Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Residual Termination Block Processing with CTS**
Date Submitted	**2005-07-14**
Source(s)	Zhengfei Xiao, Yongmao Li, Phillip Barber, Jim Carlo, David Xiang, Duke Dang, Lucy Chen, John Lee mailto:john_lee@huawei.com HUAWEI Seokheon Cho Sungcheol Chang Chulsik Yoon ETRI
Re:	Call for contribution and comments.
Abstract	Residual Termination Block Processing with CTS.
Purpose	Adoption
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>.

Residual Termination Block Processing with CTS

Zhengfei Xiao, Yongmao Li, Phillip Barber, Jim Carlo, David Xiang, Duke Dang, Lucy Chen, John Lee
HUAWEI

Problem Definition

Per D9 in section 7.8.4.2, if the final block size n is smaller than cipher block size, the next-to-last ciphertext block shall be AES encrypted for the second time, using the electronic code book (ECB) mode, and the most significant n bits of the result are XORed with the final n bits of the payload to generate the short final cipher block. There are two problem about the method .One is that the method has been proved not secure enough, though it was often used. Since the final block is not encrypted but XORed with a block, any modified bits can just affect the corresponding bits which means that the malicious attacker can easily predict the modification results. If the termination block does not contain important information, it may not matter much. However, if the termination block contains important information, it would be a serious security problem. The other is this mechanism requires the receiver supportting encryption algorithm in both ECB and CBC mode.

Remedy

Introduce the CTS mechanism to process the termination block with AES CBC mode. Using this residual termination block processing rule, all of the blocks are encrypted with AES. Further, the sender and receiver will encrypt and decrypt data only in CBC mode in most cases. Both of the sender and receiver need not support encryption or decryption in ECB mode.

Proposed Text Changes

[Modify sub-clause 7.8.4.2 in page 239, line 30 as follows:]

7.8.4.2 Data encryption with AES in CBC mode

If the data encryption algorithm identifier in the cryptographic suite of an SA equals 0x03, data on connections associated with that SA shall use the CBC mode of the US Advanced Encryption Standard (AES) algorithm [NIST Special Publication 800-38A, FIPS 197] to encrypt the MAC PDU payloads.

~~Residual termination block processing shall be used to encrypt the final block of plaintext when the final block is less than the cipher block size. Given a final block having n bits, where n is less than the cipher block size, the next-to-last ciphertext block shall be AES encrypted for the second time, using the electronic code book (ECB) mode, and the most significant n bits of the result are XORed with the final n bits of the payload to generate the short final cipher block. In order for the receiver to decrypt the short final cipher block, the receiver AES encrypts the next-to-last ciphertext block, using the ECB mode, and XORs the most significant n bits with the short final cipher block in order to recover the short final plaintext block. This encryption procedure is depicted in Figure 9.4 of Schneier [B42].~~

Residual termination block processing shall be used to encrypt the final block of plaintext when the final block is less than the cipher block size. Given a final block having n bits, where n is less than the cipher block size m, the next-to-last ciphertext block shall be divided into two parts. One of the two parts is n bits, the other part is m-n bits. The former will be sent to receiver as the final block ciphertext. Padding the final short block to obtain a complete plaintext block, then encrypt it with AES algorithm in CBC mode. The encryption and decryption procedure is depicted in Figure 137d.

In the special case when the payload portion of the MAC PDU is less than the cipher block size, the most significant n bits of the generated CBC-IV, corresponding to the number of bits of the payload, shall be XORed with the n bits of the payload to generate the short cipher block.

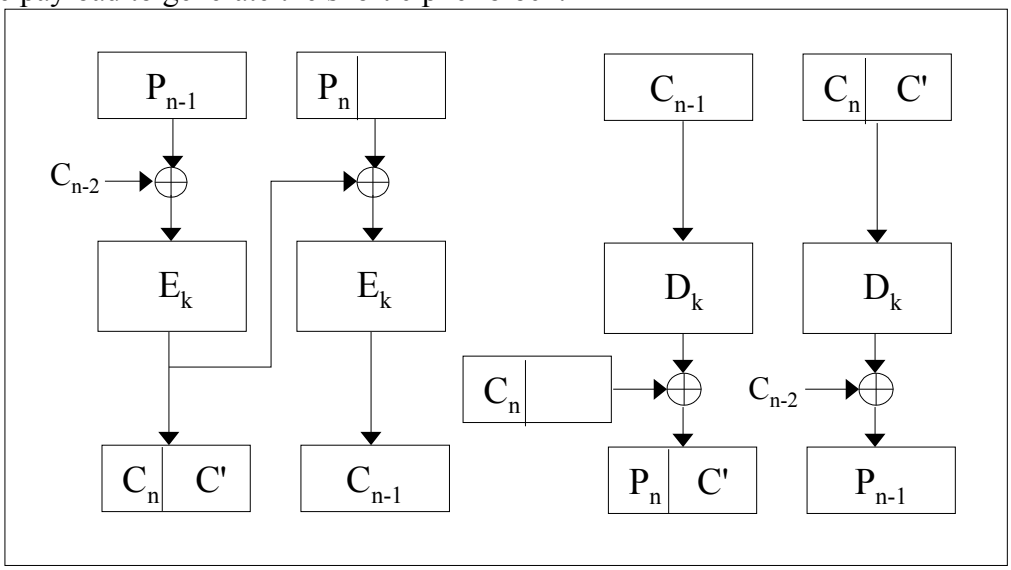

Figure 137d—Residual termination block processing with CTS

Operator Network Operator Network