World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:5, No:11, 2011

Effective Security Method for Wireless LAN using Life-Cycle of Wireless Access Point

Soon-Tai Park, Haeryong Park, Myoung-sun Noh, and Yoo-Jae Won

***Abstract*—**There are many expand of Wi-Fi zones provided mobile careers and usage of wireless access point at home as increase of usage of wireless internet caused by the use of smart phone. This paper shows wireless local area network status, security threats of WLAN and functionality of major wireless access point in Korea. We propose security countermeasures concerned with life cycle of access point from manufacturing to installation, using and finally disposal. There needed to releasing with configured secure at access point. Because, it is most cost effective resolution than stage of installation or other life cycle of access point.

***Keywords*—**Wireless LAN Security, Wi-Fi Security, Wireless Access Point, Product Life-Cycle

I. Introduction

A wireless communication technology was developed from ALOHAnet that is computer communication network using Radio Frequency in 1970. It includes local area communications like as infrared communication. A wireless local area network (WLAN) links two or more devices using some wireless distribution, and usually providing a connection through an access point to the wider Internet [1]. This gives users the mobility to move around within a local coverage area and still be connected to the network. Most modern WLANs are based on IEEE 802.11 standards, marketed under the Wi-Fi brand name [1]. IEEE 802.11 committee published IEEE 802.11n standard in 2009 and worked for standards of concerned with wireless local area network from 1991. Wireless communications using radio waves distinguished wired communications have many advantages like as mobility, easiness of installation and so on. Wireless communication technique uses a variety of ways of communication as FHSS (Frequency-Hopping Spread Spectrum), OFDM (Orthogonal Frequency-Division Multiplexing). The more increasing of usage of wireless LAN, the more security issues are also increased. According to spread of smart phone and tablet PC, it needed to cost effective countermeasures against wireless LAN security threats.

II. Wireless Data Traffic

Mobile traffic usage shows dramatically increasing more than 100% per year in the worldwide and it is similar to increasing of internet traffic in the late 1990s.

Manuscript received Sep 30, 2011. This paper was extended former paper "Effective Security Measure in Private Wireless LAN" was published at JCCI 2011, May, 2011. This work was supported in part by the Korea Communications Commission.

Soon-Tai Park (phone:+82 2 405 5564; fax: +82 2 405 5129; e-mail: cptpark@kisa.or.kr), Haeryong Park (e-mail: hrpark@kisa.or.kr), Myoungsun Noh (e-mail: nmsnms@kisa.or.kr), Yoo-Jae Won(e-mail: yjwon@kisa.or.kr) are with the Korea Internet and Security Agency(KISA), Jungdae-ro 138, Garak-dong, Songpa-gu, Seoul, Korea.

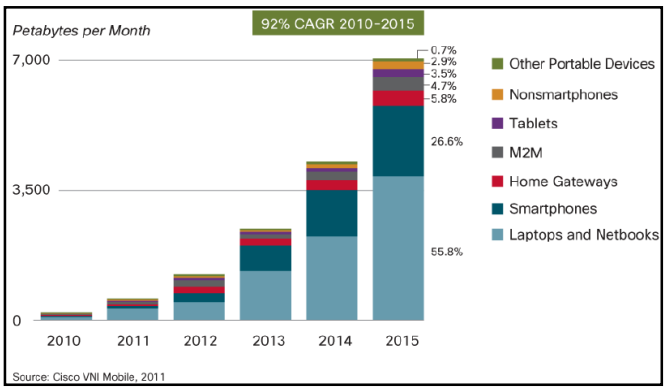

Fig. 1 Wi-Fi zone status in the world

According to CISCO, it is predicted to data traffic more than 7,000 petabyte per month in 2015. These traffics led by mobile terminal like as smart phone, portable computer [2]. There are dramatic increasing of Data traffic caused by launching i-phone by KT at Nov 2009, release of Galaxy S by SKT by Samsung at Jun 2010, Adoption of unlimited payment system for use of data communication by mobile carries in Korea. Table I shows data traffics and smart phone users.

TABLE I
WIRELESS DATA TRAFFIC STATUS & SMARTPHONE USER IN KOREA

section	'09.12	'10.6	'10.12	'11.3	'11.6
Traffic (Terabyte)	389	761	4,345	6,795	10,132
Smartphone user (ten thousand)	81		722		1,487

Increasing of wireless data traffic, mobile carriers conduct of data traffic dispersion like as early commercialization of LTE(Long Term Evolution) or Wibro(it means mobile Wimax), adoption of femtocell called compact radio base station, Wi-Fi zone extension and so on [3]. In case of Wibro and/or LTE needed to high cost burden of construction of radio base station. So, most of mobile carriers prefer to extension of Wi-Fi zone by reason of effective method that needed short period of time and low costs. In addition mobile carriers trying to traffic dispersion with conversion from wireless AP for VoIP wireless telephony to Wi-Fi AP. These results Wi-Fi zone is more than 15,000 at Jun, 2011 in Korea. According to Jiwire, Worldwide Wi-Fi zones are provided more than 570,000 [4].

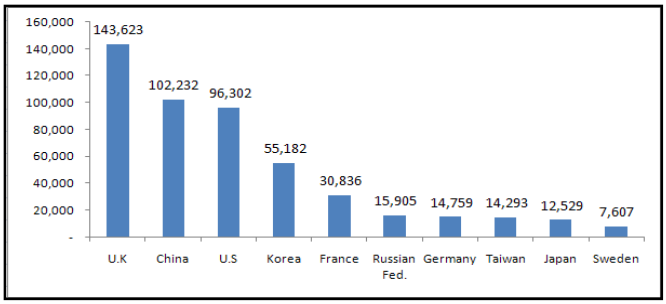

Fig. 2 Wi-Fi zone status in the world

Usage of wireless internet includes mobile internet using mobile networks by mobile phones, Wi-Fi(it means wireless LAN) using wireless access point by wireless terminals like as portable PC or smart phone, ultrahigh speed wireless internet using WCDMA, HSDP and/or Wibro by wireless terminals like as portable PC or smart phone.

TABLE II
WIRELESS INTERNET TYPE

Type	Terminal units	Used Networks
Type 1	Mobile phone (Feature phone)	Mobile communication networks
Type 2	Portable PC, Smart phone	Wi-Fi networks by wireless AP
Type 3	Portable PC, Smart phone	Wibro, WCDMA/HSDPA networks

Usage ratio of wireless internet shows mobile internet (56.6%), Wi-Fi (16.4%), ultrahigh speed wireless internet (3.6%) [5].

III. WLAN CATEGORIZATIONS AND SECURITY THREAT

WLAN (it means Wi-Fi network) can be divided into various environment according to subject of establish, management, using [6]. Generally WLAN can be categorized by provided types like as Commercial WLAN type by mobile carriers, Public WLAN type provided free, Individual WLAN type used in home, Enterprise WLAN type provided by companies. Also, it can be categorized by using environment like as public user or individual user. Table III shows 4 types of WLAN by use perspective and provide perspective [7].

TABLE III
USING ENVIRONMENT CLASSIFICATION

use perspective	provide perspective	provider & user	For example
Public	Commercial	Provided Telco, Many use	olleh WiFi zone, T-WiFi zone, U+Zone
Public	Individual	Provided Individual or Biz, Many user	Wi-Fi by Hotel, Café etc
Private	Commercial	Provided Telco, Individual user	VoIP, Home herb, U+070 etc
Private	Individual	Provided Individual or Biz, Individual user	individual AP installed at home

Wireless LAN security threats are distinguished physical, technical, managerial threat and so on. Physical threats are include separate of cable or power, physical access, injury of Access Point, theft, lost terminal etc. Technical threats are Information Gathering using Radio Frequency Gathering, Information leakage using Rogue AP, Cryptography Crack, an-authorized Access using MAC spoofing, Man In The Middle attack, Wireless Denial of Service attack etc. Managerial threats are an-authorized Access of outsider because of fail of equipments and manage of user, illegal using of WLAN cause of lack of security awareness, permit of internal WLAN access cause of missing of radio wave management and so on. The others are stand of default password of VoIP wireless telephony, spread of malicious code and spam mail using open Wi-Fi, evasion of IP tracing and so on. These threat types needed to countermeasures like as policy and management, security technique include adoption of security solution, security awareness and so on [6].

IV. WIRELESS ACCESS POINT SECURITY CONFIGURATIONS

In Korea, there are more than 540.6 million wireless AP in 2010. The portion of opened AP is 48% and totally opened ratio is 44.8% [8]. AP's secured configuration means include WEP, WPA, WPA2 or authorized by authorization server using IEEE 802.1x authentication. APs at home that's share point is 54.1% are exposed to security threats like as hacking, leakage of privacy data, unauthorized usage etc cause of knowledge of security configuration and/or lack of awareness to security.

TABLE IV
ESTIMATION OF MARKET SHARE OF AP AT HOME IN KOREA

Brand	Sales at Auction	Res.1	Res. 2	after adjustment	market share	accumulated rate
iptime	21,878	5,890	2,716	17,793	59.31%	59.31%
Anygate	578	1,409	519	2,772	9.24%	68.55%
Axler	7,652	20	48	2,066	6.89%	75.44%
Buffalo	5,055	65	54	1,469	4.90%	80.33%
ZIO	411	577	248	1,263	4.21%	84.54%
Unicorn	481	633	175	1,164	3.88%	88.42%
D-Link	870	550	148	1,116	3.72%	92.14%
NEXT	2,079	148	55	802	2.67%	94.82%
Netgear	212	358	131	719	2.40%	97.21%
BELKIN	350	308	111	657	2.19%	99.40%
3COM	15	106	30	180	0.60%	100.00%
Total	39,581	10,064	4,235	30,000		

Table III shows market share of AP at home in Korea. We presumed market share using 3 ways of investigation.

In table IV, second column 'Sales at auction' means the sales result of wireless AP 39,581 in Korean auction at Feb. 2011 and third column 'Res. 1' means the AP counts that top 10 brand security status research in Korea in 2010. Fourth column 'Res. 2' means the AP counts that top 10 brand security status research in Seoul city in Korea in 2011. The criteria of research used SSID like as '*iptime*', '*netgear*'.

Market share order was 'iptime', 'Anygate', 'Axler', 'Buffalo', 'ZIO', and so on. We searched security technology like as WPA2, WPA, hidden SSID, MAC filtering, WPS and guidance in user manual or website at AP manufacturers. Table V shows adopted security technologies, manual guidance in each manufacturer.

TABLE V
PROVIDED SECURITY TECHNOLOGY AND MANUAL GUIDANCE

Classification		iptime	Axler	Buffalo	ZIO
Security Technology	WPA2	□	□	□	□
	WPA	□	○	○	○
	WEP	○	○	○	○
	Hidden SSID	○	○	○	○
	MAC Filtering	○	○	○	○
	WPS	□	□	□	□
Manual	Sec. conf. notifying	X	X	X	X
	Sec. conf. process	○	○	○	○
Home page	Sec. conf. notifying	X	X	X	X
	Sec. conf. process	○	X	○	X
	Etc	○	○	X	X

legend: ○ exist, □ some exist, × not exist

Most of APs adopted security functions like as authentication and encryption using WPA2, hidden SSID, MAC or IP address filtering. Also manufacturers provide security guide in user manual or website.

V. EFFECTIVE SECURITY METHOD FOR WIRELESS AP USING LIFE CYCLE

Wi-Fi zone and AP within VoIP are security enhanced with adoption of 802.11i authentication, I-WLAN technology, PDG (Packet Data Gateway). Also Wi-Fi Alliance certified WPS (Wi-Fi Protection Setup) functionality for easy set up of AP [9]. WPS function uses PIN (Personal Identification Number) and PBC (Push Button Configuration) methods. But, certified APs adopted WPS are very few. The reasons that many users use AP in unsecured states are they have no knowledge of security configuration and complicated control menus. So we suppose to security enhancing to AP used in home environment. Cost effective security enhancing AP is that AP manufactured secured status like as use WPA2 mode, individual password.

As a secure software engineering view point, if we assume the cost that reduce vulnerability at the design phase is 1 than the cost that implementation phase is 6.5 times, test phase is 15 times and using and/or maintenance is more than 60 ~ 100 times[10].

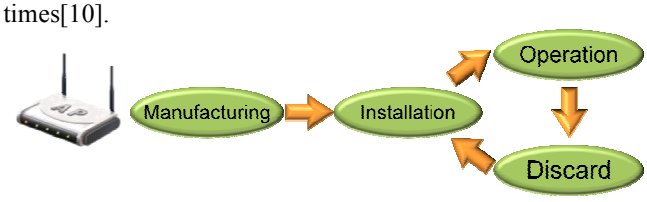

Fig. 3 Lifecycle of wireless AP

Most of hardware or software products have each lifecycle that is ① developments or manufacturing phase, ② installation phase, ③ operation phase, ④ discard phase. Wireless AP is one of hardware product. So, we can apply lifecycle model to AP. All phase of AP's lifecycle need to cost effective security adoption methods as manufacturing AP, WLAN installation, operation or management, discard. Manufacturing phase needed to security enhanced default configuration and user friendly control menu. In case of installation phase, users have to set the security configuration to more safety. Manufacturers have to provide easy firmware upgrade to each AP at operation or management phase. In case of need, they have to campaign of safe usage of AP. Lastly In case of discard phase, Users have to remove sensitive data like as configuration data, personal data.

TABLE VI
THE ROLE OF EACH SUBJECT AT LIFECYCLE OF AP

Subject	manufacturing	Install	Operation & maintenance	discard
Manufacturer	Manufacturing of secured AP	-	-	-
Wi-Fi provider	Requirement of secured AP	Installation with secured configuration	Maintenance of security status of AP	Secure discard
Wi-Fi user	-	-	Secure use	-

Table VI shows role of each subject concerned AP manufacturer, Wi-Fi provider like as telecommunication operator and Wi-Fi user. Each subject have roles at from manufacturing phase to discard phase.

① *Change of order of security configuration menu*

Order of most AP's security configuration menu shows open mode, shared mode, WPA-PSK mode, WPA2-PSK mode, WPA-PSK/WPA2-PSK mixed mode. More security enhanced order is WPA2-PSK mode, WPA-PSK/WPA2-PSK mixed mode, WPA-PSK mode, Shared mode, Open mode. Additionally WEP function has to remove in configuration menu.

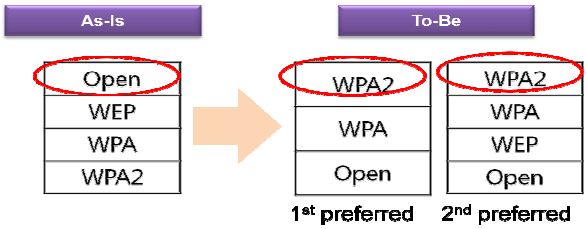

Fig. 4 Change of Configuration Menu

② *Default security configuration and individual password*

The default security mode has to WPA2 by AP manufacturer. The installed password need to individual like as serial number of APs.

③ *Hidden and Changed SSID*

We need to use hidden SSID because unauthorized user do not access to AP. Also, we have to change SSID from original SSID by manufacturer

④ *IP or MAC address filtering*

Most of APs provide functionality of IP or MAC address filtering. Address filtering prohibits unauthorized access using particular IP or MAC address. It need to authorized IP or MAC address.

VI. Conclusion

According to the result of security research concerned WLAN in 2010, 2011 there are more than 290 millions AP and 44.8% of AP was used unsecured configuration. In this paper, authors proposed the method to security enhanced AP that is make secured AP at manufacturing phase in lifecycle of AP. The most effective method is secured AP from manufacturing phase. At this point manufacturer have to consideration of performance of AP using encryption operation that user don't know performance drop of AP. It's maybe tradeoff of between safety and performance. So, we need to research about the relation of between security configuration and performance of traffic communication.

References

[1] http://en.wikipedia.org/wiki/Wireless_LAN
[2] CISCO, "Cisco Visual Networking Indes: Global Mobile Data Traffic Forecast Update, 2010- 2015", Feb. 2011.
[3] http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201012262120025&code=930201
[4] JiWire, "INSIGHTS JiWire Mobile Audience Insights Report Q4 2010", Feb. 2011
[5] Gyenam Lee etc, "Yr 2010, Survey for Behavior of Using Wireless Internet", KISA, Dec 2010.
[6] Soon-Tai Park, Yong-Geun Won, Jong-Hyun Baek, "A Study on Security Threats and Countermeasure for WLAN Environment", The 34th Korea Information Processing Society Fall Conference Proceeding Vol. 17, No. 2, pp. 1350-1353, Nov, 2010.
[7] Jong-Hyun Baek, Soon-Tai Park, "Wi-Fi Security status and Policy Direction in Korea", Review of Korea Institute of Information Security and Cryptology Vol. 21, No. 1, pp. 44-49, Feb, 2011.
[8] KCC, "A Comprehensive Plan for Smart Mobile Security in Korea", KCC, Dec 2010.
[9] Wi-Fi Alliance, "Wi-Fi CERTIFIED Wi-Fi Protected SeteupTM: Easing the User Experience for Home and Small Office Wi-Fi® Networks", Wi-Fi Alliance® Dec, 2010
[10] Kevin Soo Hoo, Andrew W. Sudbury and Andrew R. Jaquith, "Tangible ROI through Secure Software Engineering", Secure Business Quarterly: Defining the Value of Strategic Security, 4th Quarter, 2001