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
Re:	Call for contribution and comments.
Abstract	Residual Termination Block Processing with CTS.
Purpose	Adoption
Notice	
Release	
Patent Policy and Procedures	

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 0x01, data on connections associated with that SA shall use the CBC mode of the US Data Encryption Standard (DES) algorithm [FIPS 46-3, FIPS 74, FIPS 81] to encrypt the MAC PDU payloads.

The CBC IV shall be calculated as follows: in the downlink, the CBC shall be initialized with the exclusive-or (XOR) of (1) the IV parameter included in the TEK keying information, and (2) the content of the PHY Synchronization field (right justified) of the latest DL-MAP. In the uplink, the CBC shall be initialized with the XOR of (1) the IV parameter included in the TEK keying information, and (2) the content of the PHY Synchronization field of the DL-MAP that is in effect when the UL-MAP for the uplink transmission is created/received.

~~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.

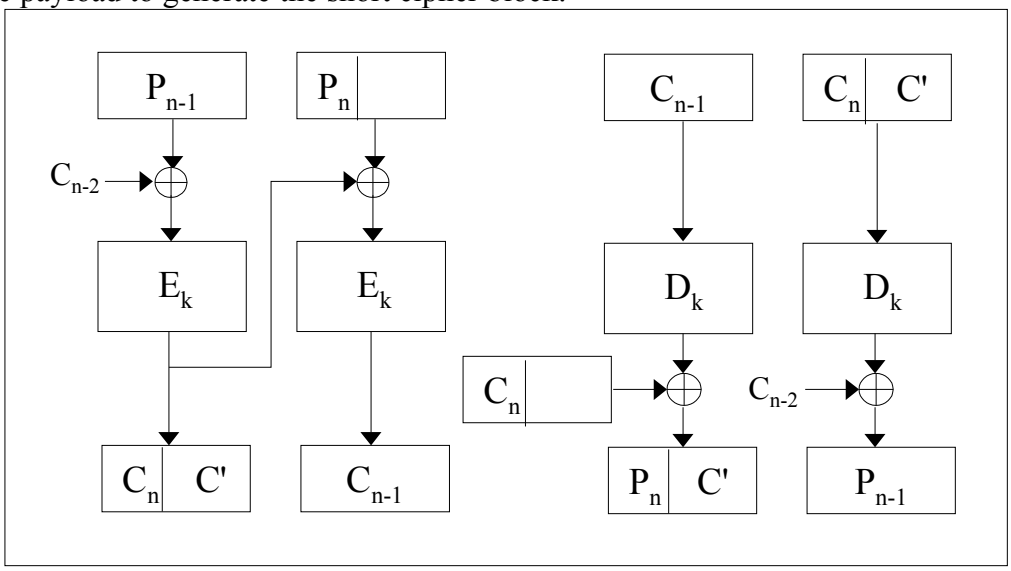

Figure 137d—Residual termination block processing with CTS

Operator Operator
Network Network