Network Working Group
Request for Comments: 3420
Category: Standards Track

R. Sparks
dynamicsoft

November 2002

Internet Media Type message/sipfrag

Status of this Memo

Copyright Notice

Abstract

This document registers the message/sipfrag Multipurpose Internet Mail Extensions (MIME) media type. This type is similar to message/sip, but allows certain subsets of well formed Session Initiation Protocol (SIP) messages to be represented instead of requiring a complete SIP message. In addition to end-to-end security uses, message/sipfrag is used with the REFER method to convey information about the status of a referenced request.

Table of Contents

1. Introduction

The message/sip MIME media type defined in [1] carries an entire well formed SIP message. Section 23.4 of [1] describes the use of message/sip in concert with S/MIME to enhance end-to-end security. The concepts in that section can be extended to allow SIP entities to make assertions about a subset of a SIP message (for example, as described in [6]). The message/sipfrag type defined in this document is used to represent this subset.

A subset of a SIP message is also used by the REFER method defined in [5] to carry the status of referenced requests. Allowing only a portion of a SIP message to be carried allows information that could compromise privacy and confidentiality to be protected by removal.

This document does NOT provide a mechanism to segment a SIP message into multiple pieces for separate transport and later reassemble. The message/partial type defined in [2] provides a solution for that problem.

The key words "MUST", "MUST NOT", REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMEND", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [4].

2. Definition: message/sipfrag

A valid message/sipfrag part is one that could be obtained by starting with some valid SIP message and deleting any of the following:

- the entire start line
- one or more entire header fields
- the body

The following Augmented Backus-Naur Form (ABNF) [3] rule describes a message/sipfrag part using the SIP grammar elements defined in [1]. The expansion of any element is subject to the restrictions on valid SIP messages defined there.

```
sipfrag = [ start-line ]
          *message-header
          [ CRLF [ message-body ] ]
```

If the message/sipfrag part contains a body, it MUST also contain the appropriate header fields describing that body (such as Content-Length) as required by Section 7.4 of [1] and the null-line separating the header from the body.

3. Examples

3.1 Valid message/sipfrag parts

This section uses a vertical bar and a space to the left of each example to illustrate the example's extent. Each line of the message/sipfrag element begins with the first character after the "|" pair.

The first two examples show that a message/sipfrag part can consist of only a start line.

```
      | INVITE sip:alice@atlanta.com SIP/2.0
   or
      | SIP/2.0 603 Declined
```

The next two show that Subsets of a full SIP message may be represented.

```
   | REGISTER sip:atlanta.com SIP/2.0
   | To: sip:alice@atlanta.com
   | Contact: <sip:alicepc@atlanta.com>;q=0.9,
   |          <sip:alicemobile@atlanta.com>;q=0.1

   | SIP/2.0 400 Bad Request
   | Warning: 399 atlanta.com Your Event header field was malformed
```

A message/sipfrag part does not have to contain a start line. This example shows a part that might be signed to make assertions about a particular message. (See [6].)

```
      | From: Alice <sip:alice@atlanta.com>
      | To: Bob <sip:bob@biloxi.com>
      | Contact: <sip:alice@pc33.atlanta.com>
      | Date: Thu, 21 Feb 2002 13:02:03 GMT
      | Call-ID: a84b4c76e66710
      | Cseq: 314159 INVITE
```

The next two examples show message/sipfrag parts that contain bodies.

```
| SIP/2.0 200 OK
| Content-Type: application/sdp
| Content-Length: 247
|
| v=0
| o=alice 2890844526 2890844526 IN IP4 host.anywhere.com
| s=
| c=IN IP4 host.anywhere.com
| t=0 0
| m=audio 49170 RTP/AVP 0
| a=rtpmap:0 PCMU/8000
| m=video 51372 RTP/AVP 31
| a=rtpmap:31 H261/90000
| m=video 53000 RTP/AVP 32
| a=rtpmap:32 MPV/90000

| Content-Type: text/plain
| Content-Length: 11
|
| Hi There!
```

3.2 Invalid message/sipfrag parts

This section uses the character "X" followed by a space to the left of each example to illustrate the example's extent. Each line of the invalid message/sipfrag element begins with the first character after the "X " pair.

The start line, if present, must be complete and valid per [1].

```
X INVITE

X INVITE sip:alice@atlanta.com SIP/1.09

X SIP/2.0

X 404 Not Found
```

All header fields must be valid per [1].

```
X INVITE sip:alice@atlanta.com SIP/2.0
X Via: SIP/2.0/UDP ;branch=z9hG4bK29342a
X To: <>;tag=39234

X To: sip:alice@atlanta.com
X From: sip:bob@biloxi.com;tag=1992312
```

```
X Call-ID: this is invalid

X INVITE sip:alice@atlanta.com SIP/2.0
X From: <sip:bob@biloxi.com>;tag=z9hG4bK2912;tag=z9hG4bK99234
```

If a body is present in the message/sipfrag part, the headers required by Section 7.4 of [1] and the null-line separating the header from the body.

```
X MESSAGE sip:alice@atlanta.com SIP/2.0
X Hi There!
```

4. Discussion

Section 23 of [1], and memos [5] and [6] provide motivation and detailed examples of carrying all or part of a SIP message in a MIME part. Briefly, using this representation along with S/MIME enables protecting and making assertions about portions of a SIP message header. It also enables applications to describe the messaging involved in a SIP transaction using portions of the messages themselves.

The SIP REFER method [5], for instance, uses this to report the result of a SIP request to an authorized third party. However, as that document details, it is rarely desirable to include the entire SIP response message in this report as a message/sip MIME part. Doing so has significant negative security implications. The message/sipfrag type, on the other hand, allows a sender to select what information is exposed. Further, it allows information required in a full SIP message that is not pertinent to a description of that message to be elided, reducing message size. For instance, this allows a SIP element responding to a REFER to say "I got a 400 Bad Request with this Warning header field" without having to include the Via, To, From, Call-ID, CSeq and Content-Length header fields mandatory in a full SIP message.

The message protection mechanism discussed in Section 23 of [1] assumes an entire SIP message is being protected. However, there are several header fields in a full SIP message that necessarily change during transport. [1] discusses how to inspect and ignore those changes. This idea is refined in [6] to allow protection of a subset of the entire message, avoiding the extra work and potential errors involved in ignoring parts of the message that may legitimately change in transit. That document also describes constructing cryptographic assertions about pertinent subsets of a SIP message header before the full header (including hop-by-hop transport specific information) may be available.

5. IANA Considerations

The message/sipfrag media type is defined by the following information:

Media type name: message
Media subtype name: sipfrag
Required parameters: none
Optional parameters: version
  Version: The SIP-Version number of the enclosed message (e.g., "2.0"). If not present, the version defaults to "2.0".
Encoding scheme: SIP messages consist of an 8-bit header optionally followed by a binary MIME data object. As such, SIP messages must be treated as binary. Under normal circumstances SIP messages are transported over binary-capable transports, no special encodings are needed.
Security considerations: see below

6. Security Considerations

A message/sipfrag mime-part may contain sensitive information or information used to affect processing decisions at the receiver. When exposing that information or modifying it during transport would do harm, its level of protection can be improved using the S/MIME mechanisms described in section 23 of [1], with the limitations described in section 26 of that document, and the mechanisms described in [6].

Applications using message/sipfrag to represent a subset of the header fields from a SIP message must consider the implications of the message/sipfrag part being captured and replayed and include sufficient information to mitigate risk. Any SIP extension which uses message/sipfrag MUST describe the replay and cut and paste threats unique to its particular usage. For example, [6] discusses how a subset of a SIP message can be used to assert the identity of the entity making a SIP request. The draft details what information must be contained in the subset to bind the assertion to the request.

Normative References

[1] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and E. Schooler, "SIP: Session Initiation Protocol", RFC 3265, June 2002.

[2] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, November 1996.

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

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

Non-Normative References

[5] Sparks, R., "The SIP Refer Method", Work in Progress.

[6] Peterson, J., "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", Work in Progress.

Author’s Address

Robert J. Sparks
dynamicsoft
5100 Tennyson Parkway
Suite 1200
Plano, TX 75024

EMail: rsparks@dynamicsoft.com

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.