Parallel Active Dictionary Attack on WPA2-PSK Wi-Fi Networks

Omar Nakhila*, Afraa Attiah†, Yier Jin‡ and Cliff Zou§
Dept. of EECS, Univ. of Central Florida
Florida, USA
Email: *omar_hachum@knights.ucf.edu, †afraa@eecs.ucf.edu, ‡yier.jin@eecs.ucf.edu, §czou@eecs.ucf.edu

***Abstract*—Wi-Fi network offers an inexpensive and convenient way to access the Internet. It becomes even more important nowadays as we are moving from the traditional computer age to the current mobile devices and Internet-of-Things age. Wi-Fi Protected Access II (WPA2) - Pre-shared key (PSK) is the current security standard used to protect small 802.11 wireless networks. Most of the available dictionary password-guessing attacks on WPA2-PSK are based on capturing the four-way handshaking frames between an authorized wireless client and the Access Point (AP). These attacks will fail if an attacker is unable to capture the four-way handshaking frames of a legitimate client. An attacker also can apply an active dictionary attack by sending a pass-phrase to the AP and waiting for the response. However, this attack approach could only achieve a low attack intensity of testing a few pass-phrases per minute. In this paper, we develop a new scheme to speed up the active pass-phrase guessing trials intensity based on two novel ideas: First, the scheme mimics multiple Wi-Fi clients connecting to the AP at the same time—each emulated Wi-Fi client has its own spoofed MAC address; Second, each emulated Wi-Fi client could try many pass-phrases using a single wireless session without the need to pass the 802.11 authentication and association stages for every pass-phrase guess. We have developed a working prototype and our experiments show that the proposed scheme can improve active dictionary pass-phrase guessing speed by 100-fold compared to the traditional single client attack.**

***Index Terms*—Wi-Fi security, WPA2-PSK, Dictionary attack.**

I. Introduction

The IEEE 802.11 Wireless Local Area Network (WLAN) standard is widely used for connecting various wireless and mobile devices to the Internet [1]. WLAN is a low cost network that supports high throughput transmission. The convenience of eliminating the use of wires makes WLAN easier to implement and adequate to user needs. However, securing these types of networks is more challenging than wired networks [2]. To protect its wireless clients, WLAN uses authentication/encryption protocols to ensure confidentiality, integrity and availability (CIA).

WLAN's security evolved over three major stages throughout its road to protect wireless clients [2]. First, Wired Equivalent Privacy (WEP) was the original security standard protocol. However, researchers found many vulnerabilities in WEP that can expose clients wireless data in a matter of seconds [3]. This led to the emergence of the second stage security standard of Wi-Fi Protected Access (WPA). WPA was created to support legacy wireless devices and at the same time to patch WEP defects [4]. The current and the third WLAN security stage was accomplished by introducing WPA2. The design of WPA2 was not limited by hardware constraints like WPA. WPA2 uses AES (Advanced Encryption Standard) and CCMP (Counter Mode CBC MAC Protocol) by default, which provides stronger encryption than WPA [2] [4].

Both WPA and WPA2 have two modes of operation. The first mode is Pre-shared key (PSK) or personal mode, which is designated for small office / home office (SOHO) wireless networks. In this mode, an access point (AP) will use only one pass-phrase (8 to 63 characters in length) to authenticate wireless clients. Each client should use the same exact pass-phrase stored in AP to pass the authentication process successfully. If a WLAN's administrator wants to change the pass-phrase, he needs to change the pass-phrase in all wireless clients and APs. For WLANs in large cooperations, changing the pass-phrase on all wireless clients and APs is not practical [5].

The second mode, also called Enterprise mode, needs administrators to set up a dedicated Remote Authentication Dial-In User Service (RADIUS). Each user will have a unique user name and password to be authenticated by the RADIUS server. After the authentication process completes successfully, the AP will receive a random key from the RADIUS server to protect the wireless communication [5].

The dictionary pass-phrase attack is one of the popular attacks on WPA2-PSK [2]. Since PSK will be the main key to protect WLAN, the attacker will try to guess the pass-phrase used to generate PSK. This can be done by capturing the initial WPA2-PSK handshaking between a legitimate wireless client and the AP. After capturing the handshaking frames, the attacker will use offline dictionary word guessing software to recover the pass-phrase.

In this paper, we present a new scheme to apply online dictionary attacks on WPA2-PSK. The main contributions of this paper are:

- To our knowledge, all the available implementations of the dictionary pass-phrase attack on WPA2-PSK are offline based attacks and they will fail if there is no legitimate wireless client connected to the AP or in the process of connecting to the AP. In this scenario, all offline brute force implementations will not work since they will need the initial WPA2-PSK four-way handshaking frames between the AP and a legitimate wireless client. On the other hand, online dictionary attacks will still work in this scenario.

- We present two novel techniques to speed up the online dictionary attack process. First, we create parallel virtual wireless clients (VWC) authenticating at the same time to an AP. Each VWC will emulate a standalone wireless client. Second, we enable each VWC to guess the PSK multiple times within a single wireless session. Each VWC will keep guessing the WPA2 pass-phrase until it receives a de-authentication frame from the AP.
- Finally our online dictionary attack was implemented and evaluated in a real-life environment using different off-the-shelf wireless APs. Our testings showed that the proposed scheme can speed up the password guessing process by 100-fold compared to the traditional online single-client attack.

The paper is organized as follows. Section II discusses related works. In Section III we explain how WPA2-PSK works. The design of the new online dictionary attack and the developed prototype is presented in Section IV. Then, we evaluate the performance of our attack in Section V. Finally, limitations and conclusions are presented in the last two sections,VI and VII, respectively.

II. Related work

WPA2-PSK uses state of the art AES/CCMP to protect wireless client data. The PSK length is 256 bits or 64 octets represented as a hex number. However, since it is more convenient for users to remember ASCII keys than hex numbers, users will use a pass-phrase that consists of 8 to 63 characters. The pass-phrase is then mapped to PSK. This mapping will drop the security of WPA2-PSK to about 2.5 bits per character [6]. Pass-phrases less than 20 characters are vulnerable to dictionary attacks.

The most feasible technique to bypass WPA2-PSK security is by recovering the pass-phrase from the four-way handshaking communication. Most of the available implementations are based on the offline dictionary attack against the four way handshake. In this section we will categorize these attacks into two parts, offline and online.

For the offline attack, one of the most popular software suits used to brute-force PSK using a dictionary work list is Aircrack-ng [7]. First, the four-way handshaking must be captured between legitimate wireless clients willing to connect to the AP. Capturing the four-way handshaking can be accomplished by using Airodump-ng software. If the wireless client is already connected to the AP, then the attacker can use Aireplay-ng which will force the wireless to de-authenticate and start the four-way handshake again [8].

After the attacker captures the four-way handshake, Aircrack-ng will start the offline dictionary pass-phrase guessing attack to recover the pass-phrase. On the other hand, other offline software can speed up the offline pass-phrase guessing attack by utilizing a GPU (e.g., Hashcat [9]).

However, all the previous attacks will fail if there is no legitimate wireless client willing to connect to the AP. Furthermore, even if there is an already connected wireless client, if the network is protected using 802.11W [10], the attacker will not be able to de-authenticate the connected clients. In contrast, our proposed technique will not be based on the condition of having a legitimate wireless client.

For the online attack, in 2007, the Wi-Fi alliance introduced Wi-Fi Protected Setup (WPS), which is an optional feature to help wireless clients connect to a WLAN with ease, while providing protection at the same time [11]. One of the methods used by WPS to authenticate a user is by asking him to enter an 8 digit PIN number written on the back of the AP. Knowing the PIN will reveal the pass-phrase used to drive the WPA2-PSK keys. However, due to poor design of WPS, using Reaver [12] software, the attacker can apply an online brute force attack and recover the PIN without having a legitimate wireless client present.

Since WPS is an optional feature, an AP may not support it. Also, some manufactures limit the number of times a wireless client can enter a wrong PIN number. If the wireless client exceeded that limit, the WPS method will be locked for a certain amount of time. Both of these cases will limit the attack on WPS. On the other hand, our proposed technique will not be affected by the availability of WPS. Furthermore, WPA2-PSK is not be limited by the number of times a wireless client can enter an incorrect pass-phrase.

III. Background of WPA2-PSK Protocol

The aim of our techniques is to improve the online dictionary attack speed on WPA2-PSK. The online attack does not require a legitimate wireless client to be present. In this section we will explain how a wireless client and an AP generate and exchange the keys used to protect WLANs using the WPA2-PSK suite.

A. Key Generation

The pass-phrase of WPA2-PSK is pre-installed in both the AP and the wireless client. The pass-phrase is secret information that will be used to derive all the required keys used to protect WLAN. More than one key will be generated and each one of them is used for different purposes. In general, there are seven keys involved in the protection of WPA2-PSK networks [13].

First, before WPA2-PSK key generation starts, an 802.11 wireless client has to authenticate and associate to the AP as shown in Figure 1 [14]. The WPA2-PSK four-way handshaking procedure starts when the wireless client passes the authentication and the association states. The names of these

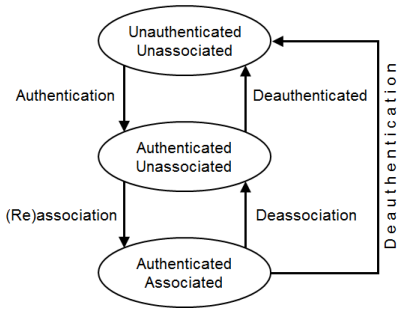


Fig. 1: 802.11 Authentication and association states.

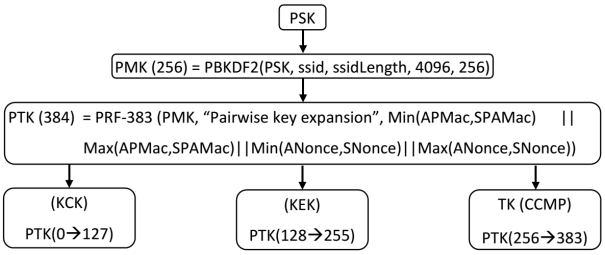


Fig. 2: WPA2-PSK key generation.

two states are somewhat misleading since both states do not have any type of security. It is merely a formality procedure used by wireless clients and an AP to exchange capability information.

Second, after the wireless client is authenticated and associated to the AP, the WPA2-PSK four-way handshake will start. WPA2-PSK uses a Pre-shared key (PSK) which is derived from the pass-phrase that was entered manually on both the wireless client and the AP. The pass-phrase length is 8 to 63 characters. Using a Password-Based Key Derivation Function 2 (PBKDF2), the pass-phrase, SSID and SSID length are hashed 4096 times to produce a 256-bit Pair Master Key (PMK) as shown in Figure 2. PMK is the same for every pair of SSID and pass-phrase.

Third, PMK, the phrase "Pairwise key expansion", AP's MAC address and the wireless client's MAC address, a random number generated by the AP (ANonce) and a random number generated by the wireless client (SNonce) will be fed to a pseudo-random function (PRF) to produce Pair Temporary Key (PTK). The length of the PTK in the WPA2-PSK(AES/CCMP) is 384 bits. [13].

Fourth, PTK will be divided into three keys as shown in Figure 2 where :

- Key Confirmation Key (KCK 128 bits) which is used to provide data integrity in the four-way handshaking communication.
- Key Encryption Key (KEK 128 bits) which is used to protect the four-way handshaking communication.
- Temporal Key (TK 128 bits) is used to protect wireless data.

All the previous keys are used to ensure integrity and confidentially and are used in unicast communication between the AP and the wireless client. On the other hand, the AP will generate a Group Temporal Key (GTK) and send it to the wireless client. GTK is used by wireless clients and AP to send broadcast data to the wireless network. The AP uses KEK to protect GTK while sending it to the wireless client.

B. Keys Exchange

Both the AP and the wireless client rely on the four-way handshake communication to confirm the possession of PSK. The four-way handshake procedure starts after the wireless client authenticates and associates (Figure 1) to the AP. Four-way handshake consists of four messages as shown in Figure 3 [6].Extensible Authentication Protocol (EAP) over LAN (EAPoL) is used to carryout the four-way handshaking messages between both parties.

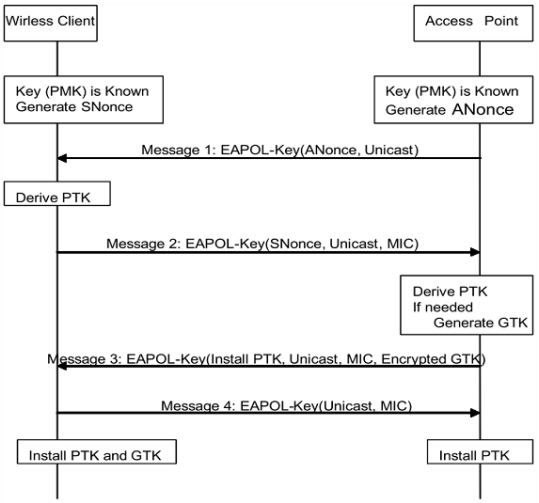


Fig. 3: WPA2-PSK four-way handshaking.

First, the AP sends Message 1 which contains an ANouse using EAPOL. ANouse is a 32 digit random number generated by the AP. When the wireless client receives Message 1, it will have all of the required parameters to derive PTK from PSK as shown in Figure 2. At this point, KCK, KEK and TPK are generated on the wireless client side. The wireless client then creates Message 2 which contains SNonce and the Message Integrity Code (MIC). Where SNonce is also a 32 digit random number which is generated by the wireless client.

MIC is used to ensure the integrity of Message 2. MIC is calculated on the whole EAPOL header plus the KCK (MIC(EAPOL,KCK)). When the AP receives Message 2, it extracts SNonce and derives KCK,KEK and TPK. Furthermore, the AP will calculate Message 2 MIC and compare it with the MIC received from the wireless client.

Message 3 is sent from the AP to the wireless client and it contains the GTK encrypted using KEK and MIC. Message 4 will be sent from the wireless client to the AP to confirm a successful end of the four-way handshaking. When the attacker receives Message 3 from the AP, they can confirm that the pass-phrase used in the creation of Message 2 was correct.

IV. Active Dictionary Attack

Active dictionary attacks on the pass-phrase of the WPA2-PSK can be applied since most APs do not limit the number of trials a wireless client can input using an incorrect pass-phrase. In our paper, we present two novel techniques to speed up the active dictionary attack. The following two subsections illustrate the design and the implementation of proposed techniques.

A. Proposed design

WPA2 was designed to provide security to WLAN. WPA2-PSK is designated for small office / home office networks and to be used without the need of a RADIUS server. The strength of WPA2-PSK security depends on how complicated the pass-phrase is. In this paper, we introduce a new proposed design that utilizes two novel techniques to speed up online pass-phrase guessing speed.

The proposed design is based on applying an active dictionary attack on WPA2-PSK. The aim of the attack is to recover the pass-phrase without the need of capturing the four-way handshaking between a legitimate wireless client and the AP.

Our software tries to automatically guess the pass-phrase by selecting a certain pass-phrase from a dictionary word list and creating Message 2 of the four-way handshaking. The program then sends Message 2 to the AP and waits for a reply. If the AP replies with Message 3 then, we have guessed the correct pass-phrase. When the AP replies with Message 1 to our Message 2 then, the pass-phrase used to create Message 2 was incorrect.

The major hurdle of the active dictionary attack is the pass-phrase guessing speed. Some APs will take a certain amount of time to reply to Message 2 of the four-way handshake, especially when the pass-phrase used to build Message 2 was wrong. Also, our program on the attacker's machine will take some time to filter responses received from the AP since the attacker will receive all the Wi-Fi frames transmitted on that channel. Furthermore, transmission propagation will add more delay time to pass-phrase guessing speed.

To speed up the WPA2-PSK pass-phrase guessing process, the first novel technique we present in our active dictionary attack is to let the attacking program initiate multiple virtual wireless clients (VWCs). Each VWC acts as a real client trying to connect to the AP. All these VWCs are generated from one wireless interface card. A VWC will use a spoofed MAC address when communicating with the AP.

To further speed up the PSK guessing process, the second novel technique we present in our active dictionary attack is to enable each VWC to try more than one pass-phrase for each wireless session. This technique speeds up the attack since the VWC will not have to pass 802.11 authentication and association states every time a new pass-phrase is tested. A single VWC will keep trying different pass-phrases until it is de-authenticated from the AP as shown in Figure-4.

B. Implementation

Our technique was implemented using C language on a Linux machine. Using the LORCON [15] library, we were able to inject and receive 802.11 wireless frames. LORCON is a cross-platform virtual interface that allows us to send and receive crafted 802.11 frames.

Our main program creates multiple processes where each process acts as a standalone wireless client. Each VWC will pick a randomly spoofed MAC address and start a wireless session to the AP. The main program will keep monitoring the state of each process.

After a VWC passes the authentication and association stages of the 802.11 WLANs, the VWC will begin the four-way handshake to the AP. Using a dictionary word list, the VWC will create Message 2 and send it to the AP. If the AP responds with Message 3 then the pass-phrase was correct otherwise the VWC will try another pass-phrase from the dictionary word list.

When the AP receives an incorrect pass-phrase, it will respond with Message 1. The VWC will disconnect from the AP and start a new wireless session to the AP with a different MAC address. After that, the VWC can inject another pass-phrase to the AP.

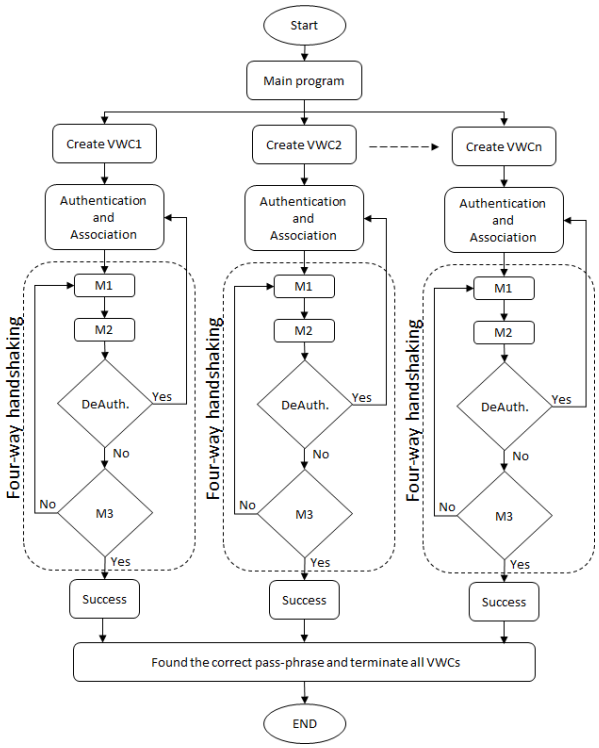


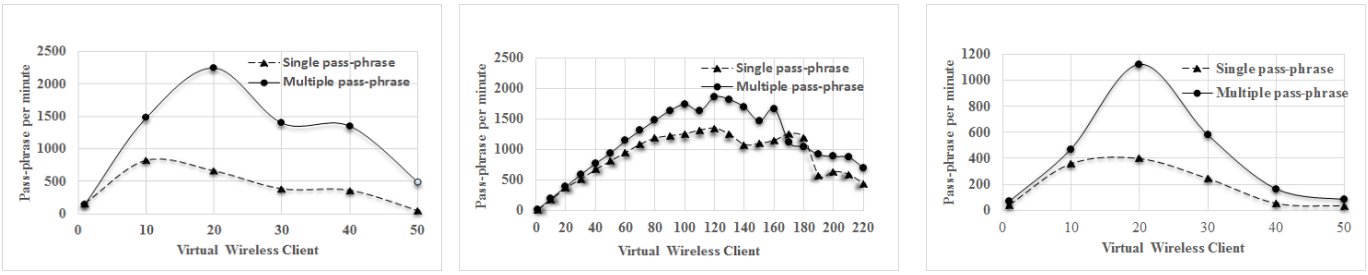
Fig. 4: Our proposed parallel active WPA2-PSK attack design. Where M1, M2 and M3 are the first three messages of the four-way handshaking. M4 message is omitted since it is only a confirmation frame from a VWC to the AP to indicate a successful end of the four-way handshaking procedure.

To further speed up the attack, we noticed that since the AP did not send any de-authentication frames due to the incorrect pass-phrase in Message 2, we can inject another pass-phrase using Message 2 within the same wireless session. This will further speed up the attack progress since the VWC does not have to send authentication and association frames again. The program will keep trying pass-phrases until the AP sends a de-authentication frame with reason code 02 (previous authentication no longer valid). At this point, the VWC will stop the current wireless session and start a new wireless session with a different MAC address.

V. Evaluation

We evaluated our proposed technique by initiating the attack on three different wireless routers. The wireless routers used in the test bed were DLink 601, Cisco Linksys EA3500 and Xiaomi Router Mini. Each wireless router was restored to its default setting, then we enabled the WPA2-PSK protection in each router with a certain pass-phrase. The attacking computer has an Atheros chipset WLAN card and was installed with Kali Linux. The APs and the attacker's WLAN card used 802.11g as their wireless communication standard.

During the attack, our prototype program will try our two techniques at the same time. For each AP, the first technique starts by creating multiple VWCs where each one of them will try only one pass-phrase at a time and wait for the response



(a) (b) (c)

Fig. 5: Comparison between three different wireless routers against our proposed attack where (a) Cisco Linksys EA3500, (b) Dlink DIR-601 (c) Xiaomi Router Mini.

from the AP. After the client sends Message 2 of the four-way handshaking to the AP, if the AP replied with Message 3 then the pass-phrase was correct. However, if the AP replied with Message 1 then the pass-phrase was wrong. The VWC will be de-authenticated from the AP and change its MAC address and start a new wireless session.

The second technique will also create multiple VWCs. However, when one VWC receives Message 1 as response to Message 2 (guessed pass-phrase is incorrect), it will not proceed with de-authentication. Instead, the VWC will pick another pass-phrase and create Message 2 and send it to the AP again. The VWC will keep sending Message 2 repeatedly until it receives de-authentication frame from the AP. At this point the VWC will change its MAC address and start a new wireless session.

To measure how many pass-phrases we can test at the same time using both techniques, for each trial,the program increases the number of VWCs from 1 to a certain number. During the test, each AP responded differently to our attack as shown in Figure 5.

For the three APs, the attack speed of the traditional online dictionary attack (one wireless client and single pass-phrase per wireless session) is shown as the first data point in each graph of Figure 5. For example, the traditional attack speed for the Dlink wireless router, as shown in the first data point on Figure5b, is 18 pass-phrases per minute. Increasing the number of VWCs will increase the intensity of the active dictionary attack. When each VWC tests more than one pass-phrase per wireless session, the attack effectiveness will further increase as shown in Figure 5-6.

When a single VWC tries multiple pass-phrase guessing at the same wireless session against Dlink wireless router, the attack intensity was on average 18 pass-phrases per minute as shown in Figure 5b-6a. In Figure 6, the average pass-phrase guessing speed can be calculated by dividing the total number of pass-phrases by 10 minutes. The total number of pass-phrases in Figure 6 is the summation of multiplying the pass-phrases(x-axis) with the wireless session (y-axis). Increasing the number of VWCs to 120 gave us the maximum pass-phrase attack guessing speed for the Dlink wireless router—on average 1833 pass-phrases per minute as shown in Figure 5b-6b. The pass-phrase guessing attack speed improvement for the Dlink wireless router at this point is about 100-fold. However, further increasing the number of VWCs to more than 120 will have negative impact on the pass-phrase guessing attack speed. As shown in Figure-5b-6c, when we have more than 120 VWCs attacking the Dlink wireless router, the pass-phrase guessing speed drops.

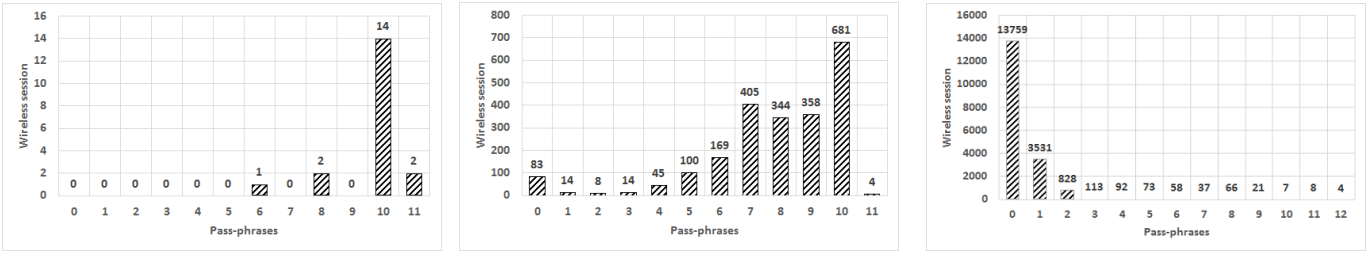
Both Figures 5 and Figure 6 show that the number of pass-phrase guesses will drop when the number of VWCs passes a certain threshold. This is because increasing the number of VWCs for each AP will increase the traffic on the wireless channel. Delay time and frame loss will increase when the wireless channel becomes saturated to a certain point that many wireless sessions will time out, and hence, reduces the overall attack speed. To prove that, Figure 7 shows a comparison between attacking Dlink wireless router with 120 VWC before and after the wireless channel being relatively busy. We say relatively busy because the 802.11g wireless channel during our test may get busy since it is a shared medium by other wireless clients. In Figure 7 we applied a continuous wireless data transmission from another wireless client during the full length of the attack to simulate a busy channel. The pass-phrase guessing speed when we have 120 VWC attacking at the same time dropped from 1833 pass-phrases per minute (Figure 5b-6b) when the channel is relatively idle to 247 pass-phrases per minute when the channel is relatively busy.

VI. DISCUSSION AND LIMITATIONS

In this paper, we presented an online active dictionary attack to tackle the current Wi-Fi home security protocol (WPA2-PSK). Our proposed attack is based on the following assumptions. First, by default, the AP does not filter the wireless client MAC addresses. Second, WPA2-PSK does not limit the number of trials a wireless client can take to enter the pass-phrase. All AP devices we tested so far satisfied these two assumptions, and thus are vulnerable to the proposed attack.

Furthermore, WLAN administrators may install more than one AP to expand the wireless coverage signal [16]. Since all APs will belong to the same Extended Service Set Identification (ESSID), our attack can be distributed to all APs. In this scenario, the attack speed will further increase with the increasing number of APs in the ESSID.

Our proposed attack will be limited by the wireless channel bandwidth and the response time of the AP. However, nowadays, the new 802.11ac standard provides high bandwidth



(a) (b) (c)

Fig. 6: Pass-phrases guessing trials per each wireless session against Dlink wireless router where (a) One VWC, (b) 120 VWC and (c) 220 VWC.

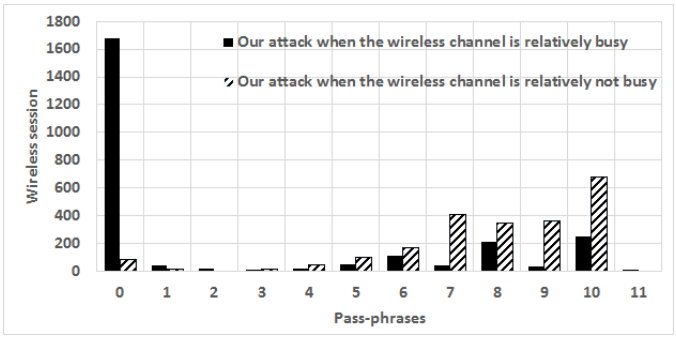


Fig. 7: Comparison between pass-phrase guessing trials per each wireless session when we have congested vs not-congested wireless channel using the same number of VWCs (120) againt Dlink wireless router.

wireless channels that can reach up to 1 Gbps [17] compared to 54Mbps for 802.11g. In addition, more powerful SOHO APs [18] are being developed that have more processing power which will reduce the response time of the AP.

Offline dictionary attacks are generally faster than online dictionary attack since the offline attack is not limited by AP and the wireless channel bandwidth. However, offline dictionary attack will fail if the attacker is unable to capture the four-way handshaking between a legitimate wireless client and the AP. In this scenario, our technique will be a feasible solution to recover the WPA2-PSK pass-phrase.

Finally, online dictionary attacks can target any network authentication/authorization device to gain access to it. Not limiting the number and the speed of pass-guessing trials will significantly magnify the danger of this type of attack. For example, recently many Apple distributed iCloud accounts have been hacked by using pass-guessing dictionary attack since the attacker was able to try many passwords without being blocked by Apple servers [19].

VII. CONCLUSION

Active WPA2-PSK dictionary attacks can be used to recover pass-phrase when the attacker is unable to capture the four-way handshaking frames between the AP and an authorized user. In this paper, the speed of the active WPA2-PSK dictionary guessing attack was improved by implementing two novel techniques. First, an attacker will create multiple virtual wireless clients (VWCs) using a single WLAN interface card. Each VWC will emulate a standalone wireless client to the AP. All the VWCs will start guessing the pass-phrase of the WPA2-PSK in a parallel manner. Second, as long as the wireless session is active, a VWC will keep guessing the pass-phrase repeatedly until a de-authentication frame is received from the AP. Our proposed attack was implemented and evaluated using different types of off-the-shelf wireless APs. Our results showed that the two proposed techniques may improve the attack speed up to 100-fold compared to the traditional single client active dictionary attack.

REFERENCES

[1] Michelle Gong, Brian Hart, Shiwen Mao; "Advanced Wireless LAN Technologies: IEEE 802.11AC and Beyond", SIGMOBILE Mobile Computing and Communications Review, ACM,(2015), Volume 18 Issue 4: pp 48-52.

[2] Halil Bulbul, Ihsan Batmaz, Mesut Ozel; "Wireless network security: comparison of WEP (Wired Equivalent Privacy) mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) security protocols",The 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop, (2008): pp 1-8.

[3] Erik Tews, Ralf-Philipp Weinmann, Andrei Pyshkin; "Breaking 104 Bit WEP in Less Than 60 Seconds", Information Security Applications, Volume 4867, (2007): pp 188-202.

[4] Bohn, S. ; Philips Semicond. Dresden AG, Germany ; Grob, S. ; Nubgen, R. ; Schwann, P.; "An automated system interoperability test bed for WPA and WPA2",Radio and Wireless Symposium, IEEE, (2006): pp 615-618.

[5] Andrew Gin, Ray Hunt; "Performance analysis of evolving wireless IEEE 802.11 security architectures", The 8th International Conference on Mobile Technology, Applications and Systems,(2008).

[6] Devin Akin; "802.11i Authentication and Key Management (AKM)",Certified Wireless Network Professional (CWNP) program,(2005).

[7] http://www.aircrack-ng.org

[8] I. P. Mavridis, A.-I. E. Androulakis, A. B. alkias, Ph. Mylonas; "Real-life paradigms of wireless network security attacks ",Panhellenic Conference on Informatics, (2011): pp 112-116.

[9] http://hashcat.net

[10] IEEE Std 802.11w -2009.

[11] Dimitris Zisiadis, Spyros Kopsidas, Argyris Varalis, Leandros Tassiulas; "Enhancing WPS Security",Wireless Days international conference, (2012): pp 1-3.

[12] https://code.google.com/p/reaver-wps/

[13] IEEE Std 802.11i -2004.

[14] Mathy Vanhoef, Frank Piessens; "Practical verification of WPA-TKIP vulnerabilities", The 8th ACM SIGSAC symposium on Information, computer and communications security (2013): pp 427-435.

[15] https://code.google.com/p/lorcon/

[16] SMC Network, "Wireless Hotspot Solutions", 2008.

[17] Der-Jiunn Deng, Kwang-Cheng Chen,Rung-Shiang Cheng; "IEEE 802.11ax: Next Generation Wireless Local Area Networks", The 10th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness (QSHINE), (2014): 77-82.

[18] www.dlink.com

[19] https://github.com/Pr0x13/iDict