Introduction

- CCMP stands for Counter Mode – CBC MAC Protocol
  - CCMP defines a set of rules that use the AES block cipher for encryption and integrity protection
  - The cipher of CCMP is AES
  - The cipher of TKIP is RC4
- The default mode for IEEE 802.11i is CCMP
- Provides stronger security compared to TKIP
  - CCMP is designed from scratch, therefore ready to use best-known techniques
  - TKIP is a compromise. It uses weaker security primitives (e.g., Michael) in order to accommodating existing hardware

- Why AES?
  - AES is secure, gone through a large amount of reviews already
  - It is export-controlled and well-understood by government agencies, and therefore easier to get export licenses

WEP, TKIP, and CCMP

- WPA/TKIP and RSN/CCMP have a lot in common: eg. Key management
- CCMP use one key for encryption and protection
- The biggest difference is the encryption algorithm – how the data is encrypted/decrypted

AES Overview

- AES is a block cipher, with the same size for the plaintext/ciphertext
- It is very unlikely that any fundamental weaknecess will be discovered in the near future
- AES allows different block sizes and key sizes
  - CCMP restricts the key size and block size to be 128 bits

AES Pairwise Key Hierarchy in CCMP

<table>
<thead>
<tr>
<th>Key Type</th>
<th>Key Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pairwise Master Key</td>
<td>256 bits</td>
</tr>
<tr>
<td>Pairwise Transient Key</td>
<td>384 bits</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key Type</th>
<th>Key Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAPOL MIC Key</td>
<td>128 bits</td>
</tr>
<tr>
<td>EAPOL Encr Key</td>
<td>128 bits</td>
</tr>
<tr>
<td>Data Encr/ MIC Key</td>
<td>128 bits</td>
</tr>
</tbody>
</table>

AES Group Key Hierarchy in CCMP

<table>
<thead>
<tr>
<th>Key Type</th>
<th>Key Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Master Key</td>
<td>256 bits</td>
</tr>
<tr>
<td>Group Transient Key</td>
<td>128 bits</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key Type</th>
<th>Key Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Encr/ MIC Key</td>
<td>128 bits</td>
</tr>
</tbody>
</table>

Protect Key Handshakes  Protect Data

Protect Multicast/Broadcast
**Modes of Operation**

- AES has up to 16 different modes of operation (published in the NIST website), and it is still seeking for new ones.
- **ECB mode**
  - Encrypt each block independently; Padding needed; Can be done in parallel
  - Same block generates the same cipher
- **Counter mode**
  - Encrypt a counter, which is increased 1 for each block, and XOR the result with the data to produce the ciphertext
  - Decryption is exactly the same as encryption, no padding is needed
  - Parallel encryption/decryption
  - No message authentication, only encryption
  - Initial value (a nonce) of the counter and its step size need to be delivered to the receiver
  - It is possible for two blocks of identical plaintexts to generate the same ciphertexts if the counter starting from 1

**Counter mode + CBC MAC: CCM**

- Created especially for IEEE 802.11i RSN
- Invented by D. Whiting, R. Housley, and N. Ferguson in the 802.11i standard group
- Built on top of the counter mode; uses counter mode in conjunction with a message authentication method called cipher block chaining (CBC)
- Encrypt the first block with AES; XOR the result with the second block and then encrypt it with AES; Repeat until no block left. The result is a single block as the MIC
- Padding is needed
- Linking authentication and encryption
- CCM mode allows the encryption to be performed on a subpart of the message that is authenticated by CBC-MAC
  - Header should be transmitted as plaintext but it should not be modified
  - The IVs (nonces) for the counter mode and for the CBC-MAC portion are different, leading different keys
  - Simple but can’t be parallelized

**Offset Codebook Mode (OCB)**

- Achieves both encryption and authentication
- OCB is parallelizable so it can be done faster using multiple hardware blocks
- OCB is very efficient, taking only a slightly more than the theoretical minimum encryption operations possible
- OCB is provably secure; It is as secure as AES
- OCB is not adopted by IEEE 802.11i
  - It is proprietary

**How CCMP is Used in RSN**

- MSDU
- Fragmentation
- MPDU
- MPDU
- MPDU
- MAC Header
- CCMP Processing
- Encrypted MPDU
- Priority Queue
- Priority Queue
- Priority Queue
- Transmission

**CCMP Processing**

- Hdr = Header
  - MAC Hdr
  - Data

- MAC Hdr
  - CCMP Hdr
  - Data
  - MIC

- MAC Hdr
  - CCMP Hdr
  - Ciphertext

**CCMP Header**

- CCMP header must be prepended to the encrypted data and transmitted in plaintext. The format is similar to TKIP
- CCMP Header contains the 48-bit packet number (PN) that provides replay protection and enables the receiver to derive the nonce for the encryption
- CCMP Header also contains the KeyID field to specify which group key has been used

- 8 bytes
  - PN0
  - PN1
  - Rev
  - PN2
  - PN3
  - PN4
  - PN5

- 8 bits
  - Reserved
  - 1
  - KeyID
CCMP Encryption

- First Block for MIC computation
  - Flag fixed to 01011001, indicating that MIC field is 64-bit in length
  - Priority, SA, and PN form a unique Nonce
  - Data Length specifies the length of the plaintext

- Padding for two parts, counter mode encryption works only on the plaintext and the MIC

- The counter for AEC Counter Mode (128 bits)
  - Ctr starts from 1 for a frame

CCMP Decryption

- A reverse procedure
  - Check PN
  - Decryption
  - Check MIC

- Counter mode AES encrypts the counter through AES, and therefore Encryption/Decryption are the same