SIP WG
Internet-Draft
Expires: April 28, 2003

J. Peterson
NeuStar
October 28, 2002

SIP Authenticated Identity Body (AIB) Format
draft-ietf-sip-authid-body-00

Status of this Memo

Copyright Notice

Abstract

RFC3261 introduces the concept of adding an S/MIME body to a SIP request or response in order to provide reference integrity over its headers. This document provides a more specific mechanism to derive integrity and authentication properties from an 'authenticated identity body', a digitally-signed SIP message or message fragment. A standard format for such bodies (known as Authenticated Identity Bodies, or AIBs) is given in this document. Some considerations for the processing of AIBs by recipients of SIP messages with such bodies are also given.

Table of Contents

1. Introduction

Section 23.4 of RFC3261 [1] describes an integrity mechanism that relies on signing tunneled 'message/sip' MIME bodies within SIP requests. The purpose of this mechanism is to replicate the headers of a SIP request within a body carried in the request in order to provide a digital signature over these headers.

The core requirement that motivates this mechanism is the problem of providing a cryptographically verifiable identity within a SIP request. The baseline SIP protocol allows a user agent to express the identity of its user in a number of headers. The primary place for identity information asserted by the sender of a request is the From header. The From header field contains a URI (like 'sip:alice@atlanta.com') and an optional display-name (like "Alice") that identifies the originator of the request. A user may have many identities that are used in different contexts.

Typically, this URI is an address-of-record that can be dereferenced in order to contact the originator of the request; specifically, it is usually the same address-of-record under which a user registers their devices (using the SIP REGISTER method) in order to receive incoming requests. This address-of-record is assigned and maintained by the administrator of the SIP service in the domain identified by the host portion of the address-of-record (which may have any of a number of relationships with the end user). However, the From field of a request can usually be set arbitrarily by the user of a SIP user agent; the From header of a message provides no internal assurance that the originating user can legitimately claim this identity. Nevertheless, many SIP user agents will obligingly display the contents of the From field as the identity of the originator of a received request (as a sort of 'Caller-ID' function).

In order to provide the recipient of a SIP message with greater assurance of the identity of the sender, a cryptographic signature can be provided over the headers of the SIP request, which allows the signer to assert a verifiable identity. Unfortunately, a signature over the From header alone is insufficient because it could be cut-and-pasted into a replay or forwarding attack. However, SIP messages can also be large, and many of the headers in a SIP message would not be relevant to determining the identity of the sender or assuring reference integrity with the request. It is therefore desirable to find a happy medium - to provide a way of signing just enough headers that the identity of the sender can be ascertained. 'message/sipfrag' [3] allows a subset of SIP headers to be included in a MIME body; the AIB format described in Section 2 is based on 'message/sipfrag'.

For reasons of end-to-end privacy, it may also be desirable to encrypt AIBs; procedures for this encryption are given in Section 6.

2. AIB Format

As a way of sharing authenticated identity among parties in the network, a special type of MIME body format, the Authenticated Identity Body (AIB) format, is defined in this section. AIBs allow a party in a SIP transaction to cryptographically sign the headers that assert the identity of the originator of a message, and provide some other headers necessary for reference integrity.

An AIB is a MIME body of type 'message/sip' or 'message/sipfrag' (see [3]). This body MUST have a Content-Disposition disposition-type of 'aib', a new value defined in this document specifically for authenticated identity bodies. The Content-Disposition header SHOULD also contain a 'handling' parameter indicating that this MIME body is optional.

AIBs using the 'message/sipfrag' MIME type MUST contain the following headers: From, Date and Call-ID; they SHOULD also contain the To, Contact and CSeq header. AIBs MAY contain any other headers that help to uniquely identify the transaction or provide related reference integrity. An example of the AIB format is:

```
Content-Type: message/sipfrag
Content-Disposition: aib; handling=optional

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
```

Unsigned AIBs MUST NOT be honored by any recipients. After the AIB has been signed, it SHOULD be added it to any existing MIME bodies in the request (such as SDP), if necessary by transitioning the outermost MIME body to a 'multipart/mixed' format.

3. Example of a Request with AIB

The following shows a full SIP INVITE request with an AIB:

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
```

```
   Call-ID: a84b4c76e66710
   CSeq: 314159 INVITE
   Max-Forwards: 70
   Date: Thu, 21 Feb 2002 13:02:03 GMT
   Contact: <sip:alice@pc33.atlanta.com>
   Content-Type: multipart/mixed; boundary=unique-boundary-1

   --unique-boundary-1

   Content-Type: application/sdp
   Content-Length: 147

   v=0
   o=UserA 2890844526 2890844526 IN IP4 here.com
   s=Session SDP
   c=IN IP4 pc33.atlanta.com
   t=0 0
   m=audio 49172 RTP/AVP 0
   a=rtpmap:0 PCMU/8000

   --unique-boundary-1
   Content-Type: multipart/signed;
     protocol="application/pkcs7-signature";
     micalg=sha1; boundary=boundary42
   Content-Length: 608

   --boundary42
   Content-Type: message/sipfrag
   Content-Disposition: aib; handling=optional

   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

   --boundary42
   Content-Type: application/pkcs7-signature; name=smime.p7s
   Content-Transfer-Encoding: base64
   Content-Disposition: attachment; filename=smime.p7s;
      handling=required

   ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6
   4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj
   n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
   7GhIGfHfYT64VQbnj756
```

```
--boundary42--

--unique-boundary-1--
```

4. Identity in Responses

Many of the practices described in the preceding sections can be applied to responses as well as requests. Note that a new set of headers must be generated to populate the AIB in a response. The From header field of the AIB in the response SHOULD correspond to the address-of-record of the responder, NOT to the From header field received in the request. The To header field of the request MUST NOT be included. A new Date header field and Contact header field should be generated for the AIB in a response. The Call-ID and CSeq should, however, be copied from the request.

Generally, the To header field of the request will correspond to the address-of-record of the responder. In some architectures where redirection is used, however, this need not be the case. Some recipients of response AIBs may consider it a cause for security concern if the To header field of the request is not the same as the address-of-record in the From header field of the AIB in a response.

5. Receiving an AIB

When a user agent receives a request containing an AIB, it should verify the signature, including validating the certificate of the signer, and compare the identity of the signer (the subjectAltName) with the From header field of the request. The two should correspond exactly; if they do not, the user agent should report this condition to its user before proceeding. User agents may distinguish between plausibly minor variations (the difference between 'atlanta.com' and 'sip.atlanta.com') and major variations ('atlanta.com' vs. 'evil.tv') when reporting these discrepancies in order to give the user some idea of how to handle this situation.

When the originating user agent of a request receives a response containing an AIB, it SHOULD compare the identity in the To header field of the AIB of the response with the original value of the To header field in the request. If these represent different identities, the user agent SHOULD render the identity in the AIB of the response to its user. Note that a discrepancy in these identity fields is not necessary an indication of a security breach; normal retargeting may simply have directed the request to a different final destination.

6. Encryption of Identity

Many SIP entities that support the use of S/MIME for signatures will also support S/MIME encryption, as described in RFC3261 Section 23.4.3. Encryption of a body prevents any parties other those that hold the decryption key from inspecting the body.

While encryption of AIBs entails that only the holder of a specific key can decrypt the body, that single key could be distributed throughout a network of hosts that exist under common policies. The security of the AIBF is therefore predicated on the secure distribution of the key. However, for some networks (in which there are federations of trusted hosts under a common policy), the widespread distribution of a decryption key could be appropriate. Some telephone networks, for example, might require this model.

When an AIB is encrypted, the AIB SHOULD always be encrypted before it is signed. Note that this means that the recipients of the request, even if they are unable to inspect the AIBF, will still be able to see who signed that body (although it will not necessarily be obvious that the body contains an AIB).

7. Example of Encryption

The following is an example of an encrypted and signed AIB (without any of the preceding SIP headers). In a rendition of this body sent over the wire, the text wrapped in asterisks would be encrypted.

```
Content-Type: multipart/signed;
  protocol="application/pkcs7-signature";
  micalg=sha1; boundary=boundary42
Content-Length: 568

--boundary42

Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
  name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m
  handling=required
Content-Length: 231

************************************************************
* Content-Type: message/sipfrag                            *
* Content-Disposition: aib; handling=optional              *
*                                                          *
* From: sip:alice@atlanta.com                              *
* Call-ID: a84b4c76e66710                                  *
* Date: Thu, 21 Feb 2002 13:02:03 GMT                     *
************************************************************

--boundary42

Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s;
   handling=required

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj
n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
7GhIGfHfYT64VQbnj756

--boundary42--
```

8. Security Considerations

This document recommends the inclusion of the Contact, CSeq and To headers in AIBs when 'message/sipfrag' is used. If these headers are omitted, some important security properties of AIB are lost. For example, the Contact header determines how new requests in a dialog are routed. If an attacker were to modify the Contact header of a SIP request in transit, and that header were not protected by the AIBF, then new requests might not return to the originator of the request.

9. IANA Considerations

This document defines a new MIME Content-Disposition disposition-type value of 'aib'. This value is reserved for MIME bodies that contain an authenticated identity, as described in section Section 2.

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 3261, May 2002.

[2] Bradner, S., "Key words for use in RFCs to indicate requirement levels", RFC 2119, March 1997.

[3] Sparks, R., "Internet Media Type message/sipfrag", draft-ietf-sip-sipfrag-00 (work in progress), September 2002.

Author's Address

Jon Peterson
NeuStar, Inc.
1800 Sutter St
Suite 570
Concord, CA 94520
US

Phone: +1 925/363-8720
EMail: jon.peterson@neustar.biz
URI: http://www.neustar.biz/

Full Copyright Statement

Acknowledgement

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