SIMPLE Working Group	C.H. Holmberg
Internet-Draft	S.B. Blau
Intended status: Standards Track	Ericsson
Expires: December 18, 2011	June 16, 2011

Connection Establishment for Media Anchoring (CEMA) for the Message Session Relay Protocol (MSRP)

draft-ietf-simple-msrp-sessmatch-13.txt

Abstract

This document defines an MSRP extension, Connection Establishment for Media Anchoring (CEMA). Support of the extension is optional. MSRP endpoints can implement the extension in order to allow MSRP communication in networks where Middleboxes anchor the MSRP connection, without the need for the Middleboxes to enable MSRP B2BUA functionality in most cases. The document also defines a Session Description Protocol (SDP) [RFC4566] attribute, a=msrp-cema, that can be used by MSRP endpoints to indicate support of the CEMA extension.

Status of this Memo

This Internet-Draft will expire on December 18, 2011.

Copyright Notice

Table of Contents

1. Introduction

The Message Session Relay Protocol (MSRP) [RFC4975] is designed to use MSRP relays [RFC4976] as a means for Network Address Translation (NAT) traversal and policy enforcement.

However, many Session Initiation Protocol (SIP) [RFC3261] networks, in which MSRP usage is emerging, also contain Middleboxes, that anchor and control media, perform tasks such as NAT traversal, performance monitoring, lawful intercept, address domain bridging, interconnect Service Layer Agreement (SLA) policy enforcement, etc. An example is the Interconnection Border Control Function (IBCF) [3GPP.23.228], defined by the 3rd Generation Partnership Project (3GPP). The IBCF controls a media relay that handles all types of SIP session media (voice, video, MSRP, etc).

MSRP, as defined in RFC 4975 [RFC4975] and RFC 4976 [RFC4976], cannot be anchored when MSRP endpoints communicate with such Middleboxes, unless the Middleboxes implement and enable MSRP Back-To-Back User Agent (B2BUA) functionality for all calls. The reason is that Middleboxes modify the address:port information in SDP c/m-line in order to anchor media, and since the active MSRP UA establishes the MSRP TCP connection based on the MSRP URI of the SDP a=path attribute, this means that the MSRP connection will not, unless the Middlebox also modifies the MSRP URI of the topmost SDP a=path attribute be routed through the Middlebox, which in many scenarios will prevent the MSRP connection from being established. However, if the Middlebox modifies the MSRP URI of the SDP a=path attribute, then the MSRP URI comparison procedure [RFC4975], which requires consistency between the address information in the MSRP messages and the address information carried in the MSRP URI of the SDP a=path attribute, will fail. The matching will fail if Middleboxes modify the address information in the MSRP URI of the SDP a=path attribute, but do not enable MSRP B2BUA functionality and perform the corresponding modification in the associated MSRP messages. However, the enabling of MSRP B2BUA functionality requires substantially more resource usage in the Middlebox, that normally result in negative performance impact.

This specification defines an MSRP extension, Connection Establishment for Media Anchoring (CEMA), that in most cases allows MSRP endpoints to communicate with Middleboxes without a need for the Middleboxes to enable MSRP B2BUA functionality. In such cases, Middleboxes that want to anchor the MSRP connection simply modify the SDP c/m-line address information (similar to what it does for non-MSRP media types), and MSRP endpoints that support the CEMA extension will use the SDP c/m-line address information for establishing the TCP (or TLS) connection to be used for sending and receiving of MSRP messages.

The CEMA extension is fully backward compatible. In scenarios where MSRP endpoints that do not support the CEMA extension are able to establish MSRP connectivity, an MSRP endpoint that supports the CEMA extension behaves in the same way as an MSRP endpoint that does not support it. The CEMA extension only provides an alternative mechanism for negotiating and providing the address information for the MSRP TCP connection. Once the MSRP TCP connection has been created, an MSRP endpoint that supports the CEMA extension acts according to the procedures (e.g. for creating MSRP messages, performing checks when receiving MSRP messages etc) defined in RFC 4975 (and RFC 4976, when it is using a relay for MSRP communication).

2. Conventions

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 BCP 14, RFC 2119 [RFC2119].

In this specification the terminology "fingerprint based TLS authentication" and "name based TLS authentication" are used to refer to the two cases where:

1. An MSRP endpoint uses a self-signed TLS certificate and sends a certificate fingerprint in SDP (fingerprint based TLS authentication).
2. An MSRP endpoint uses a certificate from a well known certificate authority and the other endpoint matches the hostname in the received TLS communication SubjectAltName parameter towards the hostname received in the MSRP URI in SDP (name based TLS authentication).

Middlebox: Within the scope of this document, Middlebox refers to a network SIP device that modifies SDP media address:port information in order to steer (anchor) media flows described in the SDP, including TCP connections used for MSRP communication, through a media proxy function controlled by the SIP device. In most cases the media proxy function relays the MSRP messages without modification, while in other cases it enables MSRP B2BUA functionality. Other SIP related functions (e.g. related to routing, modification of SIP information etc) performed by the SIP device, and whether it acts a SIP B2BUA or not, is outside the scope of the definition. Section 5 describes additional assumptions regarding how the Middlebox handles MSRP in order to support the extension defined in this document.

3. Applicability statement

This document defines an MSRP extension, Connection Establishment for Media Anchoring (CEMA). Support of the extension is optional. MSRP endpoints can implement the extension in order to allow MSRP communication in networks where Middleboxes anchor the MSRP connection, without the need for the Middleboxes to enable MSRP B2BUA functionality in most cases. The document also defines a Session Description Protocol (SDP) [RFC4566] attribute, a=msrp-cema, that can be used by MSRP endpoints to indicate support of the CEMA extension.

The CEMA extension is primarily intended for MSRP endpoints that operate in networks in which Middleboxes that want to anchor media connections are deployed, without the need for the Middleboxes to enable MSRP B2BUA functionality. An example of such network is the IP Multimedia Subsystem (IMS) defined by the 3rd Generation Partnership Project (3GPP). The extension is also useful for other MSRP endpoints operating in other networks, but that communicate with MSRP endpoints in networks with such Middleboxes, unless there is a gateway between the networks that by default always enable MSRP B2BUA functionality.

4. Connection Establishment for Media Anchoring Mechanism

4.1. General

This section defines how an MSRP endpoint that supports the CEMA extension generates SDP offers and answers for MSRP, and what SDP information elements the MSRP endpoint uses when creating the TCP connection for the MSRP messages.

4.2. MSRP Offerer Procedures

When an MSRP endpoint sends an SDP offer for MSRP, it generates the SDP offer according to the procedures in RFC 4975 (and RFC 4976, if it is using a relay for MSRP communication), with the following additions and modifications:
1) The MSRP endpoint MUST include an SDP a=msrp-cema attribute in the MSRP media description of the SDP offer.
2) If the MSRP endpoint is not using a relay for MSRP communication, it MUST include an SDP a=setup attribute in the MSRP media description of the SDP offer, according to the procedures in RFC [RFC6135].
3) If the MSRP endpoint is using a relay for MSRP communication, it MUST include the address information on the relay (the MSRP URI of the topmost SDP a=path attribute), rather than the address information of itself, in the SDP c/m-line associated with the MSRP media description. In addition, it MUST include an SDP a=setup:actpass attribute in the MSRP media description of the SDP offer.
When the MSRP endpoint receives the first SDP answer to the SDP offer above, and the SDP answer indicates that the offered MSRP media has been accepted by the remote MSRP endpoint (i.e. the port number of the MSRP media description is not set to zero), if the MSRP media description of the SDP answer does not contain an SDP a=msrp-cema attribute, the MSRP endpoint MUST check whether any of the following criteria is fulfilled:
1) The SDP c/m-line address information associated with the MSRP media description does not match the information in the MSRP URI of the topmost SDP a=path attribute, and the MSRP media description contains an SDP a=setup:active attribute (indicating that the remote MSRP endpoint is "active").
2) The MSRP media description contains multiple SDP a=path attributes (indicating that MSRP relays are used).
If any, or both, of the criteria above is fulfilled, the MSRP endpoint MUST fallback to RFC 4975 behavior, by sending a new SDP offer according to the procedures in RFC 4975 and RFC 4976. The new offer MUST NOT contain an SDP a=msrp-cema attribute.

NOTE: In the absence of the SDP a=msrp-cema attribute in the new offer, the Middlebox will in all cases have to, in order to be able to anchor MSRP media, enable MSRP B2BUA functionality.

NOTE: The MSRP endpoint can send the new offer within the existing early dialog [RFC3261], or it can terminate the early dialog and establish a new dialog by sending the new offer in a new initial INVITE request.

In all other cases, where the MSRP endpoint becomes "active", it MUST use the SDP c/m-line for establishing the MSRP TCP connection. If the MSRP endpoint becomes "passive", it will wait for the remote MSRP endpoint to establish the TCP connection, according to the procedures in RFC 4975.

4.3. MSRP Answerer Procedures

When an MSRP endpoint receives an SDP offer for MSRP, it MUST check the following criteria:

1) Both MSRP endpoints are using relays for MSRP communication.

NOTE: If the MSRP media description of the SDP offer contains contains multiple SDP a=path attributes, it can be determined that the remote MSRP endpoint is using a relay for MSRP communication.

2) The remote MSRP endpoint uses a relay for MSRP communciation, and will become "active" (either by default, or if the MSRP media description of the SDP offer contains an SDP a=setup:active attribute).

NOTE: This case should not occur if the remote MSRP endpoint supports the CEMA extension, as the remote MSRP endpoint would include an SDP a=setup:actpass attribute in the SDP offer, as described in section 4.2.

3) The MSRP endpoint uses a relay for MSRP communication, and is not able to become "passive" (the MSRP media description of the offer contains an SDP a=setup:passive attribute).

NOTE: This case should never occur, as an MSRP entity is not allowed to include an SDP a=setup:passive attribute in an SDP offer, as described in RFC 6135.

4) The MSRP media description of the SDP offer does not contain an SDP a=msrp-cema attribute, the SDP c/m-line address information associated with the MSRP media description does not match the information in the MSRP URI of the topmost SDP a=path attribute, and the remote MSRP endpoint will become "active" (either by default, or if the MSRP media description of the SDP offer contains an SDP a=setup:active attribute).

If any, or all, of the criteria above is fulfilled, the MSRP endpoint MUST fallback to RFC 4975 behavior, and generate the associated SDP answer according to the procedures in RFC 4975 and RFC 4976. The MSRP endpoint MUST NOT insert an SDP a=msrp-cema attribute in the MSRP media description of the SDP answer.

In all other cases, the MSRP endpoint generates the associated SDP answer according to the procedures in RFC 4975 and RFC 4976, with the following additions and modifications:

1) The MSRP endpoint MUST include an SDP a=msrp-cema attribute in the MSRP media description of the SDP answer.
2) If the MSRP endpoint is not using a relay for MSRP communication, it MUST include an SDP a=setup attribute in the MSRP media description of the answer, according to the procedures in RFC 6135.
3) If the MSRP endpoint is using a relay for MSRP communication, it MUST include the address information on the relay (the MSRP URI of the topmost SDP a=path attribute), rather than the address information of itself, in the SDP c/m-line associated with the MSRP media description. In addition, it MUST include an SDP a=setup: passive attribute in the MSRP media description of the SDP answer.
If the MSRP endpoint included an SDP a=msrp-cema attribute in the MSRP media description of the SDP answer, and if the MSRP endpoint becomes "active", it MUST use the received SDP c/m-line for establishing the MSRP TCP connection. If the MSRP endpoint becomes "passive", it will wait for the remote MSRP endpoint to establish the TCP connection, according to the procedures in RFC 4975.

4.4. Usage With The Alternative Connection Model

An MSRP endpoint that supports the CEMA extension MUST in addition also support the mechanism defined in RFC 6135, as it extends the number of scenarios where the CEMA extension can be used, and Middleboxes do not need to enable MSRP B2BUA functionality. An example is where a MSRP endpoint is using a relay for MSRP communication, and it needs to be "passive" in order to use the CEMA extension (instead of doing a fallback to RFC 4975 behavior.

5. Middlebox assumptions

5.1. General

This document does not specify explicit Middlebox behavior, eventhough some of the procedures will be enabled by Middleboxes. However, as the main reason behind the CEMA extension is to allow MSRP endpoints to communicate in networks where Middleboxes that want to anchor media are present, this document makes certain assumptions regarding to how such Middleboxes behave.

5.2. MSRP awareness

This document assumes that an Middlebox, in order to support interoperability between UAs that support the CEMA extension and UAs that do not support the extension, is MSRP aware, meaning that it implements MSRP B2BUA functionality, and that it enables that functionality in cases where support of the CEMA extension is not indicated. In cases where support of the CEMA extension is indicated by at least one MSRP endpoint, the Middlebox can simply modifies the SDP c/m-line address information for the MSRP connection. However, MSRP communication will work if the Middlebox enables MSRP B2BUA functionality also in such cases.

5.3. TCP connection reuse

When the CEMA extension is used, in cases where Middleboxes do not need to enable MSRP B2BUA functionality, the Middleboxes are not required to parse and modify the MSRP payload. An Middlebox that does not parse the MSRP payload might not enable re-usage of TCP connections for multiple MSRP sessions. Instead, in order to associate an MSRP message with a specific session, the Middlebox often assigns a unique local address:port combination for each MSRP session.

5.4. SDP integrity

This document assumes that Middleboxes are able to modify the SDP address information associated with the MSRP media, and therefore can not be deployed in environments that require SIP identity [RFC4916] based peer-to-peer SDP protection.

5.5. TLS

This document considers two approaches how an Middlebox handles TLS protected MSRP connections.
In the first approach, the Middlebox relays the MSRP media packets at the transport layer. The TLS handshake and resulting security association (SA) are established peer-to-peer between the MSRP endpoints. The Middlebox will see encrypted MSRP media packets, but is unable to inspect the cleartext content.
In the second approach, the Middlebox acts as a TLS B2BUA, meaning that separate SAs are established between the Middlebox and each MSRP endpoint. The Middlebox decrypts MSRP media packets received from one MSRP endpoint, and then re-encrypts them before sending them toward the other MSRP endpoint. With this approach, the Middlebox can inspect and modify the MSRP message content.

6. Security Considerations

6.1. Man in the middle

In some cases, where MSRP B2BUA functionality does not need to be enabled, the CEMA extension makes it easier for a man in the middle (MiTM) to transparently insert itself in the communication between MSRP endpoints in order to monitor or record unprotected MSRP communication. It does not however make it easier for a MiTM to monitor TLS protected MSRP, or in any significant way modify TLS protected MSRP content or even find out that the packets contain MSRP messages, since that would require the MiTM to implement MSRP B2BUA functionality, no matter if UAs support the CEMA extension or not. It would thus require the MiTM to terminate the TCP/TLS/MSRP connection in both directions.

6.2. TLS

The CEMA extension supports the usage of name based authentication for TLS, also in the presence of Middleboxes.
NOTE: If an Middlebox acts as a TLS B2BUA, MSRP endpoints will also be able to use fingerprint based authentication for TLS, no matter if they support the CEMA extension or not. In such cases, as the Middlebox acts as a TLS endpoints, MSRP endpoints might be given an incorrect impression that there is an end-to-end SA between the MSRP endpoints.
If an Middlebox does not act as a TLS B2BUA, fingerprint based authentication will not work, as the "SIP Identity" based integrity protection of SDP will break. Therefore, in addition to the authentication mechanisms defined in RFC 4975, an MSRP endpoint supporting the CEMA extension SHOULD also support an authentication mechanism that does not rely on peer-to-peer SDP integrity.
It is RECOMMENDED that an MSRP endpoint supports one of the following authentication mechanisms:
1) TLS certificates together with support of interacting with a Certificate Management Service [ref to draft-ietf-sip-certs], to which it publishes the public version of its own self-signed certificate and from which it fetches on need the public certificates of other endpoints.
2) TLS-PSK managed e.g. by MIKEY-TICKET based Key Management and Key Management Service [RFC6043].
NOTE: 3GPP has specified usage of the MIKEY-TICKET based Key Management and Key Management Service authentication mechanism for the IP Multimedia Subsystem (IMS).
When an MSRP endpoint generates an SDP offer for MSRPS it MUST, in addition to the SDP attributes associated with the TLS authentication mechanisms described in RFC 4975, it MUST include any information elements associated with the other authentication mechanisms that it supports.
Unless the MSRP endpoints are able to use name based authentication, and they support a common authentication mechanism, they MUST use that mechanism. If the MSRP endpoints do not support such common authentication mechanism, they MUST try fingerprint based authentication, which will succeed if there are no Middleboxes present.
If that also fails, the MSRP endpoints MUST either:
1) Consider the TLS authentication as failed, in accordance with RFC 4975; or
2) If the SIP signalling between the MSRP endpoints is protected through e.g. SIPS, use fingerprint based authentication without requiring peer-to-peer SDP integrity, and thus trust the network endpoints in the signaling path for SDP integrity.
NOTE: As defined in RFC 4975, if TLS authentication fails, the user need to be able to decide whether to try to anyway establish an MSRP connection.

7. IANA Considerations

7.1. IANA Registration of the SDP a=msrp-cema attribute

This section registers a new SDP attribute, a=msrp-cema. The required information for this registration, as specified in RFC 4566, is:

8. Acknowledgements

Thanks to Ben Campbell, Remi Denis-Courmont, Nancy Greene, Hadriel Kaplan, Adam Roach, Robert Sparks, Salvatore Loreto, Shida Schubert, Ted Hardie, Richard L Barnes, Inaki Baz Castillo, Saul Ibarra Corretge and Adrian Georgescu for their guidance and input in order to produce this document.

9. Change Log

[RFC EDITOR NOTE: Please remove this section when publishing]
Changes from draft-ietf-simple-msrp-sessmatch-12

*Extension name changed to Connection Establishment for Media Anchoring (CEMA).

*Middlebox defintion added.

*ALG terminology replaced with Middlebox.

*SDP attribute name changed to a=msrp-cema.

*Applicability Statement section expanded.

*Re-structuring of MSRP Answerer section.

*Changes based on comments from Saúl Ibarra Corretgé (1406111).

Changes from draft-ietf-simple-msrp-sessmatch-11

*Modification of the sessmatch mechanism.

*- Extension name changed to Alternative Connection Establishment (ACE)

*- Session matching procedure no longer updated.

*- SDP c/m-line used for MSRP TCP connection.

*- sessmatch option-tag removed.

*- a=msrp-ace attribute defined.

*- Support of RFC 6135 mandatory.

Changes from draft-ietf-simple-msrp-sessmatch-10

*Sessmatch option-tag added, based on WG discussions and concensus.

Changes from draft-ietf-simple-msrp-sessmatch-08

*OPEN ISSUE regarding the need for a sessmatch option-tag removed.

Changes from draft-ietf-simple-msrp-sessmatch-07

*Sessmatch defined as an MSRP extension, rather than MSRP update

*Additional security considerations text added

10. References

10.1. Normative References

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
[RFC3261]	Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.
[RFC4566]	Handley, M., Jacobson, V. and C. Perkins, "SDP: Session Description Protocol", RFC 4566, July 2006.
[RFC4975]	Campbell, B., Mahy, R. and C. Jennings, "The Message Session Relay Protocol (MSRP)", RFC 4975, September 2007.
[RFC4976]	Jennings, C., Mahy, R. and A.B. Roach, "Relay Extensions for the Message Sessions Relay Protocol (MSRP)", RFC 4976, September 2007.
[RFC6135]	Holmberg, C. and S. Blau, "An Alternative Connection Model for the Message Session Relay Protocol (MSRP)", RFC 6135, February 2011.

10.2. Informative References

[RFC4916]	Elwell, J., "Connected Identity in the Session Initiation Protocol (SIP)", RFC 4916, June 2007.
[RFC6043]	Mattsson, J. and T. Tian, "MIKEY-TICKET: Ticket-Based Modes of Key Distribution in Multimedia Internet KEYing (MIKEY)", RFC 6043, March 2011.
[3GPP. 23.228]	3GPP, "IP Multimedia Subsystem (IMS); Stage 2", 3GPP TS 23.228 10.6.0, September 2011.

Authors' Addresses

Christer Holmberg Holmberg Ericsson Hirsalantie 11 Jorvas, 02420
Finland EMail: christer.holmberg@ericsson.com

Staffan Blau Blau Ericsson Stockholm, 12637 Sweden EMail:
staffan.blau@ericsson.com