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 modern standard used is the Wireless Protected Access 2-Pre-Shared Key (WPA2-PSK), which protects the IEEE 802.11 wireless networks. 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. We propose the use of an encrypted global counter in the message exchange of the Extensible Authentication Protocol (EAP) over LAN (EAPoL) framework, the use of SHA-512 in Password Based Key Derivation Function - 2 (PBKDF2) and putting a limit on the number of unsuccessful connection attempts to prevent parallel active dictionary attacks on WPA2-PSK Wi-Fi networks.

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 WLAN uses the WPA2-PSK as the personal mode assigned for the connection of devices in the Small Office/Home Office (SOHO) networks. The WPA2-PSK is a significant improvement over the earlier WPA and the Wired Equivalent Privacy (WEP), which had quite a few vulnerabilities that could be exploited by the attackers. As the WPA2 uses Advanced Encryption Standard- Counter Mode Cipher Block Chaining MAC Protocol (AES-CCMP), it has better security than the previous standards.

The authentication and the connection phase in the WPA2 involves requesting the client to provide the correct pass phrase to the AP. The pass phrase is generally in the range of 8 to 63 characters. The most commonly used process to gain unauthorised access to the network through an Access Point is to generate the PSK from the pass phrase installed in the AP. The dictionary attack 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 PSK and all other keys required to initiate and complete the connection to the Internet.

1. ***Key Generation***

|  |  |  |
| --- | --- | --- |
| **Packet Type** | **Name** | **Description** |
| 0000 0011 | EAPOL-Key | Used to exchange Cryptographic Keying information. |
| 0000 0001 | EAPOL-Start | A supplicant can issue an EAPOL-Start frame instead of waiting for a challenge from the authenticator. |

The WPA2-PSK protocol suite currently used to establish a connection between a client and the AP 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 AP 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 PBKDF2 to generate the Pre-Shared Key. The function usually accepts five separate parameters to create the output. It is of the form

***O=PBKDF2(PRF, password, salt, c, dk\_len****)*

where: **PRF = Pseudo-Random Function, password = pass phrase, salt = 32-bit cryptographic salt, c = number of iterations and dk\_len = length of the key desired.** To derive the PSK, the function is given a different set of values namely the Passphrase, Service Set ID (SSID), SSID length, number of iterations and dk\_len:

***PSK=PBKDF2(passphrase, SSID, SSIDlength, c=4096, dk\_len=256)***

Similarly, the Pair Master Key (PMK) is derived from the same function as:

***PMK=PBKDF2(PSK, SSID, SSIDlength, c=4096, dk\_len=256)***

Again, the protocol generates the Pair Temporary Key (PTK) using yet another set of parameters on a pseudo random function, which creates a 384-bit key. The parameters include the Pair Master Key, the MAC Address of both client and the AP as SPMac and APMac respectively and random 32-bit nonce generated by both client and the AP as SNonce and ANonce respectively.

***PTK=PRF-383(PMK, “pairwise key expansion”, Min(APMac, SPMac) || Max(APMac, SPMac) || Min(ANonce, SNonce) || Max(ANonce, SNonce))***

The Pair Temporary Key (PTK) is divided into three equal sized keys of 128-bit each, which performs some important functions within the EAPoL. The keys are namely: Key Confirmation Key (KCK), Key Encryption Key (KEK) and the Temporal Key (TK).

1. ***Protocol for Key Exchange***

The WPA2-PSK uses the EAPoL framework for the passing of the seven different keys during the handshaking phase.

The IEEE 802.1X [1] 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

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 also creates 32-bit ANonce. The client uses a passphrase to derive its own PSK and creates 32-bit SNonce.

The AP sends an EAP response message 1 with its Nonce value to the client, which subsequently derives the Pair Master

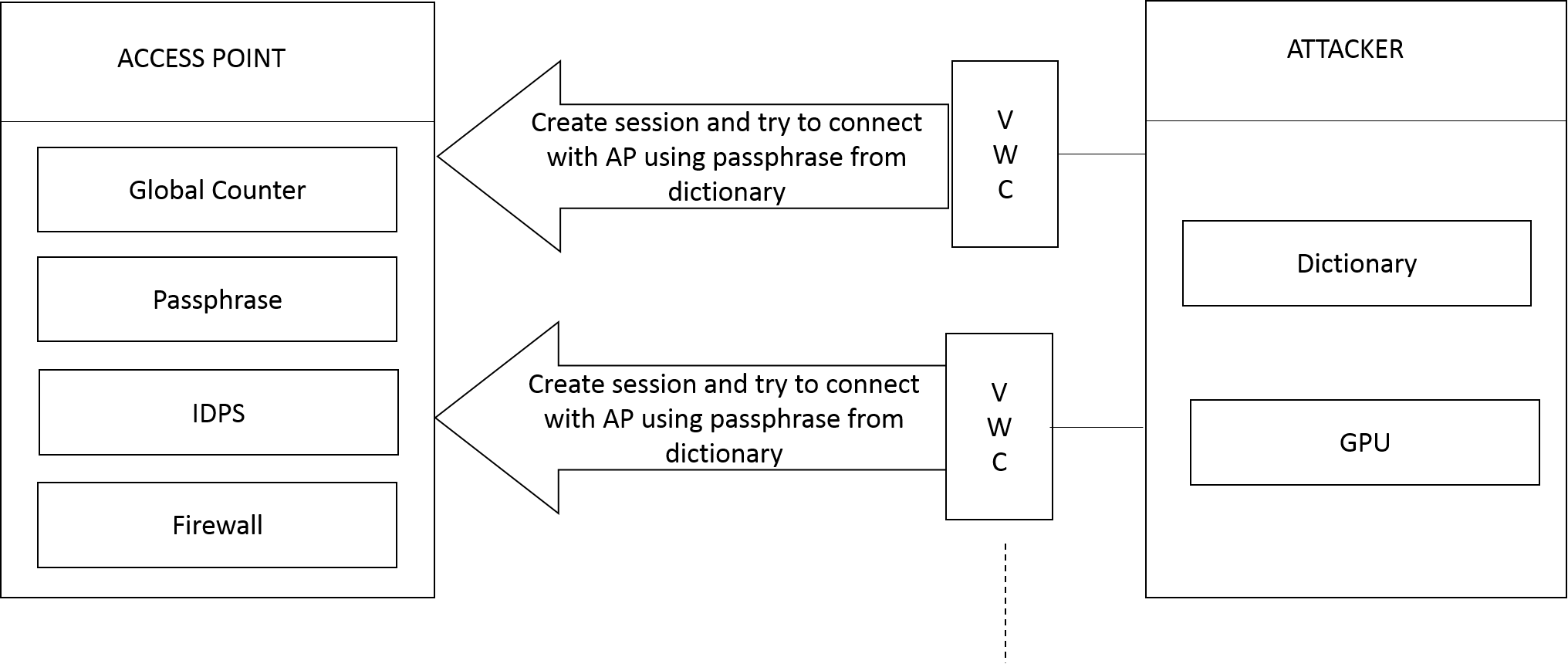


Figure 1. Architecture diagram of Proposed System

Key (PMK) and the Pair Temporary Key (PTK). The client then generates the three keys namely Key confirmation Key (KCK), Key Encryption Key (KEK) and the Temporal Key (TK).

The client sends the EAP message 2, which includes the randomly created SNonce and the Message Integrity Code (MIC) calculated on the EAPoL header frame and the KCK generated by its own PTK, **MIC(EAPoL,KCK).** The integrity code received by the AP is decoded to generate the KCK,KEK, TK. The AP then compares the integrity code generated on message 2 and that which is received from the client. If the Message Integrity Code on both are equal then, the client has the correct passphrase. The AP then derives the PTK from the SNonce it received from client.

The EAP message 3 is sent from the AP to the client containing the Group Temporal Key (GTK) computed using Pseudo Random Function (PRF-128) with the Group Master Key and the GNonce. The GTK is encrypted using the KEK and the MIC. The receipt of the message 3 by the client ensures that the passphrase is correct and the client is allowed to establish connection with the Access Point (AP). The integrity code (MIC) received by the AP will be same as that message 2 only if both client and AP have selected the same pass phrase.

The EAP message 4 sent to the AP finishes the process of the key exchange and both client and Access Point (AP) are connected.

# Proposed System

In this paper, we propose three novel techniques to improve the security of the WPA2-PSK standard as well as the EAPoL protocol which is used for the 4-way handshake. First, the use of an encrypted 32-bit Global Counter instead of the unencrypted randomly generated nonce, which is currently

being used in the standard [1].

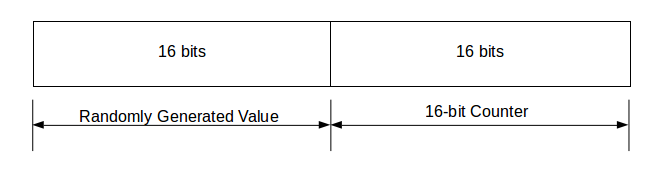


Figure 2. Proposed Global Counter

The proposed Global Counter will consist of the following fields: First 16 bits (MSB) consist 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 216 values. After 216 values, the whole counter will refresh, 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. This will prevent an attacker from connecting to the access point in the first place.

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 GPU’s are not efficient enough for 64-bit calculations.

We have 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 have been hacked by using pass-guessing dictionary attack since the attacker was able to try many passwords without being blocked by the Apple servers [1]. Hence, we propose the use of an Intrusion Detection and Prevention system that can help limit the number of wrong passwords entered to prevent an on-going dictionary attack. This will reduce the vulnerabilities for a user of WPA2-PSK.

# 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 4.1. EAPoL is used to carry out the four-way handshaking messages between both parties. First, 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 as shown in Figure 2. 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 and MIC. Message 4 will be sent from the wireless client to the AP to confirm a successful end of the four-way handshaking.

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.

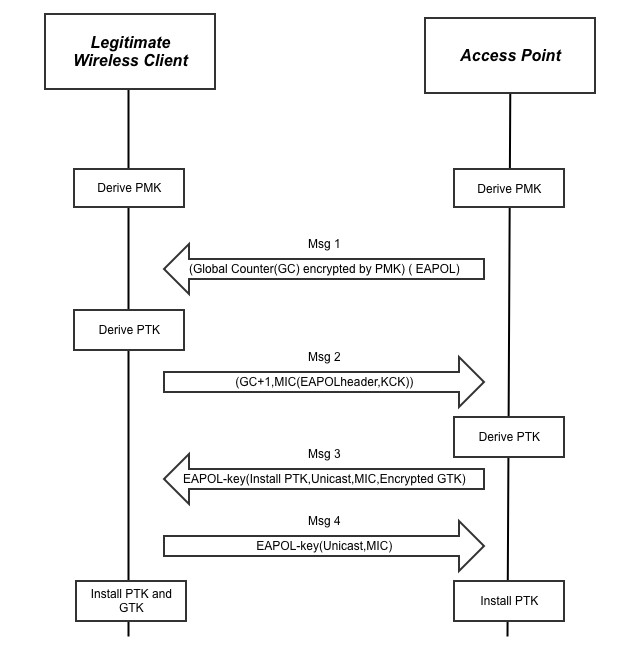


Figure 3. WPA2-PSK four-way handshaking with encrypted Global Counter (GC) (Proposed)

# WORKING

We will now discuss the algorithms for implementing our proposed system. The attacker’s algorithm does not include the use of the proposed GC on the Access Point and the algorithm for the AP includes the use of the encrypted Global Counter, SHA-512 and the use of an Intrusion Detection and Prevention System (IDPS). We also discuss the algorithm for the aforementioned IDPS that may be implemented to limit the number of unsuccessful passphrase attempts.

1. ***Attacker's Driver Program (without proposed GC)***

The algorithm for attacker’s driver program is as follows:

1. Start

2. Take input of SSID on which the attack is to be performed.

3. Create multiple Virtual Wireless Clients (VWCs) by creating multiple processes amongst which the dictionary is split.

4. Create a new session for each VWC.

5. Forcing GPU acceleration (optional) carry out the following for each VWC :

1. Accept the Message 1 from AP which consists of Anonce (Nonce generated at the AP)
2. Choose a passphrase from the available set of unused passphrases
3. From a passphrase, generate the PSK, then the PMK, and then the PTK.   
     
   **PMK (256) = PBKDF2 (PSK, SSID, SSIDLength, 4096, 256)   
     
   PTK (384) = PRF-383 (PMK, “Pairwise Key Expansion”, Min (APMac. SPAMac) || Max (APMac, SPMac) || Min (ANonce, Snonce) || Max (ANonce, SNonce))**
4. Compute the SNonce (Nonce Generated at the Client) value using the Pseudo Random Function (PRF)
5. Compute the MIC value over the EAPoL header and the KCK obtained from PTK as KCK (MIC (EAPOL, KCK))
6. Send SNonce and MIC to the AP in the form of Message 2
7. If Message 1 is received, try another passphrase from the dictionary and go to step 3.
8. If Message 3 is received, Break.
9. Found the correct pass-phrase; terminate all the active VWCs.

6. End

1. ***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. The AP keeps track of the number of wrong attempts at connection also the rate at which these attempts are being made. If the rate exceeds a certain threshold value, it indicates a dictionary attack and hence the network is blocked for a certain period using Intrusion Detection and Prevention System (IDPS).

10. End

1. ***Algorithm for IDPS at AP***

The algorithm used to implement IDPS at AP to detect and mitigate an on-going attack is as follows:

1. Monitor the network and write logs to file.

2. Filter the logs to check for the de-authentication frame (Message 4) in the logs at regular intervals of time.

3. The number of unsuccessful attempts is counted and its rate is calculated over the time interval. If the rate exceeds the a threshold value (Observed value: 1800-1850 passphrase attempts per minute) the following steps are followed using iptables:

• Block all incoming traffic except for recently established connections for a limited amount of time.

• If no connection was established before, block the entire incoming and outgoing traffic for a pre-defined amount of time.

4. Clear log file and go to step 1.

5. End

# 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.