Parallel Active Dictionary Attack on IEEE 802.11 Enterprise Networks

Omar Nakhila
Dept. of Electrical & Computer Engineering
University of Central Florida
Orlando FL, USA
omar_hachum@knights.ucf.edu

Cliff Zou
Dept. of Computer Science
University of Central Florida
Orlando FL, USA
czou@cs.ucf.edu

***Abstract*—One of the greatest challenges facing 802.11 wireless local area network (WLAN) is to provide equivalent security to wired local area network (LAN). Wi-Fi Protected Access II (WPA-II), also referred to as IEEE 802.11i standard, is the current security mechanism for enterprise wireless networks. IEEE 802.11i standard depends upon IEEE 802.1X standard to authenticate and generate the main cryptographic key used to secure wireless network traffic. In a WPA-II enterprise network, capturing wireless frames during the authentication phase between the Access Point (AP) and an authorized wireless client will not compromise the security of the WLAN. However, an attacker can apply active dictionary attack by guessing the credentials used to access the wireless network. In this case, the attacker communicates directly with the Authentication Server (AS). The main downside of this attack is the low intensity of password guessing trials that the attacker can achieve, thus security community usually does not pay attention to such an attack. In this paper, we present a new attack scheme that can increase the intensity of guessing trials against WPA-II enterprise. The new scheme is based on using one wireless interface card to create multiple virtual wireless clients (VWCs), each VWC communicates with the Authentication Server as a standalone wireless client. We have developed a working prototype and our experiments show that the proposed scheme can improve the active dictionary guessing speed by more than 1700% compared to the traditional single wireless client attack.**

***Index Terms*—Wi-Fi security, WPA-II enterprise, Brute force attack, Virtual wireless clients.**

I. Introduction

In the past two decades, 802.11 wireless local area network (WLAN) has increased in use dramatically across the globe [1]. IEEE 802.11 is the most cost-efficient WLAN that offers network access to wireless clients (WC). Whether personal or business wireless networks, IEEE 802.11 WLAN is designed to meet the market demands [2]. However, securing IEEE 802.11 WLAN is one of the top challenges facing the adaptation and spread of such a network. Since the emergence of IEEE 802.11 WLAN, researchers have been focusing on presenting new security suites to protect the wireless network.

Wireless Equivalent Privacy (WEP), is the first security protocol used to protect IEEE 802.11 WLAN [3]. Although WEP uses Rivest Cipher 4 (RC4) stream cipher to encrypt wireless data, the size of initializing vector (IV) used was small, which led to IV conflict. Furthermore, the master keys are directly used to encrypt data with no key management. Researches have demonstrated ways to break the security in WEP in less than a minute [4].

Following the vulnerabilities found in WEP, Wi-Fi Protected Access I (WPA-I) and Wi-Fi Protected Access II (WPA-II) were introduced [5]. WPA-I is used to provide temporary solution to legacy wireless devices, and WPA-II is the current standard security protocol for 802.11 wireless networks. In publications, WPA-II is also referred to as robust security network (RSN) or IEEE 802.11i-2004 [6]. WPA-II deployments can be different between Small Office / Home Office (SOHO) and enterprise wireless network. WPA-II Pre-shared key (PSK) is used in SOHO where only one passphrase is used to protect the wireless traffic. However, in WPA-II enterprise, each wireless client has his/her own username and password to protect their own wireless traffic. Network administrator sets up an authentication server (AS), such as Remote Authentication Dial-In User Service (RADIUS), to authenticate each wireless client.

Most attacks on WPA-II enterprise are based on man in the middle (MITM) attack [7] [8] [9]. The attacker positions him/her self between the WC and the AS to capture the WC credentials. However, using digital certificate on the RADIUS server side with the proper configuration on the WC side prevents most of these attacks [9]. In this case, the attacker can initiate an active brute force attack to gain access to the wireless network. The downside of such an attack is the very low password guessing speed, which makes such a brute-force attack little threat to the wireless network. In this paper, we present a new parallel attack scheme using many virtual wireless clients to attack WPA-II enterprise, which could make such an active dictionary attack a practical real threat again and thus it should be seriously considered by security community. The main contributions of this paper are:

- We present a novel technique to speed up the active dictionary attack process. By using only one wireless interface card (WIC), we are able to create many parallel virtual wireless clients (VWCs) authenticating at the same time to a RADIUS server. Each VWC will emulate a standalone wireless client, and hence, increasing the attacker's active dictionary attacking power.
- Although by default, an authentication server, such as RADIUS server, may delay rejection response to slow

down the brute force attack [10] [11], using parallel active dictionary attack will lower the impact of such a protection feature. The delay time imposed by the RADIUS server will be utilized by the attacker to start a new connections, and test other passwords.

- Finally our active dictionary attack has been implemented and evaluated in a real life environment using different off-the-shelf wireless APs and one of the most popular RADIUS servers. Our technique showed that it can speed up the password guessing speed by 1700% compared to the traditional single wireless client attack.

The rest of the paper is organized as follows: Section II discusses related works. In Section III we explain how 802.1x works. The design of the new active 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. Table I list acronyms used in our proposal and their definitions throughout the paper.

II. RELATED WORKS

IEEE 802.11i enterprise consists of two main parts: the AS, such as RADIUS server, and the authenticator, which is the AP. When the WC, also called supplicant, wants to access the WLAN, he/she should be authenticated first by the AS. The communication between the AS and the WC will pass through the AP. Extensible Authentication Protocol (EAP) is used to define the authentication method between the AP and the AS. EAP and its authentication method will be encapsulated in the RADIUS protocol between the AS and the AP. On the other hand, between the AP and the WC, EAP and its authentication method will be sent using EAP over IEEE 802 protocol, which is known as "EAP over LAN" or EAPOL [6].

After the authentication phase finishes successfully, both the WC and the AP generate a random Pair Master Key (PMK). At this point, 4-way handshaking procedure starts between the WC and the AP only. Both of the WC and AP will use PMK to generate Pair Temporary Key (PTK) which is used to protect the four-way handshaking communication and the WC data. Finally, a Group Transient Key (GTK) will be generated by the AP and sent to the WC to protect the wireless broadcast traffic [6].

802.11 enterprise WLAN depends on 4-way handshake and 802.1x protocol to secure WC data. This should not be confused with 802.11 personal, were WLAN depends only on 4-way handshake to authenticate WC traffic [6]. The proposed attack in this paper is an extension of our previous proposal of active dictionary attack on WPA-II personal [12]. We successfully increased the active dictionary intensity on WPA-II personal by creating multiple VWCs initiating 4-way handshaking procedure at the same time to the AP. Active dictionary attack on WPA-II-PSK can be the only feasible attack when the attacker was unable to capture the 4-way handshaking procedure between a LWC and the LAP.

In this paper, we focused only on WPA-II enterprise. We divided the attacks on WPA-II enterprise into two main

TABLE I: Acronyms

Acronym	Definition
WC	Wireless client
LWC	Legitimate wireless client
WIC	Wireless interface card
VWC	Virtual wireless client
AS	Authentication server
RAS	Rogue authentication server
AP	Access point
WR	Wireless router
LAP	Legitimate access point
RAP	Rogue access point
WS	Wireless sessions

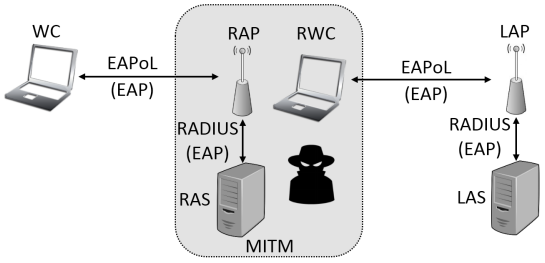

Fig. 1: Typical MITM attack on WPA-II enterprise

categories: MITM attacks [7] [8] [9] [13] [14] [15] and denials of service attacks (DOS) [16] [17].

In the first category, an attacker sets up a rogue AP (RAP) and a rogue AS (RAS). The RAP impersonates the legitimate AP (LAP) by broadcasting the same WLAN SSID. This attack can also be refer to as Evil Twin attack [9] [18]. the WC may connect first to the RAP when it offers better signal than the LAP.

When the WC connects to the RAP first, she/he will be authenticated using the RAS. At the same time, the attacker can start connecting to the LAP and be authenticated to the LAS using the WC credentials. After successfully capturing the WC credentials, the attacker can turnoff the RAP allowing the WC to connect to the LAP. This is the basic implementation behind most MIMT attacks on IEEE 802.11i.

Most of the MIMT attacks succeed only when the WC has misconfiguration that is exploited by an attacker. For example, authentication protocols such as EAP - Tunneled Transport Layer Security (TTLS) and Protected EAP (PEAP) allows the WC to check the AS digital certificate [19]. In [9] the attacker took advantage of the WC not checking the Common Name (CN) string of the digital certificate offered by the AS to have successful MITM attack. The attack would fail if the WC checks and rejects the RAP digital certificate [9].

Another successful type of MITM attacks is when the attacker makes the WC use a less secure EAP authentication protocol. For example, in [8] the attacker's RAS authenticated the WC using Light EAP protocol, which is a less secure protocol compared to both EAP-TTLS and PEAP. This attack will fail if the WC only used EAP-TTLS or PEAP as the main authentication with proper AS digital certificate checking [9] [20].

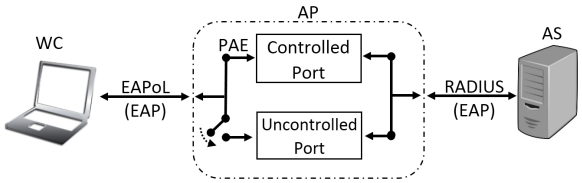

Fig. 2: 802.11i port access entry authentication.

DOS is the second category of attacks on WPA-II enterprise. Although this type of attack will not compromise the WC credentials, it will prevent him/her from accessing the WLAN. In both [16] and [17] the attacker sent crafted EAP frames to prevent the WC from successfully completing the authenticated phase. This type of attack is out off the scope of this paper.

The current proposal used the same concept in [12] to apply the attack on WPA-II enterprise. Such an attack is important when others attacks such MITM is not feasible.

III. BACKGROUND OF 802.1X PROTOCOL

IEEE 802.11i standard was developed to overcome the vulnerabilities found in WEP. IEEE 802.1x standard and 4-way handshaking procedure are the main components of IEEE 802.11i (WPA-II enterprise) standard. IEEE 802.1x standard is mainly used for authenticating the WC, and the 4-way handshaking procedure is used for exchanging cryptography keys [6]. In this paper, we present a novel technique to attack the authentication part of IEEE 802.11i standard.

When the WC (supplicant) authenticates to the AS (RADIUS), the communication will pass through the AP (authenticator) as shown in Figure 2. IEEE 802.1x standard uses port access entry (PAE) on the AP to allow the WC to send/receive frames to the AS. During the authentication phase, all data traffic from the WC will be sent only to the AS. After the WC finishes the authentication phase successfully, she/he will be switched form the controlled port to the uncontrolled port in which they can access services offered by the wired network.

One of the most popular authentication methods used by RADIUS is EAP-MD5. Since EAP-MD5 is based only on message digest 5 hashing function, it is considered fast and simple to implement [20] [21]. EAP-MD5 authentication starts after the WC finishes 802.11 authentication and association states with the AP as shown in Figure 3. The names of 802.11 authentication and association are somewhat misleading, since both communications don't have any type of security. It is merely a formality procedure used by WCs and an AP to exchange capability information.

EAP-MD5 begins when the AP sends EAP-Request (Identity) frame to the WC. Also, the WC can ask for EAP-Request (Identity) frame by sending EAPoL Start frame. At this point the WC sends his/her username to the AP. The username is passed to the AS server using RADIUS protocol. The AS generates a random challenge string and an ID, which represents a small number, and sends it to the AP. After receiving the random challenge and the ID from the AP, the WC hashes (ID + Password + MD5 Challenge) using MD5

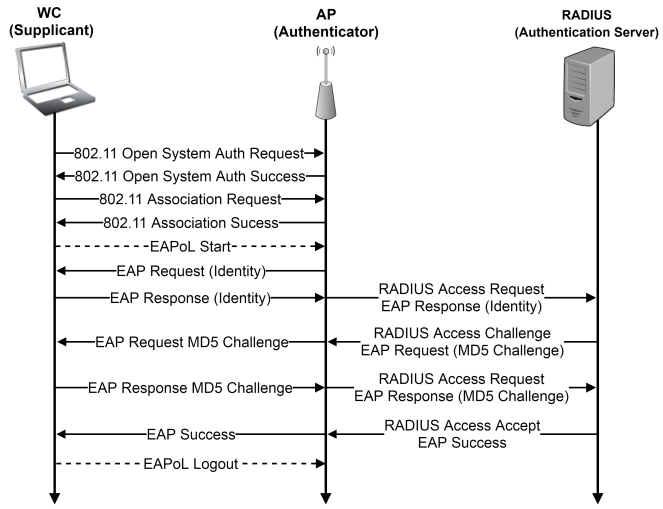

Fig. 3: EAP-MD5 authentication method.

hashing function and sends it to the AP. The AS successfully accepts the access request when the password used in the hashing function matches the one stored in the AS; otherwise, the AS rejects the access request. Also, the WC can send EAPoL Logout frame to de-authenticate from the AP.

Although EAP-MD5 is popular and simple, it is considered vulnerable to be used in the WLAN for many reasons [20] [21]. For example, the attacker can apply replay attack by capturing the hash message from the WC and send it to the AP. Furthermore, the attacker can sniff the hashed message and apply offline dictionary attack. The WC can reject EAP-MD5 authentication method by responding to the MD5 challenge by Nak frame [19].

The EAP-(TLS and TTLS) and PEAP provide better protection when compared to the EPA-MD5 in the WLAN. The EAP-TLS is considered the most secure method in WLAN [9] [20]. Both, the WC and the AS, should have their own digital certificate. EAP-TLS perform authentication by exchanging the digit certificate of the WC and the AS. The complexity added by requiring the WC to have a digital certificate makes EAP-TTLS and PEAP a better alternative.

EAP-TTLS and PEAP are the most common authentication methods in 802.11i [9]. They both use two phases of authentication. The first authentication phase provides a secure channel so that the WC can pass his/her credentials using the second authentication phase. The first authentication phase also can be refereed to as the outer authentication, and the second authentication phase is called the inner authentication. The inner authentication can use a less secure EAP authentication method, such as EAP-MD5, since it is protected by the outer phase. Table II compares between the different types of EAPs authentication methods [20].

IV. ACTIVE DICTIONARY ATTACK DESIGN

A. Design

Most EAP authentication methods requires each WC to provide his/her username and password to be allowed to access

TABLE II: Comparison between common EAP authentication methods

Property	*EAP Authentication Method*			
	MD5	*TLS*	*TTLS*	*PEAP*
Authentication attributes	Unilateral	Mutual	Mutual	Mutual
Deployment difficulties	Easy	Hard	Moderate	Moderate
Dynamic re-keying	No	Yes	Yes	Yes
Requires server certificate	No	Yes	Yes	Yes
Requires client certificate	No	Yes	No	No
Tunnelled	No	No	Yes	Yes
WPA compatible	No	Yes	Yes	Yes
WLAN security	Poor	Strongest	Strong	Strong

the WLAN. The username is used to locate the WC account and the password to authenticate him/her. To obtain both the username and password, our active dictionary attack was divided into two main steps.

The first step of our attack procedure is to capture the WC username. This goal can be accomplished by monitoring the authentication communication between a legitimate WC (LWC) and the LAP. The LWC is required to send his/her Identity when he/she receive EAP-Request (Identity) from the AP at the beginning of the EAPoL protocol, as shown in Figure 3. To simplify the implementation/management of the WLAN, network administrators use the LWC username as his/her Identity [22]. Furthermore, EAP authentication methods sends LWC Identity in a plain text [20].

After capturing the LWC username, we start the second step of our proposed procedure by initiating parallel active dictionary attack on the AS. Using only one wireless interface card, we created multiple VWCs. Each VWC communicates with the AS as a standalone WC and starts a brute force attack on the password of the captured LWC username. To speed up the brute force attack speed, VWCs use the least time consuming EAP authentication methods such as EAP-MD5 when communicating with the AS. EAP-MD5 is considered faster compared to both EAP-TTLS and PEAP because it interacts less with the AS. A VWC can rejects the EAP authentication methods offered by the AS by sending a NAK frame at the beginning of the authentication process.

By using the fastest available EAP authentication method, each VWC start authenticating to the AS using different passwords. When a VWC fails to authenticate using the selected password, it changes the MAC address and starts a new EAP authentication session. The attack stops when one of the VWCs authenticated successfully to the AS as shown in Figure 4.

B. Implementation

Our proposed parallel active dictionary attack is implemented using C language. We used Loss Of Radio CONnectivity (LORCON) library to create multiple VWCs. LORCON is an open source library used to create crafted 802.11 wireless frames [23].

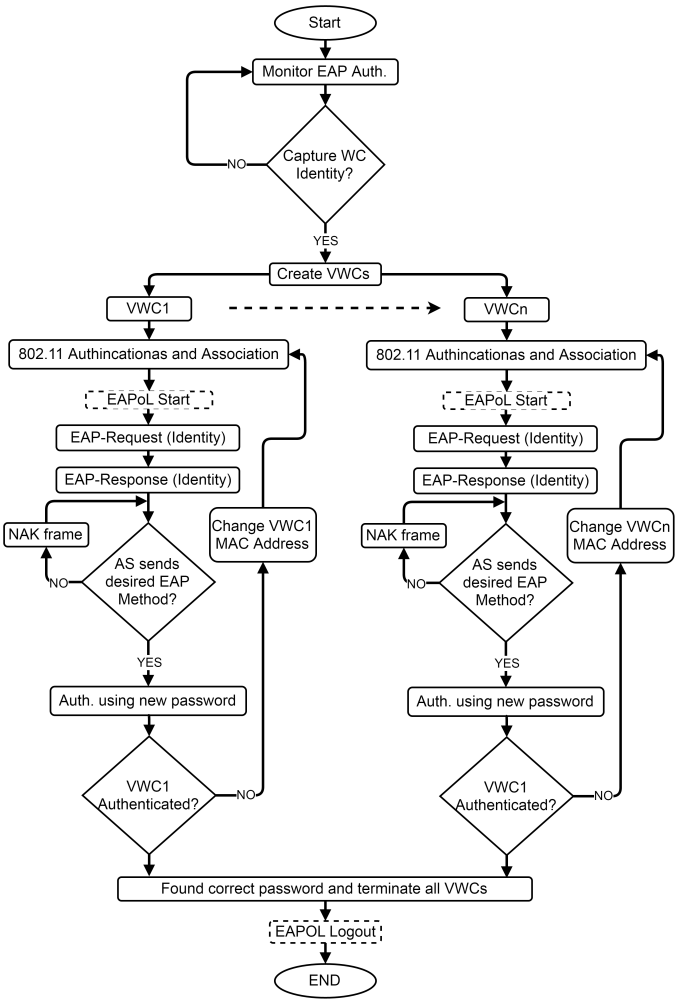

Fig. 4: Our proposed parallel active dictionary attack using one wireless interface card (WIC)

Each VWC emulates a single WC with a unique MAC address. All VWCs send/receive frame using only one wireless interface card (WIC) at the same time. Whenever one of the VWCs passes the authentication phase, the attack stops.

V. Evaluation

We set up a WLAN testbed to evaluated our proposed parallel active dictionary attack. The testbed consisted of an AP and AS. Three different types of wireless routers (WR) (ASUS-RT-AC68U, Dlink-DIR890L and Linksys WRT54) were used in the evaluation as an APs. Furthermore, we implemented the AS by installing the current version of FreeRADIUS server, which is the most popular RADIUS server [10] [11]).

The AP was configured to use WPA-II enterprise as the WLAN security protocol. The AS used RADIUS protocol on port 1812 to communicate with the AP. For the RADIUS server configuration, we added the AP as a client and the LWC as a user, which is the typical FreeRADIUS set up [11]. All other configurations in both, the AP and the RADIUS server, were set to default.

On the attacker side, our proposed software was installed on Kali Linux OS. The attacker used Penguin Wireless N Dual-

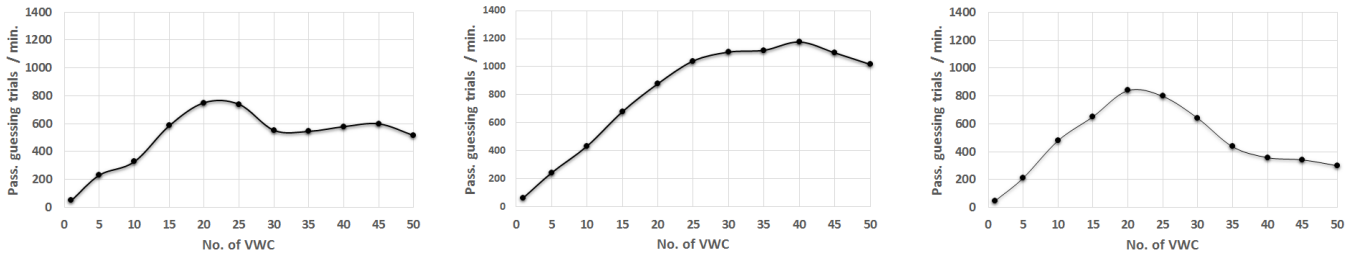

Fig. 5: Comparison between three different APs against our proposed attack where (a) Dlink-DIR890L, (b) ASUS-RT-AC68U (c) Linksys WRT54. The traditional active dictionary attack intensity is represented in the first data point.

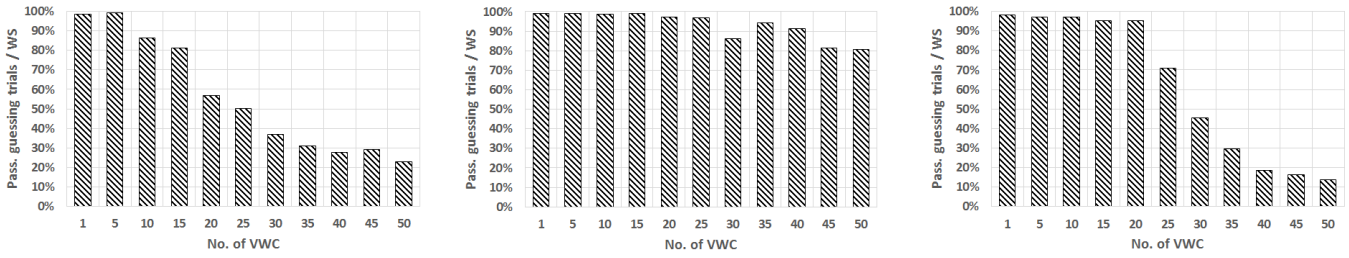

Fig. 6: The ratio between the number of password guessing trails to the total number of all wireless sessions (WS) for (a) Dlink-DIR890L, (b) ASUS-RT-AC68U (c) Linksys WRT54.

Band USB Adapter as the WIC. We used Wireshark to monitor the traffic between the LWC, VWCs, AP and the AS.

The first step of our proposed attack is to capture the username of the LWC. From the LWC PC, we connected to the testbed WLAN using the most common EAP authentication methods (TTLS and PEAP). Our proposed program successfully captured the LWC username each time the LWC send his/her Identity to the AP. We also observed that the AS requested the LWC to use EAP-MD5 as the initial EAP authentication method. However, the LWC rejected using EAP-MD5 by sending a NAK frame and accepted one of the two other authentication methods (TTLS and PEAP).

The second step of our proposed attack started after capturing the LWC username. First, our proposed software created multiple VWCs that connected to the testbed SSID and started EAPoL with the AP. The software used the LWC username in all Identity response frames when communicating with the AP. Unlike the LWC, the proposed software accepted EAP-MD5 authentication method requested by the AS. EAP-MD5 is simple to implement and requires less time to finish compared to both PEAP and EAP-TTLS.

To illustrate the increase in the brute force speed using our proposed technique, we started authenticating to the AS using only one VWC. This resembles the traditional single WC active dictionary attack. Then, we increased the number of VWCs connecting to the AP until the guessing intensity rate started to drop beyond a certain point. Each AP was tested for a total time of one hour and a half. We repeated the previous procedure for the three different type of APs used in the testbed, and the results are shown in Figure 5.

The increase in intensity of guessing trails for the three different APs reached its maximum when there were certain number of VWC authenticating at the same time. That number was different from one AP to another. For example, the rate of guessing trails in ASUS-RT-AC68U AP when we had only one WC was 65 password per minute. That number increased to 1176 password per minute when we had 40 VWCs. Such an increase in the intensity of guessing speed is equal to 1700% as shown in Figure 5b. However, increasing the number of VWC beyond that point did not show any further improvement.

Increasing the number of VWCs will increase the number of concurrent wireless sessions to the AP. Wireless sessions started to timeout, then dropped after exceeding a certain number of active VWCs. The ratio between the number of successful wireless sessions (i.e. password guessing trials) to the total number of all wireless sessions (WS) was calculated and represented in Figure 6. Almost all wireless sessions were successful when we had fewer VWCs. The number started to drop when we increased the number of VWCs.

VI. Discussion and Limitations

In this paper, we presented a new technique to increase the intensity of the active dictionary attack on WPA-II enterprise in WLAN. The attacker can improve the password trial guessing speed by creating multiple VWCs authenticating to the AS at the same time. Such an improvement can reach up to 1700% increase in the guessing trials.

In WPA-II enterprise, obtaining the PMK from the 4-way handshaking is unpractical. The PMK is a random 256 bits in length that changes every time the WC connects to the WLAN. Furthermore, retrieving the PMK will not compromise the WC password. On the another hand, our proposed technique reveals the actual password of the LWC.

The proposed technique may fail if the username was not captured in the first step of the attack. Network administrator can hide the username of the LWC by using Network Access Identifier (NAI) [22] in the outer authentication phase and use the actual LWC in the inner authentication phase. However, this requires a more complicated WLAN network implementation and can be only used with tunneled EAP authentication methods such EAP-TTLS and PEAP.

Network administrator my use locking mechanism to prevent brute force attack. However, no locking feature was activated on FreeRadius server. By default, Radius server only delayed responding to VMCs requests to slow down the brute force attack. The impact of such a protection feature is downgraded by our proposed attack. Each time a VWC is waiting for a response from the AS, another VWC can be created to test different password.

Our proposal attack intensity can be effected by the AP type, the wireless medium and the attacker/AS station performance. To have better results, an attacker can use a high performance workstation and start the attack to the least congested AP. Also, an attacker can distribute our proposed technique and attack different nearby APs that use the WIFI channel.

Finally, the proposed attack can authenticate each VWC to the AS using different EAP authentication methods including PEAP and EAP-TTLS. However, EAP-MD5 authentication method was used in our testbed because of its speed and simplicity. Also, EAP-MD5 was the initial authentication method offered by the AS.

VII. Conclusion

Active parallel dictionary attack can be used to increase the brute force intensity on WPA-II enterprise in WLAN. Such an attack is important when other attacks, such as MITM, are not feasible. The attack uses only one WIC to create multiple VWCs. Each VWC authenticates to the AS as a standalone WC.

Our proposed technique was implement and evaluated using different off the shelf APs. The most popular RADIUS server (FreeRadius) was used as an AS in the testbed setup. The final results showed an improvement of 1700% in the intensity of the active brute force attack by using VWC technique compared to the traditional one wireless client.

References

[1] Michelle X. Gong, Brian Hart, and Shiwen Mao. Advanced wireless lan technologies: Ieee 802.11ac and beyond. *GetMobile: Mobile Comp. and Comm.*, 18(4):48–52, January 2015.

[2] B. Bellalta. Ieee 802.11ax: High-efficiency wlans. *IEEE Wireless Communications*, 23(1):38–46, February 2016.

[3] Halil Ibrahim Bulbul, Ihsan Batmaz, and Mesut Ozel. Wireless network security: Comparison of wep (wired equivalent privacy) mechanism, wpa (wi-fi protected access) and rsn (robust security network) security protocols. In *Proceedings of the 1st International Conference on Forensic Applications and Techniques in Telecommunications, Information, and Multimedia and Workshop*, e-Forensics '08, pages 9:1–9:6, ICST, Brussels, Belgium, Belgium, 2008. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[4] Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin. Breaking 104 bit wep in less than 60 seconds. In *Proceedings of the 8th International Conference on Information Security Applications*, WISA'07, pages 188–202, Berlin, Heidelberg, 2007. Springer-Verlag.

[5] Andrew Gin and Ray Hunt. Performance analysis of evolving wireless ieee 802.11 security architectures. In *Proceedings of the International Conference on Mobile Technology, Applications, and Systems*, Mobility '08, pages 101:1–101:6, New York, NY, USA, 2008. ACM.

[6] Iso/iec international standard - information technology telecommunications and information exchange between systems local and metropolitan area networks specific requirements part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 6: Medium access control (mac) security enhancements. *ISO/IEC 8802-11, Second edition: 2005/Amendment 6 2006: IEEE STD 802.11i-2004 (Amendment to IEEE Std 802.11-1999)*, pages c1–178, July 2004.

[7] H. Hwang, G. Jung, K. Sohn, and S. Park. A study on mitm (man in the middle) vulnerability in wireless network using 802.1x and eap. In *Information Science and Security, 2008. ICISS. International Conference on*, pages 164–170, Jan 2008.

[8] Pieter Robyns, Bram Bonné, Peter Quax, and Wim Lamotte. Short paper: Exploiting wpa2-enterprise vendor implementation weaknesses through challenge response oracles. In *Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless; Mobile Networks*, WiSec '14, pages 189–194, New York, NY, USA, 2014. ACM.

[9] Sebastian Brenza, Andre Pawlowski, and Christina Pöpper. A practical investigation of identity theft vulnerabilities in eduroam. In *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, WiSec '15, pages 14:1–14:11, New York, NY, USA, 2015. ACM.

[10] Dirk van der Walt. Freeradius project, 2016.

[11] Dirk van der Walt. *FreeRADIUS Beginner's Guide*. Packt Publishing, 9 2011.

[12] O. Nakhila, A. Attiah, Y. Jinz, and C. Zou. Parallel active dictionary attack on wpa2-psk wi-fi networks. In *Military Communications Conference, MILCOM 2015 - 2015 IEEE*, pages 665–670, Oct 2015.

[13] K. Hoeper and L. Chen. An inconvenient truth about tunneled authentications. In *Local Computer Networks (LCN), 2010 IEEE 35th Conference on*, pages 416–423, Oct 2010.

[14] Fanzheng Kong and Weili Huang. Ieee802.1x of protocol analysis and improvement. In *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*, volume 3, pages V3–282–V3–285, Aug 2010.

[15] M. Cai, Z. Wu, and J. Zhang. Research and prevention of rogue ap based mitm in wireless network. In *P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2014 Ninth International Conference on*, pages 538–542, Nov 2014.

[16] P. Q. Ding, J. N. Holliday, and A. Celik. Improving the security of wireless lans by managing 802.1x disassociation. In *Consumer Communications and Networking Conference, 2004. CCNC 2004. First IEEE*, pages 53–58, Jan 2004.

[17] A. Alruban and E. Everitt. Two novel 802.1x denial of service attacks. In *Intelligence and Security Informatics Conference (EISIC), 2011 European*, pages 183–190, Sept 2011.

[18] O. Nakhila, E. Dondyk, M. F. Amjad, and C. Zou. User-side wi-fi evil twin attack detection using ssl/tcp protocols. In *Consumer Communications and Networking Conference (CCNC), 2015 12th Annual IEEE*, pages 239–244, Jan 2015.

[19] John Vollbrecht, James D. Carlson, Larry Blunk, Dr. Bernard D. Aboba Ph.D., and Henrik Levkowetz. Extensible Authentication Protocol (EAP). RFC 3748, March 2013.

[20] Khidir M. Ali and Thomas J. Owens. Selection of an eap authentication method for a wlan. *Int. J. Inf. Comput. Secur.*, 1(1/2):210–233, January 2007.

[21] Jyh-Cheng Chen and Yu-Ping Wang. Extensible authentication protocol (eap) and ieee 802.1x: tutorial and empirical experience. *IEEE Communications Magazine*, 43(12):supl.26–supl.32, Dec 2005.

[22] A. DeKok. The network access identifier. RFC 7542, RFC Editor, May 2015.

[23] Joshua Wright and Michael Kershaw. Lorcon2 project, 2016.