Scientific Research Publishing

Wireless Engineering and Technology, 2021, 12, 15-22
https://www.scirp.org/journal/wet
ISSN Online: 2152-2308
ISSN Print: 2152-2294

Wi-Fi: WPA2 Security Vulnerability and Solutions

Zahoor Ahmad Najar[1], Roohe Naaz Mir[2]

[1]Deaprtment of IT, Central University of Kashmir, Srinagar, India
[2]Department of Computer Science and Engineering, National Institute of Technology, Srinagar, India
Email: zahoornajar@cukashmir.ac.in, naaz310@nitsri.net

How to cite this paper: Najar, Z.A. and Mir, R.N. (2021) Wi-Fi: WPA2 Security Vulnerability and Solutions. *Wireless Engineering and Technology*, **12**, 15-22.
https://doi.org/10.4236/wet.2021.122002

Received: September 9, 2020
Accepted: April 15, 2021
Published: April 18, 2021

Abstract

The Internet of Things (IoT) is an emerging network infrastructure with more than five devices owned by a single user. Wireless connectivity forms the backbone of such infrastructure. IoT uses diverse wireless communication technologies such as IEEE 802.15.4, Wi-Fi, Zigbee, Bluetooth, RFID, BLE (Bluetooth Low Energy), and various other cellular technologies. Wi-Fi is most suitable for IoT Home or office networks. Practically wireless signals do not adhere to the boundaries of the office or home, or organization and impose inherent security risks like information leakage, unauthorized access, other security and privacy threats to networking infrastructure. Therefore Authorization/Association of devices is one of the main security concerns. This paper discusses how unauthorized access to wireless networks (Wi-Fi) can be secured by improving existing WPA2 protocol security.

Keywords

Wi-Fi, WPA2, SHA-512, IoT

1. Introduction

In the Internet of things, wireless connectivity forms the basis for connecting the devices to the Internet, especially in Smart Home or Smart office type networks. The number of devices is not less than four or five per person. Therefore it is imperative to have a robust security mechanism implemented so that only authorized devices can connect to the network; otherwise, it can lead to leakage of information or other malicious activities that will lead to different types of losses. In the Internet of things, speed and throughput are also equally important. So the choice of technology (wireless) is equally important. Wi-Fi being suitable technology for future IoT things other than Bluetooth Low Energy and

6LoWPAN [1]. Wi-Fi Technology provides the feasible data rates and throughput needed for IoT types of applications in Home or office networks. Therefore, it is important to look into the security aspect of Wi-Fi technology to secure IoT networks. So far as wireless network security is concerned, there are different types of security needs that need to be fulfilled, right from device authentication to data security. In this paper, our focus is on device association and security using Wi-Fi technology. We propose a solution to the existing Wi-Fi technology resistant to attacks like a dictionary or attaining a preshared key for network authorization.

2. Wireless Network Security Standards

IEEE 802.11 standard defines communication among networks at the MAC layer by exchanging three frames: viz, control frames, data frames, and management frames [2]. A robust security requirement at the MAC layer is to provide confidentiality, authentication, and Integrity of the frames to be exchanged. IEEE 802.11 defines models, namely pre-Robust and robust security networks, to secure the information Exchange in wireless networks [3]. The Pre-RSN (Robust Security Networks) includes Wired Equivalent Privacy (WEP), and Wi-Fi protected Access (WPA), while as RSN model uses a four-way handshake to provide authentication. IEEE 802.11 has defined three major security approaches, which are as follows:

1) WEP (Wired Equivalent Privacy);
2) WPA (Wi-Fi Protected Access);
3) WPA2/PSK.

Each protocol has two versions for personal and enterprise use.

2.1. Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy uses the RC4 cipher algorithm to encrypt data with a pre-shared key length of 64 to 128 bits. In this paper, we focus on the authentication of a device to a Wi-Fi Access Point. And we elaborate on the weakness in Authentication/Validation of the devices to the network using Wi-Fi. WEP protocol, due to numerous security flaws, has been denigrated by the Wi-Fi Alliance group [4].

2.2. Wi-Fi Protected Access (WPA)

Personnel WPA or WPA-PSK (Pre-Shared Key) used for home or organizational network with a key length of up to 256 bits. Commercial WPA uses 802.1x +EAP for authentication and replaces WEP with Temporal Key Integrity Protocol (TKIP) in this mode; no preshared key is used but instead RADIUS server is required. Robert Moskowitz released WPA weakness in a passphrase in November 2003 by capturing the four-way authentication handshake where an attacker can use the data to find passphrase using dictionary attack and found the key size of fewer than 20 characters is unlikely to resist the attack [5].

2.3. WPA2/PSK

Wi-Fi Protected Access-II, which uses Advanced Encryption Standard (AES), is the most robust and secure protocol. WPA 2 supports two modes of security viz "home User" and "Corporate User". A pre-shared passphrase or passkey is used in home user mode, and Access points are manually configured for the authentication [6]. However, it is not resistant to the attacks that can be carried through Aircrackng or Dictionary Attack for obtaining the Preshared Kay in Personnel Mode, *i.e.*, Home or Small Office networks. Although Enterprise mode is available with WPA2, authentication is carried through the RADIUS server, and no Pre Shared Key is used. However, it suffers from the vulnerabilities of accessing the open network devices like Camera, etc., and hence enterprise mode of WPA2/PSK is not secure.

The following are the vulnerabilities that exist in Wi-Fi networks and are addressed by our proposed solution.

Rogue Access Point: the adversary creates the rogue Access Point and broadcasts the Legitimate SSID, allowing the legitimate device to connect to the Fake access point with a legitimate Pre-shared Key. Hence obtains the Key which the adversary uses for authentication to the network.

De-authentication: the attacker imitates the Access Point with the MAC address of the Legitimate device and forces the device to re-associate. And eavesdrop on the beacons transmitted for re-association by the device which contains the legitimate Key. And Key can be easily acquired using Dictionary attack or Aircrackng, using Kali Linux. The network standards discussed above provide security that is insufficient to meet the present demand of security, especially in a wireless environment with no defined boundaries. The researchers have proposed several solutions, as discussed in the forthcoming section.

Mannon Mustafa *et al.* [7] proposed a one-time pad solution requiring the active cell phone number of the user to send the unique ID. Mina Malekzadeh *et al.* [8] suggested using HMAC-SHA-1 to secure management frames against the Deauthentication and re-association Attacks [9]. Bicakci *et al.* [10] WPA2 security protocols are vulnerable to Denial of Service (DoS) Attacks using re-authentication and re-association. Zhang *et al.* [11] proposed using the MAC filtering mechanism where a smart client can differentiate between legitimate and non-legitimate frames. Odhiambo *et al.* [12] proposed an Integrated Security Model(ISM), which incorporates a drop policy to avoid DoS attacks.

As described by Aqeel-ur Rehman *et al.* [1], Wi-Fi is suitable for future IoT. Therefore, it is obvious to emphasize on security concerns of Wi-Fi technology. Data rates and bandwidth available in Wi-Fi best among other technology for interconnection in IoT, which is the biggest motivation to make Wi-Fi technology better.

3. Proposed Methodology

WPA2 being a robust protocol in terms of authentication and confidentiality. WPA2 comes in two versions for home and enterprise use. Other security

schemes like RADIUS server authentication in the Enterprise version are robust and provide authentication with other openness. However, it is still vulnerable to several attacks as an association to the network is without any security, allowing them to attack networks. In-home networks, especially IoT, it is expensive to have a RADIUS server in place. So based on the available technology (Wi-Fi), use of pre-Shared Key for authentication to the Devices, is still a good choice for the Home IoT infrastructure. But WPA2 protocol is weak in terms of the attacks carried through Kali Linux. It is easy to obtain the Pre Shared Key, the reason being the key length is 128 to 256 bits which even encrypted using AES is still vulnerable to dictionary attack. In this paper, we propose wherein authentication does not involve any preshared key transmission at the time of association or re-association. Pre Shared Key will be shared among the users through manual means. Once the authentication process is to be established, the Hash of the Pre Shared Key will be transmitted and checked for the authenticity of the users (devices) to be connected to the Access point in Home or Enterprise networks. The process of the handshake is shown (Figure 1).

In the proposed method, SHA-512 is used to calculate the Preshared Key Hash, which can be of variable length 64-256 bits. The Hash value, even if captured, cannot be used by the adversary for the association to the network.

Let Pk denote the Pre Shared Key of length 64 to 256 bit, and H denotes the hash code of the Pk calculated using SHA 512 algorithm.

From the client-side hash code (H') is calculated as shown at Equation (1):

$$H' = \text{SHA-512}(Pk, t) \tag{1}$$

Access Point also calculates the hashcode (H) is calculated as shown in Equation (2)

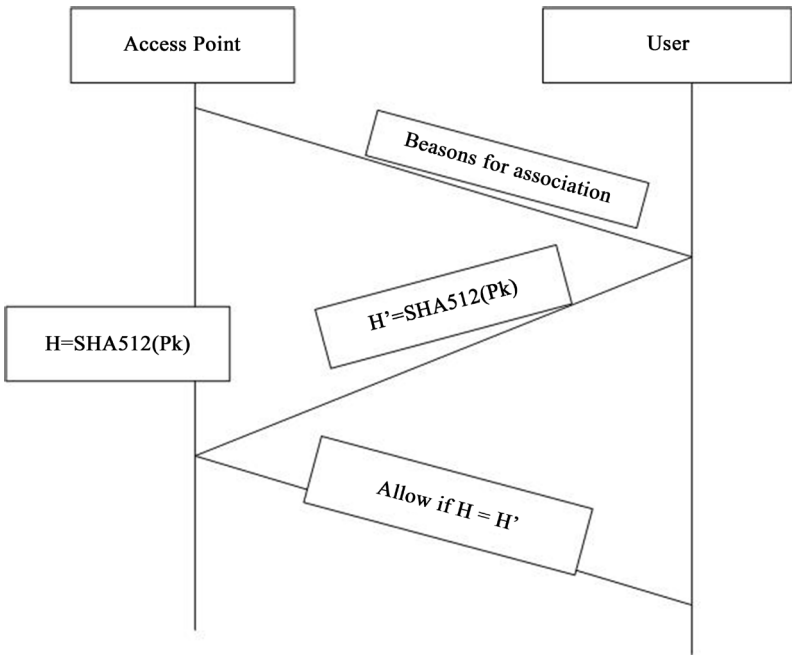

Figure 1. Secure Hand Shake at the time of association of user with accesspoint.

$$H = \text{SHA-512}(Pk, t) \quad (2)$$

H and H' are compared at the access point side, and if both are similar devices are authenticated else, device association is rejected.

Variable-length input Preshared key (Pk) and timestamp (t) are used to obtain 512-bit output code transmitted from device to Access point for authentication, is very difficult to be compromised and therefore discourages the adversary. Thus the solution is reliable and energy-efficient for the device authorization to the Home or Enterprise networks. The security of such a cryptographic hash algorithm is that if a single character is changed in the Preshared Key, the hash code obtained results in several changed bits, as depicted in Figure 2. That is a characteristic of an avalanche effect. The avalanche effect characterizes the robustness of an algorithm against the known types of attacks. Therefore, brute force attack is difficult to be carried out

Table 1 shows the same length preshared Key with a single character change (*i.e.* 8-bit change at the most) and the corresponding change in output code *i.e.*, Hash code. The graph shown in Figure 2 depicts the frequency of bits change where along y-axis, the bit position from 0 - 511 and along x-axis bit values 0 and 1 is depicted. The proposed method is resistant to Rouge Access Point attack wherein an Adversary uses a legitimate SSID.

4. Discussions

The proposed method can be implemented using SDN Technology. With the North Bound Interface (NBI) applications. An app is to be used to implement SHA-512, which can push the security protocol to layer 2 for user authorization. The enhancement of SHA-512 augments the security of WPA/PS2 in many ways:

1) The key size (Hash Length in the proposed scheme) is 512 bits compared to 256 bits. Hence will require more computing resources to check the Key (not possible through the tools available).

2) Pre-Shared Key is not transmitted, but its Hash is transmitted, which cannot be obtained even if adversary gets hold of the transmitted Hash Code for Association to the Wi-Fi.

3) By changing the single character in the pre-Shared Key the good avalanche effect is observed in Figure 2.

4) No replay attack is possible as the session is time stamped.

Table 1. Shows different passcodes with no of bits change on changing a single character.

Pre Shared Key (64 bit)	No of Bits change in output hash (512 bit)
Passkeys	Reference key
Passkays	259
Pesskeys	260
Passqeys	264

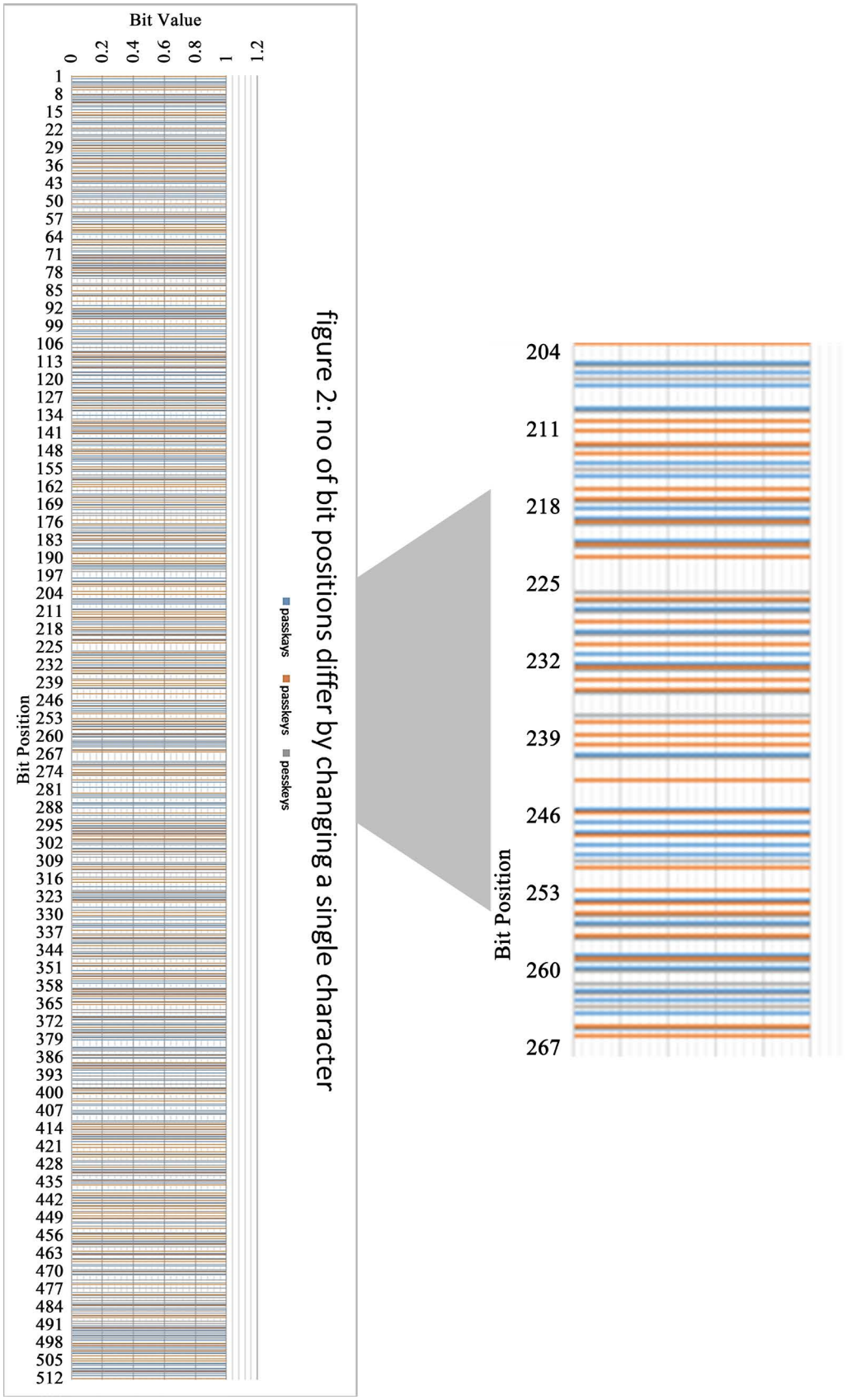

Figure 2. Change in bit position(s) of 512 bit code on changing single character of passcode.

5. Conclusion and Future Work

The proposed solution is robust to withstand cracking, as the hash code length is 512 bits long against the preshared Key of 128 bits only. That is double than AES code (256 bits), hence resistant to the dictionary attack (to which WPA2 is vulnerable) and attacks carried using aircrackng tools. Moreover, the variable-length Pre Shared Key incorporates more confusion to the Brute force attack. However, the solution is more reliable and viable for IoT to be connected to the devices as it needs no extra energy for the process. Deauthentication and re-association vulnerability proposed by Achilleas Tsitroulis *et al*. [13] using rogue access points are impossible as the adversary gets an instance of Hash Code that cannot be used as a Pre-shared key. Timestamps to the Hash code can be included to resist replay attacks. The handshake mechanism based on the public-key method can be employed instead of the symmetric Key with the available key distribution techniques.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Aqeel-ur-Rehman, K.M. and Ahmed, B. (2013) Communication Technology That Suits IoT—A Critical Review. CCIS Springer-Verilag, Heidelberg.

[2] Taskin, M. (2008) WEP Post Processing Algorithm for Robust 802.11 WLAN Implementation. *Science Direct*: *Computer Communication Journal*, **31**, 3405-3409.

[3] Sheila, F. (2007) Establsihing Wireless Robust Security Networks. NIST Special Publication, Gaithersburg.

[4] The Wi-Fi Alliance (2012) The State of Wi-Fi ®Security. https://davidhoglund.typepad.com/files/20120229_state_of_wi-fi_security_09may2012_updated_cert.pdf

[5] John, L.M. (2005) Auditing Wi-Fi Protected Access (WPA) Pre Shared Key Mode. *Linux Journal*3. https://www.linuxjournal.com/article/8312

[6] Arash, H.L., Mir, M.S.D. (2009) A Survey on Wireless Security Protocols (WEP, WPA and WPA2/802.11i). *2009* 2*nd IEEE International Conference on Computer Science and Information Technology*, Beijing, 8-11 August 2009. https://doi.org/10.1109/ICCSIT.2009.5234856

[7] Mannon M., Najar, Z.A. and Abdul Jawad, M. (2017) An Approach to Secure 802.11 Authentication Process Using One Time Pad Concept. *International Journal of Recent Scientific Research*, **8**, 20270-20272.

[8] Mina, M., Abdul, A., Zunata, A. and Zaton, M. (2007) Security Improvement for Management Frames in IEEE 802.11 Wireless Networks. *International Journal of Computer Science and Network Security*, **7**, 276-284.

[9] Chibiao, L. and Jame, Y. (2007) A Solution for WLAN Authentication and Association Attacks. *International Journal of Computer Science*.

[10] Bicakci, K. and Tavli, B. (2009) Denial of Service Attacks and Countermeasures in IEEE 802.11 Wireless Networks. *Computer Standards and Interfaces*, **31**, 931-941.

[11] Zhang, Y. and Sampalli, S. (2010) Client-based Intrusion Prevention System for 802.11 Wireless LANs, WiMob2010. *Proceedings of the 6th International Conference IEEE 2010 on Wireless and Mobile Computing, Networking and Communication*, Niagara Falls, 11-13 October 2010, 100-107. https://doi.org/10.1109/WIMOB.2010.5644978

[12] Odhiambo, O.N, Biermann, E. and Noel, G. (2009) An Integrated Security Model for WLAN. *AFRICON 2009*, Nairobi, 23-25 September 2009, 1-6. https://doi.org/10.1109/AFRCON.2009.5308183

[13] Achilleas, T., Dimitris, L. and Emmanuel, T. (2014) Exposing WPA2 Security Protocol Vulnerabilities. *International Journal of Information and Computer Society*, **6**, 93-107. https://doi.org/10.1504/IJICS.2014.059797