| | |
|---|---|
| Project | **IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>** |
| Title | TEK update decision base on PN |
| Date Submitted | **2005-07-10** |


| | | |
|---|---|---|
| Source(s) | Avishay Shraga | Avishay.shraga@intel.com |
| | Yigal Eliaspur | Voice: +972-54-5551063 |
| | Intel corp. | Yigal.Eliaspur@intel.com |
| | | Voice: +972-54-7884877 |


| | |
|---|---|
| Re: | Sponsor Ballot on IEEE P802.16-2004/Cor1/D3 |
| Abstract | In cipher suite AES the key may expire because PN space finished, the standard does not define well enough what to do in this stage |
| Purpose | Define How Bs and SS decide to update TEK based on PN value |
| 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>. |

# Define parameters and algorithm for TEK update based on PN space usage

Avishay Shraga

## 1. Motivation

The standard defines that for security suite using PN (AES-CCM), the key maintenance will be similar to the maintenance based on key lifetime i.e. change key whenever PN space reaches half of it's total value.

This solution is problematic and not working from several reasons:

1) The PN space usage is based on traffic and therefore not deterministic as time thus, the newer key PN space can reach half it's value before the old one and than it is not clear what to do.
2) Each key has 2 PNs one for DL and one for UL, each of them grows in different rates and in different positions (i.e. old key and new key).
3) If both the SS and BS should change key at the same point, there might be a race when SS asks for new key before BS created one.

The purpose of this contribution is to define TH for PN base key exchange.

## 2. Proposed solution

The proposed solution is base on keeping the TEK exchange general flow as it is in the standard i.e. the BS changes the TEK when it reaches a TH and the SS asks for TEK update before the key actually expires but after it is sure the Bs already created a new key.

Another attribute of the solution is that no matter which key PN reaches the TH, the sequence always will be:

Discard old key

Mark new as OLD key

Create fresh new key.

The TH will be set to values that the TH for the new key will be lower than the one for the old thus, even if new key is exhausted – it still has a PN space to use as the old key.

## 3. Solution Description

Each SA contains 2 keys which marked as old and new (will call them BS_old and BS_new).

Each key has 2 parameters that may effects its validity:

Lifetime – a parameter which defined by the BS, each created TEK has the same lifetime which starts running from the creation time.

When the lifetime expires the key can't be use anymore.

PN (packet number) space usage:

- Each key has a PN space to be used with the key to create different encryption combination for each PDU.
- The PN is incremented by 1 with all transmitted packet
- The size of the PN space is 32 bit meaning up to 2^32 PDUs can be sent with the same key.
- Since the same key can be used for DL and UL, the PN space is divided into halves:

from 0x0→0x7FFFFFFF for DL and from 0x80000000->0xFFFFFFFF for UL
- When one of the UL/DL spaces exhausted, the key can't be used anymore.

The standard does not define when to create new key in terms of PN space usage and when the SS knows to ask for such a key.

It is impossible to use the same algorithm as for the lifetime because PN space usage is a function of the traffic. Combining it with the definition of BS_Old_key for DL and SS_New_key for UL, the PN space behavior is not deterministic.

Analyzing the PN space usage options, the solution to the problem is:

**Definitions**:

DL PN Space – 0x00000000 → 0x7FFFFFFF

UL PN Space – 0x80000000 → 0xFFFFFFFF

MIN_TH – 1/2 of the total relevant PN space:

- For DL the min TH is 0x3FFFFFFF
- For UL the min TH is 0xBFFFFFFF

MAX_TH –¾ of the total relevant PN space:

- For DL the MAX TH is 0x5FFFFFFF
- For UL the MAX TH is 0xDFFFFFFF

TEK Lifetime – as defined in standard

TEK Grace Time – as defined in standard

**BS TEK management**

BS switch key if:

New_Key lifetime reache half-way.

Old_Key_DL_PN = MAX_TH (this is the key the BS used for DL thus no other DL PN may grow).

New_Key_UL_PN=MIN_TH.

Switch keys is:

Discard "old" key and its context.

Mark current "new" key as "old" key: "old key"← "new key"

Mark fresh key as the "new" key: "new key"←"fresh key"

**SS TEK management**

SS ask for key update if:

New Key Grace time reached

New_Key_DL_PN=MIN_TH

New_Key_UL_PN=MAX_TH

This algorithm should ensure that no key PN will reach it's maximum value (the entire space) however, if one key reaches this value this key should be discarded and not used anymore.

**Explanation of algorithm**

The definitions of the standard defines that the SS uses it's new key for UL and the BS uses it's old key for DL, we must show that in two cases DL only and UL only the algorithm works and than it is good for all combination because in mixed UL+DL combination each time one of the PN reaches it TH and than it is like working in this PN context only (UL or DL).

DL only

Start from SS and BS shares both old and new key (key update just occurred)

The old_key PN is fresh because the BS never used it for Tx.

The Bs uses old_PN_DL until it reaches MAX_TH and than it switch keys.

Now the BS_old_key is the SS_new_key

The old_key PN DL is fresh because the BS never used it for Tx

. The Bs uses old_PN_DL which is the SS_new_PN_DL until it reaches MIN_TH<MAX TH and than The SS asks for key update which return to both key shared.

Conclusion using this two TH for DL makes sure that the SS will get the key update after the BS switched keys but before it switches again – the SS successful in chasing the BS keys.

UL only

Start from SS and BS shares both old and new key (key update just occurred)

The new_key PN is fresh because the SS never used it for Tx.

The SS uses new_PN_UL until it reaches MIN_TH and than the BS recognize it and switch keys.

Now the BS_old_key is the SS_new_key

The SS continue using its new_key_PN_UL which is now the BS_old_key PN UL.

When the SS_new_key_PN_UL reaches MAX_TH>MIN_TH, the SS asks for key update which return to both key shared

. Conclusion using this two TH for UL makes sure that the SS will get the key update after the BS switched keys but before it switches again – the SS successful in chasing the BS keys.

# 4. Changes summary

**7.2.2.1 Security associations**

Remove the sentence

For ~~AES-CCM mode, when more than half the available PN numbers in the 31-bit PN number space are exhausted, the MS shall schedule a future Key Request in the same fashion as if the key lifetime was approaching expiry.The operation of the TEK state machine's Key Request scheduling algorithm, combined with the BS's regimen for updating and using an SAID's keying material (see 7.4), ensures that the MS will be able to continually exchange encrypted traffic with the BS.~~

**7.2.1.4.1 TEK exchange overview for PMP**

Add the following:

**BS TEK management**

BS switch key if:

New_Key lifetime reache half-way.

Old_Key_DL_PN = DL_MAX_TH (this is the key the BS used for DL thus no other DL PN may grow).

New_Key_UL_PN=UL_MIN_TH.

Switch keys is:

Discard “old” key and its context.

Mark current “new” key as “old” key: “old key”← “new key”

Mark fresh key as the “new” key: “new key”←”fresh key”

**SS TEK management**

SS ask for key update if:

New Key Grace time reached

New_Key_DL_PN=DL_MIN_TH

New_Key_UL_PN=UL_MAX_TH

This algorithm should ensure that no key PN will reach it’s maximum value (the entire space) however, if one key reaches this value this key should be discarded and not used anymore.

**10.2 PKM parameter values**

Add to table 343

| System | Name | Description | Min value | Default value | Max value |
|---|---|---|---|---|---|
| SS | DL min TH | Value of DL PN in new key that trigger the SS to ask for key update | | 0x3FFFFFFF | |
| SS | UL max TH | Value of UL PN in new key that trigger the SS to ask for key update | | 0xDFFFFFFF | |
| BS | DL max TH | Value of DL PN in old key that trigger the BS to switch keys | | 0x5FFFFFFF | |
| BS | UL min TH | Value of UL PN in new key that trigger the BS to switch keys | | 0xBFFFFFFF | |