Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2

Li Chenxi

me@ayayaya.org

A little note on Wi-Fi security

History & Concept

What is **Wi-Fi**?

- Wi-Fi 4
- Wi-Fi 5
- Wi-Fi 6
- …

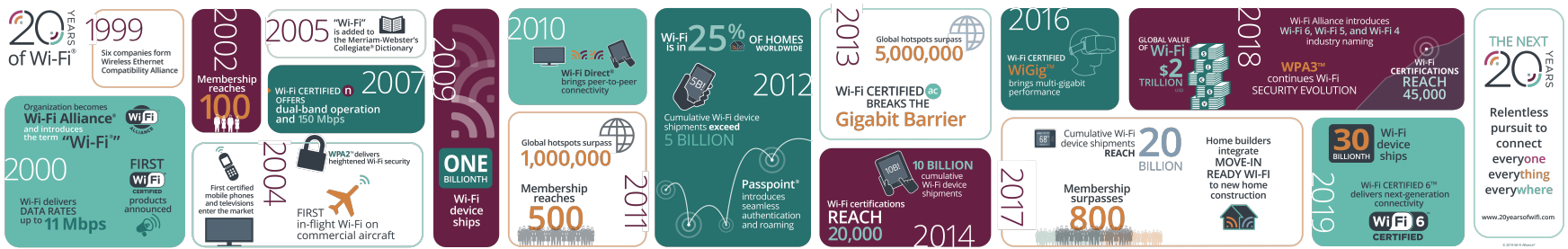
What is **IEEE 802.11**?

- 802.11 (1997)
- 802.11b (1999)
- 802.11a (1999)
- 802.11g (2003)
- 802.11n (2008)
- 802.11ac (2014)
- 802.11ax (2019)
- …

A little note on Wi-Fi security

History & Concept

In 1999, several visionary companies came together to form a global non-profit association with the goal of driving the best user experience, regardless of brand, using a new wireless networking technology. In 2000, the group adopted the term “Wi-Fi®” as the proper name for its technical work and announced its official name: Wi-Fi Alliance®.



A little note on Wi-Fi security

History & Concept

Security Standards:

- Wired Equivalent Privacy (WEP) - part of 802.11
- Wi-Fi Protected Access (WPA) - 2000
- Wi-Fi Protected Access 2 (WPA2) - 2004, 802.11i-2004,2007
- Wi-Fi Protected Access 3 (WPA3) - 2019

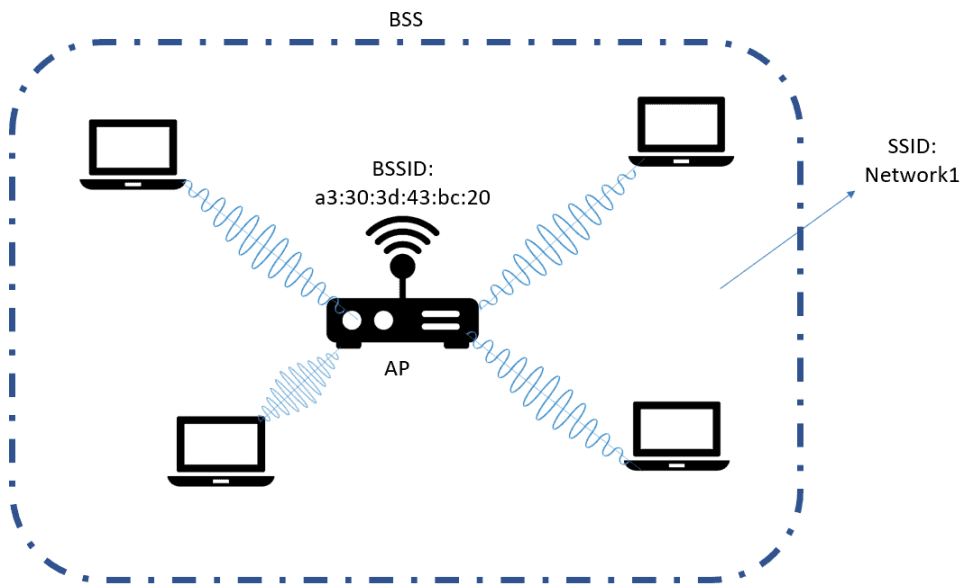
Note:

- WEP has proved to be insecure (*Weaknesses in the Key Scheduling Algorithm of RC4, Scott Fluhrer et al., 2001*)
- WAP & WAP2 - **today's topic**

WPA (2)

Notions

- Access Point (AP): A networking hardware device that allows other Wi-Fi devices to connect to a wired network
- Station (STA): A device that has the capability to use the 802.11 protocol

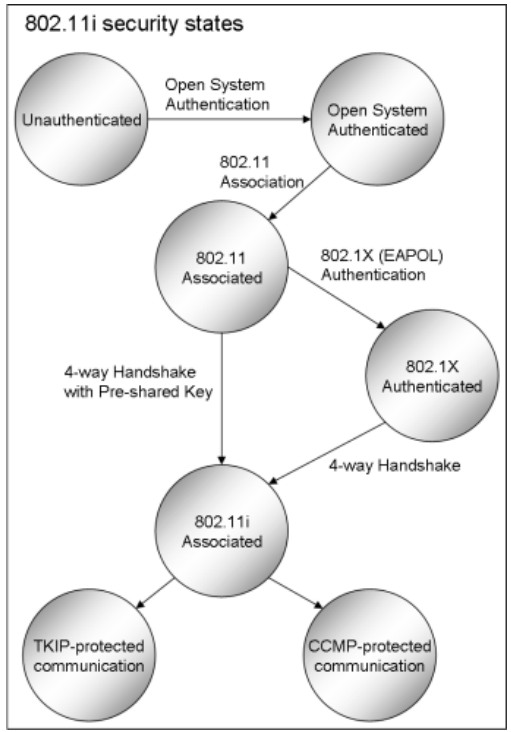


WPA (2)

RSNA setup process

RSNA (Robust Security Network Association): An association between a client STA and an AP that was established in a 4-way handshake to derive unicast keys and transfer group keys.

1. ...(skip)
2. 4-way Handshake
3. Encrypted communication



What happens in 4-way handshake?

WPA (2)

4-way handshake

Goals:

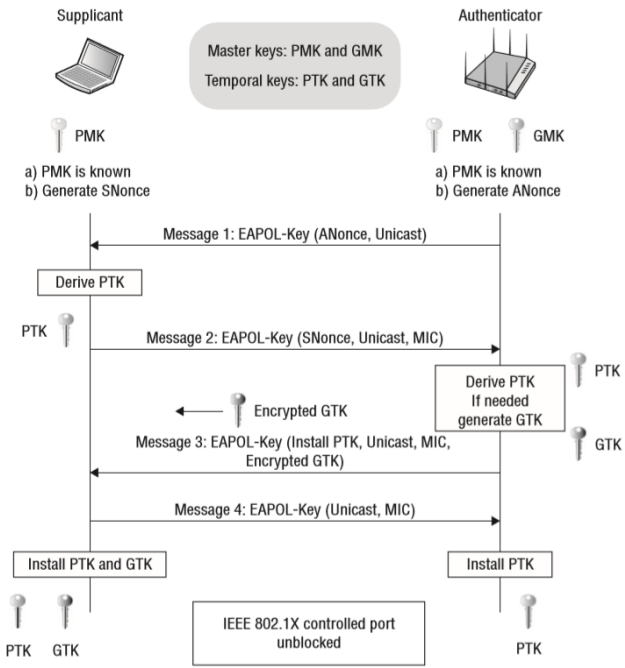
1. Authentication: verify *AP* and *STA* have same **(Pairwise Master Key) PMK**
2. Key Generation & Installation: Generate keys for further (encrypted) communication

What is **PMK** ?

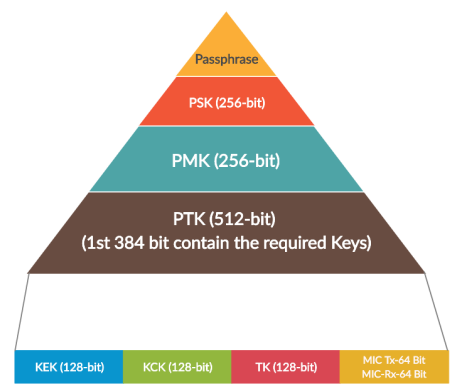
- For WPA-Personal (a.k.a, your home Wi-Fi), it's generated by your *password*
- For WPA-Enterprise, it's generated by EAP authentication.

WPA (2)

4-way handshake



- SNonce, ANonce: "nonce" stands for random number
- **(Pairwise Transient Key) PTK**: used to encrypt all unicast traffic between a client station and the access point
  - $\text{PTK} = \text{PRF}(\text{PMK}, \cdots, \text{SNonce}, \text{ANonce})$



WPA (2) Data-confidentiality Protocol

WPA (2) use three data-confidentiality protocol:

- TKIP (WPA)
- CCMP (WPA 2)
- CGMP (802.11ad, 2012)

CCMP (rfc 3610):

- CTR mode for encryption
- CBC-MAC for date integrity

WPA (2) Data-confidentiality Protocol

WPA (2) CCMP use AES as block cipher,

AES "core" algorithm (a.k.a Rijndael algorithm) is `f`.

```
f : (byte[16], byte[n / 8]) -> byte[16]
```

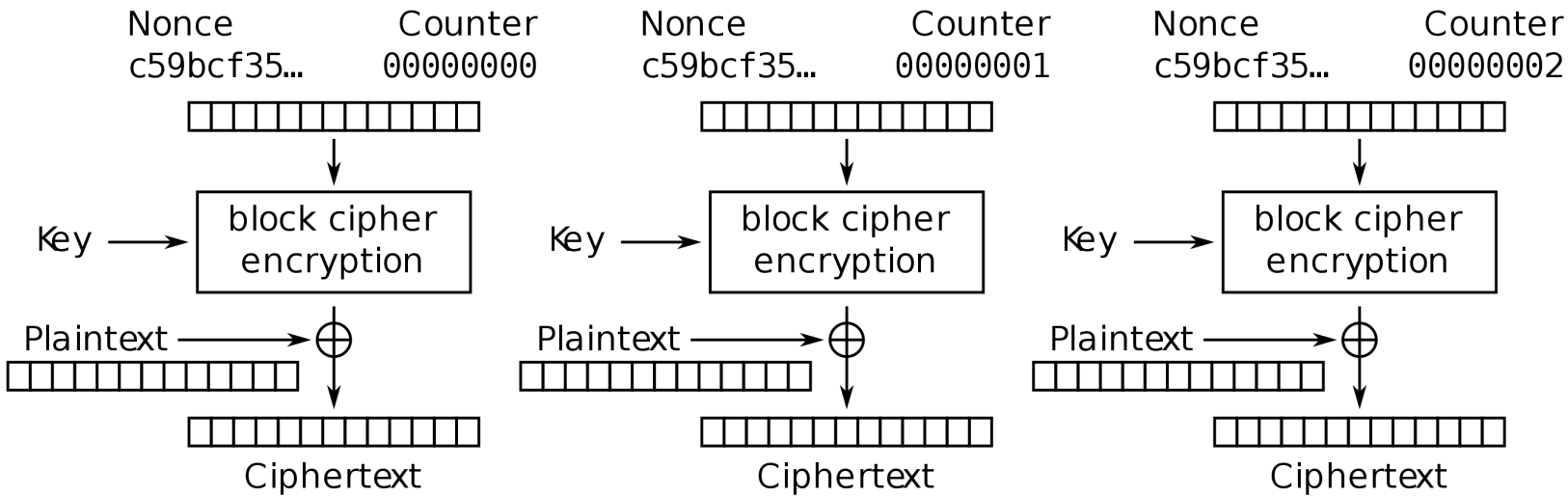
(`n` is the length of the key, 128, 192, 256)

```
f(plaintext, key) = ciphertext
```

How to encrypt *stream* data ?

WPA (2) Data-confidentiality Protocol

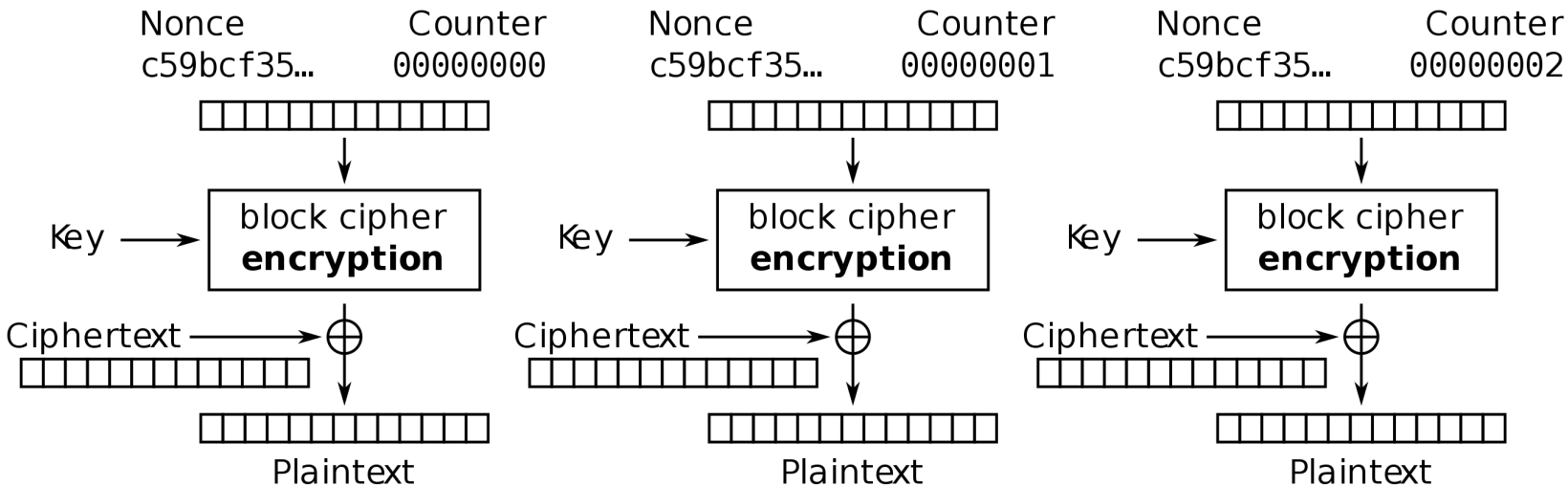
AES-CTR



Counter (CTR) mode encryption

WPA (2) Data-confidentiality Protocol

AES-CTR



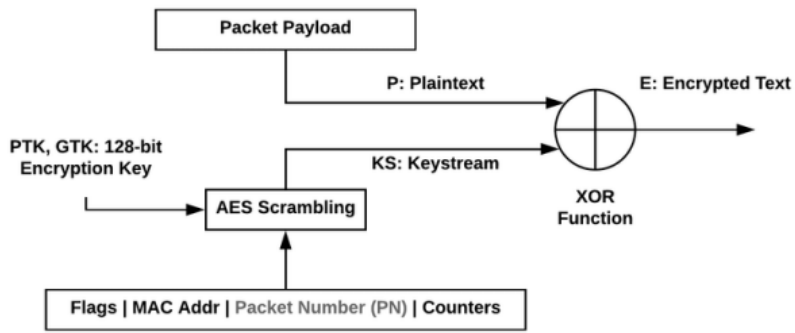
Counter (CTR) mode decryption

WPA (2) Data-confidentiality Protocol

Key installation

AES-CTR Nonce & Key: from 4-way handshake

- Key: TK
- Nonce:



- PN = 1
- CTR = 0

Crack the WPA (2)

What's wrong?

If you're STA:

- After receive **Message 3**
- You're connected.
- Send Encrypt Messages …
- AP: **Message 3** again
- You: ???

What will happen if **Message 3** is received twice?

Crack the WPA (2)

What's wrong?

IEEE 802.11i defined state machine:

- If **Message 3** is received again
- *PTK-DONE* will be exec again
- a.k.a **Key Reinstallation**

Then?

Crack the WPA (2)

By key reinstallation

- plaintext p_1, p_2
- cipertext c_1, c_2
- $c_1 = \text{Enc}^1_{\text{ptk}}(p_1)$
- $c_2 = \text{Enc}^1_{\text{ptk}}(p_2)$
- $k = f_{\text{AES}}(\text{nonce}||\text{counter}(1), \text{tk})$

We have:

- $c_1 = p_1 \oplus k$
- $c_2 = p_2 \oplus k$
- $p_1 = p_2 \oplus c_1 \oplus c_2$
- $p_2 = p_1 \oplus c_1 \oplus c_2$

Crack the WPA (2)

Conclusion

By key reinstallation, as MITM, we may decrypt / replay / forge some frames.

Crack the WPA (2)

Conclusion

A Dangerous Bug

All-Zero Encryption Key Vulnerability

In version 2.4 and 2.5 of `wpa_supplicant`, after key reinstallation,

All-zero TK is installed.

That means?

Anyone can decrypt **any** further packet.

Android phone also use `wpa_supplicant`.

Nearly 31.2% of Android smartphones are likely vulnerable to the all-zero encryption key vulnerability (2017)

Do you use `NJU-WLAN`?

An insecure wireless network

`NJU-WLAN` provides *void* security!

- No encryption
- No data integrity
- Authentication with ugly, buggy, inconvenient *Web portal*

It is a nonprofessional practice.

Refs & More info

- Original paper

If you want to know more about WPA, IEEE 802.11i and EAP, see my blogs:

- 802.1x eap认证
- 建立RSNA

Other helpful material:

- A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3
- IEEE Std 802.11™-2007
- KRACK Tools
- Wi-Fi security – WEP, WPA and WPA2