Wi-Fi security protocols

Sakhi Hashmat Khalil

7.3.2023

Haaga-Helia

Agenda

- Why we need security protocols?
- WEP
- WPA
- WPA2
- WPA2 enetrprise
- 4-way handshake
- WPA3
- SAE

Why we need security protocols

- There are a lot of risks when we use public WI-FI.

Unencrypted networks

Malware distribution

WI-FI snooping and sniffing

MITM
(Man-in-the middle)
attack

WEP

The most widespread and oldest Wi-Fi security protocol is WEP (Wired Equivalent Privacy) was introduced in 1997.

Symmetric Encryption Keys

RC4 (Rivest Cipher 4) algorithm for encryption.

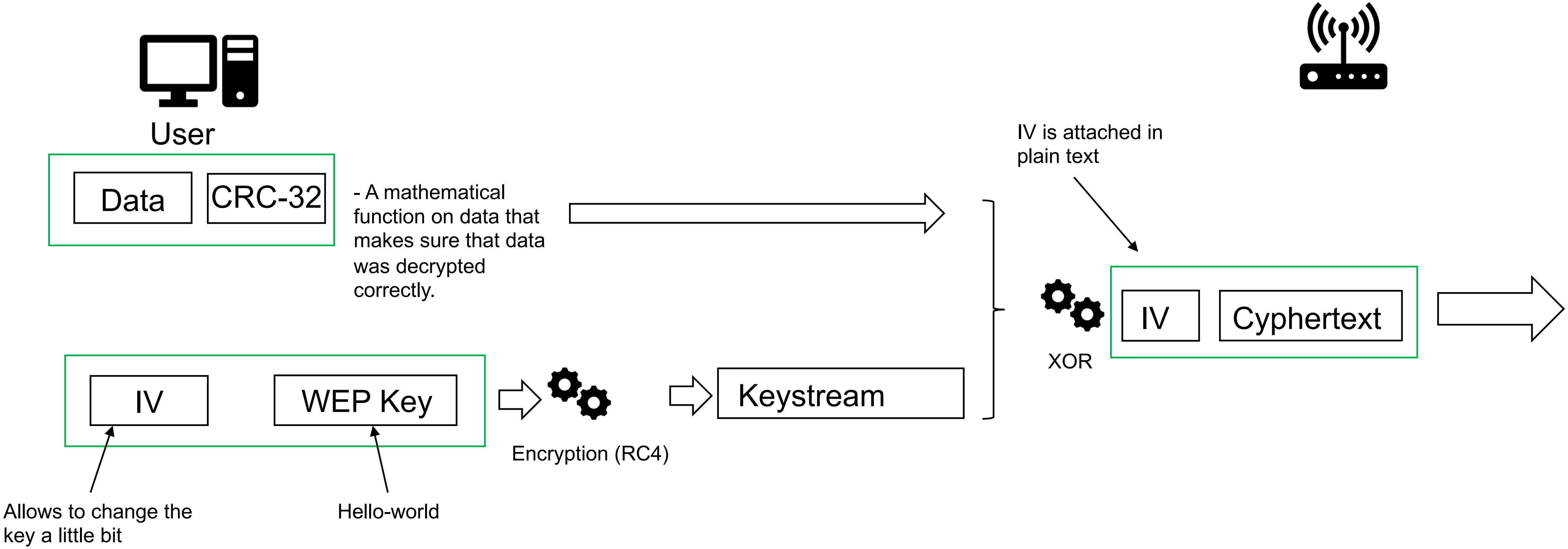
Small key size

- Initially 64-bit
- Later 128-bit

Initialization Vector (IV) Added to Protect Encryption Key

- 24-Bit (Part of Key)
- 64 - 24 = 40
- 128 - 24 = 104
- WEP uses the shared key for authentication and encryption. The shared key is static and with brute force technique can be guessed.

WEP protocol


User
Data
CRC-32
- A mathematical function on data that makes sure that data was decrypted correctly.
IV
WEP Key
Allows to change the key a little bit
Hello-world
Encryption (RC4)
Keystream
XOR
IV is attached in plain text
IV
Cyphertext

WPA protocol

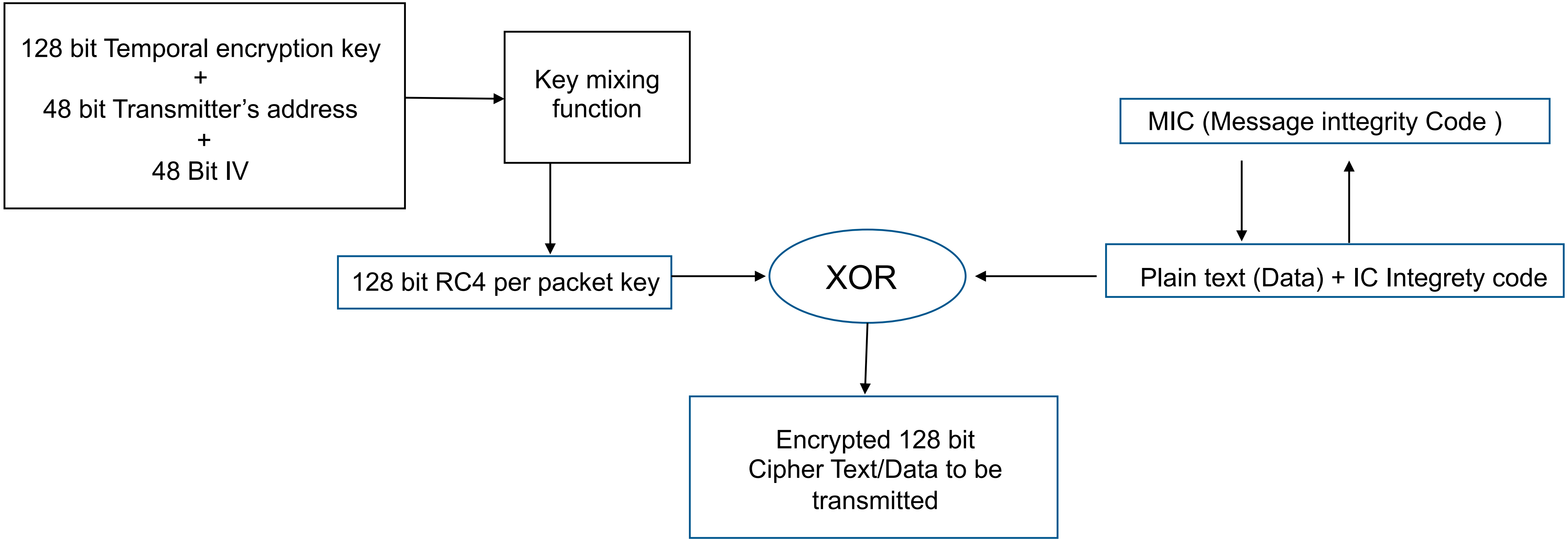
WPA (Wi-Fi Protected Access) was introduced in 2003 to overcome WEP's issues. WPA's 256-bit encryption key is safer than WEP's 64-bit or 128-bit keys. TKIP creates a fresh key for each packet in WPA.

- Encryption: WPA uses the Temporal Key Integrity Protocol (TKIP) encryption algorithm..
- Authentication: WPA uses the pre-shared key (PSK) mechanism
- Key management: WPA uses the Message Integrity Code (MIC) to protect against attacks that attempt to modify the encryption key.
- Backward compatibility: WPA is backward compatible with devices that support the original WEP protocol, which makes it easy to upgrade from WEP to WPA.
- Automatic key rotation: WPA uses automatic key rotation to change the encryption key regularly, which makes it more difficult for attackers to intercept and decrypt the data.

WPA2

- WPA2 (Wi-Fi Protected Access 2) is a wireless security protocol that was introduced in 2004 to replace the original WPA (Wi-Fi Protected Access) protocol. WPA2 is designed to provide stronger security and better protection against various attacks and vulnerabilities than the original WPA protocol.
- Here are some of the key features and improvements of WPA2:
- Encryption: WPA2 uses the Advanced Encryption Standard (AES) algorithm for encryption, which is stronger and more secure than the RC4 encryption algorithm used in WEP and WPA.
- Authentication: WPA2 uses the IEEE 802.1X/EAP (Extensible Authentication Protocol) authentication mechanism, which is a more secure and robust authentication mechanism compared to the pre-shared key (PSK) mechanism used in WPA. This mechanism provides a more granular and flexible control over authentication and encryption keys.
- Key management: WPA/WPA2 uses the 4-way handshake to generate a new encryption key for each session, making it much more difficult for attackers to intercept and decrypt the data.
- Backward compatibility: WPA2 is backward compatible with devices that support the original WPA protocol, which makes it easy to upgrade from WPA to WPA2.

WPA



128 bit Temporal encryption key
+
48 bit Transmitter’s address
+
48 Bit IV

Key mixing function

128 bit RC4 per packet key

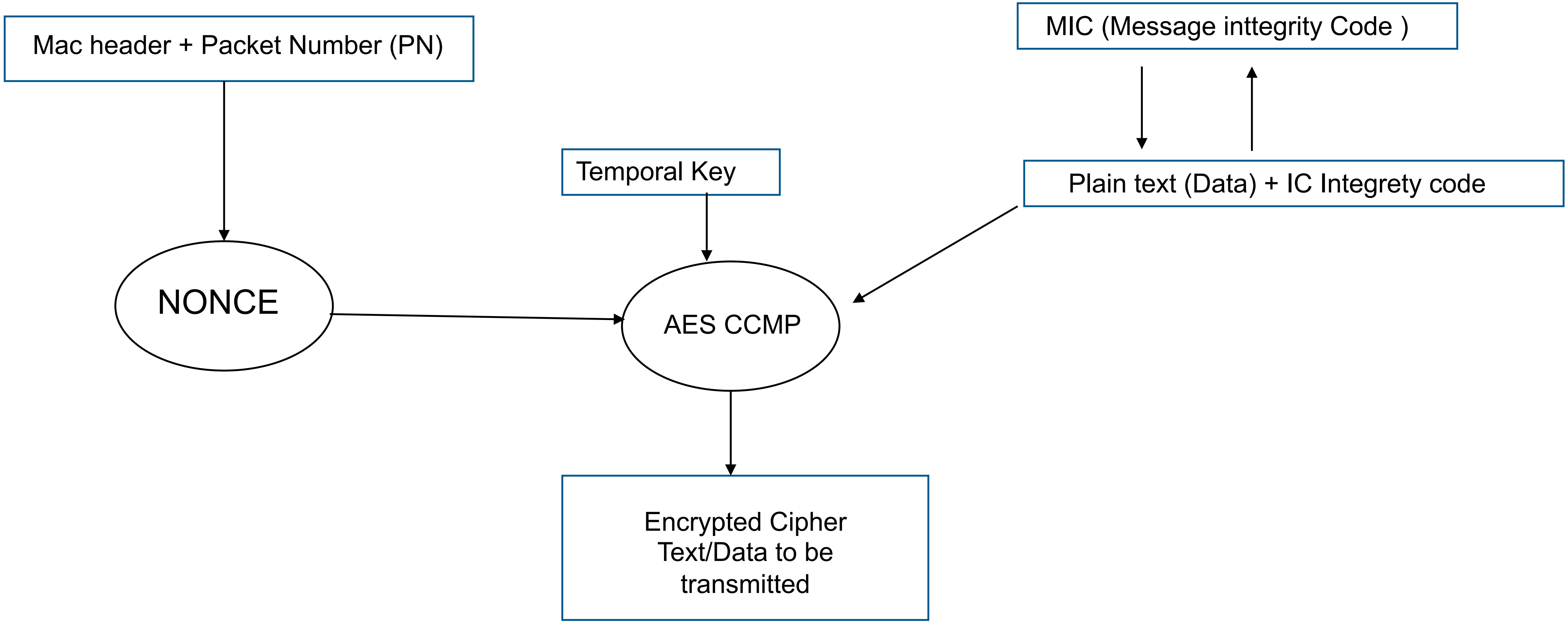
XOR

MIC (Message inttegrity Code)

Plain text (Data) + IC Integrety code

Encrypted 128 bit Cipher Text/Data to be transmitted

WPA 2



Mac header + Packet Number (PN)

MIC (Message inttegrity Code)

Temporal Key

Plain text (Data) + IC Integrety code

NONCE

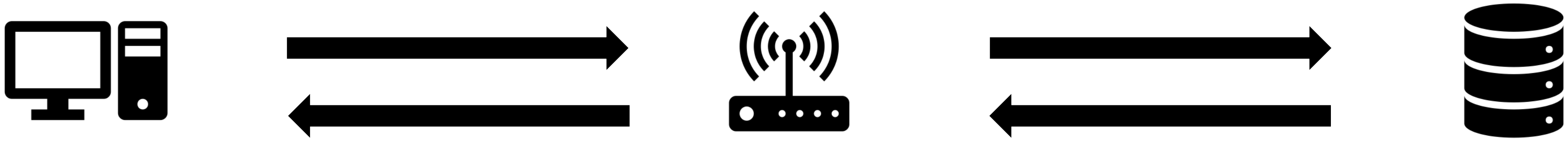
AES CCMP

Encrypted Cipher Text/Data to be transmitted

WPA2 Enterprice

Extensible Authentication Protocol (EAP)—EAP allows WPA to synchronize keys with an external RADIUS server

- Access control account
- Username
- Certificate (HTTPS)
- One-time password



WPA/WPA2 4-handshake

PTK = PMK + ANONCE + SNONCE + MAC(AA) + MAC(SA)

ANONCE - is a random number that the AP has made.

SNONCE - is a random number that the client has made

MAC(AA) - the mac address of the AP (authenticator).

MAC(SA) - the mac address of the client (supplicant).

PTK - Pairwise Transit Key

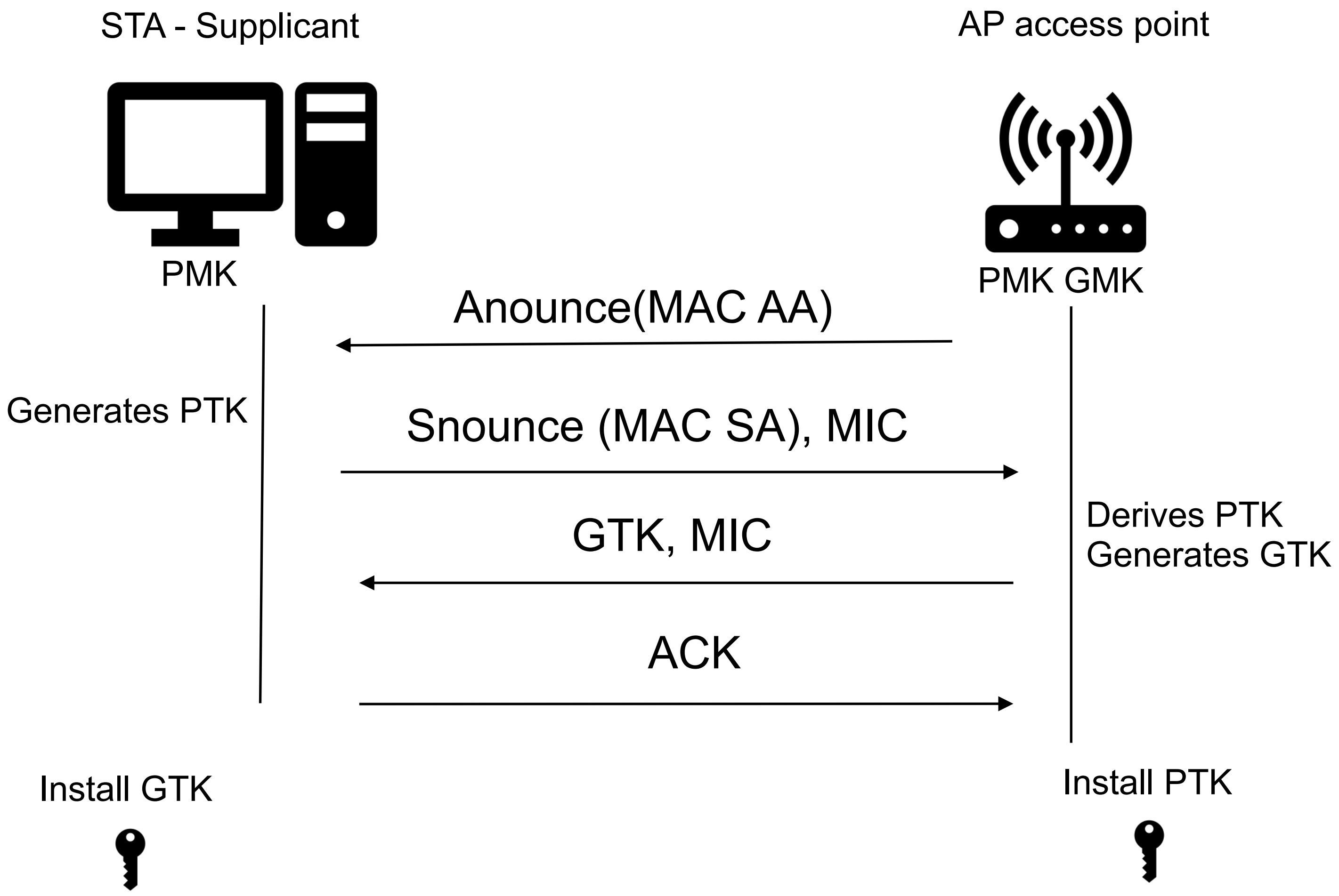
GTK - Group Temporal Key

MIC - Message Integrity Code,

PMK - Pairwise Master Key)

GMK – Group master key

ACK - acknowledgment message to the sender



- Because of the way the 4-Handshake works, hackers are able to use offline dictionary attacks to guess the password. The main point is doing it offline, because if hackers don’t have that opportunity to do an offline attack, they have to do one online. After several tries and failures, AP would deny their tries. If it is offline, theoretically, it is possible to crack the password at the end.

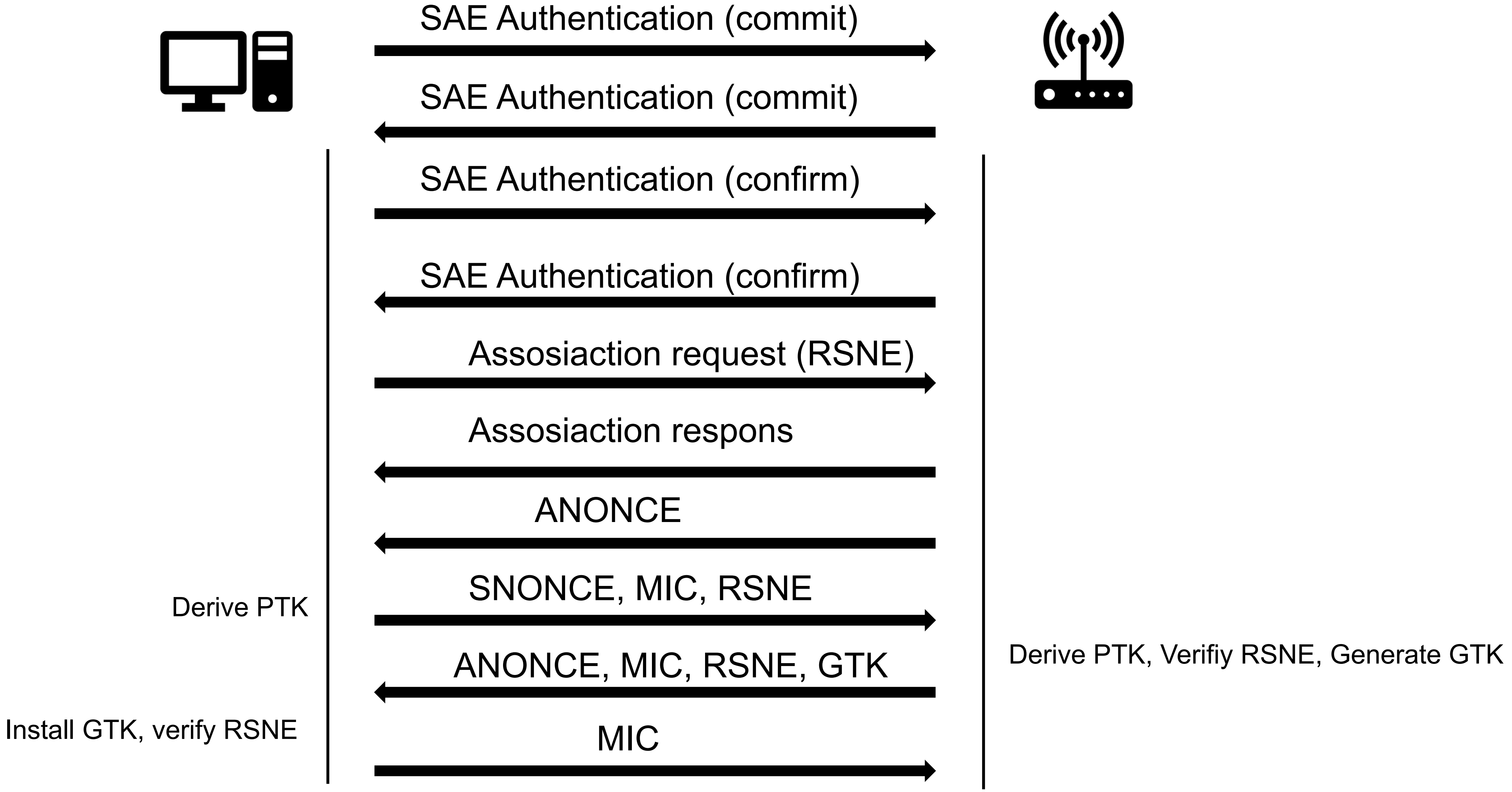
- PTK = PMK + ANONCE + SNONCE + MAC(AA) + MAC(SA)

- A hacker can listen to ANONCE and SNONCE and get the MAC (AA) and MAC (SA) only thing they cannot get is PMK (the Wi-Fi password), but the way MIC is calculated it uses PTK, and PTK has PMK. By getting PTK from the calculation of MIC, they can try to calculate MIC and compare it with the captured MIC to guess the PMK.

WPA3

- Enhanced security for public Wi-Fi networks: WPA3 provides stronger security for public Wi-Fi networks by encrypting each user's traffic with individualized data encryption keys. This helps prevent eavesdropping and other attacks on public Wi-Fi networks.
- Simultaneous Authentication of Equals (SAE): WPA3 uses the SAE mechanism, also known as Dragonfly, which is a more secure and resistant to attacks compared to the pre-shared key (PSK) mechanism used in WPA2. SAE uses a password-based authentication mechanism that is resistant to offline dictionary attacks.
- Stronger encryption: WPA3 uses the latest encryption standard, the 256-bit Galois/Counter Mode Protocol (GCMP-256), to provide stronger protection against brute-force attacks and other cryptographic attacks.
- Protection against brute-force attacks: WPA3 includes protection against offline brute-force attacks by preventing an attacker from repeatedly guessing passwords until they find the correct one.
- Easy configuration for IoT devices: WPA3 provides an easy-to-use configuration mechanism for IoT (Internet of Things) devices that have limited or no user interfaces.

WPA 3 SAE – Dragonfly



SAE Authentication (commit)

SAE Authentication (commit)

SAE Authentication (confirm)

SAE Authentication (confirm)

Assosiaction request (RSNE)

Assosiaction respons

ANONCE

SNONCE, MIC, RSNE

ANONCE, MIC, RSNE, GTK

MIC

Derive PTK

Install GTK, verify RSNE

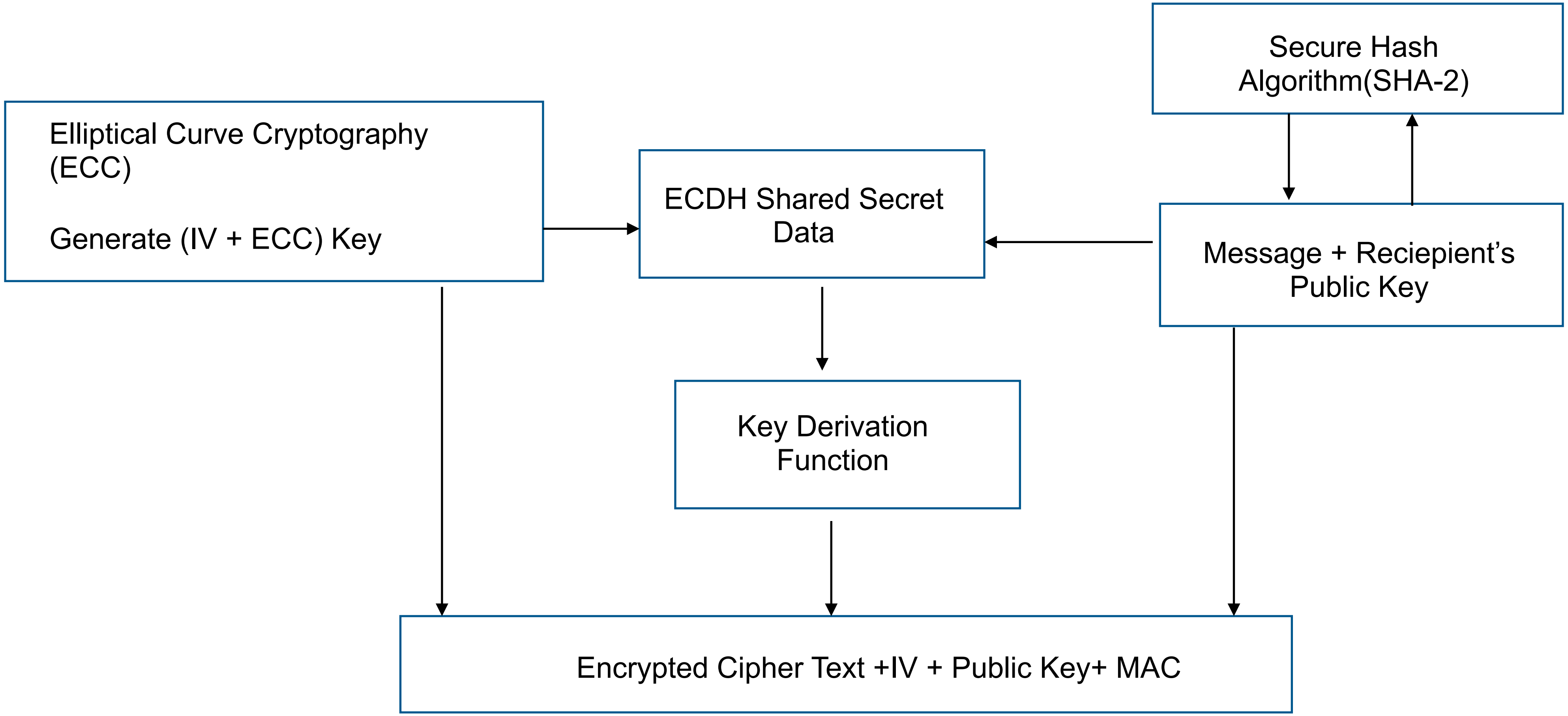
Derive PTK, Verifiy RSNE, Generate GTK

WPA 3

WPA3 comes in three main forms:

- **WPA3 Personal (WPA-3 SAE) Mode** is a static passphrase-based method. It provides better security than what WPA2 previously provided, even when a non-complex password is used, thanks to Simultaneous Authentication of Equals (SAE), the personal authentication process of WPA3.
- **WPA3 Enterprise Mode (WPA3 ENT):** Much like its predecessor, WPA2 Enterprise, WPA3 ENT is different because it requires management frame protection. An optional, stronger 192bit consistent cryptographic suite is also provided for those who are more security conscious.
- **Wi-Fi Enhanced Open Mode** increases privacy in open networks. It prevents passive eavesdropping by encrypting traffic even when a password is not used, but does not bring security – anyone can still connect to the network.
- **What are the Key Features of WPA3?**
- **Management Frame Protection (MFP):** The unicast management frames are encrypted, preventing, for example, illegitimate de-authorization of clients (for operating man-in-the-middle attack, or for IDS/IPS systems to kick clients out.
- **Simultaneous Authentication of Equals (SAE):** SAE provides a more secure, password-based authentication and key agreement mechanism even when passwords are not following complexity requirements. It protects from brute-force attacks and makes unwanted decrypting of sessions (during or after the session) a lot harder – just knowing the passphrase isn’t enough to decrypt the session.
- **Transition mode:** Personal, Enterprise and Enhanced Open Modes can also operate in Transition Mode. This means falling back to WPA2 for connecting clients that don’t support WPA3.

WPA 3


Secure Hash Algorithm(SHA-2)
Elliptical Curve Cryptography (ECC)
Generate (IV + ECC) Key
ECDH Shared Secret Data
Message + Reciepient's Public Key
Key Derivation Function
Encrypted Cipher Text +IV + Public Key+ MAC

Comparison table

	WEP	WPA	WPA2	WPA3
Encryption	RC4 Stream Cipher with 64-bit key	RC4 Stream Cipher with 128-bit TKIP key	CCMP based on AES	EEC with 192-bit security site
Integrity	CRC-32 error detecting code	64-bit Message Integrity Code	64-bit Message Integrity Code	Secure Hash Algorithm (SHA2)
Authentication	Open System and Shared Key Authentication	PSK authentication	MIC and FCS	Simultaneous Athentication of Equals (SAE)

Sources

- https://www.youtube.com/watch?v=4auUkExkV3Q
- https://www.mist.com/wpa3-just-the-essentials-on-the-latest-in-wi-fi-security/
- https://en.wikipedia.org/wiki/IEEE_802.11i-2004
- https://www.minitool.com/news/wpa-vs-wpa2-vs-wpa3.html
- https://www.youtube.com/watch?v=-Q_WXeEf8Fw&t=189s
- https://www.youtube.com/watch?v=9M8kVYFhMDw
- https://us.norton.com/blog/privacy/public-wifi
- https://www.kaspersky.com/resource-center/definitions/wep-vs-wpa
- https://www.copperpodip.com/post/2018/04/11/wpa3-next-gen-security-for-next-gen-internet-of-things

Thank you