RTCWEB
Internet-Draft
Intended status: Standards Track
Expires: October 11, 2014

M. Thomson
Mozilla

April 9, 2014

# Application Layer Protocol Negotiation for Web Real-Time Communications (WebRTC)

draft-thomson-rtcweb-alpn-00

## Abstract

Application Layer Protocol Negotiation (ALPN) labels are defined for use in identifying Web Real-Time Communications (WebRTC) usages of Datagram Transport Layer Security (DTLS). Labels are provided for identifying a session that uses a combination of WebRTC compatible media and data, and for identifying a session requiring confidentiality protection.

## 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 October 11, 2014.

## Copyright Notice

Table of Contents



## 1. Introduction

Web Real-Time Communications (WebRTC) [I-D.ietf-rtcweb-overview] uses Datagram Transport Layer Security (DTLS) [RFC6347] to secure all peer-to-peer communications.

Identifying WebRTC protocol usage with Application Layer Protocol Negotiation (ALPN) [I-D.ietf-tls-applayerprotoneg] enables an endpoint to positively identify WebRTC uses and distinguish them from other DTLS uses.

Different WebRTC uses can be advertised and behavior can be constrained to what is appropriate to a given use. In particular, this allows for the identifications of sessions that require confidentiality protection.

### 1.1. Conventions and Terminology

At times, this document falls back on shorthands for establishing interoperability requirements on implementations: the capitalized words "MUST", "SHOULD" and "MAY". These terms are defined in [RFC2119].

## 2. ALPN Labels for WebRTC

The following four labels are defined for use in ALPN:

webrtc The DTLS session is used to establish keys for a Secure Real-time Transport Protocol (SRTP) - known as DTLS-SRTP - as described in [RFC5764]. The DTLS record layer is used for WebRTC data channels [I-D.ietf-rtcweb-data-channel].

c-webrtc The DTLS session is used for confidential WebRTC communications, where peers agree to maintain the confidentiality of the communications, as described in Section 3.

A more thorough definition of what WebRTC communications entail is included in [I-D.ietf-rtcweb-transports].

## 3. Media Confidentiality

Private communications in WebRTC depend on separating control (i.e., signaling) capabilities and access to media [I-D.ietf-rtcweb-security-arch]. In this way, an application can establish a session that is end-to-end confidential, where the ends in question are user agents (or browsers) and not the signaling application.

Without some form of indication that is securely bound to the session, a WebRTC endpoint is unable to properly distinguish between session that requires confidentiality protection and one that does not.

A browser is required to enforce confidentiality using isolation controls similar to those used in content cross-origin protections (see Section 5.3 [1] of [HTML5]). These protections ensure that media is protected from applications. Applications are not able to read or modify the contents of a protected flow of media. Media that is produced from a session using the "c-webrtc" identifier MUST only be displayed to users.

A WebRTC implementation MUST only send media over a "c-webrtc" session that comes from user-controlled sources. Media from sources that are controlled by third parties (such as the signaling application) could be used to create confusion about the content and origin of data. This cannot prevent confusion when rendered as a web page, for example, but browsers are required to provide ways to identify media and its provenance (see Section 5.5 of [I-D.ietf-rtcweb-security-arch]).

Confidentiality protections of this sort are not expected to be possible for data that is sent using data channels. Thus, it is expected that data channels will not be employed for sessions that negotiate confidentiality. In the browser context, confidential data depends on having both data sources and consumers that are exclusively browser- or user-based. No mechanisms currently exist to take advantage of data confidentiality, though some use cases suggest that this could be useful, for example, confidential peer-to-peer file transfer.

Generally speaking, ensuring confidentiality depends on authenticating the communications peer. However, this mechanism explicitly does not depend on authentication; a WebRTC endpoint that accepts a session with this ALPN identifier MUST respect confidentiality no matter what identity is attributed to a peer.

## 4. Security Considerations

Confidential communications depends on more than just an agreement from browsers.

Information is not confidential if it is displayed to those other than to whom it is intended. Peer authentication [I-D.ietf-rtcweb-security-arch] is necessary to ensure that data is only sent to the intended peer.

This is not a digital rights management mechanism. Even with an authenticated peer, a user is not prevented from using other mechanisms to record or forward media. This means that (for example) screen recording devices, tape recorders, portable cameras, or a cunning arrangement of mirrors could variously be used to record or redistribute media once delivered. Similarly, if media is visible or audible (or otherwise accessible) to others in the vicinity, there are no technical measures that protect the confidentiality of that media. In other cases, effects might not be temporally localized: transmitted smells could linger for a period after communications cease.

The only guarantee provided by this mechanism and the browser that implements it is that the media was delivered to the user that was authenticated. Individual users will still need to make a judgment about how their peer intends to respect the confidentiality of any information provided.

On a shared computing platform like a browser, other entities with access to that platform (i.e., web applications), might be able to access information that would compromise the confidentiality of communications. Implementations MAY choose to limit concurrent access to input devices during confidential communications session.

For instance, another application that is able to access a microphone might be able to sample confidential audio that is playing through speakers. This is true even if acoustic echo cancellation, which attempts to prevent this from being possible, is used. Similarly, an application with access to a video camera might be able to use reflections to access confidential video.

## 5. IANA Considerations

The following two entries are added to the "Application Layer Protocol Negotiation (ALPN) Protocol IDs" registry established by [I-D.ietf-tls-applayerprotoneg].

The "webrtc" identifies mixed media and data communications using SRTP and data channels:

Protocol: WebRTC Media and Data

Identification Sequence: 0x77 0x65 0x62 0x72 0x74 0x63 ("webrtc")

Specification: This document (RFCXXXX)

The "c-webrtc" identifies confidential WebRTC communications:

Protocol: Confidential WebRTC Media and Data

Identification Sequence: 0x63 0x2d 0x77 0x65 0x62 0x72 0x74 0x63 ("c-webrtc")

Specification: This document (RFCXXXX)

## 6. References

### 6.1. Normative References

[I-D.ietf-rtcweb-data-channel]
Jesup, R., Loreto, S., and M. Tuexen, "WebRTC Data Channels", draft-ietf-rtcweb-data-channel-07 (work in progress), February 2014.

[I-D.ietf-tls-applayerprotoneg]
Friedl, S., Popov, A., Langley, A., and S. Emile, "Transport Layer Security (TLS) Application Layer Protocol Negotiation Extension", draft-ietf-tls-applayerprotoneg-05 (work in progress), March 2014.

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

[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.

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

## 6.2. Informative References

[HTML5] Berjon, R., Leithead, T., Doyle Navara, E., O'Connor, E., and S. Pfeiffer, "HTML 5", CR CR-html5-20121217, August 2010, <http://www.w3.org/TR/2012/CR-html5-20121217/>.

[I-D.ietf-rtcweb-overview] Alvestrand, H., "Overview: Real Time Protocols for Brower-based Applications", draft-ietf-rtcweb-overview-09 (work in progress), February 2014.

[I-D.ietf-rtcweb-security-arch] Rescorla, E., "WebRTC Security Architecture", draft-ietf-rtcweb-security-arch-09 (work in progress), February 2014.

[I-D.ietf-rtcweb-transports] Alvestrand, H., "Transports for RTCWEB", draft-ietf-rtcweb-transports-03 (work in progress), March 2014.

## 6.3. URIs

[1] http://www.w3.org/TR/2012/CR-html5-20121217/browsers.html#origin

## Author's Address

Martin Thomson
Mozilla
331 E Evelyn Street
Mountain View, CA 94041
US

Email: martin.thomson@gmail.com