Wi-Fi Security

Halil Kemal TAŞKIN

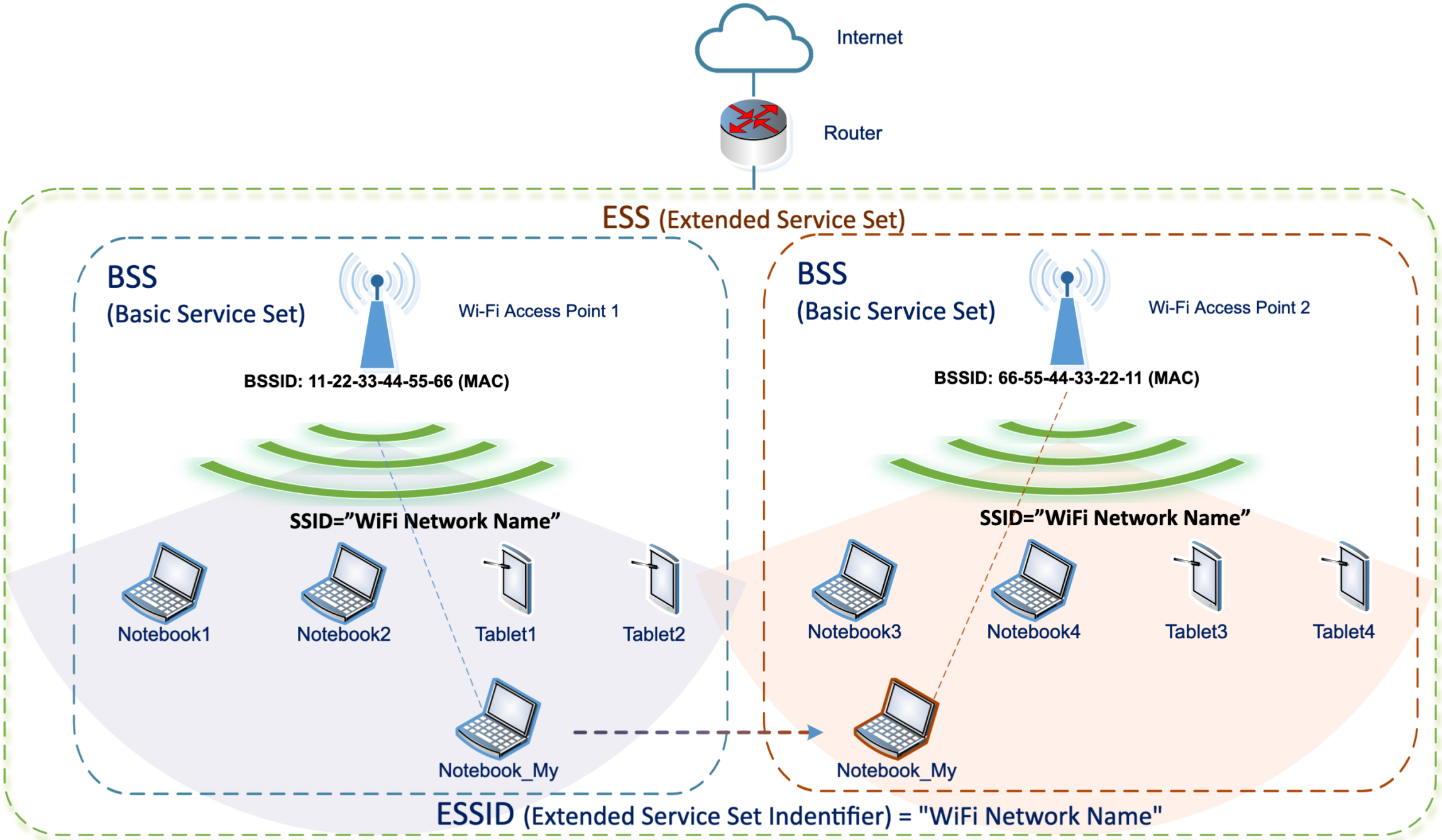
Wi-Fi

- Wi-Fi: Wireless Fidelity
- Introduced in September 1997
- Based on the IEEE 802.11 family of standards
- Commonly used for local area networking of devices and Internet access
- Designed to work seamlessly with Ethernet

Wi-Fi Generations

Generation	IEEE standard	Adopted	Maximum link rate (Mbit/s)	Radio frequency (GHz)
Wi-Fi 7	802.11be	(2024)	1.376 to 46.120	2.4 / 5 / 6
Wi-Fi 6E	802.11ax	2020	574 to 9.608	6
Wi-Fi 6		2019		2.4 / 5
Wi-Fi 5	802.11ac	2014	433 to 6.933	5
Wi-Fi 4	802.11n	2008	72 to 600	2.4 / 5
Wi-Fi 3	802.11g	2003	6 to 54	2.4
Wi-Fi 2	802.11a	1999	6 to 54	5
Wi-Fi 1	802.11b	1999	1 to 11	2.4
Wi-Fi 0	802.11	1997	1 to 2	2.4

Source: Wikipedia



Source: Wikipedia

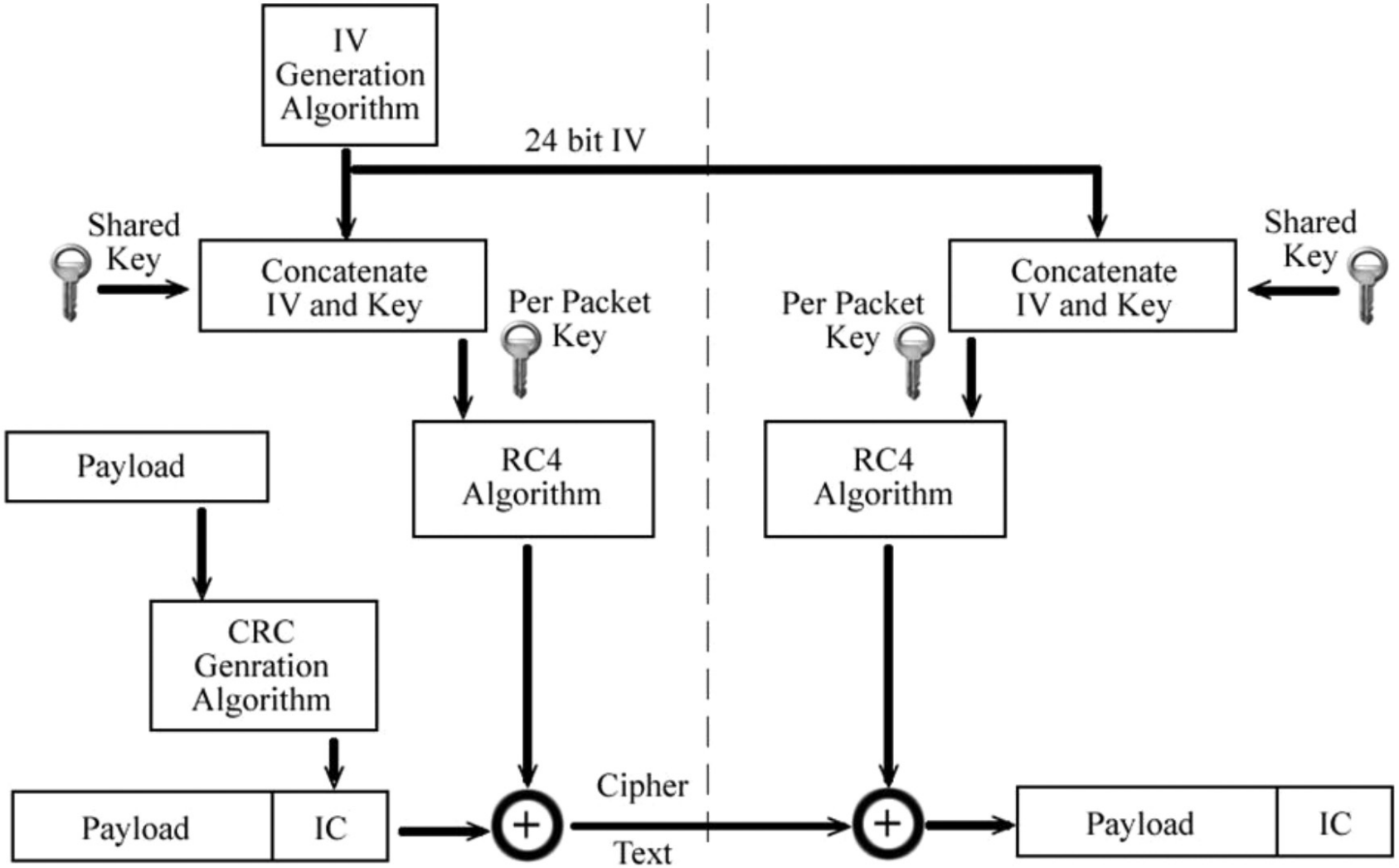
Wi-Fi Security

- Encryption Protocols
  - None / Open Access
  - WEP
  - WPA
  - WPA2
  - WPA3

WEP: Wired Equivalent Privacy

- Introduced as part of the original IEEE 802.11 standard in 1997.
- Two key sizes: 40-bit (WEP-40) and 104-bit (WEP-104).
- Uses RC4 Stream Cipher to ensure confidentiality of the data transmitted.
- Uses CRC-32 Checksum to ensure integrity of the data transmitted.
- Broken and deprecated in 2004.
- Known Attacks:
  - FMS (Fluhrrer, Mantin and Shamir) Attack, 2001
  - KoreK Attack, 2004
  - ChopChop Attack, 2004
  - Fragmentation Attack, 2005,
  - PTW (Pychkine, Tews, Weinmann) Attack, 2007

WEP Encryption and Decryption



WPA: Wi-Fi Protected Access

- Became available in 2003.
- Replacement to the WEP.
- Improved key sizes.
- Uses Message Integrity Check (MIC) protocol for integrity.
- Known Attacks:
  - Back and Tews' Improved Attack on RC4, 2008
  - Ohigashi-Morii Attack, 2009
  - Michael Attacks, 2010
  - The Hole196 Vulnerability, 2010
  - Dictionary Attack against the 4-way handshake

WPA2

- Became available in 2006.
- WPA2 replaced WPA.
- Improved encryption protocol.
- Known attacks:
  - KRACK Attack
  - PMKID Attack (PSK)
  - WPS Attack
  - The Hole196 Vulnerability, 2010
  - Dictionary Attack against the 4-way handshake

WPA/WPA2 Modes

- WPA/WPA2 can be implemented in either of two modes:
  - **Personal or Pre-Shared Key (PSK) Mode**
    - Mostly suitable for home use.
    - Define an encryption passphrase on the wireless router.
    - The passphrase must be entered by users when connecting to the Wi-Fi network.
  - **Enterprise (EAP/RADIUS) Mode**
    - Provides the security needed for wireless networks in business environments.
    - Uses IEEE 802.1X Authentication Protocol.
    - Users are assigned login credentials they must present when connecting to the network.
    - Users never deal with the actual encryption keys.

TKIP vs CCMP

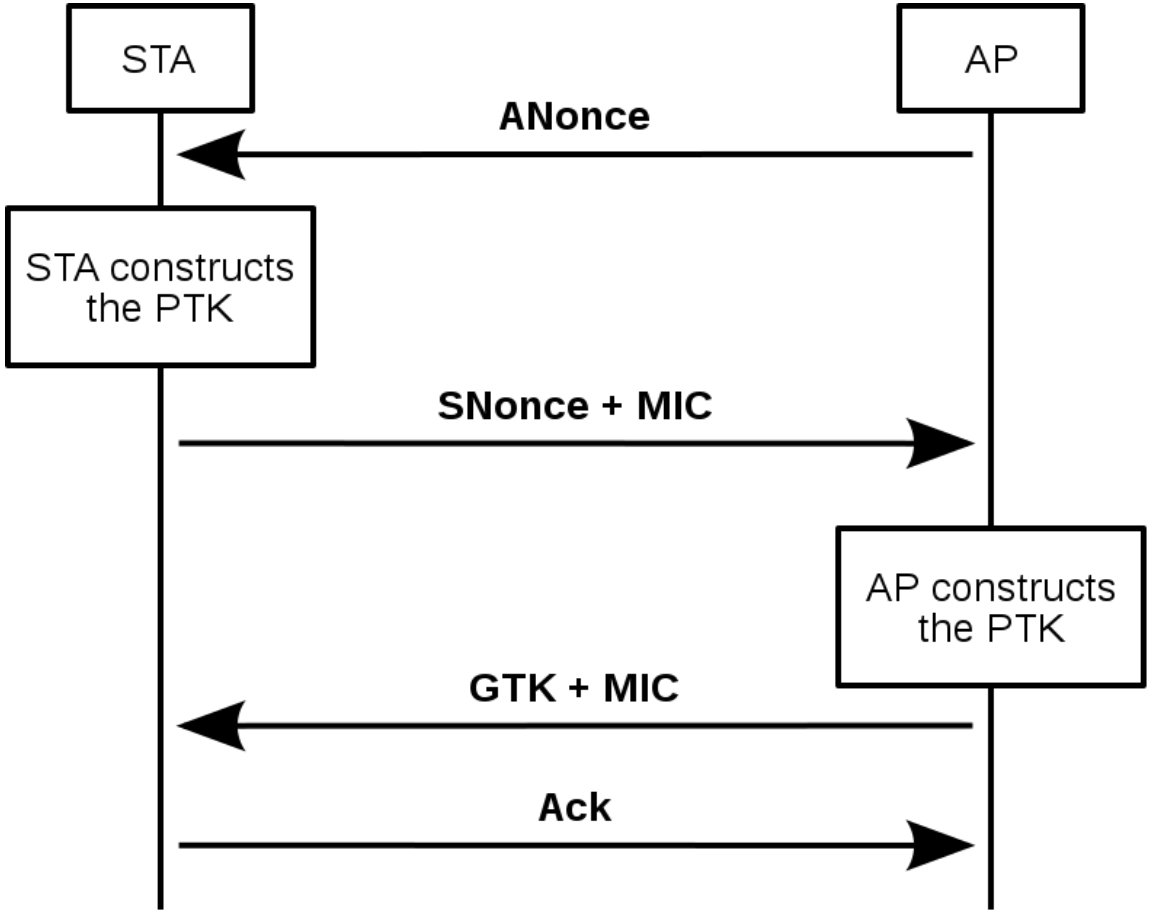
- TKIP: Temporal Key Integrity Protocol
  - Uses RC4 for encryption
  - WPA uses TKIP

- CCMP: Counter Mode CBC-MAC Protocol
  - Authenticated Encryption using AES algorithm
  - Uses Counter mode of operation for encryption
  - Uses CBC-MAC for authentication
  - WPA2 uses CCMP.

- Modes
  - WPA TKIP PSK
  - WPA2 CCMP PSK

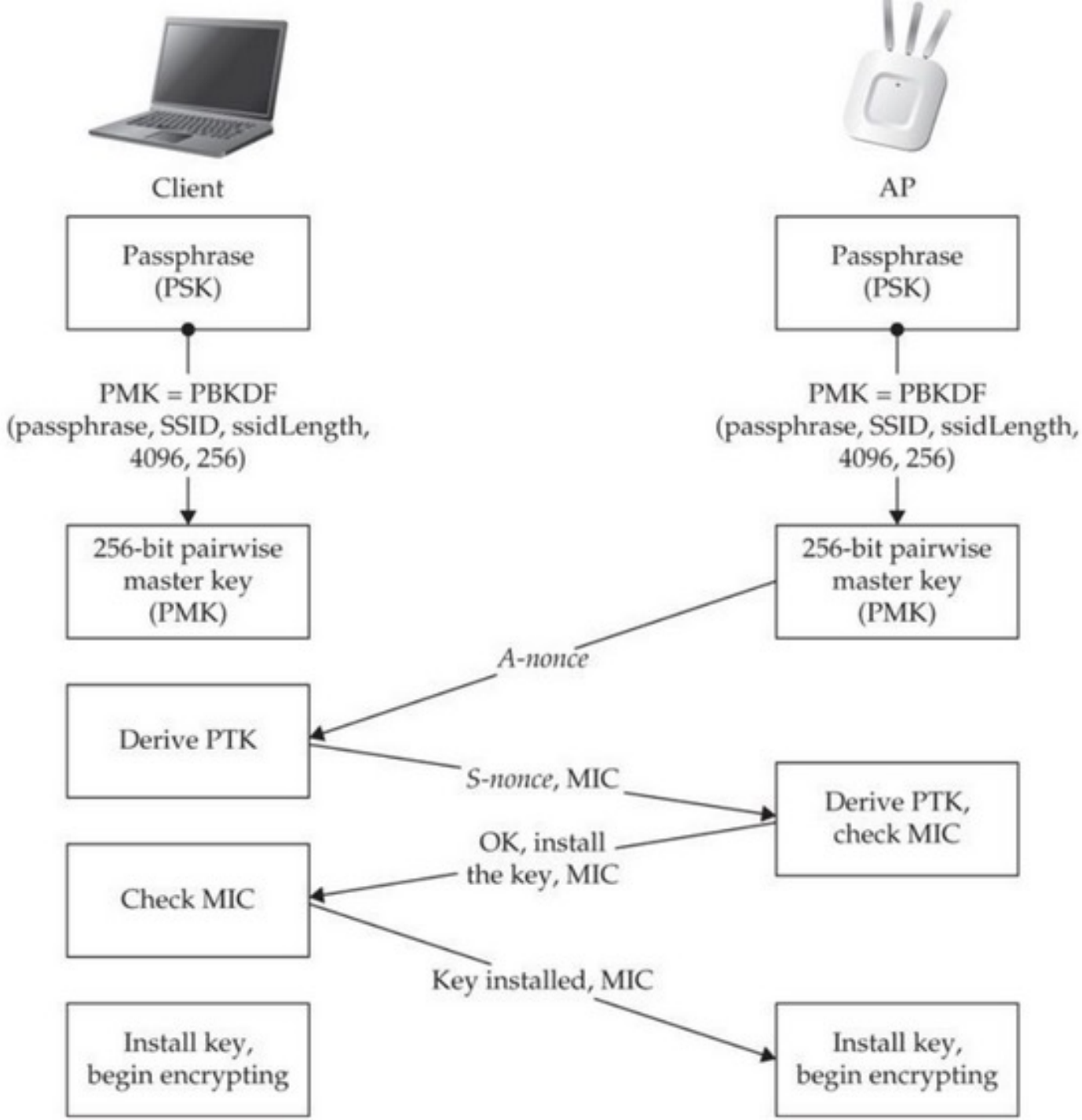
WPA/WPA2 4-Way Handshake Protocol

- Used to agree on a session key.
- Both parties are assumed to have shared secret passphrase.
- Each time a client connects to an AP, 4-Way Handshake occurs.
- ANonce and SNonce randomizes the session key.



4-Way Handshake Key Generation

- PSK: Pre-shared Key
  - Passphrase between 8-63 characters
  - Shared secret between all clients
- PMK: Pairwise-Master-Key
  - **PMK = PBKDF2(HMAC–SHA1, PSK, SSID, 4096, 256)**
  - Generated by both Client and AP before 4-way handshake
- PTK: Pairwise-Transient-Keys
  - **PTK = Hash(PMK || Anonce || Snonce || MAC_AP || MAC_Client)**
  - PTK is used to encrypt data between client and AP
  - Length is 64-bytes (512-bit)
  - PTK is splitted into KCK, KEK, TK, MICTX and MICRX keys.


Client
AP
Passphrase (PSK)
Passphrase (PSK)
PMK = PBKDF (passphrase, SSID, ssidLength, 4096, 256)
PMK = PBKDF (passphrase, SSID, ssidLength, 4096, 256)
256-bit pairwise master key (PMK)
256-bit pairwise master key (PMK)
A-nonce
Derive PTK
S-nonce, MIC
Derive PTK, check MIC
OK, install the key, MIC
Check MIC
Key installed, MIC
Install key, begin encrypting
Install key, begin encrypting

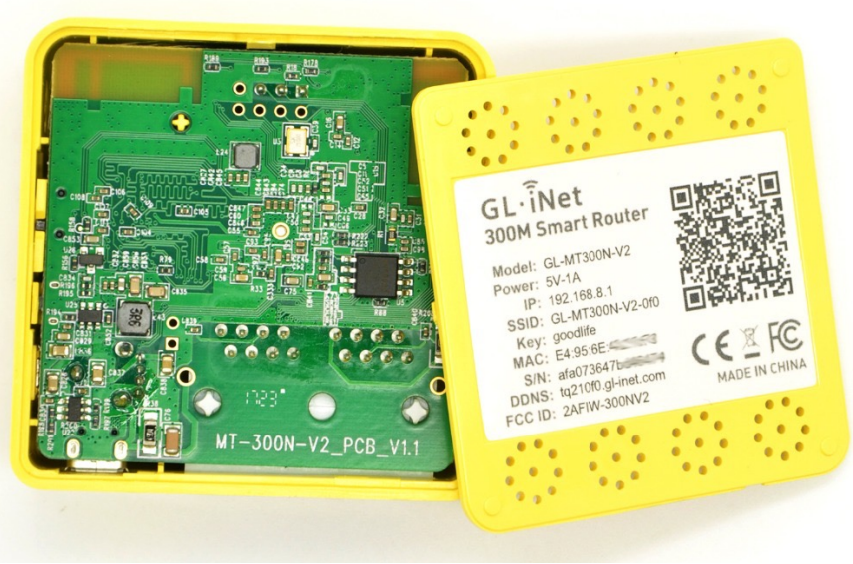
4-Way Handshake Key Generation

- PTK is splitted as follows:
  - KCK: Key Confirmation Key
    - 128-bit key used in the MIC function to create the payload checksum.
  - KEK: Key Encryption Key
    - 128-bit key used to encrypt additional data from the AP to the clients during the handshake.
  - TK: Temporal Key
    - 128-bit key used to encrypt/decrypt messages after the handshake.
  - MIC Authenticator Tx/Rx Keys
    - 64+64-bit TKIP-only keys to compute MIC on AP and client packets.
- MIC: Message Integrity Check
  - **MIC = HMAC_SHA1(KCK, payload)**

WPA3

- WPA2 handshake seems to be still secure, but vulnerable to dictionary attacks.
- WPA2 has no forward secrecy (i.e. once a key is cracked, all old captured traffic may be decrypted).
- WPA3 become available in January 2018 as a replacement to WPA2.
- WPA3 replaces the Pre-shared Key (PSK) exchange with Simultaneous Authentication of Equals (SAE) exchange, also known as Dragonfly Handshake.
- Dragonfly prevents offline dictionary attacks and ensures perfect forward secrecy
- Attacks
  - Dragonblood, 2019.

Demo Setup



Wi-Fi Access Point
with WPA2 CCMP PSK
Configuration

Mobile Phone
Connected to AP

USB Wi-Fi Dongle with
AR9271 Chipset
Connected to Kali Linux

Attack Scenario

- A client device is connected to an access point using WPA2 CCMP PSK Wi-Fi configuration.
- Attacker wants to recover/crack secret passphrase without physical access to any devices.
- Attacker is assumed to sniff Wi-Fi signals between access point and client device and also able to send packets to client's device.
- Attacker has a USB Wi-Fi dongle with monitoring mode support.
  - Can capture all Wi-Fi packets regardless of the destination MAC address.
- Attacker wants to capture a 4-way handshake and apply offline dictionary attack to crack the passphrase.

Values Needed from 4-Way Handshake

- SSID: Wi-Fi Name
- BSSID: Access Point’s MAC Address
- At least one connected client’s MAC Address
- ANonce
- SNonce
- Packets’ MIC values

Attack Steps

- Guess a Passphrase (PSK)
- Compute PMK for this Passphrase using
  - **PMK = PBKDF2(HMAC–SHA1, PSK, SSID, 4096, 256)**
- Compute PTK from the assumed PMK using
  - **PTK = Hash(PMK || Anonce || Snonce || MAC_AP || MAC_Client)**
- Use generated PTK to obtain KCK and compute a MIC for captured packets of the handshake
- If computed MIC == MIC of the captured packet;
  - PSK guess is correct
- Otherwise;
  - Go back to first step and make a new guess.

Tools

- airmon-ng
  - Enable monitor mode for the wireless interface
- airodump-ng
  - Monitor Wi-Fi traffic
  - Capture the 4-way handshake
- aireply-ng
  - Mount deauthentication attack to capture handshake faster (if needed)
  - Only active part in the attack scenario
- aircrack-ng
  - Search for passphrase using dictionary file

The end.