4-WAY HANDSHAKE

admin (https://www.wifi-professionals.com/author/admin) 24th January 2019

34 Comments (https://www.wifi-professionals.com/2019/01/4-way-handshake#comments)

I was thinking to write about the 4-way handshake and started to think that from where I should start writing. Shall I just describe 4-way handshake which can be found everywhere on the web or shall I do a deep dive? Reason for me to write is to make it easier to understand for non WiFi people who can just read and understand because sometimes different terminologies used in this process can be confusing. So, let's start with…

What is 4-way Handshake:

The 4-way handshake is the process of exchanging 4 messages between an access point (authenticator) and the client device (supplicant) to generate some encryption keys which can be used to encrypt actual data sent over Wireless medium. These keys which are generated through 4-way handshake are generated by some source key material which will be discussed later.

If you do not want to get confused about the terminologies used in 4-way handshake then let's have a quick look. Let's see what terminologies we might come across to understand 4-way handshake. I would say don't be scared of these terminologies. It's like much ado about nothing.

These are the few keys we will be discussing…

- MSK (Master Session Key)
- PMK (Pairwise Master Key)
- GMK (Group Master Key)
- PTK (Pairwise Transit Key)
- GTK (Group Temporal Key)
- ANonce
- SNonce
- MIC

I will start by talking about the keys which are generated during the 4-way handshake and towards the keys and other variables needed in order to generate these keys.

PTK (Pairwise Transit Key):

Pairwise transit key is used to encrypt all unicast traffic between a client station and the access point. PTK is unique between a client station and access point. To generate PTK, client device and access point need the following information.

$$PTK = PRF\ (PMK + Anonce + SNonce + Mac\ (AA) + Mac\ (SA))$$

Anonce is a random number generated by an access point (authenticator), Snonce a random number generated by the client device (supplicant). MAC addresses of supplicant (client device) and MAC address of authenticator (access point). PRF is a pseudo-random function which is applied to all the input.

PTK is dependent on another high-level key PMK (pairwise master key) which is discussed below.

GTK (Group Temporal Key):

Group temporal key is used to encrypt all broadcast and multicast traffic between an access point and multiple client devices. GTK is the key which is shared between all client devices associated with 1 access point. For every access point, there will be a different GTK which will be shared between its associated devices.

GTK is dependent on another high-level key GMK (group master key) discussed below.

PMK (Pairwise Master Key):

What is PMK and why we need it? Now we know what is PTK and GTK. PTK is generated with the help of PMK. As we discused above in order to generate PTK, we need the following input.

PTK = PRF (PMK + Anonce + SNonce + Mac (AA)+ Mac (SA))

Pairwise master is key generated from master session key (MSK). In case of WPA2/PSK when device authenticates with access point the PSK becomes PMK.

Point to Remember: PMK resides on all stations as in AP and client devices, so we do not need to share this information. We use this information to create PTK which are used for unicast data encryption.

GMK (Group Master Key):

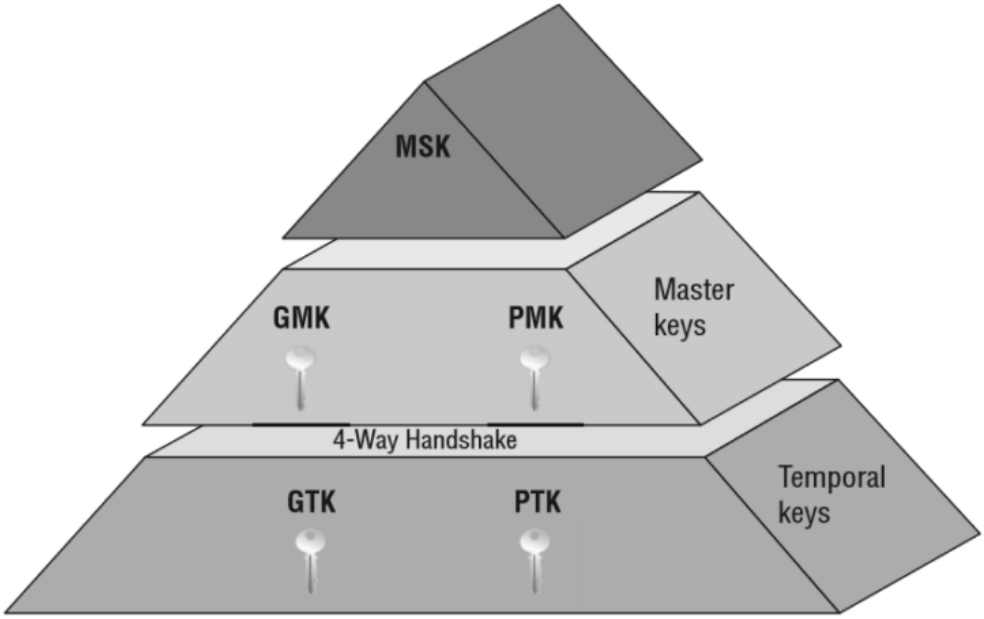
Group master key is used in a 4-way handshake to create GTK discussed above. GTK is generated on every access point and shared with the devices connected to this AP.

MSK (Master Session Key):

The master session is the first key which is generated either from 802.1X/EAP or derived from PSK authentication.

We discussed above keys from bottom to top and how keys are dependent on other keys. This is the view from top to bottom.

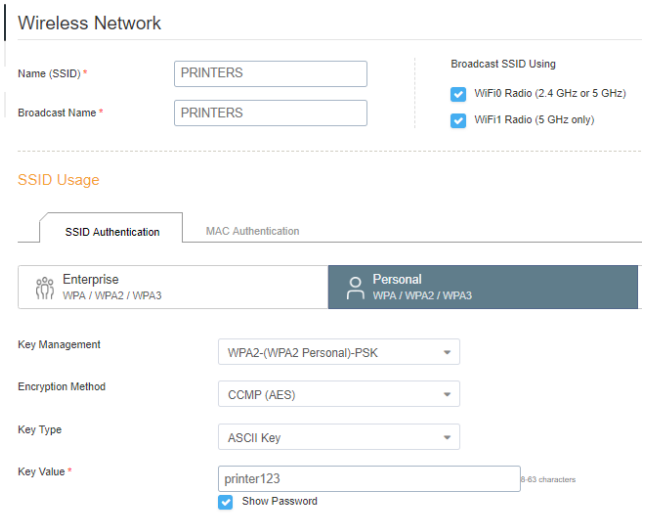
1. The first level key is generated is MSK during the process of 802.1X/EAP or PSK authentication.
2. The second level key is generated from MSK is PMK and GMK. PMK is used to generate PTK and GMK is used to create GTK.
3. Third level keys are the actual keys used for data encryption.



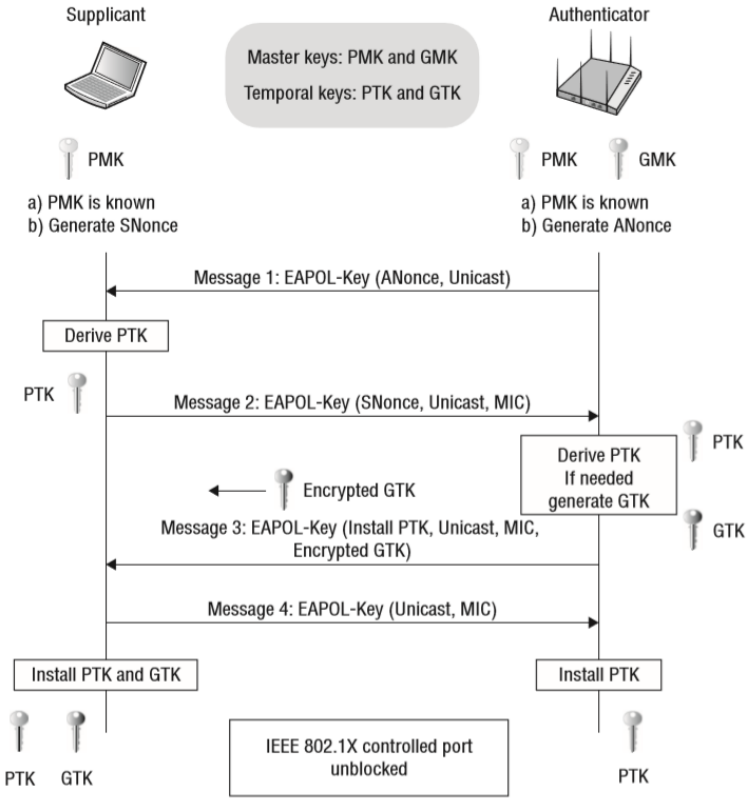
(Keys Hierarchy)

4-Way Handshake in Action:

Once we understand important keys and how they are generated now let's have a look on an actual 4-way handshake. Imagine an access point is configured with WPA2/PSK and device is trying to connect to it. In our example its SSID PRINTERS with password printer123.



Sooner user click on printers SSID it goes through the states which I have discussed in another post (http://www.wifi-professionals.com/2018/08/authentication-frame-misunderstanding). From authentication to the association to security validation. This is where 4-way handshake happens, instead of sending the password to the access points there are EAPOL (Extensible authentication protocol over LAN) messages exchange happens.



(4-way handshake)

Device States:

A device going through states from authentication to association. Once the device is authenticated and associated and now security will be checked, and 4-way handshake will start.

```
8728 802.11  Management frame   d0:c5:f3:a9:16:c5   Authentication        9c:5d:12:5e:6c:66   Authentication, SN=2002, FN=0, Flags=.......
8730 802.11  Management frame   9c:5d:12:5e:6c:66   Authentication        d0:c5:f3:a9:16:c5   Authentication, SN=1451, FN=0, Flags=.......
8749 802.11  Management frame   d0:c5:f3:a9:16:c5   Association Request   9c:5d:12:5e:6c:66   Association Request, SN=2003, FN=0, Flags=..
8755 802.11  Management frame   9c:5d:12:5e:6c:66   Association Response  d0:c5:f3:a9:16:c5   Association Response, SN=1452, FN=0, Flags=.
```

4-way handshake Wireshark view:

```
904 EAPOL   Data frame   9c:5d:12:5e:6c:66   QoS Data   d0:c5:f3:a9:16:c5   Key (Message 1 of 4)
906 EAPOL   Data frame   d0:c5:f3:a9:16:c5   QoS Data   9c:5d:12:5e:6c:66   Key (Message 2 of 4)
908 EAPOL   Data frame   9c:5d:12:5e:6c:66   QoS Data   d0:c5:f3:a9:16:c5   Key (Message 3 of 4)
910 EAPOL   Data frame   d0:c5:f3:a9:16:c5   QoS Data   9c:5d:12:5e:6c:66   Key (Message 4 of 4)
```

Message1: access point sends EAPOL message with Anonce (random number) to the device to generate PTK. Don't forget client device knows Ap's MAC because its connected to it. It has PMK, Snonce and its own MAC address. Once it receives Anonce from access point it has all the inputs to create the PTK.

PTK = PRF (PMK + Anonce + SNonce + Mac (AA)+ Mac (SA))

Mac address 9c:5d:12:5e:6c:66 is source address or mac address of the access point who is sending first EAPOL message to the device and d0:c5:f3:a9;16:c5 is Mac device. In this message access point sending ANonce to the client device.

```
904 EAPOL   Data frame   9c:5d:12:5e:6c:66   QoS Data   d0:c5:f3:a9:16:c5   Key (Message 1 of 4)
```

Wireshark · Packet 904 · airtool_2018-11-16_03.05.45.pm.pcap

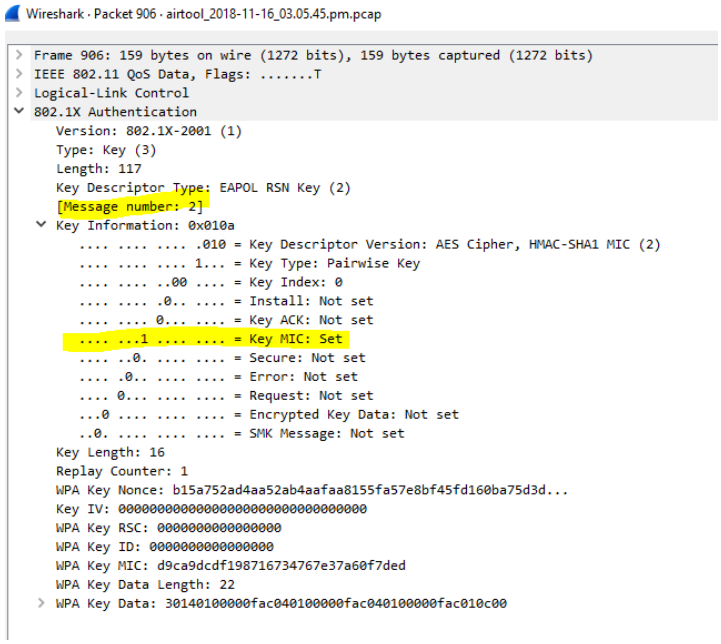
```
> Frame 904: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits)
> IEEE 802.11 QoS Data, Flags: ......F.
> Logical-Link Control
v 802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: Key (3)
    Length: 117
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 1]
  > Key Information: 0x008a
    Key Length: 16
    Replay Counter: 1
    WPA Key Nonce: 94a26c4f0e4040511d426dce3c3f7ee407d5002165c57a0b...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 00000000000000000000000000000000
    WPA Key Data Length: 22
  > WPA Key Data: dd14000fac04adfd2fc3518a51d99f2a534c47605e7c
```

(Anonce from AP to the device)

Message2: Once the device has created its PTK it sends out SNonce which is needed by the access point to generate PTK as well. The device sends EAPOL to AP message2 with MIC (message integrity check) to make sure when the access point can verify whether this message corrupted or modified. Once SNonce received by the AP it can generate PTK as well for unicast traffic encryption.

This is the second message going from the client device to AP with Snonce and MIC field set to 1.

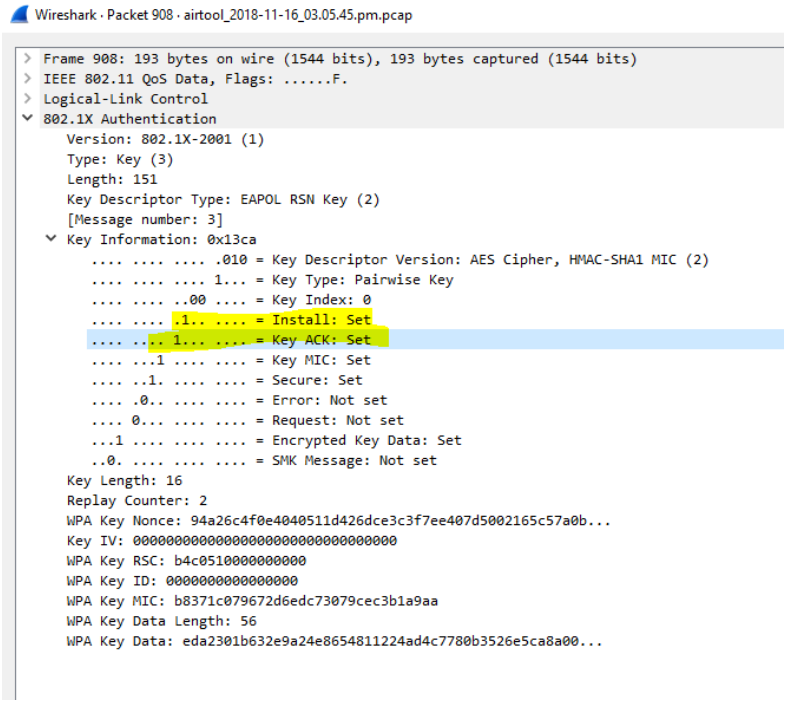
```
906 EAPOL   Data frame          d0:c5:f3:a9:16:c5      QoS Data          9c:5d:12:5e:6c:66      Key (Message 2 of 4)
```



(Message 2)

Message3: EAPOL message3 is sent from AP to client device containing GTK. AP creates GTK without the involvement of the client from GMK.

```
908 EAPOL   Data frame          9c:5d:12:5e:6c:66      QoS Data          d0:c5:f3:a9:16:c5      Key (Message 3 of 4)
```



(Message 3)

Message4: Fourth and last EPOL message will be sent from the client to AP just to confirm that Keys have been installed.

```
EAPOL   Data frame          d0:c5:f3:a9:16:c5      QoS Data          9c:5d:12:5e:6c:66      Key (Message 4 of 4)
```

4-way handshake Result:

Control port unlocked: Once the 4-way handshake is completed successfully virtual control port which blocks all the traffic will be open and now encrypted traffic can flow. Now all unicast traffic will be encrypted with PTK and all multicast traffic will be encrypted via GTK which created in the 4-way handshake process.

Summary:

Lets summaries all this what we have discussed above. I have broadcasted PRINTERS SSID and tried to connect to it. AP is beaconing SSIDs and when I clicked PRINTERS SSID to connect we can see full conversation with acknowledgment frame.

The device is requesting to connect to PRINTERS and the access point is responding with a probe response. Now device goes through the states from unauthenticated and un-associated to authenticated and associated.

Once authenticated and associated now it goes through security check and 4-way handshake happens and after successful 4-way handshake now the control port will be open for communication.

Management frame	74:3e:2b:23:13:a8	Beacon frame	ff:ff:ff:ff:ff:ff	V-home	Beacon frame, SN=3046, FN=0, Flags=.....
Management frame	74:3e:2b:63:13:a8	Beacon frame	ff:ff:ff:ff:ff:ff	Ruckus	Beacon frame, SN=771, FN=0, Flags=.....
Management frame	74:3e:2b:a3:13:a8	Beacon frame	ff:ff:ff:ff:ff:ff	PRINTERS	Beacon frame, SN=1237, FN=0, Flags=.....
Management frame	74:3e:2b:a3:13:a8	Authentication	cc:08:8d:53:66:1d		Authentication, SN=0, FN=0, Flags=.....
Control frame		Acknowledgement			Acknowledgement, Flags=.....C
Management frame	cc:08:8d:53:66:1d	Association Request	74:3e:2b:a3:13:a8	PRINTERS	Association Request, SN=3992, FN=0, Flags=
Control frame		Acknowledgement			Acknowledgement, Flags=.....C
Management frame	74:3e:2b:a3:13:a8	Association Response	cc:08:8d:53:66:1d		Association Response, SN=1, FN=0, Flags=..
Management frame	74:3e:2b:a3:13:a8	Association Response	cc:08:8d:53:66:1d		Association Response, SN=1, FN=0, Flags=..
Control frame		Acknowledgement			Acknowledgement, Flags=.....C
Data frame	74:3e:2b:a3:13:a8	QoS Data	cc:08:8d:53:66:1d		Key (Message 1 of 4)
Control frame		Acknowledgement			Acknowledgement, Flags=.....C
Data frame	cc:08:8d:53:66:1d	QoS Data	74:3e:2b:a3:13:a8		Key (Message 2 of 4)
Data frame	cc:08:8d:53:66:1d	QoS Data	74:3e:2b:a3:13:a8		Key (Message 2 of 4)
Control frame		Acknowledgement			Acknowledgement, Flags=.....C
Data frame	74:3e:2b:a3:13:a8	QoS Data	cc:08:8d:53:66:1d		Key (Message 3 of 4)
Control frame		Acknowledgement			Acknowledgement, Flags=.....C
Data frame	cc:08:8d:53:66:1d	QoS Data	74:3e:2b:a3:13:a8		Key (Message 4 of 4)
Control frame		Acknowledgement			Acknowledgement, Flags=.....C
Data frame	cc:08:8d:53:66:1d	QoS Data	b4:30:52:cd:f8:94		QoS Data, SN=2193, FN=0, Flags=.p....F.C
Control frame		802.11 Block Ack			802.11 Block Ack, Flags=.....C
Data frame	cc:08:8d:53:66:1d	QoS Data	34:2d:0d:56:88:cd		QoS Data, SN=977, FN=0, Flags=.p....F.C
Control frame		Acknowledgement			Acknowledgement, Flags=.....C
Data frame	cc:08:8d:53:66:1d	QoS Data	54:88:0e:00:1e:ae		QoS Data, SN=3802, FN=0, Flags=.p....F.C

(Full conversation from association to complete 4-way handshake)

Post Views: 50,172

Posted in Wi-Fi Blog (https://www.wifi-professionals.com/category/general)

POST NAVIGATION

Inverse Square Law (https://www.wifi-professionals.com/2018/11/inverse-square-law)

802.11 Topologies AKA Service Sets (https://www.wifi-professionals.com/2019/03/802-11-topologies-aka-service-sets)

34 THOUGHTS ON “4-WAY HANDSHAKE”

BestCliff (https://tinyJoel.blogspot.com) says:
2nd August 2019 at 5:30 am (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-167)

I see you don’t monetize wifi-professionals.com, don’t waste your traffic, you can earn additional bucks every month with new monetization method.
This is the best adsense alternative for any type of website (they approve all sites), for more info simply search
in gooogle: murgrabia’s tools

BestClarissa (https://MightyElouise.blogspot.co.uk) says:
5th August 2019 at 6:31 am (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-173)

I see you don’t monetize wifi-professionals.com, don’t waste your traffic, you can earn extra cash every month with new monetization method. This is the best adsense alternative for any type of website (they approve all sites), for more details simply search in gooogle:
murgrabia’s tools

asdsad says:
29th August 2019 at 6:03 pm (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-210)

That was the best explanation i found online , thanks

Peih says:
16th September 2019 at 8:39 am (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-252)

Thank you so much for your interpretation.

Anonymous says:
4th November 2019 at 7:39 am (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-401)

Excellent. your explanation is crystal clear.
Thank you

Anonymous says:
9th November 2019 at 5:34 am (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-432)

Thanks!

Pingback:Kali Linux on RasperryPi – Understand 802.11 – CUNG HOC ESP32 (http://cunghocesp32.com/kali-linux-on-rasperrypi-understand-802-11/)

Denniis (https://ranmcotech-distributors.business.site/) says:
5th December 2019 at 2:58 am (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-540)

The best explanation. I understood and on the way to pass the exams

Denniis (https://ranmcotech-distributors.business.site/) says:
5th December 2019 at 3:19 am (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-541)

Came here looking for the meaning of Anounce and Snounce and just got lost in the superb explanation until now, its when I remembered what I was looking for.

Mohammed says:
29th January 2020 at 5:16 am (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-784)

Nice one, Thank you.

RaviK says:
30th January 2020 at 10:11 am (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-786)

super explanation, that to also, i never seen before in my life.

Anonymous says:
25th February 2020 at 9:21 am (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-854)

It’s good

Artur says:
19th March 2020 at 4:21 pm (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-992)

You should explain in more detail how MSK, PMK and GMK are created.

Jahanzeb says:
25th March 2020 at 2:07 pm (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-995)

Thanks for the great article. However, it is still unclear how (or at what step) the password “printer123” is used. Can you explain?

gameon says:
1st April 2020 at 7:09 am (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-999)

Amazing explanation this is what I was searching for.

But could you explain where the password “printer123” Is used in 4-way handshake or is it after that?

gameon says:
1st April 2020 at 7:38 am (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-1000)

@jahanzab I got the answer for our question. It is available in quora.

MIC and KCK is the answer.

AP knows the password because we stored the password (your wifi password) in AP configuration page.

PMK is generated by encrypting the password and then send over by PTK. Here MIC needs to validate the code at Access Point and at Client. That means MIC carries the encrypted password which was created by KCK (key confirmation key).

Now let’s say using aireplay we capture the handshake and CAP file is stored offline.

Aircrack brute force will create a virtual AP and Client in our PC and they will do the 4 way handshake but here each time a new MIC (password from brute force file) will be used to compare with actual MIC in CAP file. Once the password matches bruteforce will show the password.

Quora guy explained even in more detail. Check out his answer

Julio says:
2nd April 2020 at 9:42 pm (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-1002)

@gameon, I also have the same question, can you link to the Quora answer?
Also, I understand all 4 messages but I don’t see how both ends apply the “PRF”. The post says “PRF is a pseudo-random function which is applied to all the input.”, but they are lot’s of them,

how do they know what pseudo-random function to use for the given inputs.

Great article, thanks and keep it up!

Mohammed says:
13th April 2020 at 6:50 pm (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-1020)

very good one. Thanks

Kabir says:
14th May 2020 at 6:00 pm (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-1048)

hey can anybody help me out , i want to know that do wep also used 4 way handshake. I know that wpa/wpa2 uses it but what about “wep”.

Xavier says:
28th May 2020 at 3:19 pm (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-1103)

When do the EAPOL_START message is send from supplicant to AP? Is it immediately after the the authorization and association? Does all devices send EAPOL_START?

The Holy Ghost says:
22nd June 2020 at 8:23 am (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-1153)

Where does PBKDF2 come in to this?

Sandy says:
19th July 2020 at 9:08 pm (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-1204)

My Question is , how MIC value is calculated in 3 Msgs (Msg2-4) and validated at opposite ends ? If any new client joins the BSS , Will AP generate new GTK and shared with all clients or already cretaed GTK shared to the new client ?

Alex Tse says:
3rd August 2020 at 5:33 am (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-1230)

hi, so where is AES used in the 4 way handshake?
i though PTK is xor stream cipher, isn’t it?

man says:
30th August 2020 at 10:24 am (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-1282)

perfect! thank you

admin says:
23rd September 2020 at 2:39 pm (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-1340)

@Sandy
The authenticator sends an EAPOL – Key frame to the supplicant containing the ANonce, the authenticator ' s RSN information element capabilities, and a MIC. This would be last verification before the key installed by the station.
Regarding GTK:
The authenticator can update the GTK for a number of reasons. For example, the authenticator may change the GTK on disassociation or deauthentication of a client station. WLAN vendors may also offer a configuration setting to trigger the creation of a new GTK based on a timed interval.
I don't believe GTK will be changed if a new client is joining the BSS but certainly can be tested to verify that.

admin says:
23rd September 2020 at 2:48 pm (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-1342)

@Julio
This article might help understand how PRF function will be used…

http://etutorials.org/Networking/802.11+security.+wi-fi+protected+access+and+802.11i/Part+II+The+Design+of+Wi-Fi+Security/Chapter+10.+WPA+and+RSN+Key+Hierarchy/Computing+the+Temporal+Keys/ (http://etutorials.org/Networking/802.11+security.+wi-fi+protected+access+and+802.11i/Part+II+The+Design+of+Wi-Fi+Security/Chapter+10.+WPA+and+RSN+Key+Hierarchy/Computing+the+Temporal+Keys/)

admin says:
23rd September 2020 at 6:45 pm (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-1346)

Hi @Alex Tse,
AES is not involved in the process of a 4-way handshake but being used for data encryption. AES (Advanced Encryption Standard) is just the encryption method used in this security method.

So if I summarize:

IEEE 802.11 security has:
.Robust security network and Robust security network has:
.IEEE 802.1X (authentication with AD or server etc), TKIP and WPA2 etc.
.WPA2 mandates the use of a new protocol, counter mode with cipher-block chaining message authentication protocol (CCMP)and CCMP uses the AES block cipher.
It should be understood that AES is a standard and not a protocol. A protocol is a series of steps designed to achieve a specific end, while a standard is a set of rules and guidelines that define an overall design structure. The AES standard specifies the use of the Rijandel symmetric block cipher that can process data blocks of 128 bits, using cipher keys of 128, 192, and 256 bits.
It means it takes a text of 128bits and then use cipher keys of 128, 192, and 256 bits to change that text into cipher text so it can not be read by the intruders.
hope this helps.
Regards.
.

Anonymous says:
25th September 2020 at 1:22 am (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-1358)

thanks

NN says:
12th October 2020 at 5:43 pm (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-1412)

Thank you for this enriched post. I have a little question about the three keys that will eventually be derived from the PTK. One of them is called the EAPOL KEK, which is used for encrypting keys. My question is, when will KEK be used? and for what keys will it be protecting?

Thank you for spreading your knowledge,

admin says:
16th October 2020 at 12:51 pm (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-1428)

HI,
I hope you are well.
Thanks for your question.
I think it's good to discuss these topics openly like this so people can benefit from this.
as you know PTK is consists of 3 sections or Keys.
1- KCK (Key confirmation key): From the name confirmation you can guess that it is used to confirm something. so this is the key used during a 4-way handshake and group key handshake for data integrity.
2- KEK (Key encryption key): This key also used during a 4-way handshake and group key handshake for data privacy.
3- TK (Temporal Key): This key is used to encrypt and decrypts the actual payload between the station and the access point (supplicant).

you should be able to find this information in CWNP security book (CWSP).

NN says:
16th October 2020 at 8:09 pm (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-1431)

Thank you for your reply. Regarding using those keys in the 4-way handshake, is it the same handshake explained in this site and the book as well? If so, I am confused about how we initially use those keys during the handshake while this handshake is supposed to generate them at the end.

Thank you again,

admin says:
17th October 2020 at 4:31 pm (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-1433)

Hi,
I believe you are right to be confused once you start looking into the keys and the names. Different names confuse me all the time. I wish they can use easy (IN ENGLISH) terminologies. PTK is not generated at the end of 4-way handshake but it will be created after message 1 and 2.

1- After message 1 Station has the required information to generate PTK so it can derive all other keys after message 1 of 4way handshake.
2- After message 2 of 4-way handshake now access point also has required information to generate PTK and then from PTK it can generate all other keys.
3- Message 3 is where GTK will be sent to the station and that's where KEK will be used to encrypt GTK.

There is another blog which has written about further key generations. I believe It will answer your questions.
https://praneethwifi.in/2019/11/08/4-way-hand-shake-keys-generation-and-mic-verification/ (https://praneethwifi.in/2019/11/08/4-way-hand-shake-keys-generation-and-mic-verification/)

Anjali says:
30th October 2020 at 1:26 am (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-1488)

Hi…

Great article…

I have doubts when we say the PTK or GTK will be, " installed". Consider if I am using a linux based system with a specific vendor chip.. Where exactly the interim or final keys are stored and how?

admin says:
2nd November 2020 at 1:48 pm (https://www.wifi-professionals.com/2019/01/4-way-handshake#comment-1502)

Hi Anjali,
As you know PTK and GTK are not permanent keys and will be changed depending on the situation.
If the device roams or disconnects then new keys will be generated. Keys are normally stored in the cache and will be dropped when there is a need for generating a new key.

Leave a Reply

Your email address will not be published.

Comment

Name

Email

Website

Save my name, email, and website in this browser for the next time I comment.

Replies to my comments Notify me of followup comments via e-mail. You can also subscribe (https://www.wifi-professionals.com/comment-subscriptions/?srp=494&srk=dc81194fcaedadf5c0206f1cc4a46ca1&sra=s&srsrc=f) without commenting.

POST COMMENT

Search …

RECENT POSTS

Wireless broadband alliance conference (https://www.wifi-professionals.com/2019/09/wireless-broadband-alliance-conference)

Wi-Fi 6 certification is ready (https://www.wifi-professionals.com/2019/09/wi-fi-6-certification-is-ready)

WiFi 6 devices are on way… (https://www.wifi-professionals.com/2019/09/wifi-6-devices-are-on-way)

About (https://www.wifi-professionals.com/2019/08/about)

BSS Colouring or Spatial reuse (802.11ax AKA WiFi6) (https://www.wifi-professionals.com/2019/07/bss-colouring-or-spatial-reuse-802-11ax-aka-wifi6)

MOST VIEWED POSTS

4-Way Handshake (https://www.wifi-professionals.com/2019/01/4-way-handshake) (50,172)

Wireshark Display Filters (https://www.wifi-professionals.com/2019/03/wireshark-display-filters) (15,913)

Home (https://www.wifi-professionals.com/) (15,420)

SSIDS overhead effect on channel utilisation (https://www.wifi-professionals.com/2018/08/ssids-overhead-effect-on-channel-utilisation) (4,946)

BSS Colouring or Spatial reuse (802.11ax AKA WiFi6) (https://www.wifi-professionals.com/2019/07/bss-colouring-or-spatial-reuse-802-11ax-aka-wifi6) (4,443)

CATEGORIES

CWNP Exams Prepration (https://www.wifi-professionals.com/category/cwne-journey)

Home WiFi (https://www.wifi-professionals.com/category/home-wifi)

News (https://www.wifi-professionals.com/category/news)

Uncategorised (https://www.wifi-professionals.com/category/uncategorised)

Wi-Fi Blog (https://www.wifi-professionals.com/category/general)

Wi-Fi Fun (https://www.wifi-professionals.com/category/fun)

Youtube channels (https://www.wifi-professionals.com/category/youtube-channels)

ARCHIVES

September 2019 (https://www.wifi-professionals.com/2019/09)

August 2019 (https://www.wifi-professionals.com/2019/08)

July 2019 (https://www.wifi-professionals.com/2019/07)

June 2019 (https://www.wifi-professionals.com/2019/06)

May 2019 (https://www.wifi-professionals.com/2019/05)

April 2019 (https://www.wifi-professionals.com/2019/04)

March 2019 (https://www.wifi-professionals.com/2019/03)

January 2019 (https://www.wifi-professionals.com/2019/01)

November 2018 (https://www.wifi-professionals.com/2018/11)

October 2018 (https://www.wifi-professionals.com/2018/10)

August 2018 (https://www.wifi-professionals.com/2018/08)

July 2018 (https://www.wifi-professionals.com/2018/07)

June 2018 (https://www.wifi-professionals.com/2018/06)

May 2018 (https://www.wifi-professionals.com/2018/05)

April 2018 (https://www.wifi-professionals.com/2018/04)
