

# 'WLAN Security Protocols and WPA3 Security Approach Measurement Through Aircrack-ng Technique'

Mr. Elyas Baray

Department of computer science and engineering

Sharda University

Uttarpradesh India

elyasbaray@gmail.com

Dr. Nitish Kumar Ojha

Department of computer science and engineering

Sharda University

Uttarpradesh India

nitish.kumar7@sharda.ac.in

**Abstract** - From the beginning of technology and Wi-Fi based systems wireless networks had a prominent threat upon data security. Without security measures many organizations contribute on these flaws of security to make it better. There are many vulnerabilities of security models which are discussed in this article such as hacking through Wi-Fi security by Aircrack-ng, previous security model vulnerabilities and also the performance of Aircrack-ng attack on Wi-Fi modem or routers. In order to crack WPA/WPA2, kali Linux operating system will be needed along with Aircrack-ng packages installed on any compatible PC. Some of the new standard WPA3 such like downgrade problem on which the system will let the device to downgrade from WPA3 to WPA2 in order to connect with incompatible device. Further, it makes a way for hackers to obtain Wi-Fi passwords even from new model defined such as WPA3 by using old techniques. The new model introduced Wi-Fi security protocol WPA3 is also no longer a secure model it can be penetrated. Researchers have discovered some new vulnerability enables hackers to get out the Wi-Fi passwords.

**Keywords** (Aircrack-ng, Crack, Airodump-ng, Kali Linux)

## 1. Introduction

Wi-Fi or Wireless local area networks (WLAN) IEEE 802.11 gives easy access and speedy data transfer throughout the entire network area. It is mostly popular utilized for the features of its cheapest and easy way to spread the data anytime or anywhere. The users can share files through network and access internet with maximum data transfer rate without the use of any cables, the word cable-less makes WLAN very vulnerable to attacks because the data and transmission of data are done through the air. And through the air, it means the data is vulnerable to any kind of cyber-attack.

Security is one of the most important areas in Wireless Local Area Networks because of its air data transfers, and to have wireless connections secure from the level of personal to the level of complexity, it is important to have the communication secured. The data confidentiality, integrity, and safeness of data should remain unreachable to outside unauthorized users, and to make sure safety of data and network from security breaches and threats the WLAN organization has several security standard protocols invented for WLAN which are Wired Equivalent Privacy, Wireless protected access, Wireless protected access second version (WEP, WPA, WPA2), and another one which is added in 2018 called Wireless protected access version three (WPA3) security protocol.

Aircrack-ng is another technique used for hacking through wired or wireless networks. It can be programmed on kali Linux an open system OS, for penetration over wireless networks this technique is fully featured security penetration and auditing platform. It can also come with free source online editions which make the choice for hackers where Aircrack-ng can easily crack passwords under WEP, WPA, and WPA2 encryptions. But in case of WPA3 has more enhanced encryptions which makes it much more difficult to hack than other security protocols yet it is not fully immune to attacks, university researchers has found some vulnerabilities on WPA3 which is possible to get Wi-Fi passwords yet no one has exploited these vulnerabilities, Wired Equivalent Privacy WEP is an old encryption algorithm designed in 1999 WEP uses RC4 algorithm for encryption and used 64-bit key WEP also uses CRC-32 algorithm for data integrity however there was found many flaws in WEP by crypt analysts. Further it can be replaced WEP with WPA protected access WPA in 2003 further which WPA was replaced by full IEEE 802.11i standard WPA2 in 2004, where WPA2 was so powerful and used Counter Mode

with CBC- MAC Protocol (CCMP) for encryption and (CCMP) uses advanced encryption standard (AES) as an encryption algorithm for passwords, so WPA2 was even used by NASA organization in a time being.

Both security standards WPA and WPA2 are known as hearty or robust, yet both of them are secured with passphrases further which are possible to be broken utilizing "Word reference Attack" or savage power assaults WPA3 additionally utilizes vigorous assurance yet with higher improved encryption which makes it minimal harder to break other than WPA and WPA2.

Except the Aircrack-ng, there are lots of other ways to crack the passwords from Wi-Fi modem or router and the old encryptions security protocols are all penetrated. These are bypassed by different methods and recently used security approaches for WLAN security focuses only on few security components which is not enough comprehensive for security measures. This is the reason that some of organizations used their past experience with security threats to solve their current problems. In view of literary works and explores concentrated there are insufficient examination accessible that can approve the throughput of WLAN IEEE802.11 in the genuine climate and the WLAN shows loads of weakness to each arrange assaults like meeting seizing, Mac addressing issues related, DOS Attacks and bundles of other sniffing which all can be customized in Aircrack-ng by kali Linux working framework, this paper give light on the fact how the Aircrack-ng infiltrates the Wi-Fi switch having security conventions and high security protocols with the encryption key exchange.

## 2. Relevance of Research Area

There are many researchers researching WLAN security flaws on the WPA3 approach and other security protocols to make readers known with the security measures of all the available protocols and provide knowledge on possible security breaches like Dragonblood analyzing the dragonfly handshake of WPA3 and EAP-pwd By Mathey Vanhoef and Eyal Ronen [7], where the used idea of downgrading is considered in this article. Security issues and solutions in Wi-Fi by Menal Dahiya, have pointed out the main issues with Wi-Fi security protocols and gave suggestion at the time [8]. Review on Wireless security protocols (WEP, WPA, WPA2, and WPA3) By Dr. B Indira Reddy, and V.Srikanth, which is similar but have presented some possible flaws in WLAN security protocols with references of old researchers [10]. An Overview of WLAN Security by Rajeev Singh and T.P. Sharma [11] points the main vulnerabilities old security standard has, and much exploration has been done in investigating dangers, weaknesses, assaults, and different strides to overcome them. An investigation of a security

issue on Wifi was performed by Akshika Aneja [12], where Aneja found that each security convention has its negative marks, as of recently there is no security convention which can provide 100% security. The assault on WLAN and defense mechanisms over attacks was presented by K. Lounis and M. Zulkemine [14], the authors suggested that network coordination model gives functional structure to remote security concerns and for challenges in the acknowledgment of open remote engineering. The investigation of Wireless Security Using Wi-Fi Protected Access 2 (WPA2) was performed by Mathy Vanhoef, KU Leuven, Key Reinstallation Attacks Breaking in which they discovered the very easy way to crack it also [13], in KRACK the suit used for testing was also the packages of Aircrack-ng is used to make the so-called hacking tool KRACK. IEEE 802.11 is a remote organization which uses radio to move information and subsequently is generally defenseless to the security issues, for example, WPE/WPA/WPA2 splitting, Denial of Service (DoS), and rouge access points with testing penetration work [15]. Suggestions on Wi-Fi protected access2 (WPA2) protocol vulnerabilities might be mitigated and addressed through the enhancement of new protocols and advanced attacks on wifi security standards WEP, WPA, WPA2 personal and enterprise levels by kali Linux [16], the Aireplay role was the real idea, their work and methodology are quite similar to the Aircrack-ng suit and packages while performing the handshake capture.

## 3. Need of Research and Problem Statement

The research work performed on the area of WPA3 security protocol approach and its security measurement [1] were not satisfied, specifically when hacking by Aircrack-ng which is a suite of packages along with pre-defined coding for penetration of WIFI network security. It can be downloaded and installed in any open-source operating system and this Aircrack-ng is very easily used in kali Linux OS which is another network and penetration testing open-source operating system used only for hack and social engineering purposes Aircrack-ng contains packages like monitoring bssid, airodump for capturing handshakes and Aireplay which sends data parcels to victim address for capturing the bssid and other significant useful data further to this many of university researchers have found some vulnerabilities in WPA3 [7]. They did exploit these vulnerabilities but not with the Aircrack-ng yet so in light of these factors concerning previous research articles, the work on WPA3 is not yet completely done [8]. The more practical research on these founded flaws of WPA3, the safer will be the consumption of WPA3 protocol [9]. WLAN shows heaps of weakness to every organized assault and hacking group like meeting commandeering [11]. Mac mocking and spoofing, DOS Attacks, parcel data sniffing, and handshake capturers of WPA/WPA2/WPA3 [12], further which can be modified

in a single suit Aircrack-ng by kali Linux framework. This task portrays how Aircrack-ng enters the Wi-Fi switch with security conventions, for example, WEP/WPA/WPA2 and to discover potential results of WPA3 with its main standard organization issues and imperfections with its past organization principles [13]. The more risks and vulnerabilities of WPA3 make it a more important area of research because nowadays every new Wi-Fi router or modem and organizations uses WPA3 as their latest option of security protocol [14]. These tools are the programmed packages such as Aircrack-ng suit further which can also be controlled by android mobiles even without PC makes Wi-Fi most protocols hackable. With the assistance of Aircrack-ng pre-defined codes and some other penetration techniques along with proper downgrading, the whole new standard WPA3 so-called safe when getting hacked into, so there should be more reasons to exploit such project and topic for brief knowledge of security protocol WPA3 [15].

#### 4. Methodology

The beginning will be with the evaluation and overview of WIFI security standard protocols such as WEP/WPA/WPA2. The latest technology WPA3 is the data gathering on their speed and features with comparison tables of how much speed the network has under specific security protocol. The main features of WPA3 and its newly founded vulnerabilities will be discussed and downgrade attack will be conducted. The installation of kali Linux on PC will be needed along with needed packages for penetration of WLAN networks. The programming and coding of Aircrack-ng starts hacking into WLAN networks which is unstoppable. Later on, the penetration of the security protocols with brute force and dictionary attacks by Aircrack-ng and for WPA3 downgraded it to security protocol WPA2 and then hacked it by Aircrack-ng. Due to the situation when WPA3 were not downgraded it would be impossible to hack it by passphrases. And the word attacks the security keys which are eventually changed for offline measures. This kind of feature is considered as SAE which has higher encryption than any other security standards ordinary passwords, and after hacking through security protocols. There is a possibility of having table-wise measurement of security for all the protocols in the WPA3.

Programmers who will look for information to steal or bargain usefulness follows the conventional safety efforts which are less proficient then the remote assault surface presents a solitary and troublesome test. A large portion of the remote nets are a lot unprotected so it is defenseless against attack. At the point, when one considers Wi-Fi the greater part of individuals have two significant encryption methods such as Wired Equivalency Protocol (WEP) and Wi-Fi Protected Access (WPA). WPA is higher enhanced than WEP but currently, both of the standards are out of date especially in the WEP security standard protocol.

##### a) Stage Zero:

Log in to Kali Linux OS password is always root for the user.

##### b) Stage One:

This module serves the infusion skilled remote connector (Unless local PC remote card upholds it). In the event that utilizing Kali in VMware, at that point you may need to interface the card through the symbol in the gadget menu.

##### c) Stage Two:

To extricate the process from every remote device organization, open a Terminal, and type (**airmon-ng**) code.

The code will list all the devices connected which helps screen mode monitoring. If no device cards were connected, take the stab and detach and the connector. And then connect it again (in case of utilizing), and monitor whether it upholds screen mode. In this case, an outside connector is recorded and it is required to exchange the card because it doesn't uphold screen monitoring mode, and the card upholds screen mode monitoring and it is recorded as wlan01.

##### d) Stage Three:

Type (**airmon-ng**) followed by the monitoring card name of the remote card. Here, the card name is **wlan01**, so the order should be: **airmon-ng start wlan01**

**Note:** here the name of screen interface is (**mon0**), Alter:

There has recently been discovered an error in the operating system Kali Linux in which airmon makes the monitoring channels at the fixed one channel as "1" where initially empower the mon0 interface. In the event that, by mistake, or just would prefer not to take the risk, follow these means in the wake of empowering mon0:

Type the code (ifconfig) and Enter.

Supplant the name of monitor interface mon0 likely which is wlan01 it debilitates remote card device being associating with web directly and permitting the card to zero in on-screen mode.

When the impair mon0 is done, then empower wlan01 (remote interface), with the code: ifconfig [remote card] and hit enter.

##### e) Stage Four:

In this stage use code (**airodump-ng**) and the name of the screen interface card, where it is presumably mon0.

##### f) Stage Five:

The feature Airodump gives the entirety of the remote organization's list in the general vicinity, with many other helpful data. Find the organization or organizations on which the entrance is recognized on the founded list, and then click Ctrl plus C in the console for terminating the process of the cycle.

#### g) Stage Six:

Duplicate target BSSID of organization.

And presently write the order:

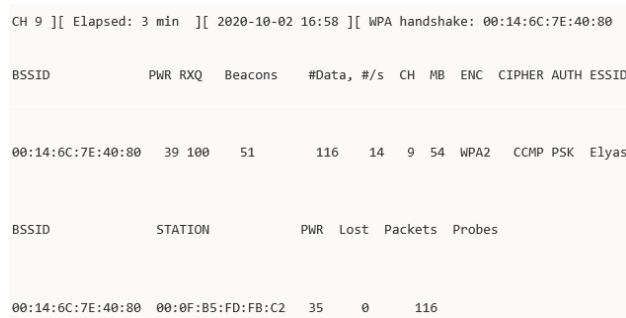
```
(airodump-ng -c - bssid - w/root/Desktop /  
####[monitor card interface]
```

Change the channel with an objective organization channel. Glue organization BSSID which the id is changed and replace the interface monitor with your screen empowered interface name mon0, The "w" document way order determines a spot which airodump gets the caught four-way hand-shakes (used further for decryption of passcode). People can put it on the desktop or anywhere else in this cracking.

The total order will be comparative this:

```
airodump-ng -c 10 - bssid 80:12:EF:E5:B8:F5 -  
w/root/Desktop/mon0 . Presently press enter.
```

After hitting enter get the data such as shown in figure one which shows the confidential data of our victim along with our bssid and channel data which shows how much the Airodump-ng has transferred to get the handshakes captured for decryption.



BSSID	PWR	RXQ	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:14:6C:7E:40:80	39	100	51	116	14	9	54	WPA2	CCMP	PSK	Elys

BSSID	STATION	PWR	Lost	Packets	Probes
00:14:6C:7E:40:80	00:0F:B5:FD:FB:C2	35	0	116	

Figure 1: Details gained by Airodump

#### h) Stage Seven:

Now airodump will permit us to get more data out of targeted bssid are depending on the whole process on the airodump to do the further job and connect with the targeted organization constraining a way to get the four-way hand-shake which need the further process to split the secret phrase.

Additionally, four documents should be visible in the work area so that all the found handshakes will be gathered once captured. However, the work not only is dependent on the package airodump but use another good tool which is suitable for Aircrack-ng. The tool is aireplay-ng, so to make the process work with the cycle. Other than depending only on the tools, reconnect it by

giving de-authentication parcels to the targeted organization bssid and making the targeted bssid is a victim to reconnect with the pre-defined organization bssid.

Obviously, for the code and gadget to work there should be another device also in use in the targeted organization. At this point, depend on airodump-ng and the user will connect where waiting is needed. There are lots of ways to pay and skip the waiting so anything is found then the organization may be vacant.

#### i) Stage Eight:

In this stage let **airodump-ng** on run and open another terminal and type the below code in orderly manner as it is written below:

```
(aireplay-ng -0 2 -a -c mon0)
```

Here above the -0 is another way of de-authentication mode and -2 is the de-authentication parcels needed to send for de-authentication.

The -a code shows the path or switches the bssid of the device to targeted bssid of the objective organization and here in this case is **80:12:EF:E5:B8:F5**.

-c shows the customer's BSSID, the gadget attempting to deauth, to be remembered in previously the customer bssid will be recorded as part of the station. Furthermore, if the interface card name mon0 is not unique then do not change it else change if it is unique.

The total order of the code will be like this:

```
aireplay-ng -0 2 -a 80:12:EF:E5:B8:F5 -c  
2C:ED:82:39:BE:21 mon0
```

#### j) Stage Nine:

After clicking the above code, send the data parcels (**aireplay-ng**). On the off chance it is sufficiently close to the objective customer, and the deauthentication cycle works, this message will show up on the airodump screen (which you left open):

This implies the handshake has been caught, the secret phrase is in the programmer's hands, in some structure or another. At this point, close the (**aireplay-ng**) terminal and hit Ctrl + C on the (**airodump-ng**) terminal to quit checking the organization; however, don't close it yet simply in this case, a portion of the data is required later.

To obtain the "handshake message," at that point, something turned out badly during the time spent sending the parcels. Shockingly, an assortment of things can turn out badly. The gadget endeavoring to deauth probably will not be set to consequently reconnect, in which case

you'll either need to attempt another gadget, or leave airodump on uncertainly until a person or thing interfaces with the organization.

Be always aware of that regardless of many earnest attempts, numerous wireless network standards which essentially not breakable so then possibly the organization router is off else the secret word may be more like 64 characters in length, and so on.

#### k) Stage Ten:

In this stage almost all the codes are running the only path to made wordlist and WPA handshake capturing are promoted here in this section initially assign a wordlist to the system for cracking the password and matching it with the wordlist, and then Open new Terminal by not closing the previous one and now type the code in below order:

```
aircrack-ng - a2 - b - w / root /Desktop /*.cap
```

The code - a2 used by aircrack is a mechanism for capturing handshakes between the devices, 2 is the standard version of WPA strategy.

The code -b shows the bssid of the main device router along with the targeted devices bssid, here the bssid is **80:12:EF:E5:B8:F5**.

The code -w represents the passwords document and along a path of that document which have made here document name is "1.1million word list" and it is the main location root folder.

This code **root-Desktop-\*.cap** has the location of the wordlist which contains the passwords and the star\* has a special effect in Linux when used it searches only for the mentioned document in the selected area further all the codes if written as mentioned in the search will work and the system will get hands-on the passwords for encryptions.

The overall code should be like:

```
aircrack-ng - a2 - b 80:12:EF:E5:B8:F5 - w/root /1.1millionwordlist.txt / root /Desktop/ *.cap
```

Now after writing above code click enter.

#### l) Stage Eleven:

Now after stage ten the Aircrack-ng will find the way to the password of WIFI using the provided the wordlist and if it didn't found the code in wordlist then change the wordlist to another one, Once in a while, it's most certainly not. At this point, an attempt is made for different wordlists. Basically, it is possible to discover the secret key regardless of the number of wordlists.

Splitting and finding the passcode will take a huge time to find if the wordlist is big and the password of the router is of more digits password was found in less amount of time.

If the password was in the wordlist then the (**aircrack-ng**) bring it up.

The code to the device was "Elyas12345678," where if this code is checked to know whether it was in the wordlist, and find that Aircrack-ng is used to discover the secret word without a battle. At that point, change the secret word in the organization. It is required to instruct to have the changes in their secret phrase at the earliest opportunity.

After all the stages are executed successfully it is possible to obtain the key as shown in figure 2.

```
Aircrack-ng 1.6

[00:01:29] 25420 keys tested (370.20 k/s)

KEY FOUND! [ Elyas12345678 ]

Master Key : CD 69 0D 11 8E AC AA C5 C5 EC BB 59 85 7D 49 3E
            B8 A6 13 C5 4A 72 82 38 ED C3 7E 2C 59 5E AB FD

Transient Key : 06 F8 BB F3 B1 55 AE EE 1F 66 AE 51 1F F8 12 98
               CE 8A 9D A0 FC ED A6 DE 70 84 BA 90 83 7E CD 40
               FF 1D 41 E1 65 17 93 0E 64 32 BF 25 50 D5 4A 5E
               2B 20 90 8C EA 32 15 A6 26 62 93 27 66 66 E0 71

EAPOL HMAC : 4E 27 D9 5B 00 91 53 57 88 9C 66 C8 B1 29 D1 CB
```

Figure 2: Encrypted key found by wordlist

### 5. WPA3 Security Protocol and Cracking

WPA3 (Wi-Fi Protected Access Edition 3) is the most recent security convention with top guidelines. WPA3 ensures against word reference assaults and uses Simultaneous Authentication of Equals handshake (SAE) and this approach makes many attacks impossible, which shields its organization from assaults that could be conceivable with the WPA2 setup. WPA3 is great on open organizations (state in an espresso place), since it naturally scrambles the association with no requirement for extra certifications the recent researchers have found many possible vulnerabilities with WPA3 security standard those vulnerabilities are only exploited by mathy and Eyal theoretically and experimental some of these vulnerabilities are done by them here in this section after downgrading part of WPA3 standard the use of Aircrack-ng with all the previous codes presented in methodology the cracking are applicable on WPA3.



### 5.1. Downgrade and Aircrack-ng Attack

The attack on WPA3 security an AP acknowledges associations utilizing WPA3 with SAE encryption and another WPA2 with a similar secret word. This furnishes similarity with more seasoned customers, while second version 4 way handshake recognizes downsize assaults an enemy adjusts reference points to fool the customer into intuition the AP just backings WPA2, the customer will distinguish this downsize assault during the second version standard 4-way handshake. So this grounds that the four-way handshake contains a confirmed RSNE component posting the AP's upheld figure suites, permitting a customer to distinguish if an enemy produced the RSNEs in signals. This implies WPA3 gives forward mystery, in any event, when utilizing the change method of WPA3-SAE.

Figure 3 is the same as figure number 1, data needed for getting encrypted keys all the codes used are also the same procedure just as WPA2 used codes but after downgrade only.

CH 6 ][ Elapsed: 34 min ][ 2020-10-02 19:28 ][ WPA handshake: 7C:A1:AE:1E:3C:5A											
BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
00:14:6C:7E:40:80	44	230	119	218	28	6	96	WPA3	GCMP	SAE	Elyas
BSSID	STATION			PWR	Lost	Packets	Probes				
7C:A1:AE:1E:3C:5A	00:0F:B5:FD:FB:C2			38	0	218					

Figure 3: Encrypted keys codes

Figure 4 depicts the Dictionary assault on the WPA3 encryption-SAE when it is experiencing significant change mode

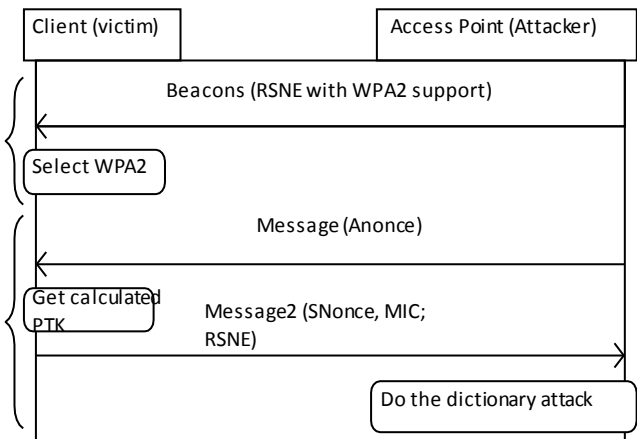


Figure 4: Dictionary assault on the WPA3

This minimizes the customer into legitimately utilizing the WPA2 version four-way handshake.

The issue that, even though downsize assaults are recognized in WPA2's four-path hand-shake is the way an enemy has top turned enough information to play out a word reference assault. This is because a foe just needs to catch a solitary validated four-way handshake message to complete a word assault. More than MITM position isn't expected to complete the assault. The main necessities are to know the SSID of the organization which is near a customer.

If these conditions are met, the foe can communicate a WPA2-just organization with the given SSID (stage 1 Fig. 2). This makes the customer associate to the maverick AP utilizing WPA2. The enemy can manufacture the principal message of the four-route handshake since this message isn't verified (stage 3 Fig. 2). Accordingly, the casualty will communicate message 2 of the four-way handshake, which is confirmed. In light of this confirmed handshake message, a word reference assault can be done.

So after the above steps continue with Aircrack-ng and old techniques to crack the password of WPA3. After downgrade the WPA3 is much vulnerable like WPA2 and its cracking password techniques happens due to the SAE approach in cracking its strong algorithm (SAE).

For experiment purposes password used is a simple 13 digit code in WPA3.

Figure 5 describes the WPA3 password cracked by dictionary attack after the encryption keys and handshakes were taken when downgraded from WPA2 to WPA3.

Aircrack-ng 1.6	
[00:32:09] 25420 keys tested (13.20 k/s)	
KEY FOUND! [ Elyas12345678 ]	
Master Key	: GC 59 2D 51 4E GC HA 65 J5 3C VB A9 55 6D 99 4E E8 A5 63 C7 8A 62 92 38 ED C5 2E 5C 69 3E EB AD
Transient Key	: 06 F8 BB F3 B1 55 AE EE 1F 66 AE 51 1F F8 12 98 CE 8A 9D A0 FC ED A6 DE 70 84 BA 90 83 7E CD 40 FF 1D 41 E1 65 17 93 0E 64 32 BF 25 50 D5 4A 5E 2B 20 90 8C EA 32 15 A6 26 62 93 27 66 66 E0 71
EAPOL HMAC	: 5A 57 79 8B 11 61 83 27 78 6C 76 C9 B2 25 D3 CA

Figure 5 : WPA3 password cracked by dictionary attack

Above is a figure of successfully found the key, the time taken the difference between WPA2 hack and key decryption and WPA3 key decryption is not the same as

seen in figures 3 and 5 although the codes used were the same with downgrading WPA3 it made it as easy just like WPA2 security standard, which made it different is the simultaneous authentication of equals algorithm named (SAE) it changes the encryption keys simultaneously to bypass the offline dictionary attacks and this was also the reason for time difference of both standards.

## 6. Findings and Results

**Table 1. Vulnerabilities of Wi-Fi Security Protocols**

Vulnerabilities	WEP	WPA	WPA2	WPA3
DoS attacks	Can be easily Attacked	Can be easily Attacked	Can be targeted	Immune to DoS attacks unless downgraded
Packet sniffers	Not Immune	Not Immune	Not Immune	Not Immune But has SAE
Mac spoofing	Mac can be spoofed	Mac can be spoofed	Mac can be spoofed	Mac can be spoofed
Dictionary Attacks	Can be done	Can be done	Can be done	Impossible unless downgraded
Brute Force Attack	Yes	Yes	Yes but takes some time	Yes but takes decades
Network Monitoring Immunity	Not Immune	Not Immune	Not Immune	Not Immune
Authentication By External Forces	Possible	Possible	Possible	Not Possible
Duplicate Access Point	Yes	Yes	Yes	No
KRACK Attack	Very much Possible	Very much Possible	Very much Possible	Impossible
Replay Attack	None	IV Sequence	IV Sequence	Very Strong IV Sequence

**Table 2. Results - after implementation**

Security Protocol	Handshake Capturing Time	Password Cracking Time	Data	Beacon	IV Size	Cipher	Authentication
WEP	40 Seconds	33 Seconds	24	11	24 bits	RCA4	WEP KEY
WPA	93 Seconds	64 Seconds	48	33	48 bits	TKIP	PSK
WPA2	270 Seconds	89 Seconds	116	51	48 bits	CCMP	PSK
WPA3	2040 Seconds	1929 Seconds	218	119	64 bits	GCMP	SAE

## 7. Suggestion: Downgrade attacks Protection just like in WPA2

An AP publicizes its upheld figure suites, i.e., confirmation and encryption calculations, in a Robust Security Network element (RSNE). The RSNE is incorporated unauthenticated in occasionally sent guides that publicize the presence of the organization. Customers likewise remember the RSNE for affiliation solicitations

to advise the AP regarding the code suite they are likely to utilize. Model verification calculations are the four-way, 802.1X, or SAE handshake. Be that as it may, a foe can parody the unauthenticated RSNE by manufacturing signals. To distinguish this, the RSNE of the AP and customer is cryptographically checked on WPA2's four-way hand-shake. Since the four-way hand-shake is constantly executed eventually when a station (for example a customer or AP) interfaces unexpectedly to an organization, the RSNE is constantly checked. On the off chance that a crisscross is identified, the handshake is prematurely ended. This keeps an assailant from mocking the RSNE.

## 8. Discussion

Results were found to be as expected but there are some limitation of using Aircrack-ng on WPA3 security standard because the Aircrack-ng suit with code packages was only used to hack through old security protocols such as WPA and WPA2 and security penetration testing as they are its features but using it on WPA3 were hard and only achievable with Samsung Galaxy S10 mobiles because they have a flaw which makes the downgrade process do not use this device as connection beacon. The Aircrack-ng suit will be useless on WPA3, as the challenges were not so much with the hacking of WPA2 but WPA3 hacking was very tricky because making the SAE encryption algorithm as victim which is not an easy task for the usage of Samsung device.

In the future, this research can be further extended during the attack on WPA3 downgrade vulnerability without Samsung galaxy s10 mobile which would lead to inventing an algorithm similar to mathy and vanhoef to help with the downgrade process and when the system with high-security protocol proceeds down to an older version of wireless protected access there would be a collection of other techniques to use for key decryption of captured handshakes.

## 9. Conclusion

In the proposed work, it can be concluded that there are no issues like WPA/WPA2 is better than WPA3. Here, the investigating of all speed comparisons of cracking and encryption algorithms performed by hacking through Aircrack-ng and WPA3 security protocol founded to be the strongest among all security protocols. There is not enough research done on WPA3 and with time there will be more chances of hackers knowing the weaknesses in WPA3 than random people utilizing this technique. And also there will be high chances of getting hacked until a new security protocol is invented with privileged to suggested vulnerabilities and stated disadvantages in this article have concluded that WPA3 is more complicated

than other security protocols. But still, with downgrade limitations, it is vulnerable to any threat applied on WPA2 and old security protocols.

## References

- [1]. Talal Mohammed Alghamdi, —Throughput Analysis of IEEE WLAN “802.11 ac” Under WEP, WPA, and WPA2 Security Protocols, Egypt (IJCN), Volume (9): Issue (1): (2019)
- [2]. Mardiana Mohamad Noor & Wan Haslina Hassan, Wireless Networks: Developments, Threats and Countermeasures, Saudi Arabia, International Journal of Digital Information and Wireless Communications (IJDIWC) 3(1): pp 125-140, (2018).
- [3]. Suroto, WLAN Security: Threats and Countermeasures, China, ISSN: 2549-9610, (2018).
- [4]. Tarek Mohamed Refaat, Tarik Kamal Abdelhamid & Abdel-Fattah Mahmoud Mohamed – Wireless Local Area Network Security Enhancement through Penetration Testing, Syria, International Journal of Computer Networks and Communications Security.(2016).
- [5]. Mahbod Tavallaee, an Overview of WLAN Authentication Protocols, Canada (2021).
- [6]. Nishant pimple, Utkarsha pawal, Tejashree Salunke, Janhavi Sangoi, “Wireless security-An Approach Towards Secured Wi-Fi Connectivity, India (2018).
- [7]. M. Vanhoef and Eyal Ronen Dragonblood: analyzing the dragonfly handshake of WPA3 and EAP-pwd, US (May, 2020).
- [8]. Menal Dahiya —Security Issues and Solutions in Wi-Fi, India, International Journal of Electronics Engineering Research. ISSN 0975-6450 Volume 9, pp. 773-777 © Research India Publications, (Number, 2017).
- [9]. Karim Lounis, Mohammad Zulkernine, WPA3 Connection Deprivation Attacks, Tunisia, 14th International Conference (pp.164-176), (February, 2020).
- [10]. Dr. B Indira Reddy, and V. Srikanth review on Wireless security protocols (WEP, WPA, WPA2, and WPA3), India (2019).
- [11]. Rajeev Singh and T.P. Sharma an Overview of WLAN Security, India (November, 2019).
- [12]. Aneja, G. Sodhi, “A Study of Security Issues Related With Wireless Fidelity (Wi-Fi), India (2017).
- [13]. Mathy Vanhoef, KU Leuven, Key Reinstallation Attacks Breaking WPA2 forcing nonce reuse Discovered, (2018).
- [14]. K. Lounis and M. Zulkernine. “Attacks and Defenses in Wireless Technologies for IoT, Tunisia In IEEE Access, vol. 8, pp. 88892-88932, IEEE, (2020).
- [15]. Wang, S., Wang, J., Feng, C., & Pan, Z. “Wireless Network Penetration Testing and Security Auditing, China (November, 2019).
- [16]. Teddy Surya Gunawan, Muhammad Kasim Lim, Mira Kartiwi, Noreha Abdul Malik “Penetration testing using Kali linux: SQL injection, XSS, wordpres, and WPA2 attacks, Indonesian Journal of Electrical Engineering and Computer Science 12(2):729-737, (November, 2018).