Prevention of Parallel Active Dictionary Attack on WPA2-PSK Wi-Fi Networks

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Drishti Kakar  Computer Engineering  DJSCOE,  Mumbai, India  drishtikakar9@gmail.com | Nagendra Kamath  Computer Engineering  DJSCOE,  Mumbai, India  nagendra.s.kamath@gmail.com | Aneek Guha  Computer Engineering  DJSCOE,  Mumbai, India  aneek.guha@gmail.com |  | Dr. N. M. Shekokar  HOD - Computer Department  DJSCOE,  Mumbai, India  narendra.shekokar@djsce.ac.in |  |  |

*Abstract* -The wireless LAN provides ubiquitous access to the Internet globally, also being extremely user-friendly and cheap. The secure access to the Internet is now of paramount importance. The standards for internet security have evolved from WEP to the present standard WPA2-PSK for the IEEE 802.11 networks. There are various types of attacks which can be performed on the WPA2-PSK but dictionary attacks are the most potent of attacks. The offline dictionary based attacks on the WPA2-PSK involves the capturing of the four-way handshaking frames transferred between the Access Point (AP) and the wireless client. The online parallel dictionary attack on the WPA2-PSK, however allows the external client to bypass the frame capture phase and continuously inject pass phrases until it is accepted and connection is established. The threat of active parallel dictionary attacks on the WPA2-PSK can be countered using a 32-bit global counter encrypted using the PMK instead of randomly generated Nonce values in the current EAPoL message transfer protocol;and using Secure Hash Algorithm (SHA-512) instead of SHA-1 in the underlying pseudorandom function (PRF) for Password Based Key Derivation Function (PBKDF2). The proposed technique will significantly reduce the parallel online dictionary attack speed and performance while attacking the WPA2-PSK.

Keywords— Wireless Networks, WPA2-PSK, Online Dictionary Attacks, EAPoL, PBKDF2, Virtual Wireless Clients.

# Introduction

Short for Wi-Fi Protected Access 2 - Pre-Shared Key, also called WPA2-PSK or WPA2 Personal, is a method of securing your network with the use of the optional Pre-Shared Key (PSK) authentication, which was designed for home users without an enterprise authentication server. To encrypt a network with WPA2-PSK, we provide our router not with an encryption key, but rather with a natural language passphrase between 8 and 63 characters long. Using PBKDF2, that passphrase, along with the network SSID, is used to generate unique encryption keys for each wireless client which are constantly changed. Dictionary attack on wireless networks can be basically classified into two types: Offline Attacks and Online Attacks. The offline dictionary attack involves the capturing of the four-way handshaking frames exchanged between the legitimate client and the Access Point using powerful software tools such as Airodump-ng [1] and then trying to guess the pass phrase using brute force method (Aircrack-ng). The biggest necessity for the offline attack to be successful is that there has to be a legitimate client requesting connection to the AP. One of the major problems associated with offline attacks is that all the available implementations of the dictionary based pass-phrase attacks on WPA2-PSK are offline and they fail if there is no legitimate wireless client connected to the Access Point (AP) or in the process of connecting to the AP. In this scenario, all offline brute force implementations will not work since they will require the initial WPA2-PSK four-way handshaking frames between the AP and a legitimate wireless client. The online dictionary attack does not require the attacker to capture the initial 4-way handshaking frames exchanged between the wireless client and the AP. Online attacks are more favourable for the attacker than the offline attacks as there is no need to wait for a legitimate client to connect to the AP in order to sniff the handshaking packets. Hence, there is a need to prevent and/or mitigate such attacks which led us to propose techniques for the same.

# Existing System

The IEEE 802.11 Wireless Local Area Networks(WLAN) is the current standard used for the interconnection of wireless devices to the Internet. The WPA2-PSK is a significant improvement over the earlier WPA and the Wired Equivalent Privacy(WEP)[]. As the WPA2 uses Advanced Encryption Standard- Counter Mode Cipher Block Chaining MAC Protocol (AES-CCMP), it has better security than the previously used WEP and WPA. The authentication and the connection phase in the WPA2 involves the requesting client to provide the correct pass phrase to the Access Point (AP).The most commonly used process to gain unauthorised access to the network through an Access Point is to generate the Pre-Shared Key(PSK) from the pass phrase installed in the Access Point(AP).The biggest flaw within the current system is the lack of an upper limit on the number of guessing attempts for deducing the pass phrase. This allows for the use of a dictionary attack that uses a series of trial and error methods to correctly guess the pass phrase of the Access Point and subsequently process it to find the Pre-Shared Key (PSK) and all other keys required to initiate and complete the connection to the Internet.

This flaw was consequently exploited when many Apple distributed iCloud accounts were hacked using dictionary based attack []. The offline dictionary attack involves the capturing of the four-way handshaking frames passed between the legitimate client and the Access Point using powerful software such as Airodump-ng[] and then trying to guess the pass phrase using brute force method(Aircrack-ng). The parallel online attack[] however manages to completely bypass the existing protection mechanisms in the Access Point such as Wi-Fi Protected Setup(WPS) and not requiring the use of the handshaking frames used during the authentication phases.

The WPA2-PSK protocol suite currently used to establish a connection between a client and the Access Point provides different keys, which are created from the PSK, which in turn is mapped from the pass phrase. The key creation phase begins after the wireless client and Access Point have completely exchanged capability information.

The Pre-Shared Key (PSK) is the primary key created after the initial association phase ends, using the pass phrase pre-installed on the Access Point. The WPA2-PSK uses the standard Password Based Key Derivation Function 2(PBKDF2) to generate the Pre-Shared Key. The PBKDF2 uses SHA-1 as the underlying hashing function for generating all the keys. However, SHA-1 has been reported to exhibit weakness against GPU based attacks. SHA-1 uses 32-bit integer operations which can be very efficiently performed using GPU as they do not require high degree of parallelism and RAM. The Pair Master Key (PMK) is similarly generated using the same function from the PSK. Subsequently, the protocol generates the Pair Temporary Key (PTK) using different set of parameters on a pseudo random function, which creates a 384-bit key. The Pair Temporary Key is divided into three equal sized keys of 128-bit each, which performs some important functions within the Extensible Authentication Protocol over LAN (EAPoL). The keys are namely: Key Confirmation Key(KCK), Key Encryption Key(KEK) and the Temporal Key(TK).

The WPA2-PSK uses the Extensible Authentication Protocol over LAN(EAPoL) for the passing of the seven different keys during the handshaking phase. The IEEE 802.1X[] describes the EAPoL framework which is used to encapsulate EAP messages into LAN protocols and carries the EAP messages between the client and Access Point(AP). The Extensible Authentication Protocol describes four types of messages:

* EAP request
* EAP response
* EAP success
* EAP failure

These messages are exchanged between the AP and the client to establish the connection and start the access to internet. The EAPoL protocol messages however are not encrypted and passed through the channel in a plaintext format. This will allow any attacker to easily capture and read the entire contents of the messages and will render the system vulnerable to unauthorised access to the WPA2-PSK as they will have the keys required to initialise connection to the AP.

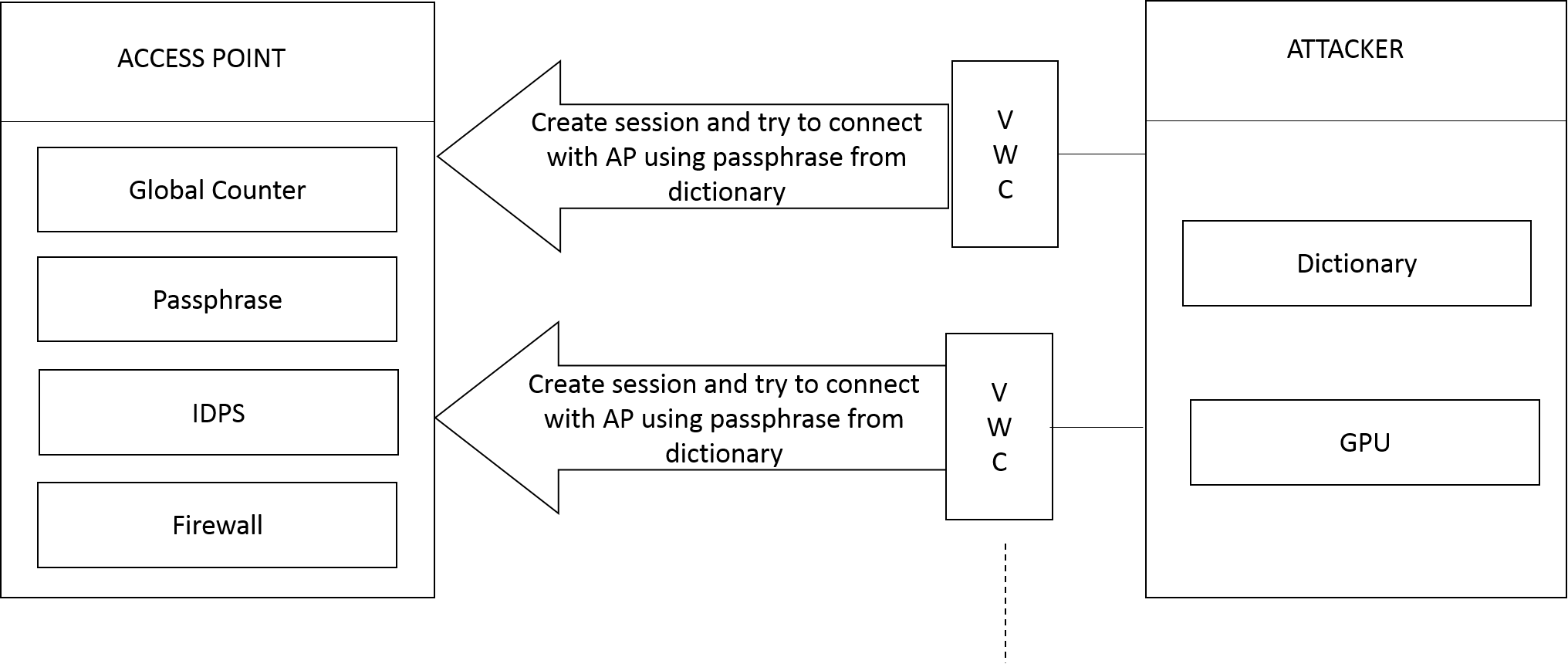


Figure 1. Architecture diagram of Proposed System

# Proposed System

In order to prevent a parallel active dictionary attack on WPA2-PSK network, we propose a solution which incorporates changes in the key generation phase and the EAPoL framework of the existing system. First, we propose the use of an encrypted 32-bit Global Counter instead of an unecrypted randomly generated nonce, which is currently being used in the standard. The proposed Global Counter will consist of the following fields: First 16 bits (MSB) consists of a randomly chosen value and it will be maintained that the value chosen will not be the same for 2 consecutive counter sessions. The last 16 bits will act as a global counter which will increment with every message sent. It will have 2^16 values. After 2^16 values, the whole counter will be refreshed, setting the value of the counter to 0, the randomly generated value is also changed and same process continues. This counter is encrypted using Pairwise Master Key (PMK - 256-bit) which itself is generated using the PBKDF2 function and the PSK as one of the inputs.

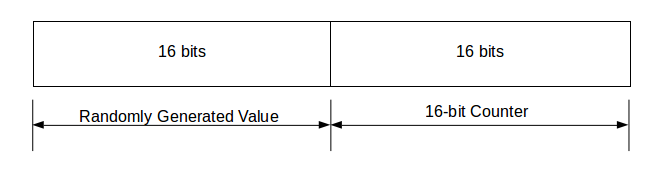


Figure 2. Proposed Global Counter

Secondly, we propose the use of SHA-512 instead of SHA-1 in the PBKDF2 function used to generate the PSK and the PMK. SHA-512 is more secure than SHA-1, which includes 64-bit calculations, which in turn reduce the efficiency of GPUs used for a GPU-based attack because GPUs are not

efficient enough for 64-bit calculations. [1]

Hence we propose the following algorithm to be incorporated into the Access Point (AP) for setting up connection to the clients.

***Access Point (AP) Program - With prevention/ mitigation methods***

The algorithm for Access Point program is as follows:

1. Start

2. PSK and PMK are generated using the PBKDF2 but uses SHA-512 instead of SHA-1

3. If the value of the Global Counter (GC) is already assigned, encrypt it using the PMK

4. If the value of GC is full or if it is not set, initialize the counter value with randomly generated first 2 bits with not having the same value as previously assigned (if any) and the remaining bits are set to 0. It is encrypted using the PMK.

5. The encrypted GC is sent as the Message 1

6. The legitimate client decrypts the Global Counter value and generates the MIC and sends it as Message 2 along with incremented Global Counter (GC+1), which is also encrypted GC = GC + 1 (at the LSB)

7. The PTK and GTK (if necessary) are generated if the MIC is correct.

8. The PTK, MIC and encrypted GTK are sent as Message 3.

9. End

We have also observed that WPA2-PSK does not limit the number of unsuccessful attempts by a user in connecting with the AP. This raises some concern, especially, for online dictionary attacks. Online dictionary attacks can target any network authentication/authorization device to gain access to it. Not limiting the number and the speed of pass-guessing trials will significantly magnify the danger of this type of attack. For example, recently many Apple distributed iCloud accounts were hacked by using a pass-guessing dictionary attack since the attacker was able to try many passwords without being blocked by Apple servers [1].

Hence, we need to keep the number of unsuccessful attempts in check in order to reduce the vulnerabilities of WPA2-PSK. A Intrusion Detection and Prevention System can be implemented at the Access Point to block any new connections for a predefined period of time when an attack is detected. An attack can be detected by analyzing the frequency of connection failures over a period of time.

# 4-way handshake with proposed global counter

Both the AP and the wireless client rely on the four- way handshake communication to confirm the possession of PSK.[1] The four-way handshake procedure starts after the wireless client authenticates and associates to the AP.

Four-way handshake consists of four messages as shown in Figure 3. EAPoL is used to carry out the four-way handshaking messages between both parties.

The exchange of EAP messages enveloped in EAPoL is performed between the client and the Access Point (AP). The AP has the pass phrase already installed, using which it derives the Pre-Shared Key(PSK) and subsequently derives the Pair Master Key (PMK) and the Pairwise Transient Key (PTK).

The AP sends Message 1, which contains a Global Counter (GC), encrypted using PMK. When the wireless client receives Message 1, it will have all of the required parameters to derive Pairwise Transient Key (PTK) from PSK.

At this point, Key Confirmation Key (KCK), Key Encryption Key (KEK) and Temporal Key (TK) are generated on the wireless client side. The wireless client then creates Message 2 which contains incremented Global Counter i.e. (GC+1) and the Message Integrity Code (MIC). MIC is used to ensure the integrity of Message 2. MIC is calculated on the whole EAPOL header plus the KCK i.e. MIC (EAPOL, KCK). When the AP receives Message 2, it extracts the value of GC and derives KCK, KEK and TK. Furthermore, the AP will calculate Message 2 MIC and compare it with the MIC received from the wireless client.

Message 3 is sent from the AP to the wireless client and it contains the Group Temporal Key (GTK) encrypted using KEK, MIC and the encrypted value of GC+2.

Message 4 will be sent from the wireless client to the AP to confirm a successful end of the four-way handshaking. It contains the MIC and the encrypted value of GC+3.

The use of the encrypted Global Counter ensures that only a legitimate client can obtain the value of GC as the PMK that is used to encrypt it is derived from the PSK, which in turn is derived from the passphrase. The first randomly generated 16-bits of the GC prevents pattern-based cryptanalysis. The other 16-bits are incremented for every message exchanged between the AP and the client. The randomly generated part of the GC ensures that even if the counter value (second half of GC) is the same for two different sessions, the first half does not match as it is taken care that two consecutive values are not the same and this will help prevent replay attacks.

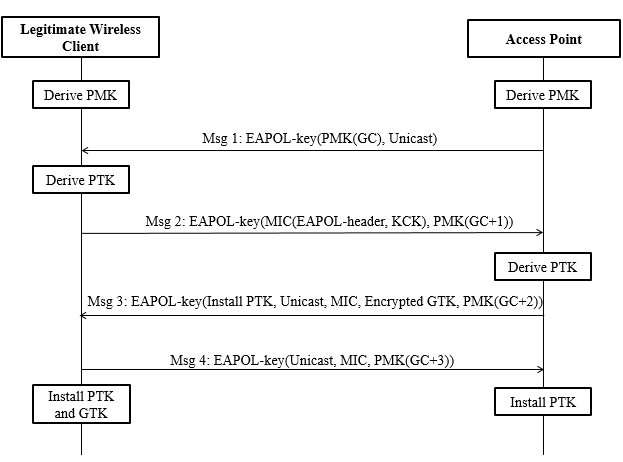


Figure 3. WPA2-PSK four-way handshaking with encrypted Global Counter (GC) (Proposed)

# CONCLUSION

##### We have proposed two novel techniques to prevent online dictionary attack - first, the introduction of a Global Counter (GC) encrypted with the Pair Master Key (PMK) instead of the randomly generated Nonce in the EAPoL protocol. This technique will make the EAPoL protocol more robust towards online dictionary attacks and provide a more secure channel for transfer of messages in the EAPoL framework.

##### Second, the use of SHA-512 instead of SHA-1 in Password Based Key Derivation Function Version 2 (PBKDF2) to generate more secure Pre-shared key (PSK) and Pair Master Key (PMK). Another flaw detected in WPA2 is that it does not limit the number wrong passphrase attempts. The proposed design of the Access Point (AP) includes an IDPS, which is responsible for blocking the network after a predetermined threshold of failed attempts.

# Future Scope

More research can be done on the use of SHA-512 to avoid GPU based attacks. Also, the use of Global Counter proposed by us can further be tested against various types of attacks and can be improved. The algorithm of the parallel active dictionary attack can be improvised further to bypass the proposed prevention methods. The Nonce value is encrypted in the proposed system. This can be tested in large scale environments to check the feasibility in everyday use. The firewall implemented by the IDPS may have vulnerabilities which can be exploited.

# References

[1] O. Nakhila, A. Attiah, Y. Jinz and C. Zoux, "Parallel active dictionary attack on WPA2-PSK Wi-Fi networks," *Military Communications Conference, MILCOM 2015 - 2015 IEEE*, Tampa, FL, 2015, pp. 665-670.

[2] MuthuPavithran. S, Pavithran. S, “Advanced Attack Against Wireless Networks Wep, Wpa/Wpa2-Personal And Wpa/Wpa2-Enterprise,” *International Journal Of Scientific & Technology Research,* Volume 4, Issue 08, August 2015

[3] [RFC2898] Kaliski B., "PKCS #5: Password-Based Cryptography Specification Version 2.0", RFC 2898, September 2000.

[4] CrackStation’s Password Cracking Dictionary [Online]. Available: https://crackstation.net/buy-crackstation-wordlist-password-cracking-dictionary.htm

[5] [RFC3580] P. Congdon, B. Aboba, A. Smith, G. Zorn, J. Roese, “IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines”, RFC 3580, September 2003.

[6] [RFC3748] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, Ed., “Extensible Authentication Protocol (EAP)”, RFC 3748, June 2004.

[7] [RFC4401] N. Williams, “A Pseudo-Random Function (PRF) API Extension for the Generic Security Service Application Program Interface (GSS-API)”,RFC 4401, February 2006.

[8] Security StackExchange on GPU attack on SHA-1 [Online] Available:https://security.stackexchange.com/questions/9061/what-algorithms-are-best-be-cracked-by-gpu