Abstract

This document defines an extension, sessmatch, for the Message Session Relay Protocol (MSRP) session matching procedure of MSRP entities. The extension extends the applicability of MSRP communication to network scenarios where Application Layer Gateway (ALG) functions modify the Session Description Protocol (SDP) MSRP address information.

Status of this Memo

This Internet-Draft is submitted to IETF 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 June 12, 2011.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of

the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.

Table of Contents

1. Introduction .................................................. 3
2. Conventions .................................................... 4
3. Applicability statement ........................................ 4
4. Sessmatch mechanism ............................................ 4
   4.1. General ...................................................... 4
   4.2. Session matching ........................................... 4
5. Security Considerations .......................................... 5
   5.1. MSRP URI as shared secret .................................. 5
   5.2. Uniqueness of the session-id ............................... 6
   5.3. Man in the middle .......................................... 6
   5.4. TLS .......................................................... 6
6. IANA Considerations .............................................. 7
7. Acknowledgements ................................................ 7
8. Change Log ....................................................... 7
9. References ........................................................ 7
   9.1. Normative References ....................................... 7
   9.2. Informative References .................................... 7
Authors’ Addresses ............................................... 8
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 SIP Application Layer Gateways (ALGs), which anchor and controls 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 Interconnect Border Control Function (IBCF) [3GPP.23.228] defined by the 3rd Generation Partnership Project (3GPP), which 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], does not work when an MSRP entities communicate with such ALGs, unless the ALGs implement MSRP Back-To-Back User Agent (B2BUA) functionality. The reason is that entities use the MSRP URI comparison [RFC4975] procedure in order to match an MSRP message to an MSRP session. That requires consistency between the address information in the MSRP messages and the address information carried in the SDP a=path attribute. The matching will fail if ALGs modify the address information of the SDP a=path attribute, but do not implement MSRP B2BUA functionality and perform the corresponding modification in the associated MSRP messages. However, few ALGs implement MSRP B2BUA functionality, due to complexity and poor scalability.

This specification defines an MSRP extension, sessmatch, that allows MSRP entities to communicate with ALGs that do not implement MSRP B2BUA functionality. MSRP entities that support the sessmatch use a different mechanism for matching an MSRP message with an MSRP session, called session matching. Instead of using the MSRP URI comparison procedure defined in RFC 4975, only the MSRP session-id part is used for the session matching by entities that support the sessmatch extension.

In case TLS with name based authentication is used, ALGs need to implement MSRP B2BUA functionality also when communicating with MSRP entities that support the sessmatch extension, in order to prevent the MSRP communication from failing due to a certificate mismatch.

The sessmatch extension is backward compatible. In the absence of ALGs, MSRP entities that do not implement the sessmatch extension can interoperate with entities that do implement it. The reason is that the matching of an MSRP message to an ongoing session will not fail. MSRP entities that do not implement the sessmatch extension, and
communicate with ALGs that do not implement MSRP B2BUA functionality, can normally not establish MSRP sessions, since the session matching will fail in case the address information of the SDP a=path attribute has been modified by the ALGs.

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 endpoint use a self-signed TLS certificate and sends a certificate fingerprint in SDP (fingerprint based TLS authentication).

2. An endpoint use 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).

3. Applicability statement

This document defines an MSRP extension, sessmatch. Support of the extension is optional. MSRP entities can implement the extension in order to allow MSRP communication in networks where ALGs that might modify the address information of the SDP a=path attribute, but do not implement MSRP B2BUA functionality, are present.

4. Sessmatch mechanism

4.1. General

This section defines how an MSRP entity that supports the sessmatch extension performs session matching, i.e. matches an incoming MSRP message to an MSRP session.

4.2. Session matching

The difference between the session matching mechanism in RFC 4975, and the one defined in this specification for the sessmatch
extension, is that while the mechanism in RFC 4975 uses the MSRP URI comparison rules for session matching, the sessmatch extension only uses the session-id part of the MSRP URI.

When an MSRP entity that receives the first MSRP request for an MSRP session, the To-Path header field of the request should contain a URI with a session-id part that was provided in the SDP associated with the MSRP session. The entity that accepted the connection looks up the session-id part of the MSRP URI in the received requests, in order to determine which session it matches. The session-id part is compared as case sensitive. If a match exists, the entity MUST assume that the host that formed the connection is the host to which this URI was given. If no match exists, the entity MUST reject the request with a 481 response. The entity MUST also check to make sure the session is not already in use on another connection. If the session is already in use, it MUST reject the request with a 506 response.

NOTE: As the sessmatch extension, in a peer to peer session, is backward compatible with the RFC 4975 mechanism, the SIMPLE WG did not see a need to define a SIP option-tag associated with the sessmatch extension. In case the session path contains an intermediary that modifies the SDP MSRP routing information, MSRP session establishments that contain RFC 4975 entities will fail. However, that is the case even without the sessmatch extension. Also, an intermediary will normally make a decision whether to insert itself in the session path when it receives the SDP offer. However, it will not be aware about whether the MSRP endpoint acting as SDP answerer supports the sessmatch extension until it receives the SDP answer.

5. Security Considerations

5.1. MSRP URI as shared secret

An MSRP entity that does not support the sessmatch extension uses the complete MSRP URI (scheme, authority, transport, session-id) as a shared secret in order to determine that an incoming transport connection originates from the intended peer device. The shared secret needs to be hard to guess, but in reality only the session-id part with its minimum 80 bit of randomness is hard to guess. Using only the MSRP URI session-id part as shared secret is therefore roughly as good as using the complete URI.
5.2. Uniqueness of the session-id

The value of the MSRP URI session-id part only needs to be unique within the scope of the MSRP entity that created it, so in order to make the session-id unique there is no need to scope its namespace by the MSRP URI authority part.

5.3. Man in the middle

A man-in-the-middle (MiTM) that wants to insert itself in the MSRP communication path, in order to modify unprotected MSRP messages, needs to implement MSRP B2BUA functionality. If the MiTM communicates with MSRP entities that support the sessmatch extension, it does not need to modify the To-Path and From-Path header fields in the MSRP messages, which is the case if it communicates with an MSRP entity that do not support the extension. In both cases, however, the MiTM needs to terminate the TCP/TLS connection used for the MSRP communication.

The sessmatch extension makes it easier for a MiTM to monitor and record unprotected MSRP communication, as it allows the MiTM to anchor the MSRP communication even if it does not implement MSRP B2BUA functionality.

The sessmatch extension does not make it easier for a MiTM to insert itself in the SIP/SDP signaling path, neither does it make it easier for a MiTM to forward MSRP messages towards malicious MSRP entities (as it does not require the MiTM to anchor the MSRP communication).

5.4. TLS

This specification does not in any way modify TLS security procedures as such. The sessmatch extension allows the usage of ALGs that do not implement MSRP B2BUA functionality in MSRP communications, unless TLS with name based authentication is used, and unless MSRP relays are used. In such cases ALGs need to implement MSRP B2BUA functionality, to prevent the MSRP communication from failing. That applies to MSRP in general, and is not specific to the extension defined in this specification.

In case TLS with fingerprint based authentication is used, the sessmatch extension allows usage of ALGs that modify the address information of the SDP a=path attribute, but no not implement MSRP B2BUA functionality, to communicate with MSRP entities. In order to use fingerprint authentication, the SDP that carries the fingerprint information needs to be integrity protected. In case an ALG needs to be able to modify SDP information, however, it will not be possible to provide full end-to-end SDP integrity protection of the SDP.

Holmberg & Blau Expires June 12, 2011 [Page 6]
Integrity protection can still be provided between MSRP entities and ALGs, however.

6. IANA Considerations

None.

7. Acknowledgements

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

8. Change Log

[RFC EDITOR NOTE: Please remove this section when publishing]

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

9. References

9.1. Normative References


9.2. Informative References

June 2002.

[3GPP.23.228]
3GPP, "IP Multimedia Subsystem (IMS); Stage 2", 3GPP
TS 23.228 10.2.0, September 2010.

Authors’ Addresses

Christer Holmberg
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

Email: christer.holmberg@ericsson.com

Staffan Blau
Ericsson AB
P.O Box 407
Sweden

Email: staffan.blau@ericsson.com