Identification of Patterns in the Use of Wired Equivalent Privacy (Wep) as a Security Protocol in Wi-Fi Networks.

Francisco Valle (✉ francisco.valle@urosario.edu.co)

Universitaria Agustiniana <https://orcid.org/0000-0002-7215-4071>

Mauricio Alonso

Universitaria Agustiniana

Research Article

Keywords: WEP, WIFI, protocol, cybersecurity.

Posted Date: February 21st, 2022

DOI: <https://doi.org/10.21203/rs.3.rs-1284620/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Abstract

The constant access to the internet is today part of our life, both in work and family environments we are forced to be connected. In 2020, the arrival and rapid spread of covid-19 have shown us this situation more firmly. Unfortunately, society continues to postpone raising awareness on cybersecurity issues at all levels. This is how today we see the use of obsolete security protocols in different environments. In this document, we focus on identifying the use of the WEP protocol in a sector of the city of Bogotá, as well as the common elements of its users, and demonstrating how with free software it is possible to break the security provided by this network protocol.

Introduction

The popularity of wireless networks (Wi-Fi) as a means of accessing the Internet can be evidenced in the data shown in recent studies, for example in the city of Bogotá (Colombia) in an estimated time of 11 minutes, 69 public wireless networks reported 6407 devices connected to them (Valle 2018). Similarly, in Malaysia, it was observed that smartphone users on average spend about 4 hours a day accessing the internet through Wi-Fi networks (Wahab et al. 2019).

However, when identifying patterns in the use of networks, it becomes clear that cybersecurity awareness is an issue that we must continue to address worldwide. In the city of Rabat, the capital of Morocco, it was identified, among other aspects, that 10% of Wi-Fi networks used WEP (Wired Equivalent Privacy) as a network security protocol (Sebbar et al. 2016). A Similar percentage to the identified in Hong Kong, where it was observed that about 7% of the analyzed networks used the same security protocol (Fong and Wong 2016).

In contrast, it is observed that nowadays there are various publications and studies that talk about the vulnerabilities associated with the WEP protocol used in the security of some Wi-Fi networks (Rana, Abdulla, and Arun 2020) (Waliullah, Moniruzzaman, and Rahman 2015) (Sepehrdad et al. 2014) (Trimintzios and Georgiou 2010) (Vinjosh Reddy et al. 2010), as well as various techniques used for the exploitation and defense of these networks (Valle, Herrera, and Pedraza 2019) (Bartoli, Medvet, and Onesti 2018) (Xiong and Jamieson 2013) (He et al. 2017). Viruses that affect Wi-Fi access points have even been investigated (Milliken, Selis, and Marshall 2013), or that use them as a means of spreading malware on different terminals (Nekovee 2007) (Hu et al. 2009) (Sanatinia, Narain, and Noubir 2013). Studies focused on obtaining confidential information reported by applications connected to Wi-Fi networks (Atkinson et al. 2018), as well as writings associated with the safe use of the internet (Gcaza and von Solms 2017) (Malone 2019) (Eleven Paths 2019) are also highlighted, which together can be considered as efforts by the academic community to generate awareness on cybersecurity issues.

Method

To identify patterns in the use of WEP as a security protocol in Wi-Fi networks, a wardriving exercise was carried out to capture the data that passes through different wireless networks in the city of Bogotá. For which, tools (hardware and software) compatible with the communication protocols associated with the IEEE 802.11 standard were used.

1. Inventory of items

The elements used to perform the data capture and the breaking of the access password of the WEP protocol in a test network, are the following:

1. Network adapter AWUS051NH - Manufacturer ALFA NETWORK.
2. Nebula 300 Router - Manufacturer NEXXT SOLUTIONS
3. X456U Laptop - Manufacturer ASUS.
4. Smartphone Huawei Mate 9.
5. Kismet - Sniffer software for wireless networks.
6. Aircrack-NG Suite
7. Share GPS App

2. Data capture

The first part of the data capture exercise consists of the proper configuration and integration of the different elements. The steps required to synchronize the GPS of the smartphone with the Kismet server are described below so that an estimated location of the different wireless access networks can be obtained. This connection is made wirelessly via Bluetooth

1. In the smartphone it is started the application Share GPS and it is set up a new connection with the following characteristics. (see figure 1):

- a. Data Type: NMEA
- b. Connection Method: Use Bluetooth to send NMEA GPS to the other device
- c. Name: Khuawei (custom name)
- d. Mac Address: 38-D5-47-4B-54-B3 (Mac of the computer where the Kismet server is running)

2. Once the connection is set up, it is activated by selecting the Listening status on the smartphone (see figure 2)

3. On the laptop where the Kismet server is implemented, the Bluetooth service must be started through the console with the service Bluetooth start instruction.

4. Again, a hcitool scan is written to the console to identify the MAC address of the smartphone with which the link is to be established (see figure 3)

5. Now proceed to write in the console `sdptool browse 94: 0E: 6B: 09: 7A: 85` the MAC address of the desired smartphone is used to identify the channel used by the ShareGPS service, as shown in figure 4 is channel 2.
6. Once the channel used by the Share GPS application has been identified, the connection is established with the instruction `rfcomm connect / dev / rfcomm1 94: 0E: 6B: 09: 7A: 85 2` (see figure 5)
7. On the smartphone, the connection must go to the Connected status (see figure 6).
8. As a last step, the Kismet server is started (see figure 7), configuring the GPS source in the `kismet.conf` file.

Following these steps, we proceed to carry out a wardriving exercise, driving in a certain area and thus obtaining information from Wi-Fi networks that use WEP as a security protocol.

3. Obtaining a network password

The WEP security protocol should not be used as a security mechanism in any Wi-Fi network, whether for domestic or corporate use, this is because breaking the password that grants access to it can be done in a matter of minutes, leaving all users inside the network compromised. Here are the steps required to break the password for any network that uses WEP using free software. In the Wi-Fi network called `Test_WEP`, the attack is implemented to illustrate the process.

Step 1: Once the network card (AWUS051NH) is connected to the computer, the `airmon-ng` suite is used to configure the wireless interface in monitor mode with the `airmon-ng start wlan0` instruction (see figure 8)

Step 2: In the Nebula 300 router, the parameters for the Wi-Fi network that uses WEP as a security protocol are established, it is configured on channel 6, with the name `Test_WEP` and the password as the access password `WEP Password` (see figure 9)

Step 3: `Airodump-ng` is used to identify the Wi-Fi network on which the attack will be carried out, with the instruction `airodump-ng -c 6 wlan0mon`. (see figure 10)

Step 4: Next, we proceed to capture the data traffic that circulates through the network, to obtain enough initialization vectors that help to identify the network password with a brute force attack. Typing in the console: `airodump-ng -c 6 -bssid C0: 25: 67: 30: 70: 90 -w testwep wlan0mon`. (see figure 11)

Step 5: Without interrupting the instruction given in step 4, and in a new tab the breaking process begins with the instruction `aircrack-ng puebawep-01.cap`.

Comparing images 9 and 12 shows that, with a brute force attack, the password of the Wi-Fi network that uses WEP as the security protocol is identified.

Results And Analysis

In the wardriving exercise carried out in the city of Bogotá in the town of Suba, 59 wireless networks were identified that use the WEP security protocol to control access to them. By reviewing the information reported by these networks through Beacon-type frames, we can identify aspects that they have in common. The most prominent of them is the lack of training in cybersecurity issues of their administrators since the 59 networks are vulnerable to brute force attacks, like the one developed in this document for the WEP_test network described in the previous section. In figure 13 you can see the map with the location of the identified networks.

The information identified also shows us patterns regarding the manufacturers most used by telecommunications operators that implement Wi-Fi networks with the WEP security protocol. As well as data of the owners of said networks, revealed by the names they assign to the SSID and the use of the channels used for wireless transmission.

1. Equipment identified according to its Manufacturer

According to the data presented by the MAC addresses of the access points (AP), it is possible to identify 13 different manufacturers, while for one of the devices it can be deduced that it corresponds to a false AP since its MAC address does not coincide with that of the manufacturers known. (see table No 1)

Table 1. Identified manufacturers

Manufacture	devices
Technico	22
HonHaiPr	13
Pegatron	7
AsustekC	4
AskeyCom	2
Sagemcom	2
ArrisGro	2
Tp-LinkT	1
GemtekTe	1
D-Link	1
Ubiquiti	1
Unknown	1
Cisco-Li	1
HuaweiTe	1
Total general	59

It can also be established that three manufacturers predominate in the sample, concentrating 71% of the networks among them. In first place is Technicolor company with 37%, followed by Hon Hai Precision in second place with 22% and in third place, we have Pegatron company with 12%. (see figure 14)

2. Channels used in WEP networks

The setup channel for the operation of the Wi-Fi network, although it does not affect the level of security that it may present, can help to establish a certain level of global maturity when it comes to improving the connectivity of each network. It would be expected to find a certain proportion between channels one (1), six (6), and eleven (11) since they do not overlap in the spectrum and for this reason, their equitable use would be the most favorable for all users of these networks. However, the mapping identified a staggering proportion of the use of these channels. The most used channel is one (1) with 37% of the samples, while channel six (6) occupies second place with 22% and channel eleven (11) is observed in third place with 17%. (see figure 15). Although the use observed of the three channels is not ideal, the fact that these three are precisely the most used and in close proportions allows us to see a certain global disposition aimed at ensuring optimal performance of the networks, making the most of the spectrum in use.

3. Names used for WEP networks

When reviewing the names used to designate the networks, interesting patterns established in them are observed. It can be seen that 76% of the networks have a name of an eight (8) digit number. It is also observed that 24% of the networks have a personalized name, which can easily identify the family that owns said network or the commercial establishment that uses it. The network called ETB Zona Wi-Fi is of particular concern since as it is associated with a recognized company in the telecommunications sector, it reflects the low awareness of cyber security issues that the personnel who work in the said company in the ICT sector have or a lack of clear policies within the entity that allows the configuration of Wi-Fi zones with the use of obsolete security protocols. (see table 2)

Table 2. Identified networks

No	Network names
1	17056664
2	19084920
3	19802453
4	21367057
5	27118975
6	33836578
7	44780773
8	46843058
9	47682075
10	50669951
11	52308749
12	58018185
13	59278606
14	62329610
15	63087126
16	65254328
17	66029380
18	68064328
19	69622652
20	70521737
21	70662127
22	72358666
23	73989089
24	76920362
25	77513349
26	81612038
27	81769556
28	82630310

29	83558064
30	84334739
31	85037984
32	86541596
33	87066833
34	88987029
35	91307777
36	92957497
37	93509552
38	94278488
39	94478252
40	95249470
41	96620570
42	96713516
43	98492168
44	98657968
45	924a
46	BEATRIZZUNIGA
47	BRAZON DORADO
48	colegiomaximino
49	DANI
50	ETB Zona Wi-Fi
51	Familia M
52	familia soto
53	FAMILIA TELLO BERNAL
54	FliaRuiz
55	Formula 1.2
56	La Estiba 2
57	MIRADOR DE LA C

Conclusions

The success of the technology identified with the acronym Wi-Fi as a means of Internet access is undeniable nowadays, however, by in 2019 it was possible to identify networks that use the WEP security protocol to manage access to the same and on which it has been shown that it presents vulnerabilities that can be exploited to gain access to the network. It is observed that, in the city of Bogotá, it is necessary to improve the cyber security culture around the use of Wi-Fi networks.

About the manufacturers of network cards that are compatible with Wi-Fi technology, it is interesting to note that companies recognized in the IT sector as market leaders are not the most widely used in the city of Bogotá. We see, as well as low-cost oriental companies, predominate in the market, which leads us to identify that, for telecommunications operators in the city of Bogotá, low cost prevails when buying equipment over quality or a good name that may have certain marks.

Although it is observed that in the field of cybersecurity awareness, work should continue in the city, it is possible to identify that, concerning the efficient use of the radioelectric spectrum in the provision of the 2.4 GHz frequency, there is a significant culture level. It was possible to establish that the most used channels are one (1), six (6), and eleven (11), which, as they do not overlap, present less interference and although their use is not in the ideal parameters (a similar percentage for each one) if they are observed similar values regarding the deployment of these.

References

1. Valle, F. (2018). *Estudio de usos y riesgos asociados a las redes abiertas bajo el protocolo IEEE 802.11 en la ciudad de Bogotá, Desarrollo e Innovación en Ingeniería tercera edición* (pp. 73–80). IAI
2. Wahab, N., et al. (2019). Wi-Fi Temporal Coverage: Analysis of Socio-Economics Influences in Malaysia. *IOP Conference Series: Earth and Environmental Science*, Vol 228
3. Sebbar, A., et al. (2018). An empirical study of WIFI security and performance in Morocco-wardriving in Rabat. *Proceedings of International Conference on Electrical and Information Technologies ICEIT 2016*, 362–367
4. Fong, K., & Wong, S. (2016). Wi-Fi adoption and security in Hong Kong. *Asian Social Science*, 12(6), 1–22
5. Rana, M., Abdulla, M., & Arun, K. (2020). Common security protocols for wireless networks: A comparative analysis. *International Journal of Psychosocial Rehabilitation*, 24(5), 3887–3896
6. Waliullah, M., Moniruzzaman, A., & Rahman, M. (2015). An Experimental Study Analysis of Security Attacks at IEEE 802.11 Wireless Local Area Network. *International Journal of Future Generation Communication and Networking*, 8(1), 9–18

7. Sepehrdad, P., et al. (2014). Smashing WEP in a passive attack. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) vol 8424 LNCS, 155–178
8. Trimintzios, P., & Georgiou, G. (2010). Wi-Fi and WiMAX secure deployments. Journal of Computer Systems, Networks, and Communications, vol 2010, no. June
9. Vinjosh, S., et al. (2010). Wireless hacking-a Wi-Fi hack by cracking WEP. 2010 2nd International Conference on Education Technology and Computer, ICETC 2010
10. Valle, F., Herrera, C., & Pedraza, C. (2019). *Hacking en servicios Web a través de redes Wi-Fi abiertas, Desarrollo E Innovación En Ingeniería cuarta edición* (pp. 178–194). IAI
11. Bartoli, A., Medvet, E., & Onesti, F. (2018). Evil twins and WPA2 Enterprise: A coming security disaster?. Computer and Security, vol 74, 1–11
12. Xiong, J., & Jamieson, K. (2013). SecureArray: improving wifi security with fine-grained physical-layer information. Proceedings of the 19th annual international conference on Mobile computing & networking MobiCom, 441
13. He, L., et al. (2017). Talking about WIFI's new security. MATEC Web of Conference, vol 139, 2–5
14. Milliken, J., Selis, V., & Marshall, A. (2013). Detection and analysis of the Chameleon Wi-Fi access point virus. EURASIP Journal on Information Security, vol 2013, no. 1, 2
15. Nekovee, M. (2007). Worm epidemics in wireless ad hoc networks. New Journal of Physics, vol 9
16. Hu, H., et al. (2009). Wi-Fi networks and malware epidemiology. *Proceedings of the National Academy of Sciences of the United States of America*, 106(5), 1318–1323
17. Sanatinia, A., Narain, S., Noubir, G. Wireless spreading of Wi-Fi APs infections using WPS flaws: An epidemiological and experimental study. 2013 IEEE Conference on Communications and Network, & Security, C. N. S. (2013). 2013, no January, 430–437
18. Atkinson, J., et al. (2018). Your Wi-Fi is leaking: What do your mobile apps gossip about you? *Future Generation Computer Systems*, 80, 546–557
19. Gcaza, N., & Von, R. (2017). A strategy for a cybersecurity culture: A South African perspective. *Electronic Journal of Information Systems in Developing Countries*, 80(1), 1–17
20. Malone, Z. (2019). *Three Common Security Mistakes and Best Practices to Eliminate Them in the New Year* (pp. 42–45). Cyber Defense Magazine
21. Eleven Paths (2019). Informe de tendencias en ciberseguridad. Recuperado: <https://www.elevenpaths.com/es/informe-de-tendencias-en-ciberseguridad-2019/index.html>

Figures

Figure 1

Share GPS Settings

Figure 2

Link in listening mode

```
root@Khuawei: ~  
Archivo  Editor  Ver  Buscar  Terminal  Ayuda  
root@Khuawei:~# service bluetooth start  
root@Khuawei:~# hcitool scan  
Scanning ...  
          94:0E:6B:09:7A:85      HUAWEI Mate 9  
          8C:79:F5:D8:62:D3      n/a  
root@Khuawei:~#
```

Figure 3

MAC address identification

```
Service Name: ShareGPS  
Service RecHandle: 0x10011  
Service Class ID List:  
  "Serial Port" (0x1101)  
Protocol Descriptor List:  
  "L2CAP" (0x0100)  
  "RFCOMM" (0x0003)  
    Channel: 2  
Profile Descriptor List:  
  "Serial Port" (0x1101)  
    Version: 0x0102  
root@Khuawei:~#
```

Figure 4

MAC address identification

```
root@Khuawei:~# rfcomm connect /dev/rfcomm1 94:0E:6B:09:7A:85 2  
Connected /dev/rfcomm1 to 94:0E:6B:09:7A:85 on channel 2  
Press CTRL-C for hangup
```

Figure 5

Connection via Bluetooth between the pc and the smartphone

Figure 6

Successful Share GPS connection

Figure 7

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# airmon-ng start wlan0
Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

PID Name
474 NetworkManager
541 dhclient
1034 wpa_supplicant

PHY      Interface      Driver      Chipset
phy0     wlan0            rt2800usb   Ralink Technology, Corp. RT2770

(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)

root@kali:~#

```

Figure 8

wlan0 interface in monitor mode

NEXXT SOLUTIONS

Home Advanced Wireless QoS Applications Security Tools

Wireless Basic Settings
Wireless Security
Access Control
Wireless Connection Status
Wireless Extender

Wireless Security Setup

Select SSID: Prueba_WEP

Security Mode: Shared

Encryption type: WEP

Default key: Key 1

WEP Key 1: ContraseñaWEP ASCII

WEP Key 2: Enter the WEP key ASCII

WEP Key 3: Enter the WEP key ASCII

WEP Key 4: Enter the WEP key ASCII

Default ASCII password : null

Help

Here you can set the wireless password for your wireless network. You are recommended to select WPA-PSK as Security Mode and AES as WPA Algorithms Type.

WEP Key: Must be either 5 or 13 ASCII characters or 10 or 26 Hex characters.

WPA/WPA2-Personal: You can enable personal (PSK) or mixed mode, but you must make sure that the wireless

Figure 9

Test_WEP network configuration

root@kali: ~

File Edit View Search Terminal Help

CH 6][Elapsed: 0 s][2020-06-25 23:31

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
	-69	0	4	1 0	6	130	WPA2	CCMP	PSK	
	-57	0	5	0 0	6	130	WPA2	CCMP	PSK	
	-65	0	4	0 0	6	130	WPA2	CCMP	PSK	
	-65	0	3	0 0	6	130	WPA2	CCMP	PSK	
	-64	0	4	1 0	6	130	WPA2	CCMP	PSK	
	-35	0	8	0 0	6	130	WPA2	CCMP	PSK	
	-46	0	6	0 0	6	195	WPA2	CCMP	PSK	
	-78	48	3	35 0	6	54e	WPA2	CCMP	PSK	
	-72	0	6	1 0	6	270	WPA2	CCMP	PSK	
	-42	0	8	0 0	6	195	WPA2	CCMP	PSK	
	-64	0	1	0 0	6	270	WPA2	CCMP	PSK	
	-51	0	6	3 0	6	270	WPA2	CCMP	PSK	
	-58	0	7	1 0	6	130	WPA2	CCMP	PSK	
C0:25:67:30:70:90	-23	0	10	2 0	6	54e	WEP	WEP		Prueba WEP
	-56	0	7	0 0	6	270	WPA2	CCMP	PSK	

Figure 10

Network with WEP encryption

root@kali: ~

File Edit View Search Terminal Help

CH 6][Elapsed: 18 s][2020-06-25 23:51

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
C0:25:67:30:70:90	-21	0	179	2564 490	6	54e	WEP	WEP		Prueba_WEP

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
C0:25:67:30:70:90	94:0E:6B:09:78:87	-48	54e-24e	26	2828	

Figure 11

WEP traffic capture


```

root@kali: ~
File Edit View Search Terminal Tabs Help

root@kali: ~
Aircrack-ng 1.3

[00:39:01] Tested 284487 keys (got 92583 IVs)

KB  depth  byte(vote)
0  0/ 1  43(127744) 2A(105728) F6(105216) B7(104960) CB(104448) 4D(103680) 60(101888) 72(101888) 7A(101888) FD(101632) 2D(101376)
1  0/ 1  6F(111360) EC(106752) 04(106240) 32(105472) 0A(104960) 2F(104192) FE(104192) A2(103936) 4B(102656) 8D(102400) FC(102144)
2  0/ 1  6E(124416) 04(106752) D7(104704) 41(103424) 34(102400) 58(102400) 74(102144) 61(101888) C2(101888) 0F(101632) 25(101376)
3  0/ 1  74(123904) 7D(107008) 26(105984) 67(103424) 81(103168) 39(102912) 33(102656) 57(102400) 87(102144) F1(102144) 5C(101888)
4  0/ 1  72(121856) EA(105984) FA(105984) 8A(104704) 7F(104448) 87(104192) 33(103936) 84(103168) 30(102912) 6B(102912) 8C(102656)
5  0/ 1  61(121600) A6(108288) 5F(104960) F4(103936) 71(103424) A0(102400) D3(102144) E4(101888) 95(101376) E1(101120) 89(100864)
6  0/ 1  73(127744) 50(104448) C6(102912) 1A(102400) C0(101888) D8(101632) C1(101376) 5C(101120) A7(101120) 46(100864) 54(100864)
7  0/ 1  65(122368) 71(108032) 54(106496) 35(105984) A6(105472) 10(104448) BB(104192) 76(103936) 30(103680) 60(103424) D6(102144)
8  0/ 1  6E(127488) 83(106496) 0B(105984) 77(105216) 1B(104960) 6F(103936) D4(103936) 06(102912) 97(102400) A2(102400) 10(102144)
9  0/ 1  61(120320) 08(104960) 97(104960) DA(104704) 3A(104192) 62(104192) 84(103936) 15(103680) 87(103424) 88(103168) D6(102912)
10 0/ 1  C0(106752) 04(105472) 4F(104704) 84(104704) E4(103936) 16(103424) 23(102400) A0(102400) 78(101632) C1(101632) DE(101376)
11 0/ 1  D6(109056) 4F(108032) 9F(107520) 5F(106240) 17(104960) A3(103168) 81(103168) 80(102656) 27(102400) 59(102144) DB(102144)
12 0/ 5  16(103492) 46(102980) 75(101148) 5B(100584) FA(100516) CD(100400) 24(99880) EE(99868) 8E(99744) BE(99720) 39(99668)

KEY FOUND! [ 43:6F:6E:74:72:61:73:65:6E:61:57:45:50 ] (ASCII: ContraseñaWEP )
Decrypted correctly: 100%

```

Figure 12

Password identification

Figure 13

Identified WEP networks

Figure 14

Market dominance by manufacturer

Figure 15

Channel usage