MSEC WG
Internet-Draft
Expires: July 25, 2005

D. Ignjatic
L. Dondeti
Nortel Networks
January 21, 2005

An additional mode of key distribution in MIKEY
draft-ignjatic-msec-mikey-rsa-r-00

Status of this Memo

Copyright Notice

Abstract

The MIKEY specification [2] describes several modes of key distribution to setup SRTP [4] sessions, viz., pre-shared key, public-key, and an optional Diffie-Hellman key exchange. In the public-key mode the initiator encrypts a random key with the responder's public key and sends it to the responder. In many VoIP calling scenarios, the initiator may not know the responder's public

key or in some cases the responder's ID (e.g., call forwarding) in advance. We propose a new MIKEY mode that works well in such scenarios.

Conventions Used In This Document

This document recommends, as policy, what specifications for Internet protocols -- and, in particular, IETF standards track protocol documents -- should include as normative language within them. The capitalized keywords "SHOULD", "MUST", "REQUIRED", etc. are used in the sense of how they would be used within other documents with the meanings as specified in BCP 14, RFC 2119 [1].

Table of Contents

1. Revision History 3
2. Problem description 3
2.1 Motivation 3
3. Solution Outline 4
3.1 Impact of the receiver choosing the TGK 4
4. A new MIKEY RSA mode 5
5. Some specific additions to RFC 3830 6
6. Conclusion 6
7. Security Considerations 6
8. IANA Considerations 7
9. Acknowledgments 7
10. References 7
10.1 Normative References 7
10.2 Informative References 7
Authors' Addresses 8
Intellectual Property and Copyright Statements 9

1. Revision History

1. **00 Initial proposal to invite discussion on the problem and the** proposal.

2. Problem description

The MIKEY protocol (RFC 3830) has several three different methods for key transport or exchange: a pre-shared key mode (PSK), a public-key (RSA) mode and finally an optional Diffie-Hellman exchange (DHE) mode. The primary motivation in the design is efficiency and thus all the exchanges finish in .5 to 1 round-trips. The PSK mode might not scale to large deployments and the RFC includes a mechanism to bootstrap the PSK mode with the RSA mode. The DH mode is optional for various reasons, including because it does not support key download, as defined.

The RSA mode while efficient, raises some deployment issues. In this mode, the Initiator selects a TEK Generation Key (TGK), encrypts and authenticates it with an envelope key and sends it to the Responder, as part of the first message, viz., I_MESSAGE. The Initiator also includes the envelope key, encrypted with the Responder's public key, in the same message.

I_MESSAGE is replay protected with timestamps, and signed with the Initiator's public key. The Initiator's ID, CERT and the responder's ID that the Initiator intends to talk may be included in I_MESSAGE. If the Initiator knows several public-keys of the Responder, it can indicate the key used in a CHASH payload. However, there is no provision in MIKEY for the Initiator to initiate key download/establishment if it is unaware of the Responder's public key.

2.1 Motivation

In many VoIP call scenarios, the Initiator may not have the Responder's public key handy. A possible solution might be to provision the Initiator with a mechanism and parameters (e.g., address of another entity) necessary to lookup any potential end-point. However, note that it might not be feasible for all deployments.

Furthermore, in some cases, the Initiator might not even know the correct ID of the responder. For instance the Responder might have several IDs and phone numbers, and the Initiator might be willing to let the other party establish identity and prove it via an Initiator-trusted third party (e.g., CA).

3. Solution Outline

The proposed solution is fairly simple and requires only 1 round trip. Suppose the Initiator does not have access to the Responder's cert. We propose that the Initiator send a signed message to the intended Responder requesting the Responder to send the SRTP keying material. In this case I_MESSAGE would include the Initiator's CERT, and the responder can include its CERT in the R_MESSAGE. The Responder can use the Initiator's public key from the CERT in the I_MESSAGE to send the encrypted TGK in the R_MESSAGE. Upon receiving the R_MESSAGE, the Initiator can use the CERT in the R_MESSAGE to verify whether the Responder is in fact the party that it wants to communicate to.

3.1 Impact of the receiver choosing the TGK

In MIKEY RSA or PSK modes, the Initiator chooses the TGK and the responder has the option to accept the key or not. The primary consideration for the Responder might be to verify whether the key is a known weak key (Q: Is this an issue with AES-CM or AES-f8 TBD). Other than that who chooses the key has no impact on SRTP (verify this).

Thus, in case of one-to-one VoIP calls, there is no impact on the functionality provided by the MIKEY RSA mode and our modified mode being outlined earlier. Whereas MIKEY RSA mode allows R_MESSAGE to be optional, in the new mode, it is required. However, as noted earlier, the new mode allows simpler provisioning at the VoIP entity.

More interestingly, the proposed mode supports group conferencing as well. First, it is clear that this mode requires that the Responder select the TGK and supply to the Initiator. Notice that this is quite similar to group key download as specified in GDOI [2], GSAKMP, and GKDP protocols (also see [5]. The catch however is that the participating entities must know that they need to contact a well-known address as far as that conferencing group is concerned. Note that they only need the Responder's ID, not necessarily its CERT. If the group members have the Responder's CERT, there is no harm; they simply do not need the CERT to compose I_MESSAGE.

At the time of this writing, the authors' opinion is that this mode may not easily support 3-way calling, under the assumptions that motivated the design. Simply put, an extra message may be required compared to the original RSA mode specified in RFC 3830. Consider that A wants to talk to B and C, but does not have B's or C's CERT. A might contact B and request that B supply a key for a 3-way call. Now if B knows C's CERT, then B can simply use the MIKEY RSA mode (as defined in RFC 3830) to send the TGK to C. If not, then the solution

is not straightforward. For instance, A might ask C to contact B or itself to get the TGK, in effect initiating a 3-way exchange. We will consider this case in detail in a future revision of this draft.

4. A new MIKEY RSA mode

MIKEY RSA_R mode exchange is defined as follows:

```
Initiator                                          Responder
---------                                          ---------

I_MESSAGE = HDR, T, CERTi, [IDr], [SP], SIGNi   -->

       R_MESSAGE = HDR, T, RAND, IDr|CERTr, {SP}, KEMAC, PKE, SIGNr
```

Figure 1: MIKEY RSA_R mode

The main objective of the Initiator's message is to present its public key/certificate to the Responder. The message also contains the timestamp (T) for replay protection, and optionally the Responder's identity (IDr) indicating the responder that the Initiator is interested in talking to. The optional SP payload allows the Initiator to specify its preferences of security parameters. I_MESSAGE is signed to protect against DoS attacks (should this be optional? Perhaps.) SIGNi is a signature covering the entire MIKEY message, using the Initiator's signature key (see Section 5.2 of RFC 3830 for the exact definition).

This method requires a full roundtrip to download the TGKs. The response message uses the envelope approach where the TGKs are encrypted (and integrity protected) with keys derived from a randomly/pseudo-randomly chosen "envelope key". The envelope key is sent to the Initiator encrypted with the public key of the Initiator. The PKE contains the encrypted envelope key: PKE = E(PKi, env_key). It is encrypted using the Initiator's public key (PKi).

The KEMAC payload contains a set of encrypted sub-payloads and a MAC: KEMAC = E(encr_key, IDr || {TGK}) || MAC The first payload (IDr) in KEMAC is the identity of the Responder (not a certificate, but generally the same ID as the one specified in the certificate). Each of the following payloads (TGK) includes a TGK randomly and independently chosen by the Responder (and possible other related parameters, e.g., the key lifetime). The encrypted part is then followed by a MAC, which is calculated over the KEMAC payload. The encr_key and the auth_key are derived from the envelope key, env_key, as specified in Section 4.1.4. of RFC 3830. The payload definitions

are also specified in Section 6.2 of RFC 3830.

Note that the V bit in the common header in this method still indicates a requirement for the Responder's authentication though since the Responder is responsible for generating the KEMAC a derived signature key cannot be used hence the optional CERTr and SIGNr should then be included. See Section 6.9 of RFC 3830 for payload definition.

5. Some specific additions to RFC 3830

Modified Table 6.1a from RFC 3830:

Data type	Value	Comment
Pre-shared	0	Initiator's pre-shared key message
PSK ver msg	1	Verification message of a Pre-shared key msg
Public key	2	Initiator's public-key transport message
PK ver msg	3	Verification message of a public-key message
D-H init	4	Initiator's DH exchange message
D-H resp	5	Responder's DH exchange message
Error	6	Error message
RSA_R I_MSG	7	Initiator's public-key message in RSA_R mode
RSA_R R_MSG	8	Responder's public-key message in RSA_R mode

Figure 2: Table 6.1a (Revised)

6. Conclusion

We propose a new MIKEY RSA mode where the Responder is responsible for generating TGKs. This mode is motivated by deployment scenarios where the Initiator might not have the Responder's CERT handy, or has no easy way of obtaining it. The proposed mode requires a full round-trip, still uses timestamps for replay protection, and requires that both messages be signed by the sending entity. The proposed mode also supports group keying easily - in a similar fashion as the group key pull paradigm suggested in several group key distribution protocols designed by the MSEC WG.

7. Security Considerations

We offer a brief overview of the security properties of the exchange. There are two messages, viz., I_MESSAGE and R_MESSAGE. I_MESSAGE is a signed request by an Initiator requesting the Responder to select a

TGK to be used to protect SRTP session.

The message is signed, which assures the Responder that the claimed Initiator has indeed generated the message. This automatically provides message integrity as well.

There is a timestamp in I_MESSAGE, which when generated and interpreted in the context of the MIKEY specification assures the Responder that the request is live and not a replay. Indirectly, this also provides protection against a DoS attack. The Responder however would have to verify the Initiator's signature and the timestamp, and thus would spend significant computing resources. It is possible to mitigate this by caching recently received and verified requests

R_MESSAGE is quite similar to the I_MESSAGE in the original MIKEY RSA mode and has all the same security properties.

More TBD.

8. IANA Considerations

TBD

9. Acknowledgments

The scenario that motivated this design was the result of discussions between the authors and several people; the authors would like to especially Francois Audet's thoughts on this problem.

10. References

10.1 Normative References

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

[2] Arkko, J., Carrara, E., Lindholm, F., Naslund, M. and K. Norrman, "MIKEY: Multimedia Internet KEYing", RFC 3830, August 2004.

10.2 Informative References

[3] Baugher, M., Weis, B., Hardjono, T. and H. Harney, "The Group Domain of Interpretation", RFC 3547, July 2003.

[4] Baugher, M., McGrew, D., Naslund, M., Carrara, E. and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)",

RFC 3711, March 2004.

[5] Baugher, M., Canetti, R., Dondeti, L. and F. Lindholm, "MSEC Group Key Management Architecture", Internet-Draft (Work in Progress) draft-ietf-msec-gkmarch-08, June 2004.

Authors' Addresses

Dragan Ignjatic
Nortel Networks
250 Sidney St.
Belleville, Ontario K8P3Z3
Canada

Phone:
Email: ignjatic@nortel.com

Lakshminath Dondeti
Nortel Networks
600 Technology Park drive
Billerica, MA 01821
US

Phone: +1 978 288 6406
Email: ldondeti@nortel.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.