Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 4, 2018

A. Melnikov
Isode Ltd

October 1, 2017

Considerations for protecting Email header with S/MIME
draft-melnikov-smime-header-signing-05

Abstract

This document describes best practices for handling of Email header protected by S/MIME. It also adds a new Content-Type parameter to help distinguish an S/MIME protected forwarded message from an S/MIME construct protecting message header.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on April 4, 2018.

Table of Contents

1. Introduction

S/MIME [RFC5751] is typically used to protect (sign and/or encrypt) Email message body parts, but not header of corresponding Email messages. Header fields may contain confidential information or information whose validity need protecting from disclosure or modification. [RFC5751] describes how to protect the Email message header [RFC5322], by wrapping the message inside a message/rfc822 container [RFC2045]:

> In order to protect outer, non-content-related message header fields (for instance, the "Subject", "To", "From", and "Cc" fields), the sending client MAY wrap a full MIME message in a message/rfc822 wrapper in order to apply S/MIME security services to these header fields. It is up to the receiving client to decide how to present this "inner" header along with the unprotected "outer" header.
>
> When an S/MIME message is received, if the top-level protected MIME entity has a Content-Type of message/rfc822, it can be assumed that the intent was to provide header protection. This entity SHOULD be presented as the top-level message, taking into account header merging issues as previously discussed.

While the above advice helps in protecting message header fields, it doesn't provide enough guidance on what information should and should not be included in outer (unprotected) header and how information from outer and inner headers should be presented to users. This document describes best UI and other practices for handling of messages wrapped inside message/rfc822 body parts. The goal of this document is to improve interoperability and minimize damage caused by possible differences between inner and outer headers.

2. Conventions Used in This Document

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].

3. Recommendations for handling of S/MIME protected header

When generating S/MIME messages which protect header fields by wrapping a message inside message/rfc822 wrapper:

1. If a header field is being encrypted because it is sensitive, its true value MUST NOT be included in the outer header. If the header field is mandatory according to RFC 5322, a stub value (or a value indicating that the outer value is not to be used) is to be included.

2. The outer header SHOULD be minimal in order to avoid disclosure of confidential information. It is recommended that the outer header only contains "Date" (set to the same value as in the inner header, or, if the Date value is also sensitive, to Monday 9am of the same week), possibly "Subject" and "To"/"Bcc" header fields. In particular, Keywords, In-Reply-To and References header fields SHOULD NOT be included in the outer header; "To" and "Cc" header fields should be omitted and replaced with "Bcc: undisclosed-recipients;".

   But note that having key header fields duplicated in the outer header is convenient for many message stores (e.g. IMAP) and clients that can't decode S/MIME encrypted messages. In particular, Subject/To/Cc/Bcc/Date header field values are returned in IMAP ENVELOPE FETCH data item [RFC3501], which is frequently used by IMAP clients in order to avoid parsing message header.

3. The "Subject" header field value of the outer header SHOULD either be identical to the inner "Subject" header field value, or contain a clear indication that the outer value is not to be used for display (the inner header field value would contain the true value).

Note that recommendations listed above only apply to non MIME header fields (header fields with names not starting with "Content-" prefix).

Note that the above recommendations can also negatively affect antispam processing.

When displaying S/MIME messages which protect header fields by wrapping a message inside message/rfc822 wrapper:

1. The outer headers might be tampered with, so a receiving client SHOULD ignore them, unless they are protected in some other way(*). If a header field is present in the inner header, only the inner header field value MUST be displayed (and the corresponding outer value must be ignored). If a particular header field is only present in the outer header, it MAY be ignored (not displayed) or it MAY be displayed with a clear indicator that it is not trustworthy(*).

   (*) - this only applies if the header field is not protected is some other way, for example with a DKIM signature that validates and is trusted.

4. New Content-Type header field parameter: forwarded

This document defines a new Content-Type header field parameter [RFC2045] with name "forwarded". The parameter value is case-insensitive and can be either "yes" or "no". (The default value being "yes"). The parameter is only meaningful with media type "message/rfc822" and "message/global" [RFC6532] when used within S/MIME encrypted body parts. The value "yes" means that the message nested inside message/rfc822 is a forwarded message and not a construct created solely to protect the inner header.

Instructions in [RFC5751] describing how to protect the Email message header [RFC5322], by wrapping the message inside a message/rfc822 container [RFC2045] are thus updated to read:

> In order to protect outer, non-content-related message header fields (for instance, the "Subject", "To", "From", and "Cc" fields), the sending client MAY wrap a full MIME message in a message/rfc822 wrapper in order to apply S/MIME security services to these header fields. It is up to the receiving client to decide how to present this "inner" header along with the unprotected "outer" header.
>
> When an S/MIME message is received, if the top-level protected MIME entity has a Content-Type of message/rfc822 or message/global without the "forwarded" parameter or with the "forwarded" parameter set to "no", it can be assumed that the intent was to provide header protection. This entity SHOULD be presented as the top-level message, taking into account header merging issues as previously discussed.

5. Example message with S/MIME header protection

The following example demonstrates a message generated to protect original message header. For example, this will be the first body part of a multipart/signed message or the payload of the application/pkcs7-mime body part.

```
Content-Type: message/rfc822; forwarded=no

Date: Mon, 25 Sep 2017 17:31:42 +0100 (GMT Daylight Time)
From: "Alexey Melnikov" <alexey.melnikov@example.net>
Message-ID: <e4a483cb-1dfb-481d-903b-298c92c21f5e@mattingly.example.net>
MIME-Version: 1.0
MMHS-Primary-Precedence: 3
Subject: Secret meeting at my place
To: somebody@example.net
X-Mailer: Isode Harrier Web Server
content-type: text/plain; charset=us-ascii

This is a secret message worth protecting.
```

[[CREF1: Extend the example to show different inner and outer header fields and clarify what should be displayed?]]

6. IANA Considerations

This document requests no action from IANA. RFC Editor should delete this section before publication.

7. Security Considerations

This document talks about UI considerations, including security considerations, when processing wrapped message/rfc822 messages protecting header fields. One of the goals of this document is to specify UI for displaying such messages which is less confusing/misleading and thus more secure.

The document is not defining new protocol, so it doesn't create any new security concerns not already covered by S/MIME [RFC5751], MIME [RFC2045] and Email [RFC5322] in general.

8. References

8.1. Normative References

[RFC2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, DOI 10.17487/RFC2045, November 1996, <https://www.rfc-editor.org/info/rfc2045>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <https://www.rfc-editor.org/info/rfc5322>.

[RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, DOI 10.17487/RFC5751, January 2010, <https://www.rfc-editor.org/info/rfc5751>.

[RFC6532] Yang, A., Steele, S., and N. Freed, "Internationalized Email Headers", RFC 6532, DOI 10.17487/RFC6532, February 2012, <https://www.rfc-editor.org/info/rfc6532>.

8.2. Informative References

[RFC3501] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1", RFC 3501, DOI 10.17487/RFC3501, March 2003, <https://www.rfc-editor.org/info/rfc3501>.

Appendix A. Acknowledgements

Thank you to Wei Chuang, Steve Kille, David Wilson and Robert Williams for suggestions, comments and corrections on this document. Some ideas were also taken from Daniel Kahn Gillmor's email on the OpenPGP mailing list.

David Wilson came up with the idea of defining a new Content-Type header field parameter to distinguish forwarded messages from inner header field protection constructs.

Author's Address

Alexey Melnikov
Isode Ltd
14 Castle Mews
Hampton, Middlesex TW12 2NP
UK

EMail: Alexey.Melnikov@isode.com