MSP BOF
Internet Draft
expires in six months

J. W. Nicolls (NSA)
R. Housley (SPYRUS)
February 1996

MIME with the Message Security Protocol

<draft-housley-msp-mime-00.txt>

Status of this Memo

Abstract

This is the first draft of the MIME with the Message Security Protocol (MSP) specification. This document defines the conventions for using MIME and MSP together. For the most part, this specification is not controvercial. However, there is significant debate about signed only MSP contents. Some people think that Multipart/alternative is best, and other people think that Multipart/mixed is best. The MSP BOF will meet at the March 1996 IETF meeting to discuss this open issue. The intent of this document is to generate productive discussion and build concensus.

Table Of Contents

1. Introduction
2. Content-Type application/msp
3. MSP Content
3.1. Protected MIME Message Format

3.2. Optional Protected MIME Message Header Fields
4. MIME with MSP Header
4.1. Content Type multipart/mixed
4.2. Optional MIME with MSP Message Header Fields
4.3. Preamble
4.4. Epilogue
5. Forwarding MIME with MSP Messages
6. MIME with MSP Signed Receipt Message Format
7. Example Protected Messages
8. Summary
9. References
10. Security Considerations
11. Author Addresses

1 Introduction

Message Security Protocol (MSP) is a electronic mail security protocol which operates between the originator and recipients of messages. As an end-user-to-end-user protocol which does not involve the intermediate message transfer system, MSP provides writer-to-reader security. The security services provided by this protocol include: confidentiality, data origin authentication, integrity, and access control, non-repudiation with proof of origin (message signature), and non-repudiation with proof of delivery (signed receipts). The MSP is independent of the cryptographic algorithms used for encryption, hash, and signature.

MSP operates by performing security operations on messages at the originator and recipients' mail applications. These functions are performed in an independent but consistent fashion at each end of the message exchange based on user security information. This security information includes the user's identity, authorizations, and cryptographic material. MSP processing includes both per-message operations and information and per-recipient operations and information. These operations involve the parsing and generation of elements of the MSP heading based on the services requested by the originator, and the encryption, when requested, of the message content.

This specification pertains only to the encapsulation of MSP protected MIME messages within the MIME environment. No changes are necessary to the MIME syntax or semantics.

2 Content-Type application/msp

This section defines the format of data used in application/msp. For the MIME with MSP body, the "application" Content-Type value and the "msp" subtype value are used.

The "application/msp" Content-Type is specified as follows:

```
application-type := "application" "/" application-subtype

application-subtype := "msp-" 1*DIGIT "." 1*DIGIT crypto-param

crypto-param := (";" "crypto=" security-applied)
        ; case-insensitive

security-applied := "signed" / "signed&encrypted" / "encrypted"
        ; all values case-insensitive
```

Messages composed in accordance with this document must set the msp value to "1.0".

A Content-Transfer-Encoding field is used to indicate the type of transformation that has been used in order to represent the MSP protected message in an acceptable manner for transport. The application must always use the Base64 encoding mechanism to encode the MSP.

3 MSP Content

The MSP content is an ASN.1 encoded structure as defined in SDN.701 which has been converted to ASCII as specified by the content transfer encoding field.

<< At some future date, SDN.701 be converted to an RFC. >>

3.1 Protected MIME Message Format

The encapsulated content of the MSP must be a MIME compliant message. The encapsulated content must include an RFC 822 optional-, user-defined-field, used as an extension to indicate the security classification of the MSP protected message. The security classification field can be set by the user to the security clearance values set in the user's certificate.

```
user-defined-field := "X-Classification" ":" security-classification
        ; case-insensitive
        ; "Sensitivity-Label" should be handled as equivalent
        ;    to "Classification"
```

```
security-classification := "unclassified" / "confidential" / "secret"
        / "top-secret" / "unclassified-but-sensitive"
```

3.2 Optional Protected MIME Message Header Fields

Users may wish to be able to add other optional extension fields for displaying information to the recipient (i.e. trusted-time from a hardware token). All extensions must use the "X-" format.

Examples:

```
user-defined-field := "X-Trusted-Time" ":" date-time "Z"
        ; case-insensitive

date-time := year ; month ; day ; hour; minutes ; seconds

year := 4*DIGIT

month := 2*DIGIT

day := 2*DIGIT

hour := 2*DIGIT

minutes := 2*DIGIT

seconds := 2*DIGIT
```

4 MIME with MSP Header

4.1 Content Type multipart/mixed

For the MIME with MSP header, the "multipart" Content-Type value and the "mixed" subtype value are used.

If the security applied has the encrypted option set then only the application/msp body part is present. If the security applied is signed-only then the body may contain a plaintext version of the message (and attached files) being sent. This is an option that may be user-selectable. The application/msp body part must be the last body part. The simplest Content-Type value for a plaintext only version would be the text Content-Type using the ASCII character set while another multipart body part could be used for text and attachments.

4.2 Optional MIME with MSP Message Header Fields

Users may wish to add other optional extension fields to the header for displaying information to the recipient (i.e., classification). All extensions must use the "X-" format.

Example:

```
user-defined-field := "X-Classification" ":" security-classification
        ";" "Untrusted"
        ; case-insensitive
        ; "Sensitivity-Label" should be handled as equivalent
        ;    to "Classification"

security-classification := "unclassified" / "confidential" / "secret"
        / "top-secret" / "unclassified-but-sensitive"
        ; all values case-insensitive
```

Note: when a security related header line such as classification is placed outside the MSP content, the end of the header line must contain a comment indicating the information is untrusted (i.e., X-Classification: unclassified-but-sensitive; untrusted).

4.3 Preamble

The preamble area of a multipart message is the area immediately after the first blank line following the header and preceding the initial boundary indicated by the "--unique-boundary". In this area the MIME specific message header information is duplicated with a "X-" prepended. The two header lines. The preamble lines should be in the order shown below.

```
X-MIME-Version: 1.0 X-Content-Type: multipart/mixed;
boundary="unique-boundary"
```

Processing Note:

Mail applications which receive a message must check the header first and then, if no valid MIME with MSP header lines are present, check the body (preamble) to determine if a valid MSP protected message is present. Since gateways do not modify messages in a uniform manner, the "blank line" and the two "X-" lines may not be immediately adjacent to the header. The receiving mail application may need to flexible enough to check as many as five lines of the message for an MSP preamble after the header. Note also that checking too many lines into a message may result in falsely identifying a message as MSP protected when it is in fact a plain SMTP message forwarding an MSP protected message or an MSP protected message rejected by a post

office.

Once a received MSP protected message is processed, the mail application may strip out the preamble if it is no longer needed for subsequent message processing.

4.4 Epilogue

This area of a multipart message is not used for MIME with MSP messages.

5 Forwarding MIME with MSP Messages

Forwarding of messages is a standard part of electronic mail, and forwarding of signed messages provides the ability to establish the identity of the original originator to a third party. A MSP enabled mail application should support forwarding of MIME with MSP messages. SDN.701 states that "any number of forwarded MSP messages may be conveyed within a new message" and "forwarded MSP messages may be nested within one another". Forwarded MIME with MSP messages shall be included as a separate "message/rfc822" Content-Type. A mail application must look for the MIME with MSP header or preamble format within each "message/rfc822" body part for the indication of a forwarded MIME with MSP message both within each received non-MSP message and within each MSP verified protected message. Forwarded signed messages which have a correct MIME header do not have to contain the duplicate MIME header lines in the preamble. In the case of a signed message with a forwarded signed message, it is not recommended that a plaintext version of the forwarded signed message be repeated in the message.

6 MIME with MSP Signed Receipt Message Format

A signed receipt is generated by a MSP enabled mail application when the MSP ReceiptsIndicator is set by the originator to indicate that the recipient should return a signed receipt. In addition to the MSP ReceiptInformation included in a signed receipt sent by a recipient in response to the originator's request, the original message protected header date, subject and SMTP message-id, and the following statement must also be included in the MSP encapsulated content. The message body may contain a plaintext version of the protected message.

> "This signed receipt confirms that the original message identified above was received and cryptographically verified by the recipient. This signed receipt along with the original message may be used to prove delivery of the original message to the recipient who signed this receipt."

7 Example MIME with MSP Messages

The following are examples of MIME with MSP messages. Examples 1 and 2 illustrate messages which has been signed and encrypted. Examples 3, 4, and 5 illustrate messages which have been signed only. The plaintext message is carried in Examples 3 to allow non-MSP enabled recipients to read the original message without validating the signature. Example 5 shows a SMTP header with MIME body message. Example 6 shows a signed forwarded signed message. Example 7 shows a signed receipt message. Additional MIME message examples can be found in RFC 1521.

Example 1: MIME with MSP Signed and Encrypted Message

```
Date: Whenever
From: Whomever
To: Someone
Subject: Whatever
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="example1-unique-boundary"

X-MIME-Version: 1.0
X-Content-Type: multipart/mixed; boundary="example1-unique-boundary"
--example1-unique-boundary
Content-Type: application/msp-1.0; crypto=signed&encrypted
Content-Transfer-Encoding: Base64

   ASN.1 Encoded MSP Message
   MSP Security Header as Defined in SDN.701
   [Encapsulated Content - Start]
   Date: Whenever
   From: Whomever
   To: Someone
   Subject: Whatever
   MIME-Version: 1.0
   X-Classification: Unclassified
   Content-Type: text/plain

   This is the sensitive message.
   Please reply today.
   Bob.

   [Encapsulated Content - End]

--example1-unique-boundary--
```

Example 2: MIME with MSP Signed and Encrypted Message with File Inclusion

```
Date: Whenever
From: Whomever
To: Someone
Subject: Whatever
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="example2-unique-boundary"

X-MIME-Version: 1.0
X-Content-Type: multipart/mixed; boundary="example2-unique-boundary"
--example2-unique-boundary
Content-Type: application/msp-1.0; crypto=signed&encrypted
Content-Transfer-Encoding: Base64

   ASN.1 Encoded MSP Message
   MSP Security Header as Defined in SDN.701
   [Encapsulated Content - Start]
   Date: Whenever
   From: Whomever
   To: Someone
   Subject: Whatever
   MIME-Version: 1.0
   X-Classification: Unclassified
   Content-Type: multipart/mixed; boundary="example2-inner-boundary"

   --example2-inner-boundary
   Content-Type: text/plain

   This is the sensitive message.
   Please reply today.
   Bob.

   -- example2-inner-boundary
   Content-Type: application/octet-stream
   Content-Transfer-Encoding: Base64

   Base 64 Encoded File Attachment

   -- example2-inner-boundary--

   [Encapsulated Content - End]

--example2-unique-boundary--
```

Example 3: MIME with MSP Signed Message with Duplicate Text

```
Date: Whenever
From: Whomever
To: Someone
Subject: Whatever
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="example3-unique-boundary"

X-MIME-Version: 1.0
X- Content-Type: multipart/mixed; boundary="example3-unique-boundary"
--example3-unique-boundary
Content-Type: text/plain

This is the message.
Bob

--example3-unique-boundary
Content-Type: application/msp-1.0; crypto=signed
Content-Transfer-Encoding: Base64

   ASN.1 Encoded MSP Message
   MSP Security Header as Defined in SDN.701
   [Encapsulated Content - Start]
   Date: Whenever
   From: Whomever
   To: Someone
   Subject: Whatever
   MIME-Version: 1.0
   X-Classification: Unclassified
   Content-Type: text/plain

   This is the message.
   Bob.

   [Encapsulated Content - End]

--example3-unique-boundary--
```

Example 4: MIME with MSP Signed Message

```
Date: Whenever
From: Whomever
To: Someone
Subject: Whatever
MIME-Version: 1.0
```

```
Content-Type: multipart/mixed; boundary="example4-unique-boundary"

X-MIME-Version: 1.0
X-Content-Type: multipart/mixed; boundary="example4-unique-boundary"
--example4-unique-boundary
Content-Type: application/msp-1.0; crypto=signed
Content-Transfer-Encoding: Base64

   ASN.1 Encoded MSP Message
   MSP Security Header as Defined in SDN.701
   [Encapsulated Content - Start]
   Date: Whenever
   From: Whomever
   To: Someone
   Subject: Whatever
   MIME-Version: 1.0
   X-Classification: Unclassified
   Content-Type: text/plain

   This is the message.
   Please reply today.
   Bob.

   [Encapsulated Content - End]

--example4-unique-boundary--
```

Example 5: Mixed SMTP and MIME with MSP Signed Message with File Inclusion

```
Date: Whenever
From: Whomever
To: Someone
Subject: Whatever

X-MIME-Version: 1.0
X-Content-Type: multipart/mixed; boundary="example5-unique-boundary"
--example5-unique-boundary
Content-Type: application/msp-1.0; crypto=signed
Content-Transfer-Encoding: Base64

   ASN.1 Encoded MSP Message
   MSP Security Header as Defined in SDN.701
   [Encapsulated Content - Start]
   Date: Whenever
   From: Whomever
```

```
      To: Someone
      Subject: Whatever
      MIME-Version: 1.0
      X-Classification: Unclassified
      Content-Type: multipart/mixed; boundary="example5-inner-boundary"

      --example5-inner-boundary
      Content-Type: text/plain

      This is the message.
      Please reply today.
      Bob.

      --example5-inner-boundary
      Content-Type: application/octet-stream
      Content-Transfer-Encoding: Uuencode

      [Uuencoded File Attachment]

      --example5-inner-boundary--

      [Encapsulated Content - End]

   --example5-unique-boundary--
```

Example 6: MIME with MSP Signed Message with Forwarded Signed Message

```
   Date: Whenever
   From: Whomever
   To: Someone
   Subject: Whatever
   MIME-Version: 1.0
   Content-Type: multipart/mixed; boundary="example6-unique-boundary"

   X-MIME-Version: 1.0
   X-Content-Type: multipart/mixed; boundary="example6-unique-boundary"
   --example6-unique-boundary
   Content-Type: application/msp-1.0; crypto=signed
   Content-Transfer-Encoding: Base64

      ASN.1 Encoded MSP Message
      MSP Security Header as Defined in SDN.701
      [Encapsulated Content - Start (Outer)]
      Date: Whenever
      From: Whomever
```

```
To: Someone
Subject: FWD: Whatever
MIME-Version: 1.0
X-Classification: Unclassified
Content-Type: multipart/mixed; boundary="example6-inner-boundary"

--example6-inner-boundary
Content-Type: text/plain

I have forwarded the message to you.
Please reply today.
Bob.

--example6-inner-boundary
Content-Type: message/rfc822

Date: Whenever
From: Whomever
To: Someone
Subject: Whatever
MIME-Version: 1.0
X-Classification: Unclassified
Content-Type: multipart/mixed; boundary="example6-fwd-boundary"

--example6-fwd-boundary
Content-Type: application/msp-1.0; crypto=signed
Content-Transfer-Encoding: Base64

   ASN.1 Encoded MSP Message
   MSP Security Header as Defined in SDN.701
   [Encapsulated Content - Start (Forward)]
   Date: Whenever
   From: Whomever
   To: Someone
   Subject: Whatever
   MIME-Version: 1.0
   X-Classification: Unclassified
   Content-Type: text/plain

   This is the forwarded message.
   Bob.

  [Encapsulated Content - End (Forward)]

--example6-fwd-boundary--

[Encapsulated Content - End (Outer)]
```

```
--example6-unique-boundary--
```

Example 7: MIME with MSP Signed Receipt Message

```
Date: Whenever
From: Whomever
To: Someone
Subject: MSP Signed Receipt <Original Message Subject>
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="example7-unique-boundary"

X-MIME-Version: 1.0
X-Content-Type: multipart/mixed; boundary="example7-unique-boundary"
--example7-unique-boundary
Content-Type: application/msp-1.0; crypto=signed
Content-Transfer-Encoding: Base64

   ASN.1 Encoded MSP Message
   MSP Security Header as Defined in SDN.701
   [Encapsulated Content - Start]
   Date: Whenever
   From: Receipt Generator
   To: Receipt Requester
   Subject: MSP Signed Receipt <Original Message Subject>
   MIME-Version: 1.0
   X-Classification: Unclassified
   Content-Type: text/plain

   Original-Message-Subject: Whatever
   Original-Message-Date: Whenever
   Original-Message-ID: 123-45-6789

   This signed receipt confirms that the original message identified
   above was received and cryptographically verified by the
   recipient.This signed receipt along with the original message may
   be used to prove delivery of the original message to the recipient
   who signed this receipt.

   [Encapsulated Content - End]

--example7-unique-boundary--
```

8 Summary

<< Write this last. >>

9 References

[RFC 822] Crocker, D., "Standard For The Format of ARPA Internet Text Messages", STD 11, RFC 822, UDEL, August 1982.

[RFC 1521] Borenstein, N. and N. Freed, "Multipurpose Internet Extensions (MIME) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies", Bellcore, September 1993.

[SDN.701] National Security Agency, "Message Security Protocol", Specification SDN.701, Revision 3.0, March 1994. { ftp://ftp.netcom.com/pub/sp/spyrus/sdn701.ps }

10 Security Considerations

This whole document deals with security. It specifies the conventions for using MSP with MIME.

11 Author Addresses

J. Weston Nicolls
National Security Agency
Attn: X22
9800 Savage Rd
Ft Meade, MD 20755-6000
USA
jwnicol@missi.ncsc.mil

Russell Housley
SPYRUS
PO Box 1198
Herndon, VA 22070
USA
housley@spyrus.com