Journal of information and communication convergence engineering
http://jicce.org

J. Inf. Commun. Converg. Eng. 10(2): 156-161, Jun. 2012 **Regular Paper**

Hacking and Security of Encrypted Access Points in Wireless Network

Se-Hwan Kwon, and Dea-Woo Park*, *Member, KIICE*

Department of IT Application Technology, Hoseo Graduate School of Venture, Seoul 137-867, Korea

Abstract

An increasing number of people who use a smart phone or tablet PC are accessing wireless networks in public facilities including cafes and shopping centers. For example, iPhones and Android Phones have been available since 2010. However, security incidents may occur through all sorts of malicious code infection of users' personal information during the use of an insecure wireless network. In this paper, we will describe the Wi-Fi protected access **(**WPA) and WPA2 encryption systems used to access a wireless network from a smart phone and tablet PC, and demonstrate the access point (AP) hacking process in a wireless network to which a password is applied on the basis of the analyzed WPA and WPA2 passwords. We will analyze the method of successful AP hacking and propose an approach to enhancing wireless LAN security. This study will contribute to enhancing the security and stability of wireless networks.

Index Terms: Aceess point, Hacking, Wi-Fi, Wi-Fi protected access, Wi-Fi protected access 2

I. INTRODUCTION

The use of the wireless internet has greatly increased since the spike in adoption of smart phones and tablet PCs in 2010.

A summary of the results of a survey investigating the use of the wireless internet issued by the Internet Statistics Info Search System in November, 2010, is shown in Fig. 1. As can be seen, mobile phones (including smart phones) that can access the wireless internet account for 98.1% of wireless connections, while laptop PCs (including netbooks and tablet PCs) and MP3 players constitute 25.8% and 16.2%, respectively.

As described above, the wireless internet is accessed with portable devices. However, the level of recognition for wireless LAN security is not high. Smart phone and tablet PC users use Wi-Fi protected access (WPA) and WPA2 encryption in non-encrypted or encrypted access points (Aps). That is, when using the wireless internet with an insecure wireless AP, hackers attack the insecure users and can steal personal information. Therefore, there is a need for studying hacking and the security of WPA and WPA2 encrypted APs.

We performed an experiment connecting a wireless LAN to Backtrack 4 to use Aircrack so as to extract the password of a wireless AP, and propose a scheme for security according to the experimental result.

Section I will describe the necessity of this study; section II will describe WPA and WPA2; section III will analyze cases of wireless network hacking; and section V will report on our experiment with obtaining WPA and WPA2 passwords. In section IV, we will propose a scheme for security to protect insecure wireless routers. Section V will also present conclusions.

Received 10 February 2012, **Revised** 05 March 2012, **Accepted** 21 March 2012
***Corresponding Author** E-mail: prof_pdw@naver.com

Open Access **http://dx.doi.org/10.6109/jicce.2012.10.2.156** print ISSN:2234-8255 online ISSN:2234-8883

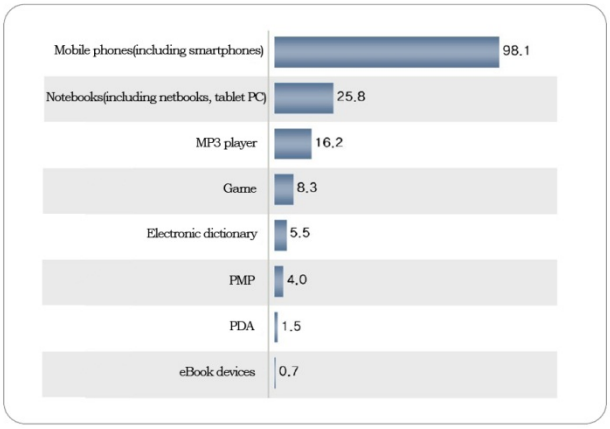

Fig. 1. Status of wireless internet terminals (multiple answers, %).

II. RELATED STUDIES

A. AP

An AP is a device for connecting a wired LAN and a wireless LAN. An AP is generally an independent device and plugged into the Ethernet or a server. That is, an AP is used for wireless signal processing and antenna and interconnecting the wired networks and the wireless networks. More and more home users use wired/wireless internet routers or wireless internet routers in which an AP is equipped with internet connection sharing.

B. Encryption at AP

1) WPA

WPA [1] is one of the Wi-Fi wireless LAN security standards. It provides more refined data encryption than wired equivalent privacy (WEP), which is incomplete in terms of user authentication, and provides satisfactory user authentication. The encryption technique employed in WPA is temporal key integrity protocol (TKIP) [2].

Since TKIP includes a key assignment per packet, confirmation of message integrity, an extended initialization vector, resetting and key values, it cannot be hacked and requires an authentication procedure for access to a network. The wireless application protocol (WAP) [3] employs 802.1x and extensible authentication protocol (EAP), which is an extended authentication protocol that provides powerful user authentication.

2) WPA2

WPA2 [4] is provided with the advanced encryption standard (AES) [5] algorithm as an industrial encryption standard, and is substituted for DES and 3DES.

WPA2 uses the counter mode (CTR) for encrypting data and message integrity code (MIC), and the cipher block chaining message authentication code (CBC-MAC) [6] protocol for authentication and retention.

The MIC of WPA2 provides data retention in a field that is not easily changed in the 802.11, unlike WEP [7] and WPA, is compatible with WPA, and is different from WPA in that data encryption, called AES, is enabled. The AES encryption technology has been used to send/receive information by the U.S. government to demonstrate its strong security.

III. CASES AND RISKS OF WIRELESS NETWORK HACKING

A. Cases of Wireless Network Hacking in Korea

On June 25, 2011, the Chosun Daily reported that 690 hacking incidents have taken place since the opening of the 18th National Assembly (May 30, 2008). The incidents of hacking the computer network in the National Assembly were reported by the National Cyber Security Center (NCSC) under the National Intelligence Service. According to this report, 148 hacking incidents were about stolen e-mail passwords and it was determined that most of the e-mail accounts were owned by assistants of assembly people who worked for security-related committees, for example, the Foreign Affairs, Trade and Unification Committee (FATUC) and the Defense Committee.

According to the confidential documents of the Legislative Information Office in the National Assembly, e-mail addresses and passwords of an assemblyman's office under the FATUC (the former Minister of Foreign Affairs and Trade) were hacked on December 17, 2010. It was said that the hacked e-mail accounts include details for reporting work processes sent from the Ministry of Unification about the Hanawon which is a shelter for people who had escaped from North Korea.

It was known that e-mail accounts of the assemblyman's office under the Defense Committee (office of the former Minister of National Defense) were hacked on March 28, 2011. In the National Assembly meeting in April, the staff of the Ministry of Unification accessed the internet through the wireless LAN in the National Assembly building, which resulted in being hacked. In the incident, it was said that the hacker first read and deleted the e-mail sent by the Ministry of National Defense before the relevant recipients read it.

It was said that the e-mail accounts of the reporters who access the wireless LAN in the National Assembly building were also hacked.

In addition, many of the details reported to the National Assembly people were disclosed by hacking. The e-mail was sent by security-related ministries including the Ministry of Foreign Affairs and Trade, the Ministry of National Defense, and the Ministry of Unification.

It was revealed that most of the hacking was performed from an internet address (IP) located in China and most of the hacked documents were received/sent through ordinary commercial e-mail accounts, not internal e-mail.

B. Cases and Risks of Wireless Network Hacking in the United States

In TJX, which is a retail chain in the U.S., approximately the personal information of 45 million credit card users was stolen through wireless LAN hacking from July 2005 to December 2006. This incident resulted in class action lawsuit for compensation and TJX had to pay penalties. People are thus interested in solutions to the issues of low wireless LAN security and payment card industry (PCI) compliance.

Since 2010 in the U.S., the Visa card and the MasterCard companies have been making a great effort to address the security issue, and franchise shops will be fined if they do not comply with PCI.

C. Threats to Wireless Networks and AP Hacking

The issue of hacking threats to wireless networks includes threats to standard modes including the IEEE 802.11 a/b/g/ mode and stealing of internally important data on wireless devices such as WiBro or T-network. Very important very valuable technical information can be stolen from companies through such wireless network devices, but we do not yet have the complete means to prevent such attacks.

There is a serious worry about service availability in addition to stolen data. It is possible to attack the wireless LAN infrastructure in an entire building with a laptop PC and a wireless LAN card after downloading a denial of service (DoS) attack tool from the internet to paralyze services. Disruption and damages can occur, for example, in shopping centers where billions of dollars of sales occur per hour or hospital systems directly connected to sustaining patients' lives, and large-scale enterprises can be stopped.

Typical threats to a wireless LAN that cause such damages include unauthorized AP installation in a company, access to external APs, wireless network sharing, AP service ID stealing in a company, illegal AP connection in a company, policy violation in a company, stealing users MAC addresses, and DoS attacks.

IV. HACKING WIRELESS NETWORK ENCRYPTED AP

The following experimental environment was built in a laboratory in our graduate school for hacking the wireless security of WPA and WPA2.

A. Experimental Environment

- IPTime N608: wired/wireless router
- IPTime G054UA: wireless router
- Samsung notebook: SenS NT-Q70A/W203
- BackTrack4

Fig. 2. Experimental environment.

As shown in Fig. 2, the IPTime G054UA wireless router was connected to a laptop PC to constitute an environment for obtaining wireless packets as shown below.

B. WPA Password Crack

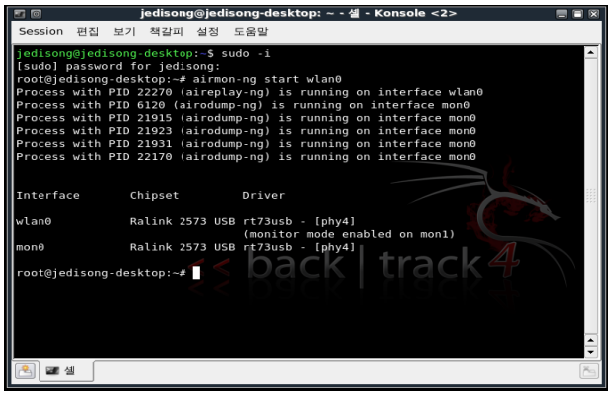

Fig. 3. Wireless router connected to BackTrack4.

In Fig. 3, we used BackTrack4 and the connected wireless router to capture packets and to attempt cracking with the collected packets, so as to hack the password of the encrypted wired/wireless router. [8].

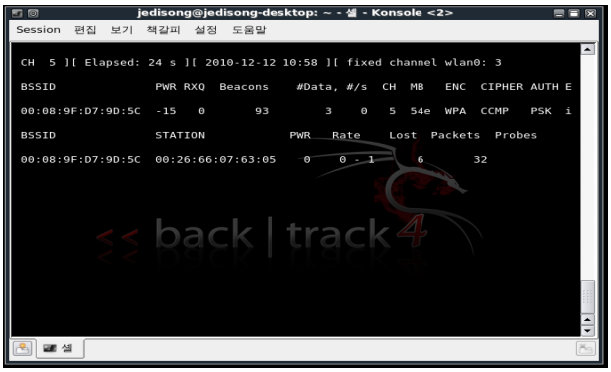

Fig. 4. Wi-Fi protected access encrypted access point.

In Fig. 4, it is identified whether there is a wireless AP in place in order to carry out the experiment of cracking the wireless AP. It is found that the AP's basic service set identifier (BSSID) is 00:08:9F:D7:9D:5C, the channel is 5, the password is WPA and the connection is made to the IPTime G054UA wireless router. It is necessary to capture packets in order to crack a WPA password, and the number of required packets is 30,000 to 40,000.

After finishing packet capturing, it is saved as a file as shown in Fig. 5. In this experiment, the packets were captured in the file output-02.cap.

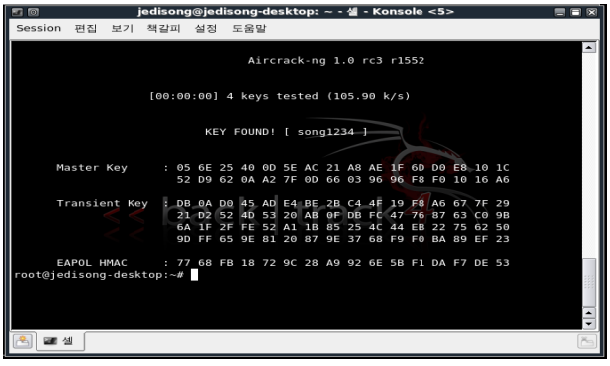

Fig. 5. Capturing packets.

The password is then extracted from the file output-02.cap of captured packets with the Aircrack tool as shown in Fig. 6.

If the encrypted password is found in the WPA protocol, "KEY FOUND!" is displayed and the found password is displayed in the brackets. In this experiment, it is seen that the password is "song1234".

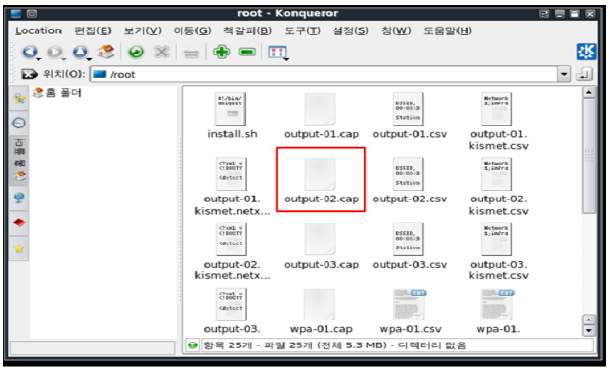

Fig. 6. Confirm Wi-Fi protected access password.

C. Cracking a WPA2 Password

For WPA2, the same process is applied as for WPA. Fig. 7 shows how to identify the encrypted wireless AP with WPA2. In the above experiment, an AP is identified in which the encrypted wireless BSSID with WPA2 identified in BackTrack4 is 00:08:9F:D7:9D:5C, the channel is 5, and the password is WPA2.

Fig. 8 shows the process of saving the encrypted packets with WPA2 as home-01.cap and then extracting the WPA2 password with the Aircrack tool. If the encrypted password is found, "KEY FOUND!" is displayed and the found password is displayed in the brackets.

D. AP Attack Access through Encrypted AP Cracking

A smart phone is used to access the network in order to check whether the password found by cracking the encrypted AP with WPA and WPA2 is correct.

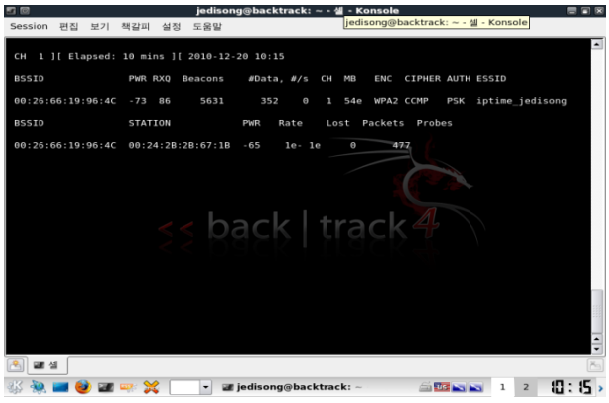

Fig. 7. Wi-Fi protected access2 encrypted access point.

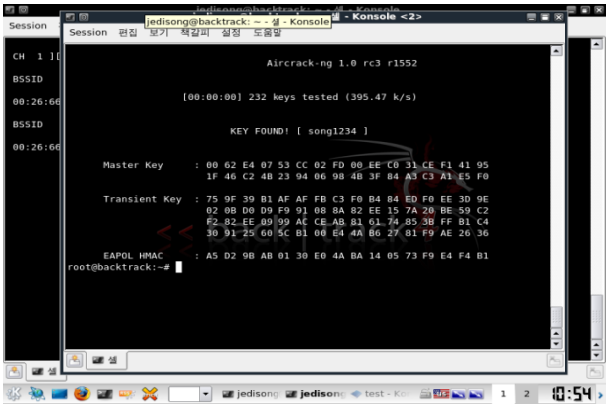

Fig. 8. Confirm Wi-Fi protected access2 password.

Fig. 9. Window showing access to access point.

In Fig. 9, access to the cracked AP is seen on the right side by entering the obtained password and then pressing the Join button to access the cracked AP.

E. Scheme for Wireless Network AP Security

We propose the following scheme for security so as to enhance wireless router security.

First, set a complicated password for a wireless router. Set a long password including numbers, English letters, and special symbols so that a hacker has to spend a long time to crack the password and then gives up hacking.

Second, activate MAC address filtering. Most routers identify only the MAC address and allow only the permitted devices to access. However, this method allows hackers to easily modify the MAC address.

Third, place your router, the wireless internet router, or the AP in a safe place. This is because it is not easy for other people to discover and intrude on the router if the wireless internet signals are far away. It is thus necessary to place the wireless router in a safe place so that other people cannot use it.

Fourth, deselect the service set identifier (SSID) broadcasting option. The SSID represents the name of the WAP in a wireless network. It is set that WAP can broadcast the SSID. Therefore, wireless network users who first access the WAP can achieve easy access. However, since hackers obtain access with such SSIDs, it is recommended not to use broadcasting.

V. CONCLUSIONS

Smart phone, laptop PC, and tablet PC users implement web surfing, e-mail, social networking service (SNS), and streaming services. However, insecurity together with easy access to a wireless network is a hacker's targets. In this study, we explained the method of attacking the WPA and WPA2 encryption scheme in a wireless AP to capture its password, and then proposed a security method.

Further study is required to determine how a user's personal information is hacked, using address resolution protocol (ARP) spoofing and sidejacking in an AP of which the password is hacked.

REFERENCES

[1] H. C. Jung and H Lee, "Study on security reinforcement method by wireless security status survey and analysis," *Proceedings of the Korea Information Processing Society Conference*, Seoul, Korea, pp. 857-860, 2006.

[2] M. S. Kang and C. S. Hong, "A prevention mechanism against DoS attack using the TKIP in wireless LAN environment," *Proceedings of the Korea Computer Congress*, Pyeongchang, Korea, pp. 145-147, 2005.

[3] C. G. Park, "Methods of WAP gateway capacity dimensioning and traffic forecasting," *Journal of the Korean Institute of Communication Sciences*, vol. 35, no. 4, pp. 576-583, 2010.

[4] Wi-Fi protected access 2 [Internet]. Available: http://choijdgo.blog.me/54403682.

[5] C. K. Hong and Y. J. Jeong, "Design and implementation of IEEE 802.11i MAC layer," *Journal of the Korean Institute of Communication Sciences*, vol. 34, no. 8, pp. 640-647, 2009.

[6] H. B. Kim and S. J. Lee, "Study on secure unattended defence system implementation using wireless sensor network," *Proceedings of the Korean Society for Internet Information*, vol. 7, no. 2, pp. 177-182, 2006.

[7] S. Lee, J. Kang, H. Moon, M. Lee, and C. K. Kim, "Per packet authentication scheme using one-bit in 802.11 wireless LAN," *The KIPS Transactions: Part C*, vol. 12C, no. 4, pp. 465-472, 2005.

[8] W. S. Chun and D. W. Park, "A study of forensic on eavesdropping from VoIP and messenger through WiBro network," *Journal of the Korea Society of Computer and Information*, vol. 14, no. 5, pp. 149-156, 2009.

Se-Hwon Kwon
was born in Seoul, South Korea in 1966. He is in doctoral studies in the IT application science department at the Hoseo Graduate School of Venture, South Korea. Currently, he is CEO of the Police Welfare Center (Co.). He received the B.S. degree in resource engineering from the Cheongju University in 1988. He also received the M.S. degree in resource engineering from the Hanyang University in 1993. He finished his doctoral studies in computer engineering at the Graduate School of Dongguk University in 2002. His research interests are hacking, forensics, information protection, IT convergence, and network security.

Dea-Woo Park
was born in Seoul, South Korea in 1959. He is an adjunct professor of the IT application science department at the Hoseo Graduate School of Venture, South Korea. Dr. Park received the B.S. degree in computer science from Soongsil University in 1995. He then received the M.S. degree in 1998. He received the Ph.D. degree from the computer science department of Soongsil University in 2004. Dr. Park has worked as the head of researcher and developer laboratories at Magic Castle Co., Ltd. His research interests are hacking, forensics, information security of computers and networks, and mobile communication security.