www.ijemr.net ISSN (ONLINE): 2250-0758, ISSN (PRINT): 2394-6962

Volume-8, Issue-4, August 2018

International Journal of Engineering and Management Research

Page Number: 1-10

DOI: doi.org/10.31033/ijemr.8.4.1

Solving Downgrade and DoS Attack Due to the Four Ways Handshake Vulnerabilities (WIFI)

Cyrille Clovis Tchouchoua Teyou[1] and Pin Zhang[2]

[1]Research Scholar, School of Communication Engineering, Hangzhou Dianzi University, Xiasha Higher Education Zone, Hangzhou 310018, CHINA

[2]Research Scholar, School of Communication Engineering, Hangzhou Dianzi University, Xiasha Higher Education Zone, Hangzhou 310018, CHINA

[1]Corresponding Author: cyrille_tchoutchoua@yahoo.fr

ABSTRACT

The growing volume of attacks on the Internet has increased the demand for more robust systems and sophisticated tools for vulnerability analysis, intrusion detection, forensic investigations, and possible responses. Current hacker tools and technologies warrant reengineering to address cyber crime and homeland security. The being aware of the flaws on a network is necessary to secure the information infrastructure by gathering network topology, intelligence, internal/external vulnerability analysis, and penetration testing. This paper has as main objective to minimize damages and preventing the attackers from exploiting weaknesses and vulnerabilities in the 4 ways handshake (WIFI).

We equally present a detail study on various attacks and some solutions to avoid or prevent such attacks in WLAN.

Keywords-- Cipher 4 (RC4), RSNE, TKIP, WPA, IEE802.11i

I. INTROCUTION

Wireless local area network (WLAN) is used to connect the computing devices with the internet through an Access Point (AP) using a wireless media. It is a fast-growing Technology in the world and it can be an alternate to the Wired Technology. It can be found everywhere including banks, telecommunication companies, hotels, hospitals, academic institutions, government sectors, intelligence organizations, and the military[1]. It creates an invisible path between the internet and the wireless network. Nowadays it is more popular due to its various advantages such as high data rate, flexible, low cost, effectiveness, mobility and easy to access by any one [2].

Even though it is popular, there is more vulnerability that exists. The nature of wireless network transmission and the emerging attacks are continuously creating or exploiting more vulnerability [3]. Despite the fact that the security mechanism and protocols are upgraded and enhanced, some companies or organization environments cannot afford a separate authentication system, and generally adopt the Wi-Fi-Protected-Access/Preshared-key(WPA2-PSK) which is not assuring 100 % security and are still exposed to some categories of attacks such as downgrade attacks, de-authentication attacks and DoS, that aims to push wireless clients to re-authenticate to Access point(AP) and try to capture the key exchanged during the handshake to compromise the network security **[4]**.

If these wireless communications are hacked, huge classified data and information will be lost to un-authorized persons globally.

Daily, the academia and industry are seeking to find a better way to achieve the security of the data.

Our research will consist of analysis, discussion, and evaluations on existing approaches to secure the communication a data exchanged between any device connected to the WLAN and the Access Point. This paper is divided into five main points:

In part II we give a brief history and background of WEP, WPA and WPA2.After that, in part III the preliminaries of WIFI 4-ways handshakes with explanation of all the states or stages before, during the handshake, exchange of messages and even after the wifi 4-ways handshake with the comparison approach of different encryption method for wifi. then in part IV we talk about flaws and vulnerabilities. we describe some attacks such DoS , downgrade attack. In part V we introduce some related works and suggested solutions before conclusion.

II. HISTORY AND BACKGROUND OF WPA2

In this section we give a brief overview and brief history of WIFI Protected Access 2 (WPA2) standard.

To start with, the first one is IEEE 802.11 originally specifies the equivalent of wired LAN security algorithm Wired Equivalent Privacy (WEP) to protect data. Unfortunately, it contains evident design flaws, and is considered completely broken. Amendment ratified on June 24th 2004, specifies security mechanisms for WLANs. However, it's shown in many researches that WEP cannot achieve the required data confidentiality, integrity, and authentication. As a result, the use of WEP for confidentiality, authentication, or access control is deprecated on later revision of the standard in 2012 [5].

Although WEP fails to satisfy the security requirements of the standard, a new standard will require a new hardware. It is not practical to easily discard the users with legacy devices supporting only WEP. IEEE 802.11 designed both a short-term and long- term solution. As short-term solution, WEP has been succeeded by Wi-Fi Protected Access (WPA) which uses the legacy hardware. WPA was just an intermediate solution to cover the weaknesses of WEP. To solve this problem, the (WPA) was designed as a short-term solution. Like WEP, it is based on the RC4 cipher, meaning WEP-capable hardware could support it using only firmware upgrades and was later superseded by WPA2.

WPA adopts Temporal Key Integrity Protocol (TKIP) for confidentiality and Integrity, which still uses Rivest Cipher 4 (RC4) for data encryption. A key mixing function is included in TKIP as well as an extended IV space to construct unrelated and fresh per-packet keys. WPA introduced Michael algorithm [6] for purpose of improving data integrity. Furthermore, WPA implements a packet-sequencing mechanism by binding a monotonically increasing sequence number to each packet. This helps in replay packets detection. Although TKIP addresses all known vulnerabilities, yet it had some limitations due to the use of legacy hardware. TKIP relies on Message Integrity Check (MIC) algorithm called Michael, which provided inadequate security [7, 8].

Their long-term solution is called (AES) CCMP, which uses AES in counter mode for encryption and CBC-MAC for authenticity. A new long-term solution is proposed for enhancing the security in the MAC layer. Unfortunately, older WEP-compatible devices were not in high performance to implement CCMP in software using firmware updates.

However, TKIP is still supported by many devices and should be discouraged [9]. IEEE 802.11i uses CCMP to provide confidentiality, integrity, and replay protection. Moreover, it uses 802.1X authentication and key management to provide mutual authentication and generate fresh session key for data transmission. IEEE 802.11i improves the security in terms of data confidentiality, integrity and authentication.

Namely that WPA2 means (AES) CCMP is used, while a WPA2 network might still use (or support) TKIP.

Both of WPA and WPA2 use the same authentication system. Enterprise networks use 802.1X/EAP frameworks for centralized mutual authentication system. For home and small office environments Pre-Shared Key (PSK) is used.

Since WPA and WPA2 are both based on the 802.11i standard, they are nearly identical to each other. Therefore, unless mentioned otherwise, we will treat WPA as identical to WPA2. There are few differences between them which are covered in the following sections.

III. THE PRELIMINARIES OF WIFI 4-WAYS HANDSHAKES AND COMPARISON APPROACH OF DIFFERENTS ENCRYPTION METHOD FOR WIFI

3.1 Preliminaries of wifi 4 ways handshake

Before any encryption everything goes from the discovery of the network by listening probe or sending request to the Access Point (AP or Authenticator) by client(Supplicant). Authentication process is carried out either using a pre-shared key (**PSK**) or following an **EAP** exchange through 802.1X (known as EAPOL, which requires the presence of an authentication server). This process ensures that the client station (Suppliant) is authenticated with the AP. After the PSK or 802.1X authentication, a shared secret key is generated, called the Pairwise Master Key (PMK). The PSK is derived from a password that is put through **PBKDF2-SHA1** as the cryptographic hash function. In a pre-shared-key network, the PSK is actually the PMK. If an 802.1X EAP exchange was carried out, the **PMK** is derived from the **EAP** parameters provided by the authentication server. After the handshake, connection is built and thanks to the encryption method, it is too hard to decrypt by the attackers.

It will be very interesting to mentioned that Even though CCMP is largely improved compare to TKIP, yet there is a significant reduction in throughput. A possible explanation of this might be the cost of combining the encryption and integrity protocols in CCMP **[10].**

3.1.1 State 1 Network Discovery

Access Point (AP) periodically broadcasts beacons to advertise its presence. These beacons include the supported link-layer encryption algorithms that are supported by the AP. This is either TKIP and/or CCMP. As said before, Suppliant can discover networks by passively listening for beacons, or by actively sending probe requests. Beacons and probe responses contain the name and capabilities of the wireless network. Although

the bit-wise encoding of the RSNE differs between WPA and WPA2, in both WPA versions the RSNE contains the same information.

3.1.2 State2 Authentication And Association

In principle, authentication may already happen at this point, but in practice most networks use Open System authentication. This mechanism allows any client to authenticate. Once authenticated, the supplicant sends an association request to the AP. This frame includes the pair wise cipher that the client wants to use, encoded in an RSNE element. If the supplicant encodes the RSNE using the conventions of WPA, the WPA variant of the handshake will be executed. Otherwise, the WPA2 variant will be executed. The AP replies with an association response, indicating the association was successful or not.

3.1.3 State3 802.1x Authentication

This stage is optional and consists of 802.1x authentication to a back-end Authentication Server. This may consist of authentication using a username and password to a RADIUS server. The result of this authentication is that the client and AP share a secret Pairwise Master Key (PMK).We assume the supplicant and authenticator derive the PMK from a secret pre-shared key.

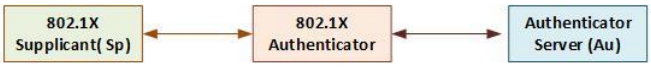

Figure 1. 802.1X Authentication

3.1.4 State 4 The 4-Way Handshake

The 4-way handshake provides mutual authentication and negotiates a fresh Pairwise Transient Key (PTK). it prevents downgrade attacks by cryptographically verifying the RSNEs received during the network discovery and association stage. The PTK is derived from the Authenticator Nonce (ANonce), Supplicant Nonce (SNonce), and the MAC addresses of the client and AP. After the optional 802.1X authentication is completed, 802.11i begins to secure the link by executing the 4-way handshake. The 802.11i 4-way handshake procedure makes the following steps.

- It derives a fresh session key (TKIP).
- Through transmission and receiver timer's management and handshake messages it synchronizes its operations.
- It distributes a broadcast key from the AP to the station.
- It verifies that peer is live.
- It confirms that peer possesses the station.
- It binds the MAC addresses of the station and AP to this key.

In the 4-way handshake only 4 types of messages (packets) are considered and structured as follows

1) M1: [Mau, ANonce, SN, M1];
2) M2: [Msp, SNonce, SN, Msg2, MIC(SNonce, SN, M2)];
3) M3: [Mau, ANonce, SN + 1, Msg3, MIC(ANonce, SN + 1, M3)];
4) M4: [Msp, SNonce, SN + 1, M4, MIC(SNonce, SN + 1, M4)];

Where

- Mau represents the MAC address of AU (authenticator);
- Msp is the MAC address of SP(supplicant);
- ANonce is a random value generated by AU;
- SNonce is a random value generated by SP;
- SN represents the sequence number of the message;
- MX identifies the type of message X.

Let go in deep of packet of each message in this state or stage.

3.1.4.1 Message1 (FIRST PACKET)

The protocol starts with the generation of a random bits string called "nonce." This nonce is generated only once. At the beginning **Au** generates this nonce (ANonce) and it puts this one inside the first message (M1) (Paquet) sent to Sp.

3.1.4.2 Message2 (SECOND PACKET)

The reception of M1 (Paquet 1) then, Sp will know Mau, SN, and Anonce. These values can be useful in the generation of PTK. Sp will produce a novel *nonce* called SNonce that will be used with PMK and ANonce to generate the PTK in the following way**:**

PTK = PRF (PMK, ANonce, SNonce, Mau, Msp), where **PRF** is a pseudorandom cryptographic function.

After calculating PTK, S will store ANonce, SNonce, and PTK and it will send the M2 to Au.

MIC will be also inserted. The MIC value is calculated through the PTK previously obtained value and for this reason it is **univocally** dependent by PTK

3.1.4.3 Message3 (THIRD PACKET)

It is sent by the Access Point (Au), and its required key info flags are Pair wise, MIC, and Secure. Here the Key Data field includes the RSNE, which contains the supported cipher suites of the Au. Additionally, if WPA2 is used; it also includes the encrypted GTK. When WPA1is used, the GTK is sent to the supplicant using a group key. When the client receives this message, it checks that the (authenticated) RSNE in message 3 is identical to the one received in beacons and probe requests. If they differ, a downgrade attack was attempted, and the handshake is aborted.

3.1.4.4 Message4 (FOURTH PACKET)

The supplicant (Sp) sends message 4 to the authenticator, to confirm that the handshake has been successfully completed. This last message is also authenticated using a MIC. When WPA2 is used, the required key info flags are Pairwise, MIC, and Secure. However, for WPA1, the required key flags do not include Secure.

We use M4 to represent the required key info flags for both WPA versions the 4-way handshake provides an asymmetric scheme of alert as presented below:

- If **Sp** and **Au** receive a message with invalid SN or MIC values, they will discard the message; this approach avoids the "man-in-the-middle" attack [11];
- If Sp does not receive the M1 within a time stamp (**TS**), it will disassociate, de-authenticate, and start the authentication procedure again;
- If Au does not receive the M2 (or M4) within TS, it will try to send the M1 (or M3) again; so, after k attempts, it will de-associate Sp.

It Is important to Notice that message 2 and message 4 have the same required key info flags if WPA1 is used. The only way to differentiate them in WPA1 is to see whether there is data present in the key data field. Once the authenticator received message 4, normal (encrypted) data frames can be transmitted. also, Message 4 is essential in preventing downgrade attacks against the 4-way handshake.

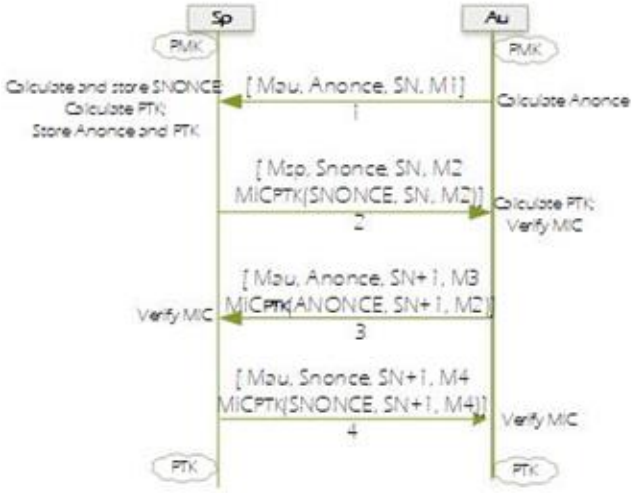

Figure2. The 4-way handshake messages

3.1.5 State5 Group Key Handshake

The last stage consists of the group key handshake and is required when using WPA. It transports the group key to the client, which is used to protect broadcast and multicast traffic. In both WPA and WPA2, the group handshake is also periodically executed to renew the group key.

In fact, the Pair wise security key system, could be resumed like follow Temporal Key in WPA2
The specificity and highlight of each pairwise security key would be useful.

1. PTK: Pairwise Temporal Key
   - Protect unicast communication between AP and client
   - Generated using EAPOL 4-way handshake
   - PTK = Function of PMK, nounce1, Nounce2

2. GTK: Group Temporal Key Protect broadcast / Multicast
3. Communication from AP to Client Transported from AP to client in EAPOL 4-way handshake on Group 2-way handshake
4. IGTK: Integrity Group Temporal Key Protection of Broadcast/Multicast management frames. (MFP) frame Transported from AP to client in EAPOL 4-way handshake

3.2 COMPARISON of different method of encryption in WIFI (WEP, WAP and WPA2)

First and foremost, TKIP makes four distinct enhancements to WEP (Table1). Firstly, it increases the Initial Vector (IV) size from 24 to 48 bits, meaning key reuse is no longer a worry. Secondly, it forces the sequence number to increase monotonically to avoid replay. Thirdly, it mixes the sequence number and transmits the address with the WEP base key to derive a per frame key. Finally, it includes a message authentication code (MIC) of the source and destination addresses, the priority, and the plaintext data, to allow forgeries to be detected.

WPA2 has less reduction on network throughput than WPA due to its encryption algorithm CCMP, which is highly improved compared to TKIP, which is adopted by WPA.

On the other hand, differences between these two security methods include; WPA2 is backward compatible with WPA. It uses a mixed mode that supports both WPA and WPA2 enabled devices on the same wireless network. Another difference is that; WPA uses TKIP encryption as a Security Protocol which in turn uses RC4 cipher, while as WPA2 uses CCMP-AES as a Security Protocol. WPA uses Michael algorithm for data integrity but WPA2 uses more robust, efficient and stronger algorithm, CBC-MAC.

	WEP	802.111 METHODS	
		WPA	WPA2
SECURITY PROTOCOLS	RC4	TKIP	CCMP
CIPHER	RC4	RC4	AES
KEY LENGTH	40 or 104 bits	128 bits encryption 64 bits authentication	128 bits
KEY LIFE	24 bits IV	48 bits IV	
KEY GENERATION	Concatenation	Two phases mixing function	Not needed
DATA INTEGRITY	CRC-32	Michael	CBC-MAC
HEADER INTEGRITY	None	Michael	CBC-MAC
REPLAY PROTECTION	None	Packet Number	
KEY MANAGEMENT	None	EAS-based	
AUTHENTICATION	Open or Shared Key	802.11x or Pre-Shared Key (PSK)	

Table 1. Comparison of WEP, WAP and WAP2

ISSN (ONLINE): 2250-0758, ISSN (PRINT): 2394-6962

IV. VULNERABILITIES AND DESCRIPTION OF ATTACKS

4.1 Vulnerabilities

4.1.1 Wpa & Wpa2 Vulnerabilities

WPA is used to strengthen security because of the weaknesses of WEP. One of the simplest ways is WPA PSK. In this case the use of WPA is similar with WEP, although using WPA can obtain higher security including stronger authentication and better encryption. WPA-PSK cannot be broken by intercepting many packets as WEP, but it is possible as long as 4-way handshake packets are obtained, we can know that SSID, Au_MAC, Sp_MAC, SNonce, ANonce, 802.1x data and MIC are included in 4-way handshake packets. And we also know the MIC is derived from the combination of the other six data and WPA-PSK key by using three hash algorithms (pdkdf2_SHA1, SHA1_PRF, HMAC_MD5). Through these theories, attacker can use dictionary attack to break WPA-PSK. First, a password dictionary is composited by possible passwords. And then using the password of the dictionary, SSID, Au_MAC, Sp_MAC, SNonce, ANonce and 802.1x data. attacker can compute a new MIC (**MIC'**) through pdkdf2_SHA1, SHA1_PRF and HMAC_MD5. Finally, if attacker find some MIC' equals with the original MIC, WPA-PSK is broken. A lot of system such as Kali Linux for example help to make this attack.

4.1.2 Impossible Tkip Countermeasures

We found a denial-of-service vulnerability in several Access Points (APs). Summarized, these APs accept TKIP MIC failure reports even when the network does not use TKIP. Someone with credentials to the network can abuse this to take make a network unusable, by sending two TKIP MIC failure reports every minute. Normally this should not be possible if the network is only configured to use CCMP. this results in a permanent denial-of-service attack (requiring a reboot the AP).

4.2 Descriptions Of Attacks

4.2.1 Key Reutilization Attack Krack

Inspired by the existing (Key Reutilization Attack) KRACK, the attacker's main use manner is as follows:

When the attacked client establishes a connection with a normal Au, the attack code (POCyystablishes a hotspot with the same BSSID and ESSID but different Channels. The Disassociate Frame is sent to force the attacked client to disassociate. At this time, the device experiences a reconnection. When the AP is ready to re-initiate a connection with the normal Access point, the Channel Switch Announcement (CSA) is injected. Beacon pairs switch the channel to the channel where the rogue Access Point resides and implement man-in-the-middle attacks; while the client state remains in State 2 (authentication state through the authentication of the access point), the next four handshakes begin. In **Message 3**, a key reinstallation attack is implemented to establish normal connection communication with the pseudo Access Point (Rogue Access Point)

These steps look as follows:

1. Establish a Rouge Access Point with the same ESSID, but different BSSID Channels;
2. Send an abnormal Deauth/Disassociate Frame to the client;
3. Resend message3 in the four-way handshake to force the reset of the nonce, the same IV;
4. Sequence Number and Timestamp disconcert, ;
5. The Client switches the Channel when establishing a handshake.

4.2.2 Downgrade Attack

As said before Some AP do not distinguish message2 and message4 and can be abused to downgrade attack the AP to TKIP. Hence M4 is essential in preventing downgrade attacks. This highlight

Notice that the beacons and probe responses only advertise support of WPA-TKIP, but the information element in message 3 of the 4-way handshake contains both WPA-TKIP and AES-CCMP. The client should have detected this mismatch, and aborted the handshake.

However, the client continues with the handshake, and is thereby downgraded into using WPA-TKIP. Hackers can abuse this flaw to trick the AP into using TKIP as follows:

First, he sets up a rogue AP that acts as a man-in-the-middle between the client and AP (see Figure3). He modifies all beacons and probe responses, so it appears that the network only supports TKIP. As a result, the client will connect to the AP and request TKIP as the pairwise cipher. At this point the adversary will forward message 1 and 2 of the 4-way handshake without modification.

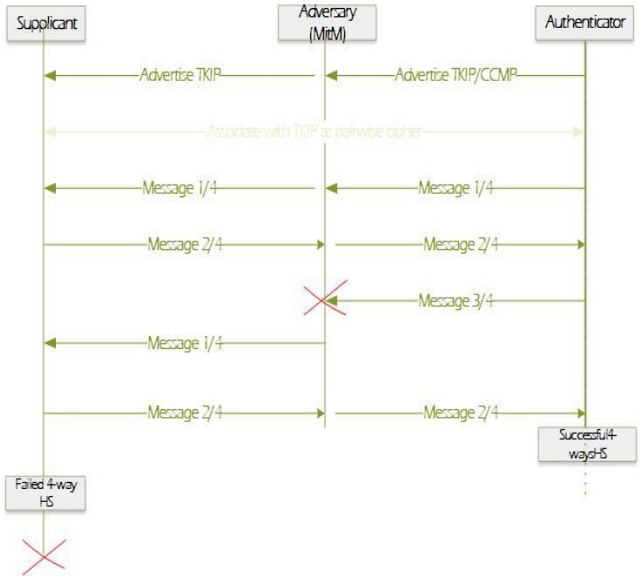

Figure 1. Visual demonstration of Message3 compromisation

However, it will block message 3, assuring that the supplicant never sees this message. Blocking this message is essential since it contains the real RSNE (supported cipher list) of the AP, which includes both TKIP and CCMP. This RSNE differs from the one that the Hacker advertised in beacon and probe requests.

The client would abort the handshake if this difference is detected.

The adversary now induces the client into retransmitting a valid message 2, by forging an unauthenticated message 1. When the client receives the forged message 1, it transmits a new message 2. The retransmitted message 2 is forwarded to the AP, which will be wrongly treated as being a (valid) message 4. The AP now thinks the 4-way handshake has been successful, and installs the session keys to enable transmission of normal (encrypted) traffic. In particular, it will transmit the first message of the group key handshake, and encrypt it using TKIP.it is important to note that the client will ignore this group key message, because it never received message 3 of the 4-way handshake. Nevertheless, it is problematic that the AP is using. TKIP.

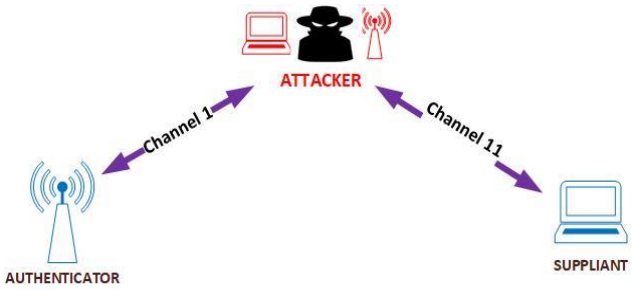

Figure 2. DoS Attach

4.2.3 Denial Of Service (DOS)

The He and Mitchell's work focuses on the 4-way handshake procedure give some guide to simulate the DoS attacks on the WLAN networks and shows the degradations when DoS or DoS flooding attacks are led to the SUPPLICANT.

DoS attacks are very easy to mount; furthermore, once an adversary successfully mounts a DoS attack, more advanced attacks, such asMitM , could be subsequently constructed. Therefore, it is necessary to deploy a security mechanism that can defend against DoS attack. The weak point of 4-way handshake is represented by the first message (M1). It is the only message that does not use the MIC field that is very important to guarantee the integrity, M1 can be falsified and a hacker can easily know all its fields such as the MAC address, ANonce, SN, and message type Through PTK, Sp calculates the MIC to be inserted in M2 and sends it to Au. After receiving the M2, Au calculates its PTK and then MIC. At this point, hacker (Hk) can play a role that prepares M1 to the message similar to that sent from Au to Sp (Figure5).

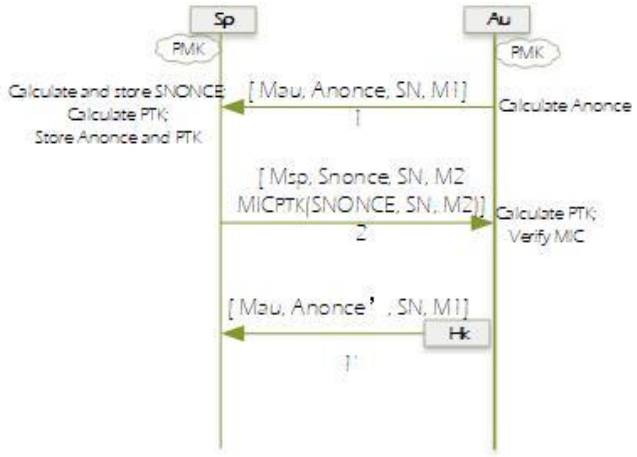

Figure 3. Hacker intrusion after Msg2 forwarding

This new M1_ message differs from M1 only in the nonce because this value is randomly generated locally in the device.

Sp calculates the PTK in the knowledge of ANonce received with Msg1. Let the value generated by Hk be indicated with ANonce so that it is possible to discriminate this from the value created by Au (ANonce). If His able to send its message (M1_) after Sp sends M2 and before Sp receives M3, Sp should accept M1 and it will calculate a novel value PTK that will be indicated by PTK. In other terms PTK will be a function of PMF, ANonce_, and SNonce:

PTK = PRF (PMF, ANonce, SNonce, MAu, MSp).

(2) The effect produced by the hacker is the storing of two new values (ANonce_ and PTK_) and the sending of a new message (M2) from Sp to Au. This new message will be silently discarded by Au in accordance with the protocol specification. In this time Au will send the message M3 to Sp with its own ANonce value. After receiving the M3, Sp will notify a failure in the integrity check because MICPTK = MICPTK. This is due to the PTK, derived by ANonce_, which produces a different MIC at Sp. Thus, a discarding of M3 is produced without giving any communication to Ap. and the authenticity of Ap). After timestamp expiration, the authenticator Au, because it does not receive the M4, will send M3 again. This novel M3 will again be discarded by Sp. After the nth attempt at transmission and timestamp expiration, Au will deauthenticate Sp and the hacker will achieve his task: to make a DoS attack.

After each reception of M1, supplicant Sp stores ANonce and PTK values in its own station if the hacker achieves a multiple attack, it is possible to achieve a DoS flooding or DoS memory exhaustion attack (such as shown in Figure 6); if the attack is repeated through flooding by the hacker, Sp is forced to store a lot of ANonce and PTK values producing

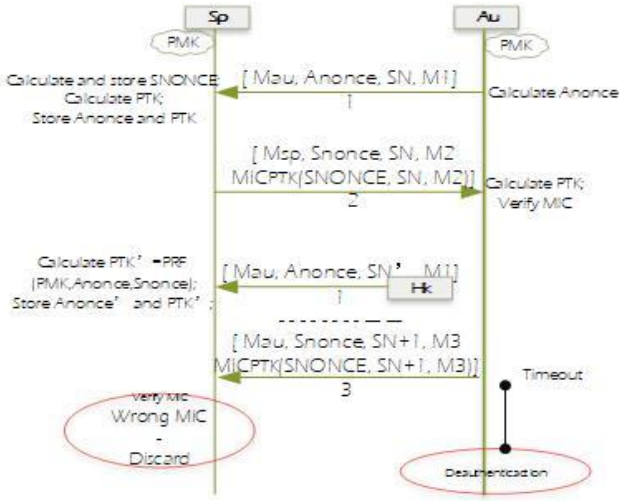

Figure 4. DoS attack in 4-way handshake phase

memory exhaustion. This attack is possible with both WPA and 802.11i protocols

One of the main issues in the 4-way handshake is the incapability to discriminate the new M1 request coming from the real node and the messages generated by Hk.

The second issue to be overcome is the memory exhaustion. In fact, even if the hacker's messages are discriminated, Hk could still produce a DoS flooding attack. A solution to this second issue can be the avoidance of storing ANonce and PTK for each M1 offering the correct working of the 4-way handshake

V. RELATED WORK AND SUGGESTED OF SOLUTIONS

5.1 Related Work

The research "A Whole-Process WiFi Security Perception Software System" Heqing Huang , Y anjun Hu, Y an Ja, Shiliang explains a design for the users during surfing the Internet through the Wi-Fi . The Whole-Process Wi-Fi Security Perception System which is based on the analysis of client's wireless access points focusing on the details of possible threats during the pre-connection, connection and after-connection [12]. It consists of three modules using different methods for dealing and protecting three periods of time ,Their software friendly warns the user and provide the attacker's distance, to give user a positive position to solve the security problem.

Dr. Sebastian Nixon-1, Yibrah Haile2 School of Informatics, Wolaita Sodo University, Ethiopia, Africa : " Analyzing Vulnerabilities on WLAN Security Protocols and Enhance its Security by using Pseudo Random MAC Address."

They used Kali Linus to conduct some penetration tests on WLAN security protocols and MAC Filtering, and consequently proposed a security Algorithm to enhance the security of MAC Filtering mechanism. That solution to secure the WLAN uses Pseudo Random MAC Address Generation Algorithm Called PRMACGA. It enhances the security of MAC Filtering Mechanism. In fact in MAC Filtering, the attackers can change their MAC to replicate the authorized Clients's MAC and as a result the attacker can access the network.[13]. But as per proposed solution, the attacker never gets the Original MAC address of the authorized Clients. Because the proposed That algorithm provides Pseudo MACs for the authorized Clients. Even if the attackers get the pseudo MAC of the authorized client's the attacker can't access the WLAN. The algorithm disables the given pseudo MAC once the authorized clients disconnected from the net and as result attacker can't access the WLAN.

Seoksoeng Jeon, Chansu Yu and Young-Joo Suh "Pre-shared Key Agreement for Secure Public Wi-Fi. "2017

They present a novel pre-shared key (PSK) agreement scheme to establish a secure connection between a Wi-Fi client and Access Point. They proposed a scheme Secure Open AP (SOAP) that adopts two public key algorithms, the elliptic curve Diffie-Hellman key exchange algorithm (ECDH) and digital signature algorithm (ECDSA) to establish a secure connection between a client and an AP without having prior knowledge of a password. They aim for a user to be able to conveniently connect to an AP in a WPA-PSK mode without having to enter a password. SOAP uses two public key algorithms, ECDH and ECDSA, prior to the 4-Way Handshake to agree on a PSK on both sides so that the handshake can use it for the 4-Way Handshake.

5.2 Suggested Solutons

Firstly, we build a model of the Wi-Fi handshake in Python that describes the expected behavior of an implementation. We then automatically generate invalid executions of the handshake, and check whether an implementation correctly reacts to these invalid executions.

We consider a proposed solution published in [**14, 15] .** Then, a second solution, suggested but not tested by He and Mitchell, is also considered, and a third novel solution that tries to release memory at the client device is also investigated. Because these solutions are prefixed at the terminal, they are called *static*. These extensions to the standard protocols need just a few operations on the client side without introducing additional fields in the WPA and IEEE 802.11i protocol frame format.

5.2.1 Solutions

5.2.1.1 First Solution

The proposal is easily presented in the following manner:

(i) On reception of the first message M1, Sp takes 3 actions:

(a) Generates and stores SNonce;

(b) Computes PTK in the same way provided by the standard protocol;

(c) Creates and sends M2 (*no stores ANonce and PTK*);

(ii) On each reception of a new M1, Sp only calculates without storing the novel PTK (PTK_); through this new PTK_ it can produce the MIC value;

(iii) On reception of M3, in order to verify the MIC, S computes the PTK again through the SNonce value that has previously memorised and the ANonce value obtained by M3; in this way the identification process gives a positive response and the attack attempted is avoided.

The replication of M3 by His not applicable because in this message the MIC field that assures the identity is present. Also, memory exhaustion is avoided because it is sufficient to store only SNonce rather than ANonce and PTK values after any reception of M1. With the proposed application we obtain positive results also in the packet loss scenario.

In fact, in the case of M2 loss, after timeout, Au sends a new M1 to Sp. This Message, called M1_, contains a new ANonce value (ANonce_) which is now legitimate and so, at the reception of M3, it will give positive response.

5.2.1.2 Second Solution with trade-off variant

The steps to be followed are presented below.

(i) On reception of the first M1, Sp has to perform the following actions:

(a) Generate and store SNonce;

(b) Calculate PTK;

(c) Create and send M2;

(d) Store ANonce and PTK.

(ii) On reception of each new message M1, Sp calculates PTK_ in accordance with the standard proposal.

(iii) After the reception of M3, S compares the ANonce value in M3 with the stored ANonce. If the two ANonce values (ANonce and ANonce M3) are the same, Sp will verify the MIC of M3 using the stored PTK. Otherwise if the two ANonce values are different, the PTK will be recomputed and after that the MIC will be verified. In this way the variant avoids storing ANonce and PTK (***memory exhaustion***) each time and recomputing PTK after each M3 arrival ***(CPU exhaustion***).

Through benefits and drawback analysis of three mechanisms for IEEE 802.11i protocol, it is possible to have a solution tries to unify the benefits of the single mechanisms.

For example, the supplicant could be equipped with an intelligent software module that monitors system parameters (or network parameters) and on their basis, it decides to adopt either mechanism I, or II. If the supplicant wants to control the CPU and memory load levels, threshold levels could be introduced and if the device overcomes these levels the system can switch among different solutions. Considering the unpredictability of an attacker, both situations of DoS attack and no-hacking are considered.

5.2.2 Mitigation Of Weaknesses

- The WPA-TKIP countermeasures disallow any clients from connecting to the AP using WPA-TKIP for one minute. This is to mitigate weaknesses in WPA-TKIP.
- An adversary must possess credentials to connect with the network.

Nevertheless, sometimes a client has the necessary credentials to connect to the network, without being a trusted device. Examples are public networks such as Edu roam, a hotel network, a conference network, etc.

5.2.3 Intrusion detection

1- Establish a test network WIFI. After the enterprise, University or Public user connects to the WLAN and passes the authentication, s/he can access the intranet resources. Through the WIPS (Wireless Intrusion Prevention System), administrator can intuitively understand the device attributes and security attributes of the WLAN, including ESSID, BSSID, Access Point vendor, and channel, encryption and so on.

WIPS products can be used to view and manage trusted WIFI and unknown hotspots in the enterprise or public place, identify and alert suspicious attack behaviors, and quickly respond to WiFi attacks and threat events. It can effectively prevent many security risks such as **malicious hotspots, unknown and external WLAN, fake hotspots, and unauthorized terminals**, thereby protecting the wireless network.

2- The hacker can then forged a WLAN with the same name and configuration as the test network and attempted to deceive the user. At this point, there were two WLAN in the wireless network environment. Non-professionals simply couldn't identify which one was a self-built WIFI, which was illegal.

It can be seen that the illegal WLAN has already been identified and blocked by the WIPS. The current number of connected terminals is “none”.

3- At the same time, WIPS also notified administrators of the occurrence and processing of counterfeit legitimate WIFI attacks. WIPS's timely response allows administrators to fight for more time to deal with emergencies.

4-. At this point, the WIPS system can find such attacks. While providing the processing suggestions, it can also locate the specific location where the attacks occur. The administrator can check whether there are any suspicious persons on the spot.

5- It can be said that the whereabouts of hackers' attacks have been completely exposed under the WIPS, and

wireless threats that cannot be touched cannot be seen. The mapping through WIPS gradually becomes clear. The hackers who do not know what happened continued their attack. The hackers forcibly reset the nonce by collecting and replaying Message3 in the four-way handshake, thereby successfully attacking the encryption protocol, decrypting the client sent communication packets, and intercepting sensitive information. However, the WIPS system has already detected the attack and blocked the implementation, thus protecting the unsuspecting "user" from threats.

5.2.4 Rogue mitigation

As said before a rogue access point can be established by an attacker to lure the user and perform various attacks on the devices of a user through WLAN. Rogue Access Point is considered to be a serious threat in context to WLAN Detection of Rogue Access Point and is a challenging task. The existing techniques were suitable for Man-In-The-Middle attack, Denial of Service attack and some malicious attacks but these current techniques will not fit into every scenario.

The proposition of a novel approach includes the Mac address, SSID and signal strength of access point in order to decide whether the access point is rogue or not.

In this technique initially, we need to filter unauthorized access points and this is done by a filtering component. At this stage MAC addresses of all the visible access point is matched against the list, which contains the list of MAC address of all the authorized access points. If there exists an access point whose MAC address doesn't match then that access point is considered to be rogue and is dropped. There can be a case where the MAC address is spoofed in order to get the MAC address of authorized access point, then the packet is passed to the anomaly detection sensors where different tools like Ettercap [16], Wireshark [17], Snort [18] and Anomaly detection heuristic payload sifting [19] are used in order to filter the unauthorized access point and detect different attacks. These attacks that can be detected are ARP spoofing, Man-in-the- middle attack, Denial-of-service (DOS) attack, Distributed denial of service (DDOS) attack and attacks like smurf . After the detection of attacks the packets are progressed to the shadow honeypot for validation. On the basis of the result obtained from anomaly detection and shadow honeypot a false negative and false positive rate is provided which in turn is passed back to filtering and detection stage for future detection of rogue access point [20].

VI. DISCUSSION AND FUTURE WORK

A lot of research is going on the way to make WLAN more secure through the four-way handshake. In the coming days WPA3 will be introducing to add more security and definitely fix this flaws and vulnerability in the preview protocol WPA2.

Four major new security features need to be considered:

1. A More Secure Handshake
2. Replacement of Wi-Fi Protected Setup (WPS)
3. Unauthenticated Encryption
4. Increased Session Key Sizes

VII. CONCLUSION

The WLAN is a multi-tenant environment, where resources are shared. Threats can happen from anywhere; inside the shared environment or from outside of it. However, sending or receiving sensitive data in the WLAN is apparently risky, whether accidental or due to a malicious hacker attack, data privacy, loss or leakage and unavailable for access would be a major security violation involving confidentiality, integrity and availability. The best strategy is to practice all security measures such as access control, encryption, auditing and redundancy to ensure that data are protected from every angle and gaining overall security.

REFERENCES

[1] Dr. Sebastian Nixon & Yibrah Haile. (2017). Analyzing vulnerabilities on WLAN security protocols and enhance its security by using pseudo random MAC address. *International Journal of Emerging Trends & Technology in Computer Science*, *6*(3), 293-300.

[2] Laurent Butti & Julien Tinnes. (2008). Discovering and exploiting 802.11 wireless driver vulnerabilities. *Journal in Computer Virology*, *4*(1), 25–37.

[3] A. Alabdulatif, X. Ma & L. Nolle. (2013). A framework for proving the correctness of cryptographic protocol properties by linear temporal logic. *International Journal of Digital Society (IJDS)*, *4*(1-2), 749–757.

[4] M. Vanhoef, D. Schepers, & F. Piessens. (2017). Discovering logical vulnerabilities in the wi-fi handshake using model-based testing. *In ACM Symposium on Information, Computer and Communications Security*, 360-371.

[5] Nikita Borisov, Ian Goldberg, & David Wagner. (2001). Intercepting mobile communications: The insecurity of 802.11. *Proceedings of the 7th annual international conference on Mobile computing and networking. ACM*, 180-189.

[6] L. Dong, K. F. Chen, & X. J. Lai. (2009). Formal analysis of authentication in 802.11 I. *Journal of Shanghai Jiaotong University (Science)*, *1*, 023.

[7] Michael R. Bartolacci, Larry J. LeBlanc, & Ashley Podhradsky. (2014). Personal denial of service (PDOS) attacks: A discussion and exploration of a new category of cyber crime. *Journal of Digital Forensics, Security and Law*, *9*(1), 19–36.

[8] E. Tews & M. Beck. (2009). Practical attacks against WEP and WPA. *In Proceedings of the second ACM conference on Wireless network security, WiSec*, 79-86.
[9] A. Wool. (2004). A note on the fragility of the Michael message integrity code. *IEEE Transactions on Wireless Communications, 3*(5), 1459-1462.
[10] A. Stubblefield, J. Ioannidis, & A. Rubin. (2004). A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP). *ACM Transactions Information System Security, 7*(2), 319–332.
[11] V.Moen, H. Raddum, & K. J. Hole. (2004). Weaknesses in the temporal key hash of WPA. *ACMSIG Mobile Computing and Communications Review, 8*(2), 76–83.
[12] S. Fluhrer, I. Mantin, & A. Shamir. (2001). Weaknesses in the key scheduling algorithm of RC4. *International Proceeding 8th Workshop Selected Areas in Cryptography*, 1–24.
[13] C. He & J. C.Mitchell. (2004). Analysis of the 802.111 4-way handshake. *In Proceedings of the ACM Workshop on Wireless Security*, 43–50.
[14] S. Singh, C. Estan, G. Varghese, & S. Savage. (2004). Automated worm fingerprinting. *In Proceedings of the 6th Symposium on Operating Systems Design and Implementation*, 45-60.
[15] J. Levine, R. LaBella, H. Owen, D. Contis, & B. Culve. (2003). The use of honeynet to detect exploited systems across large enterprise networks. *In Proceedings IEEE Workshop on Information Assurance, West Point, NY: United States Military Academy*. Available at: https://www.researchgate.net/publication/4035063_The_use_of_Honeynets_to_detect_exploited_systems_across_large_enterprise_networks
[16] E. Spafford. (1989). The internet worm: Crisis and aftermath. *Communications of the ACM, 32*(6), 678–687.
[17] S. Gaitan, L. Calderoni, P. Palmieri, M.-C. Ten Veldhuis, D. Maio, & M. van Riemsdijk. (2014). From sensing to action: Quick and reliable access to information in cities vulnerable to heavy rain. *Sensors Journal, IEEE, 14*(12), 4175–4184.
[18] D. S. Tonesi, L. Salgarelli, & A. Tortelli. (2010). Securing the signaling plane in beyond 3G networks: analysis of performance overheads. *Security and Communication Networks, 3*(2-3), 217–232.