# Wi-Fi Technology Fundamentals


Module-4

**Security in Wi-Fi**

Session-4c

Attacks and Vulnerabilities

# Last Session Recap……

## Module-4
**Security in Wi-Fi**
## Session-4b
**Basics of Authentication and encryption**

- ✓ RSN information element
- ✓ EAP authentication mechanisms
- ✓ 4-way handshake
- ✓ Importance of RADIUS Server
- ✓ Demo

# What are Wireless Network Attacks?

Wireless network attacks are deliberate and malicious actions aimed at exploiting vulnerabilities in wireless communication systems to gain unauthorized access, intercept sensitive data, disrupt network operations, or compromise the security of devices and users connected to the network. These attacks target weaknesses in the protocols, configurations, or encryption mechanisms of wireless networks, taking advantage of their inherent nature of broadcasting signals over the airwaves.

# Examples

- Wireless Eavesdropping (Passive Attacks)
- Wireless Jamming
- Rogue Access Points
- WEP/WPA Cracking
- Evil Twin Attacks
- Deauthentication/Disassociation Attacks
- Man-in-the-Middle Attacks
- Replay attacks

# Denial of service attack

Employees

Connected

Access Point
11:22:33:44:55:66

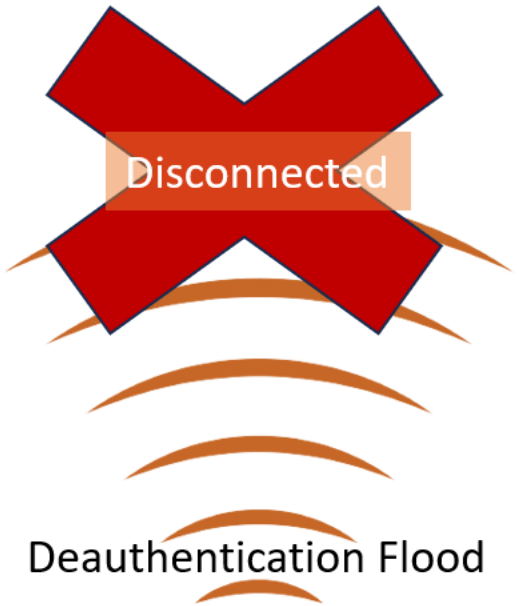
Deauthentication Flood

Spoofed DE-authentication Frame

Source Address: 11:22:33:44:55:66
Destination address: ff:ff:ff:ff:ff:ff

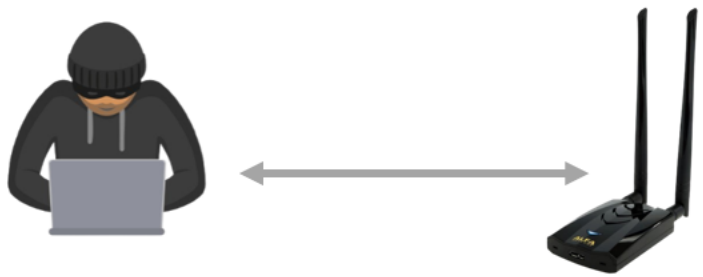
# Denial of service attack

Employees




Deauthentication Flood

Access Point
11:22:33:44:55:66



Spoofed DE-authentication Frame

Source Address: 11:22:33:44:55:66
Destination address: ff:ff:ff:ff:ff:ff

# 802.11W: Management Frame Protection

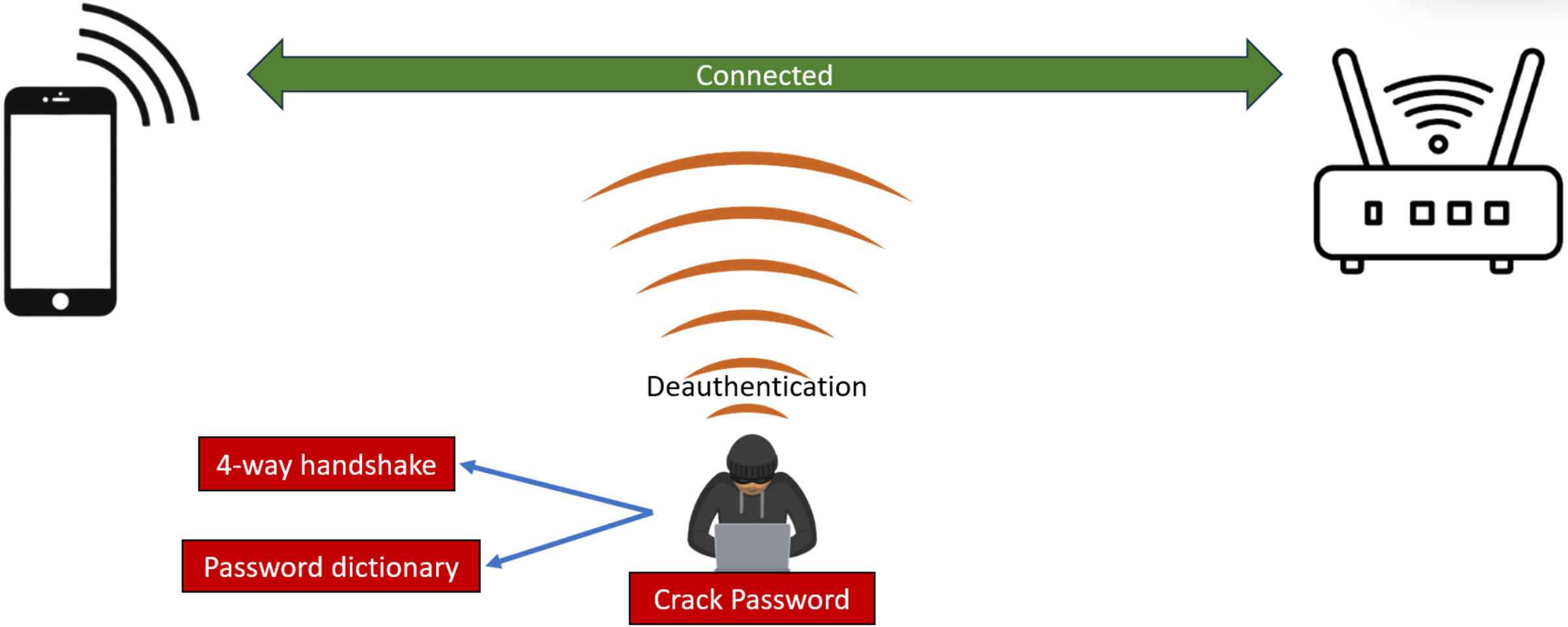
- Client will respond and perform the action to only the frames that are encrypted and coming from the BSSID of the Access Point. If any un-encrypted frame is detected in the network with the BSSID of the Access Point, then the client would be acknowledged in the WPA supplicant logs.
- Broadcast/Multicast management frames are protected using a key called INTEGRITY GROUP TEMPORAL KEY[IGTK].
- Unicast management frames are protected using a key called PAIR-WISE TEMPORAL KEY[PTK].

802.11 w

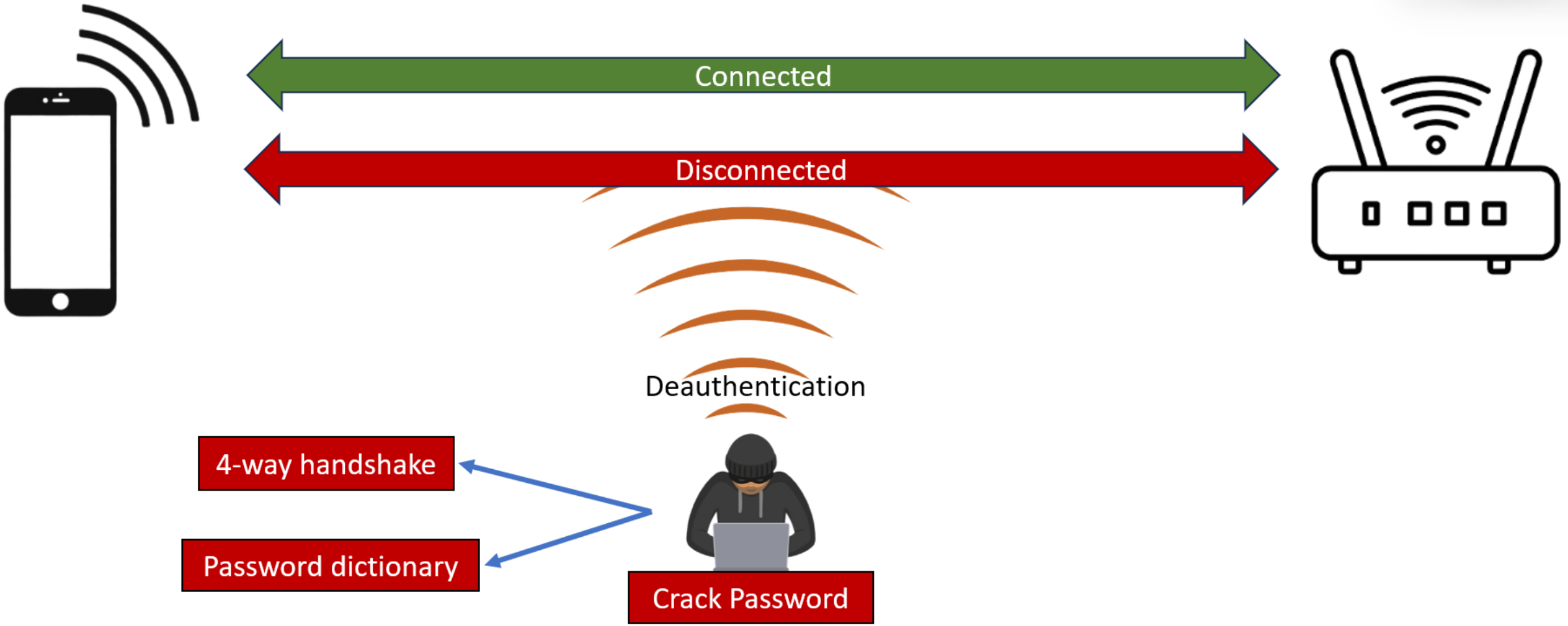
We can protect these kinds of frames using PMF:

- Dis-associations.
- De-authentications.
- Some Action frames.
- Channel switch announcement.

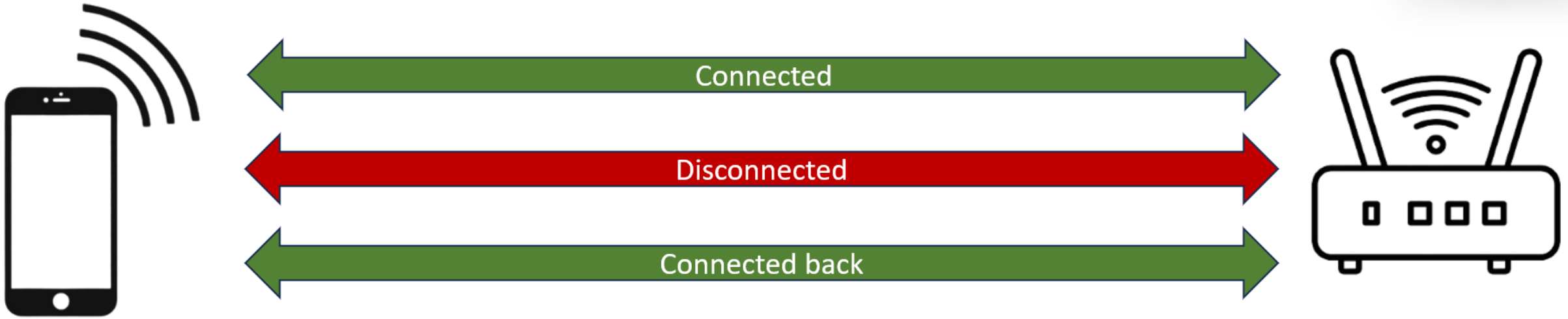
# Cracking WPA/WPA2 Passwords

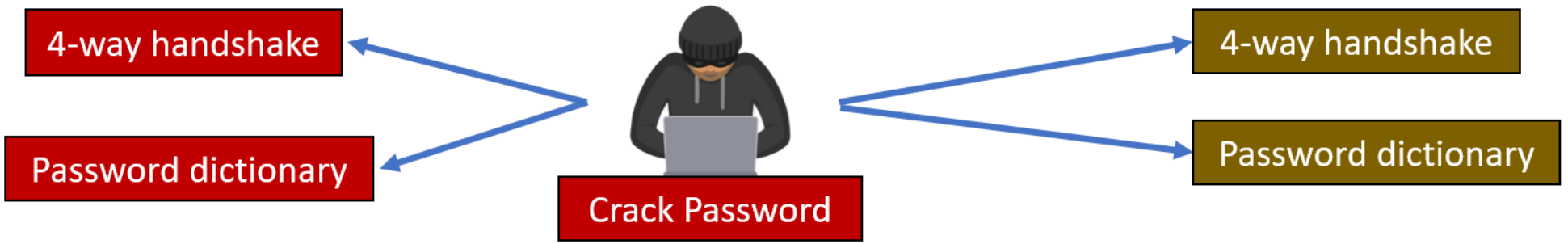


# Cracking WPA/WPA2 Passwords

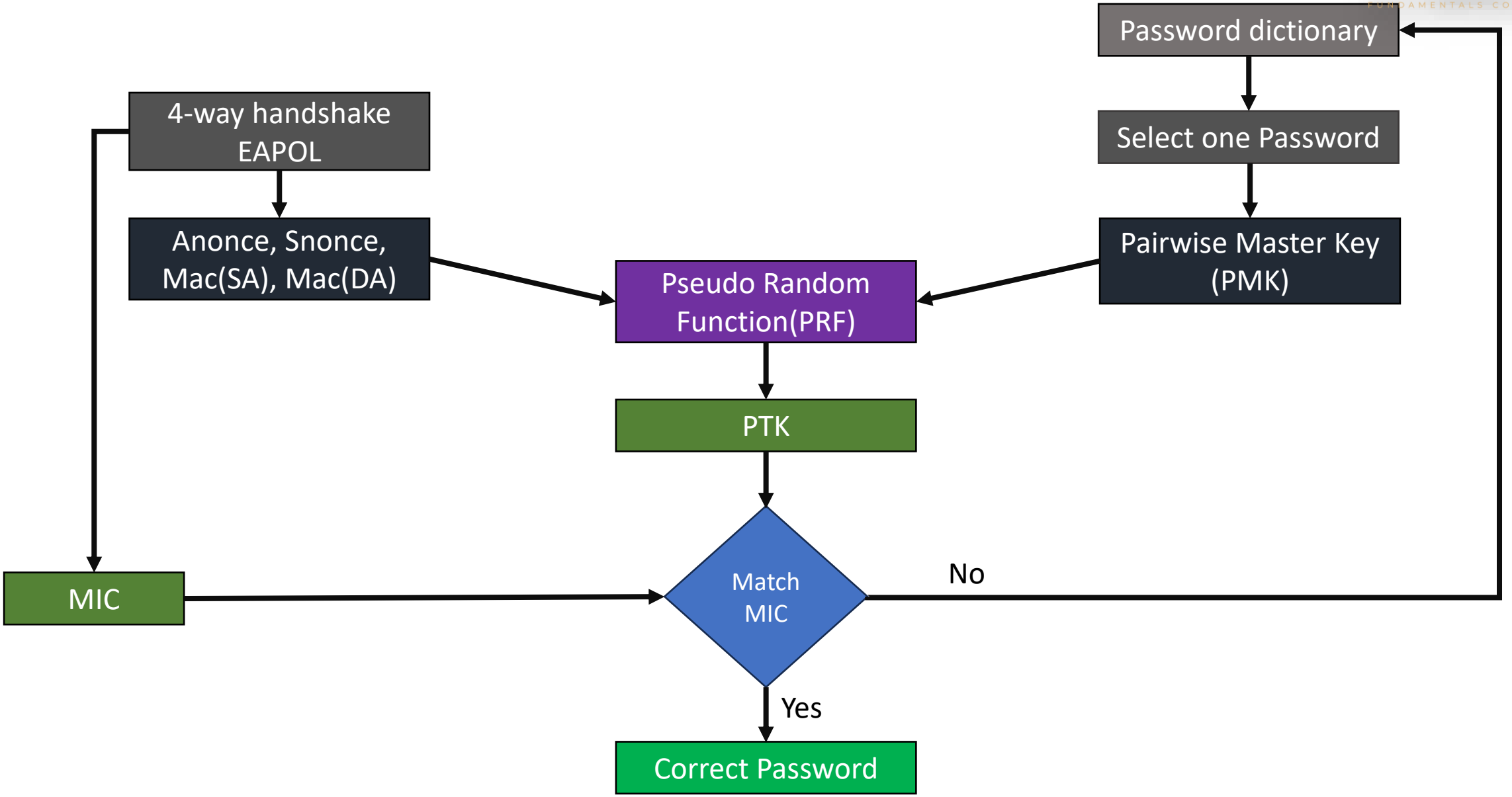


# Cracking WPA/WPA2 Passwords

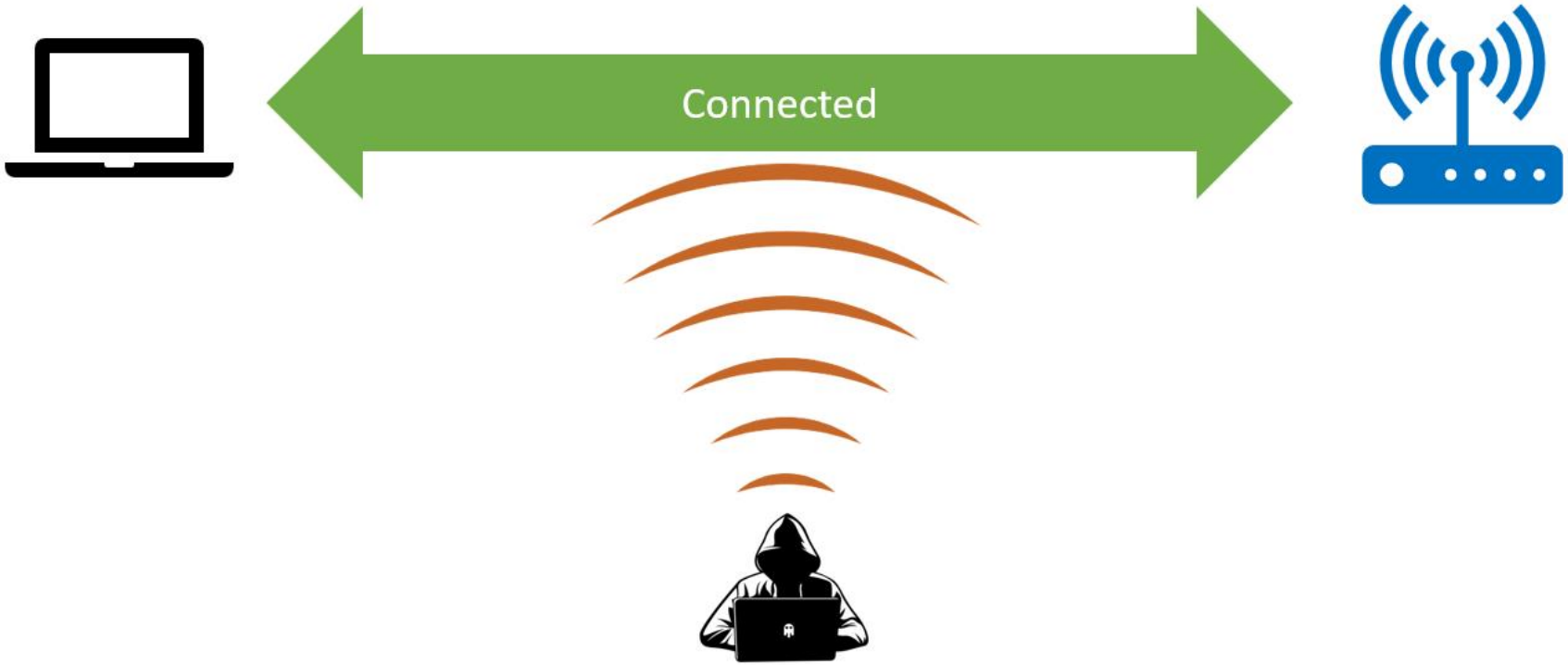


# How attackers crack the password

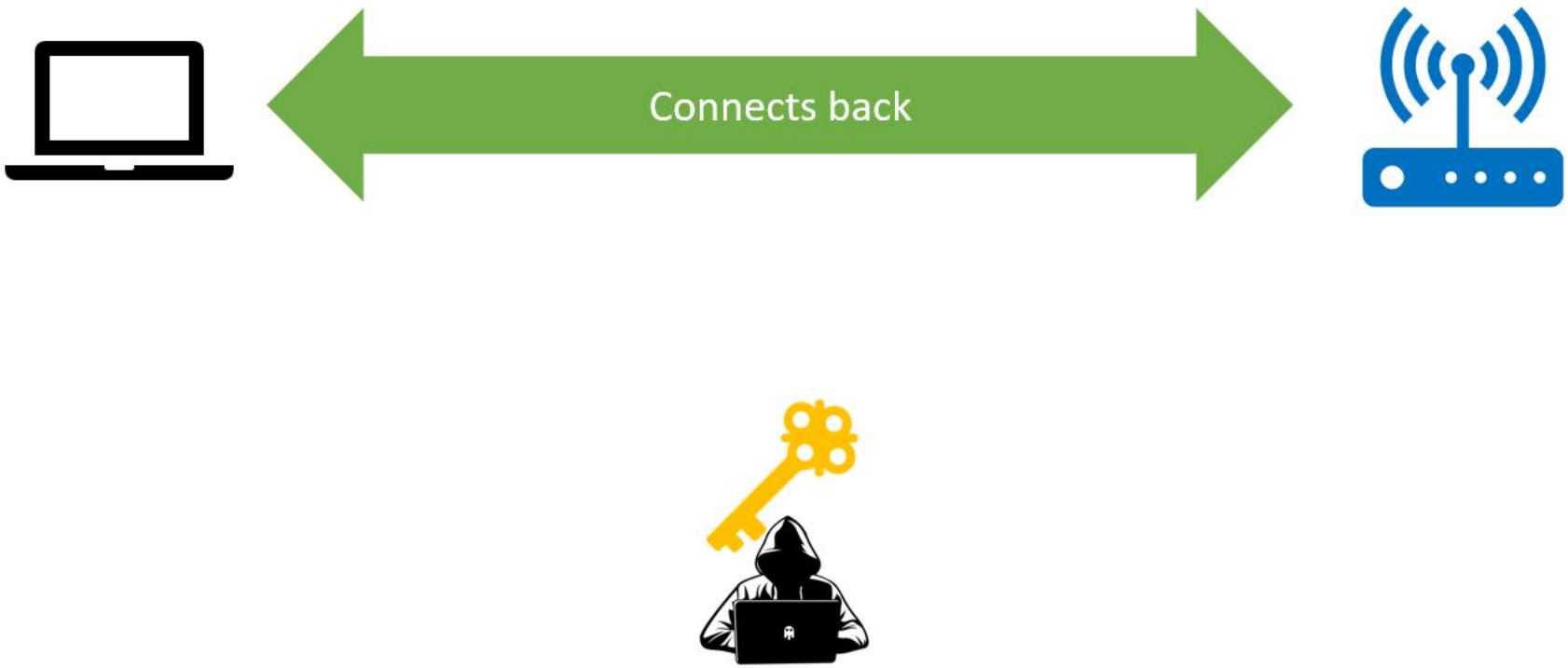


# Evil Twin Attack

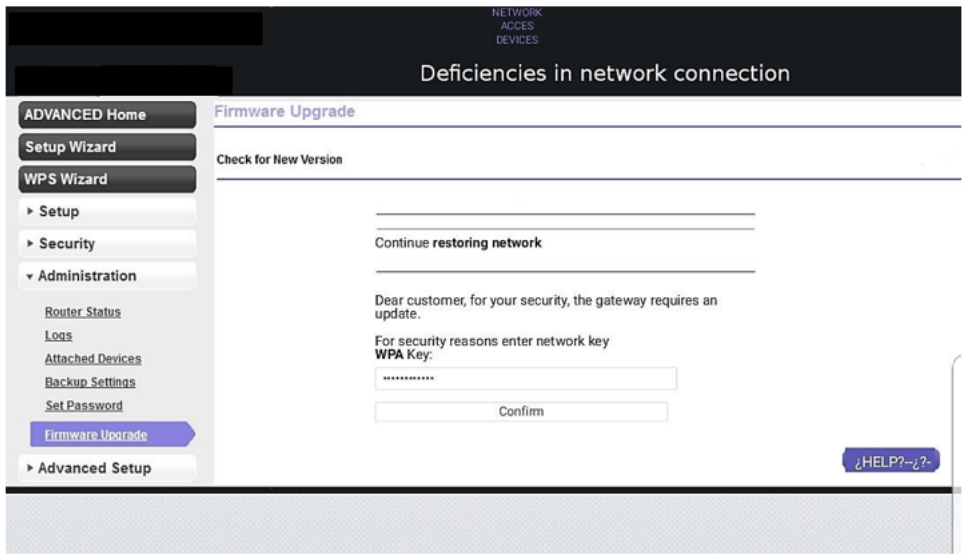


# Evil Twin Attack


# Evil Twin Attack



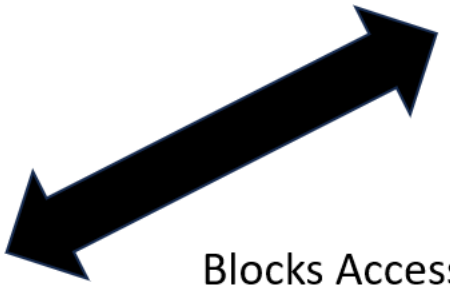
# Evil Twin Attack




Broadcast same SSID
With OPEN authentication
and captive portal

# Evil Twin Attack

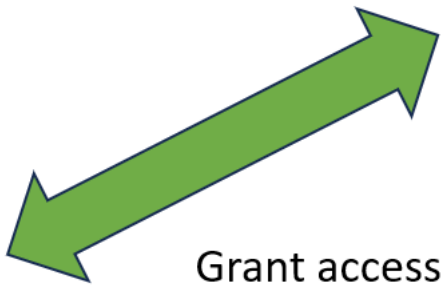
User enters wrong password




Blocks Access to internet

# Evil Twin Attack

User enters the correct password



Internet

Grant access to internet

# Preventing Wireless Network Attacks:



- Avoid connecting to Wi-Fi hotspots that say ‘Unsecure,’ even if it has a familiar name.
- Using a VPN whenever you connect to a public hotspot.
- Visit HTTPs websites only, especially when on open networks.
- Use latest Wi-Fi securities (WPA2/WPA3)
- Create a strong Wi-Fi passphrase
- Changing the default admin account of router that has Wi-Fi enabled.
- Enable 802.11W
- Setting up a RADIUS server and a certificate authority.
- Implementing EAP-TLS to use different keys.
- Use Intrusion Detection System (IDS)
- Use MAC filtering

# References

https://www.konverge.co.in/types-and-prevention-of-wireless-network-attacks/

https://purplesec.us/resources/prevent-cyber-attacks/wireless/

WI-FI TECHNOLOGY
FUNDAMENTALS COURSE


?
QUIZ!
TIME

# Quiz 4b Results


Winner

**Dummu Sneha**

**INDIA**

Number of participants - 69