Message Authorizing Email Header Field and its use for Draft & Release
draft-melnikov-mmhs-authorizing-users-14

Abstract

   This document describes a procedure for when an Military Message
   Handling System (MMHS) message is composed by one user and is only
   released to the mail transfer system when one or more authorizing
   users authorize release of the message by adding the MMHS-
   Authorizing-Users header field. The resulting message can be
   optionally signed by the sender and/or reviewer, allowing recipients
   to verify both the original signature (if any) and review signatures.

Status of This Memo

Copyright Notice

the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.

Table of Contents

1. Introduction

In some secure environments email messages can't be released to the
MTS (Message Transfer System) and, thus delivered to recipients,
unless they are authorized by one or more authorizing users (e.g.
Releasing Officers or Release Authorities). This document describes
how this mechanism can be realized by an additional Internet Email
[RFC5322] header field and optionally protected using S/MIME
[RFC5750] [RFC5751] or DKIM [RFC6376].

This document describes a procedure for how an email message composed
by one user can be released to the MTS when one or more authorizing
users authorize and optionally countersign the message. The MMHS-
Authorizing-Users header field (see Section 4) communicates which
user(s) authorized the message. If S/MIME signed, the resulting
message allows recipients to verify both the original (if any) and
counter signatures. The original S/MIME signature generated by the
sender (if any) is unaffected by additional S/MIME review signatures.

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].

   The formal syntax uses the Augmented Backus-Naur Form (ABNF)
   [RFC5234] notation including the core rules defined in Appendix B of
   RFC 5234 [RFC5234]. Terms not defined in this document are taken
   from [RFC5322].

3. Draft and Release procedure

3.1. Terminology

   Drafter: Any email user that composes a message (Draft Message)
   needing authorisation before it is released to its intended
   recipients.

   Authorizing User (also Releaser or Authorizer): The mailbox of a user
   or a group of users that must inspect and authorise the release of
   Draft Message before it can be sent. An organization may require
   more than one Authorizing User to authorize release of a Draft
   Message.

3.2. Handling of Initial Message Submission by MSA

   The original email message to be sent doesn't include the MMHS-
   Authorizing-Users header field. It may or may not include sender's
   S/MIME signature.

   The message to be sent is first submitted over SMTP [RFC6409]. The
   specific mechanism for how it arrives to authorizing user(s) is not
   specified in this document. One possibility is for the Message
   Submission Agent (MSA) to redirect all email messages not addressed
   to authorizing users and not submitted by authorizing users to a
   preconfigured mailbox(es) that can be accessed by authorizing
   user(s). Another possibility is for the MSA to redirect all email
   messages without the MMHS-Authorizing-Users header field and/or
   corresponding S/MIME review signatures to a preconfigured mailbox(es)
   that can be accessed by authorizing user(s).

   In order to prevent a malicious sender from bypassing or altering
   Draft and Release procedure, MSA MUST check that MMHS-Authorizing-
   Users header field (if present) is syntactically valid, contains
   email addresses of entities authorized to act as authorizing users
   and, when review signatures are used, that every entity listed has
   one or more matching review signature (or signature) which is valid.

3.3. Review by Authorizing User(s)

   Each user agent that is used by an authorized user MUST perform the
   following steps (if there are multiple authorizing users, the whole
   sequence of steps below is repeated for each authorizing user):

   1. Verify the origination of the message (From/Sender header
       fields). The exact mechanism to do that is out of scope for this
       document, but one example is by verifying the S/MIME signature,
       making sure that the signature protects all header fields (i.e.
       wrapped by message/rfc822, as described in Section 3.1 of
       [RFC5751]) and that it matches the sender of the message, as
       described in [RFC5750]. Another example is by verifying a DKIM
       signature [RFC6376] (added by Drafter's MUA or MSA) that covers
       From/Sender header fields.

   2. Check if the message already contains the MMHS-Authorizing-Users
       header field with the email address of the authorizing user.
       (This can happen, for example, if email system is misconfigured
       and thus contains a loop, or if a malicious sender or attacker is
       trying to affect authorization procedure.) If the message
       doesn't contain the email address of the authorizing user in the
       MMHS-Authorizing-Users header field, then go to the next step.
       If MMHS-Authorizing-Users header field contains the email address
       of the authorizing user, verify validity of the header field (for
       example by checking for S/MIME signature/review signature or for
       DKIM signature) and also verify that the email address associated
       with the signature matches the email address of the authorizing
       user. If the validity of the MMHS-Authorizing-Users header field
       can be verified, go to step 5 below. Otherwise , return the
       message to sender (bounce) or redirect the message to a
       designated abuse mailbox.

   3. Allow the authorizing user to review content of the message.
       Some of the checks can be automated (for example search for
       keywords). (See Section 3.3.1 for additional considerations.)
       If based on the check the authorizing user is happy to release
       the message to MTS (or to the next authorizing user, if multiple
       authorizations are required), the UA SHOULD enable the
       authorizing user to protect additions to the MMHS-Authorizing-
       Users header field, for example by allowing to add S/MIME review
       signature (if S/MIME is used for protecting MMHS-Authorizing-
       Users header field. See Section 3.3.2 for more details). If the
       authorizing user wants to reject the message, it SHOULD be
       returned to drafter with an explanatory note or MAY be discarded.
       The authorizing user can also choose to forward the message to
       another authorizing user for additional approval or become a new
       Drafter of the message. If the authorizing user becomes the new

Drafter, its UA MUST strip any existing email addresses from the
MMHS-Authorizing-Users header field.

4. If there is an existing MMHS-Authorizing-Users header field
    containing the email address of the authorizing user, skip this
    step. Otherwise, insert a new MMHS-Authorizing-Users header
    field (if absent) containing the email address of the authorizing
    user or append the email address of the authorizing user to the
    end of the existing MMHS-Authorizing-Users header field.

5. The (possibly) updated email message is either released to the
    MTS, or to the next authorizing user, as per email system
    configuration. Note that if the authorizing user updates the
    message in a manner that invalidates existing S/MIME/DKIM
    signature(s), the authorizing user becomes the Drafter, and need
    to reapply any protections.

3.3.1. Processing of Encrypted Messages

Any encrypted message sent in an environment where Draft and Release
procedure is in force needs to be also encrypted to all authorizing
users, so that they can perform review of the message. If a User
Agent used by an authorizing user can't decrypt the message, it
SHOULD notify the sender (which can be the drafter or a previous
authorizing user) about the problem using a non delivery DSN or
through some other means. The ciphertext that cannot be decrypted by
the Authorizing User MAY be included in the notification to aid
debugging. A possible reason not to notify the sender is in order to
avoid Denial-of-Service attacks, for example if an attacker discovers
a way to inject fake messages with encryption that doesn't validate
in order to overflow sender's INBOX.

3.3.2. Authorizing S/MIME signatures

If S/MIME were not used, the Authorizing User can become the original
signer of the message.

If a message is signed with multiple signatures (for example using
different cryptographic algorithms, as described in [RFC5752]), all
of the signatures that can be verified by an authorizing user SHOULD
be signed with a review signature (authorizing signatures). A
recipient of the message can consider any chain of review signatures
that matches MMHS-Authorizing-Users header field values as valid,
only if all signatures in the chain verify. All of the signatures
that cannot be verified MUST be stripped by the Authorizing User
Agent.

When triple wrapping [RFC2634] is used, authorizing signatures are
applied to the outer level, so that it can be verified by MTAs
without the need to decrypt content.

3.4. Role of other Messaging Agents at the sender's domain

3.4.1. MDA at the sender's domain

If a message being sent is to be delivered within the sender's
domain, Message Delivery Agents (MDAs) are responsible for ensuring
that the message was properly authorized by authorizing user(s), as
determined by the sender's domain email system configuration. They
verify presence and validity of MMHS-Authorizing-Users header field
in the message, as well as validity of associated signatures on the
message.

Note that the above requirements don't apply to direct delivery to
any user designated as an Authorizing User.

3.4.2. Border MTA at the sender's domain

Sender's domain border MTAs are responsible for ensuring that all
messages that leave sender's domain were properly authorized by
authorizing user(s), as determined by the sender's domain email
system configuration. They verify presence and validity of MMHS-
Authorizing-Users header field in outgoing messages, as well as
validity of associated signatures on the message.

4. MMHS-Authorizing-Users header field

The MMHS-Authorizing-Users header field specifies the list of
authorizing users (or entities(*)) that countersigned this email
message (for example using S/MIME) before it was authorized for
release to MTS. Each user/entity is described by her/his/its email
address.

(*) Note that in some environments identities of authorizing users
are required to be hidden from recipients of email messages, so upon
receipt MMHS-Authorizing-Users might contain an email address
associated with a group of possible users. Such email addresses need
to have signatures that don't disclose group membership.

The MMHS-Authorizing-Users header field specified in this document
MUST NOT appear more than once in message headers. (An email message
that contains multiple MMHS-Authorizing-Users is malformed. An agent
processing such malformed message SHOULD either return it to sender
(if possible) or fix the message so that it only contains one copy of
the header field.)

```
     MMHS-Authorizing-Users = "MMHS-Authorizing-Users:"
                         mailbox-list CRLF

     mailbox-list = <Defined in RFC 5322>
```

5. Updated MIXER mapping

   This section provides an updated version of the MIXER mapping
   specified in [RFC2156] for MMHS applications.

5.1. Mapping from RFC 5322/MIME to X.400

   In the absence of the MMHS-Authorizing-Users header field, From and
   Sender header fields are mapped to their X.400 equivalents as
   specified in [RFC2156].

   If MMHS-Authorizing-Users header field is present:

   1. If the Sender header field is present, it is mapped to
       IPMS.Heading.originator, otherwise the first From header field
       address is mapped to IPMS.Heading.originator.

   2. Map the From header field address(es) and the MMHS-Authorizing-
       Users header field address(es) to IPMS.Heading.authorizing-users,
       skipping the first From header field address if it was mapped to
       IPMS.Heading.originator.

5.2. Mapping from X.400 to RFC 5322/MIME

   Mapping from X.400 to Internet is controlled by whether or not a
   particular message is considered to be a military message. A message
   is considered to be a military message (as defined by ACP 123
   [ACP123] and also specified in STANAG 4406 [STANAG-4406]) if there
   are any MMHS heading extensions present. Alternatively, this MAY be
   done by configuration (i.e. all messages can be considered to be
   military messages).

   For non military messages, mapping from X.400 as specified in
   [RFC2156] is used.

   For military messages, the following mapping is used:

   1. IPMS.Heading.originator is mapped to From header field.

   2. The IPMS.Heading.authorizing-users is mapped to MMHS-Authorizing-
       Users header field.

6. IANA Considerations

IANA is requested to add the MMHS-Authorizing-Users header field specified in Section 4 to the "Provisional Message Header Field Names", defined by Registration Procedures for Message Header Fields [RFC3864]. The registration template is as follows:

Header field name: MMHS-Authorizing-Users

Applicable protocol: mail ([RFC5322])

Status: provisional

Author/Change controller: Alexey Melnikov <alexey.melnikov@isode.com>

Specification document(s): [[RFC XXXX]]

Related information:

7. Security Considerations

In some military environments, the identities of authorizing users are required to be hidden from recipients of email messages. This can be accomplished by using a group address for the MMHS-Authorizing-Users. In this way, the recipient will know that it was released by an Authorizing User in that group, but the recipient will not know which one of them took the action.

For those organizations that wish to not disclose authorizing users' group membership, care must also be taken to ensure the information included in the certificate used for signing email messages does not disclose individuals in the group.

Further security considerations are described in subsections of this section.

7.1. Forged Header Fields

A malicious sender may add/change an MMHS-Authorizing-Users header field to bypass or alter the message authorization procedure invoked for messages with no MMHS-Authorizing-Users header field. For that reason it is important for agents and clients that rely on the validity of the MMHS-Authorizing-Users header field to also verify the review signature (or a similar protection mechanism), that confirms that a particular person or entity authorized release of a message.

7.2. Intentionally Malformed Header Fields

It is possible for an attacker to add an MMHS-Authorizing-Users
header field that is extraordinarily large or otherwise malformed in
an attempt to discover or exploit weaknesses in header field parsing
code. Implementations MUST thoroughly verify all such header fields
received from MTAs and be robust against intentionally as well as
unintentionally malformed header fields.

8. References

8.1. Normative References

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

[RFC2156]   Kille, S., "MIXER (Mime Internet X.400 Enhanced Relay):
            Mapping between X.400 and RFC 822/MIME", RFC 2156,
            DOI 10.17487/RFC2156, January 1998,
            <http://www.rfc-editor.org/info/rfc2156>.

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

[RFC6409]   Gellens, R. and J. Klensin, "Message Submission for Mail",
            STD 72, RFC 6409, DOI 10.17487/RFC6409, November 2011,
            <http://www.rfc-editor.org/info/rfc6409>.

[RFC5234]   Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax
            Specifications: ABNF", STD 68, RFC 5234,
            DOI 10.17487/RFC5234, January 2008,
            <http://www.rfc-editor.org/info/rfc5234>.

[RFC2634]   Hoffman, P., Ed., "Enhanced Security Services for S/MIME",
            RFC 2634, DOI 10.17487/RFC2634, June 1999,
            <http://www.rfc-editor.org/info/rfc2634>.

[RFC5750]   Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet
            Mail Extensions (S/MIME) Version 3.2 Certificate
            Handling", RFC 5750, DOI 10.17487/RFC5750, January 2010,
            <http://www.rfc-editor.org/info/rfc5750>.

[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, <http://www.rfc-editor.org/info/rfc5751>.

[RFC6376]   Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed.,
            "DomainKeys Identified Mail (DKIM) Signatures", STD 76,
            RFC 6376, DOI 10.17487/RFC6376, September 2011,
            <http://www.rfc-editor.org/info/rfc6376>.

[ACP123]   "Common Messaging strategy and procedures", ACP 123(B),
            May 2009.

8.2. Informative References

[RFC3864]   Klyne, G., Nottingham, M., and J. Mogul, "Registration
            Procedures for Message Header Fields", BCP 90, RFC 3864,
            DOI 10.17487/RFC3864, September 2004,
            <http://www.rfc-editor.org/info/rfc3864>.

[STANAG-4406]
            "STANAG 4406 Edition 2: Military Message Handling System",
            STANAG 4406 Ed. 2, March 2005.

[I-D.melnikov-smime-msa-to-mda]
            Ottaway, W. and A. Melnikov, "Domain-based signing and
            encryption using S/MIME", draft-melnikov-smime-msa-to-
            mda-04 (work in progress), March 2014.

[RFC5752]   Turner, S. and J. Schaad, "Multiple Signatures in
            Cryptographic Message Syntax (CMS)", RFC 5752,
            DOI 10.17487/RFC5752, January 2010,
            <http://www.rfc-editor.org/info/rfc5752>.

Appendix A. Acknowledgements

   Many thanks for reviews and text provided by Steve Kille, Jim Schaad,
   Russ Housley, David Wilson, Chris Bonatti and Sean Turner.

   Some text in this document was copied from RFC 7001.

Author's Address

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

   EMail: Alexey.Melnikov@isode.com