S/MIME Working Group
Internet Draft
expires in six months

R. Housley
RSA Laboratories

August 2001

Intended Recipients Attribute for the Cryptographic Message Syntax (CMS)

<draft-ietf-smime-ira-00.txt>

Status of this Memo

Abstract

This document describes the intended recipients attribute for use with the Cryptographic Message Syntax (CMS) [CMS]. The intended recipients attribute can be used as a signed attribute or as an authenticated attribute.

This draft is being discussed on the "ietf-smime" mailing list. To join the list, send a message to <ietf-smime-request@imc.org> with the single word "subscribe" in the body of the message. Also, there is a Web site for the mailing list at <http://www.imc.org/ietf-smime/>.

1 Introduction

Don Davis has demonstrated that recipients of signed and encrypted messages can decrypt the message, preserving the original signature, then resend the message to a new recipient [MALFWD]. The new

recipient may act inappropriately based on the fact that they received a message signed by the originator.

Consider this illustrative example:

> Bob wants to have dinner with Alice. He writes a note, "Meet me at the Iron Gate at 7:00 tonight", signs it, encrypts it for Alice, and sends it to Alice.
>
> Alice the decrypts the message, validates the signature, and reads the message. She does not want to have dinner with Bob tonight, so for fun Alice encrypts the signed message for Carol, and sends it to Carol.
>
> Carol the decrypts the message, validates the signature, and reads the message.
>
> Carol and Bob meet for dinner.

The problem is that Bob did not state the intended recipient in his message. Simply saying, "Alice, please meet me at the Iron Gate at 7:00 tonight," would have fixed the problem.

In many situations, the signed message will provide adequate indication of the intended recipients to avoid malicious forwarding of signed content. For example, a Purchase Order includes information about the supplier and the purchaser.

The intended recipients attribute is being defined to protect against malicious forwarding when the message content does not inherently provide a clear indication of the intended recipients. Further, the intended recipients attribute can protect an originator of an interpersonal message in face of name collisions and typographical error. Suppose that Alice begins her message with "Dear Bill." Such a message is susceptible to forwarding to other recipients named Bill. Further, if Alice made an simple typographic error and intended to begin here message with "Dear Will," then Will (the intended recipient) is unsure if Alice meant to send him the message, and the message is easily forwarded to a person named Bill.

The problem of intent that as expressed in [MALFWD] is beyond the control of S/MIME protocol or its implementers. The use of the digital signatures and encryption is correctly in the hands of the user. However, the intended recipients attribute offers a mechanism to reduce the likelihood of undetected malicious forwarding.

2 Terminology

In this document, the key words MUST, MUST NOT, REQUIRED, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL are to be interpreted as described by Scott Bradner in [STDWORDS].

3 Intended Recipients Attribute Syntax

The intended-recipients attribute type specifies the list of recipients that the message originator intended to receive the message. It includes the members of the TO list and the CC list. However, members of the BCC list are not included. Including members of the BCC list would disclose the membership to the other recipients.

The intended-recipients attribute MUST be a signed attribute or an authenticated attribute; it MUST NOT be an unsigned attribute or unauthenticated attribute.

In the triple wrapper model described in RFC 2634 [ESS], the intended-recipients attribute MUST only appear in the inner signature.

The following object identifier identifies the intended-recipients attribute:

```
id-aa-intendedRecipients OBJECT IDENTIFIER ::=
    { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
      pkcs-9(9) smime(16) aa(2) 33 }
```

The intended-recipients attribute values have ASN.1 type GeneralNames. GeneralNames is specified in [PROFILE], but the definition is repeated here for reader convenience:

```
GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName

GeneralName ::= CHOICE {
   otherName                   [0] OtherName,
   rfc822Name                  [1] IA5String,
   dNSName                     [2] IA5String,
   x400Address                 [3] ORAddress,
   directoryName               [4] Name,
   ediPartyName                [5] EDIPartyName,
   uniformResourceIdentifier   [6] IA5String,
   iPAddress                   [7] OCTET STRING,
   registeredID                [8] OBJECT IDENTIFIER}

OtherName ::= SEQUENCE {
```

```
        type-id       OBJECT IDENTIFIER,
        value     [0] EXPLICIT ANY DEFINED BY type-id }

     EDIPartyName ::= SEQUENCE {
        nameAssigner   [0] DirectoryString OPTIONAL,
        partyName      [1] DirectoryString }
```

An intended-recipients attribute MUST have a single attribute value, even though the syntax is defined as a SET OF AttributeValue.

The SignedAttributes and AuthAttributes syntaxes are each defined as a SET OF Attributes. The SignedAttributes in a signerInfo MUST NOT include multiple instances of the intended-recipients attribute. Similarly, the AuthAttributes in an AuthenticatedData MUST NOT include multiple instances of the intended-recipients attribute.

One GeneralName MUST appear in the SEQUENCE for each intended recipient. The order of the names is not important. (A SEQUENCE is used instead of a SET to avoid the sorting associated with the distinguished encoding rules (DER) processing of SETs.)

When used with S/MIME [MSG], the rfc822Name form of the recipient name SHOULD be used. The other forms of the recipient name are permitted since the CMS is used in other protocols as well as S/MIME.

3.1 Originator Generation

Inclusion of the intended-recipients attribute is OPTIONAL. When a message content is signed but not encrypted, inclusion of the intended-recipients attribute may be counter to the originator's goal. For example, when a press release is posted wide distribution is intended. In such cases, inclusion of the intended-recipients attribute is undesirable.

Originator generation of the intended-recipients attribute is simple and straightforward. Each TO list and CC list recipient is represented by on GeneralName in the SEQUENCE. Most of the time, the rfc822Name form of the recipient name is used.

3.2 Recipient Validation

Recipient validation of the intended-recipients attribute is less straightforward than generation of the intended-recipients attribute. When a recipient receives the message as a member of a mail list or as a BCC list recipient, they will not be listed in the intended-recipients attribute, yet the originator does intend that this recipient receive the message content.

In the normal case, the recipient will locate their own name in the intended-recipients attribute. That is, no malicious forwarding is detected.

If the received message includes a mlExpansionHistory attribute, then the recipient can presume that the message was received as a normal part of mail list distribution. A particularly paranoid implementation MAY confirm membership in at least one of the mail lists named in the intended-recipients attribute.

Unfortunately, the BCC case is indistinguishable from malicious forwarding. Therefore, any display presented to a human user as a result of the recipient name not being on listed on the intended-recipient attribute SHOULD point out this possibility.

4 References

CMS Housley, R. Cryptographic Message Syntax. RFC <TBD>. <Date>. {draft-ietf-smime-rfc2630bis-*.txt}

ESS Hoffman, P., Editor. Enhanced Security Services for S/MIME. RFC 2634. June 1999.

MALFWD Davis, D. Sender Authentication and the Surreptitious Forwarding Attack in CMS and S/MIME. RFC <TBD>. <Date>. {draft-ietf-smime-<tbd>-*.txt}

MSG Ramsdell, B., Editor. S/MIME Version 3 Message Specification. RFC 2633. June 1999.

PROFILE Housley, R., W. Ford, W. Polk, and D. Solo. Internet X.509 Public Key Infrastructure: Certificate and CRL Profile. RFC 2459. January 1999.

STDWORDS Bradner, S. Key Words for Use in RFCs to Indicate Requirement Levels. RFC 2119. March 1997.

5 Security Considerations

This whole document is about a mechanism to detect the malicious forwarding of signed content [MALFWD]. The protections offered by the intended-recipients attribute are necessary when the signed content does not inherently provide an indication of the recipients that the signer intended to receive the content.

6 Acknowledgments

I extend a special thanks to Don Davis and Burt Kaliski for their efforts and support.

7 Author Address

Russell Housley
RSA Laboratories
918 Spring Knoll Drive
Herndon, VA 20170
USA

rhousley@rsasecurity.com

Full Copyright Statement