Attacks on WiFi Security Protocols

Fatimah Bayanooni
Information System Security
Concordia University
40243704

Orlando Lopez Sumalavia
Information System Security
Concordia University
40207755

Ahmad Kanj
Information System Security
Concordia University
40228148

Youssef Masmoudi
Information System Security
Concordia University
40203501

Rahma Tabakh
Information System Security
Concordia University
40218780

Mansoureh Navidpanahtoupkanlou
Information System Security
Concordia University
40221901

Hussein Al-masaabi
Information System Security
Concordia University
56454653

Abstract*— Wireless networks, particularly WiFi, have become the primary mode of network connectivity for both personal and professional use. However, with this increased reliance on wireless networks comes an increased risk of security threats. WiFi security protocols, such as WEP, WPA, and WPA2, have been developed to secure these networks. However, these protocols are not foolproof, and they have been the target of various attacks that exploit their vulnerabilities. This paper will provide an overview of the most common attacks on WiFi security protocols, including packet injection attack, Rogue Access Point attack, brute-force attack, wireless denial-of-service attack, Chop-Chop attack, and key reinstallation attack. Additionally, it will discuss countermeasures that can be employed to mitigate these attacks and provide a more secure wireless network environment. Furthermore, we implemented two attacks that exploit the vulnerability of RC4 stream cipher in WEP protocol:* FMS attack and its successor *PTW attack

Keywords—WiFi, WEP, WAP,* vulnerabilities, *Protocol, attack

I. WI-FI SECURITY PROTOCOLS BACKGROUND

Wi-Fi security protocols use encryption technology to secure networks and protect the data of their clients. The most common Wi-Fi security protocols today are WEP, WPA, WPA2 and WPA3. They use cryptographic keys to randomize data to make it undecipherable.

(1) WEP (Wired Equivalent Privacy): is the oldest and most common Wi-Fi security protocol. It was ratified by Wi-Fi Alliance as a security standard in 1999. It has been plagued over the years by many security flaws and vulnerabilities that had been exploited easily and made it to be officially retired in 2004.

(2) WPA (Wi-Fi Protected Access): It was released in 2003 to address the growing vulnerabilities of its predecessor, WEP. It uses a 256-bit key for encryption, it also uses the Temporal Key Integrity Protocol (TKIP), and dynamically generates a new key for each packet, or unit of data. TKIP is much more secure than the fixed-key system used by WEP. Since TKIP as the core component of WPA, was designed to be implemented onto WEP-enabled systems via firmware updates, It is relying on easily exploitable elements.

(3) WPA2 (Wi-Fi Protected Access 2): is the second generation of WEP which ensures that only people with your network password have access to it. It introduced the Advanced Encryption System (AES) to replace the more vulnerable TKIP system used in the original WPA protocol. Unfortunately, like its predecessor, WPA2-enabled access points (usually routers) are vulnerable to attacks through WEP. To eliminate this attack vector, disable WEP and make sure your router's firmware doesn't rely on WEP.

Here is a breakdown of the three most common Wi-Fi security types and their technical specifications [1]:

	WEP	WPA	WPA2
Year introduced	1999	2003	2004
Encryption protocol	Fixed-key	TKIP	CCMP
Session key size	64-bit/128-bit	256-bit	256-bit
Cipher type	RC4 stream cipher	TKIP (RC4-based)	AES
Data integrity	Cyclic Redundancy Check	Message Integrity Check	CCMP
Authentication method	Open system/Shared key	PSK	PSK + PMK

Key management	Symmetric key encryption	WPA + WPA-PSK	PMK + PSK

II. PACKET INJECTION ATTACK

A. *Definition*

Packet injection attack on Wi-Fi WEP is a sort of attack in which an attacker injects packets within a Wi-Fi network protected by Wired Equivalent Privacy (WEP) encryption. The objective of this attack is to compromise the confidentiality, integrity, and availability of wireless networks. The packet injection attack can be used specially against WEP encryption because it utilizes a shared key to encrypt the entire data packet, where it is easy to crack this key using the appropriate tools. Here, when the key is compromised then the attacker is able now to apply the packet injection attack on the target network. [2][3]

B. *Mechanism*

There are five basic phases in the packet injection attack, and it is described in the below figure.

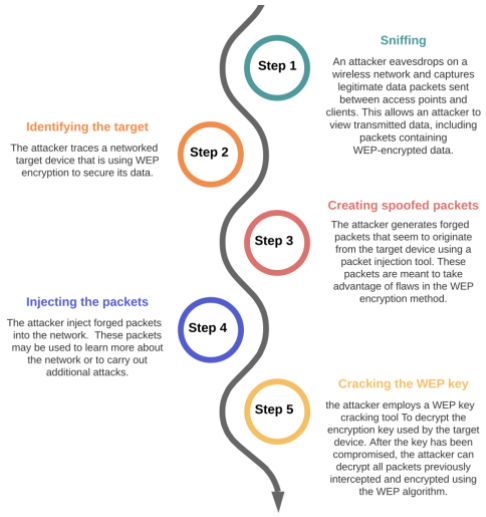


Figure 1Mechanism of Packet Injection Attack

Repeating these actions will allow an attacker to access the wireless network without authorization and might compromise sensitive data [4][5][6].

C. *Tools*

Packet injection attacks on Wi-Fi WEP networks can be implemented by the use of a variety of tools. the most commonly used tools for this kind of attack:

- Aircrack-ng
- Wireshark
- Aireplay-ng
- WepAttack
- Airdecap-ng

D. *Detection techniques*

The detection of packet injection attacks on WiFi WEP may be done using a variety of detection methods:

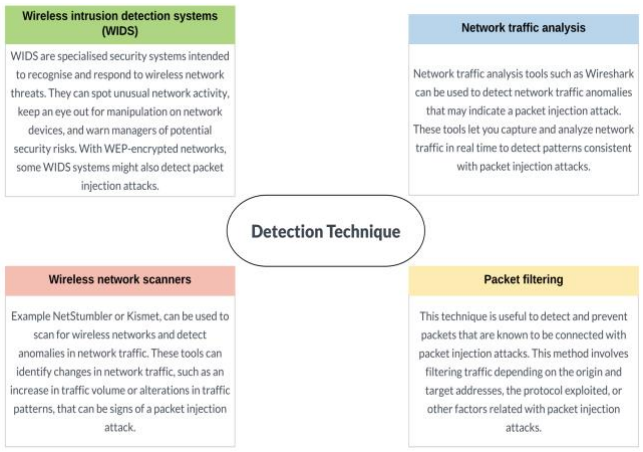


Figure 2 Detection Techniques of Packet Injection Attack

E. *Countermeasures*

Packet injection attacks are a serious threat to the security of WEP-secured Wi-Fi networks, and it is important to take steps to protect against them. Some ways to protect against packet injection attacks on Wi-Fi WEP:

- Upgrade to WPA/WPA2.
- Use stronger encryption keys.
- Implement MAC address filtering.
- Use intrusion detection and prevention systems.
- Limit network access.
- Regularly update network devices.

These countermeasures are all designed to reduce the risk of successful packet injection attacks on WiFi WEP-encrypted networks. Implementing the combination of the above countermeasures will obviously increase the security and reduce the risk of thee attack.[2][7][8]

III. ROGUE ACCESS POINT ATTACK

A. *Description of Rogue Ap*

A Rogue Access Point (Rogue AP) is an unauthorized wireless access point plugged into a corporate and secure WLAN that the network administrator usually does not know about its existence. These Rogue Access Points are frequently part of a coordinated attack; however, without the proper awareness program of users, it is easy to fall victim to the attack. [9]

It is essential to mention the difference between Rogue AP and Evil Twin:

A Rogue AP is physically plugged into a network, granting users access to the secure network. An Evil Twin can also be within the network's physical parameters; however, it is not part of the network and does not inflict damage by directly compromising its security. [9]

Some reasons exist to believe an access point is a rogue:

- First, the SSID of the AP is neither the SSID of the secured network nor listed in the permitted SSID list.
- The AP is masquerading as one of the secured SSIDs.

- The AP is an Ad-Hoc AP formed directly between two client devices.
- Management features disabled, for instance, SNMP, HTTP and Telnet.
- The MAC address of the AP is not listed in the ARP table.
- The AP operates in bridge mode.
- The AP is in the rogue list, added previously by the administrator.

Rogue clients are classified into: [10]

- *Members*: A secured identified member.
- *Neighbour*: Trusted device in a permitted third-party list.
- *Suspect*: Not enough information to define if it is or not a rogue; the administrator makes the decision.
- *Rogue: Proved unauthorized access point.*

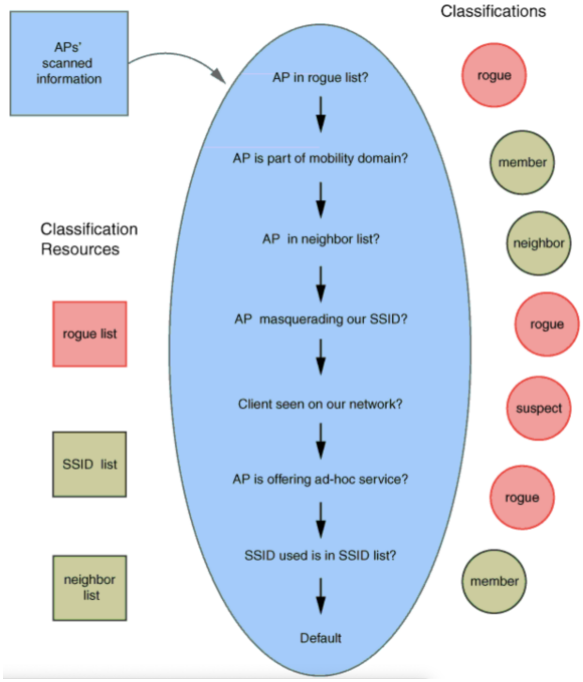


Figure 3 How scanned information is used to classify Aps

B. *Possible Actions of The Attacker*

- The attacker relays messages between the victims, making them believe their connection is private.
- The attacker generates a Denial of Service by flooding the network with useless data.
- The attacker shows a fake SSID with advertising attractive features, so once the user connects, this will be added to their client's wireless configuration, and the client starts to broadcast the fake SSID [10].

C. *Tools for Rogue Ap*

There are six known tools to recreate a Rogue AP:

1- Wifiphisher:
•This tool creates a Man-in-the-middle attack against wireless clients performing associations to access points.
•It also can be customized by using a third-party login page [11].

2- Aircrack-ng suite:
•This tool collects packet captures and exports data to text for use in third-party tools.
•Performs replay attacks and de-authentication attacks by packet injection.
•It can attack WEP. WPA and WPA-2 pre-shared keys [12].

3- Airmon-ng:
•It is used for enabling and disabling monitor mode on the wireless adapter.
•Also, it is used to check if any processes interfere with the aircrack-ng tool [13].

4- Airodump-ng:
•Captures packets of raw 802.11 frames.
•Collects WPA handshakes.
•Captures weak WEP initialization.
•It can show information about the MAC address of the AP, signal level, number of beacon frames, number of captured data packets, channel number, speed, encryption algorithm, cipher detected, authentication protocol used and the SSID of the network. [14]

5- Aireplay-ng:
•It is used to inject frames and generate traffic for later use.
•It can also be used for the following attacks: de-authentication, fake authentication, packet replay, ARP request replay, KoreK chop-chop, fragmentation, cafe-latte, WPA migration (Cisco exclusively) and injection test [15].

6- Airgeddon:
•It can manage the interface mode (monitor and controlled).
•Supports 2.4 and 5 GHz.
•Captures the WPA/WPA-2 handshake.
•Offline password cracking for WPA/WPA2.
•Evil-twin and WPS attacks [16].

D. *Countermeasures to Rogue Attack*

The following are some countermeasures to avoid Rogue AP:

•Disabling SSID Masquerade and Bridging features.

•By default, unknown devices could be classified as Rogue AP.

•Use active access scanning in addition to passive scanning.

•Add known rogue intruders.

•Use certificates in the WLAN and controller.

•Use managed switches on your network and access lists to allow only specific MAC addresses; you can also include the physical ports of connection.

•Investigate wireless bridge frames and eliminate the source.

•Use static IP's for a new AP register instead of a DHCP service.

•Perform regular sweeps of the physical spaces.

•Establish policies that only authorized IT staff can connect networking devices.

•Use hardware-based micro-segmentation to isolate endpoints onto their own protected micro-segments; this strengthens defences against lateral movements and increases granular control.

• Use network-wide Intrusion Detection and Prevention System (IDS/IPS).

IV. BRUTE FORCE ATTACK AGAINST THE 4-WAY HANDSHAKE OF WPA/WPA2

A. *Definition of WPA-PSK*

The definition of PSK (pre-shared key) is based on users using an initial secure channel to deliver a key to send later messages where the encryption depends on the initial PSK.

WPA-PSK encrypts data transmission in 128 bits and is controlled by a password generated by the end user.WPA-PSK can be used with AES standards and does not require a central server; it is usually designed for home or small networks. [17][18]

B. *Pairwise Master Key Generation*

Starting with the PSK, each device stores a PMK (pairwise master key) until the PSK or SSID changes. If a client tries to connect, a protocol named 4-Way Handshake is initialized to generate a PTK (pairwise transient key). The objective of the key is to encrypt the data between a client and the access point; this key usually changes at least 65,535 packets.

PMK is computed using PBKDF2 (password-based key derivation function 2), which reduces vulnerabilities to brute force attacks because of the high computational cost. [18]

WPA protocol generates the PMK as:

PMK = PBKDF2 (HMAC-SHA1, PSK, SSID, 4096, 256)

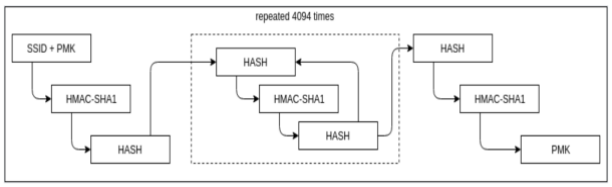


Figure 4 PMK equation

C. *4-Way Handshake*

The goal of the 4-Way Handshake is to provide mutual authentication based on a PMK to negotiate a new PTK session key.

The PTK results from the PMK, two nonces and the MAC addresses of the client and the authenticator. [19]

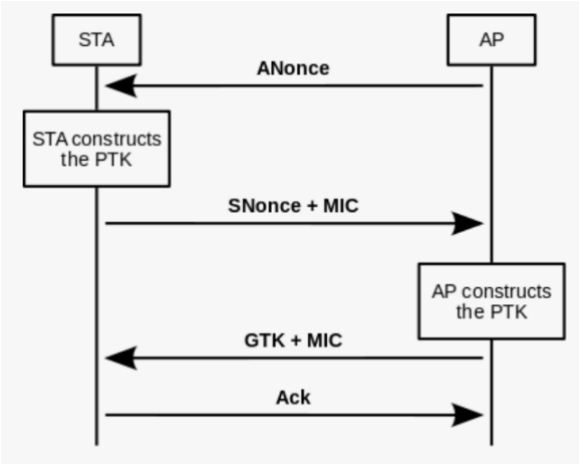


Figure 5 4-Way Handshake Diagram

Steps:

1. The AP sends an Authenticator Nonce (ANonce) to the client (STA).
2. The STA builds the PTK and sends its own Nonce (SNonce) to the AP; this way, it protects the frame with a Message Integrity Code (MIC).
3. The AP generates and sends the Group Temporary Key (GTK) and a sequence number. In addition, a MIC is used to protect the frame and prevent tampering.
4. Finally, the STA sends an acknowledgement to the AP indicating it is ready for encryption. [19]

D. *Cracking the 4-Way Handshake*

To carry out the attack, the attacker can use the tool Crunch and Airgeddon; the last one was previously mentioned and described in the Rogue AP attack. Crunch is a word list generator where an attacker can specify a standard character set or any set of characters to generate word lists created through a combination and permutation of a group of characters. It also allows the attacker to set the number of characters and list size [20].

Steps:

1.Monitoring/Scanning:

First, the network interface must be enabled to allow active monitoring mode in the attacker interface. [20]

2.Capture Packets:

In this step, Airgeddon captures 802.11 frames.This tool shows a table with the following information: BSSID (Basic Service Set Identifier), MAC address, the channel the device is broadcasting on, encryption used, and the Extended Service Set Identification (ESSID) of the network or the Service Ser Identifier SSID. [21]

3.Capture 4-Way Handshake

Users must be revoked from the network to force them to re-authenticate to capture the 4-Way Handshake. Then, during user re-authentication, Airgeddon captures the packets with the 4-Way Handshake. [21]

4. Cracking the password

Users must be revoked from the network to force them to re-authenticate to capture the 4-Way Handshake. Here the attacker uses Crunch for the Brute Force method; the initial parameters must be set to direct the attack. This means that if the attacker has clues to the password, he can choose the options he deems convenient to make the attack shorter but effective. For example, if the attacker chooses the only number option, starting at 000000000 and incrementing the value each turn, it will go until 999999999. Each time check the new value captured in the 4-Way Handshake. [21]

E. *Countermeasures*

The following are some countermeasures to avoid this attack:

• Changing the default Wi-Fi password to something complex and longer will increase the time; theoretically, it would take an attacker to crack it.

- Make an asset review frequently by looking at all connected devices to the Wi-Fi.
- Implement whitelisting by configuring only the MAC addresses of the devices we want to connect to the Wi-Fi.
- Be aware of some misbehaviours of the devices in the network, for instance, frequent Wi-Fi disconnection, slow internet surfing, etc. [21]

V. WIRELESS DENIAL OF SERVICE (WDOS) ATTACK

A. *Definition*

Today, a denial-of-service attack is considered an easy attack as the nature of wireless networks is that the medium is shared between the nodes in the network. The attacker achieves the denial of service (DOS) attack by blocking access to the medium by flooding the traffic with packets or by interfering with the network's reception. The wireless DoS attacks can be classified into two categories [22]:

1. Physical layer attacks: these attacks target the reception process and the transmission communication of the network. It involves disturbing or interfering a legitimate communication. These are some examples of attacks that target the physical layer:
   - Jamming attack:
   - De-authentication attack
   - Beacon flooding attack
2. Protocol layer attacks: these attacks target the wireless network's protocol layer. These attacks involve manipulating the communication between the client and the AP or disturbing the network communication. These are some examples that target the protocol layer of the network:
   - Fragmentation attack
   - ARP spoofing attack
   - WPA/WPA2 cracking attack

B. *Mechanism*

A de-authentication attack is a kind of DoS attack that exploits the authentication WPA protocol by sending a forged de-authentication frame to the AP, causing the client to disconnect from the AP. This is the mechanism of the attack:

1. First, the attacker uses Airplay-ng tool to capture four-way handshake between the client and the AP.
2. Then attacker sends a series of forged de-authentication packets to the AP to end the communication session with the client (victim) and force the reauthentication process for the client.
3. The attacker impersonates the client and authenticates himself to the AP.

Denial of service can be achieved by the attacker when he continuously sends de-authentication packets, causing a DoS attack on the target network. A successful de-authentication attack denies the clients from accessing the network's resources and causes them to lose connection to the network. In addition, this attack can be used to create further attacks like MITM attack or allow the attacker to crack the WPA encryption key.

C. *Tools*

These are the tools used to achieve different types of wireless DoS attacks [23][24]:

- Airmon-ng
- Airodump-ng
- Aireplay-ng
- mdk3: this tool is used to inject data into the wireless network. It's usually used to exploit WIFI 802.11 vulnerabilities.

D. *Detection*

The following are detection techniques to detect de-authentication attack:

- Mac address spoof detection:

  This technique is used to analyze the sequence number pattern of the captured traffic to detect de-authentication attack. Detection systems showed that they were able to capture and detect MAC spoofing attacks traffic to identify de-authentication attack.

- Wireless intrusion detection system

  WIDS is used to monitor and capture malicious traffic that flows inside the network.

- Wireless AP logs

  In this detection technique, the AP maintains a log of the network's traffic to identify suspicious or unusual activities that can initiate an attack on the network.

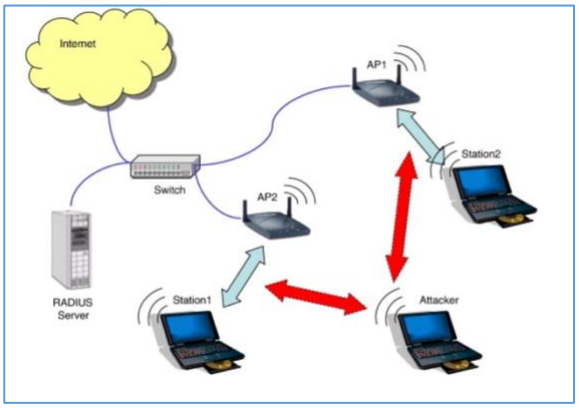


Figure 6 Generic DoS Attack

E. *Countermeasures*

Denial of service attack is a powerful attack that threatens the availability and the security of the network. However, there are defensive techniques to encounter it. The following are techniques to mitigate the risk of deauthentication attack on the wireless network:

- Upgrade to secure WIFI protocol by upgrading the WIFI protocol to secure protocols like WPA2 or WPA3 this minimizes the chance of DoS attack to occur on the network.

- Configure AP to drop deauthentication packets that originate from outside the network.
- Implementing network access control (NAC).

VI. CHOP-CHOP ATTACK

A. Definition

A chop-chop attack is a passive attack that breaks the confidentiality and integrity of the message. In this attack, the attacker tries to obtain information about the message from its ciphertext by repeatedly manipulating and retransmitting the packet until the attacker is able to determine the pre-shared key (PSK) used to encrypt the network traffic [26]. This attack is used to exploit the weaknesses of WEP. However, it's not effective against more secure encryption protocols like WPA and WPA2 with robust security features [27].

B. Mechanism

Let's assume the following conditions of the network that will be attacked [28]:

- IPv4 protocol is used where the attacker knows most bytes of the IP addresses in the network (ex. 192.168.1.X).
- The network is using TKIP which is used by the client to communicate with the access point (AP).
- IEEE 802.11e QoS features are supported by the network which allows 8 different channels for data flow.
- A long re-keying interval for TKIP is being used.

These network conditions are quite realistic for most networks deployed today. For the attacker to create a chop-chop attack against a network. First, the attacker captures an encrypted ARP request/response from the network's traffic. From this ARP packet, most of the plaintext of it is known to the attacker except the 4 bytes of the MIC, 12 bytes of the ICV (checksum), and the last byte of the source and destination IP addresses. Then, the attacker tries to guess the ICV by repeatedly manipulating the packet and sending it to the AP. When the AP receives the ARP packet it will check the last byte of the packet. If it is incorrect, it will drop it else it will send a response to the attacker where he concludes that he successfully guessed ICV. Then the attacker goes back through the rest of the bytes until he guesses the entire packet bytes [29]. With this attack, the attacker will be able to recover the MIC key, the keystream to decrypt the messages, and construct further advanced attacks.

C. Tools

Chop-chop attack can be achieved using the following tools:

- Airodump-ng
- Aireplay-ng
- Packetforge-ng: This tool is used to create encrypted packets that are used for injection. Most common use of it is to create ARP requests that will be used for an injection attack [30].
- Aircrack-ng

D. Detection

There are different techniques that can be used to detect the chop-chop attack. The following are some of the techniques:

- Packet sniffing tools: these tools are used to detect the chop-chop attack by monitoring data packets with incorrect checksum. The tool will capture and analyze data packets in the traffic to identify the chop-chop attack before it occurs.
- Wireless intrusion detection system: this system checks the anomaly behaviours in the network traffic like an unusual amount of network traffic at certain times or an unusual number of retransmissions from the client.
- Network traffic analysis: these tools are used to detect chop-chop attacks by looking for patterns in the network traffic.

E. Countermeasures

The following are countermeasures to prevent chop-chop attack:

- Use short rekeying time.
- Disabling the client from sending MIC failure report frame to the AP.
- Allow CCMP in the network and disable TKIP.

In addition, TKIP provides the following to prevent chop-chop attack [28]:

1. If the AP receives a correct, but it's out of order (lower value for the TSC counter), so the AP discards it.
2. If the client receives a packet with a correct checksum however when he verifies the MIC and the verification fails, an attack is assumed, and the AP is notified by sending a MIC failure report frame.

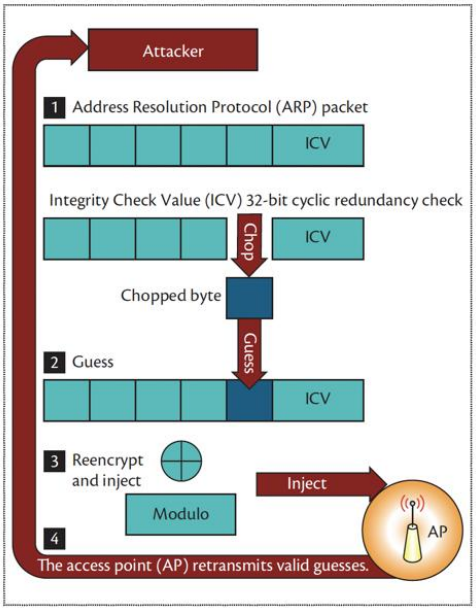


Figure 7 Chop-Chop Attack Mechanism

VII. KRACK (KEY REINSTALLATION ATTACK)

A. Description

This attack abuses design or implementation flaws in cryptographic protocols to reinstall an already-in-use key. This resets the key's associated parameters such as transmit nonces and receive replay counters. As you know all protected Wi-Fi networks use the 4-way handshake to generate a fresh session key. As described earlier in section IV-part C, The 4-

way handshake provides mutual authentication and session key agreement. Together with (AES)-CCMP, a data-confidentiality and integrity protocol, it forms the foundation of the 802.11i amendment. 4-way handshake is a process after association of the client to the Access Point, and after that Group by handshake will happen. Since its first introduction in 2003, under the name WPA, this core part of the 802.11i amendment has remained free from attacks except for known weaknesses of 802.11i are in (WPA-)TKIP. However, now it has been proved that the 4-way handshake is vulnerable to a key reinstallation attack.

B. Attack steps

In 4-way handshake architecture, there are three different key reinstallation attack scenarios base on the following vulnerable components [31]:

- 1- Typical PTK 4-Way Handshake between AP and a client
- Peerkey 4-way Handshake for communication between peer client
- Group Key Handshake for AP to inform its existence
- Fast BSS Transition (FT) Handshake

The impact of exploiting these vulnerabilities includes decryption, packet replay, TCP connection hijacking, HTTP content injection, and others. The way that Man in The Middle (MITM) works for these scenarios is the channel side MITM.[31] In two state the attack can happen; when the client (victim) accepts plaintext retransmissions of message 3 and when the victim only accepts encrypted retransmissions of message 3 as shown in Figures 8 and 9 [32].

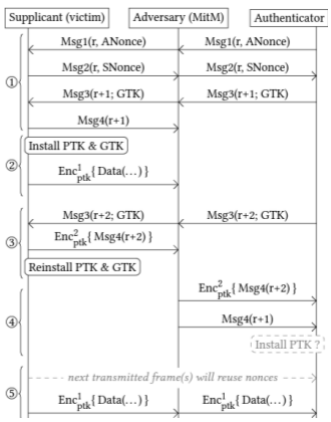


Figure 8 Attack in Plaintext Retransmission of msg3

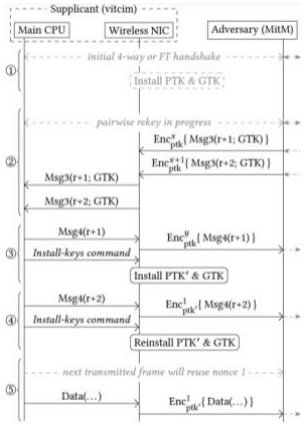


Figure 9 Attack in Encrypted Retransmission of msg 3

1- Attack while Plaintext Retransmission of message 3 :

in this case the adversary uses a channel-based MitM attack and manipulate handshake messages [32] .

o The attacker blocks message 4 from arriving at the authenticator. This is illustrated in stage 1 of Figure 8.

o Immediately after sending message 4, the victim will install the PTK and GTK. At this point the victim also opens the 802.1x port, and send normal data frames. The first data frame uses a nonce value of 1 in the data-confidentiality protocol.

o Then, in the third stage of the attack, the authenticator retransmits message 3 because it did not receive message 4. The adversary forwards the retransmitted message 3 to the victim, causing it to reinstall the PTK and GTK. Therefore, it resets the nonce and replay counter used by the data-confidentiality protocol.

2- • Attack while Encrypted Retransmission of message 3 :

Figure 9 illustrates the details of the attack. Th AP actions are clear from context while it's not in the image. Similar to the previous scenario, Again, the adversary uses a channel-based MitM position. [32]

o Fist Adversary lets the victim and adversary execute the initial 4-way handshake, and waits until a second 4-way handshake is initiated to refresh the PTK.(Base on the unique length of message.) Unlike the previous case of attack.

o in stage 2, the adversary does not instantly forward the first message 3 but waits until the AP retransmits message 3, and then forwards both messages right after one another to the victim. The wireless NIC decrypt both messages using the current PTK, and forwards them to the packet receive queue of the main CPU.

o In the third stage of the attack, the main CPU of the victim processes the first message 3, replies to it, and ask NIC to install the new PTK.

o In the fourth stage, the main CPU picks the second message 3 from the receive queue. Since a PTK is installed, the main CPU will mandate that the message was encrypted. However, it does not check under which key the message was encrypted. As a result, even though the message was decrypted under the old PTK, the main CPU will process it. The message 4 sent as a reply is now encrypted under the new PTK using a nonce value of 1.

o After this, the main CPU commands the NIC to reinstall the PTK, thereby resetting the nonce and replay counters. Finally, the next data frame that the victim transmits will again be encrypted using the new PTK with a nonce of 1.

C. Attack Tools

The way this attack works uses the MITM attack side channel, therefore all tools that can do the MITM side channel attack can be used in this scenario [31]. This attack has been never reported by attacker or cybersecurity companies, but some Cybersecurity concerned companies [33], discovered the potential attack in 2017 , and then they asked the vendors release the related patches to prevent it happen in real world.

In Feb. 2020, RSA company and ESET presented a potential attack based on the 4-way hand shake vulnerability and the vulnerability of some WiFi Chipset (Broadcom and Crypress). They discovered it when they were working on a new product, Amazon EC2. This new vulnerability was called Kr00k because it was the result of resetting the master key to "All Zero" in the hardware chipset by default after disassociation of the client from the AP. It leads the MITM can decrypt all messages that still are in the buffer until the new handshake happen. [33]

D. Countermeasures

Changing your WiFi network password or even swapping out your network router is not going to help [34]. The key to mitigating this vulnerability is patching the software. The vendor companies were informed of this vulnerability and

releases some updates and patches.[34]. The Vendors that released patched included:

O Cisco ,Intel ,Netgear ,Aruba

O OpenBSD released WPA2 patches, Debian also released patches and Ubuntu fixes have been issued.

O Microsoft, Apple and Google have stated that patches as soon as they asked.

It should be mentioned that, if the device that is being used does not have any patch available, the countermeasure is to disable the retransmission of message 3 while in a normal operation it should not be disabled. [31]

VIII. FMS (Fluhrer, Mantin, Shamir)/Korek Attack

A. Overview

During 2001, Fluhrer, Mantin, Shamir published a paper with the name: "Weaknesses in the Key Scheduling Algorithm of RC4" that uncovered a weakness in stream ciphers which can be used to crack wireless access points using WEP security protocol. [35][26][39]

FMS is a statistical attack that targets the vulnerability present in RC4 stream cipher. This attack allows the allows the recovery of the key of the RC4 encrypted stream. [35][39]

The attack depends on the use of the initialization vectors in RC4, which are a type of input required to provide an initial state. The attacker then can derive bytes of the key based on a mathematical equation derived from the keystream. The attacker will store a large amount of messages in order to retrieve the key see Figure 10 [38][39][44].

2004: Korek is an internet user that developed several attacks over WEP protocols. A group of Korek's attacks relied on the principals of the FMS attack.[39]

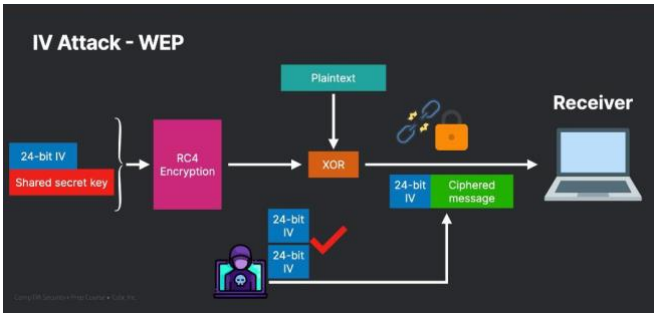


Figure 10 FMS Attack Overview

B. Tools

- Aircrack-ng: Password cracking software
- Airodump-ng: Wireless packet capture tool
- Wifi-adapter: Hardware for wireless communication

C. Implementation

The implementation will be carried out using kali linux by using airodump-ng in order to get capture packets from the target network. When sufficient number of packets are collected. Aircrack-ng will conduct a statistical attack using the FMS/Korek technique in order to exploit the weakness in RC4 and decrypt the key.

The process of the implementation is discussed in details in the appendix (section A).

IX. PTW (Pychkine, Tews, Weinmann) attack

A. Overview

Created in 2007, the PTW attack was based on an attack from 2005 called Klein attack. The PTW attack is more efficient than its predecessor FMS/Korek.[39]

PTW attack takes advantage of WEP reusing IVs to encrypt packets. This is a weakness because RC4 which is the stream cypher used in WEP protocol generates the keystream in a predictable way. The attacker captures enough packets and compares them to derive information about the keystream. this attack is able to decrypt the key with fewer packets than FMS due to the better correlation deduced between encrypted data and the keystream. [35][36]

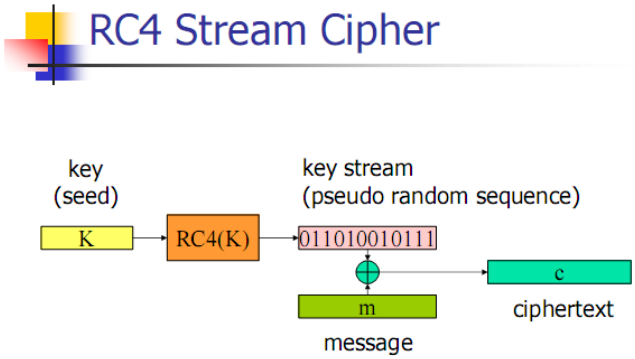


Figure 11 PTW Attack Overview

B. Tools

It uses the same tools as its processor the FMS attack:

- Aircrack-ng: Password cracking software
- Airodump-ng: Wireless packet capture tool
- Wifi-adapter: Hardware for wireless communication

C. Implementation

The implementation will be carried out using kali linux by using airodump-ng in order to get capture packets from the target network. When enough packets are collected. Aircrack-ng will conduct a combination of statistical and computational algorithm in order to exploit the weakness in RC4 and decrypt the key.

The process of the implementation is discussed in details in the appendix (section B).

Conclusion

To sum up, WiFi has become the primary mode of network connectivity for personal and professional use, but it also comes with increased security risks. Despite the development of WiFi security protocols, these networks are still vulnerable to a range of attacks, including packet injection, rogue access points, brute-force attacks, wireless denial-of-service, Chop-Chop attacks, and key reinstallation attacks. This paper has highlighted these attacks and discussed various countermeasures that can be used to mitigate them and improve the security of wireless networks. Additionally, the paper has implemented two attacks that exploit the vulnerability of RC4 stream cipher in WEP protocol. It is essential for network administrators and users to be aware of

these threats and take the necessary steps to safeguard their networks. By doing so, we can create a more secure wireless network environment and reduce the risk of security breaches

REFERENCES

[1] D.Ghimiray, "Wi-Fi Security: WEP vs WPA or WPA2" , Avast.com, https://www.avast.com/c-wep-vs-wpa-or-wpa2 , Accessed: 2'nd March, 2023

[2] T. Wrightson, "Wireless Network Security: A Beginner's Guide", (2011)..

[3] J.Wright, J.Cache, and V.Liu ,"Hacking Exposed Wireless, Third Edition: Wireless Security Secrets & Solutions", (2015).

[4] A. Al-Shemery, A.Gupta, and V.Velu, "Mastering Wireless Penetration Testing for Highly Secured Environments", (2015).

[5] S.Bhattacharya, J.K. Kalita, & S.Kar,. "A survey of security issues in wireless networks.", Journal of Network and Computer Applications, 35(2), 534-552, (2012).

[6] N.Thakur, & A.Jindal, "Packet Injection Attacks on Wi-Fi Security Protocols". Springer (pp. 375-388),(2018).

[7] M.Ciampa, "Security+ Guide to Network Security Fundamentals, 5th Edition", (2015)

[8] S.Bosworth, M.E. Kabay, and E.Whyne "Computer Security Handbook, 6th Edition", (2014)

[9] BYOS, "How to protect against Rogue Access Points on Wi-Fi.", Accessed: March 7, 2023. [Online] https://www.byos.io/blog/how-to-protect-against-rogue-access-points-on-wi-fi

[10] Juniper, "Understanding Rogue Access Points.", Accessed: March 7, 2023. [Online] https://www.juniper.net/documentation/en_US/junos-space-apps/network-director4.0/topics/concept/wireless-rogue-ap.html

[11] Kali.org, "Wifiphisher Tool Documentation.", Accessed: March 8, 2023. [Online] https://www.kali.org/tools/wifiphisher/

[12] Aircrack-Ng Official Website Aircrack-ng.org. Accessed: March 8, 2023. [Online] https://www.aircrack-ng.org/

[13] Airmon-ng Documentation Aircrack-ng.org. Accessed: March 9, 2023. [Online] https://www.aircrack-ng.org/doku.php?id=airmon-ng

[14] "Airodump-ng Documentation", *Kali Tools*. Accessed: March 9, 2023. [Online] https://en.kali.tools/?p=367#:~:text=airodump%2Dng%20%2D%20a%20wireless%20packet,of%20the%20found%20access%20points

[15] "Aireplay-ng Documentation", *Aircrack-ng.org*. Accessed: March 10, 2023. [Online] https://www.aircrack-ng.org/doku.php?id=aireplay-ng#:~:text=Description,WEP%20and%20WPA%2DPSK%20keys

[16] "Airgeddon Tool Documentation.", *Kali.org*. Accessed: March 10, 2023. [Online] https://www.kali.org/tools/airgeddon/

[17] M.Rouse, "Wi-Fi Protected Access Pre-Shared Key", Techopedia. Accessed: March 12, 2023. [Online] https://www.techopedia.com/definition/22921/wi-fi-protected-access-pre-shared-key-wpa-psk

[18] A.Croix, "How does WPA/WPA2 Wifi security work, and how to crack it?", *Cylab*. Accessed: March 16, 2023. [Online] https://cylab.be/blog/32/how-does-wpawpa2-wifi-security-work-and-how-to-crack-it?accept-cookies=1

[19] J. Lorenz,"Taking advantage of the 4-Way Handshake.", *The University of Hawai'i-West O'ahu*. Accessed: March 18, 2023. [Online] https://westoahu.hawaii.edu/cyber/forensics-weekly-executive-summmaries/taking-advantage-of-the-4-way-handshake/

[20] "Crunch Tool Documentation", *Kali.org*. Accessed: March 18, 2023. [Online] https://www.kali.org/tools/crunch/

[21] J.Weston, "Wi-Fi Attacks – Cracking the Handshake", *LinkedIn blog* Accessed: March 18, 2023. [Online] https://www.linkedin.com/pulse/wi-fi-attacks-cracking-handshake-james-weston/

[22] K.Bicakci, B.Tavli, "Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks", *Computer Standards & Interfaces*, Volume 31, Issue 5, 2009, Pages 931-941, ISSN 0920-5489, https://doi.org/10.1016/j.csi.2008.09.038.

[23] "Deauthentication Attack using Kali Linux," SudoRealm. https://sudorealm.com/blog/deauthentication-attack-using-kali-linux (accessed Mar. 30, 2023).

[24] "Denial of Service Attack", Packt, https://subscription.packtpub.com/book/networking-&-servers/9781785280856/6/ch06lvl1sec27/denial-of-service-attacks (accessed Mar. 30, 2023).

[25] K.Pelechrinis, M.Iliofotou, Marios, S.Krishnamurthy, "Denial of Service Attacks in Wireless Networks: The Case of Jammers". IEEE, IEEE. 13. 245 - 257. 10.1109/SURV.2011.041110.00022

[26] "korek_chopchop", *Aircrack-ng*. https://www.aircrack-ng.org/doku.php?%20id=korek_chopchop (accessed Mar. 30, 2023).

[27] F.T. Sheldon, J.Weber, S.Yoo, & W.D.Pan, "The Insecurity of Wireless Networks. Security & Privacy", IEEE. 10. 54-61. 10.1109/MSP.2012.60.

[28] M.Beck, E.Tews," Practical attacks against WEP and WPA". *IACR Cryptology ePrint Archive*. 2008. 472. 10.1145/1514274.1514286.

[29] "WPA Attacks," *Wireless Network Security*. http://wirelessnetworkssecurity.blogspot.com/2013/01/wpa-attacks.html (accessed Mar. 30, 2023).

[30] "packetforge-ng",*Aircrack-ng*. https://www.aircrack-ng.org/doku.php?id=packetforge-ng (accessed Mar. 30, 2023).

[31] B.Buchanan, "CRACK is Back", *Medium.com*, https://medium.com/asecuritysite-when-bob-met-alice/krack-is-back-meet-kr%C3%B8%C3%B8k-c0832fd4b598 , Accessed : 9 March [Online]

[32] M.Vanhoef, F.Piessens, "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2", 2017, https://papers.mathyvanhoef.com/ccs2017.pdf , Accessed: 9 March

[33] CWNPTV ,"KRACK - The Details and the Reality", *YouTube* , https://www.youtube.com/watch?v=pjTTG2nZax0, Accessed : 16 March [Online]

[34] R. Persy, "WPA2 KRACK Attack: The WiFi Hack and What it Means," *Auth0 - Blog*. https://auth0.com/blog/krack-attack-wpa2-and-what-it-means/ (accessed Mar. 30, 2023).

[35] Fluhrer, S., Mantin, I., and A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", *Selected Areas of Cryptography: SAC* 2001, Lecture Notes in Computer Science Vol. 2259, pp 1-24, 2001.

[36] Rivest, Ron. "RSA Security response to weaknesses in key scheduling algorithm of RC4." *Technical note, RSA Data Security*, Inc (2001).

[37] Tews, Erik. "Attacks on the WEP protocol." *Cryptology ePrint Archive* (2007).

[38] Tews, Erik, and Martin Beck. "Practical attacks against WEP and WPA." Proceedings of the second *ACM conference on Wireless network security*. 2009.

[39] Packt, "What we can learn from attacks on the WEP Protocol," *Packt Hub*, Aug. 12, 2015. https://hub.packtpub.com/what-we-can-learn-attacks-wep-protocol/ (accessed Mar. 30, 2023).

[40] "airmon-ng" , *Aircrack-ng*. https://www.aircrack-ng.org/doku.php?id=airmon-ng (accessed Mar. 30, 2023).

[41] "aircrack-ng" , *Aircrack-ng*. https://www.aircrack-ng.org/doku.php?id=aircrack-ng (accessed Mar. 30, 2023).

[42] "airodump-ng" , Aircrack-ng. https://www.aircrack-ng.org/doku.php?id=airodump-ng (accessed Mar. 30, 2023).

[43] A. Navaz, S. Syed & K.Girija,." Hacking And Defending In Wireless Networks", *Journal of Nano Science and Nano Technolgy*. 2. 353-356.

[44] Christophe, "Initialization Vector (IV) attacks with WEP - SY0-601 CompTIA Security+," Cybr, Mar. 06, 2022. https://cybr.com/certifications-archives/initialization-vector-iv-attacks-with-wep-comptia-security/ (accessed Mar. 30, 2023).

APPENDIX A

1- FMS (FLUHRER, MANTIN, SHAMIR)/KOREK ATTACK IMPLEMENTATION

A. Environment

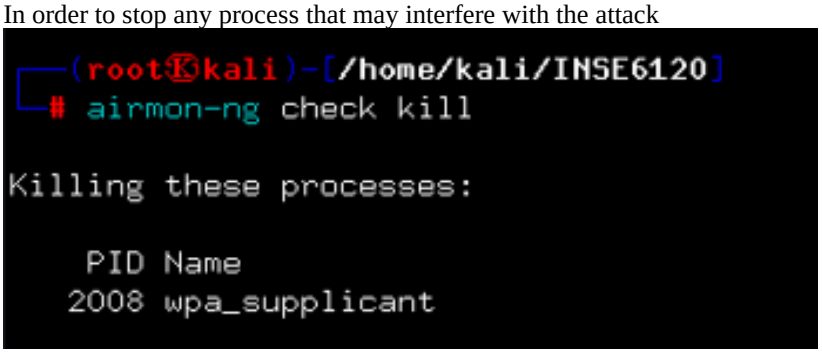
a. kali-linux-2023.1-live-amd64
b. Aircrack-ng tool suite
c. Wireless network adapter capable of monitoring mode
d. WEP capable router

B. Installation Requirements

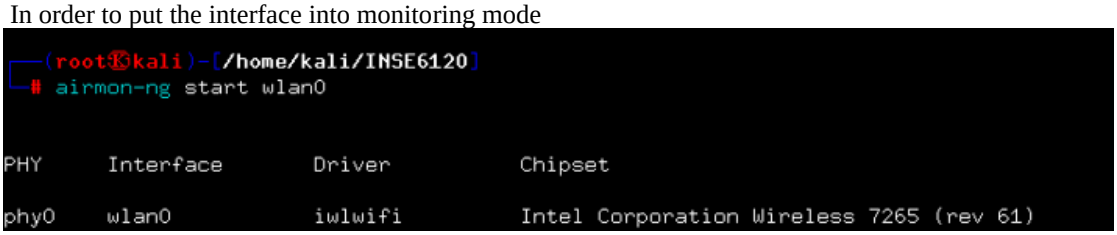
1. Kali linux iso from official website https://www.kali.org/get-kali/#kali-live
2. Aircrack-ng & Airmon-ng are installed with kali iso.

C. Implementation Steps:

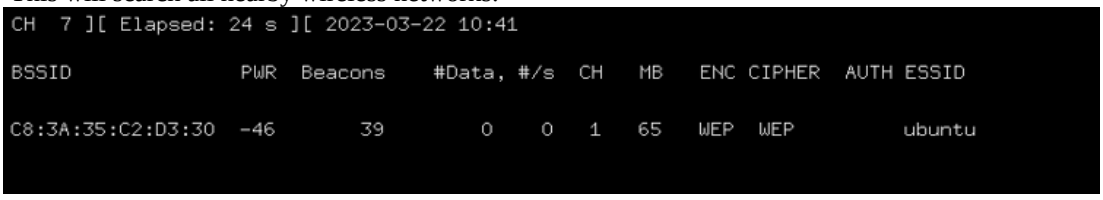
1. Command: airmon-ng check kill
   In order to stop any process that may interfere with the attack



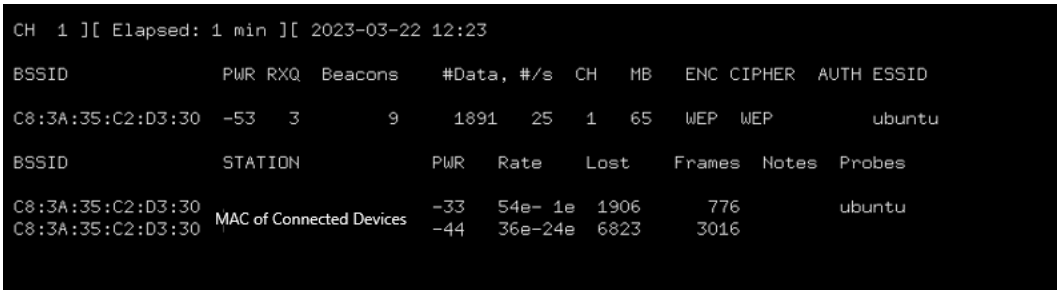
2. Command: airmon-ng start
   In order to put the interface into monitoring mode



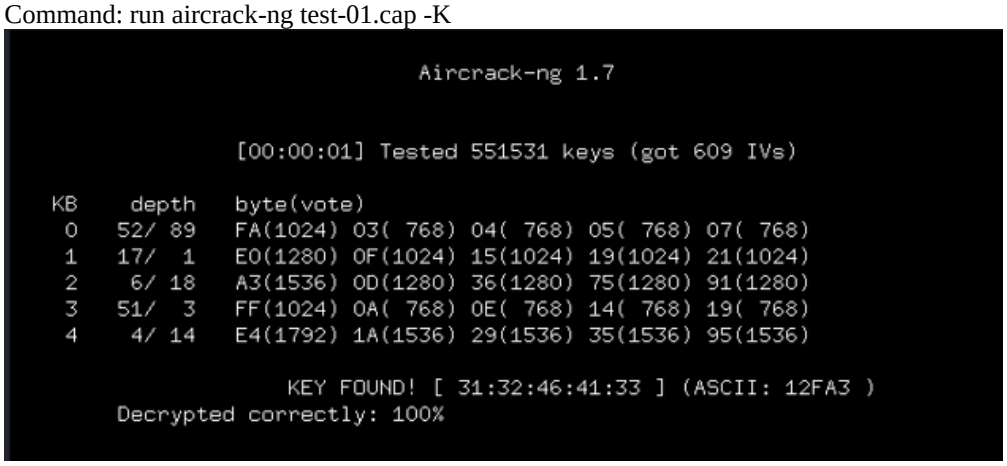
3. Command: airmon-ng start
   This will search all nearby wireless networks.



4. Command: airodump-ng -c <channel> --bssid <target mac> -w <filename> <interface name>
   Command: airodump-ng -c 1 --bssid C8:3A:35:C2:D3:30 -w test wlan0
   this will start collecting data packets between the targeted access point and connected devices then store them in file “test”



5. Keep the previous command running to collect sufficient amount of packets then in a parallel terminal run aircrack-ng with the argument -K in order to force use FMS/Korek attacks.
   Command: run aircrack-ng test-01.cap -K



   As can be seen the key was found and can be used to connect to the network

APPENDIX B

2- PTW (PYCHKINE, TEWS, WEINMANN) ATTACK IMPLEMENTATION

A. Environment

a. kali-linux-2023.1-live-amd64
b. Aircrack-ng tool suite
c. Wireless network adapter capable of monitoring mode
d. WEP capable router

B. Installation Requirements

1. Kali linux iso from official website https://www.kali.org/get-kali/#kali-live
2. Aircrack-ng & Airmon-ng are installed with kali iso.

C. Implementation Steps:

1. Command: airmon-ng check kill
   In order to stop any process that may interfere with the attack

```
┌──(root㉿kali)-[/home/kali/INSE6120]
└─# airmon-ng check kill

Killing these processes:

    PID Name
   2008 wpa_supplicant
```

2. Command: airmon-ng start
   In order to put the interface into monitoring mode

```
┌──(root㉿kali)-[/home/kali/INSE6120]
└─# airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy0    wlan0           iwlwifi         Intel Corporation Wireless 7265 (rev 61)
```

3. Command: airodump-ng wlan0mon
   This will search all nearby wireless networks.

```
CH  7 ][ Elapsed: 24 s ][ 2023-03-22 10:41

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

C8:3A:35:C2:D3:30  -46       39        0    0   1   65   WEP  WEP         ubuntu
```

4. Command: airodump-ng -c <channel> --bssid <target mac> -w <filename> <interface name>
   Command: airodump-ng -c 1 --bssid C8:3A:35:C2:D3:30 -w test wlan0
   this will start collecting data packets between the targeted access point and connected devices then store them in file "test"

```
CH  1 ][ Elapsed: 1 min ][ 2023-03-22 12:23

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

C8:3A:35:C2:D3:30  -53   3        9     1891   25   1   65   WEP  WEP         ubuntu

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

C8:3A:35:C2:D3:30                     -33   54e- 1e  1906      776         ubuntu
C8:3A:35:C2:D3:30  MAC of Connected Devices  -44   36e-24e  6823     3016
```

5. While the previous command is running
   Command: run aircrack-ng test-01.cap (“test-01.cap” were (IVs) Initialization vectors are stored)

```
                                                                      Aircrack-ng 1.7


                                                                [00:17:25] Tested 160481 keys (got 10041 IVs)
                      Got 10239 out of 15000 IVs
   KB    depth   byte(vote)
    0    6/ 10   37(13056) 96(12800) AB(12800) B1(12800) 0D(12544) 5D(12544) 68(12544) 85(12544) 8B(12544) AA(12544) 10(12288) 62(12288)
    1   17/ 19   47(12288) 24(12032) 29(12032) 2D(12032) 31(12032) 53(12032) 56(12032) 74(12032) FF(12032) 1F(11776) 3F(11776) 69(11776)
    2   20/  2   F9(12288) 3B(12032) 48(12032) 60(12032) 6E(12032) 73(12032) 78(12032) BF(12032) DD(12032) FE(12032) 0E(11776) 4C(11776)
    3   19/  3   F3(12544) 17(12288) 52(12288) 53(12288) 7E(12288) 84(12288) AC(12288) 01(12032) 28(12032) 4C(12032) 64(12032) A6(12032)
    4   17/ 18   1A(12544) 08(12288) 8F(12288) 0B(12032) 4C(12032) 50(12032) 53(12032) 65(12032) 72(12032) 76(12032) 91(12032) BB(12032)

Failed. Next try with 15000 IVs.
```

The attack will keep trying the attack after every 5000 IVs captured until the key is found

```
                                                                      Aircrack-ng 1.7


                                                                [00:20:06] Tested 242 keys (got 15073 IVs)
                    Got 15011 out of 15000 IVsStarting PTW attack with 15011 ivs.
   KB    depth   byte(vote)
    0    0/  4   31(20736) D2(19712) 13(19456) 19(19456) 3E(19200) 58(19200) C6(19200) D6(19200) 3B(18944) 72(18944) CA(18944)
    1    0/  1   32(24064) DC(21248) A7(18944) 1F(18432) 4A(18432) B2(18432) DE(18432) 29(18176) 51(18176) E9(18176) F8(18176)
    2    2/  6   23(19712) 44(19200) 76(19200) A9(19200) 33(18944) AF(18944) 07(18688) 09(18432) 0C(18176) 78(18176) 98(18176)
    3    0/  6   41(20224) 90(19712) DD(19456) 08(19200) 28(19200) 4B(19200) 4B(18944) FF(18944) 29(18688) 52(18688) 5E(18688)
    4    0/  2   33(21248) 9B(21248) 03(19456) AA(19456) 95(18944) 53(18688) 6A(18688) AD(18688) F4(18688) 2B(18432) 74(18432)

                KEY FOUND! [ 31:32:46:41:33 ] (ASCII: 12FA3 )
      Decrypted correctly: 100%
```

As can be seen the key is found in hex and in ASCII which can be used to connect to the wireless network.