Tunnel-Based EAP Effective Security Attacks

WPA2 Enterprise Evaluation and Proposed amendments

Mohamed A. Abo-Soliman
Faculty 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*— Tunnel-Based Extensible Authentication Protocol has become fundamental for wireless Network access Control. It provides authentication, privacy and authorization for enterprise network access protected by WPA/WPA2 security framework. WPA2 is considered the latest and most secure standard for wireless communication especially for Wi-Fi networks. However, WPA/WPA2-PSK have been lately threatened by advanced versions of wireless attacks. In this paper, we study WPA/WPA2-Enterprise authentication with Tunnel-Based EAP common methods focusing on their strength and weak points and the impact of recent WPA/WPA2 attacks. We also propose protection techniques to mitigate discovered security flaws.**

Keywords—EAP; Network Access Control; Wi-Fi Security; Wireless Attacks; Wireless Security; WDOS; WPA.

I. INTRODUCTION

Several new technologies and trends have adopted the 802.11 standard for wireless connectivity. The increased need for mobility, simple installation, and cable-free environments accelerate the use of wireless communication systems. "Wireless LANs", "Sensors networks", "Internet of Things", "AD-HOC networks", "VANET" and "Bring Your Own Device" are different forms of wireless networks that depend mainly or partially on 802.11 standard for data transmission. However, data confidentiality, users' privacy and integrity of travelling information through air are subject to monitoring and interference that threaten 802.11 performance and reliability. Continuous efforts exerted by attackers, penetration testers, network evaluators and researchers led to the emerging of new advanced wireless attacking techniques that threaten the future of such 802.11-based forms and technologies. These continuously emerging threats require adequate defenses. WPA2 is considered the latest and most secure protocol-set for defending 802.11 WLAN data transmission[1] that was introduced to overcome most of previous wireless security issues[2]. WPA2 accomplishes Authentication and Key Agreement in two modes: Pre-Shared Key and enterprise mode. The first depends on a fixed-shared-secret between communicating parties while the later utilizes an authentication server that generates random fresh session-keys. Key distribution and agreement in WPA2 enterprise mode are exchanged through Extensible Authentication Protocol (EAP) which is defined in IEEE RFC3748[3] as an authentication framework that supports multiple authentication methods that work in lower TCP-IP layer without the need of IP. There are two classes of EAP: password based and tunnel based. The first depends on unique secrets entered by supplicants while Tunnel-Based methods depend mainly on certificate authority for identity validation[4]. Tunnel-Based EAP Methods are widely adopted for most of wireless access control systems implemented in large networks since they achieve robustness, efficiency and security. They also provide automatic per-device key generation in 802.1x architecture[5]. Nevertheless, broadcast nature of wireless technologies has direct impact on all authentication techniques. In this paper, we focus on Tunnel-Based EAP Methods for wireless security in terms of performance, reliability, resistance against lately emerged wireless attacks. We highlight the weaknesses of such protocols and propose adequate remediation. The remainder of this paper is ordered as follows: Section II introduces Tunnel-Based EAP Methods. Section III evaluates common Tunnel-based EAP methods. Threats and attacks are highlighted in section IV. Section V proposes relative mitigation and remediation techniques, while section VI provides the conclusion.

II. TUNNEL-BASED EAP OVERVIEW

Tunnel-Based EAP is used in 802.11 WLANs to agree and distribute per-session security keys by enabling public key environment for communication between mobile devices and access points[6]. Tunneled-based EAP method is normally a combination of two subset EAP methods, outer Authentication EAP method that creates a secure tunnel and inner EAP approach that performs user/device authentication. Several existing tunnel-based EAP methods use Transport Layer Security (TLS) RFC5246[7] to establish a secure tunnel. A dedicated server is always implemented to automate and manage authentication and key agreements between devices and network access points. The authentication server authenticates clients and exports the randomly generated cryptographic keys in case of using derived-keying-material EAP method[8]. Tunneled EAP is encapsulated using various authentication schemes like Transport Layer Security (TLS)[9], Tunneled TLS (TTLS)[10], and Protected Extended Authentication Protocol (PEAP)[11]. Authentication servers should support authentication from multiple EAP methods simultaneously, in order to allow different clients OS to access the enterprise network. Transmitted EAP messages between device and access point are encapsulated in EAP over LAN (EAPOL) frames [12] while Messages between authenticator and AS are usually encapsulated in RADIUS format[13]. Figure 1 depicts the architecture of WPA2-Tunnel-Based-EAP secure network. Common Tunnel-Based EAP methods are discussed below.

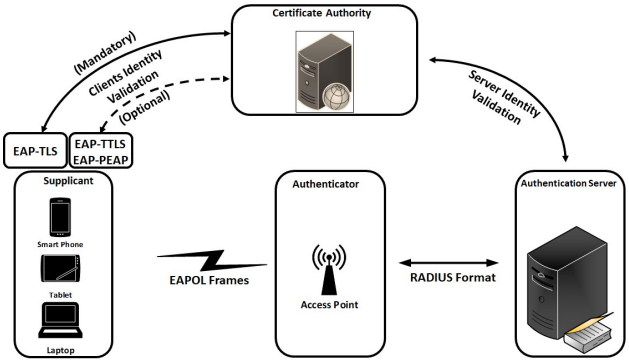

Figure 1
Tunnel-based EAP network architecture

A. EAP-TTLS

EAP-TTLS [10] is a tunneling authentication method the use symmetric encryption tunnel to allows server verification to client at phase one. Then it allows the server to verify the client's identity by another internal method through the created tunnel. TTLS supports several protocols for inner authentication such as EAP-MD5, PAP, CHAP, MS-CHAP, MS-CHAP-V2, etc... EAP-TTLS could optionally enforce client certificates [19].

B. EAP-PEAP

Similar to EAP-TTLS, EAP-PEAP has two main phases. There are two PEAP types; the first is PEAPv0 that uses EAP-MSCHAP V2 or EAP-SIM as inner authentication protocol, while the second is PEAPv1 that uses EAP-GTC or EAP-SIM as its inner authentication protocol.

C. EAP-TLS

EAP-TLS was primarily developed based on Netscape's SSL v3.0. It offers mutual authentication based on digital certificates and provides integrity protected cipher-suite negotiation. EAP-TLS is required for use with smart cards. Although EAP-TLS implementation is the most secure authentication method for WLANs, because it uses a digital certificate to authenticate the server to the client and client to server. However, it is more complex and expensive since it requires installing unique certificate for each client.

D. TEAP

Tunneled Extensible Authentication Protocol (TEAP) is a standard defined in IEEE RFC7170 which is released in 2014 [14]. TEAP is built on FAST[15] with some minor changes. TEAP is an EAP method that utilizes secure TLS handshake to provide an authenticated key exchange and to establish a protected tunnel. It executes other EAP methods under the protection of that secure tunnel. Inner authentication depends on Type-Length Value (TLV) objects, which carry channel binding information too.

III. TUNNEL-BASED EAP EVALUATION

Evaluating security protocols is usually a hard work due to the multitude and diversities of security techniques and studies. In this section, we evaluate Common EAP methods based on two dimensions; first, we practically measure each method's performance based on its consumed authentication time. Second, we evaluate security based on security requirements defined in RFC6678. Practical performance analysis and security requirements compliance are discussed sequentially. This is presented in section A, and B respectively.

A. Performance Evaluation

In this section, we practically evaluate the authentication time for the most common three Tunnel-Based EAP methods: EAP-TTLS, EAP-PEAP and EAP-TLS. The test is made on different systems and devices where time is measured and recorded in seconds for each protocol in the same device. Figure 2 displays the average Authentication time according to logs generated at both EAP server and client. Server time refers to the authentication period from the initiation of authentication until triggering EAP Accept message at the authentication server. Client time refers to duration starting from the initiation of client EAPOL start message until reaching a connected state at the client. Client authentication time includes server time and client association time to AP and consumed time for obtaining IP address from DHCP server at AP. EAP-TTLS and EAP-PEAP are faster than EAP-TLS which requires prior connectivity of client to certificate authority for server validation.

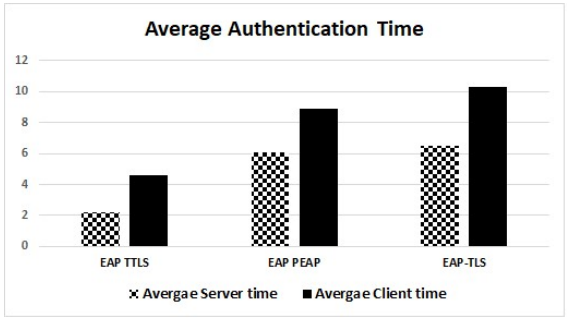

Figure 2
Average authentication time

A. Security Evaluation based on RFC6678 Compliance

In 2012, A set of requirements has been defined in IEEE RFC6678 to ensure Tunnel-based EAP security. These requirements assume the use of TLS for creating the secure tunnel. The defined requirements are considered basic guidelines for developers and implementers in creating different authentication methods. However, most of existing authentication methods include additional vendor proprietary flavors thanks to the extensibility nature of EAP. Requirements are classified into 6 main groups[16]; General requirements[17], Tunnel requirements, Tunnel payload requirements, EAP channel binding requirements, requirements associated with carrying username and password and requirements associated with carrying EAP methods. Tunnel-based EAP requirements are depicted in Figure 3. The three evaluated protocols are compliant with all listed security

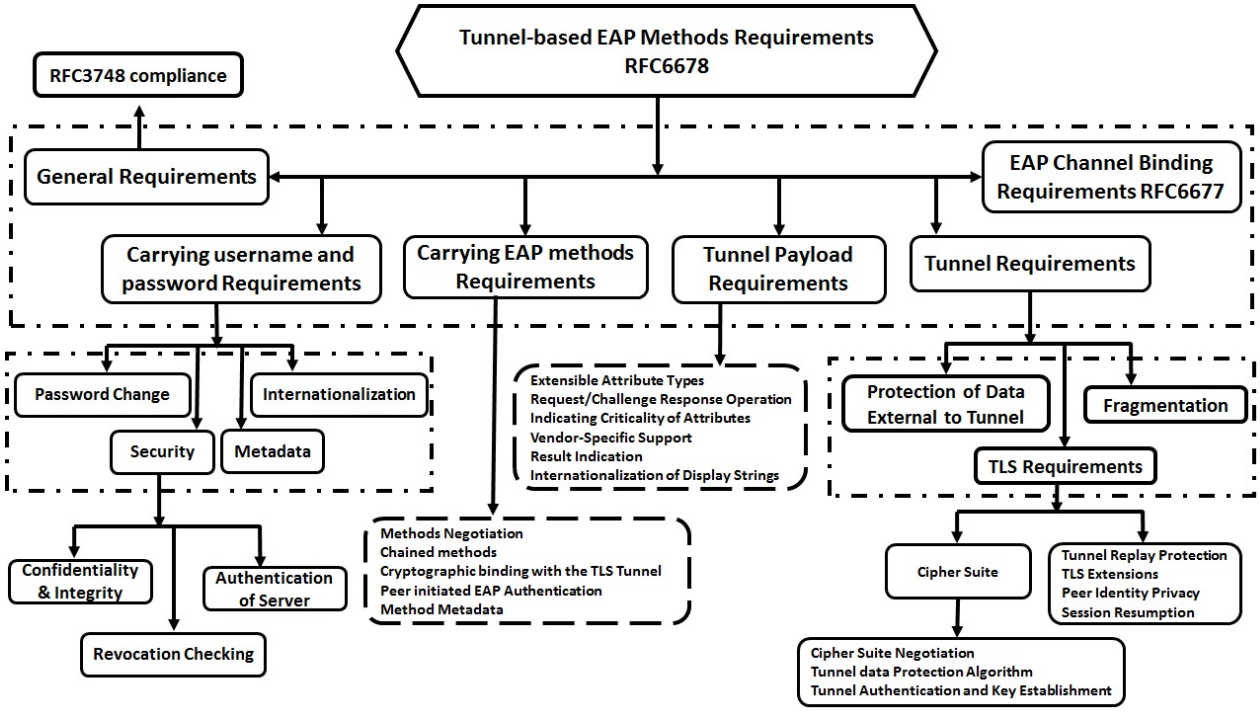

Figure 3
Tunnel-based EAP methods requirements

requirements except identity protection. All methods apply one shared "anonymous" identity for outer method while transmit the real user/device identity within the tunnel. Unfortunately, passwords are only encrypted while usernames are intentionally sent in clear text in all current implementations to allow authentication forwarders use multiple authentication servers in larger networks This vulnerability is exploited in dictionary attacks which we will discuss in a later section. Cracking EAP authentication in WPA2 enterprise mode secure network is considered of severe risk since the same credentials are always used for network and the entire domain. Thus, attackers gain access not only to network but also to all privileged network resources and services. Table 1 lists the main classes of Tunnel based EAP requirements with common methods compliance

Table 1
Methods compliance with security requirements

Requirements	*EAP-TTLS*	*EAP-PEAP*	*EAP-TLS*
General Requirements	Yes	Yes	Yes
Tunnel Requirements	Yes	Yes	Yes
Tunnel Payload Requirements	Yes	Yes	Yes
Channel Binding Requirements	Yes	Yes	Yes
Carrying Username & Password Requirements	Partially	Partially	Partially
Carrying EAP Methods Requirements	Yes	Yes	Yes

IV. Threats And Attacks

Three main factors are usually considered for wireless security: authentication, confidentiality and availability. Authentication ensures that only authorized entities can access the network. Confidentiality focuses on protecting transmitted data from eavesdropping. Availability aims to preserve network functionality and stability. Wireless attacks may be classified into three main categories based on these security factors: Authentication attacks, confidentiality attacks and availability attacks. They are shown in Figure 4. In this paper, we focus mainly on current attacks that affect tunnel-based EAP authentication and threatens the wireless transmissions security. Recent active attacks are portrayed sequentially followed by Table 2 that summarizes the impact of attacks on each authentication method.

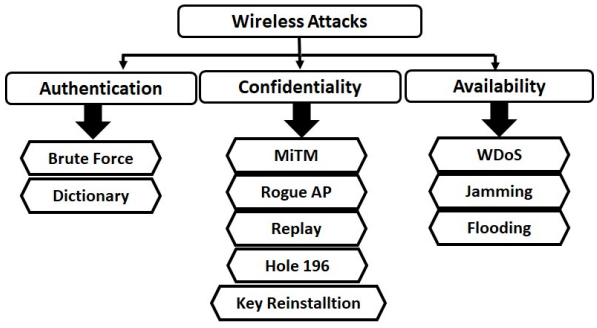

Figure 4
Wireless attacks main categories

A. *Authentication Attacks*

Authentication main objective is to allow only legitimate devices or users access the network. Authentication attacks allow malicious intruders to access the network by stealing access credentials of legitimate users. Single sign on (SSO) architecture that enable same credentials for both Network access and intranet service encourages attackers to crack wireless access secrets. Offline decryption for access credentials included in a captured legitimate handshake is the most common technique for gaining access secret codes[18]. Brute force [19] and Dictionary attacks [20] are clear examples of these attacks. Brute force is effective with short authentication values while dictionary attacks targets predictable keys or passphrases. Although brute force attacks are similar to dictionary attacks in the way of applying several authentication attempts until the success of one attempt. We focus mainly on dictionary attacks, which are faster than brute force attacks and occurring in a large scale nowadays. Dictionary attacks use stored password list in a custom dictionary files generated based on business type, devices default passwords, humans' common phrases, language and location. Dictionary files are continuously increasing in size and the possibility of success.

1) Dictionary Attacks

Dictionary attacks are divided into two types; passive dictionary attacks and active dictionary attacks. Passive attacks are more common for Wi-Fi networks due to the simplicity of capturing the authentication handshake, which is analyzed offline for decrypting the authentication secrets. Parallel active dictionary attacks[21] are active attacks that succeeded to crack WPA-PSK protected network in 100-fold time compared to traditional one client attack. Based on Virtual Wireless Client (VWC). The attackers use virtual multiple clients with spoofed MAC addresses to accelerate penetration time. In this paper, we applied multiple-clients active dictionary attack to an enterprise-mode WPA2 protected wireless network that uses tunnel-based EAP for mutual authentication. Three main vulnerabilities that allow penetration were detected. The first is the device/user identity detection due to a known vulnerability of sending identity intentionally in a clear text within the tunnel as discussed previously in point B of section III. The detected identity is used in combination with the proposed in-queue password that we retrieve from the dictionary list. The other vulnerability is that WPA/WPA2 does not apply a native locking after multiple authentication failures from same source. It rather depends on Wi-Fi protected setup (WPS)[22] for WPA-PSK protected networks. In 802.1x architecture, time intervals are set to manage session time, idle timeout, etc... These intervals are exchanged between EAP authentication servers and Authenticators through EAP methods. However, locking for client authentications after a specified number of authentication failures is not practically enforced. The third addressed issue in this attack is validating the server only by client for EAP-PEAP and EAP-TLS authentication server. This is easily compromised by accepting any certificate at the attacking devices. EAP-TLS is not susceptible to this attack because it enforce client-side validation. Figure 5 depicts dictionary attack steps for acquiring access credentials for enterprise protected wireless network.

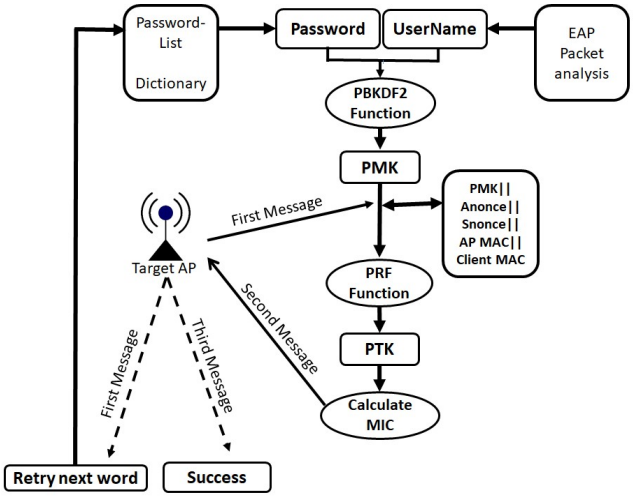

Figure 5
Dictionary attack for enterprise wireless network

B. *Confidentiality Attacks*

Man In The Middle attack (MiTM)[23] is a classic and common state that violates network confidentiality. It allows stealthy intruders to intercept, monitor or modify transmitted data between communicating systems. Evil Twin and key reinstallation attacks are effective techniques that endeavor to act as MiTM between communicating systems in an 802.1x architecture with Tunneled EAP authentication.

1) Evil Twin

The evil twin attack [24], [25] is launched by rogue access point and authentication server that are planted in covered vicinity of a victim. Based on roaming client misconfiguration that accept the server certificate, the evil twin allow any corporate device to access a fake network with SSID similar to legitimate enterprise SSID. This enables the attackers to monitor transmitted data in addition to stealing access credential, which is logged at the malicious authentication server. All EAP methods are vulnerable to this attack if the enterprise client wireless configuration is not precisely set. Evil Twin attack is getting more critical due to the increasing number of mobile and handheld devices that store users' enterprise credentials to allow business activities in BYOD environments.

2) Key Reinstallation Attacks

Key reinstallation attacks [26] targets all WPA/WPA2 protected WLANs. Exploiting WPA/WPA2 state machine vulnerability, Key reinstallation attacks enforce the reuse of already-in-use key in a communicating session by resetting key parameters such as nonce and replay counter. There are three main types of key reinstallation attacks: The first targets the 4-way handshake vulnerability. The second targets group key handshake vulnerabilities, while the third targets fast retransmission handshake vulnerabilities.

a) 4-way Handshake Key-Reinstallation Attack

Mutual Authentication takes place in all WPA2 secure networks based on a shared secret called Pairwise Master Kay

(PMK) that is used to generate session keys called Pairwise Transient Key (PTK). PMK is produced based on two random numbers called SNonce and ANonce. SNonce is generated at the Access Point while ANonce Is generated at the client. Practically, attackers may capture and replay the third message of the handshake four messages, which includes the session PTK. This enforces resetting the incremental Nonce and replay counter allowing the attackers to decrypt transmitted data regardless of the applied EAP method nor the confidentiality Protocol.

b) Group Key Handshake Key-Reinstallation Attack

Group Key Handshake takes place directly after the 4-way handshake. Two EAPOL messages exchange the encrypted group key (GTK), which is used for encrypting multicast transmitted messages. The main vulnerability behind group key reinstallation is the acceptance of any previously used replay counter at the authenticator. Thus if the attacker blocks and captures the second message of the group key handshake and replays it later, the authenticator will practically install the dated GTK because the authenticator match the replay counter with any used replay counter in the group key handshake.

c) Fast Transition Handshake Key-Reinstallation Attack

Although 802.11r amendment is developed mainly to protect 802.11 networks against key reinstallation, A recent attack [26] is performed for Wi-Fi networks using WPA2 personal mode. Fast transitions handshake is vulnerable in most Wi-Fi networks protected by WPA2 enterprise mode because 802.1x handshake is not required for roaming devices after new fast transition handshake. The re-association frames are based on previously derived session master key.

C. Availability Attacks

Availability attacks' objective is to stop or interrupt normal communication of an active wireless client or the entire network. Wireless Denial of Service (WDoS) is a prominent challenge that continuously faces wireless designers. Encrypting physical layer header is not possible in wireless communication because they contain important traffic parameters[1]. Therefore, jamming the physical layer is one of the most effective attacks against wireless networks. Exhausting resources of the communicating peers by floods of spoofed-source traffic is another effective attack that targets the transport layer. A recent paper surveyed Denial Of Service (DOS) attacks based on the different layer of the OSI model [27]. Public key cryptography utilized in EAP methods is major defense against WDOS. Unfortunately initial MAC layer frames can easily be sniffed during legacy authentication and association phases because keying material is not available before exchanging the cryptographic keys. In additions, it is not possible to cipher the probing, beacon and legacy 802.11 authentication/association frames without a long-term shared key. Thus an attacker can send continuous de-authentication frames to the client or access point, with a spoofed MAC address[28]. De-authentication DOS exploits the 802.11 management frames. These frames does not require any encryption even when the session is established with the confidentiality protocol. The attacker only needs to know the victim's MAC address, which can easily be retrieved by network monitoring. Thus, EAP-TLS, EAP TTLS and EAP-PEAP are all vulnerable to de-authentication and de-association attacks.

Table 2
Impact of recent attacks on EAP authentication

Attacks	EAP-TTLS	EAP-PEAP	EAP-TLS
Dictionary Attack	Vulnerable	Vulnerable	Resistant
Evil Twin	Vulnerable	Vulnerable	Resistant
Key Reinstallation	Vulnerable	Vulnerable	Vulnerable
Denial of Service	Vulnerable	Vulnerable	Vulnerable

V. PROPOSED SOLUTIONS AND RECOMMENDATIONS

To mitigate different risks that threaten wireless data transmission, several amendments must be added to the current security techniques applied in WPA2. These amendments should include at least the following security requirements to protect enterprise wireless networks against recent effective attacks.

A. Security Requirements for authentication attacks

Native authentication rejection after specific number of trials is a mandatory requirement to defend against online active dictionary attack. This closes the door against malicious intruders. However, multiple virtual clients' dictionary attacks that use spoofed MAC addresses may succeed to crack network access secrets. However, locking techniques decrease the possibility of penetration. Applying a dedicated application, certificate or a SIM card at the client must be enforced at the client in a cellular-style security for enterprise Wi-Fi networks. Identity hiding must be enforced because detecting the legitimate username make it easy for attacker to apply the dictionary attack.

B. Security Requirements for Confidentiality Attacks

New security requirements must be added to the current WPA2 state machine to resist against key reinstallation attacks. The first update is to prevent the re-use of Nonces during the 4-way handshake. Adequate replay counter in the group key handshake is required by not allowing acknowledgment with an already used replay counter within the same session. Another update should be enforced which is installing the GTK only after receiving acknowledgment from all supplicants.

C. Security Requirements for Availability Attacks

Amongst the open challenges for WDoS attacks is a valid defense against de-authentication attacks. Dedicated IDSs may be used in promiscuous mode to detect fake de-authentication based on transmission parameters by monitoring all traffic in the secure area. Our concern is to provide native protocol security. Legacy 802.11 authentication should undergo adequate update. Authenticating the de-authentication frames is an adequate solution. This can be applied by sending encrypted de-authentication frames within the established tunnel in addition to the clear-text frames for active communicating

clients. This will help detecting inappropriate de-authentication frames from rogue sender.

D. General Security Considerations

Other countermeasures should be considered. Using strong encryption and valid certificates for enterprise service that passes through 802.11 wireless medium. Periodic inductions and awareness sessions should be conducted for all users and administrators who deal with mobile devices and sensors. In additions, regular wireless security audits should be implemented to detect and mitigate the newly discovered vulnerabilities.

VI. Conclusions and Future Directions

This paper evaluates the performance and threat resistance of WPA2 enterprise using tunnel-based EAP, which is considered the most secure protocol-stack for enterprise wireless networks. Common authentication tunnel-based EAP methods were surveyed. This was followed by practical evaluation in terms of performance. The impact of recent enterprise WPA2 on these authentication protocols was studied. Recommended mitigation and amendments to resolve the detected holes were proposed. Finally we presented wireless attacks that threatens the future of wireless communication. This encourages the communication society to work for a new protection standard that natively protect sensitive data transmission. The new secure protocol stack for protecting the next generation of wireless communication should include several modification as discussed in the recommendation section to resist recent attacking techniques that threatens wireless authentication, confidentiality, and availability.

References

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

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

[3] J. R. Vollbrecht, B. Aboba, L. J. Blunk, H. Levkowetz, and J. Carlson, "Extensible authentication protocol (EAP)," 2004.

[4] 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.

[5] J.-C. Chen and Y.-P. Wang, "Extensible authentication protocol (EAP) and IEEE 802.1 x: tutorial and empirical experience," *IEEE communications magazine,* vol. 43, no. 12, pp. supl. 26-supl. 32, 2005.

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

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

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

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

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

[11] H. Andersson, S. Josefsson, G. Zorn, D. Simon, and A. Palekar, "Protected EAP Protocol (PEAP)," *draft-josefsson-pppext-eaptls-eap-05. txt, work-in-progress,* 2002.

[12] 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.

[13] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote authentication dial in user service (RADIUS)," 2070-1721, 2000.

[14] N. Cam-Winget, S. Hanna, H. Zhou, and J. Salowey, "Tunnel Extensible Authentication Protocol (TEAP) Version 1," 2014.

[15] N. Cam-Winget, D. McGrew, H. Zhou, and J. Salowey, "The flexible authentication via secure tunneling extensible authentication protocol method (EAP-FAST)," 2007.

[16] S. Hanna, K. Hoeper, H. Zhou, and J. Salowey, "Requirements for a Tunnel-Based Extensible Authentication Protocol (EAP) Method," 2012.

[17] D. Stanley, J. Walker, and B. Aboba, "Extensible authentication protocol (EAP) method requirements for wireless LANs," 2070-1721, 2005.

[18] M. Caneill and J.-L. Gilis, "Attacks against the WiFi protocols WEP and WPA," *Journal, no. December,* 2010.

[19] D. Bongard, "Offline bruteforce attack on wifi protected setup," *Presentation at Passwordscon,* 2014.

[20] J. Nam, J. Paik, H.-K. Kang, U. M. Kim, and D. Won, "An off-line dictionary attack on a simple three-party key exchange protocol," *IEEE Communications Letters,* vol. 13, no. 3, pp. 205-207, 2009.

[21] 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.

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

[23] H. Hwang, G. Jung, K. Sohn, and S. Park, "A study on MITM (Man in the Middle) vulnerability in wireless network using 802.1 X and EAP," in *Information Science and Security, 2008. ICISS. International Conference on*, 2008, pp. 164-170: IEEE.

[24] A. Bartoli, E. Medvet, and F. Onesti, "Evil twins and WPA2 enterprise: A coming security disaster?," *Computers & Security,* 2018.

[25] P. Sharma, P. K. Kaushal, and P. R. Sharma, "Survey on Evil Twin Attack," *International Journal of Scientific Engineering and Research (IJSER),* vol. 4, no. 4, pp. 54-58, 2015.

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

[27] R. S. Singh, A. Prasad, R. M. Moven, and H. K. D. Sarma, "Denial of service attack in wireless data network: A survey," in *Devices for Integrated Circuit (DevIC), 2017*, 2017, pp. 354-359: IEEE.

[28] V. Poddar, R. Jaipur, and M. Chopra, "Detection of the de-authentication denial of service attack in 802.11 wireless networks," *Int. J. Sci. Eng. Res,* vol. 6, no. 10, pp. 150-158, 2015.