WIFI SECURITY (WPA2)

Prepared by	Vinay B
Reviewed by	M , Ramesh Babu

WI-FI PROTECTED ACCESS 2 (WPA2): In 2004, Wi-Fi Protected Access 2 became available. WPA2 has stronger security and is easier to configure than the prior options It provides stronger data protection and more control over network access.

Before going to WPA2 we need to understand 4 way handshake which is explained below,**4 WAY HANDSHAKE:**

The 4-way handshake is defined as a process of exchanging four messages between an access point (authenticator) and the client device (supplicant) in order to generate encryption keys which can be used to encrypt actual data.

KEY WORDS TO REMEMBER IN 4 WAY HANDSHAKE:

- PSK = Pre-Shared Key
- MSK = Master Session Key
- PMK = Pairwise Master Key
- GMK = Group Master Key
- PTK = Pairwise Transient Key
- GTK = Group Temporal Key
- Nonce
- S-Nonce
- MIC

KEY GENERATION FORMULAES:

PSK = PBKDF2 (Pass Phrase, SSID, SSID Length, 4096, 256)

PMK = PBKDF2(HMAC−SHA1, PSK, SSID, 4096, 256)

PTK = PRF (PMK + A-NONCE +S-NONCE + MAC(AA) + MAC(SA))

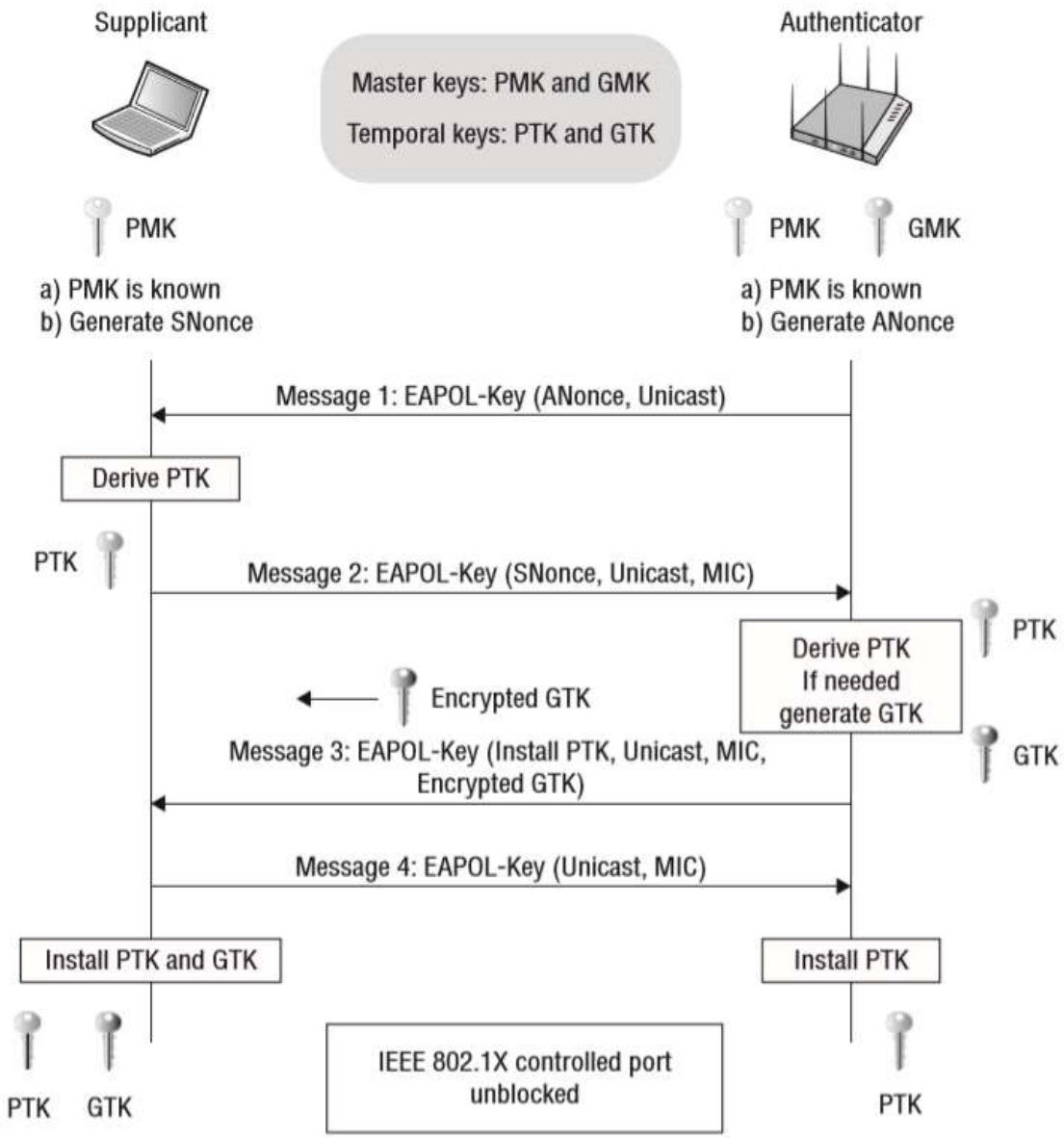
PTK WILL HAVE 5 DIFFERENT KEYS NAMELY:

1. KEK – Used to encrypt the keys [Ex: GTK will be encrypted in M3 using KEK to deliver to the client].
2. KCK – Used during the creation of the MIC, Hash will be generated using KCK.
3. TK – Encryption and decryption of unicast packets.
4. MIC Tx – Only used with TKIP configurations for unicast packets sent by access points.
5. MIC Rx – Only used with TKIP configurations for unicast packets sent by client

Size of the keys are:

```
- 128 bits -.- 128 bits -.- 128 bits -.- 64 bits -.- 64 bits -
|   KCK    |    KEK    |    TK     | MIC Tx  |  MIC Rx  |
```

4 – WAY HANDSHAKE EXPLAINED:



M1 Message: Here AP will send the Nonce and we call it as ANONCE. And the 4-way handshake uses HMAC-SHA1 procedure to generate the MIC. It is unicast message. PTK is derived using the A-NONCE sent by the AP

M2 Message: M2 Message will be sent by the Supplicant. Supplicant will send the s-nonce, and now we have the required components to generate the PTK. PTK is derived at AP side now. Message 2 will be unicast.

M3 Message: AP notifies the Supplicant to install the Keys and AP will send the GTK to the Supplicant, and the GTK will be encrypted using KEK. It will be sent to the supplicant by encrypting it with KEK. Message 3 is unicast.

M4 Message: With the message 4, The 4-way handshake procedure is completed. The message 4 would is unicast.

Once the 4-way handshake is completed successfully virtual control port which blocks all the traffic will be open and now encrypted traffic can flow. Now all unicast traffic will be encrypted with PTK, and all multicast traffic will be encrypted via GTK which created in the 4-way handshake process.

WI-FI PROTECTED ACCESS 2 (WPA2):

In 2004, Wi-Fi Protected Access 2 became available. WPA2 has stronger security and is easier to configure than the prior options It provides stronger data protection and more control over network access.

WPA2 replaces TKIP in WPA with Counter mode Cipher block chaining Message authentication Code Protocol (CCMP).

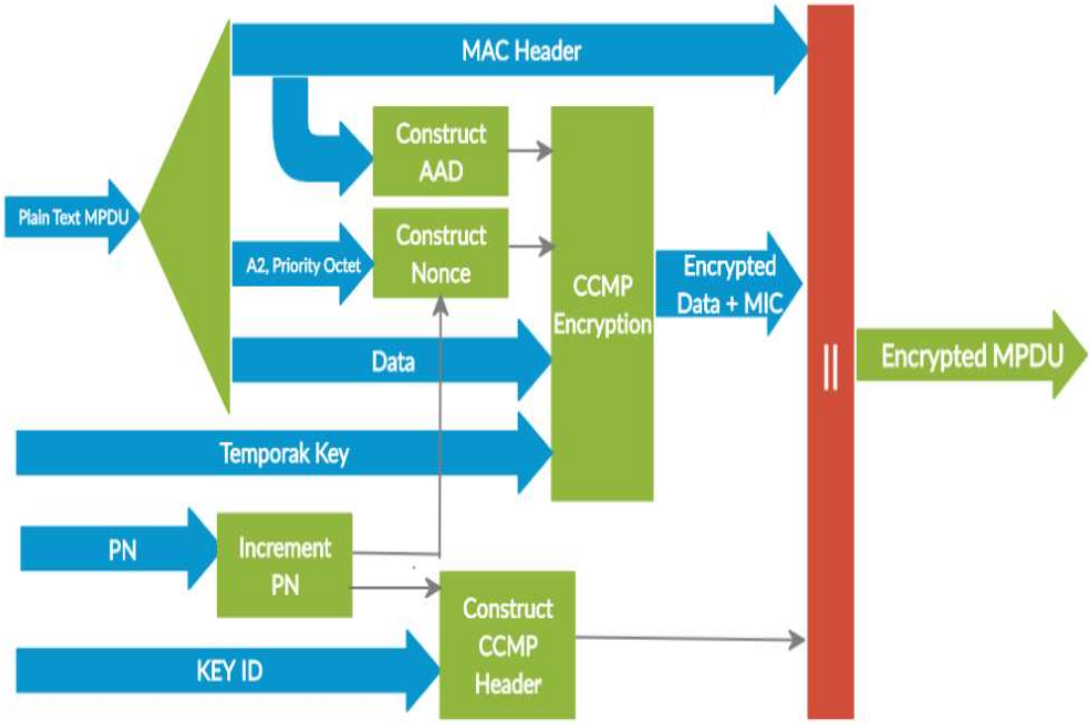
WPA2 supports 802.1X/EAP authentication or pre-shared keys and is backward compatible with WPA.

DIFFERENCE BETWEEN WPA AND WPA2:

	WPA	WPA2
Year it became available	2003	2004
Encryption method	Temporal Key Integrity Protocol (TKIP)	Advanced Encryption Standard (AES)
Security strength	Stronger than WEP, offers basic security	Stronger than WPA, offers increased security
Device support	Can support older software	Only compatible with newer software
Password length	Shorter password required	Longer password required

The WPA2 uses the CCMP protocol to provide integrity, security and encryption for the data that is to be transferred over the network.

CCMP ENCRYPTION PROCESS:



CCMP explained below:

CCMP:

- Counter mode (CTR) with the Cipher-Block Chaining Message Authentication Code (CBC-MAC) protocol.
- CCMP is based on the CCM of the AES encryption algorithm.
- CCM combines CTR to provide data confidentiality and CBC-MAC for authentication and integrity.
- CCM protects the integrity of both the MPDU data field and selected portions of the IEEE 802.11 MPDU header.

CCMP encrypts the payload of a plain-text MPDU using the following steps:

1. A 48-bit packet number (PN) is created. Packet numbers increment with each individual MPDU.A nonce is created from the packet number (PN), transmitter address (TA), and priority data used in QoS.

2. Certain fields in the MPDU header are used to construct the additional authentication data (AAD). This information is used for data integrity of portions of the MAC header.

3. The MIC provides integrity protection for these fields in the MAC header as well as for the frame body. All the MAC addresses, including the BSSID, are protected. Portion of the other fields of the MAC header are also protected.

4. The 8-octet CCMP header is constructed. The CCMP header includes the Key ID and the packet (PN), which is divided into 6 octets

5. The 128-bit temporal key, the nonce, the AAD, and the plain-text data are then processed to create an 8-byte MIC.

6. The MSDU payload of the frame body and the MIC are then encrypted in 128-bit blocks. This process is known as CCM originator processing.

7. The original MAC header is appended to the CCMP header, the encrypted MSDU, and the encrypted MIC.

8. A frame check sequence is calculated over all the fields of the header and entire frame body.

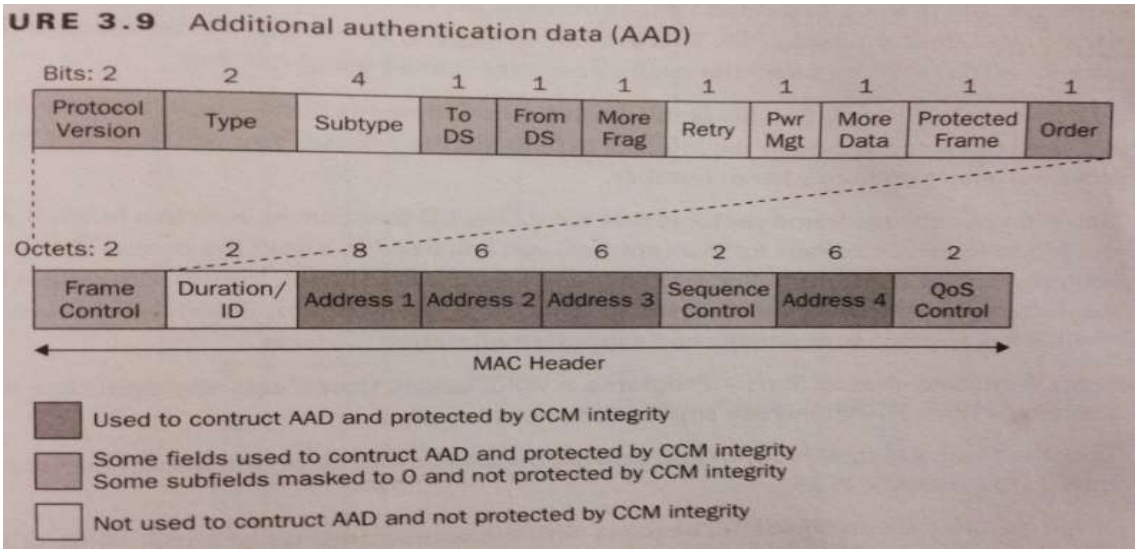
AAD (Additional Authentication Data):

Rules Involved in Constructing the AAD:

Below are the rules to generate the AAD:

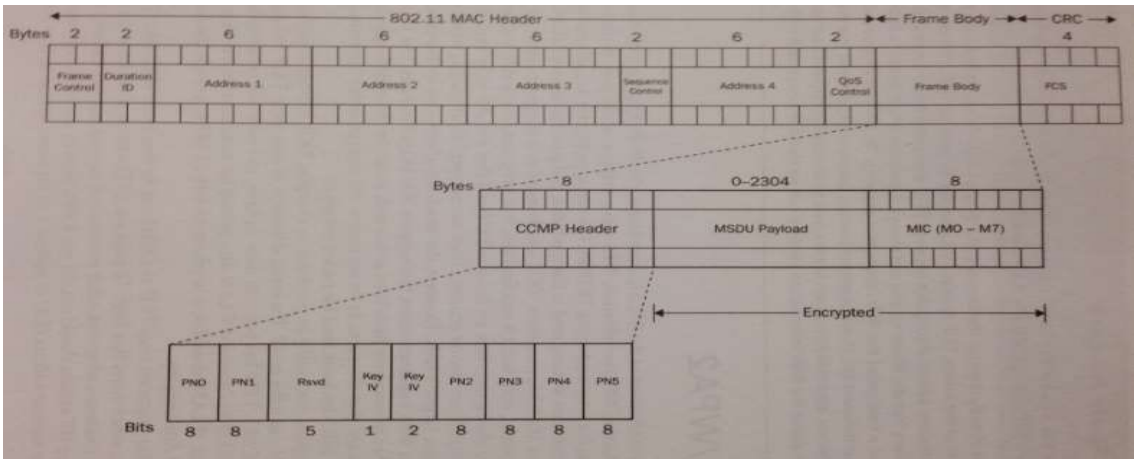
- FC – MPDU Frame Control field, with
    - Subtype bits (bits 4 5 6) masked to 0
    - Retry bit (bit 11) masked to 0
    - Pwr Mgt bit (bit 12) masked to 0
    - More Data bit (bit 13) masked to 0
    - Protected Frame bit (bit 14) always set to 1
- A1 – MPDU Address 1 field.
- A2 – MPDU Address 2 field.
- A3 – MPDU Address 3 field.
- SC – MPDU Sequence Control field, with the Sequence Number subfield (bits 4–15 of the Sequence Control field) masked to 0. The Fragment Number subfield is not modified.
- A4 – MPDU Address field, if present in the MPDU.
- QC – QoS Control field, if present, a 2-octet field that includes the MSDU priority. The QC TID is used in the construction of the AAD, and the remaining

AAD DIAGRAM:



CCMP MPDU IS SHOWN BELOW:

- Constructing the CCMP Header:
- 8 octets for the CCMP Header field and 8 octets for the MIC field.
- The CCMP Header field is constructed from the PN, ExtIV, and Key ID subfields as shown in the Figure 3.
- PN is a 48-bit PN represented as an array of 6 octets. PN5 is the most significant octet of the PN, and PN0 is the least significant.
- The ExtIV subfield (bit 5) of the Key ID octet signals that the CCMP
- Header field, The ExtIV bit (bit 5) is always set for 1 in CCMP.
- Bits 6–7 of the Key ID octet are for the Key ID subfield.
- The reserved bits shall be set to 0 and shall be ignored on reception.



Links Referred:

https://mrncciew.com/2014/08/19/cwsp-ccmp-encryption-method/

https://www.wifi-professionals.com/2019/01/4-way-handshake

Book Referred: CWAP