| | |
|---|---|
| Project | **IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>** |
| Title | **BS-specified HMAC tuple truncation** |
| Date Submitted | **2005-01-20** |


| | | |
|---|---|---|
| Source(s) | Jeff Mandin<br>Streetwaves Networking<br>Amatzia 5<br>Jerusalem, Israel | Voice: 972-50-572-4587<br>Fax: 972-50-572-4587<br>jeff@streetwaves-networks.com |
| | Yigal Leiba<br><br>Runcom | yigall@runcom.co.il |


| | |
|---|---|
| Re: | 802.16e/D5a BRC Recirc |
| Abstract | |
| Purpose | |
| Notice | This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein. |
| Release | The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16. |
| 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:chair@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>. |

# HMAC tuple truncation

*Jeff Mandin*
*Streetwaves Networking*

## 1 Problem Statement

The HMAC digest that accompanies many management messages is 21 bytes long. This is substantial and unnecessary overhead.

## 2 Security Considerations

FIPS 198 contains the NIST recommendations for use of HMAC. It states[1]:

> *When a truncated HMAC is used, the t leftmost bytes of the HMAC computation shall be used as the MAC. The output length, t, shall be no less than four bytes (i.e., 4 ≤ t ≤ L). However, t shall be at least L/2 bytes unless an application or protocol makes numerous trials impractical.*

Consequently, the FIPS minimum recommended length for digests as applied to 802.16 is 10 bytes.

However:

- an 802.16 attacker is limited as to the number of forgery attempts that could be made in a period of time. The actual number of forgery attempts that could be realistically made depends on the particular environment
- In many cases, successful forging of a particular 802.16 management message would not lead to a critical system failure
- Some messages, such as DSx in particular, would be high-value targets for forgery and should retain maximum protection

## 3 Summary of Solution – Short Digest with Flexible Length for Mobility messages

Our solution is define a separate "short HMAC" to permit HMAC lengths of 4, 8, and 10 bytes – to be specified by the BS at the end of the authentication/handover process (ie. Secure Association establishment).

We apply the "short HMAC" to Mobility management messages. DSx etc. will continue to use the 20byte HMAC.

## 4 Specific text changes to 802.16e/D5a

**[Modify section 7.5.3 ]**

[1] http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf Section 4

The HMAC sequence number in the HMAC tuple or Short-HMAC tuple shall be equal to the AK sequence number of the AK from which the HMAC_KEY_x was derived.

**[Insert new section following 11.9.6]**

### Short-HMAC digest

*Description:* This attribute contains the highest-order bytes of the keyed hash used for message authentication. The HMAC algorithm is defined in IETF RFC 2104. The 20 byte HMAC result is truncated to the length indicated by the BS in the Short-HMAC digest length parameter (see section xx), or to 10 bytes if the Short-HMAC digest length parameter was not specified.

| **Type** | **Length** | **Value (string)** |
|---|---|---|
| x | variable (4, 8, or 10 bytes as described in x ) | The highest order bytes of the truncated HMAC-SHA1 keyed hash |

**[Insert new section following 11.1.2]**

**Short-HMAC tuple**

This parameter contains the HMAC Key Sequence Number concatenated with an HMAC-Digest used for message authentication. The HMAC Key Sequence Number is stored in the four least significant bits of the first byte of the HMAC Tuple, and the most significant four bits are reserved. The HMAC-Tuple attribute format is shown in Table <new1> and Table <new2>.

**Table <new1>**

| Type | Length | Value | Scope |
|---|---|---|---|
| ?? | variable | See Table <new2> | MOB-SLP-REQ, MOB-SLP-RSP, MOB_SCN-REQ, MOB_SCN-RSP, MOB-MSSHO-REQ, MOB-BSHO-RSP, MOB-HO-IND, RNG-REQ, RNG-RSP |

**Table <new2>**

| Type | Length | Value |
|---|---|---|
| *Reserved* | 4 bits | |
| HMAC Key Sequence Number | 4 bits | |
| Short- HMAC-Digest | variable | truncated HMAC with SHA-1 |

[**Add new section after 11.9.16**]

**Short-HMAC Digest Length**

This parameter specifies the number of bytes that the BS and SS will use in the Short-HMAC Digest TLV. If this TLV is absent, the Short-HMAC digest length defaults to 10 bytes.

The output of the HMAC function is 160 bits long. To create the Short-HMAC digest field, the BS or SS truncates the 20-byte HMAC output to the requisite length and includes the highest-order bytes in the Short-HMAC digest field.

**Table <new3>**

| Value | Description |
|---|---|
| 0 | Truncate HMAC to 10-bytes in Short HMAC tuple |
| 1 | Truncate to 8 bytes |
| 2 | Truncate to 4 bytes |

| Type | Length | Value |
|---|---|---|
| ?? | 8 bits | 1 byte code specifying the Short HMAC Digest length according to table <new 3> |