Network Working Group
Request for Comments: 4563
Category: Standards Track

E. Carrara
KTH
V. Lehtovirta
K. Norrman
Ericsson

June 2006

The Key ID Information Type for the General Extension Payload in Multimedia Internet KEYing (MIKEY)

Status of This Memo

Copyright Notice

Abstract

This memo specifies a new Type (the Key ID Information Type) for the General Extension Payload in the Multimedia Internet KEYing (MIKEY) Protocol. This is used in, for example, the Multimedia Broadcast/Multicast Service specified in the Third Generation Partnership Project.

Table of Contents

1. Introduction

The Third Generation Partnership Project (3GPP) is currently involved in the development of a multicast and broadcast service, the Multimedia Broadcast/Multicast Service (MBMS), and its security architecture [MBMS].

[MBMS] requires the use of the Multimedia Internet KEYing (MIKEY) Protocol [RFC3830] to convey the keys and related security parameters needed to secure multimedia that is multicast or broadcast.

One of the requirements that MBMS puts on security is the ability to perform frequent updates of the keys. The rationale behind this is that it will be costly for subscribers to re-distribute the decryption keys to non-subscribers. The cost for re-distributing the keys using the unicast channel should be higher than the cost of purchasing the keys for this scheme to have an effect. To implement this, MBMS uses a three-level key management, to distribute group keys to the clients, and be able to re-key by pushing down a new group key. As illustrated in the section below, MBMS has the need to identify which types of keys are involved in the MIKEY message and their identity.

This memo specifies a new Type for the General Extension Payload in MIKEY, to identify the type and identity of keys involved.

1.1. 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 RFC 2119 [RFC2119].

2. Rationale

An application where this extension is used is MBMS key management. The key management solution adopted by MBMS uses three-level key management. The keys are used in the way described below. "Clients" refers to the clients who have subscribed to a given multicast/broadcast service.

* The MBMS User Key (MUK), a point-to-point key between the multicast server and each client.

* The MBMS Service Key (MSK), a group key between the multicast server and all the clients.

* The MBMS Traffic Key (MTK), a group traffic key between the multicast server and all clients.

The Traffic Keys are the keys that are regularly updated.

The point-to-point MUK (first-level key) is shared between the multicast server and the client via means defined by MBMS [MBMS]. The MUK is used as a pre-shared key to run MIKEY with the pre-shared key method [RFC3830], and to deliver (point-to-point) the MSK. The same MSK is pushed to all the clients, to be used as a (second-level) group key.

Then, the MSK is used to push to all the clients an MTK (third-level key), the actual group key that is used for the protection of the media traffic. For example, the MTK could be the master key for the Secure Real-time Transport Protocol (SRTP) [RFC3711] in the streaming case.

A Key Domain identifier defines the domain where the group keys are valid or applicable. For example, it may define a specific service provider.

To allow the key distribution described above, an indication of the type and identity of keys being carried in a MIKEY message is needed. This indication is carried in a new Type of the General Extension Payload in MIKEY.

It is necessary to specify what Crypto Session ID (CS ID) map type is associated with a given key. There are cases (for example, the download case in MBMS) where the required parameters are signalled in-band (each downloaded Digital Rights Management Content Format object [DCF] contains the necessary parameters needed by the receiver to process it). Since the parameters are not transported by MIKEY, this implies that a CS ID map type needs to be registered to the "empty map", as defined in Table 3, which is to be used when the map/policy information is conveyed outside of MIKEY.

3. Relations to MIKEY and GKMARCH

According to [RFC3830], MIKEY is a registration protocol that supports re-keying for unicast in the terms of the MSEC Group Key Management Architecture [RFC4046]. MBMS uses MIKEY both as a registration protocol and a re-key protocol, and the specified extension implements the necessary additions to [RFC3830] that allows MIKEY to function both as a unicast and multicast re-key protocol in the MBMS setting.

4. The Key ID Information Type for the General Extension Payload

The General Extension payload in MIKEY is defined in Section 6.15 of [RFC3830]. The General Extension payload type (Key ID Information) defined in the present document is not restricted to MBMS. Applications using this General Extension payload type may define new Key ID types, and these applications MUST define the semantics and usage of the Key ID Type sub-payloads according to Section 8. The MBMS use of the Key ID Type sub-payloads, defined in Table 2, is specified in [MBMS].

The Key ID Information Type (Type 3) formats the General Extension payload as follows:

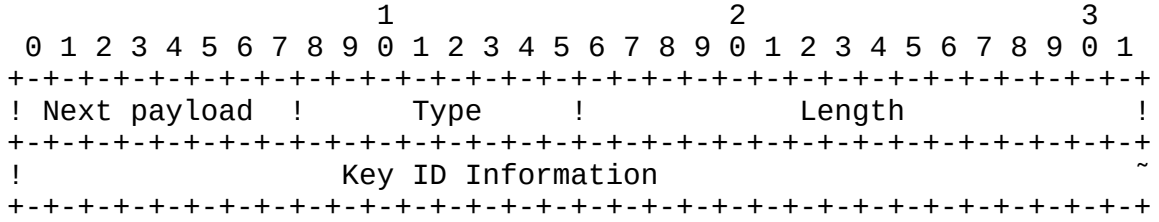

Figure 1. The Key ID Information General Extension Payload

Next Payload and Length are defined in Section 6.15 of [RFC3830].

* Type (8 bits): identifies the type of the General Extension Payload [RFC3830]. This memo adds Type 3 to the ones already defined in [RFC3830].

Type	Value	Comments
Key ID	3	information on type and identity of keys

Table 1. Definition of the New General Extension Payload

* Key ID Information (variable length): the general payload data transporting the type and identifier of a key. This field is formed by Key ID Type sub-payloads as specified below.

The Key ID Type sub-payload is formatted as follows:

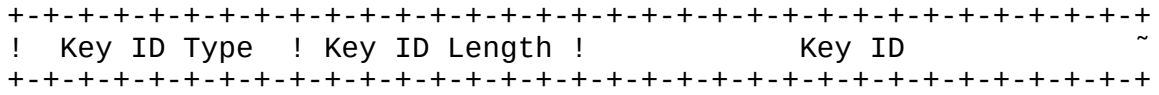

Figure 2. The Key ID Type Sub-payload

* Key ID Type (8 bits): describes the type of the key ID. Predefined types are listed in Table 2.

Key ID Type	Value	Comment
MBMS Key Domain ID	0	ID of the group key domain
MBMS Service Key ID	1	ID of the group key
MBMS Traffic Key ID	2	ID of the group traffic key

Table 2. Type definitions for Key IDs

* Key ID Length (8 bits): describes the length of the Key ID field in octets.

* Key ID (variable length): defines the identity of the key.

Note that there may be more than one Key ID Type sub-payload in an extension, and that the overall length (i.e., the sum of lengths of all Key ID Type sub-payloads) of the Key ID information field cannot exceed 2^16 - 1 octets.

5. Empty Map Type Definition for the CS ID Map Type

When the security policy information is conveyed outside of MIKEY, the CS ID map type is set to a value defined in Table 3 to indicate "empty map". In this case, there MUST NOT be any Security Policy payload present in the message.

CS ID map type	Value	Comments
Empty map	1	Used when the map/policy information is conveyed outside of MIKEY

Table 3. Definition of the CS ID Map Type.

6. Transport Considerations

As specified in Section 7 of [RFC3830], the underlying transport of the MIKEY protocol has to be defined for each type of transport. When the Key-ID payload is used with MBMS, the transport is UDP, and the usage of MIKEY over UDP in the MBMS setting is defined in [MBMS].

7. Security Considerations

The usage of MIKEY for updating the traffic encryption key (MTK) in the broadcast manner, described in Section 2, deviates from the way MIKEY [RFC3830] was originally designed. There are two main points that are related to the security of the described usage.

First, the delivery of the MTK is not source origin authenticated, but rather protected by a group MAC, keyed by the group key (MSK). The threat this raises is that users that are part of the group are able to send fake MTK messages to other group members. The origin of the MTK messages is a node inside the core network, and the trust model used in MBMS is that only trusted traffic is allowed to be sent (from within the operator's network) on the MBMS bearers. However, there is always the risk that traffic is injected on the air interface between the base stations and the user equipment. It is possible for members of the group (i.e., with access to the MSK) to spoof MTK updates to other members of the group. 3GPP decided that the technical difficulties and costs involved in performing such an attack are large enough compared to the expected gain for the attacker, that the risk was deemed acceptable. Note that, since the delivery of the MTK is not source origin authenticated, there is nothing gained by adding source origin authentication to the RTP streams (e.g., using SRTP-TESLA [RFC4383]). Hence, the current use of the specified extension is not compatible with SRTP-TESLA, which requires source origin authentication of the integrity key.

Note that in MBMS the MSK is protected end-to-end, from the multicast server to the clients, using a client-unique key MUK, but the MTK is delivered under protection by the group key MSK, so source origin authentication is not achieved.

Secondly, the delivery of the MTK is separated from the delivery of the security policy. The security policy is delivered with the MSK. The delivery of the MTKs is assumed to be frequent (some scenarios require the delivery of MTKs to be as frequent as a few seconds apart). This would imply that the cost (in terms of bandwidth) would be very high if the security policy was delivered together with each MTK. Furthermore, the security policy parameters of the streaming session are not anticipated to change during the session, even though there would be an update of the MTK. It was decided in 3GPP that there was no need for updating the policy during an ongoing session, and that the cost of allowing such a feature, only to be on the safe side, would be too high. On the other hand, updating the security policy during an ongoing session would be possible by updating the MSK.

The Empty map type used when the security policy is delivered in band relies on the security provided by DCF [DCF], and MIKEY is, in this case, only used to provide the master key for the DCF processing.

8. IANA Considerations

According to Section 10 of RFC 3830, IETF consensus is required to register values in the range 0-240 in the Type namespace of the MIKEY General Extension Payload and the CS ID map type namespace of the Common Header Payload.

A new value in the MIKEY General Extension Payload Type name space has been registered for this purpose. The registered value for Key ID is 3 according to Section 4.

Also, the value 1 has been registered for the Empty map in the existing CS ID map namespace of the Common Header Payload, as specified in Table 3, in Section 5.

The new name space for the following field in the Key ID information sub-payload (from Sections 4 and 5) has been established and will be managed by IANA:

* Key ID Type

The IANA has registered the pre-defined types of Table 2 for this namespace. IANA will also manage the definition of additional values in the future. Values in the range 0-240 for each name space SHOULD be approved by the process of IETF consensus, and values in the range 241-255 are reserved for Private Use, according to [RFC2434].

9. Acknowledgements

We would like to thank Fredrik Lindholm.

10. References

10.1. Normative References

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

[RFC3830] Arkko, J., Carrara, E., Lindholm, F., Naslund, M., and K. Norrman, "MIKEY: Multimedia Internet KEYing", RFC 3830, August 2004.

[MBMS] 3GPP TS 33.246, "Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security; Security of Multimedia Broadcast/Multicast Service".

10.2. Informative References

[RFC3711] Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, March 2004.

[DCF] Open Mobile Alliance, OMA-DRM-DCF-V2_0-20050329-C, "DRM Content Format V2.0", Candidate Version 2.0 - 29 March 2005.

[RFC4383] Baugher, M. and E. Carrara, "The Use of Timed Efficient Stream Loss-Tolerant Authentication (TESLA) in the Secure Real-time Transport Protocol (SRTP)", RFC 4383, February 2006.

[RFC4046] Baugher, M., Canetti, R., Dondeti, L., and F. Lindholm, "Multicast Security (MSEC) Group Key Management Architecture", RFC 4046, April 2005.

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

Authors' Addresses

Elisabetta Carrara
Royal Institute of Technology
Stockholm
Sweden

EMail: carrara@kth.se

Vesa Lehtovirta
Ericsson Research
02420 Jorvas
Finland

Phone: +358 9 2993314
EMail: vesa.lehtovirta@ericsson.com

Karl Norrman
Ericsson Research
SE-16480 Stockholm
Sweden

Phone: +46 8 4044502
EMail: karl.norrman@ericsson.com

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).