An analysis of security challenge and solution for Wi-Fi

Diwash Bikram Basnet

Department of Network and Computer Security

SUNY Polytechnic Institute

Utica, NY, USA

Abstract— *In this paper, we will discuss Wi-Fi security schemes such as WEP, WPA, and WPA2, also a brief discussion of common attacks on Wi-Fi. The four-way handshake in WPA2 which negotiate a secret between a client and an access point is implemented wrongly for past almost two-decade can be exploited by an adversary by forcing nonce reuse via a replay attack. The WPA2-PSK is vulnerable to key re-installation attack than WPA2-Enterprise. This paper also shows the preliminary attack on the four-way handshake to understand how we can find devices are vulnerable to KRACK attack and patch it before any attacker could attack us. The solution is to use WPA3 if possible because it has many more additional features added to it such as SAE, PMF, PFS and so on.*

Keywords—*KRACK (key re-installation attack), PMK (pairwise master key), wi-fi protectected access (WPA), WEP (wired equivalent privacy), Wi-Fi (wireless fidelity), PTK (pairwise transient key), AP (access point), DH (Diffie-Hellman), EAP (extensible authentication protocol*

I. INTRODUCTION

Wireless Communication is omnipresent and very popular because wireless devices are very portable and efficient compared to wired devices. Wireless technology can found in areas where wired technology has not even reached. There are two types of network used for communication are wired network and wireless network. The wireless network includes cellular networks, the Wi-Fi network, satellites networks and many more. For the wired network, a station must be physically connected to the LAN (local area network) to transmit or receive data, whereas, in a wireless network, a station can transmit to another device within a radio range. The wired networks are considered more secure compared to wireless networks wireless network traffic transmits or receive the traffic over the air, and it is straightforward for an adversary to eavesdrop and intercept the traffic. Therefore, there is a strong need for securing this technology [19].

Wireless security is the prevention of unauthorized access and protection of computer hardware which uses a wireless network Wireless security is necessary and relevant because a user transmit or receive the sensitive information across a network and it is vulnerable to some attacks. The attacker can eavesdrop and wait patiently to exploit any vulnerability on such network and loot all the sensitive information. Since wireless networks use the open air as the medium for transferring the information, attacks such as evil twin wireless attack, MITM (man-in-the-middle), spoofing or few using some tools on our wireless traffic are possible. There are many active and passive attacks possible on the Wi-Fi, and briefly discuss on some of the standard wireless network attacks.

a) Evil twin wireless attack: The adversary sets up a fake access point using the same SSID of the real point and with no authentication. For this attack, the fake access point needs to be closer to a victim, so that victim automatically connects to the strongest Wi-Fi signal. When the victim is tricked into using the fake access point and logs into the email or bank account using unsecured (HTTP) connection, the adversary intercepts the traffic and gains sensitive information [1].
b) Man-in-the-middle attack: The attacker uses tools such as arp-spoof and acts as the internet gateway and client at the same time. The attacker sends the message to the victim saying he/she is the gateway and fools gateway by saying he/she is the victim. So both gateway and victim's traffic go through the attacker and capture all the essential traffic [2].
c) Wi-Fi Jamming: The attacker can jam a wireless network by flooding the access point with de-authentication frames. The attacker will send many de-authentication frames to the access point, acting like a real device wishing to disconnect and prevent the legitimate user from using the access point [3].

This paper discusses the standards used such as WEP, WPA and WPA2 to secure the Wi-Fi connections, drawbacks of the standards, and mitigation techniques. Currently, Wi-Fi uses WPA2 (Wi-Fi Protected Access version 2) is used to encrypt the data frame to protect the data confidentiality, authentication, and integrity of the message. The access point and the devices need to negotiate the key-exchange in order to communicate securely; the exchange of keys happen during the four-way handshake and those keys are used to encrypt or decrypt the data [4].

In the recent year, the security researcher has found the vulnerability in message handshake of WPA2 and published a paper "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2". This paper can be useful to IT security teams, who are responsible for installing, configuring and securing the Wi-Fi system in the organization. Scholars and IT professionals who are in the information security field and want to refresh or sharpen their knowledge in the wireless security domain.

The goal for this paper is to share the fundamental knowledge on the Wi-Fi standards and the security risk associated with four-way message handshake in WPA2 and exploit the vulnerability and mitigation techniques. This paper also discusses the recently standardized WPA3 and how it will solve the security issues with WPA2 such as offline brute dictionary attack, KRACK attack, de-authentication attack and few other.

II. BACKGROUND

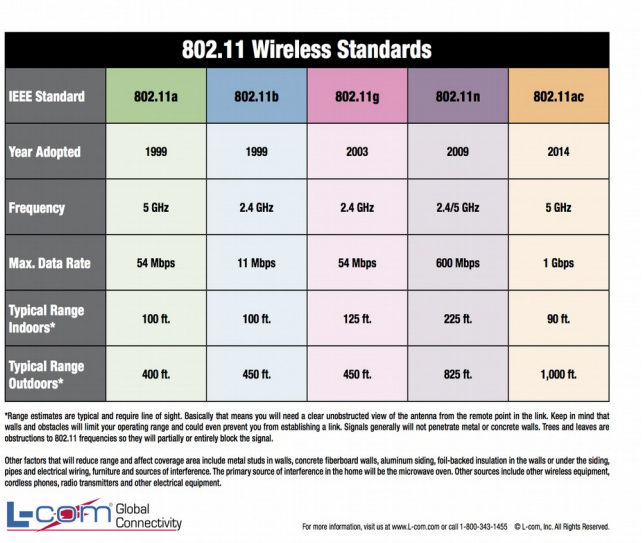
In 1990, the IEEE (Institute of Electrical and Electronics Engineers), formed a new working group IEEE 802.11 to develop a protocol and transmission specification for wireless LANs [17]. Wi-Fi supports three different security schemes are: Wired Equivalent Privacy (WEP), WPA and WPA2 (version 2) to encrypt our traffic over the air. When the device sends the data to the access point or router over-the-air, it gets encrypted by one of these security schemes. Once the AP gets the data and forwards the packet to the Internet, these security schemes are not involved [8].

802.11 defined WEP as the first encryption algorithm to maintain the privacy of user transmitting information over the air. WEP has weakness in exchanging the key safely and has security vulnerabilities. The Wi-Fi alliance created WPA to

eliminate the security issues of 802.11i. It uses RC4 stream cipher with an additional layer of encryption Temporal Key Integrity Protocol (TKIP), which use a 256-bit key and generate a unique key for each packet, message integrity check and more. The Wi-Fi Alliance certifies vendor under the WPA2 program, [9] which is a successor of WPA. WPA2 replaces RC4 and TKIP with Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) and Advanced Encryption Standard (AES). CCMP ensure the integrity of the message, whether the message did not get modified by the attacker, and AES is used to encrypt and decrypt the data in a block of 128-bits, with the key size of 128, 192 or 256-bits [9].

WPA2 provide more seamless roaming which allows clients to move from one access points to another without having the trouble of reconnecting and re-authenticate using the pairwise master key (PMK) caching or pre-authentication. Currently, WPA and WPA2 are two encryption algorithm with two different modes: personal and enterprise [9]. WPA2 enterprise mode is more secure than WPA2 personal because the user not only needs to provide the single password to connect to AP, but also the user-id and password provided by RADIUS server in order to authenticate, and is more difficult to break than just passphrase.

If a user has an old device and does not support WPA2, then they can use WPA-PSK to communicate wirelessly. However, in order to make communication secure using WPA-PSK, a user should create a long and complex password that includes all the lower, upper case letters, numbers, punctuation, not a dictionary word and difficult to guess or brute-force by an attacker. As of today, WPA2 is considered the most secure wireless security standard even there exist some vulnerabilities.



802.11 Wireless Standards

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors*	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Typical Range Outdoors*	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

*Range estimates are typical and require line of sight. Basically that means you will need a clear unobstructed view of the antenna from the remote point in the link. Keep in mind that walls and obstacles will limit your operating range and could even prevent you from establishing a link. Signals generally will not penetrate metal or concrete walls. Trees and leaves are obstructions to 802.11 frequencies so they will partially or entirely block the signal.

Other factors that will reduce range and affect coverage area include metal studs in walls, concrete fiberboard walls, aluminum siding, foil-backed insulation in the walls or under the siding, pipes and electrical wiring, furniture and sources of interference. The primary source of interference in the home will be the microwave oven. Other sources include other wireless equipment, cordless phones, radio transmitters and other electrical equipment.

L-com Global Connectivity

For more information, visit us at www.L-com.com or call 1-800-343-1455

Figure 1. 802.11 wireless standards [6].

From the above diagram, there are different versions of 802.11 wireless standards. Although 802.11b and 802.11a were released in the same year 1999, 802.11b was the first 802.11 standard to accepted by all the vendors because it was inexpensive and have adopted by the consumer market. 802.11b works frequency in 2.4 GHz and cover more range, but easily absorbed by walls and solid objects than 802.11a. 802.11b is a better option for outdoor, but 2.4GHz react better with water and may disturb the transmission.

802.11g was released in 2003 and runs on 2.4GHz and has a throughput of 54Mbps, and backward compatible with the previous version. 802.11n released in 2009 and had a higher throughput of 600Mbps. Since it operates in both frequency bands 2.4 GHz and 5 GHz, it has better indoor and outdoor coverage. This technology uses MIMO (multiple-input multiple outputs), which can send and receive multiple wireless signals on the same channel at the same time [6].

802.11ac is the recent standard by Wi-Fi Alliance that was adopted in 2014 and only uses the frequency band of 5 GHz. It provides excellent coverage outdoor but not indoor because solid objects readily absorb the signals in 5 GHz. It uses MU-MIMO (Multi-user MIMO), a set of users of wireless terminal communicate with each other using one or more antennas [6].

When a client wants to connect to an access point, it sends an authentication request to the access point, and access point replies to the client with an authentication response. After that, the client sends an association request to the AP and AP send back an association response. They now established an agreement, but they have not negotiated key-exchange. WPA or WPA2 turned some keying source material into a data encryption key and encrypt our data frame. On WPA and WPA2,

A. Four-way Handshake in WPA and WPA2

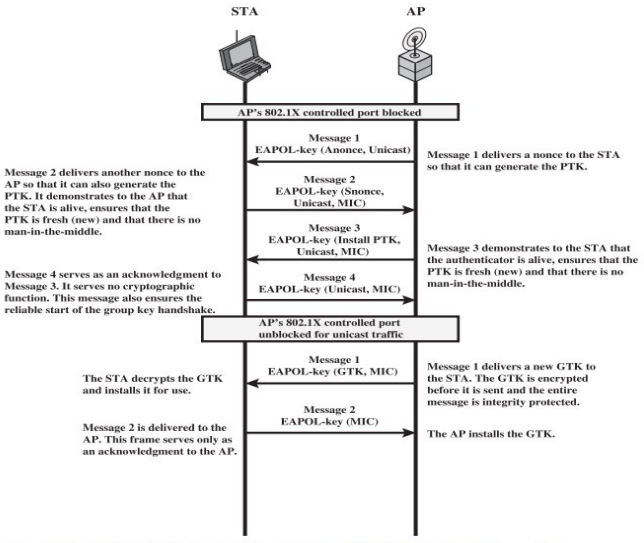


Figure 17.9 IEEE 802.11i Phases of Operation: Four-Way Handshake and Group Key Handshake

Figure 2. Four-way handshake

Whether it is Personal or Enterprise, there is the authentication process that derived the source keying material, i.e., PMK (pairwise master key). In WPA or WPA2 Personal

network, the PMK is derived from the passphrases, whereas in an enterprise network, the MSK (master session key) derived from EAP (extensible authentication protocol) exchange and the PMK derived from the MSK. So, both the station and access point are going to know the PMK, without sharing over the wireless medium. In WPA and WPA2 Personal mode, the four-way handshake happens after the association, whereas in an enterprise mode, the four-way handshake happens after the successful 802.1x EAP authentication.

The four-way handshake is essential in creating data encryption key by exchanging the information between the client and the access points [6]. In order to create the unicast and group encryption key, the station and the access point need some inputs which are needed to create the encryption key such as PMK, ANonce, SNonce, Authentication MAC address, Supplicant MAC address. The AP (Access point) start exchanging information by sending ANonce (authenticator nonce) which is pseudorandomly generated number by the AP to the station/supplicant and used as an input to the encryption key. Since they are communicating via a wireless medium, supplicant can get the MAC address of authenticator and vice versa. Now that the supplicant has all of the input to create a unicast encryption key, it generates the PTK (pairwise transient key) which consist encryption keys for a different function such as unicast encryption, and data protection. Supplicant responds to access point by sending its SNonce (supplicant random number) and protect with MIC (message integrity code). The access point got the SNonce from the supplicant, AP calculate it's PTK and validate the MIC to ensure there is no modification in the transit. Now, PTK is used for unicast encryption to send from source address to a single destination address.

They also need group key and are used for multicast communication to send MPDUs (MAC protocol data unit) from one station to multiple stations [17]. MPDU is responsible for assembling the data frame while on the transmission with address and error detection fields. The access point calculates GTK (group temporal key) that is used to encrypt and decrypt the multicast and broadcast traffic, aside from four-way handshake and sent to the supplicant with the MIC to protect the frame. Group temporal key change every time a device leaves the network. After supplicant has received the GTK and installed it, it is ready to transmit the encrypted data frames to access point [6]. The PSK (pre-shared key) is defined with the PMK, whereas in EAPOL (extensive authentication protocol over LAN), the PMK derived from the 802.1x EAP. EAPOL is much more difficult to crack than using PSK. There is a calculation to generate the PMK from the PSK:

PMK (master key) = PBKDF2(PSK, Salt, 4096, 256) [11]

where HMAC-SHA1: The Hashing function
PSK: the passphrase
Salt: name of the access point
4096: number of iterations of the hashing method
256: length of the key
PBKDF= Password-based key derivation function (Key stretching)

According to the [17], that is how station calculates the pairwise transient key for CCMP using the "PRF (pseudorandom function), which take four parameters as input and produces the number of random bits." The function is in the form of PRF (K, A, B, Len).

PTK (session key) = PRF-512 (PMK, Min (AP_Mac1, Client_Mac2) | | Max(AP_Mac1, Client Mac2) | | Min(ANonce1, SNonce2) | | Max(ANonce1, SNonce2), 384)

where K = PMK (master key)
A = the text string
B = a sequence of bytes (concatenated by AP and station MAC address and nonce's)
Len = 384 bit (number of pseudo-random bits) [17]
Similarly, a nonce is generated by
Nonce =PRF (RandomNumber, MAC | Time, 256)
Time = network time
To calculate the group temporal key,
GTK =PRF (GMK, MAC | GNonce, 256)

B. KRACK ATTACK

Even though WPA2 is considered the most secure wireless security and which is an almost two-decade-old standard used by most Wi-Fi devices, but security researchers have found a vulnerability in message handshake of WPA2. This attack takes advantages of flaw existed in the handshake protocol that forces nonce reuse via a replay attack. The Key re-installation attack (KRACK) exploit the 4-way handshake, a process between a device and a router which is designed to get the new encrypted session key. According to Mathy Vanhoef, "An adversary tricks a client into reinstalling an already-in-use key by manipulating and replaying handshake messages. When a client reinstalls the key, an associated parameter such as the incremental transmit packet number (nonce) and receive packet number reset to the all-zero encryption key." With an unencrypted session, the adversary can intercept the communication and may steal critical information. The KRACK attack can decrypt and even forge packet encrypted with WPA-TKIP and Galois/Counter Mode Protocol (GCMP). It also can decrypt the packet but cannot forge it if a packet encrypted with AES-CCMP [15].

An adversary may not need to be within the range of targeted Wi-Fi networks to use this attack; they may use an antenna to boost their range to 2-3 miles. It is not a security bug but a critical protocol problem. So, this is what happens when a client joins a network, and the four-way handshake takes place to get a fresh session key. It will install the key after receiving the third message of four-way handshake. After the key has been installed, it will be used to encrypt and decrypt the traffic. If the packet is dropped or lost in- between the transmission, and if the access point did not get a response back then it will re-transmit the message. A client receives the message three multiple times and reinstalls the same session

key [15]. An adversary can take advantage by forcing these nonce resets by collecting and replaying the third message. The data-confidentiality protocol can attack by forcing nonce reuse, and an adversary can replay, decrypt, and forged the packets. The same force nonce reuse technique can be used to attack group key, peer-key, and fast BSS transition handshake.

C. WPA3

WPA3 is the solution for most of the vulnerabilities existed in the WPA2. Every vendor is eagerly waiting for the WPA3 security scheme and protect against the vulnerabilities found in the WPA2. WPA3 was released in 2018, and an enhancement to its predecessor WPA2. There are many new features added to WPA3 are:

1) Improved Message Handshake:

WPA3 uses simultaneous authentication of equal (SAE) for key exchange instead of the pre-shared key. SAE handshake is the variant of the Dragonfly handshake, which defined in RFC 7664 [12]. In the Wi-Fi network, the SAE negotiate fresh PMK, which will then be used in the traditional four-way handshake to generate PTK or session keys. The 32-byte PMK cannot be guessed by an attacker using any dictionary-based attacks. Since the PTK/session keys derived from PMK, the passphrase used in the four-way handshake cannot be recovered [12]. SAE handshake prevents offline dictionary attack and also provide perfect forward secrecy (PFS) such that if an attacker gets hold of the password, but they cannot use that password to decrypt an old message.

2) Stronger encryption key:

WPA3 uses 128-bits AES encryption with the personal mode for confidentiality and optional 192-bit encryption with an enterprise network. WPA3 enterprise mode does not use Simultaneous Authentication of Equals (SAE), but it uses the 802.1x authentication and a four-way handshake similar to the WPA2 enterprise. All the client, RADIUS server and access points need to use at least 192-bit key, so there is no weak link between them. Otherwise, there will be no connection between them. It uses 192-bit AES with GCMP-256, HMAC-SHA-384 with ECDSA-384 bit [14].

3) Protected Management Frame:

In WPA3 both personal and enterprise mode, they activate the use of protected management frame (PMF) to ensure the integrity of the network traffic, protect against forging of management frames. PMF protect users from de-authentication attacks where an adversary can force a user to disconnect from a connected network [12].

4) Secure Public Wi-Fi:

Open authentication is used in public networks such as coffee shop and library so that a device and an access point can communicate without any encryption. WPA3 has a new feature called opportunistic wireless encryption (OWE) that uses the Diffie-Hellman key exchange to encrypt and decrypt the messages between a device and an access point. Each device has a different decryption key, and even if an attacker intercepts the messages, they cannot read the contents because they do not have the decryption key. In WPA3, when users are surfing the internet using an open network, the Diffie-Hellman key exchange happens in the background and encrypts all the communication to an access point. However, it may not work against the rogue access point which tricks a user to connect to an attacker's fake AP and acquire the sensitive information [13].

5) WPA2 Key -Exchange vs WPA3 Key-Agreement

In WPA2, the passphrase derives the session keys that are used to encrypt or decrypt the information. If somehow, the attacker gets hold of that passphrase then they can eavesdrop on not only on the single user but also on another user who is in the same LAN using the same access point. The client and AP negotiate session keys derived from the passphrase and are used to encrypt or decrypt the private messages. So if an attacker got that secret passphrase, they could decrypt all the private information of the user.

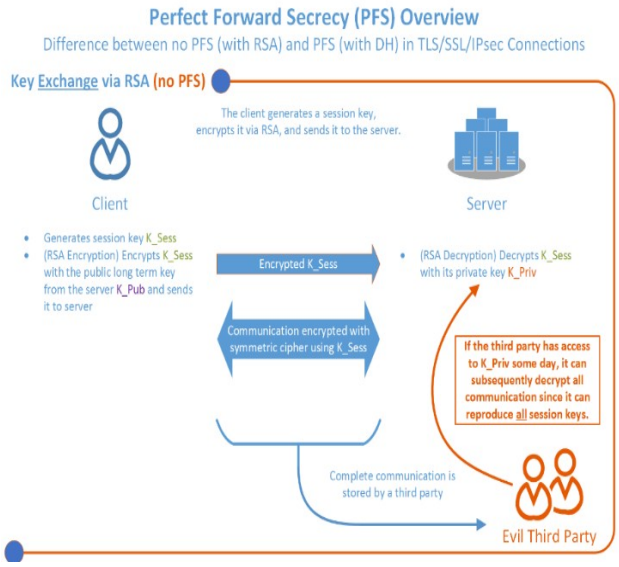


Figure 3: Key-exchange via RSA

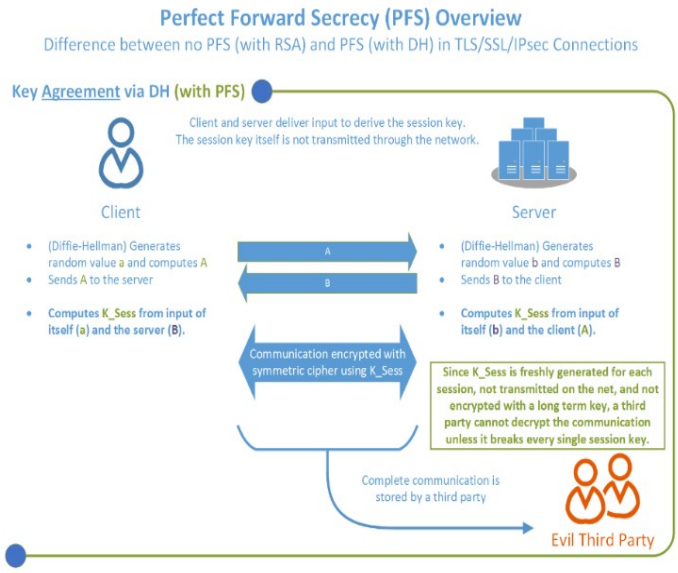


Figure 4: Key-agreement via DH

The above diagram describes perfect forward secrecy (PFS) with Diffie-Hellman (DH) in TLS (transport layer security) /SSL (secure socket layer)/IPsec (internet protocol security) connection, but similar key-exchange happens in WPA3. In order to get PFS, the client and access point agreed to exchange keys through DH cipher suite first, and the client generates random value "a" and compute "A" using the known prime number and modulo and sends the computed value "A" with known prime and modulo to the AP. Similarly, the AP generates random value "b" and computes "B" using the same known prime number and modulo and sends "B" to the client. Now, they have successfully exchanged the computed value to each other. The client computes k_session or pre-master key from the input of "a" and "B," and the access point computes k_session or pre-master key from the input of itself "b" and "A." They started communicating encrypted with advanced encryption standard (AES) symmetric cipher using k_session. Since k_session is freshly generated for each session with a new random value, even if the attacker got one correct random number, they could only decrypt for the particular session. Therefore, using DH key exchange, we can achieve the PFS in WPA3.

III. PROPOSED WORK

A. Implementation projects:

Since the security researcher has not uploaded the script for KRACK attack, therefore this project does not demonstrate the actual KRACK attack here. However, this project will run a few scripts to check whether the devices are vulnerable to the KRACK attack or not. Currently, in a home or maybe a school's wireless routers or access points use WPA2-PSK. With that in mind, the author did not release the attack script [16], since it would create fear among wireless users.

Therefore, the security researcher has informed the device vendors about the flaws and released the code to check if the device is vulnerable or not. The project uses the script to check if clients or access points (APs) are affected by the KRACK attack using nonce reuse against WPA2.

This project demonstrates how to know if our devices are vulnerable to KRACK attack and what we need to perform to prevent from that attack. This paper does not discuss the all-zero-key re-installation, which allow an attacker to decrypt all the data from the victim [15]. In this preliminary attack, we use a kalilinux as an attacker and a smartphone as a client. Therefore, we configure the kalilinux to act as a fake AP and connects our client to it and observe if the client reuse IV (initialization vector) or not. If the client does reuse IV, then it is vulnerable to the KRACK attack which is the primary goal of this project.

Firstly, we will update the kalilinux using apt-get update command

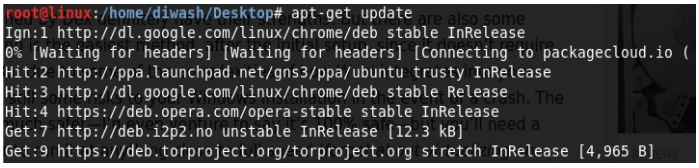


Figure 5: Updating Kalilinux

Then we will install some dependencies required for this test

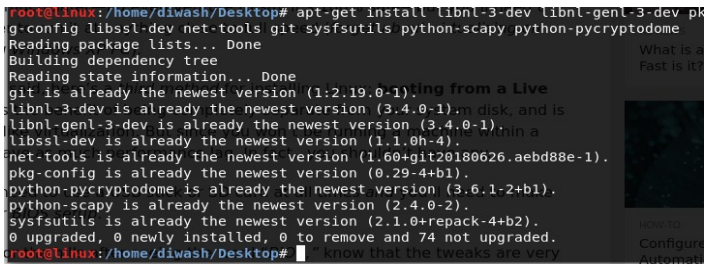


Figure 6: Installing dependencies

Then we will download the script for the test from GitHub that is provided by the author [16].

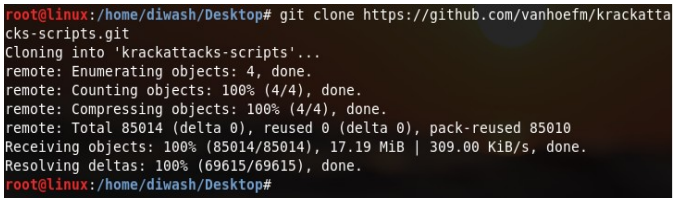
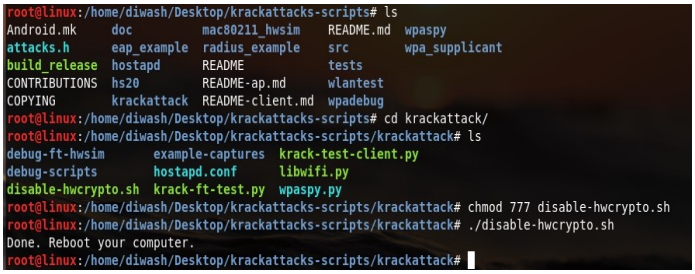
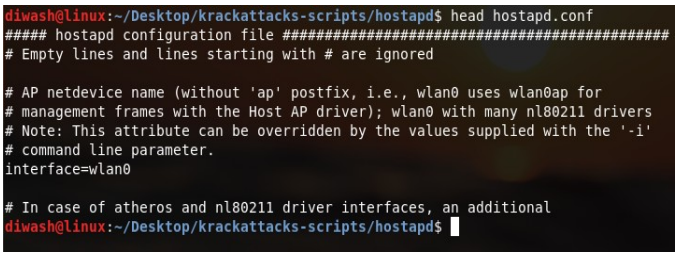


Figure 7: Downloading the scripts

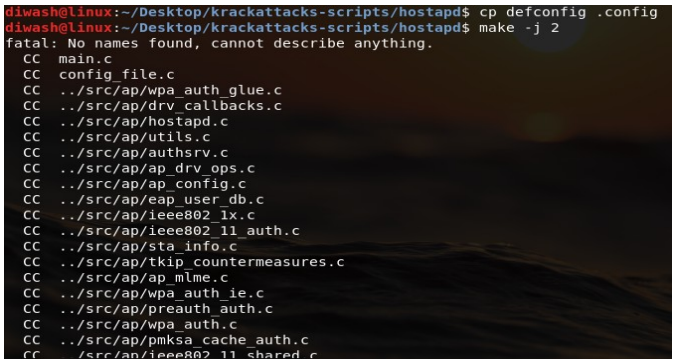
As per the instruction, we gave the full permission to read, write and execute using **chmod 777** ***filename*** and to disable-hwcrypto.sh, then ran the command the ***./disable-hwcrypto.sh***.

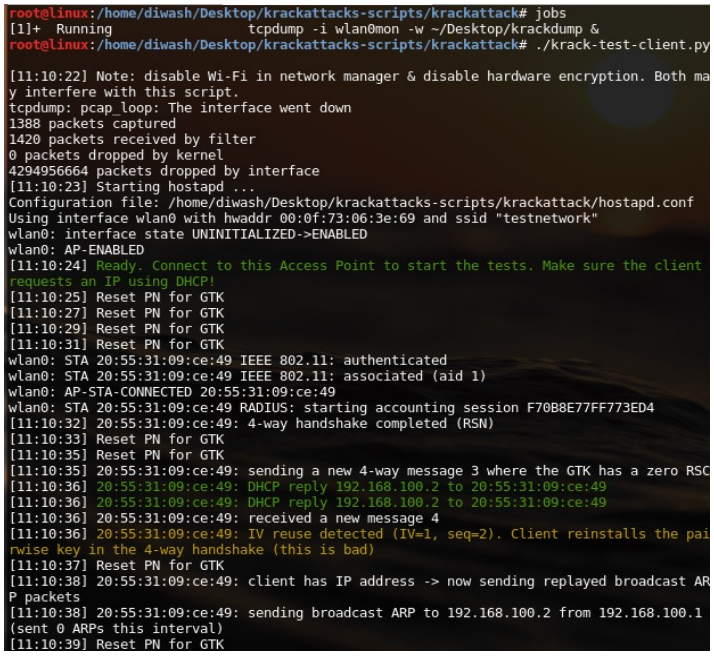


Now we are editing the **hostapd.conf** the configuration file and changing the interface to wlan0 to create a fake AP. Once the script started, the testing device must connect to SSID ***testnetwork*** with a password of ***abcdefgh*.**



Now, we will copy the defconf to .config and compiling the source code with **make** command.





We are running ***tcpdump-i wlan0mon*** on background to monitor and ran the ***./krack-test-client.py,*** python program to start the testing script. This tests is used for key reinstallations in the 4-way handshake by repeatedly sending encrypted message 3's to the client. In the screenshot above, we can see that the fake access point is started and when the victim's smartphone connects to this AP. It starts the authentication and association and after that the four-way message handshake occur and we can observe that IV reuse detected and client reinstall the pairwise key in the 4-way handshake, which is the result we want to get from running this script. Hence, the preliminary attack is successful.

IV. SOLUTION

The solution is to use the update the device or the use of the virtual private network (VPN) which will encrypt all the traffic from the network layer of the TCP/IP model. We can also install HTTPS everywhere plugin in the browser, even though the adversary can listen and intercept the traffic, it will be challenging for an adversary to decrypt the packets. WPA3 protocol is out, but it will take some time for the vendor to make devices available that can support WPA3, the use of WPA3 protocol will solve the KRACK attack.

The Wi-Fi Alliance, an industry made up of device maker including Apple, Microsoft and Qualcomm announced the next-generation wireless network security standard [20]. WPA3 will replace the WPA2, the key improvement of WPA3 will solve the common security problem with open Wi-Fi networks such as an airport or a school [5]. WPA3 include individualized data encryption, so that adversary lurking on public Wi-Fi networks will find it more difficult to eavesdrop in on the wireless communication. With WPA3, a router could be configured to restrict access or even notify the user that someone was trying to access the network.

The newer WPA3 will use a new, better message handshake since the WPA2-PSK is vulnerable to brute-force dictionary attack after capturing four-way handshake for key establishment. In order to protect against such attacks, there have been many upgrades in the Wi-Fi standards from open authentication to WPA3.

V. CONCLUSION

With the increment use of the handheld device, users find Wi-Fi very convenient to use everywhere. Nowadays, most of the devices that we use in our daily life is connected to wireless technology, there exists a strong need for security schemes or technologies which protects our devices from getting attacked and prevent accessing our information, therefore the wireless security is required more than ever. When using Wi-Fi, our messages get encrypted with the WPA2 encryption algorithm, but we came to realize that an adversary can acquire our sensitive information via replay attack on four-way handshake of WPA2. The key re-installation attack exploits the vulnerability in the WPA2 message handshake which has been existed for almost two decades, and it shows that we need

more secure encryption algorithm that protects our privacy and confidentiality of our information from an adversary. The only best solution for Wi-Fi security is to use WPA3. WPA3 has recently been standardized, and the vendors are working really hard to make WPA3 enabled-router and make available to the consumers.

REFERENCES

[1] Jeremy Kirk, “Evil Twin: Wi-Fi acess points proliferate” *Network World From IDG*, Apr 25, 2007 1:00 AM PT, Availableat: https://www.networkworld.com/article/2298370/lan-wan/-evil-twin--wi-fi-access-points-proliferate.html

[2] Rick Publico, “What is a Man-in-the-Middle Attack and How Can You Prevent It?”, *GlobalSign GMO INTERNET GROUP*, Mar 1 2017, Available at: https://www.globalsign.com/en/blog/what-is-a-man-in-the-middle-attack/

[3] Jack Mahoney, “Hacking and jamming WiFi networks”, *Medium*, Jan 11 2015, Available at: https://medium.com/@jackmahoney/hacking-and-jamming-wifi-networks-d2a6ec51f0c2

[4] Bradley Mitchell, “What Does Wi-Fi Protected Access Mean?”, *Lifewire*, Nov 25, 2018, Available at: https://www.lifewire.com/definition-of-wifi-protected-access-816576

[5] Marcus, Burton, “TThe 4-Way Handshake (Marcus Burton, CWNP)”, *CWNPTV*, Nov 5, 2010, Available at: https://www.youtube.com/watch?v=9M8kVYFhMDw

[6] L-com, ”An A to Z review of the 802.11 standards”, *L-com an INFINITE brand*, May 17, 2016, Available at: http://www.l-com.com/content/Article.aspx?Type=N&ID=10638

[7] Prof Bill Buchanan OBE, “The Beginning of the End of WPA-2 —Cracking WPA-2 Just Got a Whole Lot Easier”, *Medium Cybersecurity*, Aug 7 2018, Available at: https://medium.com/@billatnapier/the-beginning-of-the-end-of-wpa-2-cracking-wpa-2-just-got-a-whole-lot-easier-55d7775a7a5a

[8] Chris Hoffman, “ Wi-Fi Security : Should You Use WPA2-AES, WPA2-TKIP or Both?”, *How-To-Geek*, july 20, 2017 , 11:04 PM, Available at: https://www.howtogeek.com/204697/wi-fi-security-should-you-use-wpa2-aes-wpa2-tkip-or-both/

[9] Jessica Scarpati, “Wireless security protocols: The difference between WEP, WPA, WPA2”, *TechTarget Search Networking, Jan 2017, Available at:* https://searchnetworking.techtarget.com/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2

[10] Johannes Weber, “At a Glance: Perfect Forward Secrecy (PFS)”, *Blog Webernetz.net*, Feb 18 2014, Available at: https://blog.webernetz.net/at-a-glance-perfect-forward-secrecy-pfs/

[11] B Kaliski, RSA Laboratories , ” PKCS #5: Password-Based Cryptography Specification Version 2.0”, *Network Working Group Request for Comments: 2898*, Sept 2000, Available at: https://www.ietf.org/rfc/rfc2898.txt

[12] Mathy Vanhoef, “WPA3: Technical Details and Discussion”, Blog, Ma3 12 2018, Availble at: https://www.mathyvanhoef.com/2018/03/wpa3-technical-details.html

[13] Dan Harkins and Warren Kumari , “Opportunistic Wireless Encryption”, *Internet Engineering Task Force (IETF)*, March 2017, Availble at: https://tools.ietf.org/html/rfc8110

[14] Mtroi, "WPA3 – Improving your WLAN security", *WLAN BY GERMAN ENGINEERING*, Sept 14 201, Available at: https://wlan1nde.wordpress.com/2018/09/14/wpa3-improving-your-wlan-security/

[15] Mathy Vanhoef and Frank Piessens, "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2", *Association for Computing Machinery ACM*, Oct 2017, Available at: https://papers.mathyvanhoef.com/ccs2017.pdf

[16] Mathy Vanhoef, "Krackattacks-scripts", *GitHub*, 2017, Availble at: https://github.com/vanhoefm/krackattacks-scripts

[17] William Stalling, “Wireless Security”, *Cryptography and Network Security Seventh Edition*, page no. 606-610, Pearson

[18] 405ashley 1952, "Types of Wireless Network Attacks", *PHOENIXTS*, Feb 18, 2016, Available at: https://phoenixts.com/blog/types-of-wireless-network-attacks/