Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 7, 2014

H. Alvestrand
Google

September 3, 2013

Transports for RTCWEB
draft-ietf-rtcweb-transports-01

Abstract

This document describes the data transport protocols used by RTCWEB, including the protocols used for interaction with intermediate boxes such as firewalls, relays and NAT boxes.

Requirements Language

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 RFC 2119 [RFC2119].

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 March 7, 2014.

Copyright Notice

Table of Contents

1. Introduction

The IETF RTCWEB effort, part of the WebRTC effort carried out in cooperation between the IETF and the W3C, is aimed at specifying a protocol suite that is useful for real time multimedia exchange between browsers.

The overall effort is described in the RTCWEB overview document, [I-D.ietf-rtcweb-overview]. This document focuses on the data transport protocos that are used by conforming implementations.

This protocol suite is designed for WebRTC, and intends to satisfy the security considerations described in the WebRTC security documents, [I-D.ietf-rtcweb-security] and [I-D.ietf-rtcweb-security-arch].

2. Transport and Middlebox specification

2.1. System-provided interfaces

The protocol specifications used here assume that the following protocols are available to the implementations of the RTCWEB protocols:

- UDP. This is the protocol assumed by most protocol elements described.
- TCP. This is used for HTTP/WebSockets, as well as for TURN/SSL and ICE-TCP.

For both protocols, this specification assumes the ability to set the DSCP code point of the sockets opened on a per-packet basis, in order to achieve the prioritizations described in [I-D.ietf-rtcweb-qos]. It does not assume that the DSCP codepoints will be honored, and does assume that they may be zeroed or changed, since this is a local configuration issue.

If DSCP code points can only be set on a per-socket basis, not per-packet, one loses the ability to have the network discriminate reliably between classes of traffic sent over the same transport, but this does not prevent communication.

This specification does not assume that the implementation will have access to ICMP or raw IP.

2.2. Middle box related functions

The primary mechanism to deal with middle boxes is ICE, which is an appropriate way to deal with NAT boxes and firewalls that accept traffic from the inside, but only from the outside if it's in response to inside traffic (simple stateful firewalls).

In order to deal with situations where both parties are behind NATs which perform endpoint-dependent mapping (as defined in [RFC5128] section 2.4), TURN [RFC5766] MUST be supported.

In order to deal with firewalls that block all UDP traffic, TURN using TCP between the client and the server MUST be supported, and TURN using TLS between the client and the server MUST be supported.

ICE TCP candidates [RFC6062] MAY be supported; this may allow applications to achieve peer-to-peer communication across UDP-blocking firewalls, but this also requires use of the SRTP/AVPF/TCP profile of RTP.

The following specifications MUST be supported:

- ICE [RFC5245]

- TURN, including TURN over TCP[RFC5766].

TURN over TLS over TCP MAY be supported. (QUESTION: SHOULD? MUST?)

For referring to STUN and TURN servers, this specification depends on the STUN URI, [I-D.nandakumar-rtcweb-stun-uri].

Further discussion of the interaction of RTCWEB with firewalls is contained in [I-D.hutton-rtcweb-nat-firewall-considerations]. This document makes no requirements on interacting with HTTP proxies or HTTP proxy configuration methods.

2.3. Transport protocols implemented

For data transport over the RTCWEB data channel [I-D.ietf-rtcweb-data-channel], RTCWEB implementations support SCTP over DTLS over ICE. This is specified in [I-D.ietf-tsvwg-sctp-dtls-encaps]. Negotiation of this transport in SCTP is defined in [I-D.ietf-mmusic-sctp-sdp].

The setup protocol for RTCWEB data channels is described in [I-D.jesup-rtcweb-data-protocol].

For transport of media, secure RTP is used. The details of the

profile of RTP used are described in "RTP Usage" [I-D.ietf-rtcweb-rtp-usage].

RTCWEB implementations MUST support multiplexing of DTLS and RTP over the same port pair, as described in the DTLS_SRTP specification [RFC5764], section 5.1.2. Further separation of the DTLS traffic into SCTP and "other" is described in <need reference>.

3. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

4. Security Considerations

Security considerations are enumerated in [I-D.ietf-rtcweb-security].

5. Acknowledgements

This document is based on earlier versions embedded in [I-D.ietf-rtcweb-overview], which were the results of contributions from many RTCWEB WG members.

6. References

6.1. Normative References

[I-D.ietf-mmusic-sctp-sdp]
Loreto, S. and G. Camarillo, "Stream Control Transmission Protocol (SCTP)-Based Media Transport in the Session Description Protocol (SDP)", draft-ietf-mmusic-sctp-sdp-04 (work in progress), June 2013.

[I-D.ietf-rtcweb-data-channel]
Jesup, R., Loreto, S., and M. Tuexen, "RTCWeb Data Channels", draft-ietf-rtcweb-data-channel-05 (work in progress), July 2013.

[I-D.ietf-rtcweb-qos]
Dhesikan, S., Druta, D., Jones, P., and J. Polk, "DSCP and other packet markings for RTCWeb QoS", draft-ietf-rtcweb-qos-00 (work in progress), October 2012.

[I-D.ietf-rtcweb-rtp-usage]
Perkins, C., Westerlund, M., and J. Ott, "Web Real-Time Communication (WebRTC): Media Transport and Use of RTP", draft-ietf-rtcweb-rtp-usage-07 (work in progress), July 2013.

[I-D.ietf-rtcweb-security]
Rescorla, E., "Security Considerations for WebRTC", draft-ietf-rtcweb-security-05 (work in progress), July 2013.

[I-D.ietf-rtcweb-security-arch]
Rescorla, E., "WebRTC Security Architecture", draft-ietf-rtcweb-security-arch-07 (work in progress), July 2013.

[I-D.ietf-tsvwg-sctp-dtls-encaps]
Jesup, R., Loreto, S., Stewart, R., and M. Tuexen, "DTLS Encapsulation of SCTP Packets", draft-ietf-tsvwg-sctp-dtls-encaps-01 (work in progress), July 2013.

[I-D.nandakumar-rtcweb-stun-uri]
Nandakumar, S., Salgueiro, G., Jones, P., and M. Petit-Huguenin, "URI Scheme for Session Traversal Utilities for NAT (STUN) Protocol", draft-nandakumar-rtcweb-stun-uri-05 (work in progress), July 2013.

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

[RFC5245] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", RFC 5245, April 2010.

[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, May 2010.

[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.

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

6.2. Informative References

[I-D.hutton-rtcweb-nat-firewall-considerations]
Stach, T., Hutton, A., and J. Uberti, "RTCWEB Considerations for NATs, Firewalls and HTTP proxies", draft-hutton-rtcweb-nat-firewall-considerations-01 (work in progress), June 2013.

[I-D.ietf-rtcweb-overview]
Alvestrand, H., "Overview: Real Time Protocols for Brower-based Applications", draft-ietf-rtcweb-overview-07 (work in progress), August 2013.

[I-D.jesup-rtcweb-data-protocol]
Jesup, R., Loreto, S., and M. Tuexen, "WebRTC Data Channel Protocol", draft-jesup-rtcweb-data-protocol-04 (work in progress), February 2013.

[RFC5128] Srisuresh, P., Ford, B., and D. Kegel, "State of Peer-to-Peer (P2P) Communication across Network Address Translators (NATs)", RFC 5128, March 2008.

Appendix A. Change log

A.1. Changes from -00 to -01

- Clarified DSCP requirements, with reference to -qos-
- Clarified "symmetric NAT" -> "NATs which perform endpoint-dependent mapping"
- Made support of TURN over TCP mandatory
- Made support of TURN over TLS a MAY, and added open question
- Added an informative reference to -firewalls-
- Called out that we don’t make requirements on HTTP proxy interaction (yet)

Author's Address

Harald Alvestrand
Google

Email: harald@alvestrand.no