Enhanced WPA2/PSK for Preventing Authentication Cracking

Chin-Ling Chen[1(✉)] and Supaporn Punya[2]

[1] Department of Information Management, National Pingtung University, Pingtung, Taiwan
clchen@mail.nptu.edu.tw
[2] Department of Computer Science, RMUTT, Klong Luang, Thailand

Abstract. With the popularization of mobile phones and Wi-Fi hotspots, the diversification of wireless communication applications has rapidly growing. Wi-Fi Protected Access (WPA), offered by network user authentication and communication encryption, is the most generally used mechanism to protect users in wireless networks. This paper has discussed the weakness of 4-way handshake procedure in Wi-Fi Protected Access 2/Pre-Shared Key (WPA2/PSK) and proposed an enhance WPA2/PSK by adding timestamp parameter to prevent authentication cracking. The experiments have compared WPA2/PSK with Enhanced WPA2/PSK cracking using Kali Linux tool and the result is given.

Keywords: WPA2/PSK · Authentication cracking · Kali Linux tool

1 Introduction

Recently, mobile APPs are developing at a rapid pace. The security measures taken in detecting and preventing for attack cannot be ignored. Several researches have introduce the various threats and vulnerabilities related to 802.11 wireless networks. How to conduct ethical hacking and make wireless network more secure is a matter of the concern to management.

Reddy et al. (2010) have discusses the entire process of cracking WEP encryption on Wi-Fi networks, focusing on manipulating some scanning tools, such as: Cain, NetStumbler, Kismet, and MiniStumbler, to assist ethical hackers or security management in understanding the investigation of wireless security and testing to strengthen security [1]. Wi-Fi Protected Access (WPA) is the evolved version of WEP. Some studies have discussed the security issues of WPA/WPA2 encryption methods for wireless networks and have analyzed how to crack them. WPA2 now is widely deployed in Wi-Fi communication to combat wireless attacks due to its efficiency and security. WPA2 is considered a Robust Security Network (RSN) capable protocol because of supporting the process of authentication and exchange of cryptographic keys between station (STA) and Access Point (AP).

There are two modes for WPA2 targeting the different users: WPA-Personal and WPA-Enterprise. WPA-Personal is for home and small office use, requiring

W. Li and D. Tang (Eds.): MOBILWARE 2020, LNICST 331, pp. 156–164, 2020.
https://doi.org/10.1007/978-3-030-62205-3_15

no authentication server. All wireless devices, such as mobile phones and laptop computers, in the same hotspot use the same 256-bit pre-shared key (PSK), called as WPA2/PSK. On the other hand, WPA-Enterprise is designed for large businesses and requires a RADIUS authentication server that provides automatic key generation and authentication throughout the entire enterprise. However, advanced versions of new wireless attacks have been developed, which is capable of exploiting the vulnerabilities of WPA2-Enterprise.

Cui and Yin (2011) have conducted some experiments on WEP and WPA/WPA2 encryption modes [2]. Some effectual findings have been proposed based on these results. WPA uses a pre-shared key (PSK) for authentication and encryption, causing limited degree of protection. If hackers hold a PSK, they can eavesdrop on other authorized users. Alqahtani and Aloraini have proposed an improved version of Wi-Fi encryption, called Wi-Fi Secure Access (WSA), reducing limitations of WPA protection and offering more confidentiality [3].

In Linux-like systems, BackTrack5 has been used to capture WPA/WPA2 4-way handshake encrypted packets. Zhang et al. (2012) have proposed a new cracking method, in which the captured handshake packets are copied to window system and then cracked with EWSA-GPU [4]. Using a more capable GPU makes it easier to crack the password. Analysis result has proved that the proposed method can greatly improve the cracking speed by comparing BackTrack5.

Pandurang and Karia (2015) have used OpenVPN, located at the entrance of the wireless local area network (WLAN), to set up a tunnel within public network. Performance metrics of WLAN WEP and WPA2, such as throughput, delay, and frame loss rate are measured [5]. Penetration tests have been performed via Backtrack5 R3 and Fern Wi-Fi Cracker. Yacchirena et al. have used Snort and Kismet as Wi-Fi intrusion detection systems (IDS) and used Ettercap monitored IDS response [6]. Subsequent evaluations after the attack have been given. This study has analyzed the captured traffic with Wireshark to determine the response characteristics of Snort and Kismet. Radivilova and Hassan have analyzed wireless network security algorithms WPA and WPA2, whose weaknesses are described [7]. The ways of how to attack WPA and WPA2 Enterprise Wireless Networks and the results are also given. Abo-Soliman and Azer have clarified emerging attack methods and have implemented WPA2/EAP-TTLS prototypes for testing and evaluation [8]. Chang et al. have proposed an Intelligent Deauthentication Method (IDM) to capture the encrypted packets for analysis [9]. The proposed method has the capability of determining the length and strength of de-authentication decisively.

Authentication is one of the major security objectives for any wireless protocol. It ensures that associated STAs are really those who they claim. Both Dictionary attacks and Brute force are the most common methods that target authentication by stealing access pin, key, password or passphrase. To obtain a password is the best way to control the AP. The first step in authentication cracking is to obtain an encrypted packet, held by the four parties. However, there is no detailed description on how to obtain it. In this article, we have analyzed WPA2-personal supporting 4-way handshake, and described the basic

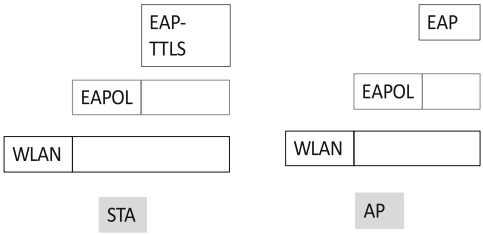

Fig. 1. Layer structure of EAP-TTLS/EAP/EAPOL/WLAN

principles, weaknesses, and launch the techniques of how to attack WPA2-personal in WLAN. The attack process and results are described. Finally, enhanced encryption is presented to counter cracking methods.

The rest of the paper is organized as follows. Section 2 describes fundamental principle of WPA2 and enhanced WPA2. Experiment and results are given in Sect. 3. Section 4 concludes this paper.

2 Fundamental Principle

2.1 Enhanced WPA2/PSK 4-Way Handshake

In WPA2/PSK, generation of the keys for authentication and data encryption during 4-way handshake comes from one shared passphrase agreed on both STAs and AP, which is carried by Extended Authentication Protocol (EAP). All the transmitted EAP messages between STA and AP are encapsulated in EAP over LAN (EAPOL) frames, which are further encapsulated in 802.11 WLAN format. EAP/EAPOL/WLAN messages allow handshaking between STA and AP without the need for IP layer. EAP-TTLS is one of Tunneled EAP method, which is usually a combination of two EAP methods: outer and inner authentication technique. The former creates a secure tunnel, while the latter performs user/device authentication. The layer structure is depicted at Fig. 1.

Enhanced WPA2/PSK 4-way handshake exchanges 4 messages between AP and STA. Let ANonce and SNonce be the randomly generated number at the AP and STA, respectively. AP sends the first message carrying ANonce to STA. STA generates PMK and PTK accordingly. Pairwise Master Key (PMK) is produced by Password based Key Derivation Function 2 (PBKDF2), in which passphrase combines timestamp, Service Set ID (SSID) and SSID length through 4096-time repeating hashing to generate a set of 256-bit key. In this regard, we call it as Enhanced-PMK (or Enhanced-PSK). A 384-bit Enhanced Pairwise Temporary Key (PTK) is generated by Pseudo Random Function (PRF), in which Enhanced-PMK associate with AP MAC address, STA MAC address, ANonce and SNonce. The Enhanced-PTK can be categorized into 3 sets of 128-bit keys. They are Key Confirmation Key (KCK), Key Encryption Key (KEK) and Temporal Key (TK). STA uses KCK as a key to calculate Message Integrity Code (MIC).

STA responds the second message carrying SNonce and MIC to AP. Consequently, AP generates its own MIC and then checks the integrity by comparing the received MIC. AP sends the third message, carrying Group Transient Key (GTK) protected by KEK, and MIC to STA. Since our objective is to authentication cracking for unicast transmission, GTK and TK can be ignored for the latter discussion and analysis. STA installs PTK and responds the fourth message back to AP to acknowledge the handshake completion.

2.2 Passphrase Cracking Procedure

We first search and display a list of detected APs and connected STAs in the surrounding. We obtain the frames from the selected channel and replay periodically in order to crack the traffic. In cracking WPA2/PSK encrypted packets, the key point is not to see how many packets are captured, but to capture the 4-way handshake packets. The 4-way handshake packets can be retrieved only when a new connection between AP and STA has established. If the handshake packet has not been captured successfully, we need to force to disconnected the exist and reestablish new one. Password/passphrase cracking can be attempted during association or periodic re-authentication. All STAs in the same WLAN use one shared passphrase to access the AP. It implies that successful passphrase cracking leads to providential access to all the keys during WPA2/PSK handshake. To prevent hacker to retrieve and crack other people's packets at will, we have proposed an Enhanced WPA2/PSK, in which time-stamp is added to generate a new PMK, called Enhanced-PMK. The time unit of time-stamp parameter in 802.11 is defined to be micro-second. AP and STA need to use its own time-stamp for making Enhanced-PMK to generate the individual MIC. The granularity of time-stamp for making an Enhanced-PMK could be tuned to be mini-second to make sure the integrity of MIC between AP and STA. However, coarse granularity of time-stamp may incur higher possibility of hacking by generating the same Enhanced-PMK, which will be $10^{-3} \times 10^{-3} = 10^{-6}$.

In next section, we try to crack both WPA2/PSK and enhanced WPA2/PSK encrypted packets.

3 Experiment and Results

An experiment is given to performance measurement of cracking technology for WPA2/PSK authentication. We have used the device like DIR-615 access points and DWL-G122 adapters from D-Link. The penetration procedures can be listed as below.

1. Install VirtualBox into your laptop.
2. Install Kali Linux Image on VirtualBox.
3. Plugin USB Wi-Fi external adapter to your laptop.
4. Use aircrack-ng tool to crack WPA2/PSK packets. Open Kali terminal and find out the name of the wireless adapter connected to the laptop by using command "iwconfig" (Fig. 2).

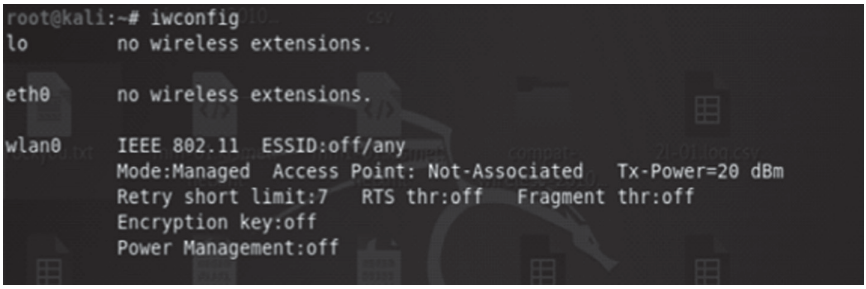

Fig. 2. Find out the name and related parameters of wireless adapter

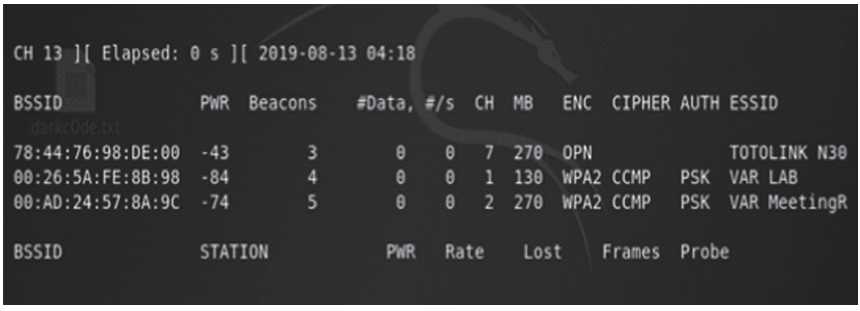

Fig. 3. Search APs in the surroundings and the STAs connected to that AP

5. Set the wireless adaptor in monitor mode by using command "airmon-ng".
6. Search the access points (APs) in the surroundings and also the clients connected to that AP by using command "airodump-ng" (Fig. 3).
7. Capture more packets for a specified channel by adding some parameters in the command "airodump-ng". In this case, the command will be "airodump-ng -c [channel] -b [bssid of wifi] -w [path to write the data of packets] [interface]"
8. The 4-way handshake packets can be retrieved only when a new client establishes a connection. If the handshake packet has not been captured successfully, we need to use airreplay-ng deauth command to force the disconnection and reestablish new one.
9. Force clients to reauthenticate to capture WPA2/PSK handshakes, which will appear on the "airodump" terminal. Leave "airodump-ng" running and open a second terminal. In this terminal, type the command "aireplay-ng [attack option] [n] -a [AP bssid] -c [client bssid] [interface]". In this case, [attack option] is "deauth" and [n] is the number of attacking (Fig. 4).
10. Obtain WPA2/PSK handshake packets and write into Packet Capture file (ar1-01.cap, in this case) in using the command "airodump-ng" (Fig. 5). The first line shows the current channel, elapsed time, current date/time, "WPA handshake: 00:26:5A:FE:8B:98". That means a WPA2/PSK handshake is successfully captured for the BSSID 00:26:5A:FE:8B:98.

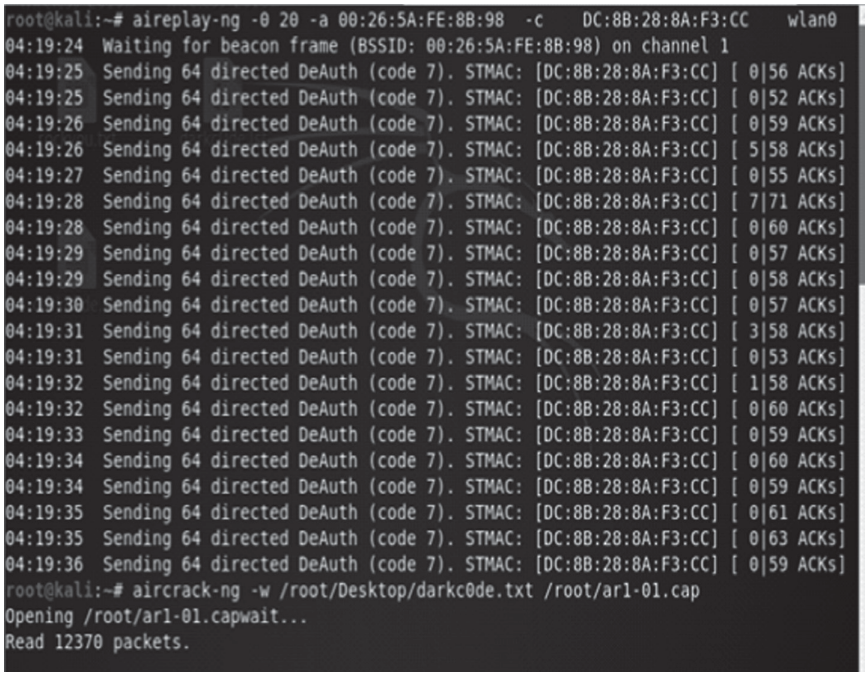

Fig. 4. Force clients to reauthenticate to capture WPA2 handshake messages

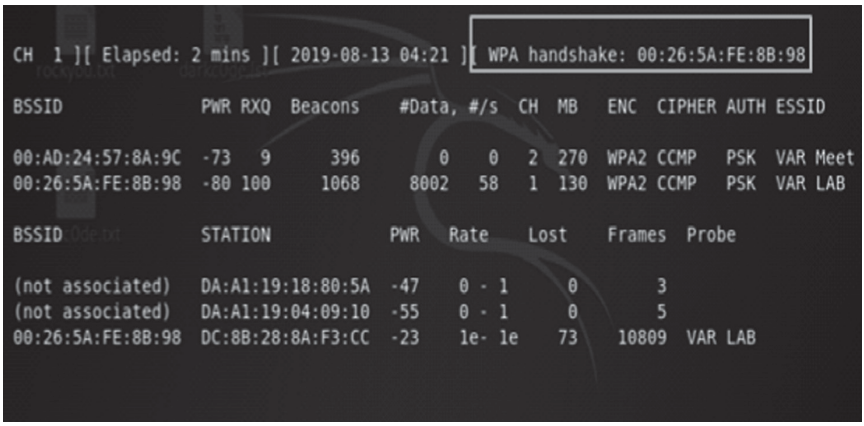

Fig. 5. Obtain WPA/WPA2 handshake message

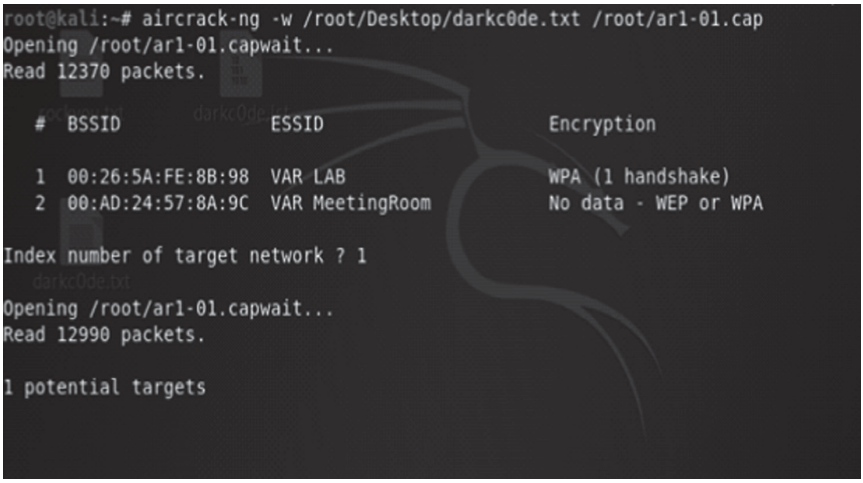

Fig. 6. Use Wordlist (.txt) and Packet Capture file (.cap) for authentication cracking

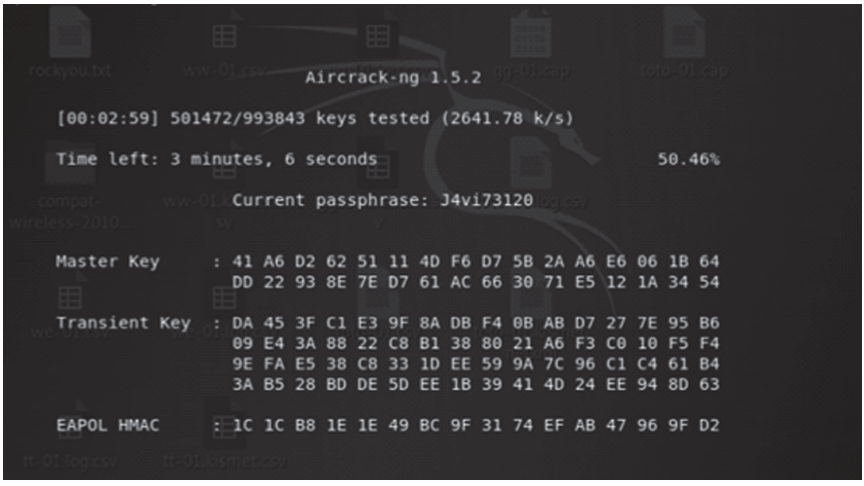

Fig. 7. Successful cracking passphrase for the wordlist

11. Both of the packet capture file and wordlist file are for the use in "aircrack-ng" for cracking the WPA2/PSK authentication. Type the command "aircrack-ng -w [path to wordlist] [path to packet capture file]". [path to wordlist] and [path to packet capture file] mean the path to a wordlist and a packet capture file that have located, respectively. In this case, we have a wordlist called "darkc0de.txt" in the root/Desktop/ folder. [path to wordlist] [path to packet capture file] should be replaced by "/root/Desktop/darkc0de.txt" and "/root/Desktop/ar1-01.cap", individually (Fig. 6).

Fig. 8. Failure of cracking passphrase in Enhanced WPA2/PSK

12. Cracking the passphrase might take a long time depending on the size of the wordlist. It takes 5 min here. If the passphrase is in the wordlist, the terminal of aircrack-ng will show as Fig. 7.
13. Fail to crack in Enhanced WPA2/PSK, even the passphrase is in the wordlist. The result of "key not found" is shown in Fig. 8.

4 Conclusions

In this regard, we have study some fundamental principle and weaknesses of WPA2/PSK. The 4-way handshake of EAPOL exchanges 4 messages between AP and STA to generate encryption keys which can be used to protect handshake and encrypt actual data. The existing rainbow tables have the top 1000 SSIDs and a large number of passwords/passphrase for general use. The hackers can speed up cracking by quick querying the rainbow tables. If WPA2/PSK wireless network is provided for free use in public places, the password/passphrase is shared with for all users in the hotspot. One password/passphrase generates one PSK. WPA2 does not have forward secrecy. Once a hacker obtains a set of PSK, they can decrypt all past and future packets encrypted with this set of PSK. Enhanced WPA2/PSK can effectively protect from the hackers who get passwords/passphrases, with time-stamp parameter added to produce a different PSK. Enhanced WPA2/PSK could be vulnerable to cracking only if hacker has used the same timestamp. However, the smaller the time granularity in timestamp, the lower the possibility for hacker to crack.

References

1. Reddy, S.V., Rijutha, K., SaiRamani, K., Ali, S.M, Reddy, C.P.: Wireless hacking - a WiFi hack by cracking WEP. In: 2nd International Conference on Education Technology and Computer (2010)
2. Cui, K., Yin, D.: Research on the security of the encrypted WLAN. In: International Conference on Computer Science and Service System (CSSS) (2011)
3. Alqahtani, S.A., Aloraini, M.: Resolving wireless security limitations using a new Wi-Fi secure access. In: IEEE 12th International Conference on Computer and Information Technology (2012)
4. Zhang, L., Yu, J., Deng, Z., Zhang, R.: The security analysis of WPA encryption in wireless network. In: 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet) (2012)
5. Pandurang, R.M., Karia, D.C.: Performance measurement of WEP and WPA2 on WLAN using OpenVPN. In: International Conference on Nascent Technologies in the Engineering Field (ICNTE) (2015)
6. Yacchirena, A., Alulema, D., Aguilar, D. Morocho, D., Encalada, F, Granizo, E.: Analysis of attack and protection systems in Wi-Fi wireless networks under the Linux operating system. In: IEEE International Conference on Automatica (ICA-ACCA) (2016)
7. Radivilova, T., Hassan, H.A.: Test for penetration in Wi-Fi network: attacks on WPA2-PSK and WPA2-enterprise. In: International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo) (2017)
8. Abo-Soliman, M.A., Azer, M.A.: A study in WPA2 enterprise recent attacks. In: 13th International Computer Engineering Conference (ICENCO) (2017)
9. Chang, T.-H., Lin, J.-W., Lai, G.H.: The method of capturing the encrypted password packets of WPA and WPA2, automatic, semi-automatic or manual? In: IEEE Conference on Dependable and Secure Computing (DSC) (2018)