDP as a valid combination.

[RFC6062] states that TCP allocations cannot be obtained using a UDP association between client and server. The fact that DTLS uses UDP implies that TCP allocations MUST NOT be obtained using a DTLS association between client and server.

By default, TURN over DTLS uses port 5349, the same port as TURN over TLS. However, the SRV procedures can be implemented to use a different port (as described in Section 6 of [RFC5766]. When using SRV records, the service name MUST be set to "turns" and the application name to "udp".

4. DTLS Support in TURN URIs

This document does not make any changes to the syntax of a TURN URI [RFC7065]. As indicated in Section 3 of [RFC7065], secure transports like TURN over TLS, and now TURN over DTLS, MUST use the "turns" URI scheme. When using the "turns" URI scheme to designate TURN over DTLS, the transport value of the TURN URI, if set, MUST be "udp".

5. Resolution Mechanism for TURN over DTLS

This document defines a new Straightforward Naming Authority Pointer (S-NAPTR) application protocol tag: "turn.dtls".

The <transport> component, as provisioned or resulting from the parsing of a TURN URI, is passed without modification to the TURN resolution mechanism defined in Section 3 of [RFC5928], but with the following alterations to that algorithm:

- The acceptable values for transport name are extended with the addition of "dtls".

- The acceptable values in the ordered list of supported TURN transports is extended with the addition of "Datagram Transport Layer Security (DTLS)".

- The resolution algorithm ckeck rules list is extended with the addition of the following step:

  If <secure> is true and <transport> is defined as "udp" but the list of TURN transports supported by the application does not contain DTLS, then the resolution MUST stop with an error.

- The 5th rule of the resolution algorithm check rules list is modified to read like this:

  If <secure> is true and <transport> is not defined but the list of TURN transports supported by the application does not contain TLS or DTLS, then the resolution MUST stop with an error.

- Table 1 is modified to add the following line:

<secure>	<transport>	TURN Transport
true	"udp"	DTLS

- In step 1 of the resolution algorithm the default port for DTLS is 5349.

- In step 4 of the resolution algorithm the following is added to the list of conversions between the filtered list of TURN transports supported by the application and application protocol tags:

  "turn.dtls" is used if the TURN transport is DTLS.

Note that using the [RFC5928] resolution mechanism does not imply that additional round trips to the DNS server will be needed (e.g., the TURN client will start immediately if the TURN URI contains an IP address).

6. Implementation Status

[[Note to RFC Editor: Please remove this section and the reference to [RFC6982] before publication.]]

This section records the status of known implementations of the protocol defined by this specification at the time of posting of this Internet-Draft, and is based on a proposal described in [RFC6982]. The description of implementations in this section is intended to assist the IETF in its decision processes in progressing drafts to RFCs. Please note that the listing of any individual implementation here does not imply endorsement by the IETF. Furthermore, no effort has been spent to verify the information presented here that was supplied by IETF contributors. This is not intended as, and must not be construed to be, a catalog of available implementations or their features. Readers are advised to note that other implementations may exist.

According to [RFC6982], "this will allow reviewers and working groups to assign due consideration to documents that have the benefit of running code, which may serve as evidence of valuable experimentation and feedback that have made the implemented protocols more mature. It is up to the individual working groups to use this information as they see fit".

6.1. turnuri

Organization: Impedance Mismatch

Name: turnuri 0.5.0 http://debian.implementers.org/stable/source/turnuri.tar.gz

Description: A reference implementation of the URI and resolution mechanism defined in this document, RFC 7065 [RFC7065] and RFC 5928 [RFC5928].

Level of maturity: Beta.

Coverage: Fully implements the URIs and resolution mechanism defined in this specification, in RFC 7065 and in RFC 5928.

Licensing: AGPL3

Implementation experience: TBD

Contact: Marc Petit-Huguenin <marc@petit-huguenin.org>.

7. Security Considerations

TURN over DTLS as a TURN transport does not introduce any specific security considerations beyond those for TURN over TLS detailed in [RFC5766].

The usage of "udp" as a transport parameter with the "turns" URI scheme does not introduce any specific security issues beyond those discussed in [RFC7065].

The new S-NAPTR application protocol tag defined in this document as well as the modifications this document makes to the TURN resolution mechanism described in [RFC5928] do not introduce any additional security considerations beyond those outlined in [RFC5928].

8. IANA Considerations

This specification contains the registration information for one S-NAPTR application protocol tags (in accordance with [RFC3958]).

Application Protocol Tag: turn.dtls

Intended Usage: See Section 5

Interoperability considerations: N/A

Security considerations: See Section 7

Relevant publications: This document

Contact information: Marc Petit-Huguenin

Author/Change controller: The IESG

This specification also contains the registration information for one Service Name and Transport Protocol Port Number (in accordance with [RFC6335]).

Service Name: turns

Transport Protocol(s): UDP

Assignee: IESG

Contact: Marc Petit-Huguenin

Description: TURN over DTLS

Reference: This document

Port Number: 5349

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3958] Daigle, L. and A. Newton, "Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS)", RFC 3958, January 2005.

[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, April 2010.

[RFC5928] Petit-Huguenin, M., "Traversal Using Relays around NAT (TURN) Resolution Mechanism", RFC 5928, August 2010.

[RFC6062] Perreault, S. and J. Rosenberg, "Traversal Using Relays around NAT (TURN) Extensions for TCP Allocations", RFC 6062, November 2010.

[RFC6335] Cotton, M., Eggert, L., Touch, J., Westerlund, M., and S. Cheshire, "Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry", BCP 165, RFC 6335, August 2011.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, January 2012.

[RFC7065] Petit-Huguenin, M., Nandakumar, S., Salgueiro, G., and P. Jones, "Traversal Using Relays around NAT (TURN) Uniform Resource Identifiers", RFC 7065, November 2013.

9.2. Informative References

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC6982] Sheffer, Y. and A. Farrel, "Improving Awareness of Running Code: The Implementation Status Section", RFC 6982, July 2013.

Appendix A. Examples

Table 1 shows how the <secure>, <port> and <transport> components are populated for a TURN URI that uses DTLS as its transport. For all these examples, the <host> component is populated with "example.net".

URI	<secure>	<port>	<transport>
turns:example.net?transport=udp	true		DTLS

Table 1

With the DNS RRs in Figure 1 and an ordered TURN transport list of {DTLS, TLS, TCP, UDP}, the resolution algorithm will convert the TURN URI "turns:example.net" to the ordered list of IP address, port, and protocol tuples in Table 2.

```
example.net.
IN NAPTR 100 10 "" RELAY:turn.udp:turn.dtls "" datagram.example.net.
IN NAPTR 200 10 "" RELAY:turn.tcp:turn.tls "" stream.example.net.

datagram.example.net.
IN NAPTR 100 10 S RELAY:turn.udp "" _turn._udp.example.net.
IN NAPTR 100 10 S RELAY:turn.dtls "" _turns._udp.example.net.

stream.example.net.
IN NAPTR 100 10 S RELAY:turn.tcp "" _turn._tcp.example.net.
IN NAPTR 200 10 A RELAY:turn.tls "" a.example.net.

_turn._udp.example.net.
IN SRV   0 0 3478 a.example.net.

_turn._tcp.example.net.
IN SRV   0 0 5000 a.example.net.

_turns._udp.example.net.
IN SRV   0 0 5349 a.example.net.

a.example.net.
IN A     192.0.2.1
```

Figure 1

Order	Protocol	IP address	Port
1	DTLS	192.0.2.1	5349
2	TLS	192.0.2.1	5349

Table 2

Authors' Addresses

Marc Petit-Huguenin
Jive Communications
1275 West 1600 North, Suite 100
Orem, UT 84057
USA

Email: marcph@getjive.com

Gonzalo Salgueiro
Cisco Systems
7200-12 Kit Creek Road
Research Triangle Park, NC 27709
US

Email: gsalguei@cisco.com