                          SDP Source-Filters
                 <draft-ietf-mmusic-sdp-srcfilter-00.txt>

Status of this Memo

This document is an Internet-Draft and is in full conformance with all
provisions of Section 10 of RFC2026.

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.

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.

Receiver applications are expected 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).

Table of Contents

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., SAP, SIP, RTSP, email, HTTP,
etc.).

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

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.

Quinn

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 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.

The source-filter attribute is comprised of two parts:

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

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

    <nettype> <address-types> <dest-address> <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.

Second sub-field <address-types> identifies the address family and for
the purpose of this document may be either <addrtype> values "IP4" or
"IP6". Alternately, when <dest-address> is an FQDN, the value may be
"*" to apply to both address types, since either address may 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 sessionÆs "connection-address"
field values. It may be either a unicast or multicast address, an FQDN
(fully-qualified domain name), or the "*" wildcard to match any/all of
the sessionÆs "connection-address" values.

And 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 (email-safe) whitespace.

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

2.1   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
should NOT include the sub-fields <ttl> and <number of addresses> from
the <connection-address> value. The <number of addresses> is implied,
and all unicast addresses in the <src-list> are valid sources for any
of the multicast addresses in the address series implied by the <number
of addresses>. See section 2.2.4 for an example.

When the <addrtype> value is the "*" wildcard, the <dest-address> must
be either an FQDN or "*" (i.e., it cannot be either an IPv4 or IPv6
address). See section 2.2.6 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 media (i.e., "session-level" or
"media-level"). A media-level source-filter will always override a
session-level source-filter.

A <source-filter> need not be located at the same hierarchy level as
its corresponding <connection-field>. Hence, a media-level <source-
filter> can reference a session-level <connection-field> value, and a
session-level <source-filter> may be applied to all matching media-
level <connection-field> values. See section 2.2.3 for an example.

Only one source filter attribute entry may be defined for each
<connection address> value at either session-level or media-level. If
more than one is provided, only the first <source-filter> attribute to
appear is used (and other <source-filter> entries MUST be ignored).

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.

2.2   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@ipmulticast.com>
     s=Elvis Impersonation
     i=All Elvis, all the time
     u=http://www.ipmulticast.com/ElvisLive/
     t=0 0
     a=recvonly

<media-description 1> =
     m=audio 54321 RTP/AVP 0

<media-description 2> =
     m=video 54322 RTP/AVP 0
```


2.2.1   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
192.168.9.10 to the multicast session address 232.3.4.5.

```
     <session-description>

     c=IN IP4 232.3.4.5/127
     a=incl:IN IP4 232.3.4.5 192.168.9.10

     <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.

2.2.2   Unicast Exclusion Example

Typically an SDP session <connection-address> value is a multicast address, although it is also possible to use of either a unicast address or FQDN. This example illustrates a scenario whereby a session description indicates the unicast source address 192.168.9.10 in an exclusion filter. In effect, this sample source-filter says, "host **192.168.10.11 destination should accept traffic from any sender** *except* 192.168.9.10."

        <session-description>

        c=IN IP4 192.168.10.11
        a=excl:IN IP4 192.168.10.11 192.168.9.10

        <media-description 1>

2.2.3   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 192.168.9.10. Traffic sent from any other unicast source address should be discarded by the receiver.

        <session-description>

        a=incl:IN IP4 * 192.168.9.10

        <media-description 1>

        c=IN IP4 232.2.2.2/127

        <media-description 2>

        c=IN IP4 232.4.4.4/63

2.2.4   Multiple Source and Destination Example

The source-filter in this example specifies a legitimate source address for each of three multicast addresses in a series. Specifically, **1.1.1.1 is the legitimate source for 232.3.4.5, 2.2.2.2 is the** legitimate source for 232.3.4.6, and 3.3.3.3 is the legitimate source for 232.3.4.7. Traffic sent from any other source addresses should be discarded.

```
<session-description>

c=IN IP4 232.3.4.5/127/3
```

```
    a=incl:IN IP4 232.3.4.5 1.1.1.1 2.2.2.2 3.3.3.3

    <media-description 1>
```

2.2.5   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 FFOE::11A is only valid from the unicast
source address 2001:210:1:2:240:96FF:FE25:8EC9

```
    <session-description>

    c=IN IP6 FF0E::11A/127
    a=incl:IN IP6 FF0E::11A 2001:210:1:2:240:96FF:FE25:8EC9

    <media-description 1>
```

2.2.6   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 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.ipmulticast.com/127
    c=IN IP6 Channel-1.ipmulticast.com/127
    a=incl:IN * Channel-1.ipmulticast.com Src-1.ipmulticast.com

    <media-description 1>
```

3 Interoperability Issues

Defining a list of legitimate sources for a multicast destination
address represents a departure from the Internet Standard Multicast
(ISM) model, as originally described in [IGMPv1]. The ISM 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

Quinn   [Page 7]

protocols. Use of source-filters do not corrupt the ISM semantics but provide more control for receivers, at their discretion.

[4] Security Considerations

See [SDP] for security other considerations specific to the Session Description Protocol in general. The central issue relevant to using unicast 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 (use one other than their own) in datagrams they send. Proper router configuration can reduce the likelihood of "spoofed" source addresses being sent to or from a network, however. Specifically, border routers are encouraged to filter traffic so datagrams with invalid source addresses are not forwarded (e.g., routers drop datagrams if the source address is non-local) [CA-96.21].

Despite the weaknesses of source address-based filtering, this mechanism provides more security than is currently available with respect to source authentication of IP Multicast senders.

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 any). If unsecured, it is conceivable that the DNS server could return illegitimate addresses.

[5] IANA Considerations

As recommended by [SDP] (in Appendix B), the new source-filter attribute described in this document should be registered with IANA.

Acknowledgements

The author would like to thank Dave Thaler and Mark Handley, whose input provided much of the substance of this document.

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

```
source-filter =     filter-mode ":" filter-spec

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

filter-spec =       nettype address-types dest-address src-list

address-types =     "*" | addrtype
                    ; "*" for all address types (both IP4 and IP6),
                    ;  but only when <dest-address> and <src-list>
                    ;  reference FQDNs

dest-address =      "*" | IP4-address | IP6-address | FQDN
                    ; "*" applies to all connection-address values

src-list =          *(addr email-safe) addr
                    ; one or more unicast source addresses (in standard
                    ; IPv4 or IPv6 ASCII-notation form) or FQDNs
```

References

[CA-96.21]   CERT Advisory CA-96.21, "TCP SYN Flooding and IP
               Spoofing Attacks," September 1996

[ABNF]   D. Crocker, P. Overell, "Augmented BNF for Syntax
               Specifications: ABNF," RFC 2234, November 1997

[IGMPv1]   S. Deering, "Host Extensions for IP Multicasting," RFC
               1112 (STD 5), August 1989

[MSF API]   D. Thaler, B. Fenner, B. Quinn, "Socket Interface
               Extensions for Multicast Source Filters," draft-ietf-
               idmr-igmpv3-api-00.txt, February 2000

[SDP]   M. Handley, V. Jacobson, "SDP: Session Description
               Protocol," RFC 2327, April 1998

[UTF-8]   F. Yergeau, "UTF-8, a transformation format of Unicode
               and ISO 10646," RFC 2044, October 1996

Author's Address

Bob Quinn
IP Multicast Initiative
Stardust.com
1901 S. Bascom Ave., Suite 333
Campbell, CA 95008
Phone: +1-408-879-8080
Email: rcq@stardust.com

Expires November 2000