WPA2 / 802.11i

Network Security - Lecture 4

Ruxandra F. Olimid

Faculty of Mathematics and Computer Science, University of Bucharest

*slides adapted from the course TTM4137 thought at NTNU

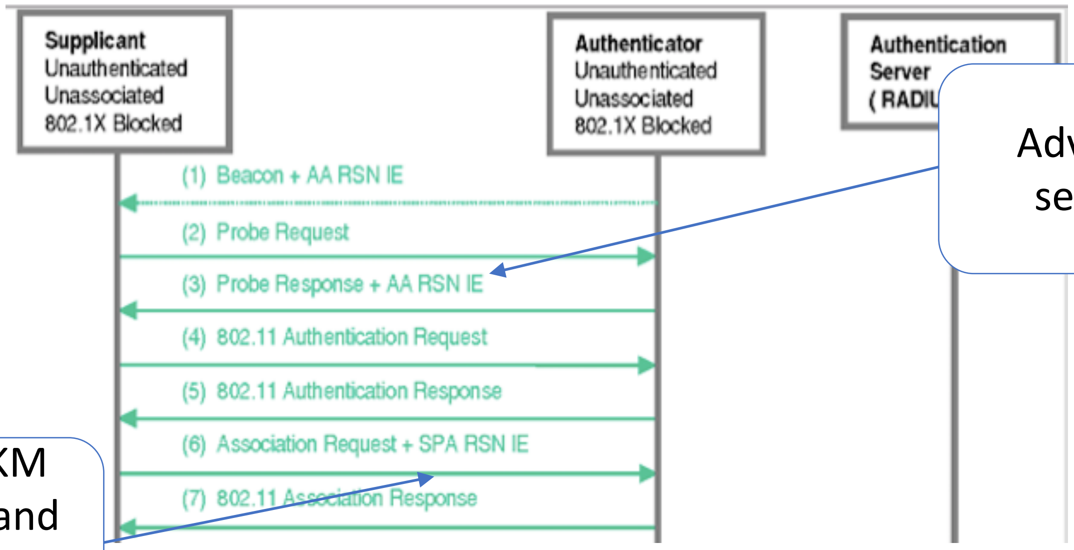
Outline

- RNS
- CCMP
- Key Hierarchy
- Security / Attacks

Robust Security Network (RSN)

RSN: a protocol for establishing a secure communication over 802.11 wireless networks

RSN Information Element (IE): data structure for advertising and negotiating security capabilities



Advertise WLAN security policy

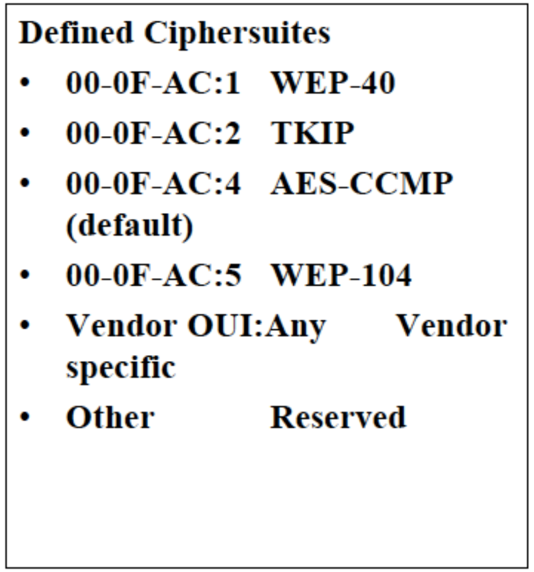
Select cipher, AKM (Authentication and Key Management) suite from advertised

[Source: He and Mitchell Security Analysis and Improvements for IEEE 802.11i https://theory.stanford.edu/~jcm/papers/NDSS05.pdf]

Robust Security Network (RSN)

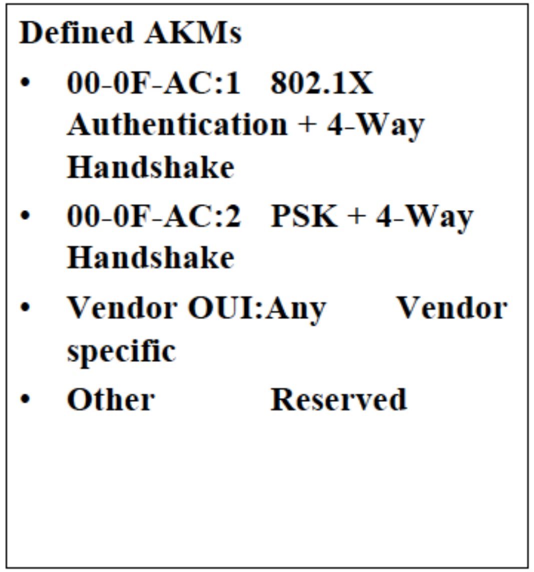
Backward compatibility with WEP!

If the cryptosystems are broken, easily change to new ones!



Defined Ciphersuites

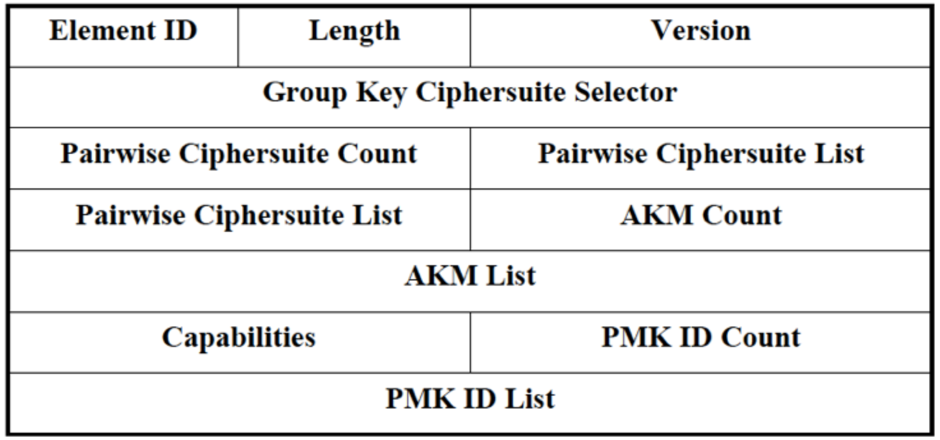
- 00-0F-AC:1 WEP-40
- 00-0F-AC:2 TKIP
- 00-0F-AC:4 AES-CCMP (default)
- 00-0F-AC:5 WEP-104
- Vendor OUI:Any Vendor specific
- Other Reserved



Defined AKMs

- 00-0F-AC:1 802.1X Authentication + 4-Way Handshake
- 00-0F-AC:2 PSK + 4-Way Handshake
- Vendor OUI:Any Vendor specific
- Other Reserved

RSN IE



<table>
<tr><td>Element ID</td><td>Length</td><td colspan="2">Version</td></tr>
<tr><td colspan="4">Group Key Ciphersuite Selector</td></tr>
<tr><td colspan="2">Pairwise Ciphersuite Count</td><td colspan="2">Pairwise Ciphersuite List</td></tr>
<tr><td colspan="2">Pairwise Ciphersuite List</td><td colspan="2">AKM Count</td></tr>
<tr><td colspan="4">AKM List</td></tr>
<tr><td colspan="2">Capabilities</td><td colspan="2">PMK ID Count</td></tr>
<tr><td colspan="4">PMK ID List</td></tr>
</table>

[Source: 802.11i Overview doc.: IEEE 802.11-04/0123r1]

Security Goals

Tries to address all known WEP Problems

- Reply detection

  Packet Number (PN), replay counter

- Key management protocols

  Similar to WPA, discussed in more details

- Access control

  Uses **802.1X architecture**

Security Goals

Tries to address all known WEP Problems

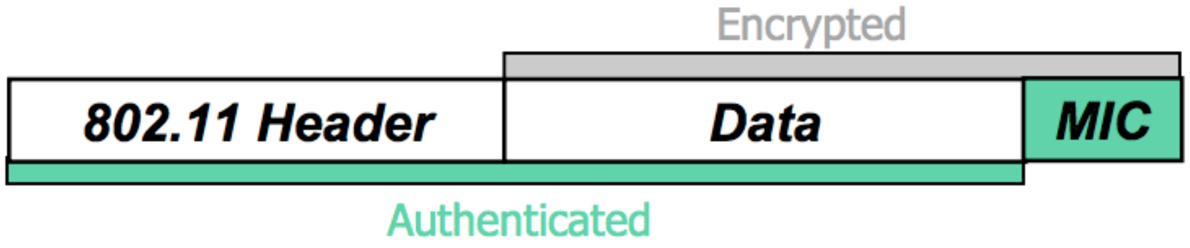
Authenticated encryption using CTR mode and CBC-MAC assumes 128-bit blocks and a single crypto key

- Confidentiality

  Uses **Advanced Encryption Standard (AES)**, instead of RC4

- Message integrity and authentication

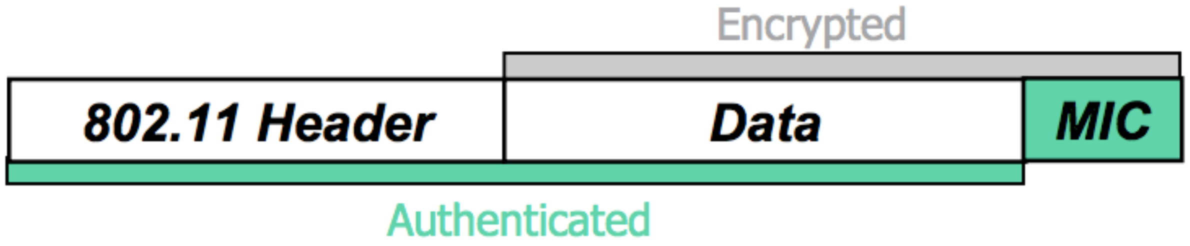
  Uses 128 bits **Counter Mode with CBC-MAC Protocol (CCMP)**



[Source: IEEE 802.11i Overview http://ieee802.org/16/liaison/docs/80211-05_0123r1.pdf]

CCM Mode

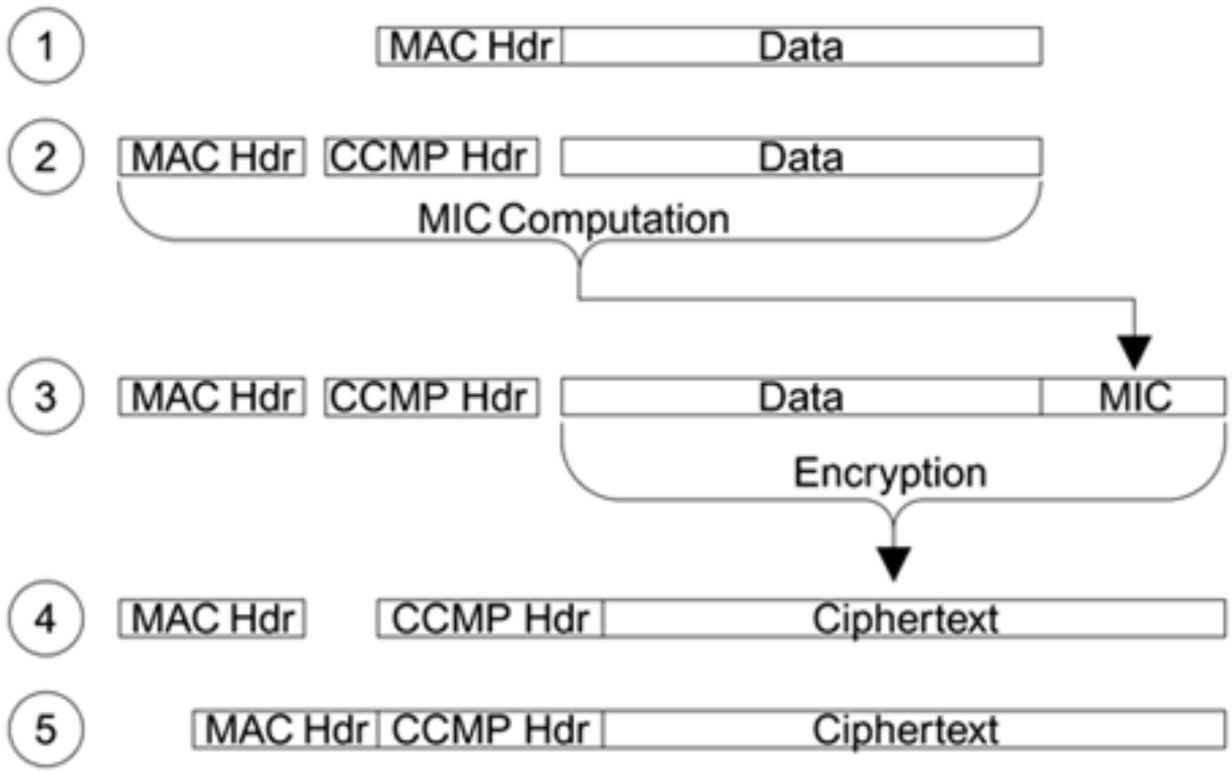
- Authenticated encryption (with associated data) combining CTR mode and CBC-MAC:
  - appends a CBC-MAC on the header, length of the header and plaintext
  - encrypts in CTR mode (plaintext blocks with 1,2,3… and MIC with counter value 0)
- Uses a single crypto key (temporal key shared by STA and AP) and assumes 128-bit blocks



[Source: IEEE 802.11i Overview http://ieee802.org/16/liaison/docs/80211-05_0123r1.pdf]

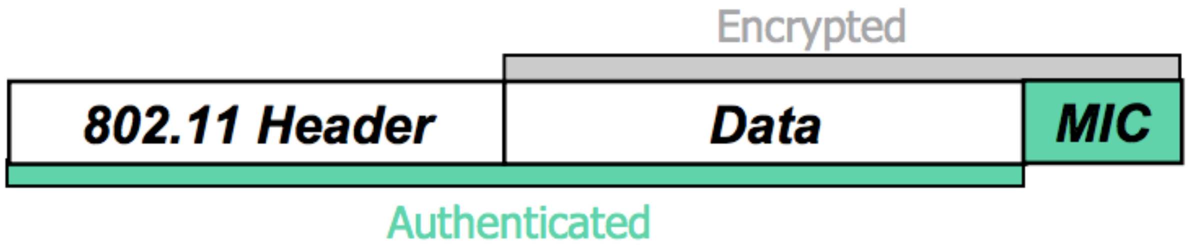
CCM Mode

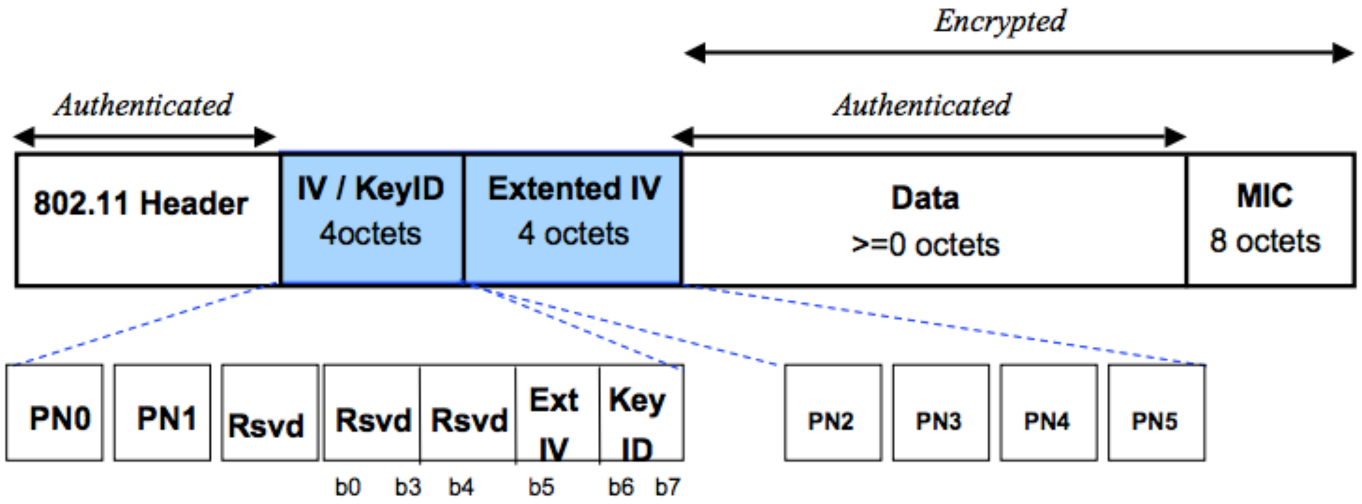
1) Unencrypted MPDU; MAC header contains source and destination addresses;
2) CCMP header (32 bits) is constructed
3) MIC is computed to protect fields from the MAC header, the CCMP header and the data
4) Data and MIC are encrypted; CCMP header is pre-appended
5) MAC header is pre-appended



[Source: Course book, Edney &Arbaugh, Chapter 12]

CCMP MPDU Format

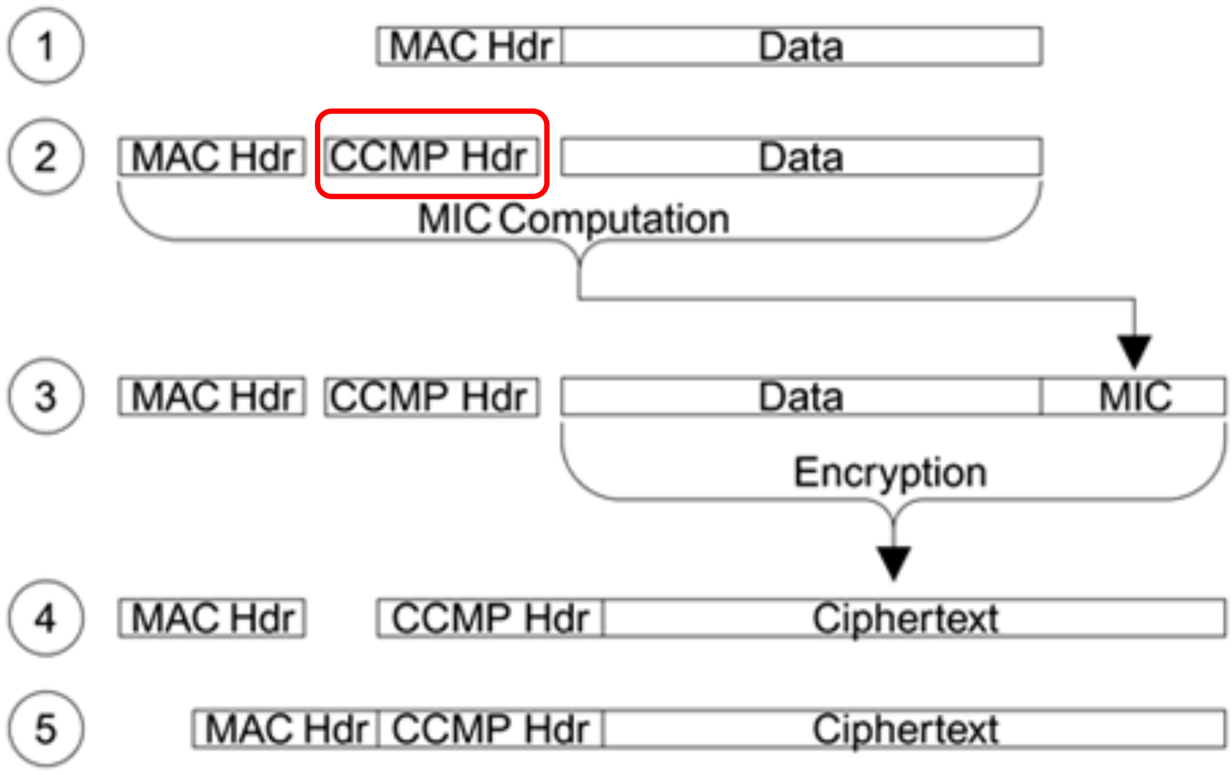




[Source: IEEE 802.11i Overview http://ieee802.org/16/liaison/docs/80211-05_0123r1.pdf]

CCM Mode

1) Unencrypted MPDU; MAC header contains source and destination addresses;
2) CCMP header (32 bits) is constructed
3) MIC is computed to protect fields from the MAC header, the CCMP header and the data
4) Data and MIC are encrypted; CCMP header is pre-appended
5) MAC header is pre-appended



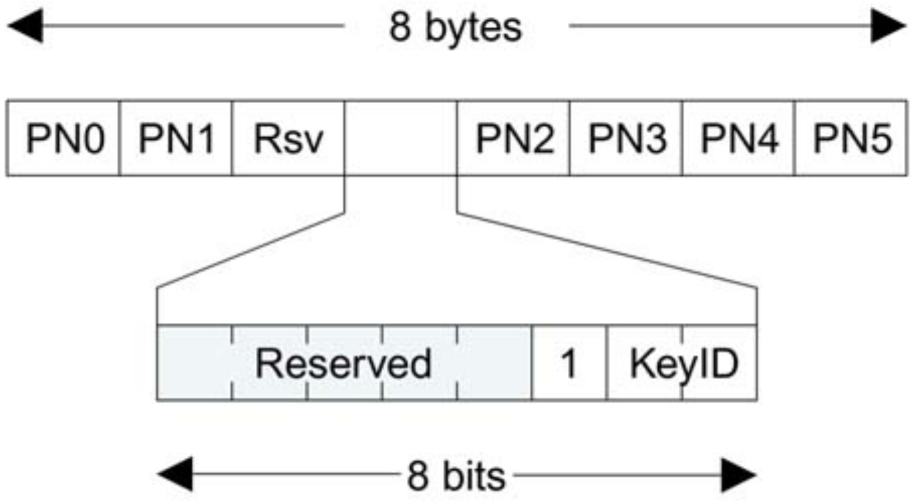
[Source: Course book, Edney &Arbaugh, Chapter 12]

CCMP Header

Purposes:

- Provides the Packet Number (PN) that provides replay protection and gives to the receiver the nonce required for decryption
- In case of multicast, it gives to the receiver the group key used for encryption

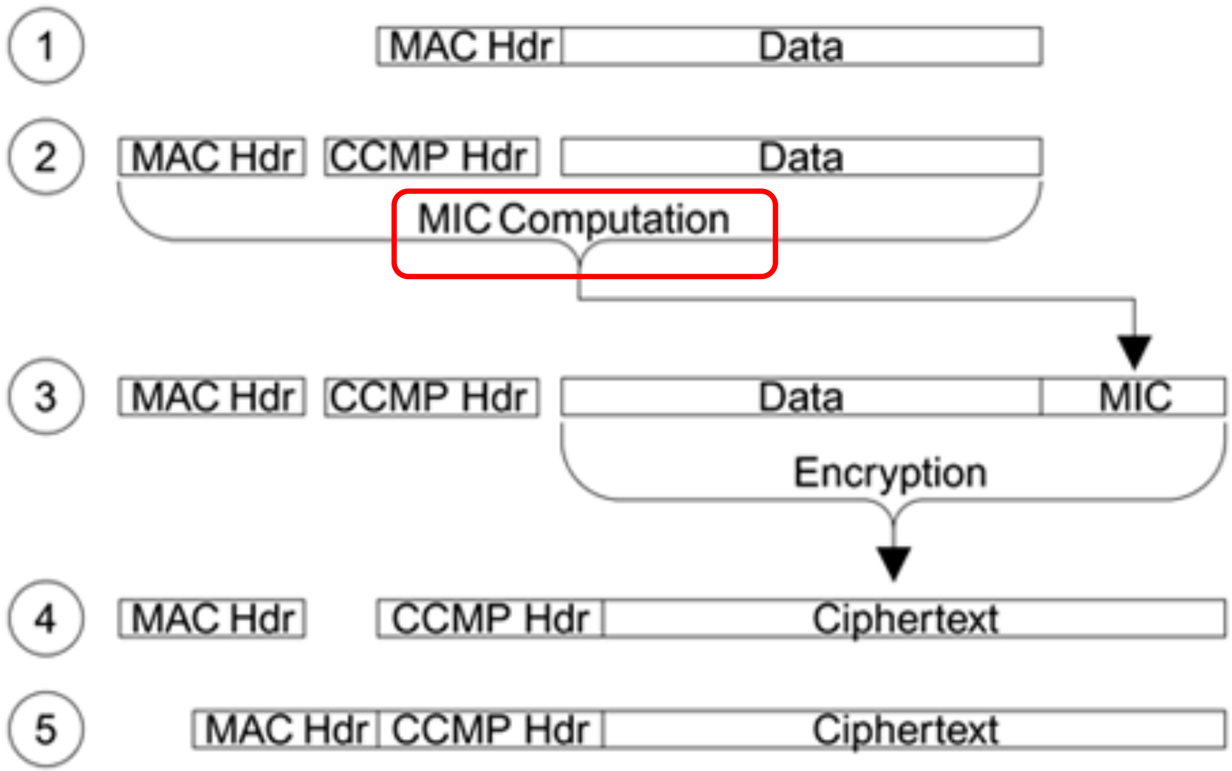
- Packet Number (PN): 48 bits (6 bytes)
- 1: indicates RSN
- KeyID: to select the group key id (from max.4 provisioned)



[Source: Course book, Edney &Arbaugh, Chapter 12]

CCM Mode

1) Unencrypted MPDU; MAC header contains source and destination addresses;
2) CCMP header (32 bits) is constructed
3) MIC is computed to protect fields from the MAC header, the CCMP header and the data
4) Data and MIC are encrypted; CCMP header is pre-appended
5) MAC header is pre-appended



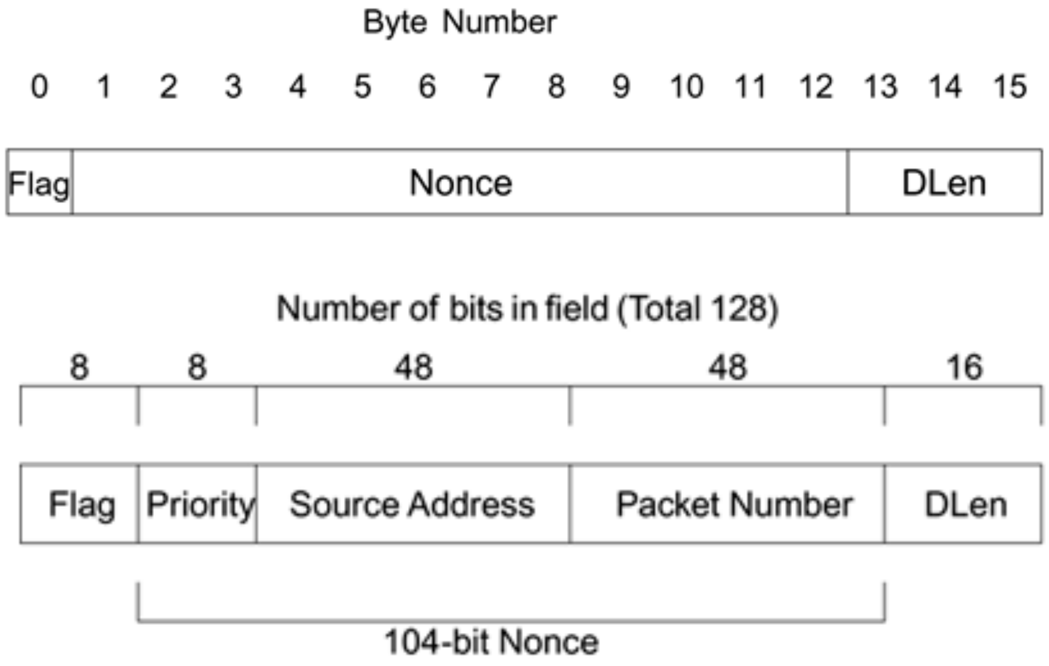
[Source: Course book, Edney &Arbaugh, Chapter 12]

MIC Computation

- Uses **CBC-MAC**, with a starting block – see CCMP Encapsulation slide
- 64-bit (8 bytes) MIC, so last 64 bits are discarded

Staring block (IV) is formed in a special way**:**

- **Flag: 01011001** (fixed)
- **Nonce:** contains both the PN and the source address to assure uniqueness (the PN could have been already used by one of the two communicating parties in another conversation); priority might refer to different streams (audio, video, etc.);
- **DLen**: length of the data



Byte Number

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Flag	Nonce												DLen		

Number of bits in field (Total 128)

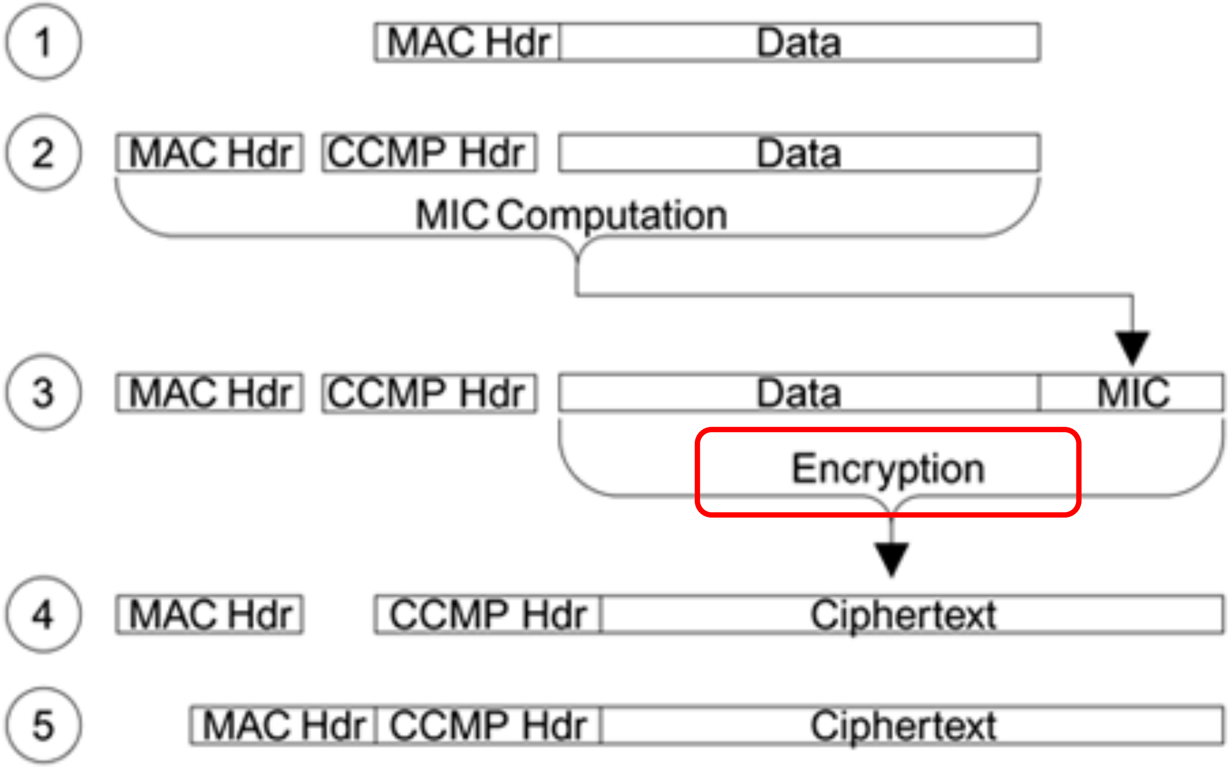
8	8	48	48	16
Flag	Priority	Source Address	Packet Number	DLen

104-bit Nonce

[Source: Course book, Edney &Arbaugh, Chapter 12]

CCM Mode

1) Unencrypted MPDU; MAC header contains source and destination addresses;
2) CCMP header (32 bits) is constructed
3) MIC is computed to protect fields from the MAC header, the CCMP header and the data
4) Data and MIC are encrypted; CCMP header is pre-appended
5) MAC header is pre-appended



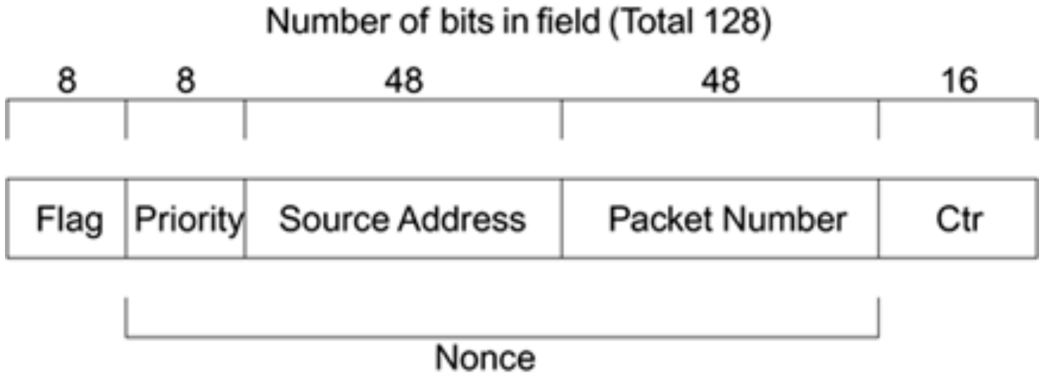
[Source: Course book, Edney &Arbaugh, Chapter 12]

Encryption

- Uses **CTR-AES**

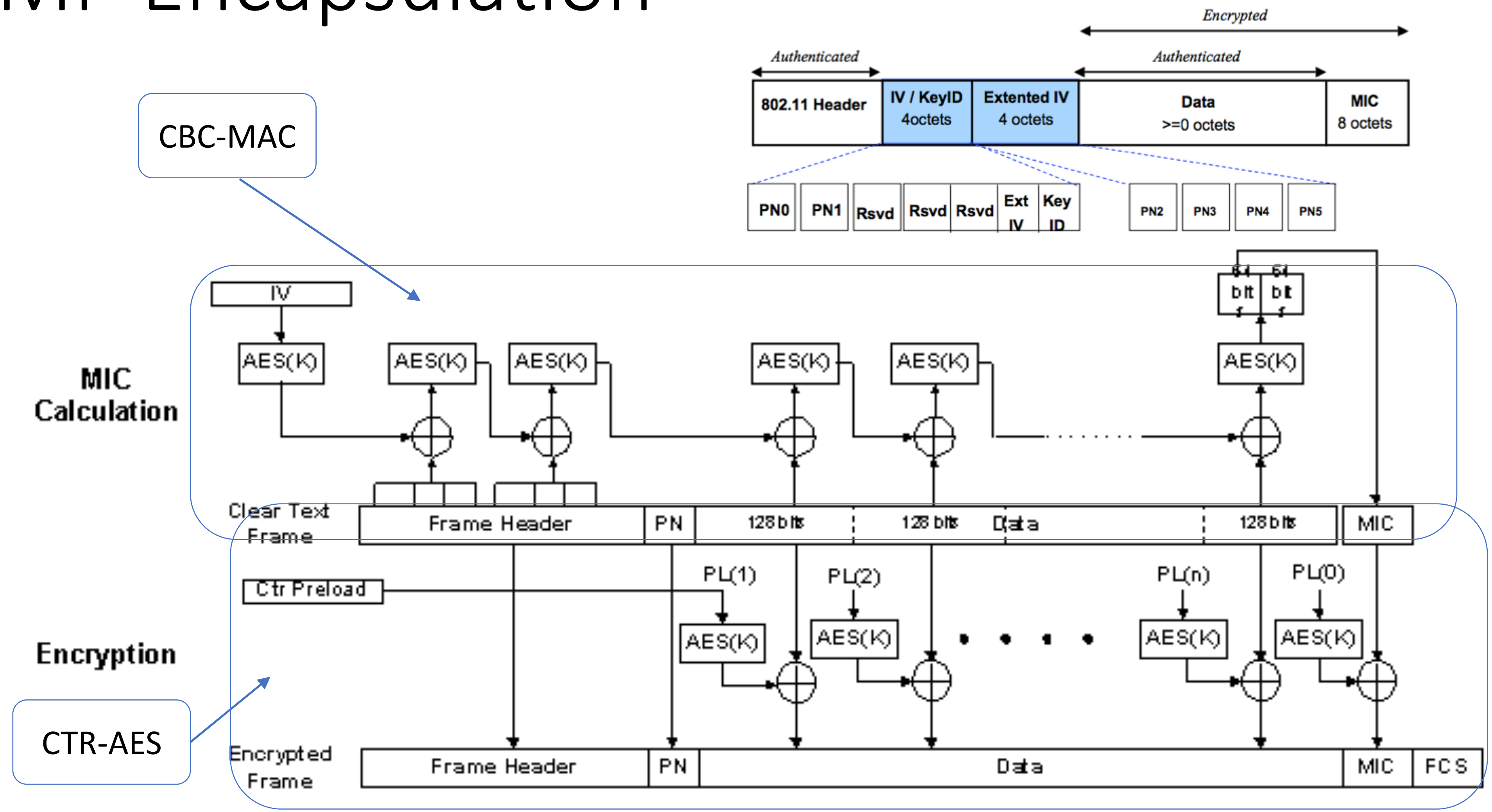
Counter block (PL0,PL1…):

- **Flag: 01011001** (fixed)
- **Nonce:** contains both the PN and the source address to assure uniqueness (the PN could have been already used by one of the two communicating parties in another conversation); priority might refer to different streams (audio, video, etc.);
- **Ctr**: starts at 1 and increases



[Source: Course book, Edney &Arbaugh, Chapter 12]

CCMP Encapsulation

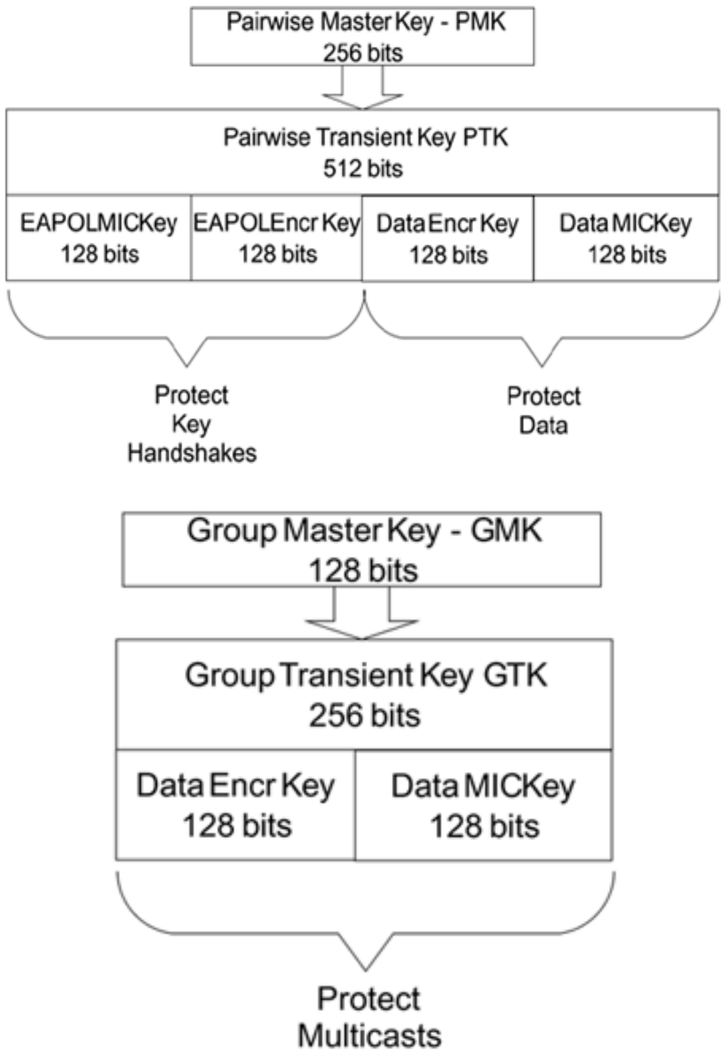


More details in the course book – Edney & Arbaugh, Chapter 12

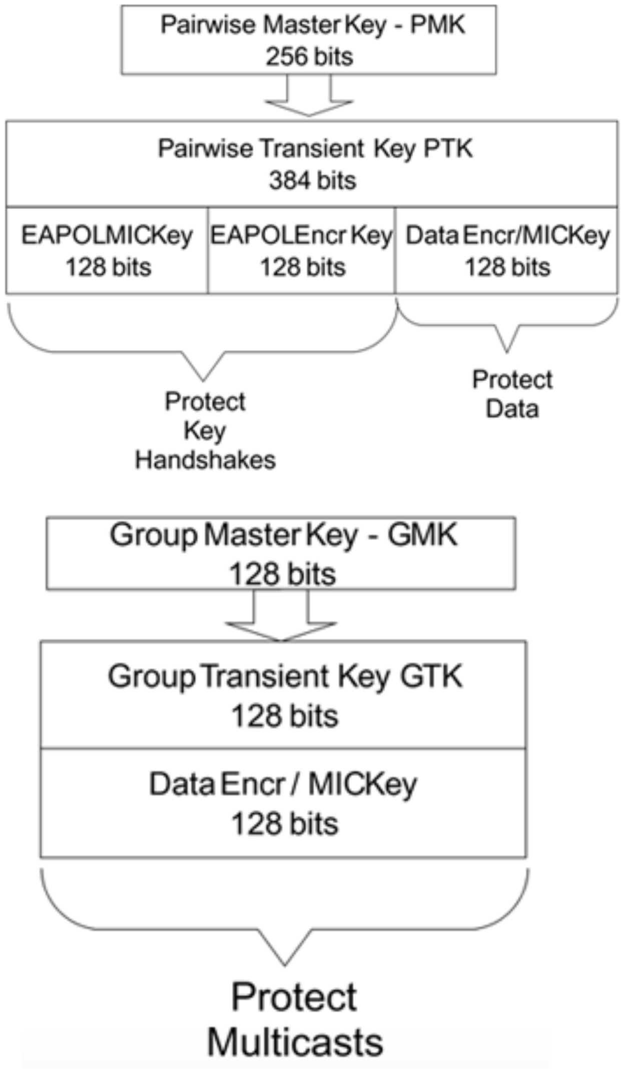
Key hierarchy (TKIP vs CCMP)

Pairwise

Group



TKIP

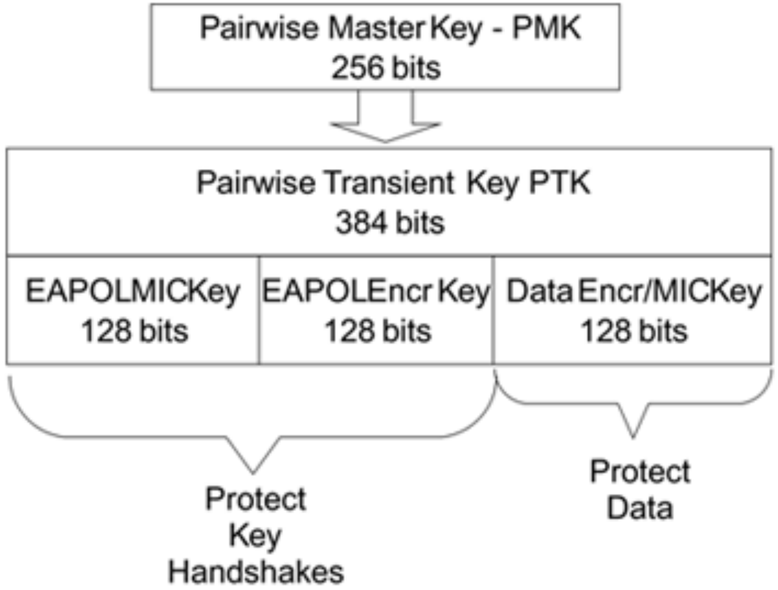


CCMP

[Source: Course book, Edney &Arbaugh, Chapter 10]

Pairwise CCMP Key Hierarchy

- Pairwise Master Key (PMK):
  - 256 bits, symmetric key
  - Preshared or server supplied by upper layers (e.g.: authentication server sends to AP)



[Source: Course book, Edney &Arbaugh, Chapter 10]

- Pairwise Transient Key (PTK):

$$PTK = f(PMK, NonceA, NonceB, A, B)$$

- Temporal Keys:
  - Up to 3 keys (128 bits):
    - EAPOL-keys: encryption key, integrity key
    - Data encryption and data integrity key (**a single key!**)

Group CCMP Key Hierarchy

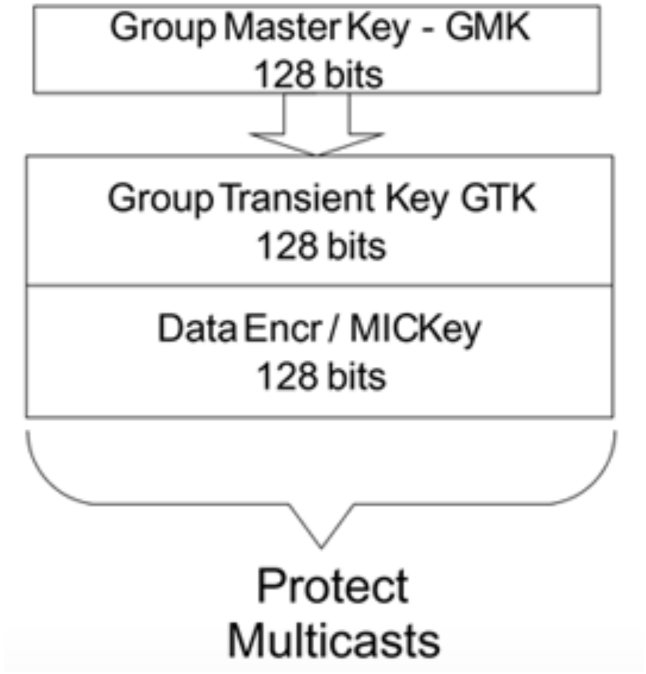
- Used for multi- and broadcast communication

- Group Master Key (GMK):
  - 256 bits, symmetric key
  - Generated by the AP

- Group Transient Keys (GTK):

  $$GTK = f(GMK, Nonce, AP)$$

- Temporal Key:
  - Encryption and integrity key 128 bits (**a single key!**)



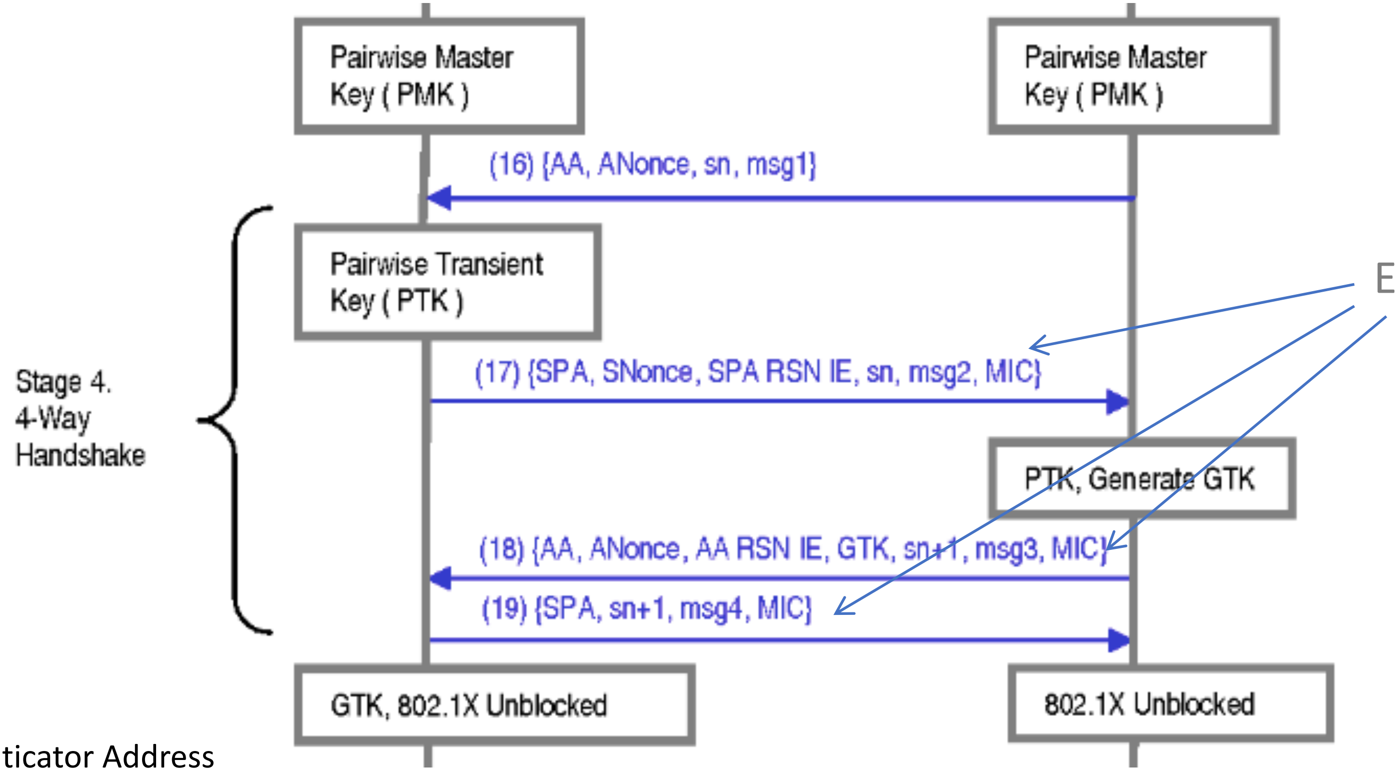
[Source: Course book, Edney &Arbaugh, Chapter 10]

802.11 Key Derivation Function (KDF)

$$\mathrm{PTK} \leftarrow \mathrm{KDF}(\mathrm{PMK}, \min\{Addr_{AP}, Addr_{STA}\} \,||\, \max\{Addr_{AP}, Addr_{STA}\}, \max\{N_{AP}, N_{STA}\}))$$

- KDF is based on **HMAC-SHA-1**

4-Way Handshake protocol


Pairwise Master Key (PMK)
Pairwise Master Key (PMK)
(16) {AA, ANonce, sn, msg1}
Pairwise Transient Key (PTK)
Stage 4. 4-Way Handshake
(17) {SPA, SNonce, SPA RSN IE, sn, msg2, MIC}
PTK, Generate GTK
(18) {AA, ANonce, AA RSN IE, GTK, sn+1, msg3, MIC}
(19) {SPA, sn+1, msg4, MIC}
GTK, 802.1X Unblocked
802.1X Unblocked

EAPOL MICKey
(KCK)

AA: Authenticator Address
SA: Supplicant Address
ANonce: nonce generated by the Authenticator (AP)
SNonce: nonce generated by the Supplicant (STA)
sn: sequence number

Encrypted data communication follows

[Source: He and Mitchell Security Analysis and Improvements for IEEE 802.11i https://theory.stanford.edu/~jcm/papers/NDSS05.pdf]

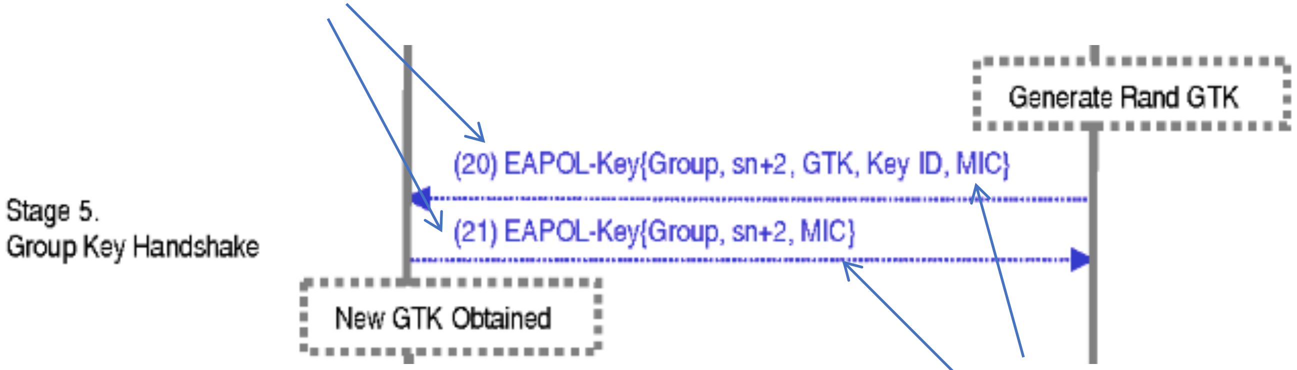
4WHS properties

- No forward secrecy
  - PMK + MACs + Nonces enough to derive PTK
  - Can decrypt old recorded communication sessions

- Vulnerable to dictionary attacks
  - If PMK derived from weak password
  - Capture MACs + Nonces → guess password → derive PMK

Group Key Generation and Distribution

EAPOL EncrKey (KEK)


Generate Rand GTK
(20) EAPOL-Key{Group, sn+2, GTK, Key ID, MIC}
Stage 5.
Group Key Handshake
(21) EAPOL-Key{Group, sn+2, MIC}
New GTK Obtained

EAPOL MICKey (KCK)

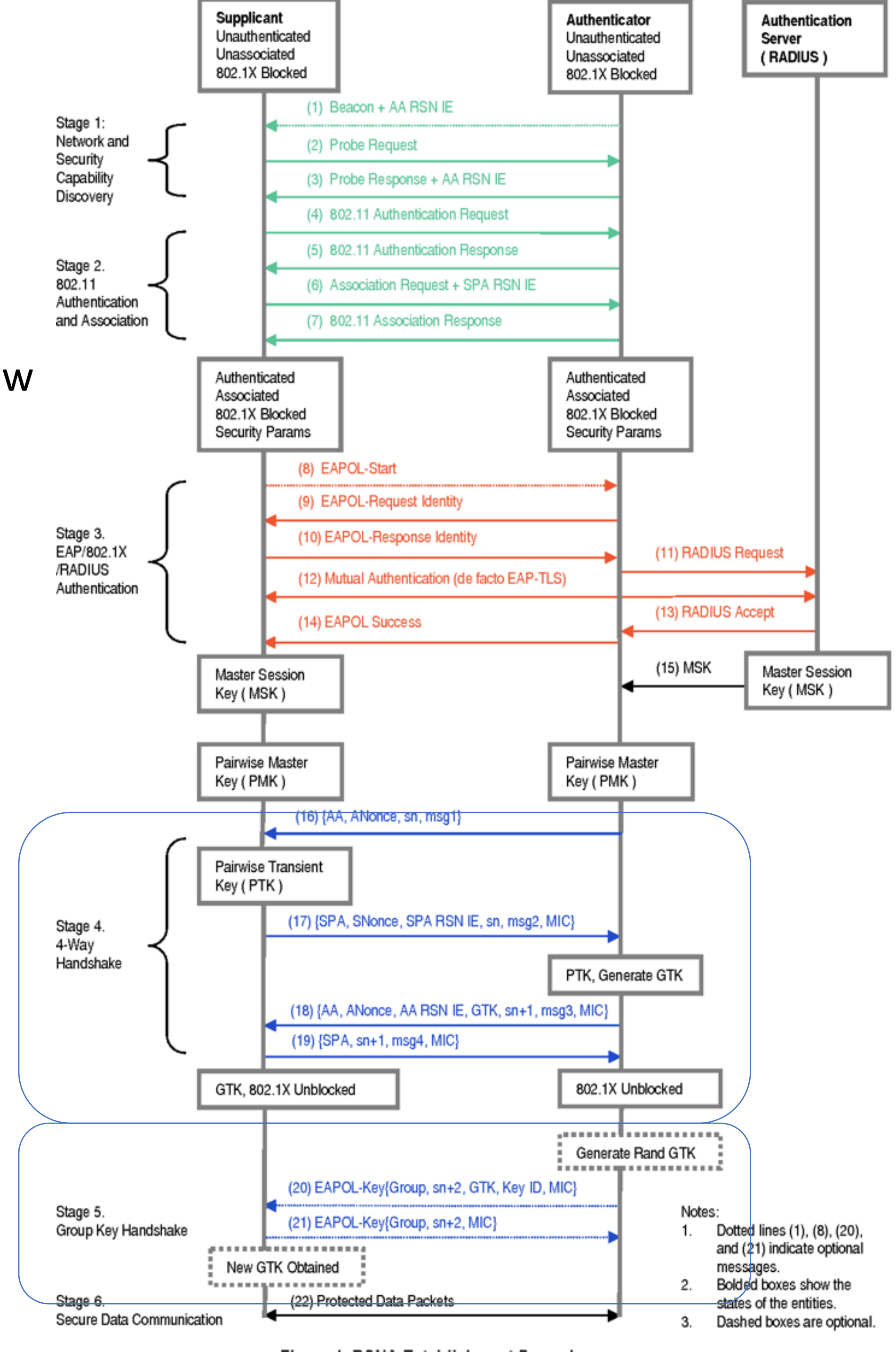
Encryption data communication follows

AA: Authenticator Address
SA: Supplicant Address
ANonce: nonce generated by the Authenticator (AP)
SNonce: nonce generated by the Supplicant (STA)
sn: sequence number

[Source: He and Mitchell Security Analysis and Improvements for IEEE 802.11i https://theory.stanford.edu/~jcm/papers/NDSS05.pdf]

RSN/WPA2

Association Overview



Supplicant
Unauthenticated
Unassociated
802.1X Blocked

Authenticator
Unauthenticated
Unassociated
802.1X Blocked

Authentication Server
(RADIUS)

Stage 1:
Network and Security Capability Discovery

(1) Beacon + AA RSN IE
(2) Probe Request
(3) Probe Response + AA RSN IE

Stage 2.
802.11 Authentication and Association

(4) 802.11 Authentication Request
(5) 802.11 Authentication Response
(6) Association Request + SPA RSN IE
(7) 802.11 Association Response

Authenticated
Associated
802.1X Blocked
Security Params

Authenticated
Associated
802.1X Blocked
Security Params

Stage 3.
EAP/802.1X /RADIUS Authentication

(8) EAPOL-Start
(9) EAPOL-Request Identity
(10) EAPOL-Response Identity
(11) RADIUS Request
(12) Mutual Authentication (de facto EAP-TLS)
(13) RADIUS Accept
(14) EAPOL Success

Master Session Key (MSK)

(15) MSK

Master Session Key (MSK)

Pairwise Master Key (PMK)

Pairwise Master Key (PMK)

Stage 4.
4-Way Handshake

(16) {AA, ANonce, sn, msg1}

Pairwise Transient Key (PTK)

(17) {SPA, SNonce, SPA RSN IE, sn, msg2, MIC}

PTK, Generate GTK

(18) {AA, ANonce, AA RSN IE, GTK, sn+1, msg3, MIC}
(19) {SPA, sn+1, msg4, MIC}

GTK, 802.1X Unblocked

802.1X Unblocked

Stage 5.
Group Key Handshake

Generate Rand GTK

(20) EAPOL-Key{Group, sn+2, GTK, Key ID, MIC}
(21) EAPOL-Key{Group, sn+2, MIC}

New GTK Obtained

Stage 6.
Secure Data Communication

(22) Protected Data Packets

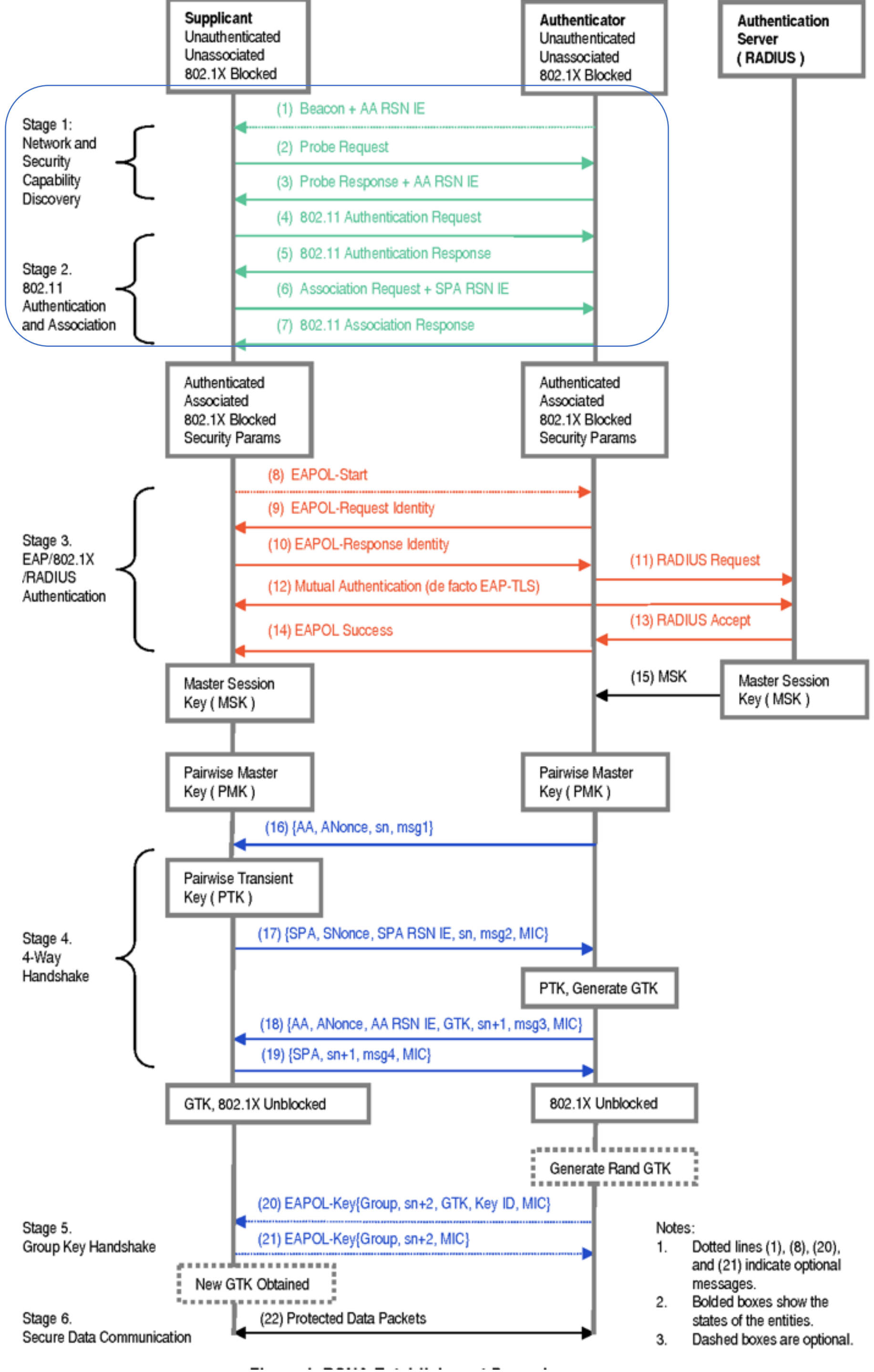
Notes:
1. Dotted lines (1), (8), (20), and (21) indicate optional messages.
2. Bolded boxes show the states of the entities.
3. Dashed boxes are optional.

RSN IE: RSN Identification Element (set of capabilities)
AA: Authenticator Address
SA: Supplicant Address
ANonce: nonce generated by the Authenticator (AP)
SNonce: nonce generated by the Supplicant (STA)

[Source: He and Mitchell Security Analysis and Improvements for IEEE 802.11i https://theory.stanford.edu/~jcm/papers/NDSS05.pdf]

RSN/WPA2

Association Overview


Supplicant
Unauthenticated
Unassociated
802.1X Blocked
Authenticator
Unauthenticated
Unassociated
802.1X Blocked
Authentication Server (RADIUS)
Stage 1: Network and Security Capability Discovery
(1) Beacon + AA RSN IE
(2) Probe Request
(3) Probe Response + AA RSN IE
Stage 2. 802.11 Authentication and Association
(4) 802.11 Authentication Request
(5) 802.11 Authentication Response
(6) Association Request + SPA RSN IE
(7) 802.11 Association Response
Authenticated
Associated
802.1X Blocked
Security Params
Authenticated
Associated
802.1X Blocked
Security Params
Stage 3. EAP/802.1X /RADIUS Authentication
(8) EAPOL-Start
(9) EAPOL-Request Identity
(10) EAPOL-Response Identity
(11) RADIUS Request
(12) Mutual Authentication (de facto EAP-TLS)
(13) RADIUS Accept
(14) EAPOL Success
Master Session Key (MSK)
(15) MSK
Master Session Key (MSK)
Pairwise Master Key (PMK)
Pairwise Master Key (PMK)
Stage 4. 4-Way Handshake
(16) {AA, ANonce, sn, msg1}
Pairwise Transient Key (PTK)
(17) {SPA, SNonce, SPA RSN IE, sn, msg2, MIC}
PTK, Generate GTK
(18) {AA, ANonce, AA RSN IE, GTK, sn+1, msg3, MIC}
(19) {SPA, sn+1, msg4, MIC}
GTK, 802.1X Unblocked
802.1X Unblocked
Generate Rand GTK
Stage 5. Group Key Handshake
(20) EAPOL-Key{Group, sn+2, GTK, Key ID, MIC}
(21) EAPOL-Key{Group, sn+2, MIC}
New GTK Obtained
Stage 6. Secure Data Communication
(22) Protected Data Packets

Notes:
1. Dotted lines (1), (8), (20), and (21) indicate optional messages.
2. Bolded boxes show the states of the entities.
3. Dashed boxes are optional.

RSN IE: RSN Identification Element (set of capabilities)
AA: Authenticator Address
SA: Supplicant Address
ANonce: nonce generated by the Authenticator (AP)
SNonce: nonce generated by the Supplicant (STA)

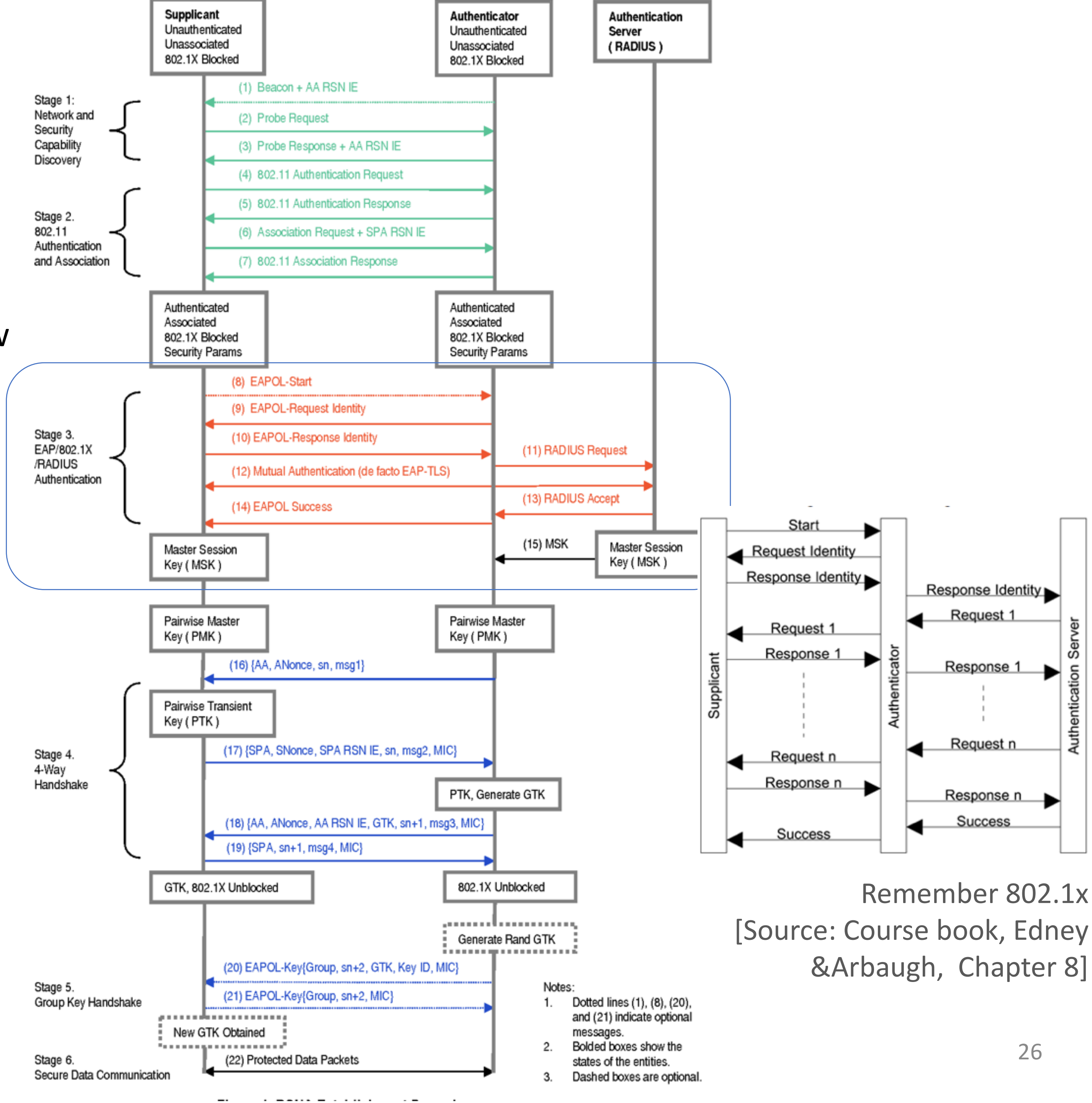
[Source: He and Mitchell Security Analysis and Improvements for IEEE 802.11i https://theory.stanford.edu/~jcm/papers/NDSS05.pdf]

RSN/WPA2

Association Overview

Both parties prove to know the same MSK

RSN IE: RSN Identification Element (set of capabilities)
AA: Authenticator Address
SA: Supplicant Address
ANonce: nonce generated by the Authenticator (AP)
SNonce: nonce generated by the Supplicant (STA)

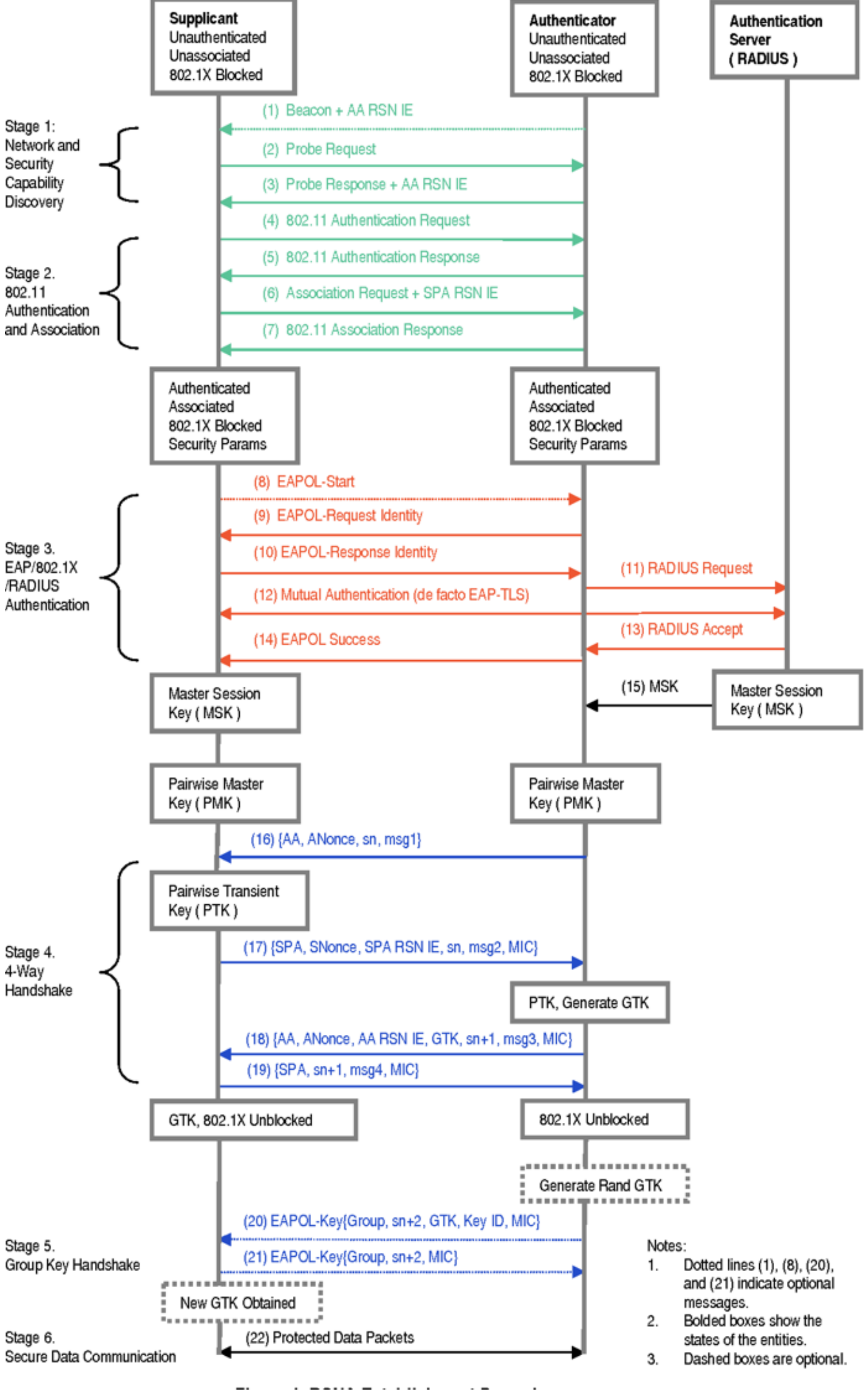

Supplicant
Unauthenticated
Unassociated
802.1X Blocked
Authenticator
Unauthenticated
Unassociated
802.1X Blocked
Authentication Server
(RADIUS)
Stage 1:
Network and Security Capability Discovery
(1) Beacon + AA RSN IE
(2) Probe Request
(3) Probe Response + AA RSN IE
Stage 2.
802.11 Authentication and Association
(4) 802.11 Authentication Request
(5) 802.11 Authentication Response
(6) Association Request + SPA RSN IE
(7) 802.11 Association Response
Authenticated
Associated
802.1X Blocked
Security Params
Authenticated
Associated
802.1X Blocked
Security Params
Stage 3.
EAP/802.1X /RADIUS Authentication
(8) EAPOL-Start
(9) EAPOL-Request Identity
(10) EAPOL-Response Identity
(11) RADIUS Request
(12) Mutual Authentication (de facto EAP-TLS)
(13) RADIUS Accept
(14) EAPOL Success
Master Session Key (MSK)
(15) MSK
Master Session Key (MSK)
Pairwise Master Key (PMK)
Pairwise Master Key (PMK)
(16) {AA, ANonce, sn, msg1}
Pairwise Transient Key (PTK)
Stage 4.
4-Way Handshake
(17) {SPA, SNonce, SPA RSN IE, sn, msg2, MIC}
PTK, Generate GTK
(18) {AA, ANonce, AA RSN IE, GTK, sn+1, msg3, MIC}
(19) {SPA, sn+1, msg4, MIC}
GTK, 802.1X Unblocked
802.1X Unblocked
Generate Rand GTK
Stage 5.
Group Key Handshake
(20) EAPOL-Key{Group, sn+2, GTK, Key ID, MIC}
(21) EAPOL-Key{Group, sn+2, MIC}
New GTK Obtained
Stage 6.
Secure Data Communication
(22) Protected Data Packets
Notes:
1. Dotted lines (1), (8), (20), and (21) indicate optional messages.
2. Bolded boxes show the states of the entities.
3. Dashed boxes are optional.
Supplicant
Authenticator
Authentication Server
Start
Request Identity
Response Identity
Response Identity
Request 1
Request 1
Response 1
Response 1
Request n
Request n
Response n
Response n
Success
Success

Remember 802.1x [Source: Course book, Edney &Arbaugh, Chapter 8]

RSN/WPA2

Association Overview

RSN IE: RSN Identification Element (set of capabilities)
AA: Authenticator Address
SA: Supplicant Address
ANonce: nonce generated by the Authenticator (AP)
SNonce: nonce generated by the Supplicant (STA)



Supplicant
Unauthenticated
Unassociated
802.1X Blocked
Authenticator
Unauthenticated
Unassociated
802.1X Blocked
Authentication Server (RADIUS)
Stage 1: Network and Security Capability Discovery
(1) Beacon + AA RSN IE
(2) Probe Request
(3) Probe Response + AA RSN IE
Stage 2. 802.11 Authentication and Association
(4) 802.11 Authentication Request
(5) 802.11 Authentication Response
(6) Association Request + SPA RSN IE
(7) 802.11 Association Response
Authenticated
Associated
802.1X Blocked
Security Params
Authenticated
Associated
802.1X Blocked
Security Params
Stage 3. EAP/802.1X /RADIUS Authentication
(8) EAPOL-Start
(9) EAPOL-Request Identity
(10) EAPOL-Response Identity
(11) RADIUS Request
(12) Mutual Authentication (de facto EAP-TLS)
(13) RADIUS Accept
(14) EAPOL Success
Master Session Key (MSK)
(15) MSK
Master Session Key (MSK)
Pairwise Master Key (PMK)
Pairwise Master Key (PMK)
Stage 4. 4-Way Handshake
(16) {AA, ANonce, sn, msg1}
Pairwise Transient Key (PTK)
(17) {SPA, SNonce, SPA RSN IE, sn, msg2, MIC}
PTK, Generate GTK
(18) {AA, ANonce, AA RSN IE, GTK, sn+1, msg3, MIC}
(19) {SPA, sn+1, msg4, MIC}
GTK, 802.1X Unblocked
802.1X Unblocked
Generate Rand GTK
Stage 5. Group Key Handshake
(20) EAPOL-Key{Group, sn+2, GTK, Key ID, MIC}
(21) EAPOL-Key{Group, sn+2, MIC}
New GTK Obtained
Stage 6. Secure Data Communication
(22) Protected Data Packets
Notes:
1. Dotted lines (1), (8), (20), and (21) indicate optional messages.
2. Bolded boxes show the states of the entities.
3. Dashed boxes are optional.

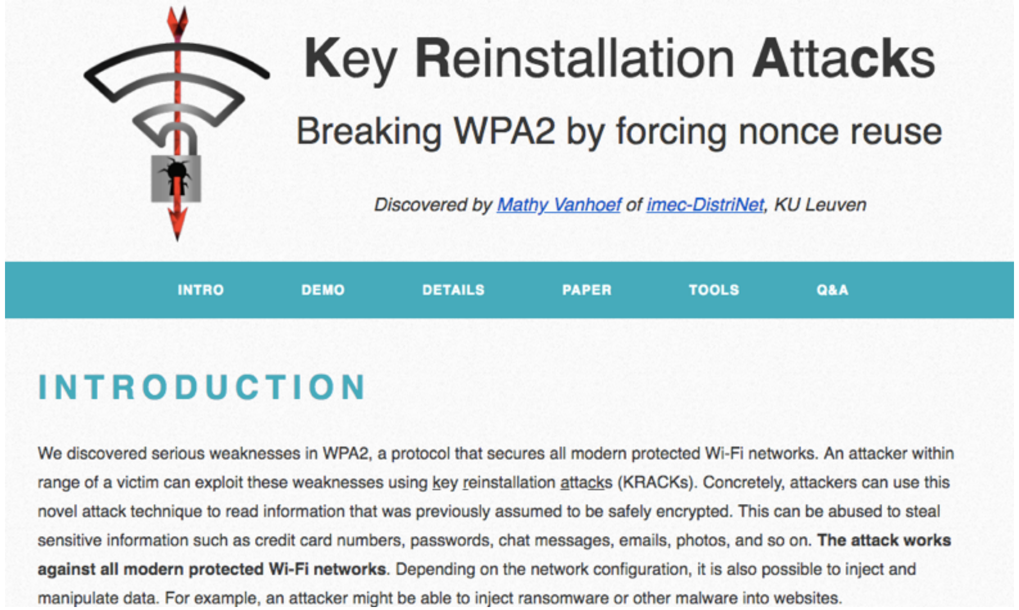
[Source: He and Mitchell Security Analysis and Improvements for IEEE 802.11i https://theory.stanford.edu/~jcm/papers/NDSS05.pdf]

Security / Attacks

- CCM Mode: theoretical security proof

[Jonsson, J. (2003, January). On the security of CTR+ CBC-MAC. In SelectedAreas in Cryptography(pp. 76-93). Springer Berlin Heidelberg]

- In practice: does the security proof model applies to the protocol?



Key Reinstallation Attacks

Breaking WPA2 by forcing nonce reuse

Discovered by Mathy Vanhoef of imec-DistriNet, KU Leuven

INTRODUCTION

We discovered serious weaknesses in WPA2, a protocol that secures all modern protected Wi-Fi networks. An attacker within range of a victim can exploit these weaknesses using key reinstallation attacks (KRACKs). Concretely, attackers can use this novel attack technique to read information that was previously assumed to be safely encrypted. This can be abused to steal sensitive information such as credit card numbers, passwords, chat messages, emails, photos, and so on. **The attack works against all modern protected Wi-Fi networks**. Depending on the network configuration, it is also possible to inject and manipulate data. For example, an attacker might be able to inject ransomware or other malware into websites.

https://www.krackattacks.com/

Paper: https://papers.mathyvanhoef.com/ccs2017.pdf
Video: https://youtu.be/Oh4WURZoR98

WPA2

- We will look into WPA3 next time