Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 5, 2015

A. Melnikov
Isode Ltd

July 4, 2014

Draft and Release using Internet Email
draft-melnikov-mmhs-authorizing-users-06

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

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 http://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 January 5, 2015.

Table of Contents

1. Introduction

In some secure environments email messages can't be released to the MTS (Mail 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 header communicates which users authorized the message. If signed, the resulting message allows recipients to verify both the original (if any) and counter S/MIME signatures. The list of authorizing users is specified in the MMHS-Authorizing-Users header field Section 4. The original S/MIME signature generated by the sender (if any) should be 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. 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 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 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.

3.2. 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, these steps are repeated for each):

1. Verify the origination of the message. The exact mechanism to do that is out of scope for this document, but one example is by verifying the S/MIME signature and making sure that it matches the sender of the message, as described in [RFC5750] [RFC5751].

Another example is by verifying a DKIM signature [RFC6376] 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 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). If the validity of the MMHS-Authorizing-Users header field can be verified, go to step 5 below. Otherwise strip the MMHS-Authorizing-Users header field or return the message to sender (bounce).

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 3.2.1 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 3.2.2 for more details). If the authorizing user wants to block the message, it can be discarded or returned to sender. The authorizing user can also choose to forward the message to another authorizing user for approval.

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.

3.2.1. 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. A message

that can't be decrypted by an authorizing user MUST be returned to sender.

3.2.2. Authorizing S/MIME signatures

If a message is signed multiple times (for example using different cryptographic algorithms), 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 should consider any chain of review signatures that matches MMHS-Authorizing-Users header field values as valid, only if all signatures in the chain verify.

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.

3.3. Role of other Messaging Agents

3.3.1. 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.

3.3.2. 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.

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.

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.) [[An alternative is to allow for multiple copies of the header field and treat them as additive. This might work better with DKIM!]]

```
MMHS-Authorizing-Users = "MMHS-Authorizing-Users:"
                  [FWS] mailbox-list [FWS] CRLF

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

5. Updated MIXER mapping

This section updates MIXER mapping specified in [RFC2156].

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. The first From header field address is mapped to IPMS.Heading.originator if there is no Sender header field and the remaining From header field addresses + the MMHS-Authorizing-Users header field address(es) are mapped to IPMS.Heading.authorizing-users. If a Sender header field is present, the From header field address(es) and the MMHS-Authorizing-Users header field address(es) are mapped to IPMS.Heading.authorizing-users.

2. The Sender header field (if present) is 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 "Permanent 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: Standard

Author/Change controller: IETF

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

Related information:

7. Security Considerations

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. Open Issues

Netnews Approved header field has the same syntax and semantics as the one described here. Should it be used (and be formally registered for email) instead?

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2156] Kille, S., "MIXER (Mime Internet X.400 Enhanced Relay): Mapping between X.400 and RFC 822/MIME", RFC 2156, January 1998.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, October 2008.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, October 2008.

[RFC6409] Gellens, R. and J. Klensin, "Message Submission for Mail", STD 72, RFC 6409, November 2011.

[RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, September 2009.

[RFC2634] Hoffman, P., "Enhanced Security Services for S/MIME", RFC 2634, June 1999.

[RFC5750] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Certificate Handling", RFC 5750, January 2010.

[RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, January 2010.

[RFC6376] Crocker, D., Hansen, T., and M. Kucherawy, "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, September 2011.

[ACP123] CCEB, , "Common Messaging strategy and procedures", ACP 123, May 2009.

9.2. Informative References

[RFC3864] Klyne, G., Nottingham, M., and J. Mogul, "Registration Procedures for Message Header Fields", BCP 90, RFC 3864, September 2004.

[STANAG-4406] NATO, , "STANAG 4406 Edition 2: Military Message Handling System", STANAG 4406, 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.

Appendix A. Acknowledgements

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

Some text in this document was copied from RFC 7001.

Author's Address

Alexey Melnikov
Isode Ltd
5 Castle Business Village
36 Station Road
Hampton, Middlesex TW12 2BX
UK

EMail: Alexey.Melnikov@isode.com