Network Working Group
Request for Comments: 4570
Category: Standards Track

B. Quinn
BoxnArrow.com
R. Finlayson
Live Networks, Inc.

July 2006

Session Description Protocol (SDP) Source Filters

Status of This Memo

Copyright Notice

Abstract

This document describes how to adapt the Session Description Protocol (SDP) to express one or more source addresses as a source filter for one or more destination "connection" addresses. It defines the syntax and semantics for an SDP "source-filter" attribute that may reference either IPv4 or IPv6 address(es) as either an inclusive or exclusive source list for either multicast or unicast destinations. In particular, an inclusive source-filter can be used to specify a Source-Specific Multicast (SSM) session.

1. Introduction

The Session Description Protocol [SDP] provides a general purpose format for describing multimedia sessions in announcements or invitations. SDP uses an entirely textual data format (the US-ASCII subset of [UTF-8]) to maximize portability among transports. SDP does not define a protocol, but only the syntax to describe a multimedia session with sufficient information to discover and participate in that session. Session descriptions may be sent using any number of existing application protocols for transport (e.g., Session Announcement Protocol (SAP), SIP, Real Time Streaming Protocol (RTSP), email, and HTTP).

Typically, session descriptions reference an IP multicast address for the "connection-address" (destination), though unicast addresses or fully qualified domain names (FQDNs) MAY also be used. The "source-

filter" attribute defined in this document qualifies the session traffic by identifying the address (or FQDN) of legitimate sources (senders). The intent is for receivers to use the source and destination address pair(s) to filter traffic, so that applications receive only legitimate session traffic.

Receiver applications are expected to use the SDP source-filter information to identify traffic from legitimate senders, and discard traffic from illegitimate senders. Applications and hosts may also share the source-filter information with network elements (e.g., with routers using [IGMPv3]) so they can potentially perform the traffic filtering operation further "upstream," closer to the source(s).

The "source-filter" attribute can appear at the session level and/or the media level.

1.1. Motivation

The purpose of a source-filter is to help protect receivers from traffic sent from illegitimate source addresses. Filtering traffic can help to preserve content integrity and protect against Denial of Service (DoS) attacks.

For multicast destination addresses, receiver applications MAY apply source-filters using the Multicast Source Filter APIs [MSF-API]. Hosts are likely to implement these APIs using protocol mechanisms to convey the source filters to local multicast routers. Other "upstream" multicast routers MAY apply the filters and thereby provide more explicit multicast group management and efficient utilization of network resources. The protocol mechanisms to enable these operations are beyond the scope of this document, but their potential provided motivation for SDP source-filters.

2. Terminology

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 [REQMNT].

3. The "source-filter" Attribute

The SDP source-filter attribute does not change any existing SDP syntax or semantics, but defines a format for additional session description information. Specifically, source-filter syntax can prescribe one or more unicast addresses as either legitimate or illegitimate sources for any (or all) SDP session description "connection-address" field values.

Note that the unicast source addresses specified by this attribute are those that are seen by a receiver. Therefore, if source addresses undergo translation en route from the original sender to the receiver - e.g., due to Network Address Translation (NAT) or some tunneling mechanism - then the SDP "source-filter" attribute, as presented to the receiver, will not be accurate unless the source addresses therein are also translated accordingly.

The source-filter attribute has the following syntax:

```
a=source-filter: <filter-mode> <filter-spec>
```

The <filter-mode> is either "incl" or "excl" (for inclusion or exclusion, respectively). The <filter-spec> has four sub-components:

```
<nettype> <address-types> <dest-address> <src-list>
```

A <filter-mode> of "incl" means that an incoming packet is accepted only if its source address is in the set specified by <src-list>. A <filter-mode> of "excl" means that an incoming packet is rejected if its source address is in the set specified by <src-list>.

The first sub-field, <nettype>, indicates the network type, since SDP is protocol independent. This document is most relevant to the value "IN", which designates the Internet Protocol.

The second sub-field, <address-types>, identifies the address family, and for the purpose of this document may be either <addrtype> value "IP4" or "IP6". Alternately, when <dest-address> is an FQDN, the value MAY be "*" to apply to both address types, since either address type can be returned from a DNS lookup.

The third sub-field, <dest-address>, is the destination address, which MUST correspond to one or more of the session's "connection-address" field values. It may be either a unicast or multicast address, an FQDN, or the "*" wildcard to match any/all of the session's "connection-address" values.

The fourth sub-field, <src-list>, is the list of source hosts/interfaces in the source-filter, and consists of one or more unicast addresses or FQDNs, separated by space characters.

The format and content of these semantic elements are derived from and compatible with those defined in [SDP]. For more detail, see Appendix A of this document.

3.1. Processing Rules

There are a number of details to consider when parsing the SDP source-filter syntax.

The <dest-address> value in a "source-filter" attribute MUST correspond to an existing <connection-field> value in the session description. The only exception to this is when a "*" wildcard is used to indicate that the source-filter applies to all <connection-field> values.

When the <dest-address> value is a multicast address, the field value MUST NOT include the sub-fields <ttl> and <number of addresses> from the <connection-address> value. If the <connection-address> specifies more than one multicast address (in the <number of addresses> field), then a source filter, if any, for each such address must be stated explicitly, using a separate "a=source-filter" line for each address (unless a "*" wildcard is used for <dest-address>). See section 3.2.4 for an example.

When the <addrtype> value is the "*" wildcard, the <dest-address> MUST be either an FQDN or "*" (i.e., it MUST NOT be an IPv4 or IPv6 address). See section 3.2.6 for an example.

As has always been the case, the default behavior when a source-filter attribute is not provided in a session description is that all traffic sent to the specified <connection-address> value should be accepted (i.e., from any source address). The source-filter grammar does not include syntax to express either "exclude none" or "include all."

Like the standard <connection-field> described in [SDP], the location of the "source-filter" attribute determines whether it applies to the entire session or only to a specific medium (i.e., "session-level" or "media-level"). A media-level source-filter will always completely override a session-level source-filter.

A "source-filter" need not be located at the same hierarchy level as its corresponding <connection-field>. So, a media-level <source-filter> can reference a session-level <connection-field> value, and a session-level "source-filter" can be applied to all matching media-level <connection-field> values. See section 3.2.3 for an example.

An SDP description MUST NOT contain more than one session-level "source-filter" attribute that covers the same destination address, or more than one media-level "source-filter" attribute that covers the same destination address.

There is no specified limit to the number of entries allowed in the <src-list>; however, there are practical limits that should be considered. For example, depending on the transport to be used for the session description, there may be a limit to the total size of the session description (e.g., as determined by the maximum payload in a single datagram). Also, when the source-filter is applied to control protocols, there may be a limit to the number of source addresses that can be sent. These limits are outside the scope of this document, but should be considered when defining source-filter values for SDP.

3.2. Examples

Here are a number of examples that illustrate how to use the source-filter attribute in some common scenarios. We use the following session description components as the starting point for the examples to follow. For each example, we show the source filter with additional relevant information and provide a brief explanation.

```
<session-description> =
     v=0
     o=The King <Elvis@example.com>
     s=Elvis Impersonation
     i=All Elvis, all the time
     u=http://www.example.com/ElvisLive/
     t=0 0
     a=recvonly

<media-description 1> =
     m=audio 54320 RTP/AVP 0

<media-description 2> =
     m=video 54322 RTP/AVP 34
```

3.2.1. Source-Specific Multicast Example

Multicast addresses in the Source-Specific Multicast [SSM] range require a single unicast sender address for each multicast destination, so the source-filter specification provides a natural fit. In this example, a session member should receive only traffic sent from 192.0.2.10 to the multicast session address 232.3.4.5.

```
<session-description>

c=IN IP4 232.3.4.5/127
a=source-filter: incl IN IP4 232.3.4.5 192.0.2.10

<media-description 1>
```

This source-filter example uses an inclusion list with a single multicast "connection-address" as the destination and single unicast address as the source. Note that the value of the connection-address matches the value specified in the connection-field.

Also note that since the connection-field is located in the session-description section, the source-filter applies to all media.

Furthermore, if the SDP description specifies an RTP session (e.g., its "m=" line(s) specify "RTP/AVP" as the transport protocol), then the "incl" specification will apply not only to RTP packets, but also to any RTCP packets that are sent to the specified multicast address. This means that, as a side effect of the "incl" specification, the only possible multicast RTCP packets will be "Sender Report" (SR) packets sent from the specified source address.

Because of this, an SDP description for a Source-Specific Multicast (SSM) RTP session SHOULD also include an

```
a=rtcp-unicast ...
```

attribute, as described in [RTCP-SSM] (section 10.1). This specifies that RTCP "Reception Report" (RR) packets are to be sent back via unicast.

3.2.2. Unicast Exclusion Example

Typically, an SDP session <connection-address> value is a multicast address, although it is also possible to use either a unicast address or FQDN. This example illustrates a scenario whereby a session description indicates the unicast source address 192.0.2.10 in an exclusion filter. In effect, this sample source-filter says, "destination 192.0.2.11 should accept traffic from any sender *except* 192.0.2.10."

```
<session-description>

c=IN IP4 192.0.2.11
a=source-filter: excl IN IP4 192.0.2.11 192.0.2.10

<media-description 1>
```

3.2.3. Multiple Session Address Example

This source-filter example uses the wildcard "*" value for <dest-addr> to correspond to any/all <connection-address> values. Hence, the only legitimate source for traffic sent to either

232.2.2.2 or 232.4.4.4 multicast addresses is 192.0.2.10. Traffic sent from any other unicast source address should be discarded by the receiver.

```
<session-description>

a=source-filter: incl IN IP4 * 192.0.2.10

<media-description 1>

c=IN IP4 232.2.2.2/127

<media-description 2>

c=IN IP4 232.4.4.4/63
```

3.2.4. Multiple Multicast Address Example

In this example, the <connection-address> specifies three multicast addresses: 224.2.1.1, 224.2.1.2, and 224.2.1.3. The first and third of these addresses are given source filters. However, in this example the second address - 224.2.1.2 - is *not* given a source filter.

```
<session-description>

c=IN IP4 224.2.1.1/127/3
a=source-filter: incl IN IP4 224.2.1.1 192.0.2.10
a=source-filter: incl IN IP4 224.2.1.3 192.0.2.42

<media-description 1>
```

3.2.5. IPv6 Multicast Source-Filter Example

This simple example defines a single session-level source-filter that references a single IPv6 multicast destination and source pair. The IP multicast traffic sent to FF0E::11A is valid only from the unicast source address 2001:DB8:1:2:240:96FF:FE25:8EC9.

```
<session-description>

c=IN IP6 FF0E::11A/127
a=source-filter incl IN IP6 FF0E::11A 2001:DB8:1:2:240:96FF:FE25:8EC9

<media-description 1>
```

3.2.6. IPv4 and IPv6 FQDN Example

This example illustrates use of the <addrtype> "*" wildcard, along with multicast and source FQDNs that may resolve to either an IPv6 or IPv4 address, or both. Although typically both the multicast and source addresses will be the same (either both IPv4 or both IPv6), using the wildcard for addrtype in the source filter allows asymmetry between the two addresses (so an IPv4 source address may be used with an IPv6 multicast address).

```
<session-description>

c=IN IP4 channel-1.example.com/127
c=IN IP6 channel-1.example.com/127
a=source-filter: incl IN * channel-1.example.com src-1.example.com

<media-description 1>
```

3.3. Offer-Answer Model Considerations

The "source-filter" attribute is not intended to be used as an 'offer' in an SDP offer-answer exchange [OFFER], because sets of source addresses do not represent 'capabilities' or 'limitations' of the offerer, and because the offerer does not, in general, have a priori knowledge of which IP source address(es) will be included in an answer. While an answerer may include the "source-filter" attribute in his/her answer (e.g., to designate a SSM session), the answerer SHOULD ignore any "source-filter" attribute that was present in the original offer.

4. Interoperability Issues

Defining a list of legitimate sources for a multicast destination address represents a departure from the Any-Source Multicast (ASM) model, as originally described in [IGMPv1]. The ASM model supports anonymous senders and all types of multicast applications (e.g., many-to-many). Use of a source-filter excludes some (unknown or undesirable) senders, which lends itself more to one-to-many or few-to-few type multicast applications.

Although these two models have contrasting operational characteristics and requirements, they can coexist on the same network using the same protocols. Use of source-filters do not corrupt the ASM semantics but provide more control for receivers, at their discretion.

5. Security Considerations

See [SDP] for security considerations specific to the Session Description Protocol in general. The central issue relevant to using source address filters is the question of address authenticity.

Using the source IP address for authentication is weak, since addresses are often dynamically assigned and it is possible for a sender to "spoof" its source address (i.e., use one other than its own) in datagrams that it sends. Proper router configuration, however, can reduce the likelihood of "spoofed" source addresses being sent to or from a network. Specifically, border routers are encouraged to filter traffic so that datagrams with invalid source addresses are not forwarded (e.g., routers drop datagrams if the source address is non-local) [FILTERING]. This, however, does not prevent IP source addresses from being spoofed on a Local Area Network (LAN).

Also, as noted in section 3 above, tunneling or NAT mechanisms may require corresponding translation of the addresses specified in the SDP "source-filter" attribute, and furthermore, may cause a set of original source addresses to be translated to a smaller set of source addresses as seen by the receiver.

Use of FQDNs for either <dest-address> or <src-list> values provides a layer of indirection that provides great flexibility. However, it also exposes the source-filter to any security inadequacies that the DNS system may have. If unsecured, it is conceivable that the DNS server could return illegitimate addresses.

In addition, if source-filtering is implemented by sharing the source-filter information with network elements, then the security of the protocol(s) that are used for this (e.g., [IGMPv3]) becomes important, to ensure that legitimate traffic (and only legitimate traffic) is received.

For these reasons, receivers SHOULD NOT treat the SDP "source-filter" attribute as being its sole mechanism for protecting the integrity of received content.

6. IANA Considerations

As recommended by [SDP] (Appendix B), the new attribute name "source-filter" has been registered with IANA, as follows:

The following contact information shall be used for all registrations included here:

```
     Contact:      Ross Finlayson
                   email: finlayson (at) live555.com
                   phone: +1-650-254-1184

   SDP Attribute ("att-field"):
     Attribute name:     source-filter
     Long form:          Source Filter
     Type of name:       att-field
     Type of attribute:  Session level or media level
     Subject to charset: No
     Purpose:            See this document
     Reference:          This document
     Values:             See this document, and registrations below
```

7. Acknowledgements

The authors would like to thank Dave Thaler and Mark Handley, whose input provided much of the substance of this document. Magnus Westerlund also provided valuable feedback during editing.

8. Normative References

[ABNF] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 4234, October 2005.

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

[SDP] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol", RFC 4566, July 2006.

[UTF-8] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, November 2003.

9. Informative References

[FILTERING] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, May 2000.

[IGMPv1] Deering, S., "Host extensions for IP multicasting", STD 5, RFC 1112, August 1989.

[IGMPv3] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.

[MSF-API] Thaler, D., Fenner, B., and B. Quinn, "Socket Interface Extensions for Multicast Source Filters", RFC 3678, January 2004.

[OFFER] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)", RFC 3264, June 2002.

[RTCP-SSM] Chesterfield, J., E. Schooler, J. Ott, "RTCP Extensions for Single-Source Multicast Sessions with Unicast Feedback", Work in Progress, October 2004.

[SSM] Bhattacharyya, S., "An Overview of Source-Specific Multicast (SSM)", RFC 3569, July 2003.

Appendix A. Source-Filter Attribute Syntax

This appendix provides an Augmented BNF [ABNF] grammar for expressing an exclusion or inclusion list of one or more (IPv4 or IPv6) unicast source addresses. It is intended as an extension to the grammar for the Session Description Protocol, as defined in [SDP]. Specifically, it describes the syntax for the new "source-filter" attribute field, which MAY be either a session-level or media-level attribute.

The "dest-address" value in each source-filter field MUST match an existing connection-field value, unless the wildcard connection-address value "*" is specified.

```
source-filter =  "source-filter" ":" SP filter-mode SP filter-spec
                 ; SP is the ASCII 'space' character
                 ;  (0x20, defined in [ABNF]).

filter-mode =    "excl" / "incl"
                 ; either exclusion or inclusion mode.

filter-spec =    nettype SP address-types SP dest-address SP src-list
                 ; nettype is as defined in [SDP].

address-types =  "*" / addrtype
                 ; "*" for all address types (both IP4 and IP6),
                 ;  but only when <dest-address> and <src-list>
                 ;  reference FQDNs.
                 ; addrtype is as defined in [SDP].

dest-address =   "*" / basic-multicast-address / unicast-address
                 ; "*" applies to all connection-address values.
                 ; unicast-address is as defined in [SDP].

src-list =       *(unicast-address SP) unicast-address
                 ; one or more unicast source addresses (in
                 ;  standard IPv4 or IPv6 ASCII-notation form)
                 ;  or FQDNs.
                 ; unicast-address is as defined in [SDP].

basic-multicast-address =   basic-IP4-multicast / basic-IP6-multicast
                            / FQDN / extn-addr
                            ; i.e., the same as multicast-address
                            ;  defined in [SDP], except that the
                            ;  /<ttl> and /<number of addresses>
                            ;  fields are not included.
                            ; FQDN and extn-addr are as defined
                            ;  in [SDP].
```

```
   basic-IP4-multicast =       m1 3( "." decimal-uchar )
                               ; m1 and decimal-uchar are as defined
                               ;  in [SDP].

   basic-IP6-multicast =       hexpart
                               ; hexpart is as defined in [SDP].
```

Authors' Addresses

Bob Quinn
BoxnArrow.com
31 Caldwell Road
Waltham, MA 02453

Phone: +1-781-577-1539
EMail: rcq@boxnarrow.com

Ross Finlayson
Live Networks, Inc.
650 Castro St., suite 120-196
Mountain View, CA 94041

EMail: finlayson@live555.com

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).