A Study in WPA2 Enterprise Recent Attacks

Mohamed A. Abo-Soliman
School of Communication and Information Technology
Nile University, Cairo, Egypt
Moh.soliman@nu.edu.eg

Marianne A. Azer
National Telecommunication Institute
Nile University, Cairo, Egypt
mazer@nu.edu.eg

***Abstract*— Organizations and network developers continuously exert much money and efforts to secure wireless transmission. WPA2 framework is widely deployed for Wi-Fi communications since it is efficient and secure against several wireless attacks. However, WPA2 security has been lately threatened by advanced developed versions of wireless attacks. The increase of computer processing power, continuous efforts by penetration testers, network evaluators and researchers led to the emerging of new advanced attacking techniques that may exploit WPA2 wireless systems detected vulnerabilities. In this paper, we shed the light on the newly emerged attacks conducting practical tests to evaluate WPA2 security through a prototype of WPA2/EAP-TTLS implementation. This evaluation comes out with recommendations and guidelines for protecting wireless enterprise communication.**

Keywords— Authentication, confidentiality, EAP, Network Access Control, wireless Security, Wi-Fi, WPA2.

I. INTRODUCTION

WPA2 resistance against several threats lasted for about 14 years before discovering some weaknesses and vulnerabilities in most of its implementations[1]. Recent studies practically exploited some discovered vulnerabilities of both WPA2 personal and enterprise implementation modes[2, 3]. However, it's still considered the latest and most secure 4-way handshake protocol for wireless security that comply with 802.11i version D9:0 [4]. The major security objectives for any wireless protocol are authentication and confidentiality. Authentication ensures that associated clients are really who they claim, while confidentiality focus on secrecy of transmitted data. Brute force and Dictionary attacks are common examples that target authentication by retrieving network access secrets. Man in the middle, replay and key reinstallation attacks target data confidentiality by eavesdropping transmitted data without the need to crack network access secrets. In this paper, we practically launch advanced techniques of common wireless attacks to evaluate current WPA2 security against recent threats. The remainder of this paper is organized as follows. Section II is a background about WPA2 framework and applied defenses. Section III portrays recent wireless threats and attacks. In section IV, we describe the implementation prototype environment and evaluation methodology of WPA2. Finally, conclusions and future directions are discussed in section V.

II. WPA2 FRAMEWORK

WPA2 was introduced to overcome most of previous wireless security issues [5]. The process of authentication and exchange of cryptographic keys between communicating peers is one of the main difference between wireless security frameworks. According to 802.11i, WPA2 is considered a Robust Security Network (RSN) capable protocol that supports 4-way handshake in the 2.4 GHz or in 5 GHz wireless Networks[2]. It allows the use of TKIP like WPA, but it recommends AES for data confidentiality and mandates Cipher Block Chaining Message Authentication Code Protocol (CCMP) for integrity. It supports strong authentication based on 802.1x architecture in enterprise mode or up to 64 ASCII character (256-bit key length) for pre-shared key in personal mode[6]. In WPA2, the supplicant refers to the client while authenticator refers to the Access Point (AP). The four-way handshake authenticates a client to access the network and allows encryption ciphers and keys to be exchanged between supplicant and authenticator. Three items are negotiated through handshake, pairwise cipher suite, group cipher suite and authentication information. Pairwise cipher suite encrypts unicast data transmission between each associated client and access point while group cipher suite encrypts multicast data transmitted from access point to all associated clients. Pre-shared key or 802.1x authentication scrambled information are exchanged during the handshake. Authentication and confidentiality techniques are explained in the following sections.

A. WPA2 Authentication

WPA2 accomplishes Authentication and Key Agreement (AKE) via two different modes, Pre-Shared Key (PSK) mode for personal networks or enterprise mode via Extensible Authentication Protocol (EAP) in 802.1x architecture for larger corporate networks.

1) WPA2 Personal

WPA2/PSK is usually implemented for home use or small office networks. AES is typically utilized for encryption. AES is a symmetric-key algorithm that uses one key for both encryption and decryption. CCMP is typically combined with AES for data integrity during authentication and key exchange. Generation of cryptographic keys for authentication and data encryption in WPA2/PSK is initially fed by a shared passphrase configured on both client and AP. All clients of the same network use the shared passphrase to access same network. The shared passphrase is used with other variables like Service Set Identifier (SSID) and SSID length to produce Pairwise Master Key (PMK), which is used for authentication and production of unicast protection keys. Passphrase cracking in WPA2/PSK is mathematically easier than randomly generated keys in 802.1x architecture especially with the rapid increase of processing power and distributed brute-force techniques [7].

978-1-5386-4266-5/17/$31.00 ©2017 IEEE

Authorized licensed use limited to: SLIIT - Sri Lanka Institute of Information Technology. Downloaded on February 23,2021 at 14:46:40 UTC from IEEE Xplore. Restrictions apply.

2) WPA2 Enterprise

Larger enterprise networks require a dedicated server to automate and manage authentication and key agreements. Integrating organization access points with authentication server like RADIUS provide unique credentials for each associating device or user. When WPA2 enterprise is used, each user has his own username and password [8]. Per-device authentication information and Encryption keys are exchanged through EAP. EAP is an authentication flexible framework that supports multiple authentication methods and is always implemented as part of 802.1x architecture [9]. The authentication server authenticates clients and exports the randomly generated cryptographic keys in case of using derived-keying-material EAP method [10]. Authentication server AS communicates with clients through authenticators that act as pass-through device. AS could be implemented as a service on the AP [11]. EAP is encapsulated using various authentication schemes like Message Digest 5 (MD5) [12], Transport Layer Security (TLS) [13], Tunneled TLS (TTLS) [14], and Protected Extended Authentication Protocol (PEAP). These authentication schemes aka methods are classified into two main categories, password based and tunnel based. Authentication in password-based EAP depends on unique secrets entered by supplicants while Tunnel-Based methods depend mainly on certificate authority for identity validation [15]. In this work, we use EAP TTLS as an example of EAP for authentication which is considered one of the most secure tunnel-based method[16]. Transmitted EAP messages between supplicant and authenticator are encapsulated in EAP over LAN (EAPOL) frames [17] while Messages between authenticator and AS are usually encapsulated in RADIUS format. Figure 1 depicts all possible EAP messages communicated during EAP handshake. EAPOL and EAP-TTLS are discussed below.

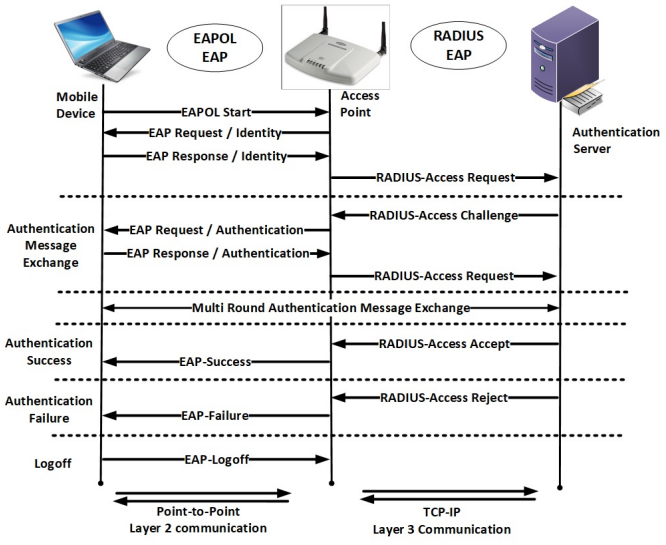

Figure 1 EAP Messages

3) EAPOL

EAPOL messages are defined as network media-access-layer frames that allow handshaking between client and access point without the need for IP layer. EAPOL messages carry required information fields like a message type, replay counter, nonce, Receive Sequence Counter (RSC), Message Integrity Check (MIC) and key data field. The type header defines which particular message of EAPOL frame. The replay counter is an incremental number initiated by AP where the client respond to each frame with same number to protect authenticating session against replay attack. The nonce field holds a randomly generated key that is used for deriving fresh session keys at both client and authenticator. In case of sending group keys, RSC contains the starting packet number of the key while the group key itself is hosted in the key data field. Figure 2 shows the EAPOL message header while Figure 3 shows an example of a captured message that illustrates different packet fields.

Type	Replay Counter	Nonce		RSC		MIC	Key Data

Figure 2 EAPOL Headers

```
802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: Key (3)
    Length: 117
    Key Descriptor Type: EAPOL RSN Key (2)
  > Key Information: 0x008a
    Key Length: 16
    Replay Counter: 1
    WPA Key Nonce: 2c52389b858e44ceaa1edc5196869e6f926e0efbfafd5ec1...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 00000000000000000000000000000000
    WPA Key Data Length: 22
  > WPA Key Data: dd14000fac04f402d6b24a20f36500fc7ed2a4ba6043
```

Figure 3 EAPOL Frame Headers

4) EAP-TTLS

Tunneled EAP method is normally a combination of two EAP methods, outer Authentication EAP technique that creates a secure tunnel and inner EAP approach that performs user/device authentication. An EAP tunnel method can be used in any lower-layer protocol that supports EAP authentication. Several existing EAP tunnel methods use Transport Layer Security (TLS) RFC5246 [18] to establish a secure tunnel. Standard EAP TTLS [14] is a tunneling authentication method that is formed of two steps: Step one's objective is to create a symmetric encryption tunnel based on the server digital certificate that allows server verification to client. While step two allows the server to verify the client's identity by another internal method through the created tunnel. Attributes-Value Pairs (AVPs) are exchanged in the second phase through the tunnel including authentication challenges. TTLS support several protocols for inner authentication such as EAP-MD5, PAP, CHAP, MS-CHAP, MS-CHAP-V2, etc... EAP-TTLS has similar properties like EAP-PEAP but because not all supplicants natively support both EAP-TTLS and EAP-PEAP at the same time, Authentication servers should support authentication from multiple EAP methods at the same time in order to allow different clients OS to access the enterprise network. EAP-TTLS could optionally enforce client

Authorized licensed use limited to: SLIIT - Sri Lanka Institute of Information Technology. Downloaded on February 23,2021 at 14:46:40 UTC from IEEE Xplore. Restrictions apply.

certificates [19] in addition to the server certificate but client certificates are very expensive and complex since it is required to install a certificate for each client. The set of used algorithms in TLS-based secure networks is called cipher suite. Cipher suites differs according to the combination of algorithms it performs during authentication. Key exchange algorithm, key length, and message-authentication-code algorithm are types of cipher suite components.

B. Confidentiality Techniques

WPA2 supports Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES). TKIP uses two separate keys to encrypt wireless traffic, the first is 128-bit key used to produce a per-packet encryption key, and a 64-bit MIC key used to verify packets contents against modifications during transmission [20]. TKIP usage is deprecating and not advised by Wi-Fi Alliances [21] since March 2015 due to security flaws. WPA2 uses AES and CCMP by default which provide stronger cypher suite than WPA [22]. Generating and distributing encryption keys are major factor in protecting the confidentiality and integrity of wireless secure communication. In the following, we explain the key generation and key distribution processes.

1) Key Generation

According to IEEE 802.11i, there are seven generated keys to protect WPA2. Pairwise Master Key (PMK) is 256-bit key produced by password based key derivation function 2 (PBKDF2) through 4056 times repetitive hashing to the combination of 3-to-63 character passphrase, SSID and SSID length [23]. This implies that access points configured with same passphrase and SSID produce the same master key. PMK is consequently combined with AP MAC address, client MAC address, ANonce, SNonce to generate Pairwise Temporary Key (PTK) by applying Pseudo Random Function (PRF). ANonce is randomly generated number at the AP while SNonce is a randomly generated number at the client. The 384-bit PTK is then divided into 3 subset 128-bit keys: Key Confirmation Key (KCK), Key Encryption Key (KEK) and Temporal Key (TK). Both KCK and KEK are used for handshake protection while TK for transmitted data protection.

2) Key Distribution

Cryptographic keys are exchanged through the 4-way handshake messages defined by EAPOL. The communication starts by initiating first message at the AP carrying ANonce. Consequentially clients use the first message to generate all required keys then respond with the second message including the SNonce and Message Integrity Code (MIC), which is produced, based on EAPOL header plus KCK. AP uses the SNonce to generate all required keys in addition to checking the integrity by comparing local generated MIC with received MIC. A third message is then transmitted from access point including Group Transient Key (GTK) protected by KEK and MIC. Two MIC failures occurring within 60 seconds let both client and access point stop and start rekeying a fresh session key. The fourth message is transmitted from the client to acknowledge the handshake completion. The 4-way handshake messages are shown in Figure 4.

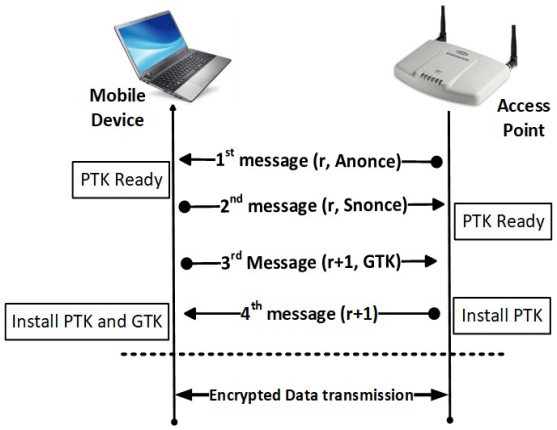

Figure 4. Four-way Handshake

III. WI-FI THREATS AND ATTACKS

Wireless threats can be classified into four major types; interception, interruption, modification and fabrication [5]. It can also be categorized based on the affected OSI-Model Layer [24]. Attacks are also classified into active and passive attacks [25]. There are attacks that target weak implementations versus attacks that target protocols vulnerabilities. In this work, we categorize Wi-Fi attacks into authentication attacks, confidentiality attacks and availability attacks. Attacks main categories are shown in Figure 5. Authentication attacks target stealing access credentials to reuse later for accessing the network, among these attacks are brute force and dictionary attacks. Confidentiality attacks are real-time stealthy attacks that monitor, decrypt and analyze wireless transmitted information without the need to gain network access credentials, such as MiTM attack, replay attack, key reinstallation and key recovery attacks. Availability attacks' objective is to stop or interrupt normal communication of an active wireless client or the entire network like Wireless Denial of Service (WDoS), flooding and Jamming attacks. In this work, we launch active dictionary attack as an example of authentication attacks and Key reinstallation attack as an example of confidentiality attacks to test WPA2/EAP-TTLS security defenses.

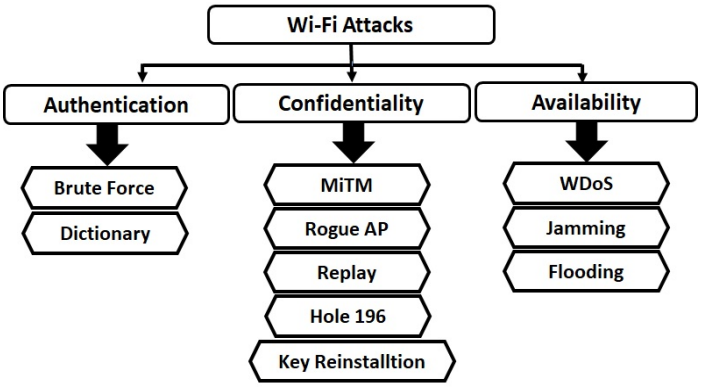

Figure 5 Main Categories of Wi-Fi Attacks

Authorized licensed use limited to: SLIIT - Sri Lanka Institute of Information Technology. Downloaded on February 23,2021 at 14:46:40 UTC from IEEE Xplore. Restrictions apply.

A. Dictionary Attack

In order to crack a wireless network authentication key, pin, code, password or passphrase, intruders can test accessing the target network several successive times with different guessed values until one hit. Although it is similar to brute force attacks in the way of repeating the access trials, dictionary attacks are faster and support authentication values of different lengths. Brute force might be theoretically more effective especially with short authentication values since it applies all possible combination of characters. However, this attack fails in networks with longer authentication values. A list of frequently used/guessed words are saved in a custom file made for specific target network. Dictionary attacks target weak implementation of networks that use predictable weak keys, passphrases or passwords. Dictionary attacks are launched in two different mechanisms; passive dictionary attacks and active dictionary attacks.

1) Passive Dictionary Attack

Passive dictionary attacks are one of the most common attacks against wireless communication. The broadcast nature of wireless communication allows malicious intruders to collect WLAN authentication information such as EAPOL messages in WPA/WPA2 WLANs. Then can later retrieve authentication codes by running an offline dictionary attack on the captured packets. The authentication codes are either, an AP passphrase in WPA2-PSK or username and password in WPA2-enterprise. Dictionary attacks apply hashing technique similar to target network technique to a list of guessed passphrases one by one, and then match each output with the captured ciphered authentication information of the collected handshake messages. Matching between one of the guessed encrypted passphrases with captured encrypted authentication information denotes a successful crack.

2) Active Dictionary Attack

In active dictionary attack, the network access trials target the AP directly requesting to join the network. If the access point responds with successful authentication for one attempt, then the guessed authentication value is correct. One of the main defenses against active dictionary attacks is Wi-Fi Protected Setup (WPS) introduced by Wi-Fi alliance as an optional defense against online dictionary attack [26]. WPS depends on 8-digit pin number related to the AP to be entered by clients before network access authentication. However, this pin number can be retrieved by an online brute force attack due to bad design [27]. Another defense mechanism against active dictionary attack is to reject authentication requests from the attempting client after specific number of trials to lock the door against intruders. Parallel active dictionary attacks overcome the locking mechanism by emulating several virtual clients with different spoofed MAC addresses to mislead the target AP and to complete the attack in 100-fold faster than single client attack [23]. Figure 6 explains the applied steps of Active Dictionary attack against WPA-PSK network access point. Legitimate client who is requesting access to network is impersonated. Once PTK is generated, second message of the handshake is sent to AP. If third message is received then we have a match, which means that the current secret is correct. On the other hand, when receiving first message then the secret does not match repeating same process with the next guessed word until success or completing the dictionary file.

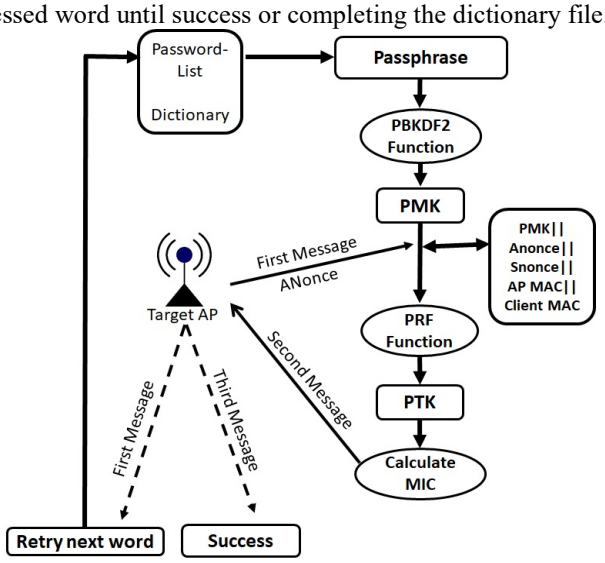

Figure 6 Active Dictionary Attack

B. Key Reinstallation Attack

Unlike Dictionary attacks, exporting authentication values is not an objective for key reinstallation attack. It rather targets confidentiality of data, by intercepting the transmitted data flow between client and AP. In key reinstallation attack, intruders do not target retrieving wireless encryption keys to reuse for interception like traditional man in the middle (MiTM) attack. Intruders try to replay a captured wireless encryption key based on nonce reuse vulnerability of the 4-way handshake [1]. The 4-way Handshake allows generating encryption key based on values from both communicating sides. In WPA2, fresh PTK is generated based on randomly generated values called Nonces. The ANonce is generated at the AP while SNonce is generated at the client. Nonces are encrypted with PMK while they are exchanged between AP and client during the first and second message of the handshake. The third handshake message carries the PTK. This key is installed at both sides to encrypt data frames using data confidentiality protocol (AES in this work). As per design, most APs allow the retransmission of the third message in case of loss or dropping. Malicious intruders may collect and retransmit encrypted third message of the handshake. This causes the client to reinstall same session key and resetting the incremental packet transmission number (Nonce) and receive reply counters. Group keys and Fast BSS Transition handshakes are also subjected to key reinstallation attacks. In our implementation, we exploit a replay counter vulnerability during group key exchange.

IV. IMPLEMETATION

In this section, we launch two recent advanced penetration tests to evaluate WPA2 enterprise latest threats. Our evaluation would detect/confirm WPA2 vulnerabilities and come out with recommendations and guidelines required to overcome these vulnerabilities. Two separate tests are

Authorized licensed use limited to: SLIIT - Sri Lanka Institute of Information Technology. Downloaded on February 23,2021 at 14:46:40 UTC from IEEE Xplore. Restrictions apply.

performed respectively. The first test evaluates authentication protocols resistance against an active dictionary attack while the second test targets confidentiality mechanism by running key reinstallation attack. Figure 7 shows our test environment, the attacking device has Kali Linux installed, attacking python scripts and required dependencies. Wireshark for packets monitor, capture and analysis. Target clients are android-based, Linux-based and windows-based systems. FreeRadius [28] is implemented as the authentication server using EAP-TTLS for authentication. Access point is configured as Pass-through authenticator with WPA2 corporate mode.

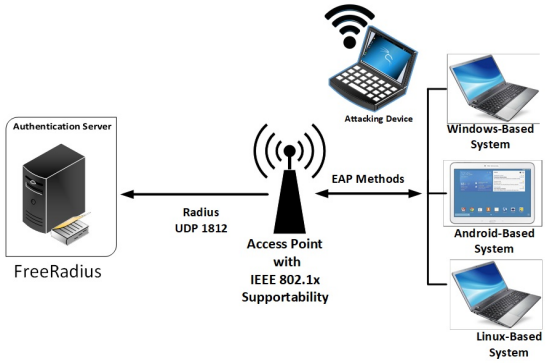

Figure 7 Test Environment

A. Ethical Considerations

Most of experiments were applied to test the effectiveness of the attacks on target devices under our possession, these devices are identified by MAC addresses. We also applied some tests for other networks in coordination with network administrators after getting owner's permissions.

B. Practical Analysis

Packet capture is initially applied to authentication messages. EAP-TTLS starts by traditional EAP messages that negotiate and agree authentication techniques. EAP TTLS messages then initiates phase one by creating the TLS tunnel preceded by phase two that provides mutual authentication, key generation, client identity privacy and cipher suites negotiation.

1) EAP messages

Authenticator sends an EAP request (code 1) including type fields that define what is requested such as identity, authentication challenge, secret key, etc. in our scenario EAP-TTLS is requested. The peer sends a response packet (code 2) in response to a valid request. Response packets contain type field that corresponds to EAP request message. Authenticator sends additional request packets and the peer replies with equivalent respond packets. The sequence of requests and responses continues as long as needed. EAP is a lock step where a new request cannot be sent prior to receiving a valid response except for the first request. The conversation continues until the authenticator cannot authenticate the peer (unacceptable response to one or more requests). Thus the authenticator must send an EAP failure (code 4). On the other hand, authenticator can authenticate the peer where the authenticator must transmit an EAP success (code 3). Sample EAP request and response packets are shown in Figure 8.

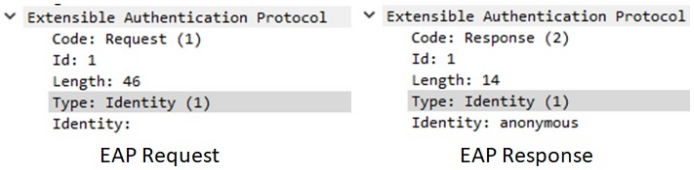

Figure 8 Sample of EAP Packet Captures

2) EAP-TTLS Messages

Figure 9 Displays EAP-TTLS packet format where code field identify type of packet, it could be 1, 2, 3 or 4 meaning request, response, success or fail respectively. The identifier field matches response with requests. Type identifies the applied method noting that 21 means EAP-TTLS. Flags field may be used to identify start flag and more fragments. TLS data field host the attribute-value pairs (AVPs) including authentication information. Figure 10 displays sample captured packets.

Code	Identifier		Length
Type	Flags	Ver	TLS Message Length…
…TLS Message Length			TLS Data….

Figure 9 EAP-TTLS Packet Format

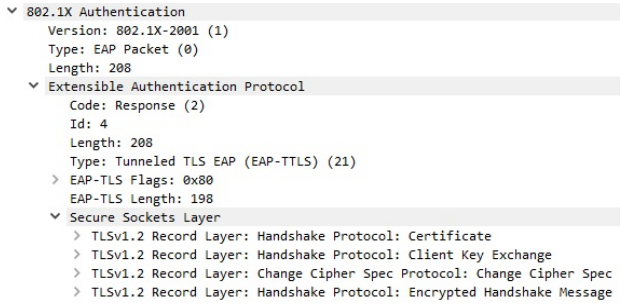

Figure 10 EAP TTLS Response Packet

3) Attribute Value Pairs (AVPs)

AVPs exchange authentication information in addition to other extensible attributes. AVPs are encrypted by TLS tunnel and encapsulated in EAP-TTLS packet during authentication. AVPs format can easily be converted to radius format since it complies with diameter and Radius AVP format. Figure 11 displays AVP headers where AVP Code and Vendor-ID denotes attribute type or purpose. V bits shows whether AVP is vendor-specific or not while M bits indicate whether to ignore or fail negotiation if the AVP is not supported.

AVP Code	
V M r r r r r r	AVP Length
Vendor-ID (optional)	
Data…	

Figure 11 AVP Format

Authorized licensed use limited to: SLIIT - Sri Lanka Institute of Information Technology. Downloaded on February 23,2021 at 14:46:40 UTC from IEEE Xplore. Restrictions apply.

C. Active Dictionary Attack Evaluation

Offline dictionary attacks after capturing WPA2 handshake is not feasible in enterprise WPA2 since exporting the PMK is not currently possible, and it does not include authentication information. Our Dictionary attack runs actively by enumerating normal authentication request by legitimate corporate username. In most cases authentication is based on valid username and valid equivalent password. Corporate user name is detected in our attack through EAP-TTLS packet analysis since username are sent in clear text. Most EAP tunneled methods use "anonymous" username for outer unencrypted authentication while hiding the real authenticating username inside the encrypted TLS tunnel. Nevertheless, we noticed that user identities are sent in clear text in most implementations. Although identity protection is addressed and defined in "Requirements of Tunnel-Based EAP methods" IEEE RFC6678. However, implementers and products' vendors may not cope with the standard. This is intentionally coded by implementers, to allow relaying the authentication realms in complex environments with distributed authentication servers. After getting username, dictionary passwords test trials starts. WPA2 does not natively limit number of authentication attempts. This makes cracking user passwords easier even if encrypted by AES. WPA2 enterprise cracking is considered of higher risk than other wireless security protocols because the cracked values are usually domain or enterprise user credentials, which allow the attacker to gain access not only to layer two Wi-Fi network but also to all user's resources. Figure 12 summarizes the targeted points of weakness and recommended solutions.

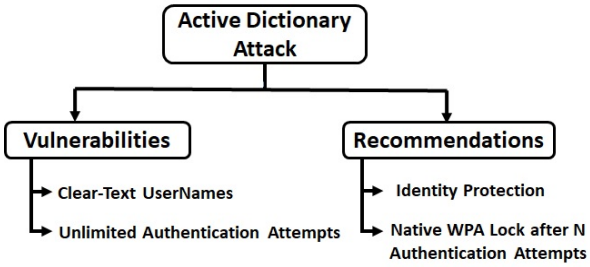

Figure12 Active Dictionary Attack issues and advises

D. Key Reinstallation Attack Evaluation

Key reinstallation attack has been lately tested on WPA-PSK [1, 29] based on WPA2 state machine vulnerability. Key reinstallation attacks are generally applied against three techniques of key distribution. The first targets the 4-way handshake vulnerability. The second targets group key handshake vulnerabilities, while third targets fast BSS retransmission handshake vulnerabilities. These attacks have been previously performed on WPA-PSK implementations. Our work evaluates group key replay attack on WPA2-EAP. In WPA2-Enterprise, encryption keys are generated at the authentication server based on TLS master key. The authenticator periodically sends group Transient key (GTK) to all associated clients. GTK is encrypted by PTK during transmission. Group keys are used for transmitting broadcast and multicast data. The group key handshake starts immediately after fourth message of EAPOL handshake. Two messages comprise group key distribution; the first message carries a KEK-encrypted group key in the data filed of an EAPOL defined frame. It also carries the receive replay counter in RSC, as shown in (Figure 2 EAPOL Headers). The second message is a response EAPOL frame sent from client to server acknowledging GTK reception. According to the standard, Authenticators should install the GTK after receiving group ACK frame from all clients. However, this is not the fact in some implementations sine some authenticators install the GTK immediately after sending the first group message. We apply the attack on both types of authenticators.

1) Direct GTK Installation after sending 1st message

The attack is based on three steps. First, we monitor traffic flow until transmission of first message of a group key handshake. We then allow supplicant to receive such a message in order to install the GTK but we have to block the transmitted second message from the victim to authenticator. This causes retransmission of first message by authenticator with incremented replay counter, which is captured by our attacking machine. Second step is to wait for a broadcast data frame and forward it to the client. Note that broadcast data frames are encrypted by current GTK. This means if GTK were not installed at authenticator, an older key would encrypt this broadcast message causing transmission failure. Finally, we send the retransmitted first message with actively used group key to client urging him to reinitialize the replay counter.

2) Standard GTK Installation

Authenticators that do not install GTK directly but wait after receiving acknowledgment from all clients are harder to penetrate but practically feasible. This is achieved through slight modification to replay counter of the re-transmitted captured group first message.

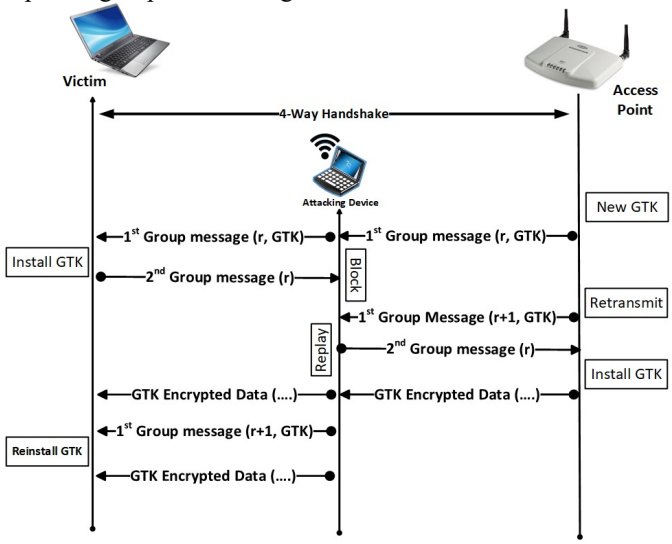

Figure 13 Group Key Reinstallation Attack

As shown in Figure 13, previous steps are applied but when the authenticator retransmits the first message with incremented replay counter to authenticator, this message has to be blocked and captured then the captured second message is to be sent to authenticator with original replay counter, which is minus one

Authorized licensed use limited to: SLIIT - Sri Lanka Institute of Information Technology. Downloaded on February 23,2021 at 14:46:40 UTC from IEEE Xplore. Restrictions apply.

than the retransmitted first message. Fortunately for attackers, the authenticator accepts the acknowledge frame due to the fact it match the replay counter with any used replay counter in the group key handshake. In other words, the replay counter in the second message is not matched with most recent replay counter only; it is rather matched with any replay counter of the same handshake. This allows authenticator to install GTK. Then we proceed with the next steps by waiting a broadcast transmission, replaying it to victim. Key reinstallation attacks should be resolved by WPA2 updates. Among these updates, GTK installation at AP must wait acknowledgements from all supplicants, and precise technique for group key handshake replay counter.

V. Conclusion and Future directions

In this paper, we surveyed wireless WPA2 security techniques in terms of authentication and data confidentiality. We also discussed latest wireless threats and categorized attacks into three categories: authentication attacks, Confidentiality attacks and availability attacks. In additions, we conducted two different advanced attacks on WPA2: Active dictionary attack and key reinstallation attack. The first targets authentication while the later targets transmitted data confidentiality. Some vulnerabilities have been detected and exploited such as “identity leakage” and “unlimited number of authentication attempts” which are exploited by active dictionary attack. Other vulnerabilities like “direct GTK installation at authenticator” and “replay counter client reset” have been exploited by group key reinstallation attack. We have recommended some modifications for WPA2 handshaking mechanisms for these vulnerabilities to resist against recent attacks. Other penetration tests should be performed on the 4-way handshake and fast transition handshake to detect other vulnerabilities of WPA2 native security techniques. In additions, regular wireless security audits may be implemented to mitigate the newly discovered vulnerabilities.

VI. References

[1] M. Vanhoef and F. Piessens, "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2," ed. Conference on Computer and Communications Security: CCS, 2017.

[2] A. K. Mohan and M. Sethumadhavan, "Wireless Security Auditing: Attack Vectors and Mitigation Strategies," *Procedia Computer Science,* vol. 115, pp. 674-682, 2017.

[3] A. Cassola, W. K. Robertson, E. Kirda, and G. Noubir, "A Practical, Targeted, and Stealthy Attack Against WPA Enterprise Authentication," in *NDSS*, 2013.

[4] S. Alblwi and K. Shujaee, "A Survey on Wireless Security Protocol WPA2," in *Int. Conf. security and management*, 2017, pp. 12-17.

[5] S. Lamichhane, "Penetration Testing in Wireless Networks," 2017.

[6] A. H. Lashkari, M. M. S. Danesh, and B. Samadi, "A survey on wireless security protocols (WEP, WPA and WPA2/802.11 i)," in *Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on*, 2009, pp. 48-52: IEEE.

[7] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: current challenges and future developments," *IEEE Communications Magazine,* vol. 54, no. 6, pp. 152-158, 2016.

[8] P. Robyns, B. Bonné, P. Quax, and W. Lamotte, "Short paper: exploiting WPA2-enterprise vendor implementation weaknesses through challenge response oracles," in *Proceedings of the 2014 ACM conference on Security and privacy in wireless & mobile networks*, 2014, pp. 189-194: ACM.

[9] S. S. Rezaie, S. A. Hoseini, and H. Taheri, "Implementation of Extensible Authentication Protocol in OPNET Modeller."

[10] K. Hoeper, *Recommendation for EAP Methods Used in Wireless Network Access Authentication*. DIANE Publishing, 2010.

[11] K. Yang and J. Ma, "Implementation of IEEE802. 1x in OPNET," in *System Simulation and Scientific Computing, 2008. ICSC 2008. Asia Simulation Conference-7th International Conference on*, 2008, pp. 1390-1394: IEEE.

[12] L. J. Blunk, "PPP extensible authentication protocol (EAP)," 1998.

[13] D. Simon, B. Aboba, and R. Hurst, "The EAP-TLS authentication protocol," 2070-1721, 2008.

[14] P. Funk and S. Blake-Wilson, "Extensible authentication protocol tunneled transport layer security authenticated protocol version 0 (EAP-TTLSv0)," 2008.

[15] C.-I. Fan, Y.-H. Lin, and R.-H. Hsu, "Complete EAP method: User efficient and forward secure authentication protocol for IEEE 802.11 wireless LANs," *IEEE Transactions on Parallel and Distributed Systems,* vol. 24, no. 4, pp. 672-680, 2013.

[16] R. Dantu, G. Clothier, and A. Atri, "EAP methods for wireless networks," *Computer Standards & Interfaces,* vol. 29, no. 3, pp. 289-301, 2007.

[17] J.-C. Chen, M.-C. Jiang, and Y.-w. Liu, "Wireless LAN security and IEEE 802.11 i," *IEEE Wireless Communications,* vol. 12, no. 1, pp. 27-36, 2005.

[18] T. Dierks, "The transport layer security (TLS) protocol version 1.2," 2008.

[19] K. M. Ali and T. J. Owens, "Selection of an EAP authentication method for a WLAN," *International Journal of Information and Computer Security,* vol. 1, no. 1-2, pp. 210-233, 2007.

[20] K. Vilius, L. Liu, J. Panneerselvam, and T. Stimpson, "A Critical Analysis of the Efficiencies of Emerging Wireless Security Standards Against Network Attacks," in *Intelligent Networking and*

Authorized licensed use limited to: SLIIT - Sri Lanka Institute of Information Technology. Downloaded on February 23,2021 at 14:46:40 UTC from IEEE Xplore. Restrictions apply.

Collaborative Systems (INCOS), 2015 International Conference on, 2015, pp. 472-477: IEEE.

[21] W.-F. Alliance, "<Wi-Fi_Alliance_Technical_Note_TKIP_v1.0.pdf>," 2015.

[22] H. I. Bulbul, I. Batmaz, and M. Ozel, "Wireless network security: comparison of wep (wired equivalent privacy) mechanism, wpa (wi-fi protected access) and rsn (robust security network) security protocols," in *Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop*, 2008, p. 9: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[23] O. Nakhila, A. Attiah, Y. Jinz, and C. Zoux, "Parallel active dictionary attack on wpa2-psk wi-fi networks," in *Military Communications Conference, MILCOM 2015-2015 IEEE*, 2015, pp. 665-670: IEEE.

[24] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," 2015.

[25] W. Stallings, *Cryptography and network security: principles and practices*. Pearson Education India, 2006.

[26] D. Zisiadis, S. Kopsidas, A. Varalis, and L. Tassiulas, "Enhancing WPS security," in *Wireless Days (WD), 2012 IFIP*, 2012, pp. 1-3: IEEE.

[27] S. Aked, C. Bolan, and M. Brand, "A Proposed Method for Examining Wireless Device Vulnerability to Brute Force Attacks via WPS External Registrar PIN Authentication Design Vulnerability," in *Proceedings of the International Conference on Security and Management (SAM)*, 2012, p. 1: The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[28] A. DeKok, "FreeRADIUS," *Http://Freeradius. org,* 2008.

[29] M. Vanhoef and F. Piessens, "Predicting, Decrypting, and Abusing WPA2/802.11 Group Keys," in *USENIX Security Symposium*, 2016, pp. 673-688.

Authorized licensed use limited to: SLIIT - Sri Lanka Institute of Information Technology. Downloaded on February 23,2021 at 14:46:40 UTC from IEEE Xplore. Restrictions apply.