KDC Authentication for Secured Communication using Four-Way Handshake Protocol

Iyswarya R.
Assistant Professor
Department of Computer Science and Engineering
Sri Venkateswara College of Engineering

Muthunagai S.U.
Assistant Professor
Department of Computer Science and Engineering
Sri Venkateswara College of Engineering

Poorani S.
Assistant Professor
Department of Computer Science and Engineering
Sri Venkateswara College of Engineering

Anitha R., PhD
Professor and Head
Department of Computer Science and Engineering
Sri Venkateswara College of Engineering

ABSTRACT
All the Wi-Fi connected devices are currently secured by WPA2 protocol but in recent studies it proves that the major vulnerability which exploits the man-in-the-middle attack it also referred as KRACK (Key Re-installation AttaCK). In this research, the improvisation of the current scheme of 4-way handshake in the WPA2 (Wi-Fi Protected Access-2) is discussed and has an advantage of already-in-use key exchanged in the handshake. The Key Distribution center (KDC) protocol improvises the WPA2 by randomly generating a session key per communication along with 4-way handshake key exchange in the protocol. Session key is used as a Pre- shared key for the derivation of further components in the key exchange. Thus, the confidentiality in the proposed protocol is maintained in secured manner.

General Terms
Security, Session Key, Access Point

Keywords
Key Distribution Center(KDC), KRACK(Key Re-installation AttaCK, Message Integrity Check (MIC)

1. INTRODUCTION
The current version of Wi-Fi uses the encryption protocol known as WPA-2 (Wi-Fi Protected Access 2) which is the enhanced and better version of its previous WPA [5]. WPA used 3-way handshake while WPA2 is different by applying 4-way handshake. Both the versions of Wi-Fi, Wi-Fi-Personal and Wi-Fi- Enterprise, used in private and public networks respectively relies on the encryption protocol. The 4-way handshake is a key exchange protocol where the two parties agree on the key for further encryption of the messages transmitted between them. The key where they agree upon is called as Pr -Shared Key (PSK). Hence, the WPA2 is also referred as WPA2-PSK. WPA2 uses CCMP-AES (Counter Mode/CBC-MAC Protocol) Protocol as its security protocol. The size of the key used is 128 bits length.[5] Thus it provides and maintains both confidentiality and integrity. Although the security has been improvised, a recent flaw has made it vulnerable. The vulnerability exploits the confidentiality through man-in-the-middle attack [1]. The attack have to be at the range of the network and sniffs the packet through a software (which can be used for penetration testing).Wi-Fi does not have a reliable medium such as optical fibre cables as its [3] only medium is air. Here messages at the medium can be dropped easily, which makes the attack easily. The attacker requires repeated packet data to derive the key and hence penetrate the network [7]. This happens between the Access Point (AP) and any Wi-Fi supported devices (smart phone, laptops, PCs etc). The PSK which is installed at the end of exchange, the attacker captures it and these results in the AP to re-transmit the same key again which is referred as re-authentication phase [3]. During this phase, the attacker will attempt to capture the HMAC (Hashed Message Authentication Code) of the PSK and by using several reversed encryption process, the key is identified [2].

2. RELATED WORK
The data transferred via public Wi-Fi is not secured. WPA2 (Wi-Fi Protected Access-2) is a protocol which provides security for public Wi-Fi access. However, this protocol has vulnerability, which is a serious threat [1]. The messages from Wi-Fi modem/router drop in the medium while transmission, it can be eavesdropped and loses confidentiality and integrity [9]. The vulnerability in the algorithm gives the way for the middleman to gain access to the encrypted data. As a result, the middleman can control and modify the data in user's IOT devices. The authentication before the key exchange might enhance the confidentiality in the key [8] .

2.1 Four-way Handshake
The handshake is the mutual exchange of Pair-wise Master Key (PMK) and a session key called as Pair wise Transient Key. The handshake happens after when the client (any WPA2 supported device) is authenticated with the AP [3]. It consists of four messages passed over the WLAN. The first is given from AP called as Anonce (Authenticator nonce or number used once) [5]. On receiving the Anonce, the client computes from the parameters from PSK and derives PMK using Password-Based Key Derivation Function 2(PBKDF2).

PMK=PBKDF2(PSK,SSID,SSID-Length,4096)

The PMK is same as the PSK since there is no authentication server[6].With the PMK, PTK is again derived after client's confirmation of its authentication along with Snonce and MIC(Message Integrity Check).PTK derived by client is given to AP which further derives its own PTK. It extracts nonce received and generates KCK(Key Conformation Key),KEK(Key Encryption Key),TCK()This MIC maintains the integrity in the exchange [5].

After generating the PTK, the AP checks MIC generated with the MIC received to ensure the integrity. GTK is also derived during this process. Then the AP transmits the PTK, GTK and permits the client to install the keys to its system [4].

2.2 Key Re installation Attack

The key re-installation attack occurs during the key exchange because the AP still accepts re-transmissions of keys, even when it is in the PTK acknowledgement state, the attacker can force a re-installation of the PTK. More precisely, he establishes a man-in-the-middle (MitM) [1] position between the supplicant and authenticator. This prevents the acknowledgement transferred. As a result, it will re-transmit key install message, which causes the AP to reinstall an already-in-use PTK. In turn, this resets the nonce being used by the data-confidentiality protocol [3]. Depending on which protocol is used, this allows an adversary to replay, decrypt, and/or forge packets.

Traffics in the air between a station and an AP can be eavesdropped by sniffing tools like wire shark. By using sniffing tools, attackers can capture data packets and get information from the packets. If an attacker analyzes packets that are not encrypted, it would be critical threat to users. Based on traffic analysis, other attacks can be tried such as Denial of Services (DoS), key recovery, fake authentication and Man in the Middle attack [1].

3. PROPOSED METHODOLOGY

The proposed architecture uses the Key Distribution Center (KDC) protocol. Since in the current WPA2 the authentication of client and server is not performed before the exchange, KDC authenticates only the client. This authentication is unique and random and is available only for the current session.

The use of a key distribution center is based on the use of a hierarchy of keys. At a minimum, two levels of keys are used. Communication between end systems is encrypted using a temporary key, often referred to as a session key. Typically, the session key is used for the duration of a logical connection, such as a frame relay connection or transport connection, and then discarded. Each session key is obtained from the key distribution center over the same networking facilities used for end-user communication. Accordingly, session keys are transmitted in encrypted form, using a master key that is shared by the key distribution center and an end system or user. For each end system or user, there is a unique master key that it shares with the key distribution center. Of course, these master keys must be distributed in some fashion. However, the scale of the problem is vastly reduced. If there are entities that wish to communicate in pairs, then, as was mentioned, as many as session keys are needed at any one time. However, only master keys are required, one for each entity. Thus, master keys can be distributed in some non cryptographic way, such as physical delivery.

Algorithm for KDC:

Input: Requesting key from KDC

Output: Session key generation

1. Compute A -> KDC:IDA||IDB||N_1
2. Authentication in KDC for both A and B
   KDC -> A:E($K_{a,}$ [K_s||ID_B||N_1||E($K_{B,}$[K_S||ID_A])])
3. A-> B:E($K_{b,}$[K_b,[K_S||ID_A])
4. B->A:E($K_{S,}$[N_2])
5. A->B:E($K_{S,}$[F(N_2)])

When user A wishes to establish a logical connection with B and requires a one-time session key to protect the data transmitted over the connection. A has a master key, , known only to itself and the KDC; similarly, B shares the master key with the KDC. The following steps occur.

A issues a request to the KDC for a session key to protect a logical connection to B. The message includes the identity of A and B and a unique identifier,for this transaction, which we refer to as a nonce. The nonce may be a timestamp, a counter, or a random number; the minimum requirement is that it differs with each request. Also, to prevent masquerade, it should be difficult for an opponent to guess the nonce. Thus, a random number is a good choice for a nonce.

The KDC responds with a message encrypted using. Thus, A is the only one who can successfully read the message, and A knows that it originated at the KDC.
A stores the session key for use in the upcoming session and forwards to B the information that originated at the KDC for B, namely, E(Kb,[Ks || IDA]).Because this information is encrypted with , it is protected from eavesdropping. B now knows the session key, knows that the other party is A (from IDA), and knows that the information originated at the KDC (because it is encrypted using).

The proposed model uses the session key generated during the first receipt of client to AP. The session key is 6-bit randomly generated key which is further used as the PSK and added to the passphrase. And this key is allowed only for the current session. Once the session is done, the key is eliminated.

Metrics comparison is done between WPA3 and KDC protocol such that KDC provides acceptable authentication before the handshake.

A Python program is implemented to demonstrate the working of the model.

4. SYSTEM ANALYSIS

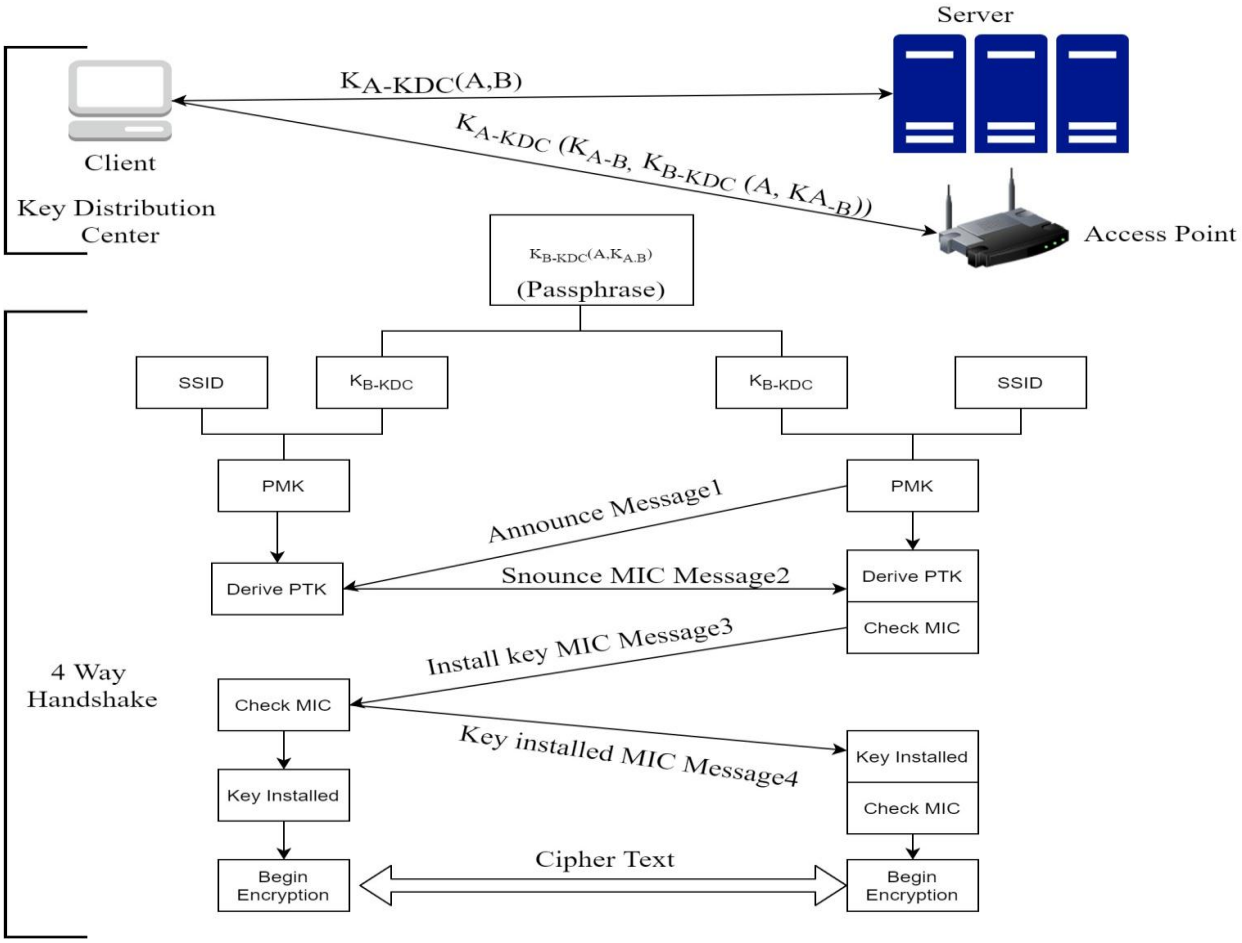

Fig 1 : Proposed architecture

4.1 MakePRF function:

This function is a pseudo random function used to generate the PTK.

```
def PRF (key,A,B)
nbyte=64
i=0
R=b
While(i<=((nbyte*8+159)/160));
hmacsha1=hmac.new(key,A+chr(0*00).encode()+3+chr(I).en
code(),sha1)
P=R+hmacsha1.digest()
i=i+1;
return R[0:nbyte]
```

4.2 MakeAB function

It generates the parameters required for PTK. These are Anonce, Snonce, client and AP's MAC addresses.

```
def  makeAB(anonce,snonce,apmac,climac)
A=b "pairwise key expansion"
B=(min(apmac,climac)+max(apmac,climac)+min(
        anonce,snonce)+max(anonce,snonce))
return(A,B)
```

4.3 MakeMIC function

It generates the Message Integrity Check (MIC) to ensure the unauthorized message modification.

```
def makemic(pwd,SSID,A,B,data,wpa = false):
Pmk=pbkdf2_hmac('sha1',pwd.encode('ascii'),ssid.encode('a
scii'),4096,32)
ptk =PRF(pmk,A,B)
hmacfunc=md5 if wpa else sha1
mics =[hmac.new(ptk[0:16],I,hmacFunc).digest()
for I in data]
return (mics,ptk,pmk)
```

4.4 KDC function

This is the proposed scheme implemented as a function.

```
def kdc(msg1,ida):
if(ida=="thisisida"):
ks=str(random.randint(10000000,19999999))
msg2=msg1+ks
return msg2
```

This function first authenticates and verifies the client and after verification sends the PSK and concatenates it with request message. The client must separate the key and further use it for derivation.

The below two screenshots described the output with using the KDC authentication protocol and without using the authentication protocol.

```
pmk:
0416E4E8AF389A1C76618915187FD063317990B4D4BF63DC577BEAD4AA50DD38

ptk:
C8E213223BE23084CAEBA6A8CE381255619295C60C9E48FC297D7242C1816A670220D
A439249861CAC0FB02991575AF0C81AD95832A2B53A1A7FA8FFBF599341

desired mic:    D48AD11C97F076B84138E9CED6969CB2
actual mic:     31B257A9D772F97D9A4B0EB482A1676B
MISMATCH

desired mic:    1E228672D2DEE930714F688C5746028D
actual mic:     8F1A321F4BD31A9B993FC892666786CB
MISMATCH

desired mic:    D5F07A0FBC8F376541D46591FDA74470
actual mic:     68BCE94EA2F86D10044E06F462BC4D17
MISMATCH
```

Fig 2: Output when KDC is applied

```
In [1]: runfile('C:/Users/Venkatesan S/Documents/Hari class XI-XII 2013-2014-2015/
College assignments/Sem 8/PyCrack-master/pywd.py', wdir='C:/Users/Venkatesan S/
Documents/Hari class XI-XII 2013-2014-2015/College assignments/Sem 8/PyCrack-
master')
pmk:            EBB5D703F8834A08D61A67A982FA009E08F747DD65D82C240169E604218B3ACF

ptk:
63E412CE67759BD5CEBD0F5B5A487CA155ADD51D771293E31C05BF05A3A98BCFE645F29203956E34C6A5
B0CC2186B1161F643807349576CDB2FB1C158B03648F

desired mic:    C2EE0E125962261C897A05E33B579F5C
actual mic:     C2EE0E125962261C897A05E33B579F5C
MATCH

desired mic:    1E228672D2DEE930714F688C5746028D
actual mic:     6D60808DE292A32BAE1D381B3D295B2F
MISMATCH

desired mic:    D5F07A0FBC8F376541D46591FDA74470
actual mic:     D5F07A0FBC8F376541D46591FDA74470
MATCH

In [2]:
```

Fig 3: Output when KDC is not applied

Table 1: WITHOUT KDC

Session	Desired MIC	Actual MIC	Integrity
1	C2EE0E125962262C897A05E33B579F5C	C2EE0E125962262C897A05E33B579F5C	MATCHED
2	1E228672D2DEE930714F688C5746028D	6D60808DE292A32BAE1D38183D295B2F	MISMATCHED
3	DSF07A0FBC8F376541D46591FDA74470	DSF07A0FBC8F376541D46591FDA74470	MATCHED

Table 2: WITH KDC

Session	Desired MIC	Actual MIC	Integrity
1	D48A11C97F076B84138E9CED6969CB2	31B257A9D772F97D9A4BOEB482A1676B	MISMATCHED
2	1E228672D2DEE930714F688656746028D	8F1A321F4BD31A9B993FC8926667 86CB	MISMATCHED
3	D5F07A0FBC8F376541D46591FDA74470	68BCE94EA2F86D10044E06F462BC4D17	MISMATCHED

Table 3 : Metrics Comparisons between WPA3 and KDC

Attack	WPA3	KDC
De-authentication	Yes	Yes
Handshake capture dictionary	Yes	Yes
PMKID Hash dictionary Attack	Yes	Yes
Rough Access point	**Partial**	**Fully**
Handshake Capture En/Decryption	Yes	Yes
KRACK	Yes	Yes
Before Handshake authentication	**No**	**Yes**

5. CONCLUSION AND FUTURE WORK

The proposed scheme provides the improvisation of the current WPA2 security protocol in Wi-Fi networks. The key generated from the protocol is random and temporary. This makes it impossible for derivation of messages using key obtained by packet sniffing. Without KDC the Desired MIC and Actual MIC will be matched so that packet sniffing can be done easily.But with KDC the Desired MIC and Actual MIC will not be matched so that packet sniffing is impossible. After implementing KDC parameters like Rough Access Point is achieved fully and Before Handshake Authentication has been successfully implemented for the packet sniffing attack as shown in fig

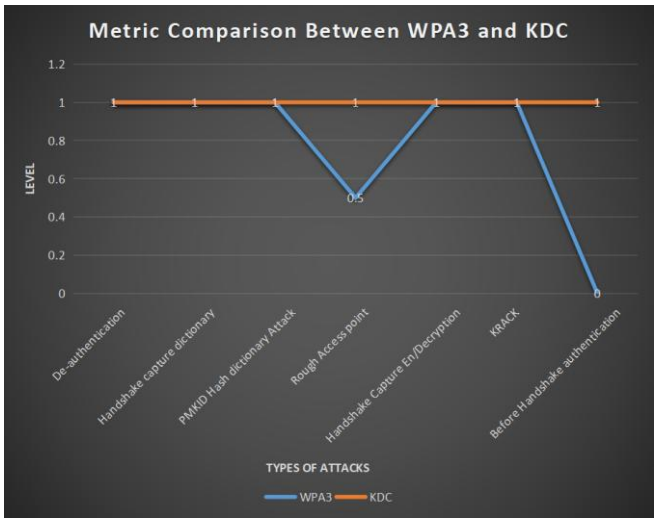

Fig 4: Metric Comparison Between WPA3 and KDC

In future, the scope of this scheme can give random session key for each key exchange.

6. ACKNOWLEDGMENTS

We would like to express our special thanks of gratitude to our institution who helped us to complete the paper.

7. REFERENCES

[1] Agarwal M, Biswas S,and Nandi S, Apr. (2015).'Advanced stealth man-in-the-middle attack in WPA2 encrypted Wi-Fi networks,'IEEE Commun. Lett., Vol. 19, No. 4, pp. 581-584

[2] Bai Qinghai, Zhang Wenbo, Jiang Peng , LU Xu ,(2012) , 'Research on Design Principles of Elliptic Curve Public Key Cryptography and Its Implementation' IEEE Explore ,pp 3-5.

[3] Ghanem M.C and Ratnayake D.N , (2016),'Enhancing WPA2- PSK four-way handshaking after re-authentication to deal with de-authentication followed by brute-force attack a novel re- authentication protocol' in Proc. International Conference. Cyber Situational Awareness, Data Analyst Assessment (CyberSA), London, U.K.,pp. 1-7.

[4] Ghilen, M. Azizi, and Bouallegue R, (2015), 'Integration of a quantum protocol for mutual authentication and secret key distribution within 802.11i standard' in Proc. IEEE/ACS International Conference Computer System Application. (AICCSA), Marrakech, Morocco, pp. 1-7.

[5] Jae Won Noh , Jeehyeong Kim And Sung Yun Cho, (2018) ' Secure Authentication and Four-Way Handshake Scheme for protected Individual Communication in Public Wi- Fi Networks' in IEEE Explore.

[6] Liu Y, Wang Y, and Chang G , (2017), 'Efficient privacy- preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm,' IEEE Trans. Intell. Transp. System , Vol. 18, No. 10, pp. 2740-2749.

[7] Mitchell J.C and C. He, (2005), 'Security analysis and improvements for IEEE 802.11i' ,in Proc. Network Distributed System Security Symptoms (NDSS), San Diego, CA, USA, pp. 90-110.

[8] Noh J, Kim J , Kwon G, and Cho S , (2016) , 'Secure key exchange scheme for WPA/WPA2-PSK using public key cryptography,' in Proc. IEEE International Conference Consum. Electronic-Asia (ICCE), Seoul, South Korea, pp.1-4.

[9] Subhas Barman,Samiran Chattopadhyay,Debasis Samanta,(2015) 'An Approach to Cryptographic Key Distribution Through Fingerprint Based Key Distribution Centre' IEEE.pp3-4.