Available online at www.ijsrnsc.org

IJSRNSC

Volume-7, Issue-3, Jun 2019
Research Paper

www.ijsrnsc.org

Int. J. Sc. Res. in
Network Security
and Communication

ISSN: 2321-3256

A Proposed Model for Enhanced Security against Key Reinstallation Attack on Wireless Networks

G. Abare[1*], E. J. Garba[2]

[1,2]Department of Computer Science, Modibbo Adama University of Technology, Yola, Adamawa State, Nigeria

[*]Corresponding Author: abare4cplusplus@gmail.com, Tel.: +2347030097462

Received: 10/June./2019, Accepted: 18/June/2019, Published: 30/June/2019

***Abstract*—** Wireless network security is advancing consistently. This progress can be easily seeing by recounting the success stories achieved through the years since the modification of its first security protocol, WEP; then the WPA and finally the WPA2. The Wireless Protocol Access Pre-Shared Key (WPA2-PSK) mode is usually adopted by Small Office Home Office (SOHO) environments as it does not require a costly investment on a dedicated authentication system. Nevertheless, despite the fact that this mode was improved consistently, the core part (4-way handshake) still presents several vulnerabilities such as the key reinstallation attack (KRACK) which was discovered by Vanhoef and Piessens in 2016 and published in October, 2017. Here, we proposed an enhanced model which involved a Boolean variable that switches from true to false once the Key is installed; also, we include handshake messages encryption with Pair-wise Master Key as the encryption/decryption key, using Advance Encryption Standard (AES). Results obtained from the simulations of the enhanced model were compared with that of the existing model. The message execution time measured in micro seconds shows that the proposed model is more efficient than the existing four-way handshake model and it prevent the reinstallation of the Pair-wise Master key (PTK) during the handshake process.

***Keywords*—** Wireless Protocol Access, Wireless Local Area Networks Security, Pire-wise Transient Key, Group Temporal Key, Key Reinstallation Attack.

I. INTRODUCTION

The fast development in wireless technologies and introduction of Bring Your Own Device (BYOD) policy has creates opportunities for many small organizations to perform work using employees' laptops, smart phones, tablets and other mobile devices. However, new threats and attacks also emerged aiming to compromise the confidentiality, the integrity and/or the availability of these organizations. Therefore, securing the wireless infrastructure becomes a crucial step to achieving the overall network security. Broadcasting nature of wireless signal and different protocol vulnerabilities are the major security flaws of Wireless Local Area Networks (WLAN) and some remain threatened [10]. The mostly used cost effective technology to secure wireless network is Wi-Fi-Protected-Access-2 /Pre-Shared-Key (WPA2/PSK). The WPA2-PSK mode is usually adopted by Small Office Home Office (SOHO) environments, since it does not require a costly investment on a dedicated authentication system. Nevertheless, despite the fact that WPA2-PSK mode was improved consistently, and its history of security proofs though, the core part (4-way handshake) still presents several vulnerabilities such as the key reinstallation attack (KRACK). Here, the adversary tricks a victim into reinstalling an already-in-use key. According to [23], the KRACK attack is carried out by manipulating and replaying handshake messages and when reinstalling the key, associated parameters such as the incremental transmit packet number (nonce) and receive packet number (replay counter) are reset to their initial values.

In this paper, we analyzed various wireless security protocols and their vulnerabilities. We also compare some related works. We also analyzed the existing four way handshake model and its vulnerabilities to key reinstallation attack. Finally, we proposed an enhanced model to tackle key reinstallation attack on wireless networks.

II. WIRELESS SECURITY PROTOCOLS

A. Wireless Extended Protocol (WEP)

WEP was the first protocol designed to provide wireless security in terms of confidentiality, access control and data integrity for users implementing 802.11 wireless networks [21]. WEP was developed by a group of volunteer IEEE members [4]. Research conducted by [20], shows that the

WEP employs RC4 algorithm that was designed in 1987 by Ron Rivest. The encryption algorithm uses two key sizes: 40 bit and 104 bit; to each is added a 24-bit initialization vector (IV) which is transmitted directly. At the transmitter side, the plaintext is XOR'ed with the key stream generated after Key Scheduling Algorithm (KSA) and Pseudo-Random Generation Algorithm (PRGA) process of Rivest Cypher 4 (RC4) and cipher text is obtained. These steps take place in the reverse order at the receiver side using the same key. WEP uses Cyclic Redundancy Check (CRC-32). [9] show the WEP encryption and decryption processes in Figure1a and 1b respectively.

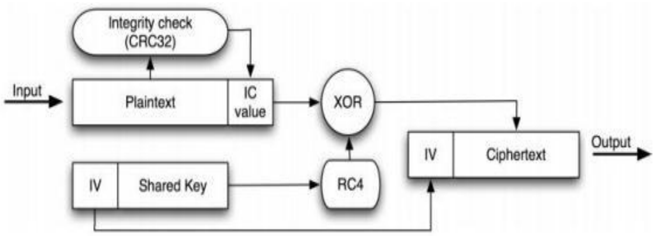

Figure 1a: WEP Encryption (Source: [9])

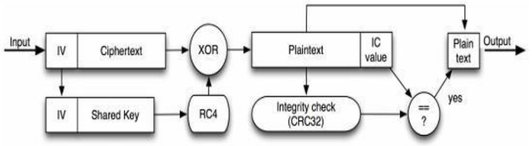

Figure 1b: WEP Decryption .Source: [9]

The WEP protocol quickly proved vulnerable to RC4 issues described in [17].The research shows two vulnerabilities in the RC4 encryption algorithm on WEP: invariance weaknesses and known IV attacks. The integrity check stage also suffers from a serious weakness due to the CRC32 algorithm used for this task. CRC32 is commonly used for error detection, but was never considered cryptographically secure due to its linearity [13] and [17] list weaknesses of WEP such as that it does not prevent forgery of frames or replay attacks, it uses weak RC4 keys and reuses Initialization Vectors (IV) which made data decryption possible with cryptanalytic methods or data modification without knowing encryption key and lack of key management.

It is indicated in Singh [18] that ICV algorithm is not a good choice for cryptographic hash. There are various off-the-shelf tools that exploit these vulnerabilities, allowing WEP keys to be recovered by analyzing the traffic as described in [3]. Through the years several attack techniques had been successfully implemented on the WEP. Some of the famously known attacks are: Flurhrer, Mantin and Shamir (FMS) attack described in [17], koreK attack, Fragmentation attack in 2005, Pynchkine-Tews-Weinmann (PTW) attack in [15] and Café-latte attack 2015.

B. *Wireless Protocol Access (WPA)*

The drastic weakness of the WEP to provide adequate security to its users has led the IEEE 802.11 committee to design and come up with an improved security standard that avoids most of the weaknesses that had previously doomed the WEP to failure. WPA addresses all known vulnerabilities in WEP by using a greatly enhanced encryption scheme, Temporal Key Integrity Protocol (TKIP) together with 802.1x/ EAP authentication.

TKIP is a major enhancement over traditional WEP protocol. Since Access Points and wireless interface cards are equipped with hardware necessary for WEP, TKIP was introduced to work on the same hardware for backward compatibility but with software enhancement for additional security as described Ozasa [15]. Another research work by [2] explains that TKIP uses a key hierarchy and key management methodology, by leveraging the 802.1x\EAP framework, and thus removes the predictability which intruders relied upon to exploit the WEP key. Moreover, it also uses the message Integrity Check (MIC), which is also commonly called Michael, on the data frames it sends to check the integrity of the data received. The steps for building of TKIP per-frame keys are showed in Figure 2 bellow.

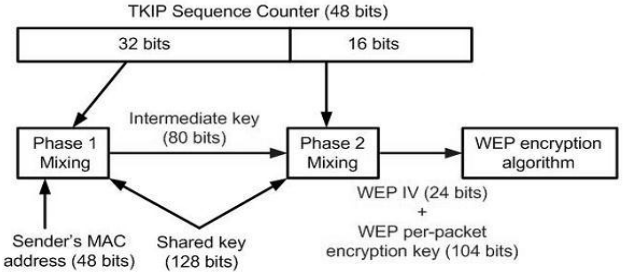

Figure 2: Construction of TKIP per-frame keys . Source: [2]

In 2005, Stanley [20] summarizes the benefits of WPA over WEP concisely. It summarizes that WPA applies strong network access control through mutual authentication, it supports 802.1x\EAP framework or pre-shared keys, adopts dynamic keys in TKIP which improves the key management, enforces data integrity through Michael MIC and provides forward compatibility to802.11i. The WPA security protocol, nevertheless avoided several of the WEP's weaknesses, as it has been subject to various attacks.

Benton [4] and Naamany [11], explain that the IEEE task Group I of the 802.11 was formed to replace the original authentication and privacy. The WEP algorithm provided by the initial 802.11 standard with an enhanced security as well as support to legacy protocols for backward compatibility. IEEE802.11i is based on IEEE 802.11 standard with security enhancement in the MAC layer. According to paper work by [11] several of the 802.11 standards (a, b, d, e, g, h, i, j) were rolled up into the new base 802.11 standard "IEEE 802.11-

2007" on March 8th, 2007. Networks compatible with the new security protocols are referred to as Robust Security Networks (RSNs).

Robust Security Network (RSN) as the term applied to the strongest security model that 802.11i uses to authenticate, authorize and protect the connection between the STA and AP according to [14]. It further explains the robust parts of the 802.11i standard: 802.1x for authentication and authorization, EAP for authentication transport and support for stronger message encryption and integrity mechanisms such as Counter Mode CBC-MAC Protocol (CCMP) and optionally Temporal Key Integrity Protocol (TKIP).

Pre-RSN stations cannot connect to an RSN network. An association between two RSN stations is referred to as Robust Security Network Association (RSNA). Each RSNA has its own unique set of keys and key lifetimes. This is necessary because RSN networks introduce an entirely new key management and authentication protocol in addition to new encryption algorithms [5].

C. Wireless Protocol Access 2 (WPA2)

The final IEEE 802.11i security protocol which fully implements the requirements of the 802.11i amendment is called Wi-Fi Protected Access Version 2 (WPA2). The predecessor, WPA was only designed as a transitional protocol to address the weaknesses found in WEP so it didn’t fully contain all the requirements of the 802.11i but it is supported in WPA2 for backward compatibility purpose. WPA2 differs from WPA because it includes specification for IBSS (Independent Basic Service Set), pre-authentication and Counter Mode CBC-MAC Protocol. The authentication piece of 802.11i (which include both WPA and WPA2) operates in two modes: *Personal* and *Enterprise* mode according to [6] and [1].

i. The Personal Mode

This mode requires the use of a PSK (Pre-Shared Key) and does not require users to be separately authenticated while in the Enterprise mode, which requires the users to be separately authenticated through the authentication server. The IEEE 802.1x authentication standard uses the Extended EAP (Extensible Authentication Protocol) which offers other EAP standards to choose from [14]. So both WPA2 and WPA enjoy two modes of operations which made them fit enough to organizational-level security while at the same time they are feasible to be used for Small Office/Home Office (SOHO) environments. There are five specific key types that are of particular interest in the 802.11i amendment; which are the Access Point Mac Address (APMAC) key, Pair-wise Master Key (PMK), Pair-wise Transient Key (PTK), Group Master Key (GMK) and Group Temporal Key (GTK).

According to IEEE 802.11 IEEE standard for information, the APMAC key is jointly negotiated between the Supplicant and the Authentication Server (AS).This key information is transported via a secure channel from the AS to the Authenticator. The pair-wise master key (PMK) is derived from the Pre-Shared-Keys along with the other information such as Server Set Identifier (SSID) and the SSID Length. The PTK is a key value used to protect unicast Medium access control (MAC) protocol Data Units (MPDUs) from that source and it is derived from PMK.

As stated in [8], a GTK is random value, assigned by the broadcast/multicast source, which is used to protect broadcast/multicast medium access control (MAC) protocol data units (MPDUs) from that source. It may be derived from GMK which is an auxiliary key used to derive a GTK.

Generally, a successful authentication process means that the station and the access point verify each other’s identity and generate some shared secret for subsequent secure data communication.

In case of Enterprise mode, the authentication server can be implemented either in an access point or through a separate server.

ii. Pre-Shared key (PSK)

This mode of operation is meant only for Small Office/Home Office (SOHO) environments where users don’t have to install the Authentication server. This mode is not safe to be used in an organizational mode. Since except for the 802.1x authentication all the phases are similar with the Enterprise’s mode.

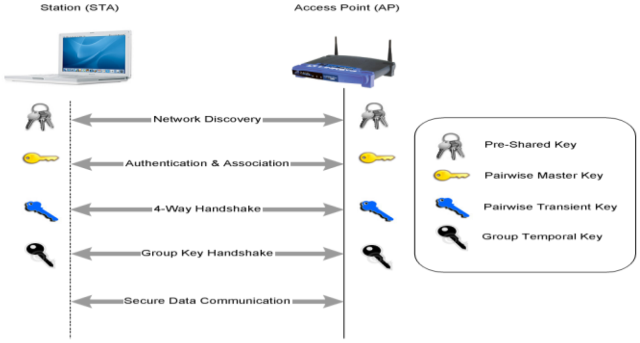

Figure 3: The 802.11i Authentication Procedures in PSK Mode. Source: [24]

iii. Enterprise Mode

In this mode the 802.1x authentication framework is deployed. Clients are authenticated separately. This mode is safe to be deployed for organizational level security.

III. RELATED WORK

WPA2 as the strongest security protocol of the IEEE 802.11i standard since it has implemented the block cipher AES which is much secure than the RC4 algorithm which was

used in previous security protocols [16]. But it is still vulnerable to several attacks due to transmission of unencrypted management and control frames and misuse of shared Group Temporal Key (GTK) among peers connected to the WLAN.
They proposed a solution to the Hole 196 vulnerability as follows: “First the authenticator can assign a random and unique GTK to every peer in the network. Then the access point generates a random and unique GTK and during a multicast or broadcast the sender sends encrypted text using its key to the access point. The access point then transmits the encrypted text along with the originating station’s GTK to the recipient stations. The recipient stations then decrypt the text at their end using this GTK. At the end of the session, a new GTK is assigned to the sender station. The authors claim that each peer connected to the network is unaware of the GTK of the rest of the peers.

The problem with this proposed solution is that there is no mechanism described that can possibly prevent any of the peers in the network from forging a valid group addressed data frame using a particular peer’s (or its own or a fake) GTK and broadcast it directly to other peers along the GTK value it used. Thus, distributing unique GTKs to each peer and when peers want to send a broadcast or multicast message, the AP’s sending of these GTK keys along the encrypted group addressed message to receiver peers does not prevent authenticated peers from forging a valid group addressed message. In this research paper there is no mechanism to control group addressed messages replay attacks.

The worst scenario is in this research clients can even generate a fake GTK keys and use it to encrypt a malicious data frame, they prepared, also which they want to send/ broadcast it as a group addressed data frame. This makes the existing Hole 196 vulnerability get worse because in the current case forging group addressed data frames possibility is limited to authenticated clients but according to this research’s proposal the Hole 196 vulnerability would also be open to outsiders or unauthenticated clients which makes the current hole only bigger and more dangerous than it is already.

The reason, unauthenticated clients are able to inject fake group addressed frames is because there is no notion of shared GTK within the associated clients of the WLAN. When a client receives a broadcast or multicast message, all it does is use the GTK that came along the received encrypted message and use it for decrypting the message. Even if the authors do not state it, if we assume clients check for the origin of received group addressed data frames, then spoofing the address of the access point would be sufficient. In general, this research does not provide a valid and thoroughly studied solution at all; it widens the Hole 196 vulnerabilities.

The “Hole 196” is the name of WPA2 vulnerability that was showcased by *Air Tight Networks* researchers in the Black Hat and *Defcon security conferences* in Las Vegas [7]. The vulnerability is, in fact, buried on the last line on page 196 of the 1232-page IEEE 802.11 Standard [8]. And that’s why AirTight Networks named the vulnerability as “Hole 196”.The vulnerability can lead to a potentially fatal insider attack, where an insider can bypass the WPA2 private key encryption and authentication to scan the authorized devices for vulnerabilities, install malware on these and steal personal or confidential corporate information from the devices. Although specifically mentioned for WPA2, the vulnerability applies to the WPA version also, irrespective of the authentication method used.

In order to collect traffic data communication within the Wi-Fi which will be fed to the server for analysis, they claimed to use a tool from air cracking (2014) called Air serving which is a wireless card server. This tool allows multiple wireless application programs to use a wireless card independently via client-server TCP network connection. So it must be installed on every client node so that it can send the captured data frame to the server. This can be infeasible in corporate networks where there can be many clients because it will need to process each client’s action in the WLAN to build trust profiles and also it learns only little about client’s profiles or behaviors in smaller networks where the clients can be random (every time new clients joining and others leaving the WLAN – in places like Internet cafe).

Moreover, the author didn’t indicate what kind of approach is exactly used to analyze a data frame in order to categorize it as a risky or non-risky and also didn’t explain how the analysis can work to categorize/rate clients based on the reputation to score for any of the vulnerabilities including Hole 196.

Suggestion on how to prevent the WPA2 protocol from the Hole 196 was provided in [19]. The suggestion is to deprecate use of GTK and group-addressed data traffic and send broadcast or multicast data frames as unicast data frames because of the following arguments. APs in controller based WLAN architectures often do not broadcast data frames over the air. For backward compatibility, unique GTKs can be assigned to individual authorized Wi-Fi clients in the network. If data frames have to be broadcasted, then transmit as unicast.

The authors indicated the downsides of this approach can be an increase of throughput on the WLAN if broadcast traffic is sent as unicast. Sending every broadcast/multicast addressed data frame as a unicast data frame would totally destroy the notion of using broadcast/multicast data frames in the network. The very aim of using broadcast or multicast addresses is to achieve less overhead (things like encryption are done only once since the message is supposed to be the same copy at every receiver end) and then sending a once processed copy of the group addressed frame only to the desired receivers instead of doing processing a "frame x" *n* times for *n* number of recipients if it were going to be sent as a unicast data frame since the process of preparing the group addressed data frame for each user is supposed to be unique.

Preventions and countermeasures to prevent the Hole 196 vulnerability were suggested by [19]. There are end point security solutions that are client side software which can be used to detect ARP cache poisoning. But the two limitations of such end point security as listed in the research paper are:

1. Varieties of client devices connect to WPA2 secured Wi-Fi networks while such software is available only for either Windows or Linux running devices.
2. It is infeasible for a large scale environment as every end-point is supposed to install such client side software.

A mitigation of Key Reinstallation Attack in WPA2 Wi-Fi networks by detection of Nonce Reuse was proposed in [12]. The work involved monitoring of the Wireless interface of the device and the traffic going through the device and then alerts the victims that it's being attacked. This mitigation approach cannot completely prevent a victim from the KRACK attack but only provides alert to the victim that it's being attacked.

IV. PROPOSED MODEL

Here, we proposed a model which is free from Key Reinstallation Attack .The model is described in Figure 4.

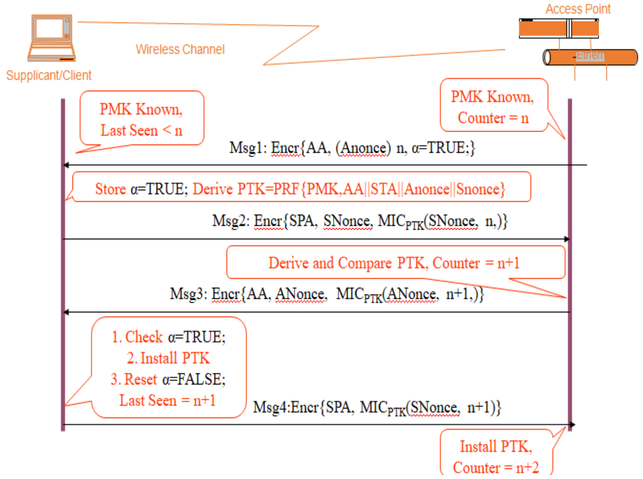
Access Point
Wireless Channel
Ethern
Supplicant/Client
PMK Known, Last Seen < n
PMK Known, Counter = n
Msg1: Encr{AA, (Anonce) n, α=TRUE;}
Store α=TRUE; Derive PTK=PRF{PMK,AA||STA||Anonce||Snonce}
Msg2: Encr{SPA, SNonce, MIC_PTK(SNonce, n,)}
Derive and Compare PTK, Counter = n+1
Msg3: Encr{AA, ANonce, MIC_PTK(ANonce, n+1,)}
1. Check α=TRUE;
2. Install PTK
3. Reset α=FALSE;
Last Seen = n+1
Msg4:Encr{SPA, MIC_PTK(SNonce, n+1)}
Install PTK, Counter = n+2

Figure 4: Proposed Model for Enhancing Security against Key reinstallation Attack.

The message flows are:
Message1: *Encpt* [**AMAC,. ANonce , SN** , and **α =TRUE**]
Message2: *Encpt* [**SMAC, SNonce , and PTK**]
Message3: *Encpt* [**AMAC,. SNonce ,** and **SN+1**]
Message4: *Encpt* [**AMAC, SN +1** and **MIC**]

A. *Discussion*

As stated in [22] and [23], the key reinstallation attacker established a man-in-the-middle (MitM) position between the supplicant and authenticator to trigger retransmissions of message 3 by preventing message 4 from arriving at the authenticator during the Handshake process. As the result, it will retransmit message 3, which causes the supplicant to reinstall an already-in-use PTK. In turn, this resets the nonce being used by the data confidentiality protocol.

To provide a solution to this problem, here we include encryption of the handshake messages Encryption in order to secure the generated Nonce and also Boolean variable which check the reinstallation of the key during the 4-way handshake Authentication process.

At first, the Access Point (AP) generates the ANonce, set the Boolean variable (***α***) to TRUE and then encrypt everything together with the AMAC as first message using the PMK as the Encryption/decryption key. The Supplicant then decrypts the First message using the same PMK as a decryption key and then stores the value of the Boolean variable (***α*).**

In the second step, the supplicant calculates PTK_S and SNonce and combined with its SMAC, all encrypted as second message. Once the Access Point (AP) receives the second handshake message, it decrypts the message, calculate PTK_A and compare it with PTK_S. It reset the SN=SN+1 and package message3 with MIC and forward it to the Supplicant. Otherwise it terminates the handshake process.

In order to ensure that a key is only installed once, the supplicant after decrypting the third message and it then check for the value of alpha. If the value is still at its initial stage i.e if is still **α = TRUE**, then it carry out the installation of the key (PTKs) and reset **α = FALSE** before sending the fourth message to the Authenticator. Otherwise it terminates the handshake process.

The fourth message is like confirmatory message and once the AP receive this message, it then installed PTK_A, increment the packet number (**SN=SN+2**). Immediately, packet exchange starts between the Access Point and the Client.

B. *Result Analysis Between Existing and Proposed Model*

The average execution time in microseconds from the proposed model and existing model were taken and compared. The Result is presented in table 1.

Table 1: Results Comparisons

Handshake Message	Existing Model (Exc. time in micro second)	Proposed Model (Exc.time in micro second)
Message1	0.00069	0.00029
Messahe2	0.00038	0.00038
Message3	0.00053	0.00035
Message4	0.00024	0.00022

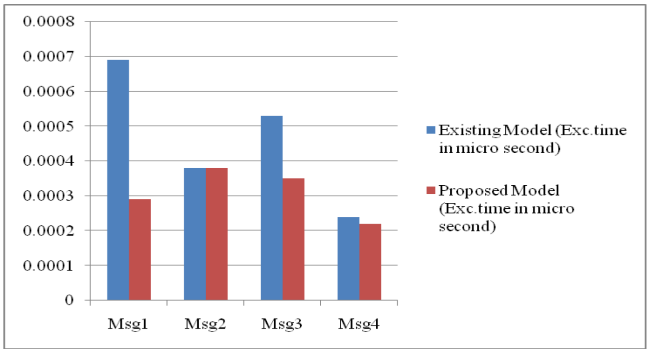

Figure 5: First Results Analysis between the Proposed and the existing Model.

V. CONCLUSSION

The key Reinstallation Attack targets the four-way handshake used to establish a nonce (a kind of "shared secret") in the WPA2 protocol. The adversary tricks its victim into reinstalling an already-in-use key by manipulating and replaying handshake messages and when reinstalling the key, associated parameters such as the incremental transmit packet number (Nonce) and receive packet number (replay counter) are reset to their initial values.

In this work we proposed an enhanced model to prevent the KRACK attack. Our proposed model involves encrypting of the entire handshake messages and the Nonce values generated. Here, we proposed an alpha check (a kind of Boolean switching) which switches from 1 to 0 when the Pair-wise Transient Key (PTK) is first installed. To prove the efficiency of the proposed model, the results obtained from the comparison between the two models in terms of average execution time was measured in micro second and it shows how the proposed model performed better.

This proposed model will help in enhancing security at the four-way handshake authentication process against reinstallations of the Pair-wise Transient Key.

REFERENCES

[1] Alblwi, S., & Shujaee, K. (2017). A Survey on Wireless Security Protocol WPA2. In *International Conference Security and Management*.

[2] Alliance, W. F. (2001). Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks. *White paper, University of Cape Town*, 492-495.

[3] Arana, P. (2006). Benefits and Vulnerabilities of Wi-Fi Protected Access2 (WPA2). INFS 612–Fall.

[4] Benton, K. (2010). The evolution of 802.11 wireless security. *Journal, UNLV Informatics- Spring, n. INF*, 795, 1-56.

[5] Hailemariam, M. A. (2016). *Securing the Transmission of Group Addressed Data Frames by Enhancing the IEEE 802.11i Security Protocol* (Doctoral dissertation, Addis Ababa University).

[6] He, C., & Mitchell, J. C. (2004). Analysis of the 802.11 i 4-Way Handshake. In *Proceedings of the 3rd ACM workshop on Wireless security* (pp. 43-50). ACM.

[7] He, C., Sundararajan, M., Datta, A., Derek, A., & Mitchell, J. C. (2005). A modular correctness proof of IEEE 802.11 i and TLS. In *Proceedings of the 12th ACM conference on Computer and communications security* (pp. 2-15). ACM.

[8] IEEE 802.11 Working Group. (2010). IEEE standard for information technology–Telecommunications and information exchange between systems–Local and metropolitan area networks–Specific requirements–Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Wireless Access in Vehicular Environments. *IEEE Std*, *802*(11).

[9] Kumkar, V., Tiwari, A., Tiwari, P., Gupta, A., &Shrawne, S. (2011). Vulnerabilities of Wireless Security protocols (WEP and WPA2). *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, *1*(2), pp-34.

[10] Liu, Y. L., & Jin, Z. G. (2015). SAEW: A security Assessment and Enhancement System of Wireless Local Area Networks (WLANs). *Wireless Personal Communications*, *82*(1), 1-19.

[11] Naamany, A. M., Al Shidhani, A., &Bourdoucen, H. (2006). IEEE 802.11 wireless LAN security overview. In *IJCSNS* (Vol. 6, No. 5B, p. 138).

[12] Naitik, T., Raiton L., Pradnya, V., & Vamshi, S. (2018). Mitigation of Key Reinstallation Attack in WPA2 Wi-Fi networks by detection of Nonce Reuse. *International Research Journal of Engineering and Technology (IRJET)*, *5*(5),pp-4.

[13] Nikita, B., Ian, G., & David, W.(2001).Intercepting Mobile Communications. *The Insecurity of IEEE802.11*. 7th Annual International Conference on Mobile Computing and Networking, July 2001.

[14] Nowicki, G. D. (2004). Wireless Security:The Draft IEEE 802. 11i Standard.

[15] Ozasa, Y.,2007. A Study on the Tews-Weinmann-Pyshkin Attack Against WEP. *IEICE Technical Report 2007*, *2007*: pp. 17-21.

[16] Rajotiya, A. (2012). *Enhancing Security of Wi-Fi Network* (VOL. 3). International Journal of Computer Applications.

[17] Scott R. F., Itsik, M., & Adi S. (2001). *Weaknesses in the Key Scheduling Algorithm of RC4*," In Selected Areas in Cryptography , Vol. 2259 of Lecture Notes in Computer Science, pp. 1-24.

[18] Singh, S., & Amit G. (2014). Study and Analysis of Dictionary attack and Throughput in WEP for CRC-32 and SHA-1. *International Journal of Computer Applications 96*.(pp. 15-18).

[19] Sohail, A. (2010). WPA Too! *Airtight Networks, DEF Conference 18*

[20] Stanley, D., Jesse W., & Bernard, A. (2005). Extensible Authentication Protocol (EAP). *Method Requirements for Wireless LANs*. Request for Comments 4017.

[21] Vanhoef, M., & Piessens, F. (2013). *Practical verification of WPA-TKIP vulnerabilities*. In ASIA CCS. ACM (pp. 427–436).

[22] Vanhoef, M., & Piessens, F. (2016). Predicting, Decrypting, and Abusing WPA2/802.11 Group Keys. In *USENIX Security Symposium* (pp. 673-688).

[23] Vonhoef, M., & Piessens, F. (2017). Key reinstallation attacks:Forcing nonce reuse in WPA2. *In Proceeding of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1313 – 1328). ACM.

[24] Xing, X., Shakshuki, E., Benoit, D., &Sheltami, T. (2008). Security analysis and authentication improvement for ieee 802.11 i specification. In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE* (pp. 1-5). IEEE

Author Profile

Dr. Etemi Joshua Garba (PhD, MEng, BSc) is a Consultant in Data Science, Software Engineering and Multimedia Technology. He is also a Senior Lecturer (Assistant Professor) in the department of Computer Science at the Federal University of Technology (Modibbo Adama University of Technology), Yola, Adamawa State, Nigeria. He is a graduate of B.Sc. Computer Science and has Master Degree in Software Engineering from the St. Petersburg State University of Information Technology, Mechanics & Optics. St. Petersburg, Russia. He has 14 years of experience in teaching, research and community development. He is a member of Institute of Electrical and Electronics Engineers (IEEE); member of editorial board of peer-reviewed Software Engineering Journal and member of editorial board of peer-reviewed American Journal of Software Engineering and Applications.

Mr. G. Abare holds Bachelor degree of Technology (B.Tech) in Computer Science from Modibbo Adama University of Technology, Yola in 2011 and Masters Degree (M.Tech) in Computer Science from Modibbo Adama University of Technology, Yola in the year 2019. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT and software.