IT's Emergency Patient: Wi-Fi Protected Access II (WPA2)

Abstract

Out of all wireless network security protocols that have released so far, Wi-Fi Protected Access II (WPA2) is the most widely implemented, the most secure one, until late 2016. It was discovered to be vulnerable to what is called Key Reinstallation Attacks (KRACK). In spite of all of its encryption improvements compared to the previous versions of security protocols, a flaw in the protocol's 4-way handshake – a process that establishes a secure network connection – has brought about a profound threat to the industry in cybersecurity department. The attack involves a man-in-the-middle who prompts the retransmission of the third message, leading to the reinstallation of an encryption key, which ultimately results in reusing the same piece of encryption information while transferring data; this allows the man-in-the-middle to decrypt, steal, and in some cases, forge data. The threatening nature of this attack lies in the scope of its potential victims. Since the vulnerability KRACK exploits is in the design of the protocol itself, there is no easy fix, and even if there were, it would take time to apply it all over the world. As of now, there are temporary fixes released by companies for their own particular products, but there are also some devices that do not receive updates at all.

I. Introduction

Wireless networks are used all over the world and most of them employ Wi-Fi Protected Access II (WPA2), which is a network security protocol and certification introduced by the Wi-Fi Alliance since 2004. It is an update from the previous protocol versions Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) that have both been compromised in their security assurance. Hence, unlike these old ones, WPA2 has been a robust wall to any potential attackers who might have been aiming to hijack a network itself, to intercept data transmission. After all, the only attacks possible since WPA2 came about are by exploiting faulty network drivers or weak pre-shared keys[1]. By implementing the 4-way handshake, the network's data transmission process has remained intact, until now. Basically, 4-way handshake is the initial stage where the client's device and the access point – where the wireless network is transmitted from – exchange four messages to establish a secure connection by installing and generating an encryption key. This has been proven to be secure for 13 years, but a vulnerability in the protocol implementation itself was discovered in late 2016 by a researcher in Belgium. He coined this security hole KRACK Attack, an acronym for Key Reinstallation Attack, and this issue was later publicly announced on November 1st, 2017. This attack manages to intercept the data transmission between the client and the access point and disrupts the security of the process by forcing the handshake to reinstall the encryption key generated, thus the name. This allows the attacker to decrypt, replay and steal data.

This poses much threat to the IT industry because this is no mere crack in the security certificate; the whole design and implementation of the protocol has just been proved to be

[1] the password users have to input in order to get connected to a protected wireless network

flawed. Moreover, almost every user who connects to a wireless network is using this WPA2 protocol that was believed to be very secure; the others are using even less secure protocols like the old WEP and WPA. Therefore, this is a problem affecting, arguably, the largest possible range of users around the world. Although, as of now, the attack has some limitations to its executions, it would not be wrong to deduce that a cyberterrorist may come up with a more developed or easier way to carry out the attack. After all, throughout the history of the industry, the cybercriminal community has been relentlessly advancing with their mischievous cyber exploits. This is a problem requiring immediate attention. Therefore, to shed light on this matter, this research aims to explore the formerly widely trusted WPA2 protocol and how the KRACK Attack exploits the 4-way handshake used by it. From there, analysis of the potential damages this can inflict comes, to be followed by a discussion of potential solutions to tackle this problem.

II. Understanding the Protocol

To begin analyzing the KRACK Attack and its damages on WPA2, it is necessary to look at the wireless security protocol Wi-Fi Protected Access II itself. As mentioned, the first WPA was deemed flawed in its encryption protocol called Temporal Key Integrity Protocol (TKIP). The reason this was not so reliable was because "TKIP is a compromise, designed to accommodate existing WEP hardware" (Edney & Arbaugh); it merely wraps additional code to WEP to encapsulate and modify it (Rouse). In other words, it was just hastily designed to patch the hole in WEP security protocol. On the other hand, the new WPA2 uses CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) which was created "using the best-known techniques" (Edney & Arbaugh) from scratch. CCMP implemented here, along with its block cipher called Advanced Encryption Standard (AES), has been proven to be

very secure, thus WPA2 had been able to stand tall as the most secure protocol after the other failures.

i. WPA2 Introduced

On June 24 2004, Institute of Electrical and Electronics Engineers approved the complete implementation of the original draft (WPA) of IEEE 802.11i standard, which is Wi-Fi Protected Access II. As the security protocol acts as a thorough, secure update from the WPA protocol, it is comprised of new encryption algorithms and protocols in order to reinforce the security. In addition, it also introduces a new method of establishing secure wireless connection and data transmission: the 4-way handshake.

CCMP is the new data-confidentiality protocol implemented when WPA2 was introduced. It incorporates AES for its encryption purposes and offers data authenticity by using Message Integrity Code[2] (MIC). CCMP generates nonces, which are unique numbers that are to be used only once, to generate the MIC for use in data transmission. In addition, nonces are used to create Initialization Vectors (IV) by being concatenated with the data sender's MAC address[3] to produce a completely new number. There is also the use of replay counter [4]in CCMP in order to prevent scrambling data packets in transmission or resending old packets. In other words, it prevents replay attacks[5].

[2] a tag that can be used to verify the authenticity of the data packets
[3] Media Access Control address: a unique identifier of a device in a network
[4] A number tag that accompanies data packets; it increases after each successive data transmission
[5] an attack where a stolen data during a previous transmission is replayed and sent again to trick the receiver

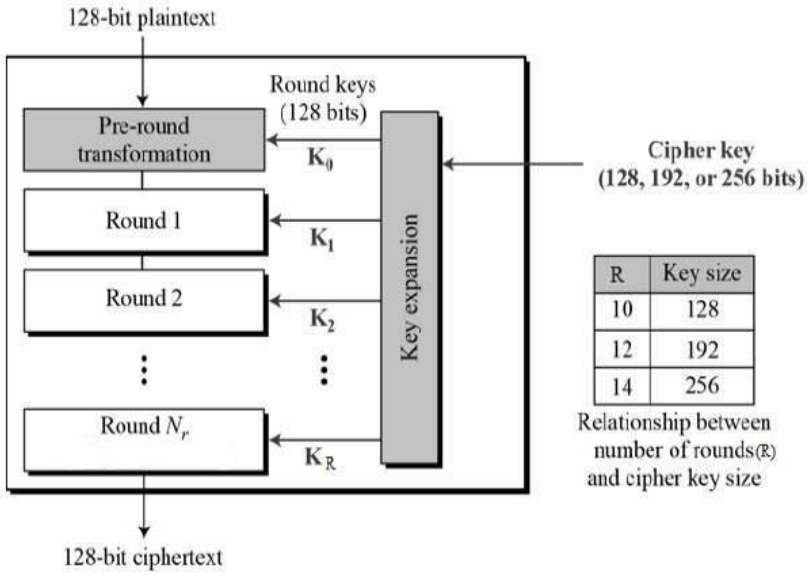

Figure 1: The structure and the overview of the AES encryption process

The new encryption algorithm used by WPA2 is the AES block cipher[6] used to encrypt and decrypt messages using the same AES key. Nevertheless, the whole process itself is not so simple. It can use three types of keys, of different sizes – 128-bit key, 192-bit key and 256-bit key – which are used to encrypt plaintext[7] to ciphertext of a corresponding size; for instance, the 128-bit key will encrypt a plaintext of 128 bits into a ciphertext[8] of 128 bits. Depending on the type of these keys, AES executes its encryption process for different number of rounds: 10 rounds for 128-bit, 12 rounds for 192-bit, 14 rounds for 256-bit key.

[6] an encryption method used to encrypt blocks of text of some bit rather than encrypting one bit of text at a time
[7] a plain text with no encryption or any form of formatting done
[8] text that has gone through some form of encryption or encoding

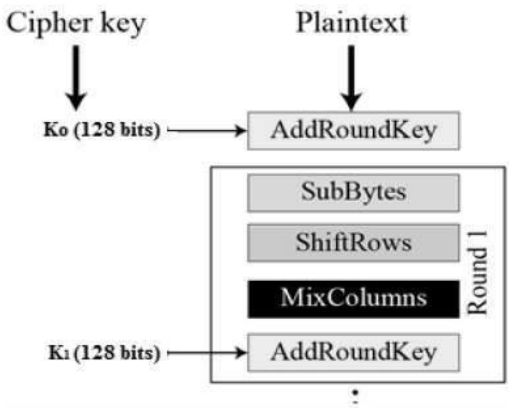

Figure 2: The steps taken to each round of the AES's encryption process

For each round, it incorporates a substitution-permutation network. Before anything, the plaintext is merged with the unique IV obtained from CCMP. Then, first comes the substitution method in which each bit of the plaintext is replaced by the corresponding value from a fixed table called S-box, producing a four by four matrix of the plaintext, now meaningless. Nevertheless, since the replacement is done using a fixed table, it is still not yet safe. As for the second step, the rows of the matrix are shifted, then thirdly, its columns are mixed according to a special mathematical function. Lastly, a round key, derived from the original AES key, is added to the final product. This ends the first round with a ciphertext produced; this ciphertext then acts as the IV for the next round. Then, after a certain number of rounds, a completely new ciphertext is produced. Although, in 2009, some researchers gathered at Microsoft discovered that the AES encryption key can be acquired by the attacker about four times faster than initially believed to be possible, they have assured that this encryption cipher is very powerful and is deemed uncrackable since it would take about two billion years to execute it even with colossal amount of mechanical power and system resources (Katholieke Universiteite te Leuven).

Next, the 4-way handshake is the process that allows a client device that wants to connect to a wireless network to establish a secure connection before sending and receiving any personal data over the network.

ii. The 4-way Handshake

Before moving on to the actual 4-way handshake and its mechanism, there is a process to be examined that takes place before the 4-way handshake: Association stage. In any case of a device trying to connect to a network, the client's side is called Supplicant and the access point – a station that transmits and receives data within a network – is called Authenticator. Generally, when a supplicant tries to connect to a wireless network, an Open System authentication takes place where the user inputs the correct password to join the network. In the association stage, the first stage in figure 3, the supplicant simply sends the association request, and the authenticator responds, establishing a mutual connection. In a case where the supplicant moves to a different authenticator within the same network, reassociation request is sent as well to reestablish the connection, to be responded by the authenticator. As the last step in this stage, both the supplicant and the authenticator generate PMK, Pairwise Master Key from the shared password the supplicant had to input to connect to the network.

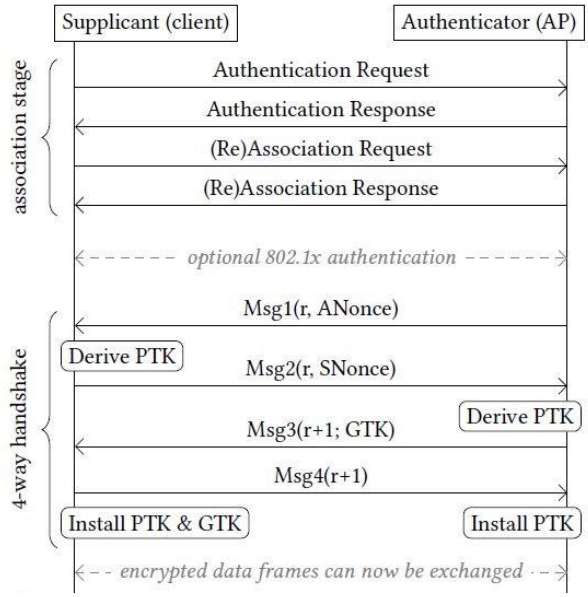

Figure 3: Messages exchanged during the Association Stage and the 4-way handshake

From this stage, it moves on to execute the process called 4-way handshake whose purpose is to establish a secure connection and data transmission. Both the supplicant and the authenticator each has their own MAC address, and once the connection is established, they know each other's MAC address. In addition to that, from the PMK, the supplicant derives Snonce[9] while the authenticator derives the transmit packet number called Anonce[10]; they both are randomly generated numbers that are to be used only once.

To actually begin the handshake, the authenticator starts with the first message containing its Anonce sent to the supplicant. Now, the supplicant has both sides' MAC addresses, Snonce it generated and the Anonce from the authenticator. These are the four necessary components to generate a fresh session key called Pairwise Transient Key (PTK), which is basically an

[9] SNonce or STA nonce: a random receiving packet number generated by the client side of the network that is to be used only once

[10] ANonce or AP nonce: a random transmit packet number generated by the authenticator that is to be used only once

encryption key. As the second message in the handshake, the supplicant sends its Snonce encrypted with PTK to the authenticator. From that, the authenticator also tries to derive PTK and checks if they have the same key derived. Then, at this stage, the authenticator goes to generate a new encryption key called Group Temporal Key (GTK). As the name suggests, this key's role lies in a group when the network needs to carry out multicast[11] and broadcast[12] communication, while the PTK is solely for the transmission between one supplicant and the authenticator. Hence, for the third message, the authenticator sends the GTK it generated to the supplicant for both of them to possess it. As the final message, the supplicant replies to the authenticator with the confirmation of the receipt, and then a secure connection is established. It is also important to note that these messages are tagged with replay counters (see Section III. i.) that are incremented after each mutual transmission between the authenticator and the supplicant. This is to prevent replay attacks (see Section III. i.).

III. Key Reinstallation Attack (KRACK)

Nearly at the end of 2016, a researcher named Mathy Vanhoef from imec-DistriNet research group at Ku Leuven, a university in Belgium, discovered a major loophole sitting in the heart of, then assumed, the most secure wireless network security protocol, WPA2; it certainly held such title for about 14 years after all. Although several cyberattacks have been occurring constantly, they are resulted from cases such as fault in a part of the encryption protocol, or faulty network drivers and other hardware, or password cracking due to weak or unchanged passwords. However, Vanhoef has claimed that this particular vulnerability is quite new and unique in that the design of the security protocol itself is flawed. To prove this, he has

[11] Network communication where data is sent from one or more station/device to multiple stations
[12] Network communication where data is send from one station to multiple stations

performed an attack called KRACK (Key Reinstallation Attack). This attack successfully hijacks a wireless network, decrypt, replay and steal data, and WPA2's 4-way handshake is its primary target.

i. KRACK Attack on the 4-way Handshake

The loophole of the WPA2 protocol that they learned to be susceptible to KRACK lies in the 14-year-old transmission method, the 4-way handshake. The loophole that KRACK is exploiting here lies in the transmission of the messages, particularly in the third and fourth messages. Firstly, the attacker establishes the man-in-the-middle (MitM)[13] position amidst the supplicant and the authenticator. In a normal case, this MitM does not pose much of a threat since the attacker cannot obtain the data in transmission which is encrypted. However, with KRACK attack, the attacker forces the handshake process repeat a portion of the handshake process with the same encryption form as before, leading the attacker to use the previous encrypted form to decrypt the data packet. More in depth explanation follows in the next paragraph.

[13] an attacker secretly interposes between the parties that are involved and interacting within a wireless network

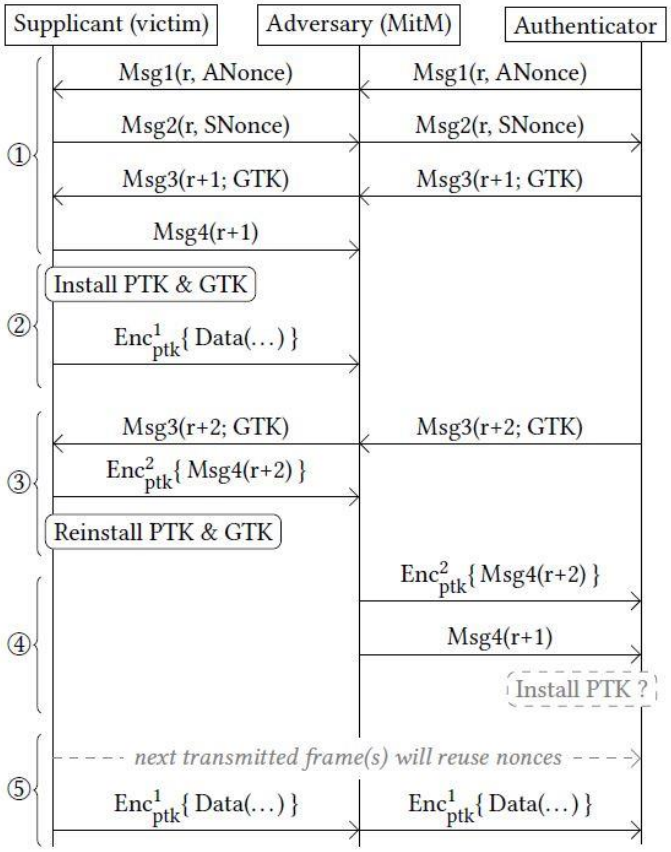

Figure 4: Behind the scene of KRACK attack on the 4-way handshake

The first two stages of the handshake are carried out the same as under any normal condition: authenticator sending the Anonce before the supplicant derives PTK and sending it along with the SNonce to the authenticator. After the authenticator generates the GTK, it sends the third message to the supplicant with the GTK. Then, the supplicant, upon receiving it, sends the fourth message, confirming its receipt while, at the same time, installing the PTK key. It is here the attacker starts its assault by blocking this fourth message from the supplicant to the authenticator. Hence, when the authenticator does not receive the confirmation message from the supplicant, it resends the third message to the supplicant. Thus, this takes the supplicant back to the third stage, after that, it resends the second confirmation fourth message to the

authenticator and reinstalls the PTK again. Hence, this resets the nonces used in the PTK key to the original value used in the first normal data transmission. Generally, when nonces are reset, it means the client is reusing the nonces that have been used to encrypt its data transmission. So, this time, the attacker, who has the first data frame with the encryption can then use it against the second data frame that has the same encryption, decrypting and stealing data effectively. In addition, this process of reinstalling the PTK key also resets the replay counter accompanying the messages. Thus, the notion previously believed – having replay counters prevent replay attacks – is now proved to be violated since the replay counters have lost its purpose of keeping track of the sequence of the messages.

IV. Damages

The above explanation of how KRACK attack exploits the loophole of WPA2's 4-way handshake has illustrated that this is not a mere vulnerability that users can easily avoid. Even when WPA2 uses notably secure AES encryption which would not let any attacker get its encryption key in billions of years, and CCMP protocol that uses unique random IV numbers (for encryption) and replay counters (to prevent replay attacks), the assurance of protection for users worldwide has been thwarted by KRACK. This is because the whole design of the protocol's 4-way handshake is flawed. Due to this loophole, the attacker does not even need to confront the reinforced encryption standard (AES) or the data-confidentiality protocol (CCMP) with their promise of strong security.

As of now, KRACK attack is considered to pose a threat of intermediate level in the cybersecurity industry, due to the attack itself being quite difficult to execute; particularly, the code to construct a program that will be able to execute the attack demands skills of very high caliber. Hence, KRACK attack has not been exploited by the various communities of

cybercriminals, yet. Nevertheless, once the code has been successfully written by one, it can be shared with anyone, and other hackers would also be able to use it at will to carry out the KRACK attack. And since the vulnerability is found in the implementation or the structure of the wireless protocol itself, every device that supports Wi-Fi could be affected. After all, over 60% of the world's Wi-Fi networks are configured with WPA2 protocol (Mike, 2017), the strongest one yet, with others such as WEP and WPA being even more devastating in the face of KRACK; in fact, these two protocols do not even take KRACK to crumble. And, they are not just limited to computers and mobile phones; all devices in the Internet of Things (IoT), every appliance that can be connected to a network is vulnerable as well. Moreover, according to the information on a Vulnerability Notes Database, there are approximately 85 vendors whose products have been affected by the attack tested by Vanhoef and his team; these include a large number of famous names such as Google, Cisco, Dell, Lenovo, Samsung and more (Department of Homeland Security Office of Cybersecurity and Communications). While a large number of users have utilized and relied on reliable protection tools like VPN[14] and HTTPS[15] – additional private and secure solutions for internet browsing –they also have been bypassed in his executions to test for the extent of the KRACK attack (Vanhoef). Likewise, although Windows and Mac OS were initially believed to be immune to it, he has discovered a way to get past them too. Additionally, a factor misinterpreted by many to be a big hindrance on KRACK attack, the fact that the attacker has to be well within close proximity to the target network, has been denied by Vanhoef himself when he says that the attacker can be well within up to 8 miles and still infiltrate the network.

[14] Virtual Private Network – grants the secrecy of a private network, able to escape the eyes of observers
[15] Hypertext Transfer Protocol Secure – secure version of the protocol over which data is sent when connected to the internet

Michael Shatter, National Director at Security and Privacy Risk Services, says that the extent to how much damage or how big this issue will be is still a bit early to tell (Shatter, 2017). After all, it has not been long that the news of the exploit was made public. On top of that, KRACK attack is no easy feat to carry out, and no known packaged or pre-prepared hacking software is not yet available as of now. However, it is only a matter of time someone malicious manages to accomplish this, even more so if we think lightly of this matter and prolong our mission to quash the threat.

KRACK mainly targets to decrypt and steal data. Hence, the potential harm lies in the department of confidentiality and privacy. For instance, online shopping, the most common scenario almost everyone can relate to, makes use of not only usernames and passwords but also credit or debit card numbers. If the man-in-the-middle intercepting a wireless network and executing KRACK attack were to obtain such information, they can exploit other people's shopping accounts to buy anything with the victim's money without his or her consent. At least, if they were to attain only the log-in credentials, they may have to attempt on another try for the card information, and it would save the victim from theft. However, if the victim has the credit or debit card information saved with his or her account for convenience, like many people do, it becomes a huge convenience for the attacker once the log-in credentials have been stolen.

Aside from online shopping, people also often resort to online banking, either via computers or mobile phones. The effect is also similar to the previous scenario where the man-in-the-middle would be able to freely access people's bank accounts by stealing and decrypting their account identification information and password.

What is even more devastating is when KRACK attack is directed at large organizations. To give a relevant example, a case in point would be a bank's network getting targeted with

KRACK. Banks are always dealing with financial transactions and bank account information; it would not even be wrong to say such data entry and transmission takes place in bank every minute. And, since the man-in-the-middle has the power to block and keep the transmitted data for any amount of time while delaying the retransmitted third message from the authenticator, he or she can choose to gather as much confidential information as possible of different bank account holders before sending the retransmitted third message to the client or clients. Therefore, the amount and the type of data they can obtain is a very serious matter. And, this is not just a case where it is a result of a bank's security being lax, for instance. The whole WPA2's 4-way handshake is flawed in its design, rendering every bank vulnerable to the attack.

KRACK attack is remarkably damaging and threatening in the sense that the scope of possible impact is extremely wide. Moreover, it is not a matter quickly fixable by mediocre technicians; the problem lies with the security protocol itself which is the responsibility of the IEEE institute that developed and released the protocol.

V. Solutions

When Vanhoef first discovered the vulnerability in WPA2 in the late 2016, the first action he took was to secretly notify as many vendors as he could contact. This was to prevent any news of this shocking vulnerability leaking to the general public without proper announcement or explanation. Then, Vanhoef worked collaboratively with the vendors to devise patches for KRACK attack. A patch is usually a piece of software that makes changes to an already existing computer program or a system; it can contain additional features, fixes, improvements and updates. These security patches include temporary fixes for WPA2, particularly to prevent the reinstallation of the PTK key in the 4-way handshake, since that is the primary focus of KRACK (Key Reinstallation Attacks). When KRACK was publicly

announced in late 2017, some vendors are already patches and some even have secretly patched their products through regular software updates. According to Osborne, Whittaker and Day (2017), Microsoft, Netgear, Intel, Linux among many others have already released their patches as of the announcement date of KRACK. Back then, Google and Apple were preparing for their own release, but now their patches are delivered to user's devices. It is to be noted that these are temporary fixes and updates while the Wi-Fi Alliance is currently working on the construction and implementation of a new wireless security protocol: Wi-Fi Protected Access III. WPA3 was first announced at CES 2018 (Consumer Electronics Show), to be released in late 2018; no particular date was specified. It outlines various security reinforcements including security and privacy for open networks – a completely new feature. Nevertheless, according to Pastorino (2018), "WPA3 is not an immediate replacement for its predecessor," meaning that WPA2 will not go obsolete once WPA3 enters the industry. It will continue to serve networks worldwide while WPA3 is being integrated into products. Hence, WPA2 will be continued to be tested and improved for its security with the aim of reducing KRACK's impact on it; it will be around for quite some time.

Therefore, as of now, what users can do to alleviate the damages of KRACK is to update their devices as soon as the patches are out; for some products, this is done readily by the vendors through automatic updates. One detail to note is that users have to update both their client devices – laptops, phones, etc. – as well as their routers and access points to be able to protect against the attack; just patching one end would not secure safety. Then later, when WPA3 becomes available, users can opt to adopt the new protocol by obtaining devices and routers that support WPA3.

V. Conclusion

WPA2 had been the most secure security protocol for 14 years. It certainly was powerful in its ability in encryption and data protection with AES and CCMP, but the fault lies in the 4-way handshake, between its handshake messages. Although the Wi-Fi Alliance has proof that the 4-way handshake is secure, what they deemed secure was the fact that the handshake would not reveal the encryption key PTK in any part of its message exchanges. If that were the case, the 4-way handshake would be indeed secure and effective since KRACK doesn't involve revealing the encryption key itself. However, they did not account for the reinstallation of the encryption key, and that is what gives birth to KRACK. Therefore, as unfortunate as it is, although other parts of WPA2's security measures are quite robust, like the multiple rounds of different encryption methods of AES, one slip in the design of the 4-way handshake has crumbled the whole protocol. Since the protocol itself has been proven to be compromised, this is an issue concerning all devices capable of connecting to a network, thus the damage scope is extremely wide. Moreover, WPA2 is the most widely implemented protocol throughout the world, so it would take time to implement any kind of short-term or long-term fixes.

References

Brown, Mike. (2017, October 16). *Wi-Fi Security Flaw Researcher Warns 'We're Just Getting Started'*. Retrieved from https://www.inverse.com/article/37419-mathy-vanhoef-wifi-security-flaw-researcher

Comay, Odded. (2017, October 20). *KRACK Attack: The Impact and How To Mitigate Risk*. Retrieved from https://www.forescout.com/company/blog/krack-attack-impact-mitigate-risk/

Department of Homeland Security Office of Cybersecurity and Communications. *Vendor Information for VU#228519* [Data file]. Retrieved from https://www.kb.cert.osrg/vuls/byvendor?searchview&Query=FIELD+Reference=228519&SearchOrder=4

Edney, J., & Arbaugh, W.A. (2004). *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*. Boston, MA: Pearson Education, Inc.

Katholieke Universiteite te Leuven. *RESEARCHERS IDENTIFY FIRST FLAWS IN THE ADVANCED ENCRYPTION STANDARD.* Retrieved from https://www.kuleuven.be/english/newsletter/newsflash/encryption_standard.html

Molta, David. (2017, October 25). *The KRACK Attack and Lessons for IT Professionals*. Retrieved from https://ischool.syr.edu/infospace/2017/10/25/the-krack-attack-lessons-information-technology-professionals/

Ong, Thuy. (2018, January 9). *Wi-Fi Alliance announces new WPA3 security protections*. Retrieved from https://www.theverge.com/2018/1/9/16867940/wi-fi-alliance-new-wpa3-security-protections-wpa2-announced.

Osborne, C., Whittaker, Z. & Day, Z. (2017, October 17). *Here's every patch for KRACK Wi-Fi vulnerability available right now*. Retrieved from https://www.zdnet.com/article/here-is-every-patch-for-krack-wi-fi-attack-available-right-now/.

Shatter, Michael. (2017, October 24). *How damaging is the KRACK Wi-Fi attack?* Retrieved from https://www.rsm.global/australia/insights/assurance-updates/how-damaging-krack-wi-fi-attack

Vanhoef, Mathy. *Key Reinstallation Attacks Breaking WPA2 by forcing nonce reuse*. Retrieved from https://www.krackattacks.com/

Vanhoef, M. & Piessens, F. (2017, October 3). *Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2*. Retrieved from https://papers.mathyvanhoef.com/ccs2017.pdf

Vilanueva, John Carl. (2015, May 19). *What AES Encryption Is And How It's Used To Secure File Transfers*. Retrieved from http://www.jscape.com/blog/aes-encryption