International Journal of
Advanced Science and Convergence

ISSN : 2619-8150
Volume 3, Number 2, June 2021
https://doi.org/10.22662/IJASC.2021.3.2.001

Blocking techniques for various hacking attacks on wireless Internet services

Hye-Ryeon Nam[1] and Sunghyuck Hong[2]

[1]Student, Chemistry, Kongju National University, Republic of Korea
[2]Division of Information & Communication Technology, Baekseok University, Cheonan, 31065, Republic of Korea

Abstract

Background/Objectives: The wireless internet service, which has positioned as an important element to support all industries, can be connected to notebook computers and smartphones everywhere. Using wireless internet access increases, the risk of hacking also increases. **Methods/Statistical analysis:** There is information leakage accident by modulating DNS address of home router and hacking threats by using wireless router always exists **Findings:** In this paper, we search hacking techniques using vulnerabilities in wireless LAN, and analyze the need for security for wireless LANs through WEP encryption algorithms and improved encryption algorithms. **Improvements/Applications:** We also suggest countermeasures against hacking techniques such as DoS attacks, WEP Crack, and DNS Spoofing.

Index Terms

Wireless Internet, Service, Encryption Algorithm, Hacking Technology, WEP, Security

Corresponding author : Sunghyuck Hong
shong@bu.ac.kr

• Manuscript received May 1, 2021
• Revised June 10, 2021 ; Accepted June 20, 2021
• Date of publication June 30, 2021

I. INTRODUCTION

Wireless internet is an important element in modern society. Laptops and smartphones can be used in public places and by connecting to the wireless Internet everywhere, including subways and buses. But, As the use of wireless Internet has increased, the risk of hacking into it has also increased. There are several risks of hacking, including information leakage through tampering with the Internet router DNS address.

To ensure the security of the wireless router, you do not use products from vendors with weak security and you need to set security for the router itself. Also, the problem with wireless security lies not only in the simple router, but also in the wireless LAN used in memory. Laptops and smartphones of corporate insiders are defenselessly exposed to hacking risks by access of external wireless AP. Especially, if an external wireless AP is combined between a carrier-provided wireless AP or an external public wireless AP, A attacker can invade inside when the wireless device inside the corporation is connected to wireless AP of the external attacker.

Because of this, this article deals with the concept of wireless LAN, hacking attack technology using vulnerabilities of wireless LAN, and hacking techniques.

And we suggest the need for security about that and countermeasures against hacking risks.

II. RELATED WORK

A. *Wireless LAN*

Wireless LAN technology is the connection of two or more devices to each other using a wireless signal communication method. This allows users to continuously access the Internet network while moving in a nearby area. Nowadays, the Wi-Fi Alliance's trademark name, Wi-Fi, is popularly used in field of Wireless LAN technology. Wi-Fi is a technology that provides connections between wireless LANs and devices based on IEEE 802.11. Although early Wi-Fi was synonym with IEEE 802.11, it includes several 802.11-based software technologies now. Some technologies are supported in 802.11 but not used in Wi-Fi, and we should not confuse the two kinds of them.

Basically, Wi-Fi is a communication between the AP, which take on delivering data to the Internet, and the terminal where the user receives service using a laptop or smartphone. User can use Wi-Fi without any specific settings because easy-to-move terminals such as smartphones and laptops are installed by default and user who uses only laptops can use it after easily using. Currently, devices that support Wi-Fi increase such as Game console and TV, Printer.

B. *IEEE Standard*

RFIEEE 802.11 is a technology developed by the LAN/MAN Standards Committee (LAN/MAN) that is used for wireless networks, wireless LAN and Wi-Fi, and other computers.

Table 1. IEEE Standards

	802.11a	802.11b	802.11g	802.11n
Speed	54Mbps	11Mbps	54Mbps	300Mbps
Distance	450m	300m	450m	450m
Frequency	5GHz	2.4GHz	2.4GHz	2.4GHz/ 5GHz
Advantage	Less interference	being used mostly	Compatible with 802.11b	performance through a multi-antenna technique /a channel bonding
Disadvantage	No Compatibility	Transfer speed is slow	There may be interference from 2.4GHz devices	It requires a wireless

1) 802.11

Early versions of 802.11 allowed multiple devices to participate in the network using 2.4 GHz bandwidth, supporting a maximum speed of 2 Mbps, and transmitting data, but were not widely used due to lack of compatibility and slow speed among other manufactured products.

An advanced technology based on the 802.11 specification, 802.11b is known to have a peak transmission rate of 11 Mbps. But is actually only as efficient as 6-7 Mbps in implementing CSMA/CA technology [4].

Once the standard specifications were finalized, a variety of products supporting realistic speeds emerged, were distributed to replace wired networks used in homes and businesses, and some provided services in public places [4]. Using OFDM technology, 802.11a supports transmission rates up to 54 Mbps [4]. In addition, for standards that use radio waves of 5 GHz, 5 GHz has less interference between wireless phones, Bluetooth devices and communication devices can use wider radio wave bandwidth. However, due to the feature of the signal, it is easily affected by surrounding environments such as urban buildings and obstacles, and not used now because the 802.11g standard which supports the speed of 54Mbps is also invented in the 2.4GHz band of radio wave[4]. Although the specification and transmission rate are the same, the g specification uses 2.4 GHz band radio waves and is widely used due to its advantages of being easily

compatible with the 802.11b specification, which is currently widely used [4].

The current standard commercialized in South Korea is 802.11n, which uses the 5GHz and 2.4GHz bandwidth and supports speeds up to 600Mbps [4].

2) Radio Frequency Identification

RFID is an auto-recognition technology that contains information about the entire process from production, distribution, storage, and consumption in the tag of a product and is used in conjunction with information systems with mobile networks or satellites[2]. RFID Tag has a chip built in, So it sends and receives data wirelessly and automating data collection[3,4]. The ID of the object is stored in the tag, and objects, animals, and people attached with this tag can be recognized, managed, and tracked using a reader and antenna. Data can be recognized without direct contact, and the time to recognize the data is short. In addition, it is easy to maintain, does not cost maintenance, can transfer large amounts of data without restrictions on temperature, humidity, and dust, and can be reused.

III. Encryption Algorithms

A. Wired Equivalent Privacy

WEP encryption method was specified in the IEEE 802.11 Wireless LAN standard in 1990. As RC4 stream cryptography, MAC frames that can be transmitted in radio intervals are combined into 40-bit WEP shared secret codes and intentionally selected 24-bit initialization vector (IV) codes, using a total of 64-bit keys[5]. Like that, four types of long-term shared code are automatically generated from the same password sentence for encryption between the device and the AP by WEP. These four types of unique codes are separated by two bits of KeyID. Since then, only one of the four routers is used for the WEP password about MAC frames.

With the encrypted data, the transmitted MAC frames also contain the IV, KeyID, and ICV values used for encryption. So, the MAC frame will be added up to 8 bytes originally. WEP encryption method includes 40-bit WEP and 104-bit WEP, which is WEP2.

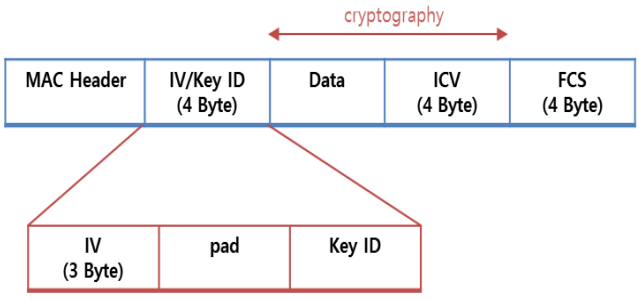

Fig. 1. WEP Cryptography

B. WPA/WPA2-PSK

It is called Wi-Fi Protected Access and has emerged as an alternative after the secure vulnerability in WEP is discovered.

WPA was used temporarily before the completion of the standard protocol, 802.11i, as an alternative to WEP's security vulnerabilities. The TKIP encryption algorithm was used, and WPA2 used the AES encryption algorithm to replace it, providing stronger security.

In contrast to WPE, WPA enhanced its ability to encrypt data through TKIP (temporary key integrity protocol). Also, WPA2 with improved security features as the second-generation WPA consisted of advanced password standardization (AES) and pre-authentication. WPA only supported Infrastructure mode, while WPA2 supported both Infrastructure mode and Ad-hoc mode.

		WPA	802.11i
	WEP	**TKIP**	**AES-CCMP**
Cipher	RC4	RC4	AES
Key Size	40 or 104 bits	128 bits encryption, 64 bit auth	128 bits
Key Life	24-bit IV, wrap	48-bit IV	48-bit IV
Packet Key	Concat.	Mixing Fnc	Not Needed
Integrity — *Data*	CRC-32	Michael	CCM
Integrity — *Header*	None	Michael	CCM
Replay	None	Use IV	Use IV
Key Mgmt.	None	EAP-based	EAP-based

Fig. 2. WPA/WPA2-PSK Encryption

C. WPA-EAP(WPA Enterprise)

Compared to WPA-PSK, which focuses on WEP's encryption code management method, WPA-EAP supplements for vulnerabilities in users' authentication areas. Called WPA-EAP, the method selected various encryption algorithms and security standards to enhance user authentication and encryption. The most important of these is the adoption of the IEEE 802.1x standard and the EAP authentication protocol [6]. The IEEE 802.11x standard is used as a port-based authentication standard in wired LAN environments, and the IETF's EAP authentication protocol allows it to accommodate a variety of authentication mechanisms [6].

To implement the WPA-EAP method in a large wireless LAN environment, an authentication server is added that performs authentication of client, AP, and user. This is

acceptable in the 802.11x standard.

802.11x is a standard for network access control based on port [7]. This is due to the authentication procedures required in the ADSL/VDSL environment. It was used as a means of communication using the Internet connection or dial-up at home. It required authentication procedures for users and devices to allow network access. The 802.11x standard consists of requestors, certifiers, and authentication servers.

D. Need for security about wireless LAN

The supply of wireless LANs has made Internet usage and the environment more convenient, but this has also increased the risk. Public institutions building VPNs and Firewalls believe they are safe from wireless LAN threats. However, it is not known that wireless LAN signals invades security facilities in wired networks and open them to attackers. If the security of wireless LANs used by companies or organizations is not complete, it can invade the corporate backbone network, steal various information, and contaminate the network. Therefore, security issues in wireless networks are not problem to individuals.

Understanding the vulnerabilities of all security also makes it easy to understand the risks of wireless LANs. Wireless LAN is more dangerous because it is wireless, as well as having all the security problems that wired networks have. As laptops with wireless LAN functionality are increasing and operating systems become more wirelessly friendly, most laptops have ability that automatically detect and connect AP basically.

Finally, wireless network devices have many ways of connecting to APs. If a very strong signal is detected, the new AP can be accessed immediately, and the AP can become a laptop computer used by hackers.

With the addition of more wireless networks, the risk of hackers invading is also increasing. Companies and institutions must also think about public security being built across the enterprise and around the world.

IV. HACKING TECHNOLOGY FOR VULNERABILITY OF WIRELESS LAN

A. DoS(Denial of Service) Attack

Denial-of-service attack (DoS) is that attack a system that maliciously shortens resources in that system and prevents it from being used for its original use [8,9]. An attacker forces to disconnect by sending DeAuthentication packets and DeAssociation packets that trick the user into their AP and refuse to join the 802.11 binding process. In Wireless environment, it is primarily an attack that forces the connection between the AP and the Station to be broken, accompanied by a DoS attack in the process of WPA Crack.

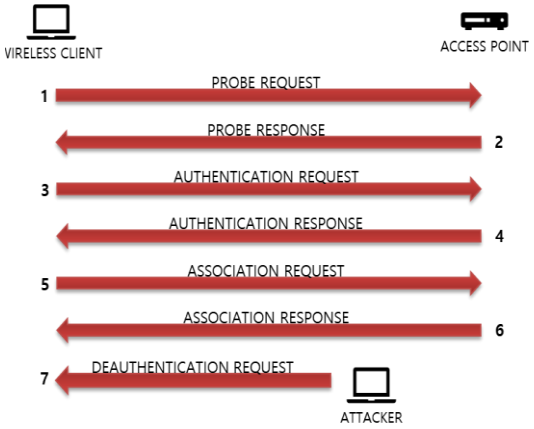

Fig. 3. Dos Attack Principle

B. WEP Crack

WEP Crack requires a lot of packets encrypted with the same key. Thus, an attacker must force a packet injection (data packet) into the network. The ARP Replay is sent to the target AP using the air-playing tool. And causes a lot of data traffic to the network. Many of these generated data packets collect encrypted packets, which can be identified as ARP packets by examining the size of the packets. These packets can be checked with the air-dump tool and are automatically stored. In this way, the attack was carried out using the air-cracking tool and then hacked if it appeared to be an ASCII value.

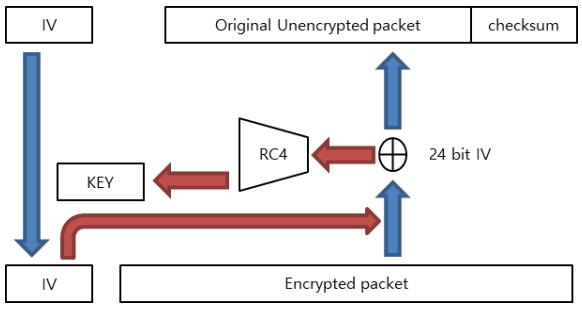

Fig. 4. WEP Crack Method

C. DNS Spoofing

It is a technique in which hackers intervene between normal DNS servers and user communications to obtain information by sending out unusual DNS answers. First, if an attacker's IP is tricked into Gate Way, the user's computer sends a packet to the attacker disguised as Gate Way. If a hacker sends a reply to a user's request and logs in to a fake homepage, the victim's ID and password will remain with the attacker.

As shown in Figure 5, the normal process sends a DNS Query via Gate Way to the DNS server to ask for the IP of the homepage when the user connects to a specific homepage. The DNS server that receives Query finds the company's IP and sends it again and connects to the company's web server when it connects to the IP it receives.

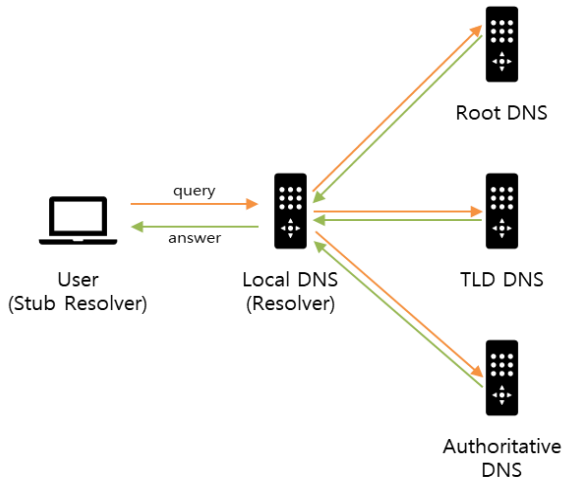

Fig. 5. DNS Process

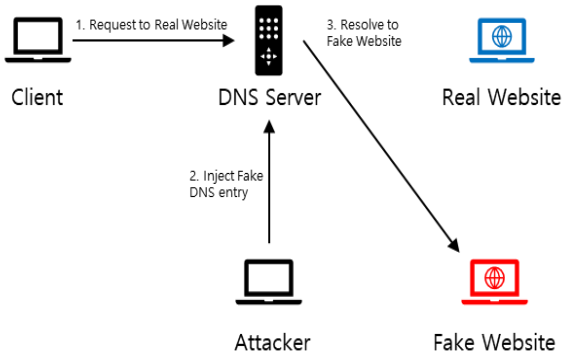

Fig. 6. DNS Spoofing

The principle of DNS Spoofing is shown in Figure 6. A user sends DNS Query packets to both attackers and DNS servers to access the homepage. The user receives DNS Reply packets sent by the attacker and accesses the address, and DNS Reply packets sent by the DNS server are discarded in the process.

D. Hacking countermeasures

Usual OpenAP without authentication are defenseless for hacking. These AP periodically broadcasts the SSD(Service Set Identifier) which is the unique ID of the AP user group, so they can access location via programs such as "Netstumbler".

Usually, an AP that supports IEEE 802.11b must be found within 100 meters of the neighborhood. However other abnormal standard AP can be found in the range of up to 4 km. Attackers usually use the "War Driving" method that contains PDA and laptop with antennas like Netstumblers in car and drive around to find APs without security features. ADSL router that provides wireless LAN AP feature used by individual users often do not have special security settings. Hackers connected to these APs can use packet-sniffing programs such as Ethereal Kismet Wireless to detect IP bandwidth for institutions or businesses. And they retrieve information such as their IDs and passwords with access to intranet with The Airopeek Sniffer Wireless tool.

For APs with web secret key functionality that encrypts data between the AP and the client wireless LAN adapter, the secret key also can be found through programs such as Airsnort WEP Crack. Crack programs are available on P2P programs or websites because they are free software based on partial open source, although there are commercial products.

In addition, the Ad hoc program allows the laptop to be configured to function as an AP, which can be accessed and hacked. Usually, internal users of a company are likely to use it, and with just one wireless LAN adapter, all information of the company can be leaked.

To respond to hacking, the AP's SSID broadcasting feature should not be used and speculative SSID names should not be used. It should also enable the ability to authenticate to the AP via the MAC address, which is the unique number of the wireless LAN adapter and activate the feature that set up web keys. Setting up this level of security prevents hacking.

To enhance security more, it is necessary to check whether NULL values are allowed, character sets allowed, minimum or maximum allowable length, and data formats, and to prevent unauthorized users from accessing the system. Also, to checks permission of web content, caching checks of clients, and Path Traversal functions. Hacking can be prevented by eliminating the use of vulnerability services, using packet filtering access control and encryption protocols, and IP authentication-based access control.

V. CONCLUSION.

With the development of wireless network, various service is made and the risk of hacking is increasing. Users should be more careful not to leak important information from companies or individuals stored in smartphones and laptops when accessing public Wi-Fi. Although security considerations are essential, efforts should be made to enhance security in many ways, as the application of consistent security policies is challenging due to the diversification of wireless LAN usage environments.

Various attack methods have been proposed as vulnerabilities have been identified in the security mechanisms of WPA and WEP provided by IEEE. We also present a defense against hacking techniques targeting these vulnerabilities. Responding to hacking requires banning the use of SSIDs that continuously expose the location of the AP and avoiding using speculative SSID names. An exception rule for web requests must be established to thoroughly validate source code.

Because it is possible to take and abuse personal information using the convenient open wireless network

We should always be aware of how to respond and be careful about hacking, such as not accessing advertisements and inappropriate sites.

ACKNOWLEDGMENT

This research is supported by 2021 Baekseok University Research Fund.

REFERENCES

[1] S.M. Park, H.J. Kim, J.G. Kim, T.G. Hwang, and S.J. Lee(2013). Design and Implementation of Multiple Access Game Control System using Bluetooth. *Journal of IKEEE*, 17(4), 492-498.

[2] J.A. Son, and K.M. Heo(2013). Fear and Measures of Motor Vehicles Communication Network Hacking. *Korean Police Studies Review*, 12(1), 113-142.

[3] S.H. Hong(2013). Disconnection of Wireless LAN Attack and Countermeasure. *Journal of Digital Convergence*, 11(12), 453-458)

[4] H.B. Shim(2012). Comparative analysis for advanced technologies of the location based service. *Journal of the Korea Institute of Information and Communication Sciences*, 16(4), 853-871)

[5] J.H. Choi, and S.H. Oh(2012). Study on Vulnerability and Countermeasures of Authentication Mechanism in Wireless LAN. *Journal of the Korea Institute of Information Security & Cryptology*, 22(6), 1219-1230)

[6] K.S. Lee, and H.S. Seo(2010). The Methodology of Access Point Default WEP Key an Alteration. *Journal of Knowledge Information Technology and Systems*, 5(4), 1-8.

[7] S.R. Lee, and Y.J. Park(2004). Design of PKI Cryptosystem enabling Efficient Mutual Authentication on Wireless LAN. *The institute of Electronics Engineers of korea*, 41(3), 69-78.

[8] S.W. Jang, and K.Y. Kim(2013). Detection of Network Attacks Based on an Improved Clustering Algorithm. *Journal of Korean Institute of Information Technology*, 11(3), 141-150.

[9] J.S. Hong, N.O. Park and W.H. Park(2012). Detection System Model of Zombie PC using Live Forensics Techniques. *The Journal of Society for e-Business Studies*, 17(3), 117-128.

[10] J.K. Kook, and H.W. Kim,(2016). Hacking Countermeasures for Wireless Internet Service. *Journal of Service Research And Studies*, 6(3), 79-90.