Opaque MSRP Path Uri
draft-macdonald-simple-msrp-opaque-path-01

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), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on September 10, 2009.

Copyright Notice

Copyright (c) 2009 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.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow
Abstract

The Message Session Relay Protocol (MSRP) does not allow privacy and topology hiding, such that MSRP users can hide the IP Address of their systems. This limitation is due to the fact that MSRP Path headers contain physical IP addresses. This document describes a mechanism which adds a level of indirection to allow privacy and topology hiding, to prevent remote parties and a man-in-the-middle from learning the IP Address and port information of the MSRP client. It also defines the option tag msrp-opaque, to indicate such support.

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 [RFC2119].
Table of Contents

1. Applicability ................................................. 4
2. Introduction ............................................... 4
3. Overview of Operations ................................. 5
4. MSRP Opaque URI ........................................... 6
   4.1. Opaque URI Format .................................... 6
   4.2. Generating an Opaque Uri ............................. 6
   4.3. MSRP URI Parameter .................................. 6
5. SIP Option Tag ............................................... 6
6. Backwards Compatibility with RFC 4975 and 4976 ..... 7
7. Example Scenario ........................................... 7
8. Security Considerations ............................... 9
9. Normative References ................................. 10
Author’s Address ........................................... 10
1. Applicability

This technique may be used in any MSRP deployment where all MSRP endpoints support the [I-D.ietf-simple-msrp-acm] extension when routing to/from on an MSRP URI. Not all MSRP endpoints must support this opaque extension; they only need to support draft-ACM. This document only describes an SDP based mechanism for binding a physical address to an opaque MSRP URI that limits possible topologies. [RFC4976] MSRP relays will not be able to route from opaque MSRP URI’s.

2. Introduction

A frequent requirement of network architectures is to hide the systems of the core network from external user agents. It is also often desirable to hide the IP address of a user agent from other user agents in the network. This is usually accomplished using a SIP B2BUA or other relay element. MSRP does not allow an efficient approach to this problem because the payload of the protocol contains physical IP addresses, and thus the B2BUA needs to modify MSRP messages in order to hide topology information.

Furthermore, users of MSRP or their system administrators may not wish to provide remote MSRP agents the IP Address and port of their local MSRP host machines, for security or anonymity reasons. Revealing such might expose the host machines to external attacks, even through NATs/Firewalls. One means of providing user anonymity is by using a TURN server; however in practice there are few TURN servers available, and other relay agents such as SBC’s may already be in the path. The opaque MSRP URI concept defined in this draft is usable with a TURN server, SBC, or MSRP B2BUA. It is not usable with MSRP Relays unless their functionality is extended.

This specification defines an opaque MSRP URI, that does not contain a routable IP address. The opaque URI is a mapping to a physical address that is exchanged outside the MSRP protocol. This allows topology hiding without re-writing any MSRP messages between the MSRP User Agents.

The opaque URI is a pointer to an externally conveyed routable URI. This document describes a mechanism to convey the routable URI in the SDP offer/answer exchange used to initiate the MSRP session, based on the changes in draft-ACM. The opaque URI is used in the MSRP message headers, while the transport addressing conveyed in SDP is used for the transport layer connections.

The basic concept is that instead of indicating the MSRP transport
connection information in the MSRP "path" SDP attribute, and using such in the to-path/from-path MSRP headers, a pseudo-random string is used instead: the MSRP opaque URI. An MSRP client inserts a pseudo-random MSRP opaque URI value in the SDP MSRP path attribute, and uses this value in MSRP messages for its path headers. Actual transport connection information is instead conveyed in the standard SDP connection and media lines, per draft-ACM.

3. Overview of Operations

An MSRP User Agent following this document's mechanism will generate a SIP INVITE for an MSRP-based media session by populating the SDP connection line and media line with transport addressing information, as is done for COMEDIA and draft-ACM, along with an MSRP opaque URI for the SDP MSRP path attribute. It will also insert the new 'msrp-opaque' option tag into a SIP Require header field.

The SIP UAS receiving the INVITE request will see the MSRP URI is an opaque type, due to a new 'opaque' URI parameter defined later in this document. It will then respond with an SDP answer also indicating an MSRP opaque URI, with its actual transport address information in the SDP connection and media lines.

Per [RFC4975], the UAC will initiate the TCP connection to the UAS, however per draft-ACM the TCP connection would use the SDP connection and media lines for addressing info instead of the MSRP URI directly.

The MSRP messages generated by the UAC and UAS MUST continue to use the MSRP path attribute opaque URI for the to/from-path MSRP headers. Since the URI is not directly dereferenceable for transport addressing, each UA maintains an internal binding of MSRP opaque-URI to connection transport information.

If the TCP connection for MSRP were to go directly from the UAC to the UAS, then clearly one could simply learn the UA addressing on the wire, or by looking at SDP information, and anonymity would not be achieved. It is expected that in typical deployment the media transport information is obfuscated through some other means, such as SBC’s or ALG’s performing media relay functions, but that is beyond the scope of this document: the goal of this document is to provide anonymity for MSRP, not SIP nor SDP.

The approach defined in this document does not fit with the MSRP Relay model of RFC 4976, where an MSRP client can use a special intermediary called an "MSRP Relay". Instead, this mechanism works with MSRP Application Servers, acting as full MSRP Back-to-Back User Agents, or with typical SIP intermediate types of devices, such as
SBCs and ALGs. One of the goals of this specification is to be able to make MSRP work across such intermediaries.

[Note: the MSRP opaque URI model *could* be made to work with MSRP Relays, if the Relays were to know about such URIs in advance - it is TBD whether it is worth specifying how that could/should work]

4. MSRP Opaque URI

4.1. Opaque URI Format

The opaque URI is an MSRP URI that has a domain name in the .invalid TLD, and an ‘opaque’ URI parameter as defined later. A globally unique identifier is generated and encoded as a URI in the .invalid TLD. For example:
path:msrp://f7jey483rydfhkyerky3.invalid:7394/2s93u93udj;tcp;opaque. The opaque URI pointer is the first portion of the URI before .invalid: f7jey483rydfhkyerky3. The port is arbitrary. [Note: Should there be a fixed value for the port?]

4.2. Generating an Opaque Uri

The identifying portion of the opaque uri is the portion up to .invalid. This portion should be cryptographically unique and MUST be encoded so it obeys rfc3986. Opaque URIs do not modify the grammar of rfc4975.

TODO: determine generation scheme and encoding

4.3. MSRP URI Parameter

This document defines a new MSRP URI parameter: "opaque". The opaque URI parameter indicates that this URI follows this specification, and MUST appear to identify an opaque URI whenever one is used. The ABNF for this parameter, following RFC4975 [RFC4975], is as follows:

\[
\begin{align*}
\text{URI-parameter} & = \text{opaque-param} / (\text{token} \ ["=\" \ \text{token}]) \\
\text{opaque-param} & = \text{"opaque"}
\end{align*}
\]

5. SIP Option Tag

This specification registers a new SIP option tag, as per the guidelines in Section 27.1 of [RFC3261].

Name: msrp-opaque
Description: This option-tag is used to identify UAs that support the mechanism defined in this document.

SIP User Agents MUST include a Requires header field with the "msrp-opaque" option-tag when using an opaque URI in an SDP offer or answer in a SIP message.

SIP User Agents SHOULD include a Supported header field with the "msrp-opaque" option-tag if they support this specification but still wish to generate a non-opaque URI in the SDP. This allows the UAS to reject the request with a Require header field containing "msrp-opaque" to indicate the UAS requires the UAC to use an opaque URI; and this allows for backwards compatibility as described in the next section.

6. Backwards Compatibility with RFC 4975 and 4976

When a UAC initiates an MSRP session, it may need to interoperate with legacy devices based on RFC 4975 and 4976. This can be accomplished with the opaque URI mechanism in the following way, as long as the UAC does not itself require anonymization of its URI: the UAC generates a legacy RFC 4975 MSRP URI, but adds the 'opaque' parameter to the end of it, and sets the SDP connection and media lines to be the real transport addresses as well, and adds a Supported option tag of "msrp-opaque".

If the answering UAS only supports RFC 4975 and/or 4976, it will ignore the opaque parameter and Supported option tag, and respond and act as per RFC 4975. If the UAS supports the opaque mechanism, and wishes to anonymize its MSRP URI, it responds with a real MSRP opaque URI, and a SIP Require header field with the "msrp-opaque" option tag.

7. Example Scenario

In the following example, Alice invites Bob to an MSRP session. Alice does not wish her IP address to be known, as it conveys information about her location and might make her system vulnerable to attacks. Similarly, the Atlanta network has a policy of not exposing such details about their network or their users. In this case Alice and Bob are both at atlanta.example.com.
Message 1 is an INVITE where msrp-opaque is required and an opaque MSRP URI is used in the SDP.

```
INVITE sip:bob@atlanta.example.com SIP/2.0
To: <sip:bob@atlanta.example.com>
From: <sip:alice@atlanta.example.com>;tag=786
Call-ID: 3413an89KU
Requires: msrp-opaque
Content-Type: application/sdp
-
c=IN IP4 192.168.0.100
m=message 12454 TCP/MSRP *
a=path:msrp://f7jey483rydfhkyerky3.invalid.com:7394/jshA7weztas;tcp;opaque
```

The connection c-line of the SDP identifies Alice’s actual transport address for the MSRP connection, and the media m-line port portion identifies the TCP port; as opposed to the msrp path attribute as defined in [RFC4975]. They may be changed by intermediate nodes to point to an address:port on a TCP relay service in the Atlanta network.

```
c=IN IP4 border.altanta.example.com
m=message 22454 TCP/MSRP *
a=path:msrp://f7jey483rydfhkyerky3.invalid.com:7394/jshA7weztas;tcp;opaque
```

The relevant portion on the SDP from Message 3. For simplicity, Bob’s UA has been given a publicly reachable IP address.

```
c=IN IP4 bob.altanta.example.com
m=message 34313 TCP/MSRP *
a=path:msrp://a6ghr7yv6egw33r.invalid.com:7394/kjhd37s2s20w2a;tcp;opaque
```

Which is re-written to point to the border element.

```
c=IN IP4 border.altanta.example.com
m=message 27784 TCP/MSRP *
a=path:msrp://a6ghr7yv6egw33r.invalid.com:7394/kjhd37s2s20w2a;tcp;opaque
```
After this exchange is complete Alice will form a connection to the border.atlanta.example.com which will in turn connect to Bob’s UA. border.atlanta.example.com acts as a simple TCP relay between Bob and Alice until the TCP connection is torn down by either party.

While some of this functionality can be achieved with the MSRP relay specification, or by using TURN-TCP, this approach has its own advantages and disadvantages.

Advantages:
The opaque-uri provides topology hiding. This can also be provided by TURN-TCP, but will end up w/ two TURN allocations being used.
At the media level, the opaque-uri approach only requires a TCP relay that has no knowledge of MSRP.
It is a small change for endpoints that already support MSRP.

Disadvantages:
Until the TCP relay has connected to the second peer(Bob), any MSRP requests from Alice must be rate-limited or cached. In practice, rate limiting seems to work well; if the connection to Bob fails, the connection to Alice would be torn down. This does not provide the same level of error reporting as MSRP-Relay.
Mapping rules must be conveyed from the signal-plane(SIP/SDP) to the Media Plane(TCP relay)

8. Security Considerations

Hiding host system IP Address and port information may be considered by some to be a form of anonymity or obfuscation for malevolent purposes, but it actually represents a simple form of host protection. SIP and MSRP User Agents are not just clients - they are servers as well, from both a protocol and use-case perspective. SIP in particular typically uses a UDP socket, and even when using TCP, agents frequently run a listen server socket in order to receive inbound requests. If the connection information of SIP or MSRP applications running on a host are revealed, the local user of the system and/or its administrators have no simple means by which to prevent any device on the Internet from attempting to send messages to the host for malicious purposes. For example, the NAT will have opened a port and created a binding for the SIP UDP port, and some NATs are fully conical and will allow any remote device to send packets in through their open bindings.
9. Normative References


Author’s Address

Derek C. MacDonald
CounterPath Solutions, Inc.
Suite 300, One Bentall Centre, 505 Burrard St
Vancouver, BC  V7X1M3
Canada

Phone: +1-604-320-3344
Email: derek@counterpath.com