Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Corrections for CMAC/HMAC Tuple Usage**
Data Submitted	**2005-07-14**

Source(s)	Seokheon Cho Sungcheol Chang Chulsik Yoon ETRI 161, Gajeong-dong, Yuseong-Gu, Daejeon, 305-350, Korea	Voice: +82-42-860-5524 Fax: +82-42-861-1966 chosh@etri.re.kr

Re:	IEEE P802.16e/D9

Abstract	In general, the CMAC/HMAC-Digest is used to authenticate PKM-related MAC messages and the CMAC/HMAC Tuple is used to authenticate the other MAC messages. The CMAC/HMAC Tuple included in the PKM-related MAC messages should be changed to the CMAC/HMAC Digest.

Purpose	Adoption of proposed changes into P802.16e/D9

Patent Policy and Procedures	The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard. "Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:chiar@wirelessman.org> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.

Corrections for CMAC/HMAC Tuple Usage

Seokheon Cho, Sungcheol Chang, and Chulsik Yoon

ETRI

Introduction

0.1 IEEE P802.16e/D9 Status and Problems

In general, the CMAC/HMAC-Digest is used to authenticate the PKM-related MAC messages and the CMAC/HMAC Tuple is used to authenticate the other MAC messages.

The CMAC/HMAC Tuple can be used, after both MS and BS share the valid AK sequence number and then have the CMAC/HMAC sequence number, because the CMAC/HMAC Tuple compound attributes contain the CMAC/HMAC sequence number.

There are several the PKM-related messages containing the CMAC/HMAC Tuple, such as a PKMv2 SA-TEK-Challenge message, a PKMv2 SA-TEK-Request message, and a PKMv2 SA-TEK-Response message. However, both MS and BS can't share the valid AK sequence number, before exchanging these messages. Therefore, these messages should not include the CMAC/HMAC Tuple but the CMAC/HMAC-Digest for message authentication.

0.2 Solutions

PKMv2 SA-TEK-Challenge, PKMv2 SA-TEK-Request, and PKMv2 SA-TEK-Response messages shall include the CMAC-Digest and the HMAC-Digest for message authentication.

Proposed Changes into IEEE P802.16e/D9

[Change sub-clauses 6.3.2.3.9.18 as follows]

6.3.2.3.9.18 PKMv2 SA-TEK-Challenge message

The BS transmits the PKMv2 SA-TEK-Challenge message as a first step in the 3-way SA-TEK handshake at initial network entry and at reauthorization. The BS shall send this message to the MS after finishing authorization procedure(s) selected by the negotiated Authorization Policy Support included in the SBC-REQ/RSP messages. Both BS and MS can check out whether or not they share the same AK by verifying HMAC/CMAC-Digest. ~~It identifies an AK to be used for the Secure Association, and includes a random number challenge to be included by the MSS in its SA-TEK-Request.~~

Code: 20

Attributes are shown in Table 37g

Table 37g – PKMv2 SA-TEK-Challenge message attributes

Attribute	Contents
BS_Random	A freshly generated random number of 64bits
Key Sequence Number	AK sequence number
AKID	BS transmits newly assigned AKID.
~~CMAC Tuple/HMAC Tuple~~	~~Message integrity tuple for this message~~
Key lifetime	PMK lifetime, this attribute shall include only follows EAP-based authorization or EAP-based re-authorization procedures.
HMAC-Digest/CMAC-Digest	Message authentication digest for this message

~~The CMAC key sequence number/HMAC key sequence number included in the OMAC Tuple/HMAC Tuple should be equal to the newly assigned RK sequence number.~~

The generation of the AK sequence number and the AKID is defined in 7.2.2.4.1.

The HMAC-Digest attribute or the CMAC-Digest attribute shall be the final attribute in the message's attribute list.

Inclusion of the HMAC-Digest or the CMAC-Digest allows the MS and BS to authenticate a PKMv2 SA-TEK-Challenge message. The HMAC or the CMAC authentication keys are derived from the AK.

[Change sub-clauses 6.3.2.3.9.19 as follows]

6.3.2.3.9.19 PKMv2 SA-TEK-Request message

The MS transmits the PKMv2 SA-TEK-Request message after receipt and successful ~~HMAC/CMAC~~ HMAC-Digest or CMAC value verification of ~~an SA-Challenge~~ a PKMv2 SA-TEK-Challenge message from the BS. The PKMv2 SA-TEK-Request ~~Request~~ proves liveliness of the MS and its possession of the AK to the BS. If this message is being generated during initial network entry, then it constitutes a request for SA-Descriptors identifying the primary and static SAs and GSAs the requesting MS is authorized to access and their particular properties (e.g., type, cryptographic suite).

If this message is being generated upon HO, then it constitutes a request for establishment (in the target BS) of TEKs, GTEKs and GKEKs at the MSS and renewal of active primary, static and dynamic SAs and associated SAIDs used by the MSS in its previous serving BS.

Code: 21

Attributes are shown in Table 37h.

Table 37h – PKMv2 SA-TEK-Request message attributes

Attribute	Contents
MS_Random	A 64-bit number chosen by the MS for every new handshake.
BS_Random	The 64-bit random number ~~from the SA-Challenge~~ used in the PKMv2 SA-TEK-Challenge message.
Key Sequence Number	AK sequence number

AKID	This identifies the AK to the BS that was used for protecting this message.
Security_Capabilities	Describes requesting MS's security capabilities
Security Negotiation Parameters	Describes ~~requesting MS's security capabilities~~ the security negotiation parameters used in the SBC-REQ message (see 11.8.4)
~~CMAC/HMAC~~	~~Message integrity code for this message~~
HMAC-Digest/CMAC-Digest	Message authentication digest for this message

[Change sub-clauses 6.3.2.3.9.20 as follows]

6.3.2.3.9.20 PKMv2 SA-TEK-Request message

The BS transmits the PKMv2 SA-TEK-Response message as a final step in the 3-way SA-TEK handshake.

Code: 22

Attributes are shown in Table 37i.

Table 37i – PKMv2 SA-TEK-Response message attributes

Attribute	Contents
MS_Random	~~The number received from the MS~~ The 64-bit random number used in the PKMv2 SA-TEK-Request message.
BS_Random	The random number included in the PKMv2 SA-TEK-Challenge message or SA-Challenge TLV.
Key Sequence Number	AK sequence number
AKID	This identifies the AK to the BS that was used for protecting this message.

SA_TEK_Update	A compound TLV list each of which specifies an SA identifier (SAID) and additional properties of the SA that the MS is authorized to access. This compound field may be present at the reentry. Additionally, in case of HO, for each active SA in previous serving BS, corresponding TEK, GTEK and GKEK parameters are also included.
Frame Number	An absolute frame number in which the old PMK and all its associate AKs should be discarded.
(one or more) SA-Descriptor (s)	Each compound SA-Descriptor attribute specifies an SA identifier ~~idenfier~~ (SAID) and additional properties of the SA. This attribute is present at the initial network entry.
~~CMAC Tuple /HMAC Tuple~~	~~Message integrity tuple for this message~~
HMAC Digest/CMAC Digest	Message authentication digest for this message