Enhancing WPA2-PSK four-way handshaking after re-authentication to deal with de-authentication followed by brute-force attack

A novel re-authentication protocol

Mohamed Chahine GHANEM
Cyber Security Research Group
School of Computing
London Metropolitan University
London, UK
mcghanem@hotmail.com

Deepthi N. RATNAYAKE
Cyber Security Research Group
School of Computing
London Metropolitan University
London, UK
d.ratnayake@londonmet.ac.uk

***Abstract*— The nature of wireless network transmission and the emerging attacks are continuously creating or exploiting more vulnerabilities. Despite the fact that the security mechanisms and protocols are constantly upgraded and enhanced, the Small Office/Home Office (SOHO) environments that cannot afford a separate authentication system, and generally adopt the IEEE 802.11 Wi-Fi-Protected-Access-2/Pre-Shared-Key (WPA2-PSK) are still exposed to some attack categories such as de-authentication attacks that aim to push wireless client to re-authenticate to the Access Point (AP) and try to capture the keys exchanged during the handshake to compromise the network security. This kind of attack is impossible to detect or prevent in spite of having an Intrusion Detection and Prevention System (IDPS) installed on the client or on the AP, especially when the attack is not repetitive and is targeting only one client. This paper proposes a novel method which can mitigate and eliminate the risk of exposing the PSK to be captured during the re-authentication process by introducing a novel re-authentication protocol relying on an enhanced four-way handshake which does not require any hardware upgrade or heavy-weight cryptography affecting the network flexibility and performances.**

Keywords—WLAN, De-Authentication, IDPS, WPA2-PSK, brute-force, DoS attack, IEEE 802.11, Four-way Handshake.

I. INTRODUCTION

The widespread and rapid increase of wireless technologies, and introduction of Bring Your Own Device (BYOD) policy creates opportunities for many small organisations to perform work using employees' laptops, smartphones, tablets and other mobile devices, however, new threats and attacks also emerged aiming to compromise the Confidentiality, the Integrity and/or the Availability of these organizations[1,2]. Therefore, securing the wireless infrastructure becomes a crucial step to achieve the overall network security [3]. Broadcasting nature of wireless signal and different protocol vulnerabilities are the major security flaws of Wireless Local Area Networks (WLAN) and some remain threatened [4]. Whilst securing the networks, security administrators also have to balance the cost and usability. The widely used cost effective technology to secure small WLAN is Wi-Fi-Protected-Access-2/Pre-Shared-Key (WPA2/PSK). WPA2-PSK mode is usually adopted by Small Office/Home Office (SOHO) environments as it does not require a costly investment on a dedicated authentication system. Nevertheless, despite the fact that this mode was improved consistently, it still presents several vulnerabilities such as management frame spoofing and brute force attacks [5] which could lead to forced de-authentication and re-authentication where an adversary could acquire PSK, capturing and cracking the four-way handshake protocol and therefore regaining illegitimate access to the Access Point (AP) [6].

An attacker in the range of the wireless network could use a combination of software and hardware solutions to firstly, sniff frames passively, secondly, forge (spoof) its own de-authentication management frames and finally inject them into the network by either targeting a specific client using the client's Media Access Control (MAC) address or the whole WLAN Basic Service Set Identifier (BSSID) in order to push one or more connected clients out of the network and force it to authenticate itself again [6,7]. During the re-authentication stage the attacker will attempt to capture the Hashed Message Authentication Code (HMAC) of the PSK [8]. Then, by comparing the captured HMAC to a reference dictionary along with the use of other advanced cryptographic reversing processes, the attacker will try to identify the used PSK and therefore compromise the WAP2-PSK encryption keys to gain a full access into WLAN [7]. The de-authentication attack illustrates the WPA2-PSK handshake vulnerabilities because it is impossible to detect when using conventional network security solutions such as firewalls and IDPSs [6]. As this attack injects very few forged de-authentication frames it is hard to distinguish it from the legitimate traffic and also will not alert the IDPS as a Denial-of-Service (DoS) attack [9]. Another issue related to the de-authentication attack is that it could be launched using minimum resources, but its impact on the network security, especially the Integrity (forging the fake frames), Availability (due to DoS attacks) and the

Confidentiality (when the PSK is captured) is enormous [10,11,12].

This research seeks a solution to prevent acquiring PSK using forced re-authentication by introducing a novel re-authentication protocol using an enhanced four-way handshake. The rest of the paper is organised as follows: Section II reviews the related current work to prevent de-authentication attacks; Section III defines the existing de-authentication methodology; Section IV discusses the WLAN organisation and methods of testing the defence limits; Section V discusses proposed re-authentication protocol, its strengths and weaknesses against existing solutions; Section VI concludes the paper.

II. REVIEW OF EXISITNG DE-AUTHENTICATION ATTACK PREVENTION METHODS

IEEE 802.11 [1] is a set of standards for wireless networks that was initially released in 1997, and revised several times. New versions published in 1999, 2007, and 2012. Security algorithm Wired Equivalent Privacy (WEP) is introduced with the original standard, Wi-Fi Protected Access (WPA) and WPA2 were introduced using IEEE 802.11i, algorithms for protected management frames were introduced in 802.11w amendment [1]. The next version is expected in 2016, however there are no security enhancements forthcoming [1,13,14]. There are three types of IEEE 802.11 frames: management frames which enable clients to establish and maintain communications, control frames which assist in the delivery of data frames and data frames which carry data [1, 13, 14]. IEEE 802.11w made separate authentication of the de-authentication and dis-association management frames, mandatory. The authentication prevents spoofing thereby preventing the de-authentication attack. However, due to heavyweight integrity checks proposed in 802.11w, the performance of the network decreases. Also switching to IEEE 802.11w requires firmware upgrades on both client and AP [10,15].

Many academic researchers tackled the WPA2-PSK vulnerability against de-authentication attack.

Cryptographic methods: The common cryptographic solution is authenticating management frames to prevent spoofing. [16] proposed the use of an additional secret shared key between the client and the AP which will be used for authenticating the de-authentication frame. This approach appears efficient in preventing de-authentication attack but hardware and firmware upgrades are required on both client and the AP [7].

Sequence Number based methods: [8] suggested different schemes for detection of spoofing attacks based on the sequence number analysis. Sequence number is a MAC frame field. It starts from zero and increases the number every time it sends out a non-fragmented frame and wraps at 4095. The technique is based on the assumption that sending a frame with correct sequence number at the precise timing is often difficult if the number of frames to be sent are high. However, this approach was proved to be ineffective due to frame losses/delays and quality of service re-ordering [9].

Delaying the effect of Management frames: Another method is to prevent de-authentication attack by shortly postponing the effect of all management frames. If a de-authentication frame is received from a client and subsequently a data frame is received from the same client, then the previous de-authentication frame(s) is not considered, as, a legitimate client that sends a de-authentication frame never sends a data frame directly to the AP before re-establishing a 4-way handshake with the AP [8]. Therefore, if this sequence is observed, then it is likely that the previous de-authentication frame(s) received is spoofed. Nevertheless, delaying the effect of all management frames may create connection problems for roaming clients and may cause hand-off issues [9].

Statistical and Machine learning methods: [5] proposed a method to detect the de-authentication attack by setting a threshold on the number of de-authentication frame(s) received by a client. If for a client, more than threshold number of de-authentication frame(s) are observed, an alarm is raised indicating the occurrence of de-authentication attack. However, this threshold is static and is set by the administrator making the technique prone to misjudgement. The Machine learning method is also limited as it allows several intrusions before becoming effective [7,17,18].

It has been observed that the acceptance of the above discussed solutions have been mainly affected due to the following reasons: changes to IEEE 802.11 protocol stack; deployable on legacy as well as new networks; additional hardware/software cost; dependency on the client's operating/application systems, patching of client software; lightweightness of the cryptographic-based scheme [19].

III. EXISTING WPA2-PSK AUTHENTICATION PROTOCOL

This section briefly describes the different phases of WPA2-PSK protocol.

A. *Authentication and Association phase*

WPA2-PSK security relies mainly on the Pre-shared key (PSK) which is entered manually on both wireless client and AP as a pass-phrase (secret information) of 8 to 63 American Standard Code for Information Interchange (ASCII) characters. An IEEE 802.11 wireless client has to authenticate and associate to the AP using the pass-phrase already pre-shared between both the AP and the clients. The Figure 1 illustrates the process of authentication and association [1].

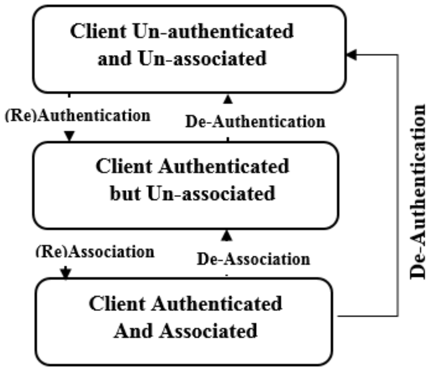

Client Un-authenticated and Un-associated
(Re)Authentication
De-Authentication
Client Authenticated but Un-associated
(Re)Association
De-Association
Client Authenticated And Associated
De-Authentication

Figure 1: Authentication and association process.

B. Key Generation

The key generation procedure is an integrated part of the WPA2-PSK four-way handshaking. It takes place before the four-way handshaking starts and continues during its progression. This procedure starts when the wireless client passes the authentication and the association phases. Both these phases do not require any security, but share information about capabilities between wireless clients and the AP. Key Generation process and derivation procedure stated in [1] are summarised as below (Figure **2**):

i. The pass-phrase used in authentication and association phase, will also be used as a seed in the derivation process of the required seven keys, which will be generated to be used for different purposes involved in the protection of WPA2-PSK networks.

ii. Password-Based Key Derivation Function 2 (PBKDF2) is used to generate the Pair Master Key (PMK) from PSK, Service Set Identifier (SSID) and SSID length which will be hashed 4096 times to produce a 256-bit PMK.

iii. PMK, the "Pairwise key expansion", AP's MAC address and the wireless client's MAC address, randomly generated numbers on both AP side (ANonce) and client side (SNonce) will be fed to a Pseudo-Random Function (PRF) to produce Pairwise Temporary Key (PTK). The length of the PTK in the WPA2-PSK (AES/CCMP) is 384 bits.

iv. PTK will be split into three 128 bit keys: Key Confirmation Key (KCK), Key Encryption Key (KEK) and Temporal Key (TK). KCK guarantees data integrity in the four-way handshaking communication, KEK protects the four-way handshake correspondence and TK protects wireless data.

v. AP will generate a Group Temporal Key (GTK) and transmit it to all wireless clients to be used in broadcasting data over the WLAN.

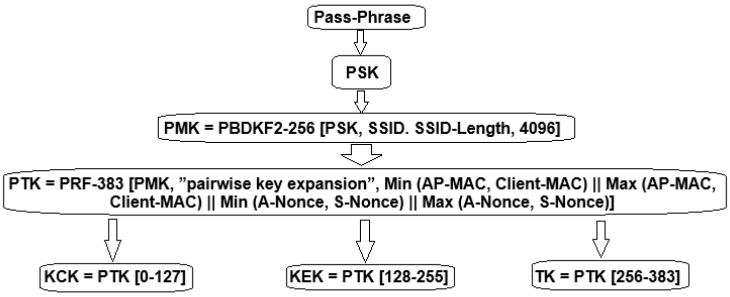

Pass-Phrase
PSK
PMK = PBDKF2-256 [PSK, SSID. SSID-Length, 4096]
PTK = PRF-383 [PMK, "pairwise key expansion", Min (AP-MAC, Client-MAC) || Max (AP-MAC, Client-MAC) || Min (A-Nonce, S-Nonce) || Max (A-Nonce, S-Nonce)]
KCK = PTK [0-127]
KEK = PTK [128-255]
TK = PTK [256-383]

Figure 2: The key generation process.

C. Four-Way Handshake

Both AP and the wireless client rely on the four-way handshake communication to confirm the possession of PSK. The four-way handshake procedure starts just after the wireless client is authenticated and associated to the AP. The four-way handshake [1] consists of four messages (Figure **3**) in which Extensible Authentication Protocol over LAN (EAPoL) is used to secure their transmission between Client and AP as follows:

i. First, the AP sends Message 1 which contains a locally generated ANonce (32 digits random number) upon EAPoL. When the wireless client receives Message 1, it will possess all of the required parameters to derive PTK from PSK and therefore, generates KCK, KEK and TK.

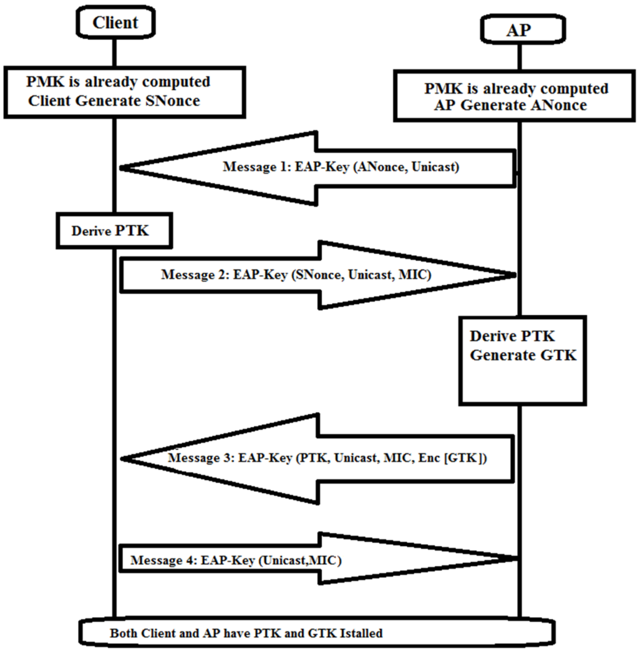

Client
AP
PMK is already computed
Client Generate SNonce
PMK is already computed
AP Generate ANonce
Message 1: EAP-Key (ANonce, Unicast)
Derive PTK
Message 2: EAP-Key (SNonce, Unicast, MIC)
Derive PTK
Generate GTK
Message 3: EAP-Key (PTK, Unicast, MIC, Enc [GTK])
Message 4: EAP-Key (Unicast,MIC)
Both Client and AP have PTK and GTK Istalled

Figure 3: The four-way handshake protocol.

ii. The wireless client will then reply by Message 2 which contains the SNonce (32 digits random number) and the Message Integrity Code (MIC). The MIC is used to guarantee the integrity of Message 2 and is calculated for the entire EAPoL and KCK data. When the AP receives Message 2, it will extract SNonce and derives KCK, KEK and TPK. Additionally, the AP will check the integrity of the received information by calculating Message 2 MIC and comparing it with the MIC received from the client.

iii. Message 3 is generated on the AP and transmitted to the client. It contains the GTK, encrypted using KEK and the associated MIC.

iv. Finally, Message 4 is generated by the client and transmitted to the AP to confirm the successful end of the four-way handshaking.

IV. The defence Limits against De-Authentication attack

A. The De-athentication Attack

The active de-authentication attack is easy to perform and difficult to stop or detect [5,7]. To illustrate the vulnerability of the existing WPA2-PSK authentication protocol, the research performs a de-authentication attack, captures the data of the four-way handshake during the client re-authentication and uses it to crack the PSK key. The testing de-authentication attacks could be launched either against the AP or a specific wireless client. When a client authenticates itself to the AP, the same authentication protocol (WPA2-PSK) is used to exchange security keys and confirm that the client possess the key. To de-authenticate from the AP, the client sends a de-authentication management frame, which leads to

AP disassociating and de-authenticating the client. The client must authenticate itself again to re-gain access to the AP. The de-authentication is different from the authentication process as it requires no handshaking and thus no security [10,17].

B. WLAN organization

To test the IDPS and firewall configuration against the de-authentication attack, the following equipment and software were used (Figure 4):

i. AP: TL-WR841N wireless router armed with an integrated DD-WRT open source firewall.

ii. Client: Dell Inspiron 11 laptop running Windows 7 Operating System. The client is also secured with a COMODO firewall Internet Security Premium 2016 and SNORT Host-based Intrusion Prevention System (IDPS).

iii. Attacker: Dell Latitude E6330 laptop running Debian Linux Operating System armed with a high gain Wireless Universal Serial Bus (USB) Adaptor and Kali Linux penetration testing platform. TL-WN722N Adaptor can be set to monitor mode and compatible with Aircrack-ng (allows frame injection) running on Kali Linux system [20].

AIRCRACK-NG is a suite of tools that can be used to crack IEEE 802.11 WEP/WPA-PSK keys. Once sufficient data packets have been captured, Aireplay-ng module can be used to inject and replay wireless frames, Airbase-ng can be used to attack the client and Packetforge-ng can be used to forge and spoof management frames used for frame injection. A network interface card in monitor mode can capture packets in the air without having to associate with the AP [21]. However, it will not send any traffic. On the other hand, Promiscuous mode allows to capture all wireless packets on a network that has been associated, whilst sending packets as well. Further, although the IEEE 802.11 adapter at the radio level can receive packets on other SSIDs, it does not forward them to the host [5,7,22].

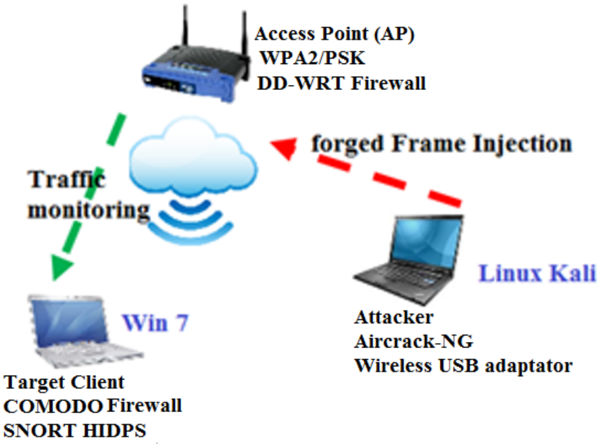
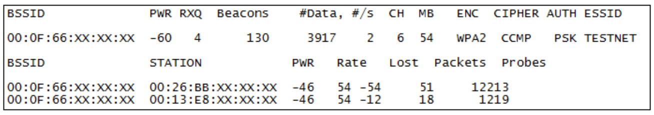


Figure 4: The simulation platform

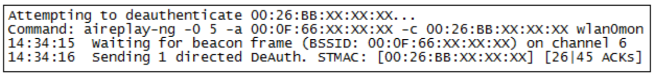
C. Test and results

After setting the wireless USB adaptor into monitoring mode, the attacker launched the Aircrack-ng to capture management frames (Figure 5). Then attacker created a spoofed de-authentication frame and injected it into the network in order to disconnect the targeted client. This forced the client to authenticate again (Figure 6). The attacker used Aircrack-ng to monitor and capture the client re-authentication process. The captured PSK HMAC is used to identify the corresponding PSK from the reference dictionary (Figure 7) enabling the attacker to gain full access to the network (Figure 8). The de-authentication attack was carried out successfully against the client running Windows 7 without being detected by neither the firewalls (client and AP) which were configured to block all suspicious traffic, nor by the client's SNORT IDPS configured to alert on traffic with all known attack signatures (Figure 9).



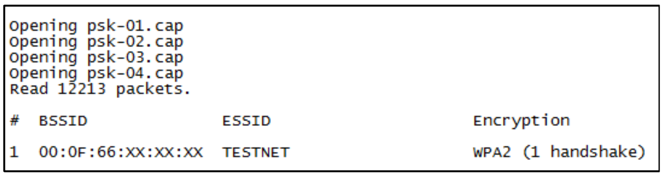
```
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:0F:66:XX:XX:XX  -60   4      130     3917    2   6  54   WPA2  CCMP   PSK TESTNET

BSSID              STATION            PWR   Rate   Lost  Packets  Probes

00:0F:66:XX:XX:XX  00:26:BB:XX:XX:XX  -46   54 -54     51    12213
00:0F:66:XX:XX:XX  00:13:E8:XX:XX:XX  -46   54 -12     18     1219
```

Figure 5: Monitoring of the AP.



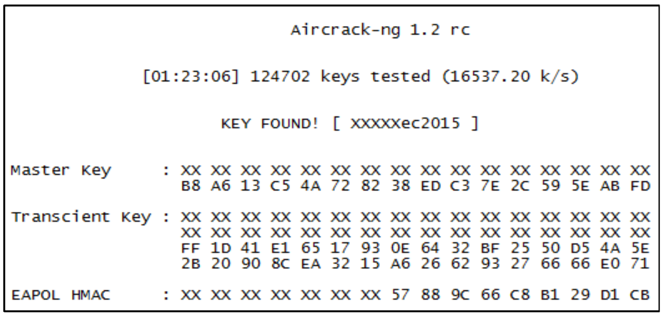
```
Attempting to deauthenticate 00:26:BB:XX:XX:XX...
Command: aireplay-ng -0 5 -a 00:0F:66:XX:XX:XX -c 00:26:BB:XX:XX:XX wlan0mon
14:34:15  Waiting for beacon frame (BSSID: 00:0F:66:XX:XX:XX) on channel 6
14:34:16  Sending 1 directed DeAuth. STMAC: [00:26:BB:XX:XX:XX] [26|45 ACKs]
```

Figure 6: De-authentication frame targeting the client.



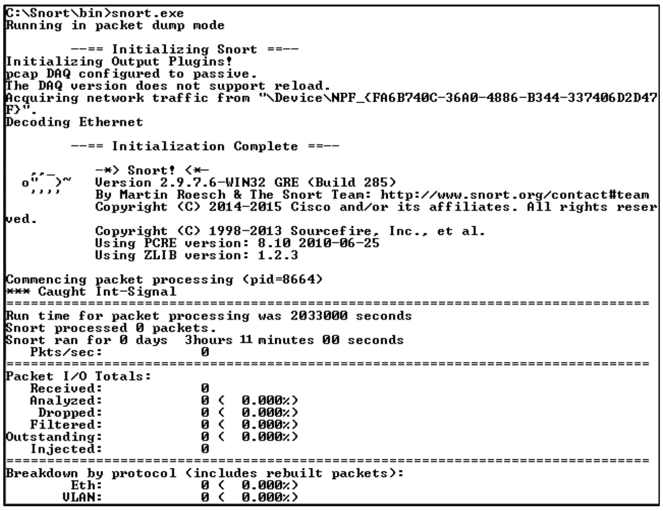
```
Opening psk-01.cap
Opening psk-02.cap
Opening psk-03.cap
Opening psk-04.cap
Read 12213 packets.

#  BSSID              ESSID                  Encryption

1  00:0F:66:XX:XX:XX  TESTNET                WPA2 (1 handshake)
```

Figure 7: Capturing the handshake after re-authentication.



```
                          Aircrack-ng 1.2 rc

          [01:23:06] 124702 keys tested (16537.20 k/s)

                      KEY FOUND! [ XXXXXec2015 ]

Master Key     : XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
                 B8 A6 13 C5 4A 72 82 38 ED C3 7E 2C 59 5E AB FD

Transcient Key : XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
                 XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
                 FF 1D 41 E1 65 17 93 0E 64 32 BF 25 50 D5 4A 5E
                 2B 20 90 8C EA 32 15 A6 26 62 93 27 66 66 E0 71

EAPOL HMAC     : XX XX XX XX XX XX XX 57 88 9C 66 C8 B1 29 D1 CB
```

Figure 8: Brute forcing the HMAC and retrieving the Key.



```
C:\Snort\bin>snort.exe
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{FA6B740C-36A0-4886-B344-337406D2D47
F}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.7.6-WIN32 GRE (Build 285)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2015 Cisco and/or its affiliates. All rights reser
ved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3

Commencing packet processing (pid=8664)
*** Caught Int-Signal
===============================================================================
Run time for packet processing was 2033000 seconds
Snort processed 0 packets.
Snort ran for 0 days  3hours 11 minutes 00 seconds
   Pkts/sec:            0
===============================================================================
Packet I/O Totals:
   Received:            0
   Analyzed:            0 (  0.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:            0 (  0.000%)
       VLAN:            0 (  0.000%)
```

Figure 9: SNORT IDPS monitoring result.

D. Discussion

The reason why the firewalls did not detect the attack is because the frame injected is legitimate and therefore it does not differ from normal traffic signatures [22, 23]. Also, Snort IDPS installed on the client can only use the wireless interface on promiscuous mode when it is in normal operation. Therefore it was able to detect the traffic transiting on the interface but was unable to process raw IEEE 802.11 frames and decode them in order to inspect them. Therefore, no action was launched against the de-authentication attack. The re-authentication traffic is considered as normal in this work, therefore will not be detected by the IDPS. The next section presents a novel protocol which relies on the IEEE 802.11 existing protocol by introducing the new re-authentication approach [24].

V. THE PROPOSED RE-AUTHENTICATION PROTOCOL

The novel re-authentication protocol (Figure 10) works as follows:

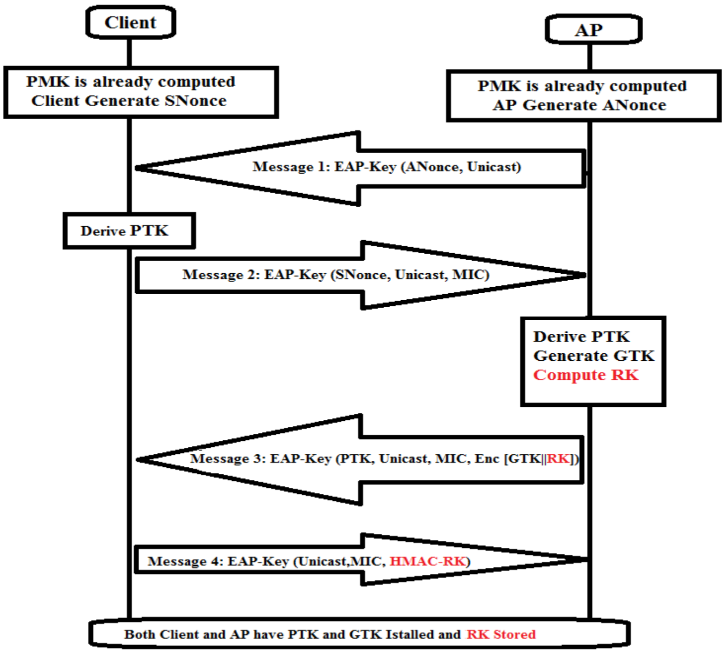

Client
AP
PMK is already computed
Client Generate SNonce
PMK is already computed
AP Generate ANonce
Message 1: EAP-Key (ANonce, Unicast)
Derive PTK
Message 2: EAP-Key (SNonce, Unicast, MIC)
Derive PTK
Generate GTK
Compute RK
Message 3: EAP-Key (PTK, Unicast, MIC, Enc [GTK||RK])
Message 4: EAP-Key (Unicast,MIC, HMAC-RK)
Both Client and AP have PTK and GTK Istalled and RK Stored

Figure 10: the proposed enhanced four-way handshake.

In the current four-way handshake, just after AP receives the Message 2, it simultaneously, but independently generates both GTK and RK (Re-authentication Key) which will be concatenated (separated by padding bits) and encrypted, before being sent along with Message 3 with following content.

Message 3: EAPoL-Key (Install PTK, Unicast, MIC, Encrypted (GTK || RK)).

The RK should meet certain requirements such as:
- The Seed used for generation should not be related to the PSK (the AP could use a pseudo-random function),
- Strong (pre-eliminating weak key scenarios by using a pre-assessment function installed on the AP) and 1024 bits long.

The last message in the handshake (Message 4) should contain, in addition to the regular message, the confirmation of the reception of the RK by sending back the hash and digital signature associated to the RK (HMAC-RK). This step guarantees the authentication of the receiver, the integrity and the non-repudiation of the sender. The Message 4 contains EAPoL-Key (Unicast, MIC, RK-HMAC).

The Re-authentication Key (RK) generation is as follows:

RK= Initial-seed (random-data) XOR (AP-MAC||Client-MAC||Client-Time-First-ever-connection).

The proposed protocol in contrast with [1] is adapted to deal with real de-authentication attack, despite the fact that it remains hard to distinguish the legitimate one from a suspicious one, in case when the de-authentication is not used as a DoS attack, and targeting only one client. Nevertheless, the AP remains listening even after receiving the de-authentication frame because an active client did not request the de-authentication. If the client did not initiate a de-authentication process, it usually continues to send data frames. The proposed re-authentication protocol rely mainly on:

- Security of the first connection (four-way-handshake),
- Accuracy of the logged data (which is used as a reference for determining the duration between the connection requests)
- Minimum duration allowed between two connections (excluding the roaming client as the WPA2-PSK is mainly used for unique AP architecture).

This protocol requires both client and AP store some information about the last authentication and de-authentication activity. The following information is used as seed along with the shared RK to generate the session re-authentication key SRK:

- The time of the last sent/received de-authentication frame,
- The last de-authentication frame sequence number,
- The MIC (Message Integrity Check) of the last de-authentication frame,
- The time of the de-authentication.

The re-authentication algorithm (Figure 11) introduces the concept of minimal duration between two authentication requests (RMT - Re-authentication Minimal Time). RMT is crucial as in de-authentication attack, RMT permits to differentiate between normal and suspicious de-authentication. Suspicious de-authentication is handled separately relying on the proposed re-authentication protocol. RMT could be set according to the user preference. At AP this pseudo-algorithm is applied to each authentication request to determine if the authentication will follow the normal procedure or the procedure for suspicious re-authentication requests.

```
Begin:
Receive Connection Request;
Authenticate Client;
Associate Client;
LAT= Get (last-Auth-Time);
CT= Get (Current-Time)
If (CT < (LAT + RMT))
{
    LDFT= Get (last-Deauth-Frame-Time);
    LASN= Get (last-Deauth-Sequence-Number);
    LMIC= Get (last-frame-MIC);
    SRK= RK || (LDFT XOR (LASN||CT);
    SN= LASN+1;
    HMAC= LMIC XOR SHA-2(SRK);
    Perform 4-way-handshake using RSK instead of PSK;
}
Else:
    Perform 4-way-handshake using PSK;
End.
```

Figure 11: the authentication procedure selection algorithm.

The re-authentication 4-way handshake for a given period less than RMT is similar to the existing protocol [1] as it just replaces PTK with SRK. This allows a legitimate client to re-authenticate and regain access and also to protect the PSK from being disclosed during this particular time, as a potential attacker who provoked the re-authentication process may be observing the handshake in order to capture the PTK from which the attacker could easily obtain PSK, and perform a brute force attack.

Analysis and Discussion

The proposed protocol attempt to mitigate the risk of capturing the key exchange on the four-way handshake by forcing a client to re-authenticate itself while the attacker is monitoring the exchange. Nevertheless, the possibility of an attacker capturing the initial 4-way handshake still exists, that is, for an example a four-way handshake which was not provoked by de-authentication attacks. This solution uses the security of the first connection (four-way-handshake), and the accuracy of the logged data as a reference for determining the duration between the connection requests (CT) and the allowed minimum duration between two connections (RMT) are the key factors which can contribute on the efficiency of the proposed protocol. Meanwhile, these factors should be set in a manner that guarantees the best performances by estimating the false-acceptance and false-rejection rates.

Because of the nature of de-authentication attack which in some situations injects very few forged de-authentication frames making it hard for any IDPS to distinguish it from the legitimate traffic and launch an alert like it does with other type of attacks such as DoS. The proposed re-authentication protocol covers this flaw in particular situations (injection of one or few targeted de-authentication frames to disconnect a client) without requiring a software or hardware upgrade or distributing the WLAN performances which is the case in the previously proposed enhancements such as cryptographic method [1,7], delaying the effect management frames [9]. Moreover, the proposed machine learning methods [8] remains insufficient especially to deal with single de-authentication frame attack where the sequence number remains unable to counter this type of attack [9].

The proposed protocol does not require any software or hardware upgrade to be implemented. Nevertheless, some vulnerabilities still exist such as the attacker capturing the initial handshake without launching a de-authentications attack against the connected clients.

VI. CONCLUSION:

The proposed protocol contributes to the enhancement of the WPA2-PSK security against the de-authentication attack. A de-authentication attack forces a client to re-connect to the AP while the attacker is monitoring the handshake process in order to capture enough information to be able to reverse the process and retrieve the PSK which is the only security provided on WPA2-PSK. Therefore, once compromised the wireless network will be subjected to different misuses and attacks. Another strength is that all current APs regardless of their capabilities can adopt the proposed protocol with slight modifications. Further, the proposed protocol make use of time factor which makes it impossible for an attacker to guess (brute force attack) or to spoof (capture the information about first ever connection time) this information. Nevertheless, its dependency on the minimum duration factor to determine whether the re-connection will be using the normal handshake or the proposed re-authentication handshake is the main weakness of this protocol.

The proposed protocol could be further enhanced by introducing more variables (behaviour and traffic) which the AP could rely on to determine whether a returning client will be authenticated using the regular handshake or the proposed re-authentication handshake. The re-authenticated protocol could also be enhanced by implementing an additional mechanism inside the algorithm to deal with special scenarios such as: AP software/hardware failure or reboot, AP power off or legitimate clients losing last authentication session data.

REFERENCES

[1] IEEE Computer Society. (2012). Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Standard Association, IEEE Std 802.11-2012, ISBN 978-0-7381-7245-3 STDPD97218.

[2] Dave, S., Trivedi, B. Mahadevia, J. (2013). Efficacy of attack detection capability of IDPS based on its deployment in wired and Wireless environment. International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.2, March 2013. DOI :10.5121/ijnsa.2013.5208 103.

[3] Weaver, R., Weaver, D. and Farwood, D. (2014). Guide to Network Defense and Countermeasures. *Chap 8: Intrusion Detection and Prevention Systems*. International third edition. P 256-290.

[4] Yong-lei, L. (2015). Defense of WPA/WPA2-PSK Brute Forcer. 2nd International Conference on Information Science and Control Engineering.

[5] Agarwal, M., Biswas, S., and Nandi, S. (2013). Detection of De-authentication Denial of Service attack in 802.11 networks. Annual IEEE India Conference (INDICON).

[6] El-Khatib, K. (2010). Impact of Feature Reduction on the Efficiency of Wireless Intrusion Detection Systems. IEEE transactions on parallel and distributed systems, Vol. 21, No. 8.

[7] Korcák, M. Lámer, J. and Jakab, F. (2014). Intrusion Prevention/Intrusion Detection System (Ips/Ids) For Wifi Networks. International Journal of Computer Networks & Communications (IJCNC) Vol.6, No.4, July 2014.

[8] Raju, K., Vallikumari, V., and Raju, K. (2011). Modeling and Analysis of IEEE802.11i WPA2-PSK Authentication Protocol. IEEE Journal, 978-1-4244-8679-3/11.

[9] Yong-lei, L. (2015). Defense of WPA/WPA2-PSK Brute Forcer. 2nd International Conference on Information Science and Control Engineering.

[10] Nakhila, O., Attiahy, A., Jinz, Y., and Zou, C. (2015). Parallel Active Dictionary Attack on WPA2-PSK Wi-Fi Networks. Milcom 2015 Track 3 - Cyber Security and Trusted Computing.

[11] Angela, A. (2014). Evaluation of Enhanced Security Solutions in 802.11-Based Networks , International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.4, 10.5121/ijnsa.2014.6403 29.

[12] Scarfone, K & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). *Recommendations of the National Institute of Standards and Technology,* Special Publication 800-94.

[13] McCann, S. and Ashley, A. (2016). official ieee 802.11 working group project timelines. IN PROCESS - Standards, Amendments, and Recommended Practices, http://www.ieee802.org.

[14] IEEE 802.11. (2016). What is IEEE 802.11 doing. A short summary of the current IEEE 802.11 activities and description of IEEE processes, http://www.ieee802.org/11/Publicity.

[15] Phifer, L. (2015). A list of wireless network attacks. *http://searchsecurity.techtarget.com*. Accessed on 07/10/2015.

[16] Nguyen, T., Nguyen, D., Tran, B., Vu, H., and Mittal, N. (2009). A lightweight solution for defending against deauthentication/ disassociation attacks on 802.11 networks. http://www.utdallas.edu/~nxm020100/publications.

[17] SANS Institute. 2014. Detecting and Responding to Data Link Layer Attacks, InfoSec Reading Room.

[18] Yusof, M., Hafiz Fakariah, M. and Mohd Ali, H. (2014). Profiling and Mitigating Brute Force Attack in Home Wireless LAN. *International Conference on Computational Science and Technology* (ICCST'14).

[19] Kim, J., Baek, J., and Shon, T. (2011). An Efficient and Scalable Re-authentication Protocol over Wireless Sensor Network. IEEE Transactions on Consumer Electronics, Vol. 57, No. 2, May 2011.

[20] Aharoni, M., Kearns, D., and Hertzog, R. (2016). KALI Linux. https://www.kali.org accessed on 01/01/2016.

[21] Aspyct. (2016).Aircrack tools. http://www.aircrackng.org/ documentation, accessed on 02/12/2015.

[22] K'Ondiwa, N., and Ochola, E. (2013). An Anti-DoS Attack Architecture for Wireless IT Infrastructure. Pan African International Conference on Information Science, Computing and Telecommunications.

[23] Mattsson, U.T. (2002). A Practical Implementation of a Real-time Intrusion. Prevention System for Commercial Enterprise Databases.

[24] Sembhi, S. (2015). How to defend against data integrity attacks. *http://www.computerweekly.com/,* Accessed on 08/10/2015.