

Masterclass : Wi-Fi



<https://github.com/JulienFink/WiFi-Project>



Summary

- Wi-Fi definition and presentation
- Core mechanism - protocols overview
- Security issues



Summary

- **Wi-Fi definition and presentation**
- Core mechanism - protocols overview
- Security issues



Wi-Fi definition and presentation (1/N)

- Radio waves
- 2.4 GHz and/or 5.8 GHz
- Provides local network and Internet access to devices

Designed for :	2.4 GHz	5.8 GHz
Range	✓	✗
Linkrate	✗	✓
Penetration	✓	✗



Summary

- Wi-Fi definition and presentation
- **Core mechanism - protocols overview**
- Security issues



Wi-Fi core mechanism (1/N)

IEEE 802.11 standard

- IEEE 802.11 refers to the set of standards that define communication for wireless local area networks (WLANs)
- A 1985 decision by the U.S. Federal Commission for Communication that opened up the ISM band for unlicensed use
- Various security algorithms for IEEE 802.11 wireless networks



Wi-Fi core mechanism (1/N)

Open System Authentication

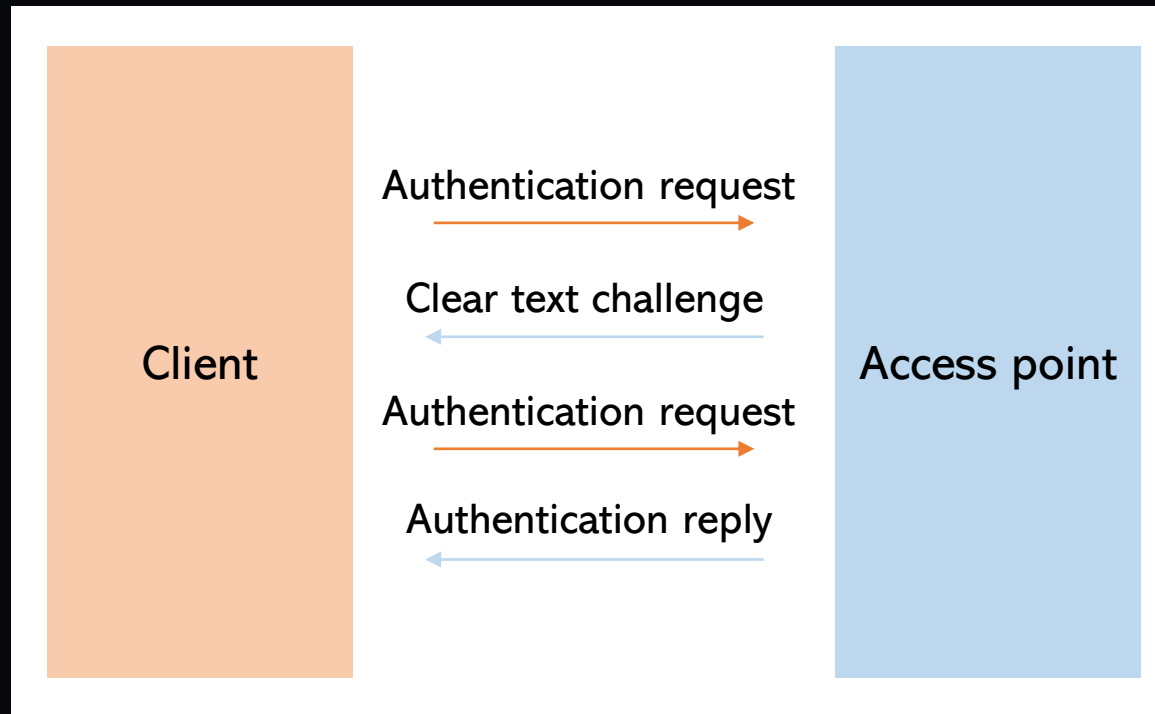
- In Open System authentication, the WLAN client does not provide its credentials to the Access Point during authentication.
- Any client can authenticate and associate with the Access Point
- Data travels in a clear format, except if other protocols perform encryption (e.g. TLS)



Wi-Fi core mechanism (1/N)

WEP (Wired Equivalent Privacy) - Shared Key authentication (1/2)

In Shared Key authentication, the WEP key is used for authentication in a four-step challenge-response handshake :



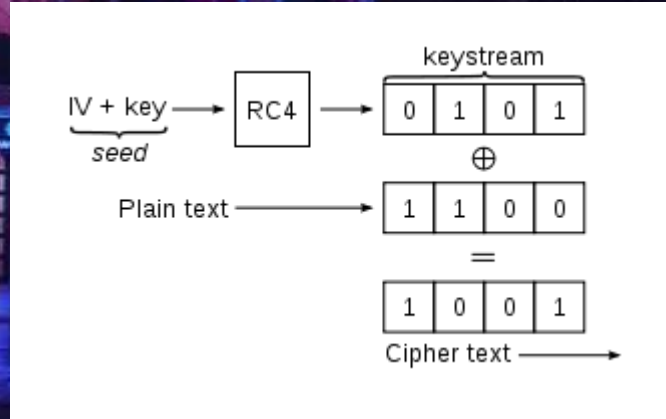
After the authentication and association, the pre-shared WEP key is also used for encrypting the data frames using RC4.



Wi-Fi core mechanism (1/N)

WEP (Wired Equivalent Privacy) - Payload encryption (2/2)

- Stream cipher RC4
- 64-bit, 128-bit WEP key
- 104 bits + 24 bits IV = 128-bit WEP key



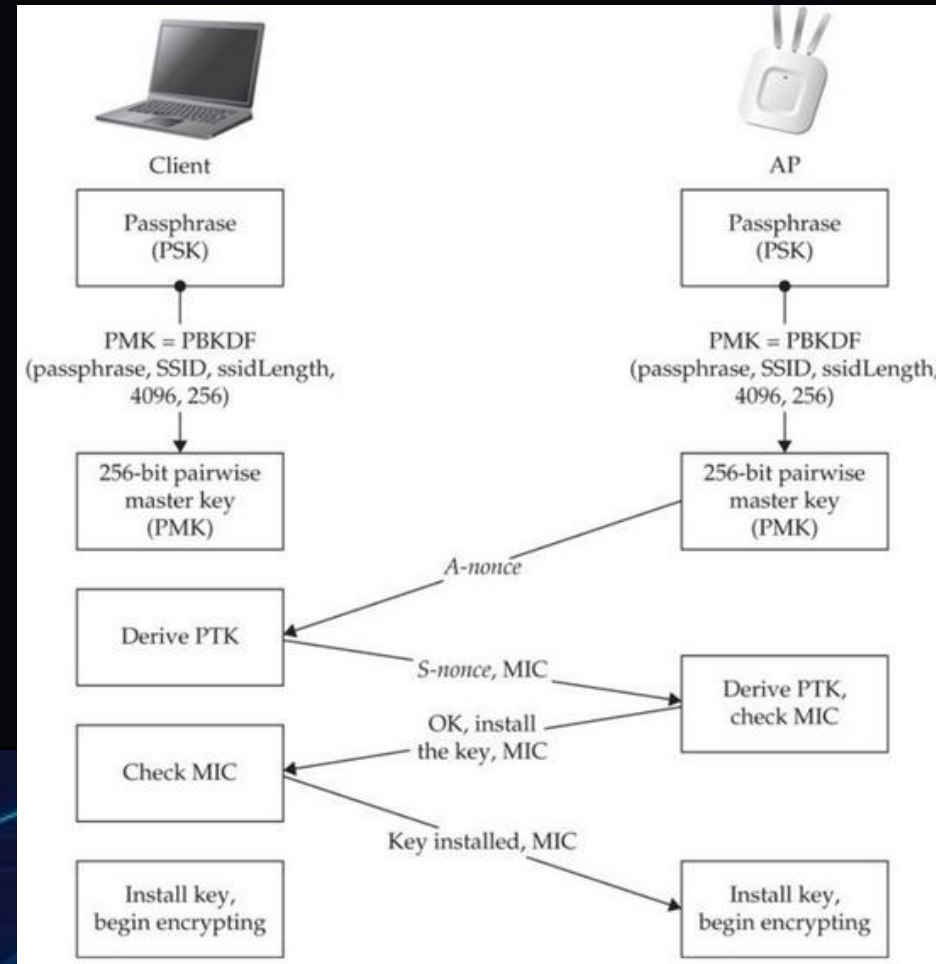
**Basic WEP
encryption: RC4
keystream XORed
with plaintext**



Wi-Fi core mechanism (1/N)

WPA & WPA2 (Wi-Fi Protected Access) - PSK authentication

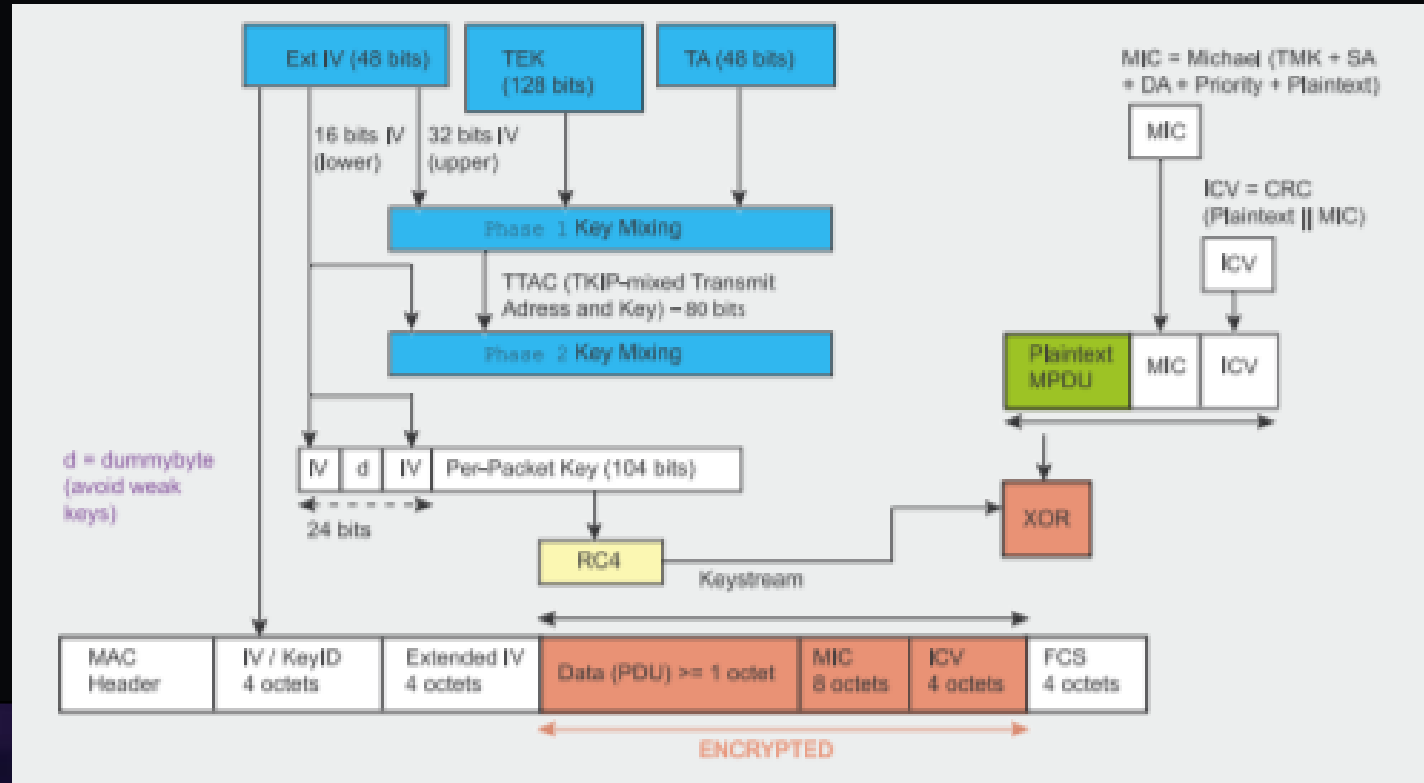
- PSK (Pre-Shared Key) authentication



Wi-Fi core mechanism (1/N)

WPA - Payload encryption

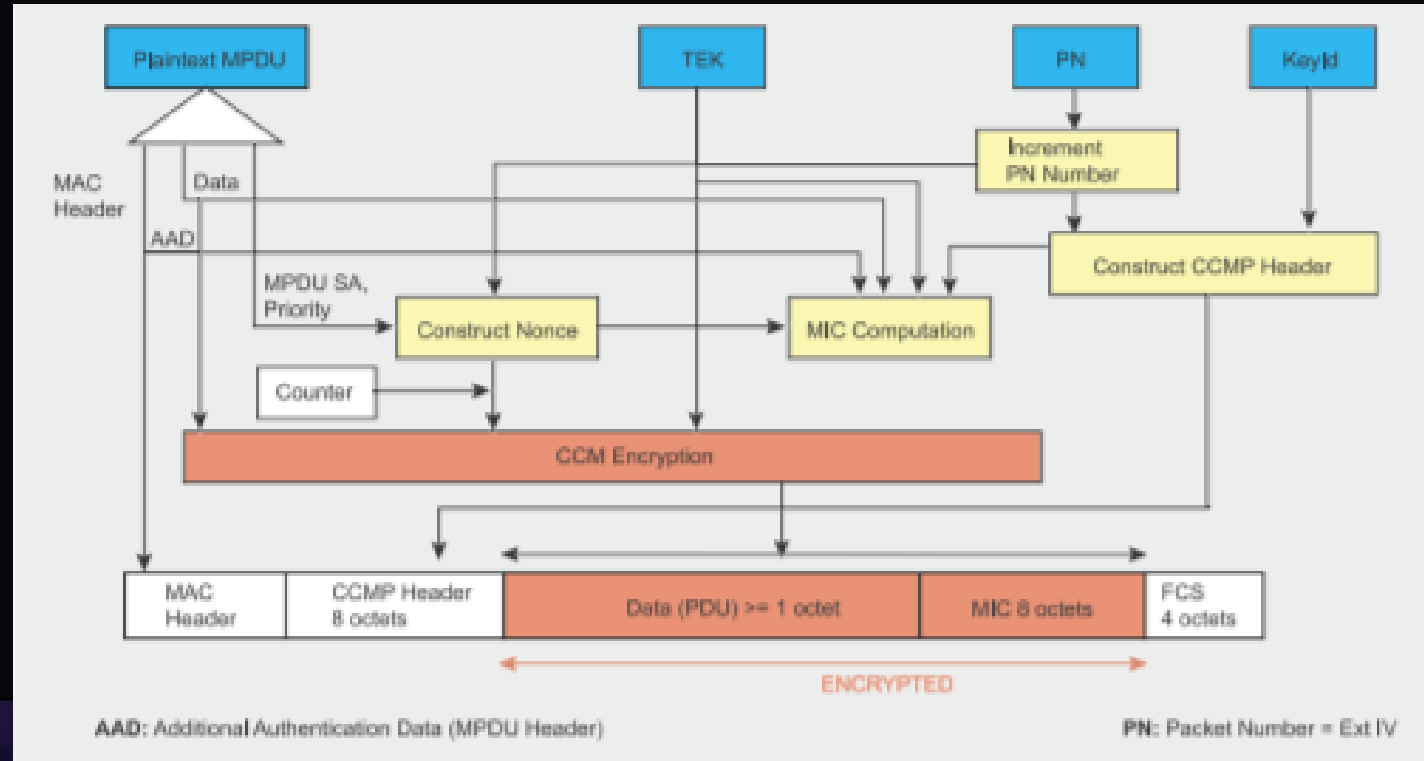
- TKIP (Temporal Key Integrity Protocol) encryption



Wi-Fi core mechanism (1/N)

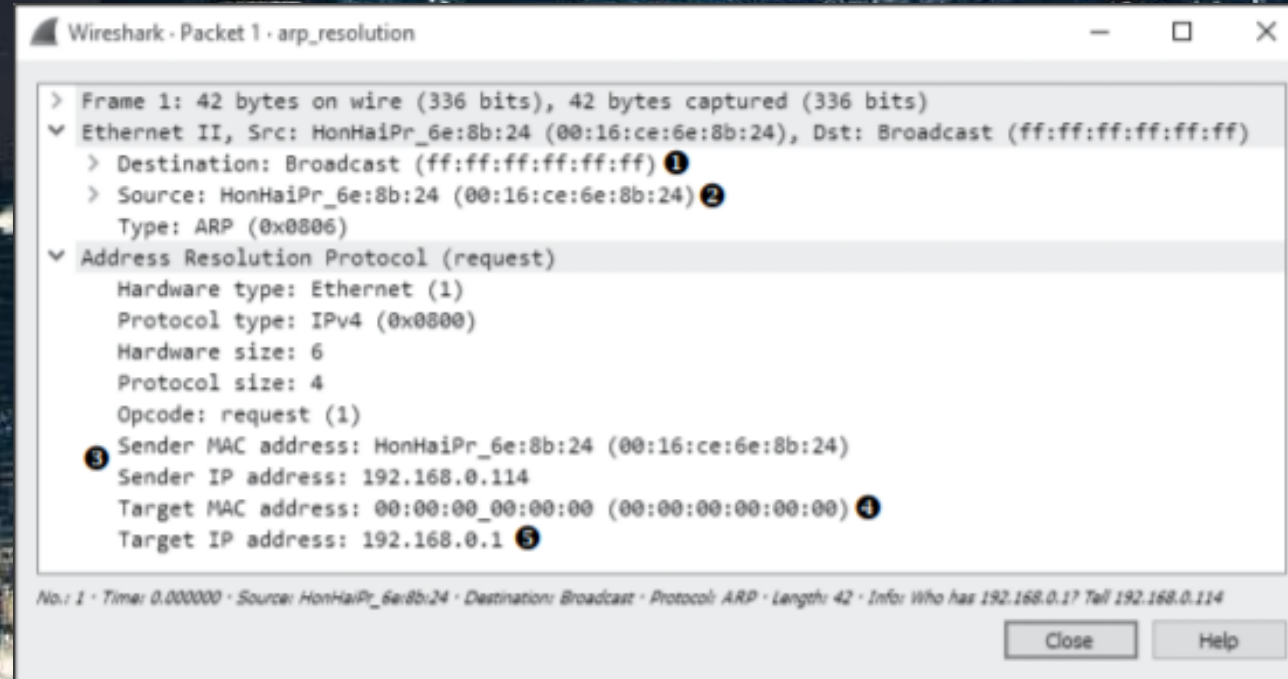
WPA2 - Payload encryption

- CCMP (Counter-Mode/CBC-Mac protocol) encryption



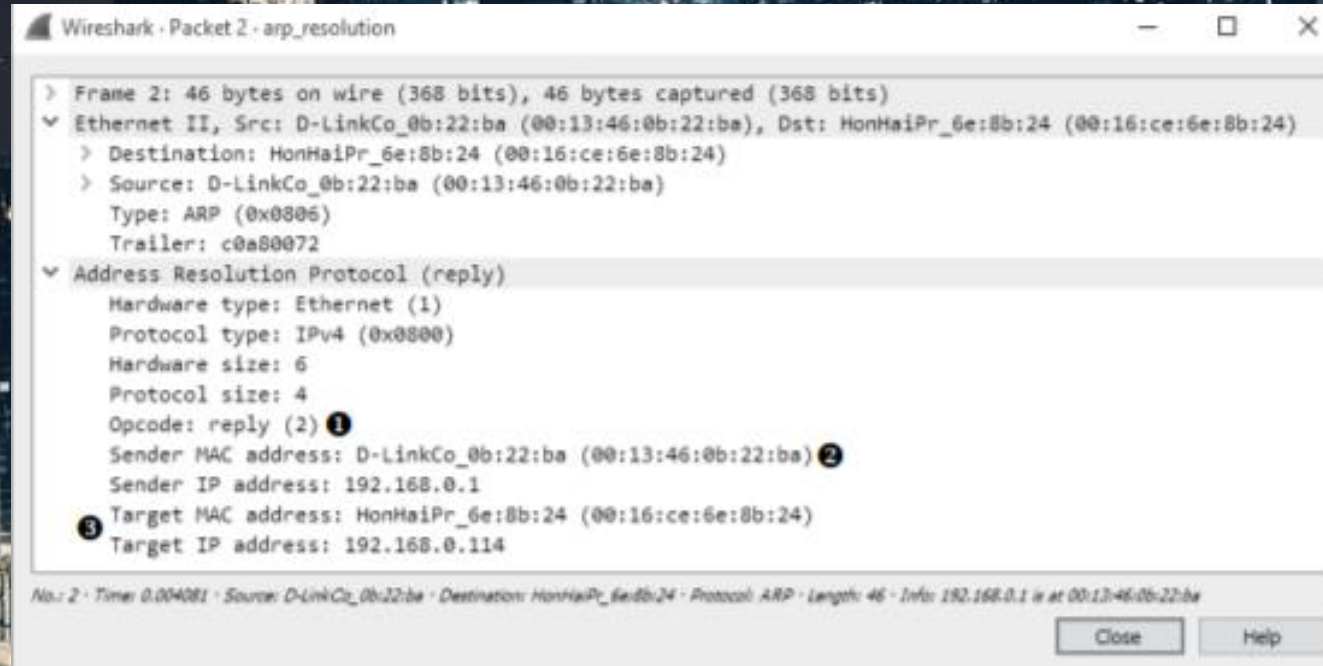
Wi-Fi core mechanism (1/N)

ARP (Address Resolution Protocol) - ARP request



Wi-Fi core mechanism (1/N)

ARP (Address Resolution Protocol) - ARP reply



Summary

- Wi-Fi definition and presentation
- Core mechanism - protocols overview
- **Security issues**



Security issues (1/N)

For radio communications in general

- Eavesdropping
- RF Denial of Service (DoS)
- Media Access Control (MAC) address spoofing
- Hijacking
- Man-in-the-Middle attacks
- Encryption Cracking



Useful links

- <https://repository.root-me.org/R%C3%A9seau/EN%20-%20Hacking%20wifi.pdf>
- [https://github.com/koutto/pi-pwnbox-rogueap/wiki/O5.-WPA-WPA2-Personal-\(PSK\)-Authentication](https://github.com/koutto/pi-pwnbox-rogueap/wiki/O5.-WPA-WPA2-Personal-(PSK)-Authentication)
- <http://www.c-jump.com/bcc/common/Talk/WIFIconfig/index.html>
- <https://cylab.be/blog/32/how-does-wpawpa2-wifi-security-work-and-how-to-crack-it>
- <https://wifi.pressbooks.com/chapter/securite/>

