The Method of Capturing the Encrypted Password Packets of WPA & WPA2, Automatic, Semi-Automatic or Manual ?

Tien-Ho Chang
Departmment of Information Management
National Sun Yat-sen University
Kaohsiung, Taiwan
D024020001@student.nsysu.edu.tw

Chia-Mei Chen
Departmment of Information Management
National Sun Yat-sen University
Kaohsiung, Taiwan
cmchen@mis.nsysu.edu.tw

Gu-Hsin Lai
Department of Technology Crime Investigation
Taiwan Police College
Taipei, Taiwan
ghlai@cc.tpa.edu.tw

Jiunn-Wu Lin
Departmment of Information Management
National Sun Yat-sen University
Kaohsiung, Taiwan
jiunnwu@vghks.gov.tw

***Abstract*—The development of Wi-Fi application is on its high leap in various aspects, and its security can't be ignored by the kinds of attack methods. The best way to take control of the AP (Access Point) is get the password ,which is easier to crack it by the more and more powerful GPU. The first step for the password is get the encrypted packets-the four ways handshake packets, and there is no specific description in how to take it efficiently. We proposed the IDM (Intelligent Deauthentication Method) in capturing the real street encrypted packets for the cryptanalysis, and the method is semi-automatic which can decide the length and strength of the Deauthentication by the situations on the scene.**

***Keywords*—Cryptanalysis, GPU, parallel-computing, WPA & WPA2, wireless security.**

I. Introduction (*Heading 1*)

With the prosperous development of Wi-Fi in all kinds of applications, such as IoT, IpV6 and the intensity of access points getting higher and higher in various areas, the security of Wi-Fi could not be ignored as depicted in Fig. 1 [1] and the IoT devices as depicted in Fig. 2 [2]. We found that the usage of wireless network is enormously in its leap progress. The protocol of wireless network is mostly the Wi-Fi ,which is the relatively more stable with longer transmitting distance to other protocols, such as Bluetooth, RFID, and so forth. The communication of Wi-Fi is by far the most popular and will be lasting its advantage in the future for the ease of use and usefulness. And with the development, the price is getting lower and lower, be a kind of ordinary living necessity in our daily life. So the use of Wi-Fi is the way we live now and in the future.

The protection of Wi-Fi communication, the protocol of WPA & WPA2 is the now the toughest mechanism developed by IEEE, but it only protects the data frames are protected, not the control and management frames [3]. From the management frames mentioned above, there is the very chance to challenge its security of password with the higher and higher intensity of the Wi-Fi AP deployment everywhere as in the Fig. 3. The cracking is through the two major types of techniques, at first, the capturing of the four ways handshake encrypted packets and do the comparison of the hashed keys of the WPA & WPA2 ,which is irreversible. The processes will be faster and faster than before because of the applications of GPUs with great parallel computing capabilities. So the cracking now is a common and easy thing for password protection, it will change all the ways we implemented in passwords because it's just matters of time. We didn't find any literature specifically describing the procedures of password cracking in detail. In fact, it is partly scattered in different papers which made the readers unclear on the whole picture of Wi-Fi cryptanalysis. Here, we integrate several techniques and our findings to show the procedures step by step in order to analyze the security of the Wi-Fi protection.

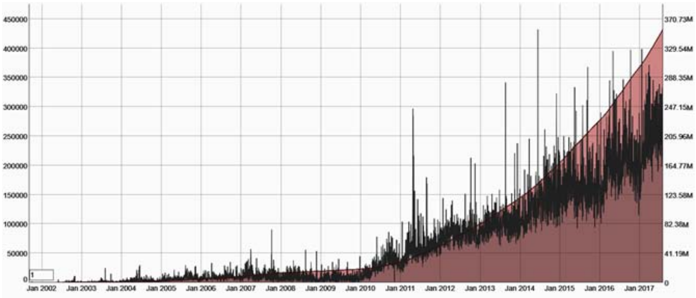


Fig. 1. The leap progress of the Wi-Fi development.

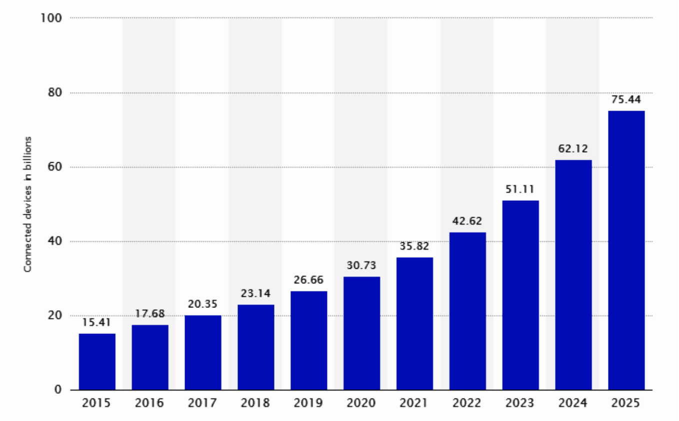


Fig. 2. The leap progress of the IoT development.

978-1-5386-5790-4/18/$31.00 ©2018 IEEE

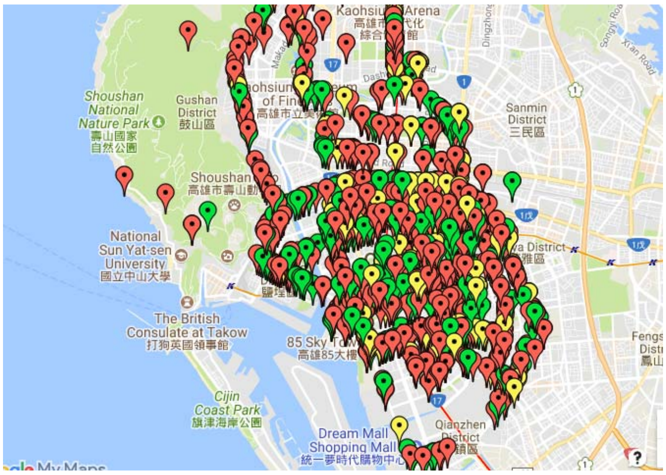


Fig. 3. The high intensity of the Wi-Fi AP deployment in the city.

We proposed an efficient procedure of catching the encrypted packets of WPA & WPA2 ,which is Intelligent Deauthentication Method (IDM). It is not specifically discussed in detail in the literature. Most of those methods or tools of collecting the 4 ways handshake encrypted packets are inefficient or just dumb packets collection because it depends on the situations on the scene , such as the strength of the wireless wave-RSSI, the communication condition between the target AP and its end users. The RSSI is the key element of Wi-Fi attack, and we can only do the cryptanalysis with the minimum range of the radio wave that we can detect, or nothing we can do about it. The present tools are grouped into fully automatic and fully manual in command lines, and both are faced with the deficit of not responding or lose its signals. The whole process must be monitored by one who can decide to keep or stop the deauthentication in the capture of the encrypted packets by its current conditions of the communication or the RSSI strength [4] which means that the wave of the target has the power to send the packets back. What bothering us most is the dumb packets or not responding because the target AP has no the power ability to send the radio wave back with the encrypted packets in it. Mostly, the penetration test analyzers usually couldn't identify the situations in the real street conditions. There is no an efficient method of catching Wi-Fi encrypted packets, and the proposed procedures are semi-automatic plus human brain with high efficiency. We can do the cryptanalysis of Wi-Fi in the real street environment to show the world that how dangerous the situation it is. For the ethical regulations, this study obeys the laws of Taiwan which allows specific sniffing the wireless radio wave with the academic usage. We keep the data secret no logging in, no data theft, and no denial of service [14].

II. The Related Work of the Wi-Fi Attack

A. Simulation in the Lab Inside

It is mostly implemented inside the lab or simulations because its difficulty in capturing the real street encrypted packets for the key element-RSSI which dominate the most of the process because it is unstable in the buildings and the interfering of other radio wave. On the contrary, the situation or environment is relatively simple with the strong RSSI, powerful radio wave exchange with minimum interfering, and no distance concerns. Distance from the target is also an important variable because the power of the radio wave may change among buildings or weather conditions in the real environment. The followings are the table of the simulation inside the lab environment [5], [6], [7], [8]. From these simulations, the passwords are set in advance, so there is no the problem of analyzing the combinations of passwords. We can find that the complicated situations we faced in the cryptanalysis of Wi-Fi security.

B. Types of Attacks in Wireless Network

The wave of wireless APs is exposed to the air without boundaries, and directions, and that's why the APs are so vulnerable to the attackers. So the attackers can receive the wave in any directions as long as he can be within the range of the radio wave. We can do several types of propagation secretly. One of the wireless attack features is that we can do that without being identified because one can do with a laptop plus an extra antenna acting like usual users. This is the worst thing in the wireless security, though, we have the tough protection protocol, WPA&WPA2. We can get the certain information from the target Aps, and the best way to take the full control of the AP is via the password cracking. Here are some typical kinds of attacks as the followings:

TABLE 1. THE TYPICAL KINDS OF WI-FI ATTACKS

Active [9], [10]	**Passive [11]**
Dos flooding,	Monitor and Eavesdropping
Routing attack	Camouflage Adversaries
Wormhole	Traffic Analysis

C. The Relations between the RSSI and the Wireless Attack

The RSSI [12], [13] is the most fundamental and key element of the attack over the air, and it takes enough strength of both sides for a successful attack. The wave of the attacker must reach to the range of the victim and the wave of the victim also has to be sent back to the device of the attackers. Presently, we don't find any literature in this aspect, and we usually sit and wait there for the dumb communication in the capturing the encrypted packets in the real street environment. The tools we find for capturing the encrypted packets have no such mechanism handling this part of monitoring the situations on the scene, and make the whole process in vain. The strong strength of the radio wave and intelligent monitoring are the important successful techniques in capturing the encrypted packets of the Wi-Fi network for the passwords.

D. The Deauthentication and Passwords

The deauthentication is a type of Dos attacks implemented in the air by the radio wave which stop the connection of the Aps and its clients. The only way we can get the encrypted packets from the air is the deauthentication which stops the connection between target and its clients, and take the packets once they reconnected to each other if it is a correct 4 ways handshake. The man-in-the-middle is also a nice way to collect the encrypted packets, but it is an inactive method without the mobility because we can do nothing without the target device connected to us. The method of deauthentication is easy to do, and most important of all, the cryptanalysis is getting easier and easier with GPU and the lazy passwords. We can do the deauthentication anywhere as long as we can identify the target, and will stop the procedures once we find that there is a dumb responding. Here is a sample for the high cracking rate of 68 % [14] and the deauthentication is active and selective which we can control the attack procedure. On the contradictory, the attack of man-in-the-middle is passive waiting the victims.

In sum, we proposed a method is different from the previous literature, which is all inside the lab setting [5], [6], [7], [8]. The key point is that the present software are either fully automatic or fully manual with very low efficiency because the possible signal losing or not responding. What we improved is adding the "observation" during the attack to see whether we should abort or not.

III. Design: The procedure of IDM

Here we use the open source software, aircrack-ng [15] as the base of the proposed procedures as in Fig. 4.

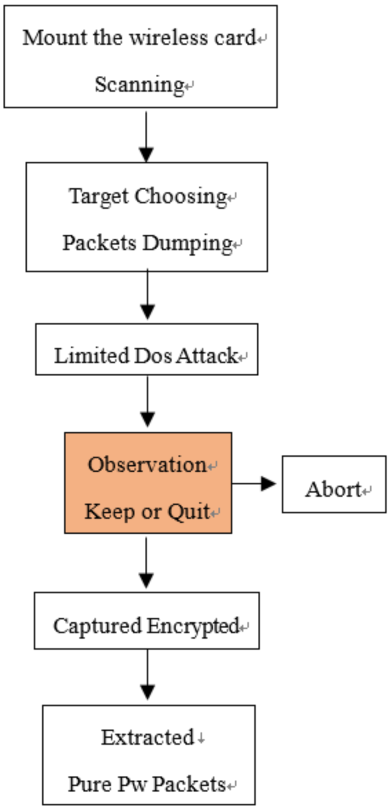


Fig. 4. The flow chart of the IDM

A. Mounting the Extra Wireless Card and Scanning

Particularly, we need the wireless card with strong scanning ability. The built-in wireless card of the mobile device is equipped with only the basic, limited scanning ability, so we implemented the extra amplifying chip device connected to the mobile device. With this, we can expand our searching range and targets.

1. ifconfig wlan0 up (ifwconfig)

Where: make sure the extra wireless card connected to the device.

2. airmon-ng start wlan0

Where: mount the external wireless card into the system.

B. Target choosing and packets dumping

With the strong excellent scanning power, we can monitor at least 500~800 M or more range of the wireless activities depending on the situations of the buildings with which the radio wave influenced. We can have more targets to choose by its RSSI and communication conditions from the monitoring.

1. airodump-ng –w FileNanme –c 6 00:11:22:33:44:55 mon0

Where: writing the packets during the communication.

C. Deauthentication (DoS attack) and Observation

After we chose the one to attack, we can focus on the target AP and its clients by the mac address. We can decide how many times doing the deauthentication (DoS attack) from one to unlimited, and have to control the amount of DoS attack. It will easily be a dumb attack if we don't manually control the number of the DoS attack and monitor the situations that the radio wave of the target AP couldn't have the radio strength to send the encrypted packets back. With the control, we can design our strength in attacking, and not being discovered by certain defense system.

1. airplay-ng -5 10 –a 00:11:22:33:44:55 –c aa:bb:cc:dd:ee:ff mon0

Where: we do the deauthentication and the number 5 is the times we attack.

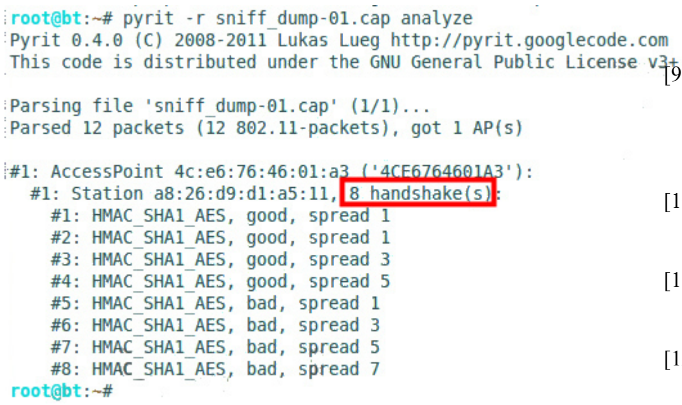
The airplay-ng is the fully manual software which makes the process longer and inefficient, so we use the tool, "gerix-wifi-cracker" [17], a fully automatically in choosing the targets and doing the deauthentication. We can do the capturing of the encrypted password packets of WPA & WPA2 efficiently with "gerix-wifi-cracker" [17] and our decisions on the spots. Human brain is the very crucial factor for the cryptanalysis of WPA& WPA2 because the situations there are handful.

D. Packets extracting

Once, the encrypted WPA & WPA2 packets captured, it might be with other types of internet information which makes the needed packets uneasy or unable to be analyzed, e.g., one AP authenticated with more than one client as depicted in Fig. 5 with eight clients. We have to make the encrypted packets pure with the necessary elements only for the coming cryptanalysis.

1. pyrit –r "the path of the encrypted packets" analyze [16]

Where: extract the pure 4 ways handshake packets.



```
root@bt:~# pyrit -r sniff_dump-01.cap analyze
Pyrit 0.4.0 (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Parsing file 'sniff_dump-01.cap' (1/1)...
Parsed 12 packets (12 802.11-packets), got 1 AP(s)

#1: AccessPoint 4c:e6:76:46:01:a3 ('4CE6764601A3'):
  #1: Station a8:26:d9:d1:a5:11, 8 handshake(s):
    #1: HMAC_SHA1_AES, good, spread 1
    #2: HMAC_SHA1_AES, good, spread 1
    #3: HMAC_SHA1_AES, good, spread 3
    #4: HMAC_SHA1_AES, good, spread 5
    #5: HMAC_SHA1_AES, bad, spread 1
    #6: HMAC_SHA1_AES, bad, spread 3
    #7: HMAC_SHA1_AES, bad, spread 5
    #8: HMAC_SHA1_AES, bad, spread 7
root@bt:~#
```

Fig. 5. The encrypted handshake packets with 8 clients.

With this pure extracted packets, we can put it into the designed system with GPUs [14], and the socially simple passwords are easily analyzed in a few seconds to minutes.

IV. Conclusion and Future Work

From the procedures we proposed, outside the lab conditions, and no simulations, we can truly do the capturing the encrypted packets easily in the real environment. Now, we got 298 extracted, pure 4 ways handshake packets for the cryptanalysis, and these were collected from the living street environment ,which is the important data for the challenge of the WPA & WPA2 security protection. It is never mentioned before that there are so many raw data can be analyzed from the real environment, practically, and the cracking rate is at least over 50 % by the different types of sorting the categories and as a whole. In the future, we plan to compile those open source program into one UI ,which is a semi-automatic system with any command lines, and will make the capturing of the WPA & WPA2 encrypted packets more efficiently than we did presently. And more, visualization is also a good way to show the risky map of the WPA & WPA2 protection with different types of passwords cracked integrating with wardriving map of the certain areas in the city.

References

[1] Wigle.net. General Stats. Retrieved from https://wigle.net/gps/gps/main/stats/, 2018.

[2] Connected IoT. Retrieved from https://www.statista.com, 2018.

[3] D. Luminita, “Wireless LAN Security-WPA2-PSK Case Study, AWER Procedia Information Technology and Computer Science,” pp. 62–67, 2012.

[4] R. Wu, Y. Lee, H. Tseng, Y. Jan, and M. Chuang, “Study of Characteristics of RSSI Signal,” ICIT 2008 IEEE International Conference, pp. 3–5, 2008.

[5] V. Kumkar, A. Gupta, S. Shrawne, A. Tiwari, and P. Tiwari, “Vulnerabilities of Wireless Security Protocols (WEP and WPA2),” International Journal of Advanced Research in Computer Engineering & Technology, vol. 1, no.2, pp. 34–38, 2012.

[6] M. Agarwal, S. Biswas, and S. Nandi, “Detection of De-Authentication DoS Attacks in Wi-Fi Networks.: A Machine Learning Approach,” IEEE International Conference on Systems, Man, and Cybernetics, SMC 2015, pp. 246–251, 2016.

[7] A. Yacchirena, D. Alulema, D. Aguilar, D. Morocho, F. Encalada, and E. Granizo, “Analysis of attack and protection systems in Wi-Fi wireless networks under the Linux operating system,” 2016 IEEE International Conference on Automatica, pp. 1-7, 2016.

[8] M. Aye, and C. Aung, “Detection and Mitigation of Wireless Link Layer Attacks,” Software Engineering Research, Management and Applications (SERA), IEEE 15th International Conference, pp. 173–178, 2017.

[9] N. Dharini, R. Balakrishnan, and A. P. Renold, “Distributed detection of flooding and gray hole attacks in Wireless Sensor Network,” International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials, ICSTM 2015, pp. 178–184, 2015.

[10] S. Ji, T. Chen, and S. Zhong, “Wormhole attack detection algorithms in wireless network coding systems,” IEEE Transactions on Mobile Computing, vol.14, no.3, pp.660–674, 2015.

[11] Wahid, A., &Kumar, P.: A Survey on Security Attacks in Wireless Sensor Network. In: International Journal for Innovative Research in Science and Technology on Proceedings, 1(8), pp.1684–1691(2012).

[12] R. Wu, Y. Lee, H. Tseng, Y. Jan, and M. Chuang, “Study of Characteristics of RSSI Signal,” Industrial Technology, IEEE International Conference, pp.3–5, 2008.

[13] M. Khanderiya, and P. M. Panchal, “A Novel Approach for Detection of Sybil Attack in Wireless Sensor Networks,” IJSRSET, vol.2, no.3, pp. 113–117, 2016.

[14] C. M. Chen, and T. H. Chang, “The Cryptanalysis of WPA & WPA2 in the Rule Based Brute Force Attack, An Advanced and Efficient Method,” 2015 10th Asia Joint Conference on Information Security, AsiaJCIS 2015, pp. 37–41, 2015.

[15] www.aircrack-ng, Retrieved from Aircrack-ng, http://aircrack-ng.org/, 2018.

[16] pyrit.wordpress.com, Retrieved from Pyrit, https://pyrit.wordpress.com/, 2018.

[17] https://github.com, Retrieved from Gerix-wifi-cracker, https://github.com/kimocoder/gerix-wifi-cracker, 2018.