584 PROJECT REPORT

WPA2 WIRELESS SECURITY PROTOCOL

Rahul Godugupally

CWID -10470581

OVERVIEW:

This final report concerns the wireless security protocol Wi-Fi Protected Access Version 2 (WPA2) which implements the security elements of IEEE 802.11i as it uses Advanced Encryption Standard with Counter Mode with cipher block chaining message authentication code (CBC-MAC) Protocol (CCMP) with an Initialization Vector size of 48 bits.

WPA2 is classified into two types depending on the way it accomplishes authentication and key agreement they are WPA2- Pre shared key (WPA2-PSK) and WPA2-Enterprise. WPA2-PSK is designed to depend on a fixed-shared-secret between the parties and is designed for home users, public Wi-Fi networks as it is more accessible to users and easy to deploy. It supports 128bit key size derived from a 256-bit shared key. The key may be a string of up to 64 hexadecimal digits or as a passphrase of 8-63 ASCII Characters. If ASCII characters are used, the 256-bit key is calculated with the help of PBKDF2 key derivation function. While WPA2 Enterprise utilizes an authentication server that generates random fresh session-keys. It is based on IEEE 802.1X that needs a particular authentication server such as RADIUS. The Key distribution and agreement in WPA2 enterprise mode is done through Extensible Authentication Protocol (EAP). Various kinds of EAP are used for authentication in enterprise mode such as EAP-TTLS, EAP-PEAP, EAP-TLS, TEAP etc.

WPA2 uses a 4-way handshake mechanism which is a process of exchanging 4 initial messages between the Access point (AP) and the user. This is done to generate encryption keys which are used to encrypt data sent over the wireless network. Each new user goes through this process to get a new key which is used to encrypt data between

them and the access point this was each and every connection is made secure and the keys do not repeat.

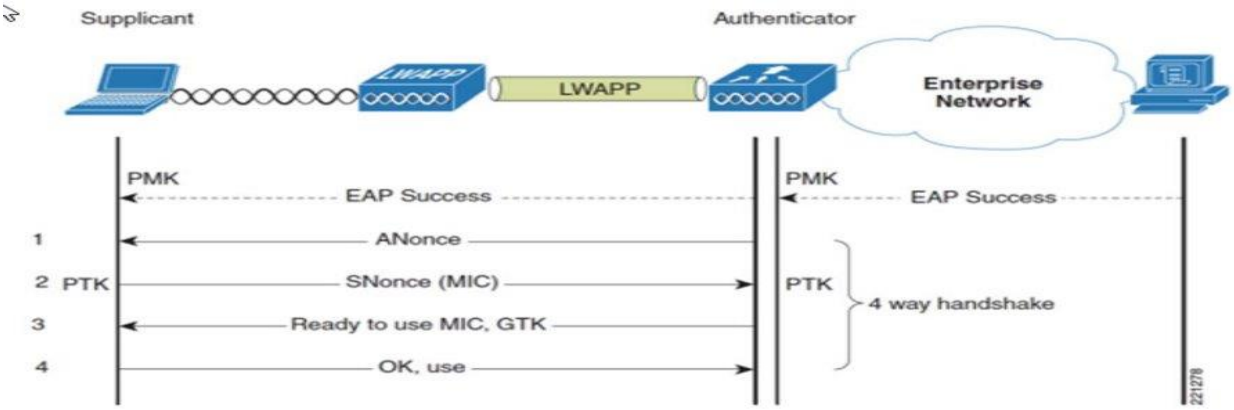

Figure 1. shows the 4-way handshake process [1]

Here 4-way handshake process is performed after the Open system authentication and EAP authentication are complete. In this process, Initially the authenticator (AP) send his Authenticator nonce (ANonce) to the supplicant (client). The supplicant checks the replay counter to make sure that no replay attacks have been performed. Then the supplicant uses his Pairwise Master Key (PMK) derived EAP or directly from Pre shared key (PSK) in personal networks, and his Supplicant nonce(Snonce) to generate the Pairwise Transient key (PTK). Then the supplicant sends his Snonce to the authenticator and the PTK is generated at the AP. This way the PTK is never sent across the network in air. In the third step the AP sends a new Group Temporal Key (GTK) with a Message Integrity Check (MIC) to protect the message. Then the supplicant finally verifies that it is in communication with a trusted AP and there has been no attempts to tamper with communication. In the ultimate step, the supplicant sends a EAPoL- Key ACK Frame which tells the AP that both parties have the same key values and connection are successful. In recent times, this 4-way handshake protocol which was considered very secure came into scrutiny when Key Re-installation Attacks (KRACK) exploited the vulnerabilities in this process. WPA3 was created to address the issues which were found in WPA2 with WPA3 introducing a more secure handshake mechanism called Simultaneous Authentication of Equals (SAE).

WPA2 protocol is the most popular wireless security protocol in the present day. As all the devices in the present-day support WPA2 certificates and use WPA2 to encrypt wireless communications. It is important to study the security impacts of this protocol.

Assessments of Security in WPA2

Here is a brief assessment of WPA 2 networks

- **ASSETS -** Encrypted Data, Encryption Keys (PTK), Handhake, Data Integrity, Network Components, Network Information, Mac Address, Certificates, Authentication Server, Passwords, Device information,
- **PERPETRATORS -** Disgruntled employees, Disgruntled customers, Rival companies, Black Hat hackers, Hacktivists, Script kiddies, Terrorists, Nation States, Rouge organizations, Organized crime, Cyber criminals
- **THREATS -** Evil twin attacks, Replay attack, Denial of service attacks, Key reinstallation attacks (KRACK), De-authentication attacks, Sniffing, Jamming Brute-force, dictionary attacks and rainbow table attack.
- **SAFEGUARDS -** Existing safeguards for wpa2 include encryption with AES (advanced encryption standard) along with CCMP for data protection. HTTPS for web traffic. Key distribution in enterprise mode is done through Extensible Authentication Protocol (EAP). Tunnel bases EAP provides per device key generation in 802.1x architecture
- **VULNERABILITIES -** Potential vulnerabilities of WPA2 could include the 4-way handshake, no locking after multiple authentication failures from the same source, De-authentication frame, Rogue AP’s, Flooding attacks
- **ADDITIONAL CONTROLS -** Authentication rejection after specific number of attempts, Identity Hiding, Intrusion Detection Systems can be used to detect fake de-authentication requests. Using strong encryption and good passwords. Using larger size keys to encrypt data. Using a VPN

THE ASSESSMENTS

Assets: Here the assets are taken for the following reasons:

1.Confidential data – Confidential data is the primary asset as it is the main target of an attacker. He tries to gain information on what's been sent over the network. The most critical asset is the information which is encrypted and sent over the network.

He can monitor, manipulate and even inject the data to cause serious issues in the communication process if he manages to get a hold of data.

2.Encryption key – Encryption key is important and it valuable to the attacker. If an attacker gets the encryption key, he can in turn decrypt the data making the security useless.

3.Network information as the attacker can use it for enumeration and even sometimes social engineering. Same goes for endpoint, AP and Enterprise information.

4.Certificates and Authentication server: In case of an WPA2 enterprise network it is essential to keep these assets secure as they might be valuable to the attacker.

Perpetrators: can include anyone from Rival companies, Organized crime, Rouge organizations for financial gains.

Disgruntled employees, disgruntled customers and script kiddies who want to mess with the systems to cause problems.

Hacktivists for Social and political purposes, damage reputation or in order to prove a point.

Terrorists, Nation states to cause harm to the functioning of a nation or its defense.

Threats: Here are some of the most common threats found for WPA2 encryption.

Threats such as Evil twin is a man in the middle attack which can compromise the confidentiality, integrity and availably of the message.

Attacks such as KRACK exploit the vulnerabilities in the 4-way handshake process of the WPA2 security protocol.

De-authentication attacks are used to disconnect a legitimate user from the AP. Can further be used for replay attacks or Denial of service attacks.

Once the attacker manages to obtain the handshake, he can crack the password given he has enough resources. He can do this by Brute-force, dictionary attacks and rainbow table attacks.

Safeguards:

The existing safeguards for WPA2 which include 128bit AES with CCMP are designed to be very strong encryption method. The WPA2 is most widely used standard in the present day as it overcame the difficulties faced by the previous two technologies.

WPA2 has a list of safeguards which include a 128bit Aes encryption using CCMP. Which makes it harder to decrypt data without the key.

WPA2 along with Extensible Authentication Protocol (EAP) Provides the best security in enterprise among other protocols as it is immune to most of the vulnerabilities found in the previous versions of the protocol

WPA2 PSK for home networks is more vulnerable as it does not have an authenticating server such as RADIUS. However, the implementation of a 128bit key makes it reasonably secure

Vulnerabilities – Potential Vulnerabilities have to do with the design of the 4-way handshake protocol which makes it vulnerable to Key reinstallation attacks and the process of transmission of data. Also, the design of WPA2 protocol as it does not have a mechanism to protect against retransmission of data.

The de-authentication frame is a major vulnerability as it causes the user to disconnect from the AP without any authentication. Flooding and Denial of service is a major vulnerability of WPA2.

Additional controls - Authentication rejection after specific number of attempts is important to defend against online dictionary attacks. This makes it harder for intruders.

Identity hiding should be applied as detecting legitimate username makes it easy for attacker to apply a dictionary attack.

IDS can be used to detect fake de-auth requests by monitoring the traffic in a enterprise.

Stronger encryption algorithms along with good passwords will make it difficult to the attacker to decrypt the data.

Using larger size keys can lead to high computational requirements but when critical data is being transmitted it could be very useful.

Major security issues of WPA2

The Major security Issues of WPA2 systems are classified into 3 types based on the impact of these wireless attacks. They are Authentication attacks, Confidentiality attacks and Availability attacks.

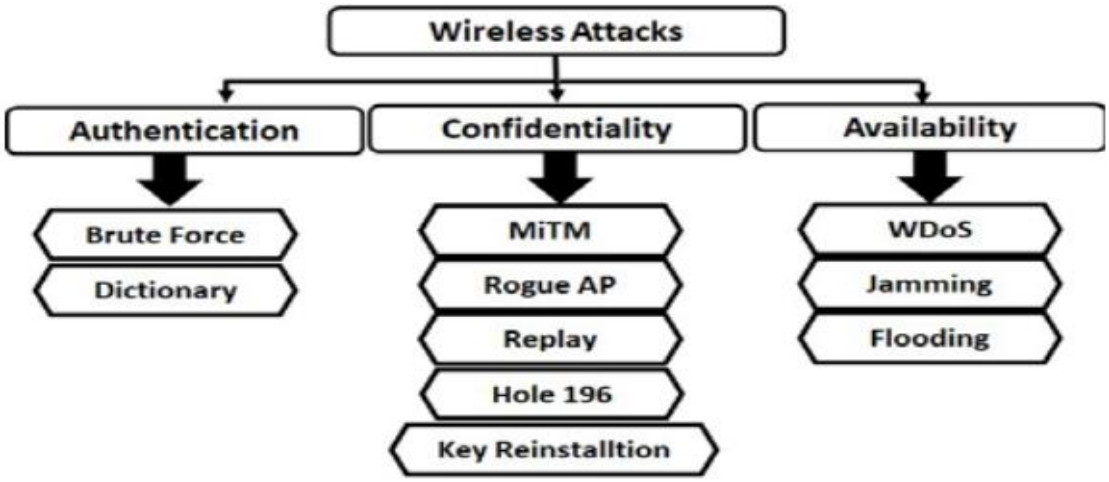

Figure 2. Wireless attacks classification on WPA2 Networks [2]

Authentication attacks- These attacks allow attackers to access the network when they are not supposed to. This can be done by stealing access credentials or by capturing a legitimate handshake and cracking them offline with **Brute forcing** or **Dictionary attacks**. Although brute forcing works but they are much slower than dictionary attacks and require a lot of computational resources. Dictionary attacks on the other hand are faster and occur more frequently. In this attack the attackers run through a list of commonly used passwords. As people use simple, easy to remember passwords they are easy to crack. Hence, it is important to have strong passwords which are complex and involve a lot of characters.

Further, other kind of attacks called **rainbow table** attacks are used to compute hashes and passwords with much better speed than the other ones discussed above. However, their effectiveness is thwarted using salting.

Confidentiality attacks: Confidentiality focuses on keeping data from eavesdropping, however, these attacks allow the attacker to not only access the data but also to intercept, modify the contents of the data. Few popular examples of these attacks include Man in the middle attack, Evil twin attack, Key reinstallation attack (KRACK) and Replay Attacks.

1. **Man in the middle attack (MitM):** MitM attacks take advantage of the insecure networks to eavesdrop on the communication between two legitimate end points.

It can be done by SSID spoofing or Address Resolution Protocol (ARP) poisoning to set up a MitM. “Advanced stealth MitM exploits the Hole 196 vulnerability to set up a Man-in-The-Middle environment by injecting spoofed ARP frames to poison the ARP cache of the client(s) in the network.” [8] By doing this the attacker re-directs all the traffic to himself and can perform packet injection to modify the contents of the message or simply deny forwarding the message.

2. **Evil Twin:** An evil twin attack is launched by rogue AP’s that look like a legitimate source with similar SSID. This enables attackers to acess, monitor and even modify the data. Evil twin attacks are critical due to an increase in the number of mobile devices that store credentials, financial information and other confidential data.
3. **Key Reinstallation Attacks:** Key reinstallation attacks (KRACK) “tricks the victim into reinstalling already used keys by manipulating and replaying cryptographic handshake messages.” [1][7] This attack is directed to the 4-way handshake of WPA2 protocol particularly the message 3 of the Handshake process. In case of drop in packets the AP retransmits message 3 and as a result the client receives multiple messages and each time it recives the message it reinstalls the encryption key. “An attacker can force these nonce resets by collecting and replaying retransmissions of message 3 of the 4-way handshake.” [7] and hence the encryption protocol is attacked. With KRACK, it is possible to inject/manipulate data without even breaking or knowing the password.

Availability Attacks: The availability attacks try to stop or interrupt normal communication process in the network. **Wireless Denial of Service attack** (WDOS) is one of the most common attacks which target availability of a network. This type of attack tries to degrade the efficient use of network resources and disrupts the communication process. This is considered as one of the major threats against wireless systems and is of many types such as ICMP flooding, SYN flood, Slowloris etc. **Jamming** is also one of the most effective attacks against wireless networks as encryption of physical layer which contains important traffic parameters is not possible in wireless communications. In jamming, interfering signals are sent on a network that cause denial of service to legitimate users.

Another type of Availability attack is **De-authentication** attack which uses the de-authentication frame which when sent over to a device forces the device to disconnect from an access point. The concerning part of de-authentication attacks is that the attacker does not even have to be inside a network. This can force the device to reconnect and then the attacker can lead the user into performing multiple types of attacks.

Severity of Security Concerns

Since WPA2 is widely used across the globe the likelihood of attacks is extremely high. WPA2 has been used for the past 15 years and it has been fairly reliable. However, since it has been deployed for such a long time there have been numerous threats developed to exploit the vulnerabilities in the protocol.

As all the wireless devices use WPA2 encryption standards to communicate in networks any major threats could have a huge significance in wireless security. The data being transmitted and confidential information can all be vulnerable to attacks. With Internet becoming commonplace all the applications done on the internet can be vulnerable if the WPA2 encryption protocol is tampered with. With cloud computing and online banking becoming the norms for today's world the need for a stronger encryption is necessary.

Efficient Ways to improve security.

There are multiple measures that can be taken to improve the security of the WPA2 protocol networks. They include :

- Implementing authentication rejection after specific number of trials to connect to the network as it will defend against online dictionary attacks. Identity hiding should be enforced as detection of legitimate usernames will make it easy for attackers to perform dictionary attacks.
- As the 4-way handshake does not prevent the reuse of Nonces it leads to Key Reinstallation attacks hence It should be able to prevent the retransmission of messages during this process. Along with this adequate replay counter is also required as each time it resets the incremental transit packet number (Nonce).

- Using Intrusion Detection Systems in promiscuous mode will help in detecting fake de-authentication attacks and replay attacks. Authenticating the de-authentication frames is also a solution in dealing with de-authentication attacks.
- Digital certificates must be implemented for each device connecting to the Wi-Fi network to prevent unauthorized users from accessing the network.
- Regular traffic checks should be implemented for detection of suspicious activity in critical areas. These can help in detection of suspicious activity.
- SSL-bump filtering should be used to counter Man in the middle attacks .
- The use of stronger encryption with complex passwords should be enforced to make decryption harder for attackers.
- In enterprise situations regular security audits for wireless systems should be implemented.
- Artificial intelligence programs should be developed to detect and alleviate the wireless security attacks. If anything out of the ordinary shows up in the network the program could alert by learning the default behavior of the network.

Future Directions:

As WPA2 protocol has been in play for a long time the future technology which is supposed to take over WPA2 I.e WPA3 will become more prominent. WPA 3 improves upon the issues faced by WPA2 such as the 4-way handshake mechanism.

WPA 3 introduces a new more secure handshake mechanism called the Simultaneous Authentication of Equals (SAE) replacing WPA2's Pre-Shared Key exchange protocol. This mechanism allegedly fixes the problems faced by key reinstallation attacks in WPA2. WPA3 also adds Opportunistic Wireless Encryption (OWE) to replace the open network authentication in WPA2 which is widely used in public networks and hotspots. WPA3 also uses longer key size at 192 compared to 128 bits used in WPA2 which makes WPA3 a more secure protocol.

WPA3 addresses offline dictionary attacks by its dragonfly key exchange system. "Dragonfly uses forward secrecy to protect previous browsing sessions, along with a high-entropy pairwise master key to prevent password guessing." [10] Hence it is resistant to

these attacks which were prevalent in WPA2 systems. However, the new dragonblood vulnerability [11] which forces WPA3 encrypted devices to downgrade to WPA2 and then launches KRACK attack making it vulnerable to key reinstallation attacks. Fortunately, this vulnerability was fixed by a software update rolled out by WiFi alliance and addressed the issue.

Despite all the improvements WPA3 it increases the compute resource overhead and introduces additional challenges for low-powered IoT devices. And even WPA3 personal might still be susceptible to Man in the middle attacks as it does nothing to address it.

Conclusions

The WPA2 protocol is still a robust wireless security protocol and given the popularity of WPA2 it will still be present in the near future. The security and vulnerabilities of WPA2 will not affect the popularity of WPA2 as it is still the most widely used solution for wireless security .

The Future technology in WPA3 will make improvements upon WPA2 in a large scale. However, there is still a lot of time for the world to completely shift to WPA3. This might not be until few years down the road.

The issues regarding WPA2 are well known as many have reported vulnerabilities on WPA2 for very long time. Continuous improvements have been made to make this technology sustain for so long. As WPA2 was designed to address issues concerning WEP and WPA, it has been in practice for around 15 years.

The Issues of security In WPA2 is a chronic one as almost all the devices in the present-day use WPA2. The lack of support for legacy devices makes them vulnerable to many attacks and not safe for them to be used for critical applications. Also, with powerful computers being widely available for common people stronger encryption keys must be used, as passwords and keys can be decrypted in short amount of time.

With the arrival of WPA3 in 2018 most of the devices will be using it in the future and given some time WPA2 will slowly start to fade away.

REFERENCES

[1] D. J. Fehér and B. Sandor, "Effects of the WPA2 KRACK Attack in Real Environment," 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY), 2018, pp. 000239-000242, doi: 10.1109/SISY.2018.8524769.

[2] M. A. Abo-Soliman and M. A. Azer, "Tunnel-Based EAP Effective Security Attacks WPA2 Enterprise Evaluation and Proposed Amendments," 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), 2018, pp. 268-273, doi: 10.1109/ICUFN.2018.8437043.

[3] J. Guo, M. Wang, H. Zhang and Y. Zhang, "A Secure Session Key Negotiation Scheme in WPA2-PSK Networks," 2020 IEEE Wireless Communications and Networking Conference (WCNC), 2020, pp. 1-6, doi: 10.1109/WCNC45663.2020.9120510.

[4] M. A. Abo-Soliman and M. A. Azer, "A study in WPA2 enterprise recent attacks," 2017 13th International Computer Engineering Conference (ICENCO), 2017, pp. 323-330, doi: 10.1109/ICENCO.2017.8289808.

[6] K. Moissinac, D. Ramos, G. Rendon and A. Elleithy, "Wireless Encryption and WPA2 Weaknesses," 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), 2021, pp. 1007-1015, doi: 10.1109/CCWC51732.2021.9376023.

[7] Mathy Vanhoef and Frank Piessens : Key Reinstallation Attacks Breaking WPA2 by forcing nonce reuse, www.krackattacks.com

[8] Advanced Stealth Man-in-The-Middle Attack in WPA2 Encrypted Wi-Fi Networks, IEEE COMMUNICATIONS LETTERS, VOL. 19, NO. 4, APRIL 2015.

[9] An overview of the Wi-Fi WPA2 vulnerability - https://www.enisa.europa.eu/publications/info-notes/an-overview-of-the-wi-fi-wpa2-vulnerability

[10] Adam Shepherd “Why WPA3 may be no safer than WPA2” - https://www.itpro.com/security/30848/why-wpa3-may-be-no-safer-from-attack-than-wpa2

[11] M. Vanhoef and E. Ronen, "Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd," 2020 IEEE Symposium on Security and Privacy (SP), 2020, pp. 517-533, doi: 10.1109/SP40000.2020.00031.