Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 21, 2019

A. Melnikov
Isode Ltd

October 18, 2018

Considerations for protecting Email header with S/MIME
draft-melnikov-lamps-header-protection-00

Abstract

This document describes best practices for handling of Email header protected by S/MIME. Procedures described in this document are also applicable to OpenPGP.

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 21, 2019.

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 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. Additionally, there are very few implementations of the header

protection mechanism specified in [RFC5751]. Email clients that don't support this mechanism display messages with header protection as if they are forwarded email messages. Some of them don't display content of forwarded messages by default (e.g. they display at attachment or an icon), so viewing them requires an extra action by the user.

[[Alexey: Depending on WG consensus, the following text will be updated to either suggest and alternative approach that is friendlier to non compliant email clients or to reinforce use of message/rfc822 for header protection + recommend use of the new "forwarded" parameter to Content-Type.]] This document describes best UI and other practices for handling of message header protection. 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", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The terms "header field" and "header section" are defined in [RFC5322].

The following terms are defined in this document:

Signed-only message: a multipart/signed or application/pkcs7-mime containing SignedData message which doesn't contain any encrypted layer. I.e. this is a message which is not encrypted and not encrypted + signed.

3. Recommended algorithms for email header protection

[[LAMPS WG should pick between the following 2 alternatives. They are described in details in subsections of this section.]]

Examples in subsequent sections assume that an email client is trying to protect (sign) the following initial message:

```
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: Meeting at my place
To: somebody@example.net
X-Mailer: Isode Harrier Web Server
Content-Type: text/plain; charset=us-ascii

This is an important message that I don't want to be modified.
```

Without message header protection the corresponding signed message might look like this. (Lines prepended by "O: " are the outer header.)

```
O: Date: Mon, 25 Sep 2017 17:31:42 +0100 (GMT Daylight Time)
O: Message-ID: <e4a483cb-1dfb-481d-903b-298c92c21f5e@mattingly.example.net>
O: Subject: Meeting at my place
O: From: "Alexey Melnikov" <alexey.melnikov@example.net>
O: MIME-Version: 1.0
O: content-type: multipart/signed; charset=us-ascii; micalg=sha1;
O:  protocol="application/pkcs7-signature";
O:  boundary=.cbe16d2a-e1a3-4220-b821-38348fc97237

   This is a multipart message in MIME format.
   --.cbe16d2a-e1a3-4220-b821-38348fc97237
   Content-Type: text/plain; charset=us-ascii

   This is an important message that I don't want to be modified.

   --.cbe16d2a-e1a3-4220-b821-38348fc97237
   Content-Transfer-Encoding: base64
   content-type: application/pkcs7-signature

   [[base-64 encoded signature]]

   --.cbe16d2a-e1a3-4220-b821-38348fc97237--
```

3.1. Option 1: Memory Hole

Memory Hole approach works by copying the normal message header fields into the MIME header section of the top level protected body part. Since the MIME body part header section is itself covered by the protection mechanisms (signing and/or encryption) it shares the protections of the message body.

The following example demonstrates how header section and payload of a protect body part might look like. For example, this will be the first body part of a multipart/signed message or the signed and/or encrypted payload of the application/pkcs7-mime body part. Lines prepended by "O: " are the outer header section. Lines prepended by "I: " are the inner header section.

```
O: Date: Mon, 25 Sep 2017 17:31:42 +0100 (GMT Daylight Time)
O: Message-ID: <e4a483cb-1dfb-481d-903b-298c92c21f5e@mattingly.example.net>
O: Subject: Meeting at my place
O: From: "Alexey Melnikov" <alexey.melnikov@example.net>
O: MIME-Version: 1.0
O: content-type: multipart/signed; charset=us-ascii; micalg=sha1;
O:  protocol="application/pkcs7-signature";
O:  boundary=.cbe16d2a-e1a3-4220-b821-38348fc97237

   This is a multipart message in MIME format.
   --.cbe16d2a-e1a3-4220-b821-38348fc97237
I: Date: Mon, 25 Sep 2017 17:31:42 +0100 (GMT Daylight Time)
I: From: "Alexey Melnikov" <alexey.melnikov@example.net>
I: Message-ID: <e4a483cb-1dfb-481d-903b-298c92c21f5e@mattingly.example.net>
I: MIME-Version: 1.0
I: MMHS-Primary-Precedence: 3
I: Subject: Meeting at my place
I: To: somebody@example.net
I: X-Mailer: Isode Harrier Web Server
I: Content-Type: text/plain; charset=us-ascii

   This is an important message that I don't want to be modified.

   --.cbe16d2a-e1a3-4220-b821-38348fc97237
   Content-Transfer-Encoding: base64
   content-type: application/pkcs7-signature

   [[base-64 encoded signature]]

   --.cbe16d2a-e1a3-4220-b821-38348fc97237--
```

3.2. Option 2: Wrapping with message/rfc822 or message/global

Wrapping with message/rfc822 (or message/global) works by copying the normal message header fields into the MIME header section of the top level protect body part and then prepending them with "Content-Type: message/rfc822; forwarded=no\r\n" or "Content-Type: message/global; forwarded=no\r\n", where \r\n is US-ASCII CR followed by US-ASCII LF. Since the MIME body part header section is itself covered by the protection mechanisms (signing and/or encryption) it shares the protections of the message body.

The rest of this section formally defines the new "forwarded" Content-Type header field parameter and how header section wrapping works.

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 signed or encrypted body parts. The value "yes" means that the message nested inside "message/rfc822" ("message/global") is a forwarded message and not a construct created solely to protect the inner header section.

Instructions in [RFC5751] describing how to protect the Email message header section [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 section along with the unprotected "outer" header section.
>
> 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 section merging issues as previously discussed.

The following example demonstrates how header section and payload of a protect body part might look like. For example, this will be the first body part of a multipart/signed message or the signed and/or encrypted payload of the application/pkcs7-mime body part. Lines prepended by "O: " are the outer header section. Lines prepended by "I: " are the inner header section. Lines prepended by "W: " are the wrapper.

```
O: Date: Mon, 25 Sep 2017 17:31:42 +0100 (GMT Daylight Time)
O: Message-ID: <e4a483cb-1dfb-481d-903b-298c92c21f5e@mattingly.example.net>
O: Subject: Meeting at my place
O: From: "Alexey Melnikov" <alexey.melnikov@example.net>
O: MIME-Version: 1.0
O: content-type: multipart/signed; charset=us-ascii; micalg=sha1;
O:  protocol="application/pkcs7-signature";
O:  boundary=.cbe16d2a-e1a3-4220-b821-38348fc97237

   This is a multipart message in MIME format.
   --.cbe16d2a-e1a3-4220-b821-38348fc97237
W: Content-Type: message/rfc822; forwarded=no
W:
I: Date: Mon, 25 Sep 2017 17:31:42 +0100 (GMT Daylight Time)
I: From: "Alexey Melnikov" <alexey.melnikov@example.net>
I: Message-ID: <e4a483cb-1dfb-481d-903b-298c92c21f5e@mattingly.example.net>
I: MIME-Version: 1.0
I: MMHS-Primary-Precedence: 3
I: Subject: Meeting at my place
I: To: somebody@example.net
I: X-Mailer: Isode Harrier Web Server
I: Content-Type: text/plain; charset=us-ascii

   This is an important message that I don't want to be modified.

   --.cbe16d2a-e1a3-4220-b821-38348fc97237
   Content-Transfer-Encoding: base64
   content-type: application/pkcs7-signature

   [[base-64 encoded signature]]

   --.cbe16d2a-e1a3-4220-b821-38348fc97237--
```

4. Recommendations for handling of S/MIME protected header

[[This section needs more work. Don't treat anything in it as unchangeable.]]

For a signed-only message, it is RECOMMENDED that all "outer" header fields are copied into the "inner" protected body part. This would mean that all header fields are signed. In this case, the "outer" header fields simply match the protected header fields. And in the case that the "outer" header fields differ, they can simply be replaced with their protected versions when displayed to the user.

When generating encrypted or encrypted+signed S/MIME messages which protect header fields:

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 in the outer header section.

2. The outer header section SHOULD be minimal in order to avoid disclosure of confidential information. It is recommended that the outer header section only contains "Date" (set to the same value as in the inner header field, 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 section 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 typically only apply to non MIME header fields (header fields with names not starting with "Content-" prefix), but there are exception, e.g. Content-Language.

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

When displaying S/MIME messages which protect header fields (whether they are signed-only, encrypted or encrypted+signed):

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.

5. Mail User Agent Algorithm for deciding which version of a header field to display

[[TBD: describe how to recurse to find the innermost protected root body part, extract header fields from it and propogate them to the top level. This should also work for triple-wrapped messages.]]

6. Open Issues

[[This list should be empty before publication:]]

7. IANA Considerations

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

8. Security Considerations

This document talks about UI considerations, including security considerations, when processing 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.

9. References

9.1. 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>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

9.2. 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. Text on "Memory Hole" approach was taken from Daniel Kahn Gillmor's emails.

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