A Survey on Wi-Fi Protocols:WPA and WPA2

Mahmoud Khasawneh, Izadeen Kajman, Rashed Alkhudaidy, and Anwar Althubyani

Faculty of Engineering and Computer Science, Concordia University, Montreal, Canada
{m_khasaw,i_kajman,r_alkhu,a_althu}@encs.concordia.ca

Abstract. Wireless Network (Wi-Fi) becomes extremely popular over the world on the lastly two decades. Nowadays, most people are using the wireless networks for online banking and shopping. It also allows people to share information and communicate with each other whenever and wherever they are. Moreover, it has the advantages of flexibility and freedom of mobility and enables smart phones and laptops to provide a rapid and easy access to information. All of that makes the protection of the wireless network highly demanded to be existed. Therefore, security should be applied on Wi-Fi networks to keep users' confidentiality and privacy. Hence, different protocols have been developed and applied. Nowadays, Wi-Fi Protected Access (WPA, and WPA2) protocols are considered as the most applied protocols in wireless networks over the world. In this paper, we discuss the advantages, vulnerability, and the weaknesses of both of these protocols. This paper ends up with some suggestions on how to improve the functionality of these protocols.

Keywords: Wi-Fi, Security, WPA, WPA2, Confidentiality.

1 Introduction

In the last years of the 20th century, Wi-Fi technology has accessed our houses without getting permission. In general, Wi-Fi is considered as one of the most commonly used and trusted technologies over the world. Wi-Fi networks are available everywhere, at school, at home, at hospitals, and at restaurants, etc... Therefore, users can access Wi-Fi networks anywhere and anytime with their laptops, PDAs, smart phones to share the pleasant moments with their friends.

The medium of all the data carried over Wi-Fi networks is open access i.e. the channels that carry the information exchanged in Wi-Fi networks are shared between the different users of different networks. However, this data should be securely exchanged between the users of Wi-Fi networks. Therefore, security concepts and issues have become a hot topic of research and investigation.

Starting in 1990, many wireless security protocols have been developed and adopted, but none of them could be considered as the best protocol ever because of the different security threats that daily arise with new vulnerabilities and problems to our data and applications.

G. Martínez Pérez et al. (Eds.): SNDS 2014, CCIS 420, pp. 496–511, 2014.

Three main security protocols have been developed by the researchers which are: Wireless Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA, and WPA2) [1]. WEP was the first default encryption protocol introduced in the first IEEE 802.11 standard, aimed to make the wireless network as secure as the wired network. However due to its technical failures, it was not widely applied.

In order to solve the WEP problems of the cryptography method, Wi-Fi protected access (WPA) has been proposed [1]. Wi-Fi Protected Access2 (WPA2) is a new protocol that has been developed after both WEP and WPA failed to secure the communication over Wi-Fi networks [1]. WPA2, also known as IEEE 802.11i standard, is an improvement to the 802.11 standard which specify security mechanisms for wireless networks [2].

Through this paper, we address different issues of WPA and WPA2 protocols such as: protocols' architecture, security services provided threats, strengths and weakness [3].

2 Wi-Fi Protected Access (WPA)

Due to the fact that WEP is not secure enough, the IEEE 802.11 Task Group I (TGi) presented a new protocol which is the Wi-Fi Protected Access, widely known as WPA by improving WEP. WPA contains the Temporal Key Integrity Protocol (TKIP) [4]. There are two modes under which WPA functions: the first being Pre shared Key (PSK) and the other is Enterprise [5]. Typically, the Enterprise mode is more comprehensive in terms of security; it provides as it does not share any key or information but it is harder to set up than PSK. While RC4 Stream Cipher is used for encryption in WPA, there are three elements with which TKIP differs from WEP protocol which are: Michael, a message integrity code (MIC), a packet sequencing procedure, and a per packet key mixing [6]. Figure 1 shows the Flow of TKIP Processing.

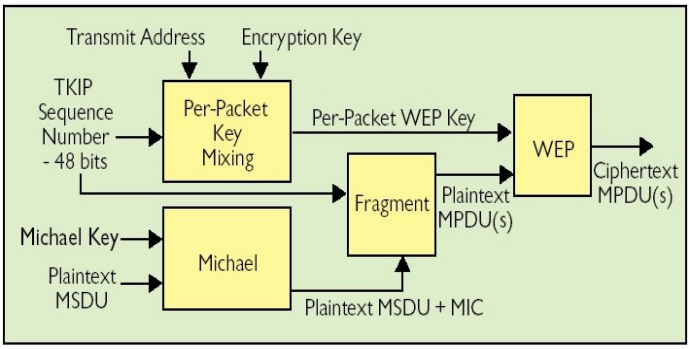

Fig. 1. Flow of TKIP Processing [4]

The main security features that are applied in WPA and different from WEP are as following:

2.1 WPA Encryption Process

- The Temporal Key Integrity Protocol (TKIP) is a protocol used for encryption and generating a new key for each packet. The size of each key is 128 bits.[2]
- For message integrity, there is an algorithm called "Michael". This algorithm is used to compute a Message Integrity Code (MIC) for TKIP, and (MIC) will be added to data to be sent.[3]
- In the encryption process, a new packet sequencing number will be processed to prove freshness of the packet that is being sent.
- For replay attack protection, TKIP offers two different data units which are: Medium Access Control Service Data Unit (MSDU) and Medium Access Control Protocol Data Unit (MPDU) [7].
- WPA uses RC4 for encryption process as WEP does but the main difference is that in TKIP the Base Kay and IV are hashed together before RC4 is being used. The result of hashing IV and the Base key will be used in RC4 with IV to generate a sequential key. The plaintext will be XORed with the sequential key and the result will be sent as a coded message [8]. The encryption algorithm is shown in figure2.

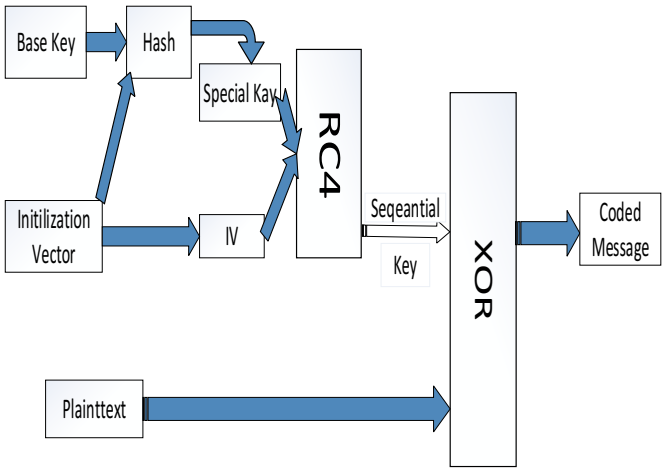

Fig. 2. WPA Encryption Algorithm (TKIP) [10]

2.2 WPA Authentication Mechanisms

In order to authenticate users and issue new keys that ensure a key management, TKIP utilizes the IEEE 802.1x standard, TKIP necessitates both a 64-bit key, that Michael uses, and a 128-bit key, that the aforementioned mixing function uses to receive a per packet key. In WPA there are two modes WPA Personal, WPA Enterprise and the authentication Mechanisms for each mode could be described as following:

- WPA Personal: It is also called WPA-PSK (Pre-Shared Key). This mode is usually used for home network or small office networks, and it does not use an authentication server. In this mode there is a key shard between the client and the access point (AP) and this key must be known to both sides for an association to be established. All wireless devices use 256 bits key to authenticate with their access point(s). It is extremely important that the shared key will never be transmitted between the client and the AP. By using the shard key the MIC and encryption key will be founded. MIC is in size of 64 bits and the encryption key size is 128 bits [4].
- WPA Enterprise: It is usually used for business network. No shred key is used in the authentication process; however an Extensible Authentication Protocol (EAP) is used. (EAP) offers two ways authentication. In this mode Remote Authentication Dial In User Service (RADIUS) server is obligatory and it delivers an excellent security for wireless network traffic [4].

3 Wi-Fi Protected Access (WPA2)

In 2004, the ratification of WPA2 is widely known as the second generation of WPA and it is recognized to be the most secure protocol used in wireless networks. This protocol uses the implementation of the 128-bits Advanced Encryption Standard (AES) block cipher algorithm for both authentication and encryption processes. In WPA2 there are two modes of authentication that could be used which are Pre-Shared Key and Enterprise. Instead of TKIP, WPA2 uses Pair wise Transient Key (PTK) for key generation. Instate of using Michael algorithm, WPA2 uses CCMP (Counter Mode CBC MAC Protocol) which applies block cipher Advanced Encryption Standard (AES) algorithm. In order to ensure integrity and provide accurate authentication, CCM (CBC-MAC) has been used in WPA2 [9].

3.1 WPA2 Encryption Process:

The encryption process, as shown in figure 3, could be done by applying the following steps:

- For each Medium access control Protocol Data Unit (MPDU) there is a packet number (PN) and this number will incremented for each next MPDU.

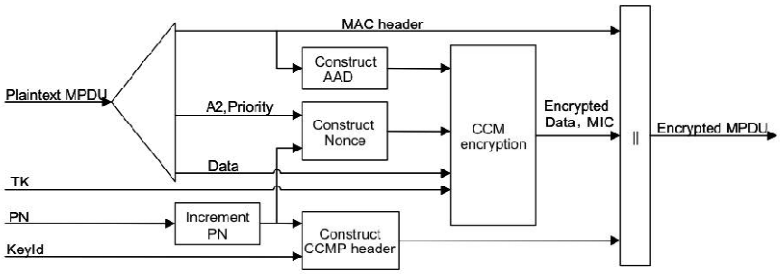

Fig. 3. CCMP Encryption Process [2]

- In the header of MPDU, there is something called Additional Authentication Data (AAD) and in this field the integrity delivered by CCMP is represented.
- To create the CCMP Nonce block the PN and, A2 (MPDU address 2) and Priority field of MPDU will be used. The Priority field has reserved value of zero.
- In addition the new PN with the key identifier together will be used to build the 64 bit CCMP header.
- The group of temporal key, AAD, nonce, and MPDU data are used to create the cipher text and MIC.
- Finally, the encryption of MPDU is obtained by combining the CCMP header, original MPDU header, encrypted data and MIC [2].

3.2 WPA2 Decryption Process

WPA2 does not use the XOR to decrypt the plaintext, and the decryption process will be done in the same steps. The steps for decryption, as shown in figure 4, are described as following:

- After the encrypted MPDU is received, the AAD and nonce values could be extracted from the encrypted MPDU.
- The header of the encrypted MPDU is used to build the AAD.
- To create the nonce value, the values of different fields of the header will be used which are the MPDU address 2 (A2), PN, and Priority fields.
- To recover the MPDU plaintext, temporal key, MIC, AAD, nonce and MPDU cipher text data are combined together. Moreover at this point the integrity of AAD and MPDU plaintext is confirmed.
- Finally, by combining MAC header of MPDU and decrypted MPDU plaintext data, the Plaintext of MPDU is decrypted See figure4 [2].

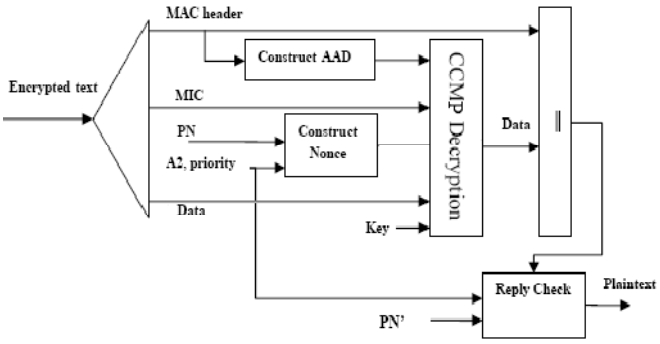

Fig. 4. CCMP Decryption Process [2]

3.3 Authentication Mechanisms

For authentication there are two types of key management systems, each of which utilize different means: an authentication server system or a pre-shared key system and once the keys are generated the authentication could be done same as it is used in WPA [4]. There are two types of key management systems which are described as following:

- A pre-shared key system is less comprehensive in terms of security than a system that uses an authentication server. However, despite such relatively incomprehensive security and the fact that complete implementation of the 802.11i protocol restrict any usage of pre-shared keys, small business and home users can still implement and utilize pre-shared keys with much ease[10].
- A system that generates keys through an authentication server is relatively hierarchical; what facilitate the creation of matching Pairwise Master Keys (PMK) at both supplicant and the authentication server sides is the 802.1x key generation protocols. Every time a device interacts with an AP, four types of 128-bit temporal keys, known as the Pairwise Transient Key (PTK), are generated: they are a data encryption key, a data integrity key, EAPOL-key encryption, and EAPOL-key integrity key [11]. In order not to only increase randomness but also relate the keys to its creator device, the key incorporates a random nonce and MAC addresses of the device. Then there are the four exchange ways called 4-way handshake between the AP and the authentication server, which identify and verify the key. Following the first step, which is the generation of a temporal keys and a pair of nonces, which the supplicant and authenticator have made, the supplicant verifies its knowledge of the PMK, and subsequently, the authenticator does so too. Finally, both devices have encryption turned on for unicast packets [10]. Also, it should be noted that 802.11i supports broadcast messages. In order to ensure efficiency, a Group Master Key (GMK) is created, and the GMK facilitates the generation of the

Group Encryption Key and Group Integrity Key that all participating g clients receive through a secure channel. Figure 4 illustrates how the protocols differ from each other. It is interesting to note that a hardware upgrade is necessary for 802.11i [12].

4 Comparison of Wi-Fi Protocols: WPA and WPA2

4.1 Data Integrity: WPA and WPA2

WPA uses Michael to verify the integrity of the message. In addition the Packet Sequencing is used to prevent replay attacks. On the other hand, WPA2 uses CCMP to provide integrity for both data and packet header [13]. A 48-bit sequence number that changes whenever there is a replacement of a MIC key prevents replay attacks; this sequence is what TKIP utilizes and labels as packet sequencing. The method mixes the aforementioned sequence number with the encryption key, encrypting the MIC and WEP ICV while detecting and removing packets that contain an out-of-sequence number. This section represents the Michael and Counter Mode with Cipher Block Chaining MAC Protocol (CCMP) protocols [7].

4.1.1 Michael or MIC

These MIC algorithms protect data integrity from the modification that could be caused by counterfeiting and forging [14]. Simply, a predefined algorithm and data both together calculate a tag value that the sender transmits with the key and the comparison between the sent value and the other value that the receiver calculates determine whether data integrity is intact or not [10]. In particular, Michael necessitates a new 64-bit key and represented as two 32-bit little Endian words (K_0 ,K_1). The functionality of MIC works as following:

- The length of total message is a multiple of 32-bits and to ensure that message will be a multiple of 32-bits add a message with the hexadecimal value 0x5A and enough zero pad.
- Dividing the message of a multiple of 32-bits into sequence of 32-bit words (M_1 , M_2 ……M_n)
- finally calculates the tag from the key and the message words by following format [10]:

  (L, R) ← (K_0 , K_1)
  do i **from** 1 **to** n
  L←L *XOR* M_i
  (L,R)← Swap (L,R)
  return (L,R) as the tag
- The verification step is done by matching the tag received with the message and the tag that achieved by computing the previous step.

- The time that an attacker needs to be able to build his/her MIC and not be detected is as following: if MIC is a S bits the average time will be after 2^{-S+1} packet [10].

4.1.2 Counter Mode with Cipher Block Chaining MAC Protocol (CCMP)

Michael was used in WPA for data integrity. Michael was developed to let existing wireless devices to overcome the several flaws of WEP. Michael may be implemented through software updates; it does not require hardware replacement of AP and STAs. However, it still depends on RC4 cryptographic algorithm so it is not a good solution for high assurance environments. Therefore, Counter Mode with Cipher Block Chaining MAC Protocol (CCMP) is developed and considered as a better solution [15]. However hardware upgrades are required for the wireless devices used.

CCMP relies on CCM which is a cipher mode of AES that is used to authenticate an encrypted block. In CCM, a 128-bit block size is ciphered. Cipher Block Chaining MAC (CBC-MAC) is used in CCM for both authentication and integrity protection. CCMP compromise the integrity of both the packet data and the MAC portion of the IEEE 802.11 header. In order to prevent replay attacks CCMP uses a nonce which is constructed by using a 48-bit packet number PN [16].

CCMP is considered as the best solution for both confidentiality and integrity. It uses the same cryptographic key for both confidentiality and integrity which reduces the complexity. CCMP provides integrity of both packet header and packet payload.

Figure 5 illustrates the integrity process of the packet's data and header. The process is done in 5 phases which are:

- Packet Number (PN) Increment: A 48- bits packet number used for each session is incremented. PN prevents replay attacks from occurring and ensures that the TK of each session lives more time than that of any possible STA-AP association.
- Nonce construction: A nonce is constructed by combining the packet number PN with the transmitter ad address (A2) as well as with the priority bits.
- CCMP Header Construction: a 48-bits Key ID used to identify the Temporal Key (TK) is joined with the incremented PN to form the CCMP Header.
- Additional Authentication Data (AAD) Construction: AAD is one of the important inputs to the CCM encryption module; it is either a 22-bytes or 28 bytes in length. It is constructed by using different fields of the MAC header such as the quality-of-service QoS parameter.
- CCM Encryption: it is considered the main sub-process in the data integrity procedure in WPA2 protocol. It is constructed by combining Tk, Data, AAD, and nonce all together and outputs the encrypted data. This encrypted data is concatenated with MAC header, CCM header, and MIC to form the ciphered MPDU

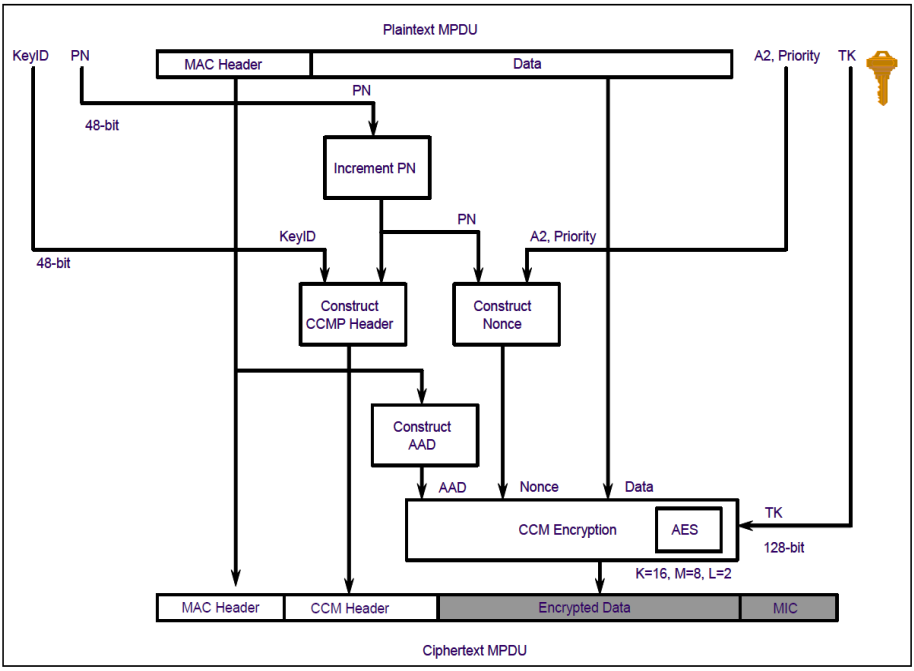

Fig. 5. Integrity in WPA2 [20]

Temporal Key TK changed through each association between the station STA and the access point AP. MIC encrypted with the data is 8 bytes in size. The ciphered frame is sent over the medium and a reversed procedure used to decrypt the encrypted data [5].

4.2 WPA/WPA2 Weaknesses

Although WPA/WPA2 security schemes are strong, there are a number of trivial weaknesses have been found, still, none of them are risky with the security recommendations. However, Authentication mechanisms in WPA-PSK is vulnerable to dictionary attack, which have already been implemented [3]. This attack is based on capturing the 4-way handshake between client and AP which clearly provide enough information to start an attack. Unlike WEP, where statistical methods can be used to speed up the cracking process [3], the Pre-Shared Key (PSK) is derived using the Password Based Key Derivation Function (PBKDF2) which is pseudorandom function that takes several inputs and hashes them multiple times to produce a key [12]. This means that the attacker has all the information and the only thing that the attacker needs is brute force the hand shake to match the 256 bit key which can be a passphrase of 8 to 63 printable ASCII characters. [3].

The Pairwise Transient Key (PTK) is derived from the PMK via the 4-Way Handshake with information used to calculate its value is transmitted in plain text [1]. This information includes MAC address of the client, MAC address of the AP and the two random numbers (ANonce and SNonce) [1]. The only item missing is the PMK/PSK, so the attackers can simply brute force PMK with the need to know the SSID which is easy to be obtained with a sniffer [3].

Even though WPA-PSK is a 256 bits key in length, it has a major weakness because it is based on the pairwise master key (PMK) that is generated by PBKDF2 key derivation function. The PBKDF2 in WPA has five input parameters which are: PMK = PBKDF2 (password, SSID, SSID length, 4096, 256) [1].

Where 4096 is number of the iterations of a sub-function and 256 is length of the output. This means that the strength of PTK relies only on the PMK value, which is the Pre-Shared Key (passphrase) [1].

4.3 WPA/WPA2 Strengths

WPA and WPA2 have several improvements that have helped and supported the Wi-Fi to be more secure than that previously.

As the Clint which is a station (ST) and the access point (AP) have one sharing data cryptography key which is secret between them, the WPA/WPA2 provide mutual authentication in order to prevent the key from being captured when it is transmitted over air [15]. In WPA protocol, data encryption has been improved by using a Temporal Key Integrity Protocol (TKIP). It also has a hashing function that mixes the keys by integrating two components which are the initialization vector (IV) and the base key [17]. Moreover, in order to make sure that the keys have not been changed, the WPA uses an integrity-checking feature. One of the most developments made by WPA and WPA2 are extending the length of Initialization Vector (IV) to 48 bits instead of 24 bits to make sure the IV is not used before, as well as it is used for the TSC (TKIP Sequence Counter) in order to protect against replaying data [15]. In terms of integrity, WPA uses a 'Michael', which is a Message Integrity check mechanism (MIC) while WPA2 uses CCM. On the other hand, enterprise mode is another type of WPA/WPA2 modes. Enterprise mode uses 802.1X+EAP for authentication mechanism via an authentication server (802.1x) that offers a perfect control and security to the client's wireless network traffic. Moreover, in this mode does not use a pre-shard key but it needs a RADIUS server, which is called an authentication server [15]. To avoid reusing the keys there is a rekeying mechanism to afford the freshness of the encrypted plaintext and integrity keys that will be used [10]. One of the most strength things in WPA2 is that it uses an Advanced Encryption Standard (AES) for data encryption. It also uses a block cipher which is working to cipher all blocks of the text every time [8].

Table 1 summarizes the main differences between WPA and WPA2.

Table 1. Differences between WPA and WPA2

Features of Mechanism	WPA	WPA2
Purpose	Solves the problems that are in WEP protocol	Solves the problems that are in WPA protocol
Require new Hardware	No	Yes
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)	CCMP
Header Integrity	MIC (Michael)	CCMP
Replay Attack Prevention	IV Sequence	IV Sequence

5 Attack SCENARIO

In the following scenario we will walk through the approach to capture the WPA/WPA2 authentication handshake and then use aircrack-ng to crack the pre-shared key. First, we set up our network target as it appears in Figure 6 which uses WPA2 encryption.

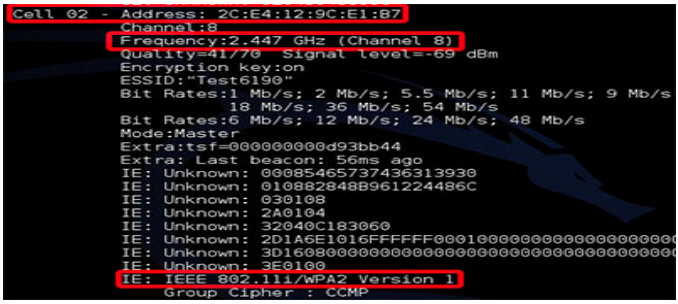

Fig. 6. The target network

5.1 Four-Way handshake capture

In order to capture the four-way authentication handshake we need to set up our wireless interface to monitor mode. The purpose of this step is to allow the card to monitor the packets received filtering [1].

```
airodump-ng -c 8 -w hk.cap --bssid 2C:E4:12:9C:E1:B7 --ivs mon0
```

Fig. 7. Start airodump-ng

Where the parameters are [18]:

- -c 8 is the channel for the wireless network
- --bssid 2C:E4:12:9C:E1:B7 is the access point MAC address. This eliminates extraneous traffic.
- -w hk.cap is the file name prefix for the file which will contain the IVs.
- mon0 is the interface name.
- --ivs is option to save only captured IVs

```
CH  8 ][ Elapsed: 52 s ][ 2013-07-29 09:52

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

2C:E4:12:9C:E1:B7  -63 100      520       50    0   8  54e  WPA2 CCMP   PSK  Test6190

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

2C:E4:12:9C:E1:B7  E8:99:C4:93:14:B2  -40    0e- 1      0       84
2C:E4:12:9C:E1:B7  78:CA:39:BA:F4:8E  -40    1e- 1      0       59
```

Fig. 8. Discovering network client

Figure 8 shows what the results look like, there are two wireless clients are connected to the network. To capture the WPA/WPA2 authentication handshake we can perform either active or passive attack [1]. The passive attack simply is to wait for a client to re-associate to the PA. In contrast, the active attack means that a client is forced to de-authenticate in order to accelerate the process [1].
In this case, we are performing active attack using Aireplay-ng which supports various attacks such as deauthentication, to capture WPA handshake data [1].

```
aireplay-ng -0 1 -a 2C:E4:12:9C:E1:B7 -c 78:CA:39:BA:F4:8F mon0
```

Fig. 9. Client Deauthentication attack

Where as in [18]:

- -0 means de-authentication.
- 1 is the number of de-authenticate to be sent.
- -a 2C:E4:12:9C:E1:B7 is the MAC address of the access point.
- -c 78:CA:39:BA:F48F is the MAC address of the target client that we are de-authenticating.
- mon0 is the interface name.

Fig. 10. De-authentication output

Figure 11 illustrates what the output looks like of the pervious command. This means that the client is authenticated in order to capture the four-way handshake [1].

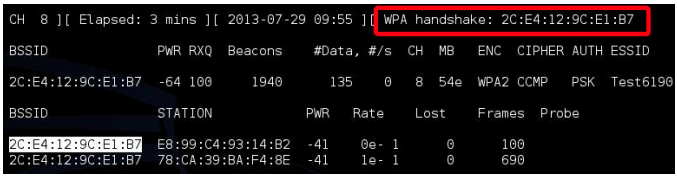

Fig. 11. Four-Way handshake capture

Also, as a result of the Aireplay-ng command, the four-way handshake is obtained successfully as it shown in figure 11.

5.2 Dictionary Attack

The final step is to launch a dictionary attack, which is a technique for defeating authentication mechanism by trying to each client to determine its passphrase. Aircrack-ng can be used to perform a dictionary attack in order to recover a WPA key [1].

```
aircrack-ng -w wordlist.lst -b 2C:E4:12:9C:E1:B7 hk.cap.ivs
```

Fig. 12. Launching a dictionary attack

In figure 12, the parameters are [18]:

- -w wordlist.lst is the name of the dictionary file.
- --bssid 2C:E4:12:9C:E1:B7 is the access point MAC address
- hk.cap.ivs is name of files that contain the captured four-way handshake.

The purpose of using Aircrack-ng is to duplicate four-way handshake to determine if a particular passphrase in the wordlist matches the results of the four-way handshake [3]. Aircrack-ng takes three inputs ehich are a dictionary file of either ASCII or hexadecimal keys, the mac address of Access point and the file that contains the handshake data [1]. This process is very computationally intensive in practice because it must take each dictionary word and perform 4096 iterations of HMAC-SHA1 before it generates valid PMK. Figure 13 shows that the pre-shared key has been successfully identified [1].

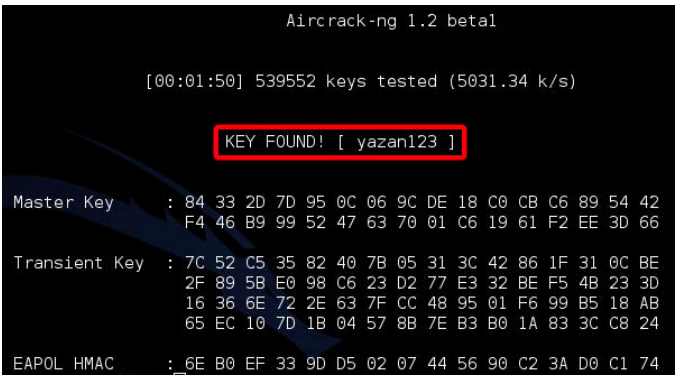

Fig. 13. Successfully cracking the pre-shared key

Calculating the PMK is very slow since it uses the PBKDF2 algorithm as we mentioned early. The example above has shown that using this technique in Aircrack-ng can check more than 4943 passwords per second. However, it is possible to achieve a time-space tradeoff by pre-computing PMK for given ESSID which is impractical [1].

6 Defence against WPA-PSK Attack

Unfortunately, the vulnerabilities in WPA-PSK authentication, which make the exploit feasible, cannot be avoided [19]. However, there are several steps that can be taken in order to mitigate these vulnerabilities and protect your WLAN against pre-shared keys (PSK) attack which are:

Step 1: avoid using a short PSK that can be guessed too easily or found in a password dictionary. In configuring a passphrase, the IEEE 802.11i standard recommends very strongly to use at least 20 characters [20]. The strongest passphrases which are randomly-generated that mix of lower and uppercase letters, numbers and symbols, the more PSK is protected against dictionary attacks [20].

Step 2: Changing the SSID do not achieve enhanced wireless security but can help to prevent users from accidentally connecting to the wrong WLAN. Also, to make it more difficult for attackers to identify the organization's WLANs [20].

The dictionary attacks can be infeasible on WPS-PSK by using D-WPA-PSK mechanism which is regular replacement of PSK that are generated by a key generator distributed to all clients in advance [21]. In this method the AP sends a random number to all clients every certain time. The client will send an acknowledgement to the AP when it receives the random number [21]. After all the clients that associated with the AP get random numbers, a new pre-shared keys (PSK) will be generated

between the AP and clients which is derived from key generator distributed in advanced [21]. At this point, the clients and the AP will restart the network configuration using the new PSK. This method provides frequent updates of the PSK based on the time that an attacker needs to crack PSK. Therefore d-WPA-PSK achieves somehow enhanced security on a WLAN network [1].

7 Conclusion

The paper described the new protocols developed in Wi-Fi such as WPA and WPA2. Different security services provided by each of them, WPA provides user privacy and confidentiality by using TKIP for encryption and Michael for data integrity. Despite the advantages provided by WPA, it still has some weaknesses regarding the authentication and data integrity processes. Therefore, WPA2 was developed. New mechanism for data integrity in WPA2 was proposed which is CCMP. WPA2 also requires new hardware equipment in order to be installed in. A scenario attack was illustrated in detail and shows that some vulnerability still can take place despite all the security improvements that have been done.

References

1. Mylonas, P., Mavridis, I.P., Androulakis, A.-I.E., Halkias, A.B.: Real-life paradigms of wireless network security attacks (2011)
2. Sukhija, S., Gupta, S.: Wireless Network Security Protocols A Comparative Study (January 2012)
3. Lehembre, G.: Wi-Fi security – WEP, WPA and WPA2 (June 2005)
4. Mathews, M., Hunt, R.: Evolution of Wireless LAN Security Architecture to IEEE 802.11i (WPA2). In: Proceedings of the fourth IASTED Asian Conference on Communication Systems and Networks (2007)
5. Lehembre, G.: ―Wi-Fi security –WEP, WPA and WPA2 ‖, Article published in number 1/2006 (14) of hakin9 (January 2006), Publication on, http://www.hsc.fr
6. Turab, N., Masadeh, S.: ―Recommendations guide for WLAN Security. The International Journal of ACM 1(1) (March 2010)
7. Park, S.H., Ganz, A., Ganz, Z.: ―Security protocol for IEEE 802.11 wireless local area network. Mobile Networks and Applications 3 (1998)
8. Katz, F.H.: ―WPA vs. WPA2: Is WPA2 Really an Improvement on WPA? In: 2010 4th Annual Computer Security Conference (CSC 2010), Coastal Carolina University, Myrtle Beach, SC, April 15-16 (2010)
9. Frankel, S., Eydt, B., Owens, L., Scarfone, K.: Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, NIST Special Publication 800-97, National Institute of Standards and Technology (2007)
10. Lashkari, A.H., Danesh, M.M.S., Samadi, B.: FCSIT. A survey on wireless security protocols (WEP, WPA and WPA2/802.11i). In: 2nd IEEE International Conference on Computer Science and Information Technology, ICCSIT (2009)
11. Benton, K.: ―The evolution of 802.11 wireless security ‖, INF 795. UNLV Informatics-Spring (April 18, 2010)

12. Beck, M., Tews, E.: ―Practical attacks against WEP and WPA‖. In: WiSec 2009: Proceedings of the Second ACM Conference on Wireless Network Security. ACM, New York (2009)
13. Arockiam, L., Vani, B.: ―A Survey of Denial of Service Attacks and its Countermeasures on Wireless Network‖. International Journal on Computer Science and Engineering 2(5), 1563–1571 (2010)
14. Arockiam, L., Vani, B.: ―A Survey of Denial of Service Attacks and its Countermeasures on Wireless Networkİnternational Journal on Computer Science and Engineering 2(5), 1563–1571 (2010)
15. Bulbul, H.I., Batmaz, I., Ozel, M.: Wireless Network Security: Comparison of WEP (WiredEquivalent Privacy) Mechanism, WPA (Wi-Fi ProtectedAccess) and RSN (Robust Security Network) Security Protocols, e-Forensics 2008, Adelaide, Australia, January 21-23 (2008)
16. Miller, B.: WPA2 Security: Choosing the Right WLAN Authentication Method for Homes and Enterprises. Global Knowledge (2008)
17. Macmichael, J.L.: Auditing Wi-Fi Protected Access (WPA) Pre-Shared Key Mode. Linux Journal (137), 56, 58–60 (2005)
18. Cracking Wireless. Ryan Curtin Ryan at, `http://igglybob.com`
19. De Rango, F., Lentini, D.C., Marano, S.: Static and dynamic 4-wayhandshake solutions to avoid denial of service attack in Wi-Fi protected access and IEEE 802. I li. EURASIP 1. Wire!' Commun. Netw. (2) (April 2006)
20. Scarfone, K., Dicoi, D., Sexton, M., Tibbs, C.: Recommendations of the National Institute of Standards and Technology. Guide to Securing Legacy IEEE 802.11 Wireless Networks (July 2008)
21. Wang, Y., Jin, Z., Zhao, X.: Practical Defence against WEP and WPA-PSK Attack for WLAN (September 2010)