A Study on Client-based Authentication and Access Control of Wireless Access Point

Jong Kyung Baek[1] and Jae Pyo Park[2]

[1] *Ph. D. Course of Computer Science, Soongsil University*
[2] *Graduate School of Information Science, Soongsil University*
{jkbaek[1], pjerry[2]}@ssu.ac.kr

Abstract

As wireless technology widely spreads and invites its development with changes in wireless network system which supports rapid transmission, defects in security are, however, constantly witnessed. As a result, these problems have called for the needs to strengthen the hole in the technology. Though it seems that security issues between wireless communication are solved with the adoption of IEEE 802.11i as a standard, numerous attacks targeted for vulnerability of wireless mobile are increasing these days.

When accesses to wireless AP from server-based, or client-based authentication, either of them determines an authorization status for use. A number of measures to prevent external attacks or information leakages are presented through the use of authorized wireless AP. Still, both server-based and client-based authentication have not only low confidentiality to external network but low solubility to a wireless AP packet which is unauthorized.

In this paper, we use MAC Address to get authentication from an AP. It searches the NDIS Intermediate Driver from the wireless network card, and then controls the packets after operating the scope of IP and PORT. After having implemented the proposed model here, we came to conclusion that it is possible to solve the drawbacks of server-based authentication in security and cost. Also it showed that the proposed model enhances solubility and scalability of client-based authentication.

Keywords: *Wireless Authentication, Access Control, Network Driver, MAC Address, Access Point*

1. Introduction

These days, Smartphone, WiBro (Wireless Broadband), HSDPA (High Speed Downlink Packet Access), and other wireless technologies are being developed and widely used. Because of this development, the number of attacks on wireless device vulnerability continues to grow. As a result, there are a number of cases reported about the inside information spills to the outside of the source which are caused by wireless AP mobility and scalability. There are proposals such as server-based control against wireless AP attack, wireless sensor-used control, and client side control, etc. But all of them have vulnerability issues in security and less availability in the external network. In this paper, we propose that client determine authorized/unauthorized AP by authenticating wireless AP. And we strengthen the security by controlling the unauthorized AP packets. We augment availability by using the part of IP and PORT.

In Chapter 2 we are going to cover network driver, weak point of wireless AP, and wireless authentication. Chapter 3 is about wireless authentication through proposed model in the paper, and counter measurement. In Chapter 4 there are analysis and comparison of proposed

model with the previous one leading to the result on its effectives. Last, there is conclusion in Chapter 5.

2. Wireless Access Point Control

2.1 NDIS Intermediate Driver

NDIS(Network Driver Interface Specification) Intermediate Driver is a component which is included in NDIS version 4.0, and it is placed on between transport driver and NDIS NIC(Network Interface Card) mini port. It is NDIS Intermediate Driver that seems like transport driver to NIC driver, whereas NDIS miniport to transport driver.

NDIS Intermediate Layer is useful when try to connect to transport driver or any new type of media, and it performs conversion and transmission, all of which are needed between transport driver and NIC miniport that manages new type of media.

Figure 1 is about 2 organizations of NDIS Intermediate Driver.

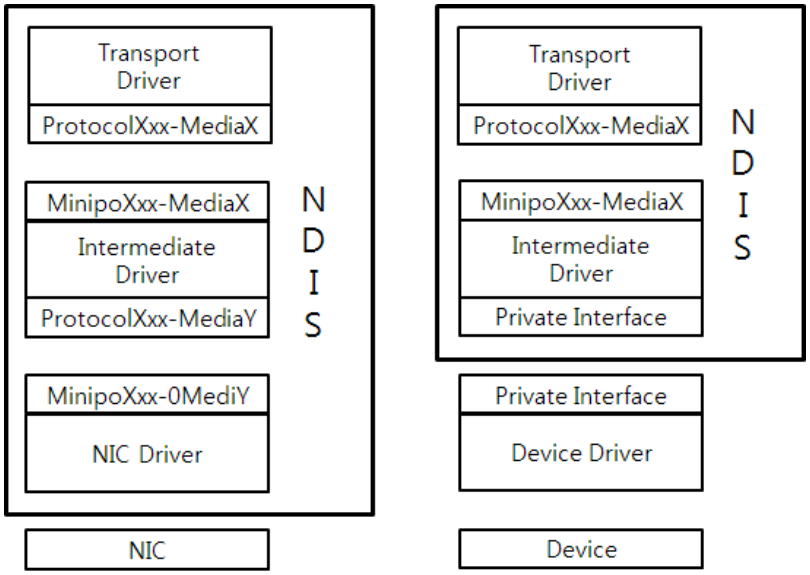

Figure 1. NDIS Intermediate Driver Layer

NDIS intermediate driver usually sends MiniportXxx Function from its upper edge, and the Protocol from lower edge. Another case is, though not generally, the default is able to send a separate interface that intermediate driver utilizes MiniportXxx functions on the upper, and non-NDIS driver on the lower edge. Of an Intermediate driver, it is typically layered below transport driver which supports TDI on the upper edge and more than of NDIS NAC driver. However, Intermediate driver cannot be 'Layer A' above or below of other Intermediate driver theoretically [13].

2.2 Wireless AP Security

IEEE 802.11b, which is wireless AP standard, provides authentication and confidentiality and it is composed of SSID and WEP. SSID is the name of wireless AP network and is possible to be renamed. When user requests a connection to SSID, authentication on wireless

AP will be processed. However, any access to SSID and authentication are available for anyone who wants to approach them without any control, so it causes vulnerability in security.

Stream encryption of telecommunication packet is performed by WEP so that IEEE 802.11b may enhance security of data communications between a user and a wireless AP. The received packets are descrambled at wireless APs, and then authenticate terminal equipments.

The IEEE 802.11b standard provides two ways - open authentication system and public key authentication. Open authentication is the way which the entire authentication process is performed in plain text and the terminal is able to have access to AP without having WEP key.

Public key authentication system sends terminals packets which attempt to authenticate wireless AP, and the terminals are encrypted, transmitted to the wireless AP [1].

Data confidentiality is provided using the WEP. The terminal and the wireless AP share a 40-bit encryption key within WEP algorithm, and the wireless AP sends a random challenge to authenticate the terminal. The terminal combines a 40-bit encryption key and a 24-bit of IV together, then it encrypts and transmits the plain text after creating a random key stream by using RC4 PRNG (Pseudo Random Number Generator) [1].

The received packets are descrambled at wireless APs, and then authenticate terminal equipments. When a user accesses to a wireless AP, only a user who has the correct WEP key is allowed to access to network by comparing the conventional set WEP key with the access-requested WEP key. Compared to the way of SSID connection, it is higher in authentication and security [10].

However, when the virtual wireless AP is created by the user with deliberate intentions, especially if it is requested for authentication by the insider, the information of WEP key would be exposed. In this case, there are high probability that a malicious user would access the internal wireless AP and attack the internal network by using the intercepted WEP key information.

2.3 The Vulnerability of Wireless AP in Security

2.3.1 The Vulnerability by Rogue AP: Rogue AP is a wireless AP that is not allowed for security authentication though connected to the internal network. Rogue AP could jeopardize the security of cable infrastructures by detouring defense wall and VPN frame. For the hackers, who are closely watching at the wireless environments of corporations with the intention of the information leakage, the networks of any corporations can be exposed.

2.3.2 Probing Station: Probing Station sends probing signals containing any connected SSID informations in the past. It refers to a device such as a malicious user, a laptop that can connect to the external wireless AP. It has vulnerability in security because there is a high possibility of connecting a malicious user to the internal cable network without any control.

2.3.3 Ad-Hoc Network: Ad-Hoc network is an autonomous structure network. Without an AP, scattered nodes can communicate wirelessly with each other. Since there are not the nodes for controls in the middle, each node has to communicate on the network while utilizing the informations they can collect at their best, and in the case of communication with distant node, it takes place via other nodes. Ad-Hoc network communication leads to a significant risk of network security. A laptop with the activated Ad-Hoc network, which is Peer to Peer Communication, may be subject to an easy hacking target, and it potentially can be a good path for attackers that are eager to be connected to the internal network.

2.3.4 External Wireless AP: External Wireless AP is referred to wireless AP used by the neighboring offices or homes as opposed to wireless AP for the use of the internal network. These wireless APs cannot be a threat to the internal network by themselves, but there are always security weaknesses that are possibly combined with wireless AP within the internal network.

If the inside PC connect to this wireless AP, then it plays its role as a connection with another company's network. Furthermore, If the neighboring wireless AP is not assorted in advance, it would cause difficulty for a manager to detect a hacker accurately.

There would be a great difficulty for the internal stations to prevent phishing attacks throughout the Evil-twin if management of the neighboring wireless AP is ignored.

2.4 Wireless Access Point Control

The countermeasure to control wireless packet is mostly divided into server-based control and client-based control.

Figure 2 is a diagram of server-based wireless AP control.

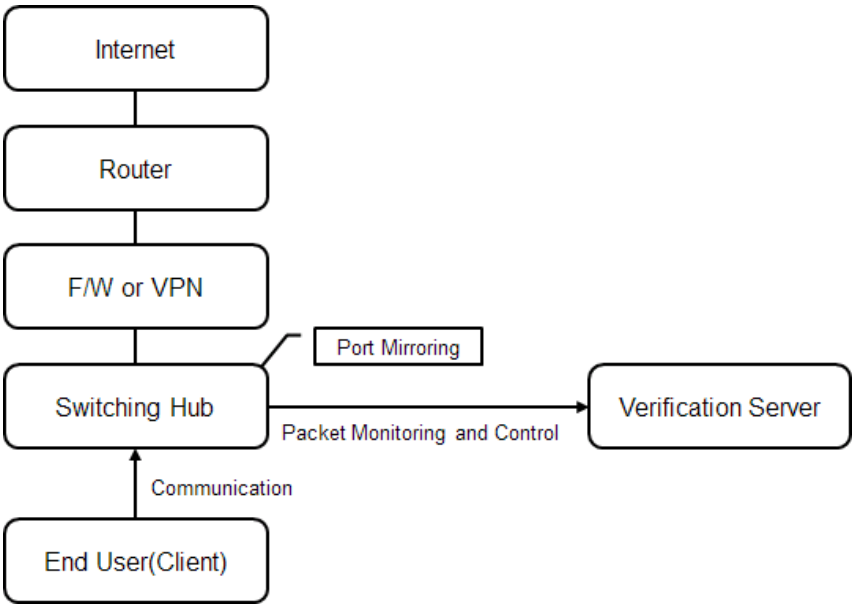

Figure 2. Sever-based Wireless Access Point Control

Server-based wireless AP control method has an authentication server, and the server is monitoring packets and checking on them if those are wireless packets which go externally out of the internal network.

Wireless AP is not controllable in the external network, but in the internal network, and it is hard to control when an authorized person takes a laptop out outside and he/she sends the information to the wireless AP. The additional devices are needed to monitor packets, therefore server-based control is expensive than client-based. The control method with devices controls a wireless AP by placing sensors in controlling areas. 500 AP's can be controlled as per each sensor and each of them is able to have multiple defenses against about 20 wireless threats at the same time. Since the sensors are placed in each area, the problems are easily traceable. It is very vulnerable, however, when the sensor goes out of the range or

the inside information is transferred by an authorized person with a laptop from the external area. So that the need of more sensors arises, it causes additional costs.

Client-based control is needed to supplement the limitation and the cost. When client tries to get access to wireless AP, it determines the status of authorization on AP and controls them, collecting MAC Address of wireless AP. However, it is only able to allow permission/blockage on wireless AP, it causes less availability.

Though unauthorized wireless AP, it needs a countermeasure to enhancing availability within the range of which is not violated. Since it is also the client-based, there will be vulnerability issues in security threatened by malicious codes, hacking tools and reversing tools.

3. Wireless Access Point Authentication and Control Method

3.1. Security Model Configuration and Definition

If there are an authorized wireless AP, an internal unauthorized wireless AP and an external illegal wireless AP, the configuration diagram of control is as follows figure 3.

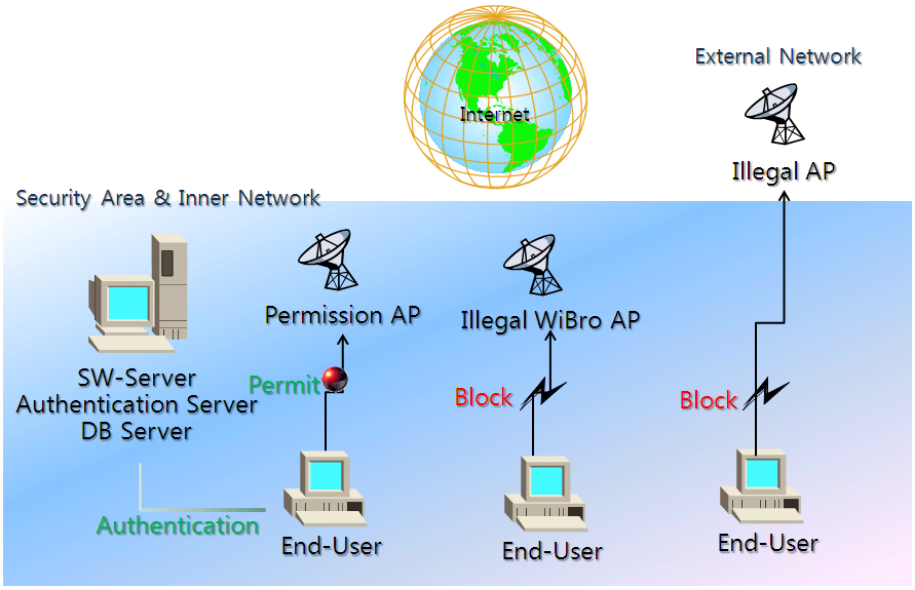

Figure 3. The Proposed Model Configuration

The authentication system structure on wireless AP manages an authorized wireless AP list from server, and it approves, or rejects requested wireless AP. It is the way that client only approves the access of authorized wireless AP, and it controls the packet of unauthorized wireless AP. It is to prevent dysfunctional monitoring caused by different IP bandwidth when the inside information is spilled with the use of IP bandwidth from the external network, not from the internal network. In this paper, we have configured a security model to authenticate and control wireless AP. The model is shown as follows in Figure 4.

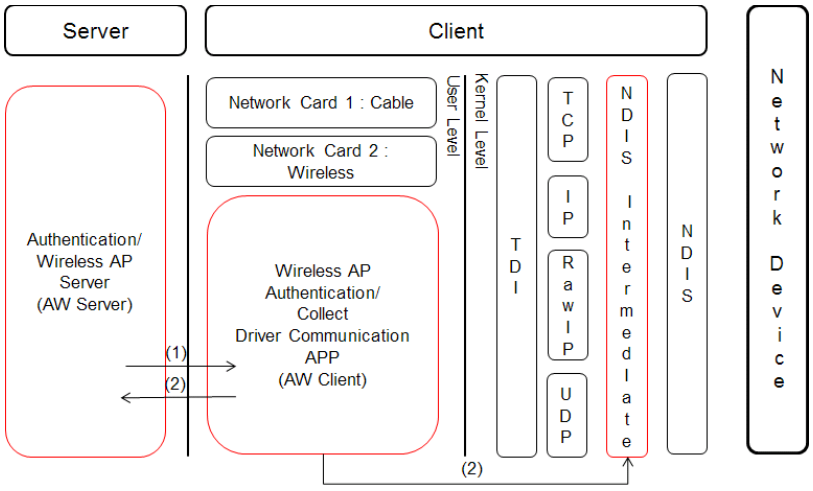

Figure 4. Proposed Wireless Access Point Authentication Model

There are three different modules such as server (AW-Server), Client User-Lever (AW-Client), Client Kernel-Level (NDIS Intermediate Driver).

Network transmitting packet goes out like User-Level Client, TDI Layer, NDIS Layer, network device in this order.

AW-Server receives requested wireless authenticating AP information and sends only authorized AP information to AW-Client. AW-Client receives authorized wireless AP list from AW-Server, after that client decides if the AP is authorized when it accesses wireless AP. It controls network packets by the policy after receiving unauthorized wireless AP driver name.

3.2. Wireless Access Point Authorization Process in Server

Authorization process of the requested wireless AP from AW-Client is as in the following Figure 5.

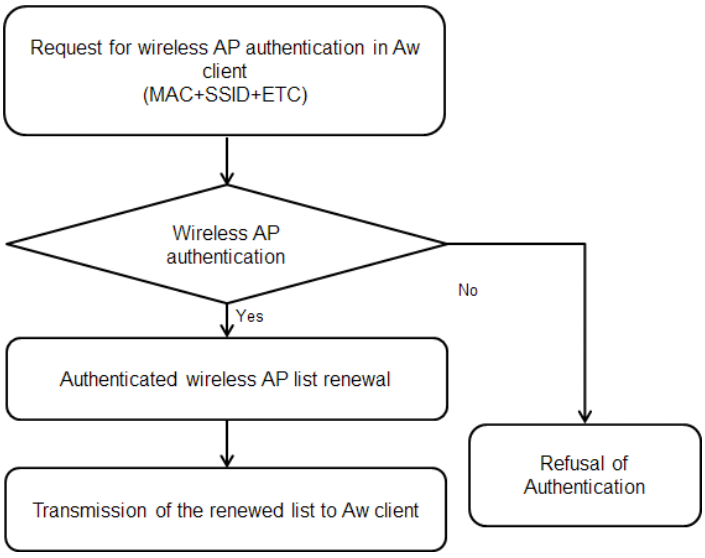

Figure 5. Wireless Access Point Authorization Process in Server

After checking the authorized list from AW-Client, it authorizes a wireless AP which is the internal network. Then, a result of the process is directed to the list, and transferred to AW-Client. The client updates the list as soon as it receives, and it deletes a wireless AP that is not authorized.

3.3. Wireless AP Authentication Process in Client

The process to control an unauthorized wireless AP is as follows in Figure 6.

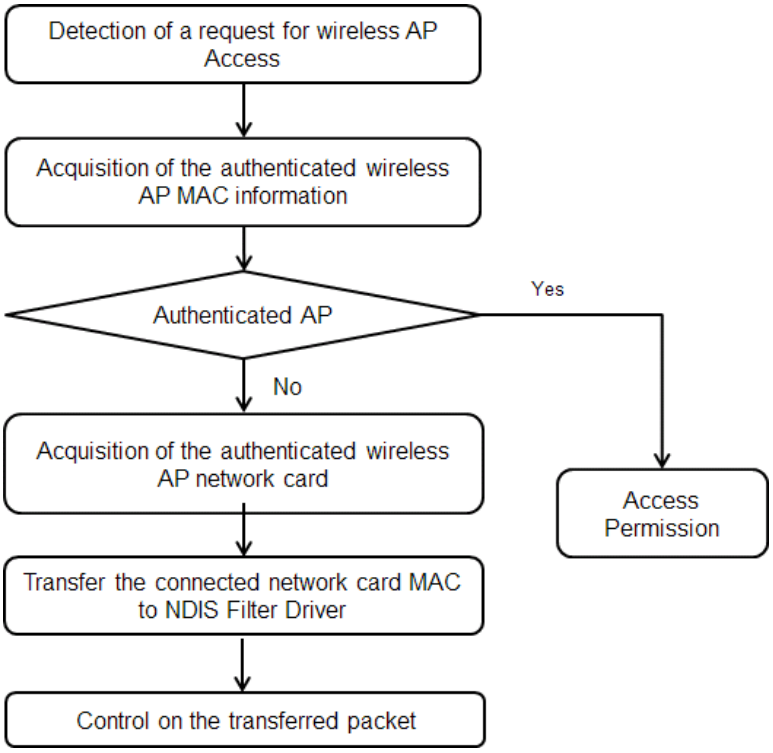

Figure 6. Wireless AP Authentication Process in Client

When SW-Client is initiating, it receives the authorized wireless AP information, and stores it in the memory. If SW-Client monitors wireless AP access and detects an access request, it checks on the network card and finds a connected network card. It requests MAC Address from the related wireless network card, and decides if it is authorized wireless AP. In the case of unauthorized wireless AP, if SW-Client finds the name of a device by searching network card, it sends MAC Address of the network card to NDIS Intermediate Driver, using the device name. When NDIS Intermediate Drive is sending a data, if it is MAC Address of unauthorized network card, it controls the network packet by unauthorized policy.

3.4 Policy of AW-Client

AW-Client based on the value of the policies and actions, policies, values are shown in Table 1.

Table 1. Policy of AW-Client

Section	Key	Note
CERTIFICATION	Count	The number of authorized wireless AP
	mac%	The number of authorized MAC Address
	ssid%	SSID of authorized wireless AP
CFG	gzwr_poli	Policy 0 : Permit 1 : Block 2 : Authentication
	mode	100 : MAC based Authentication 101 : SSID based Authentication
	logpath	Log Path

The policy of AW-Client consists of two sections in total. 'CERTIFICATION' is the section of authentication, and 'CFG' is the section of the setting. 'Count' refers to the number of authorized wireless AP, the equivalent numbers of wireless AP can be certified. Authentication method is determined by `mode` key, and in the case of MAC-based authentication, the `CERTIFICATION` section of the `mac%` authentication is done by referring the value of a key, SSID-based case of a witness `ssid%` key is the value of the reference. 'logpath' key is the route to store the information wireless AP connection, and the stored logs are transmitted to SW-Server.

3.5. NDIS Intermediate Driver Packet Control Policy

The control scope of unauthorized wireless AP is calculating the value of the OR and AND operations with each policy IP and PORT scope.

If it blocks unauthorized wireless AP unconditionally, the availability drops, so that it increases the availability by permitting a part of unauthorized wireless AP, and it decides the policy to maintain the security.

This is an example of the control policy operation as follows:

|192.168.1.225-192.168.1.225|21-21|&

|0.0.0.0-255.255.255.255|80-80|

We enabled unauthorized wireless AP to utilize FTP Server of the internal network (192.168.1.225, 21 PORT) and the internet (80 PORT).

In the first of the operation, possible IP scope is within it and PORT scope in the second operation as well.

Next condition will be determined in the third operation, and if there is any next decision, then the control scope is determined after AND operation.

The scope of the first IP and the second PORT set their control scopes after OR operation.

In the case of network communication with unauthorized wireless AP, a control process with policy is as in the following Figure 7.

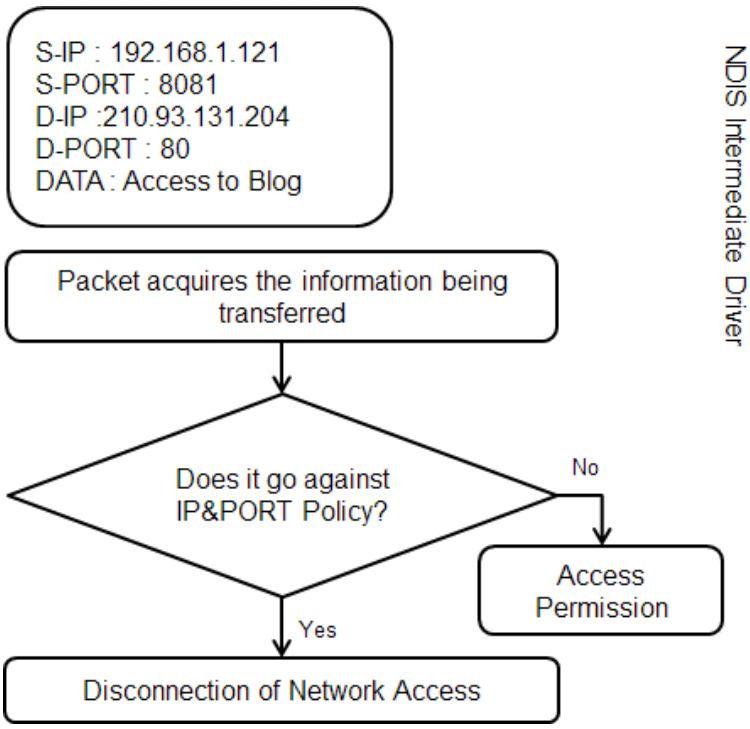

Figure 7. Wireless AP Authentication Process

When sending a packet, NDIS Intermediate Driver detects a packet, and blocks a packet if it is against the policy by scanning IP and PORT, in other case, it allows enhancing the availability through the permission.

4. Implementation and Performance Analysis

4.1. Implementation Environment and Method

The test environment is configured as Table 2 below. Except wireless AP devices, we have added the test item; a smart phone which is converted into AP mobile equipment, using WiBro and tethering technology.

Table 2. Test Environment

Detail	O/S	Language	Note
Server	Windows 2008 R2	C/C++/JSP	MS-SQL 2008
Client	Windows 2000NT ~ Windows 7 (x86/x64)	C/C++/ Assembly/Kernel C	DWA-140/Dell Wireless 1520 Wireless-N WLAN Mini-Card
Wireless AP	-	-	DWL-3200AP
Smart Phone	I-OS/ Android	-	I-Phone 4/ Galaxy-S
WiBro	-	-	DM-MR100

Client side shows a requested list for wireless AP authentication, and we configured the WEB (JSP) in order to authenticate the requested wireless AP previously. Authenticated wireless AP is stored in a file and DB (MS-SQL 2008), and the stored information is transferred to AW-Client.

We have used C/C++ language to configure the AP authentication process in AW-Client, and Assembly/Kernel C language was used to control unauthorized wireless AP. Smart phone and WiBro device were used as connecting devices which can convert wireless AP into AP devices. After implementing DB and WEB server in the server, we have set unauthorized wireless AP control policy. The policy reflects the usage, the description, and the scope of IP & PORT, used time, used date all of which are set by manager.

We needed to set wireless AP on adjacent test client pc, but make sure to set more than 2 of them due to the identification of their authorized status.

If the policy is established, we need to install SW-Client for client.

Wireless authentication registration and unauthorized wireless AP scenario are as follows:

① Install more than 1 of wireless LAN card in client.

② Request wireless AP authentication to SW-Server.

③ Bring the possible connecting list and signal through wireless LAN card when AW-Client is searching wireless AP. Then, select the wireless LAN on the list, and request a registration from the server.

④ The requested wireless AP from the server is able to verify on the web page as;

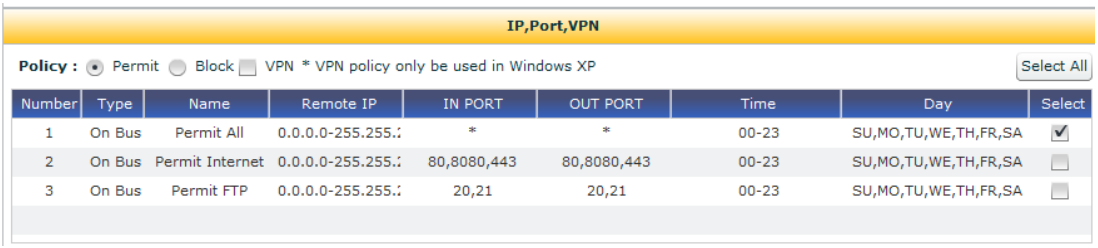

Figure 8. Wireless Access Point Registration in Server

If manager considers it as an inappropriate wireless AP, he/she deletes the relevant list, and rejects authentication request. When approves authentication, manager clicks the box and reflects the policy.

⑤ Client tries to access wireless AP, and unauthorized wireless AP is controlled by policy. If blocked wireless AP is normal, it is requested to AW-Client for authentication and the use. If it is not, however, manager can modify the control policy on unauthorized wireless AP, and leads to use different IPs and PORTs throughout the modification.

4.2 The Implementation Result and Performance Evaluation

We have checked if both authorized wireless AP and unauthorized wireless AP are controlled by AW-Client. As soon as the AW-Client module operates, it brings the OS version and the list of wireless AP.

Figure 10 is a log in the event that the proposed module is executed and a wireless AP is connected.

```
gzwr_LoadWlanapi, Wlanapi.dll Load Complet!!
gzwr_Init, g_szcfgpath(C:₩gzwrcfg.ini)
gzwr_Control, Major:5, Minor:1, Service Pack 3
gzwr_Control, init fail
gzwr_Control, Policy Start
gzwr_WLanXPThread, g_apcfg.dwWaitTime(0)(0)
gzwr_WLanXPThread, g_apcfg.dwWaitTime(-1)(0)
gzwr_Control, Count(8)
gzwr_Control, gzwr_poli(2)
gzwr_Control, waittime(3000)
gzwr_Control, mode(101)
gzwr_Control, ssid1:KAir3
gzwr_Control, ssid2:KAir4
gzwr_Control, ssid3:KAir5
gzwr_Control, ssid4:KAir6
gzwr_Control, ssid5:KAir7
gzwr_Control, ssid6:KAir8
gzwr_Control, ssid7:KAir9
gzwr_Control, ssid8:KAir2
index(0), keyname(SOFTWARE₩Microsoft₩Windows NT₩Cu
gzwr_Send2NdisDriver, Index= 1 Name= {59C5051F-1635-4D9
gzwr_Send2NdisDriver, IOCTL_NDIS_QUERY_GLOBAL_STATS
gzwr_Send2NdisDriver, OID_802_11_SSID ok (KAir3)
gzwr_Send2NdisDriver, g_lpcfgCertiV[L].cfgCertiV(KAir3)
gzwr_Send2NdisDriver, PASS SSID(KAir3)
```

Figure 9. Log of AW-Client

The proposed model has two kinds of operation modes – MAC-based authentication method and SSID-based authentication method of a wireless AP. The above log is a log in the

event of SSID-based authentication. In case of running AW-Client, bring authorized wireless AP list, operation modes and monitoring cycle from setup file, and start to monitor wireless AP access.

If the wireless AP is connected, it performs the authentication process after collecting wireless network card.

If the wireless AP is connected, it compares the wireless AP with authenticated list. And it blocks unauthorized wireless AP and informs the user by alert window if it is not on the list.

There are control methods for identified wireless AP; the one is to block a relevant frequency, using the electronic jamming devices in the server, and another is to place authentication server in NAC level.

In client side, there is control method for wireless AP by installing a program to user PC.

We have compared securing method in the server and controlling method by using a proposed model in Table 3.

Table 3. Comparison of Server-based Control Method and Proposed Model

Detail	frequency based	NAC based	proposed model
control method	frequency	NAC	Client control
scope limitation	high	high	none
external network leakage prevention	normal	low	high
scalability	low	low	high
cost	high	low	low

Because frequency-based scope is within the range of jamming signals, and NAC-based is in the internal network range, user cannot control a wireless AP when he/she is out of the range with a laptop. However, it is possible to control external network packets at the outside because the proposed model is able to control it in client level. Therefore, frequency-based control and NAC-based control have strong vulnerability in security toward the external networks. With their limited scope of frequency-base and NAC-based control, scalability is very low. There will be incurred expanse by installing the devices additionally. As the proposed model controls the program, it does not require extra expanse for the devices.

In table 3, server-based control is very vulnerable in the outside, so client-based control is chosen.

We have compared client control method and the proposed model in Table 4.

Table 4. Comparison of Client-based Control Method and Proposed Model

Detail	client based	proposed model
confidentiality	high	high
availability	low	high
scalability	low	high
program security	low	high

Between client-based and proposed model show high confidentiality, but it also showed many differences in availability, scalability and program security part.

The client-based shows high security strength on unauthorized wireless AP by controlling permit/block, but it cannot control every each packet.

However, security model is able to use the internet and FTP while maintaining the security strength by settings of manager, and to monitor on used logs after saving them.

In scalability, client-based only blocks, it cannot expand more but proposed model is more flexible in expanding additional functions such as mail, messenger, Web hard, etc.

Because the proposed model only allows authentication in User-Level, and controls in Kernel-Level, it does not get attacked by debugs.

A proposed model does not have limitation on the place compared with frequency-based and NAC-based control, data can be secured in the external network, and it is cost-effective. Moreover, the availability is higher than client-based model, and it is also higher in the scalability and has strong security in the program.

5. Conclusion

In wireless AP authentication, the existing methods have security weaknesses and low availabilities about the limited scope. Therefore, in this paper, we proposed client-based model which allows authentication of the external network, and wireless AP that is out of range. All these are the weakness of server-based authentication. And also, we have installed network driver of Kernel-Level to increase availability by controlling packets, instead of permit/block method on unauthorized wireless AP.

Proposed model can have various polices depending on the packet algorithm, and it can have high scalability by users` having different policies.

As wireless-based services have continuously developed, various types of attacks that capitalize on this development have increased in large. We should control the wireless packets and defend various attacks and information spillage by the eclectic use of server-based authentication and client-based authentication method.

References

[1] J. H. Lee, M. S. Lee and J. H. Ryou, “Implementation of a Secure Wireless LAN System using AP Authentication and Dynamic Key Exchange”, Korea Information Processing Society, vol. 11-C, no. 4, **(2004)**, pp. 497-508.

[2] J. H. Kwo and J. T. Park, “User Pre-Authentication Method for Support of Fast Mobility in IEEE 802.11 Wireless LAN”, The Institute of Electronics of Korea, vol. 44, no. 11, **(2007)**, pp. 191-200.

[3] M. H. Kim, J. W. Lee, Y. G. Choe and S. J. Kim, "DoS-Resistance Authentication Protocol for Wireless LAN", Korea Institute of Information Security, vol. 14, no. 5, **(2004),** pp. 3-10.
[4] Y. M. Go and K. H. Kwon, "Detecting and Isolating a Cloned Access Point IEEE 802.11", The Korea Contents Association, vol. 10, no. 5, **(2010),** pp. 45-51.
[5] C. L. Song and B. H. Jung, "Wireless LAN Security Mechanism, Korean institute of Information Scientists and Engineers, vol. 20, no. 4, **(2002)**, pp. 5-13.
[6] S. C. Im, "A Study of Hand-off Scheme Using Mutual Authentication between APs in Wireless LAN Environments", Korean Institute of Information Technology, vol. 8, no. 9, **(2010),** pp. 95-101.
[7] D. W. Lee, "IP-Paging base Resource Management and Task Migration in Mobile Grid Environments", International Journal of Grid and Distributed Computing, vol. 3, no. 3, **(2010)**, pp. 29-40.
[8] E. Hooper, "An Efficient and Intelligent Intrusion Detection and Response System using Virtual Private Networks", Firewalls and Packet Filters, International Journal of Security and Its Applications, vol. 1, no 1, **(2007)**, pp. 15-23.
[9] J. S. Hong, J. W Kim and J. H. Cho, "The Trend of the Security Research for the Insider Cyber Threat", International Journal of Security and Its Applications, vol. 4, no. 3, **(2011)**, pp. 55-63.
[10] ANSI/IEEE Std 802.11: Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specification, **(1999)**.
[11] IEEE Standard for Port Based Network Access control, IEEE Draft P802.1X/Dll, **(1998)**.
[12] IEEE Standard 802.11i, Medium Access Control(MAC) Security Enhancements, Amendment 6 to IEEE Standard for Information technology - Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) specifications, IEEE **(2004)**.
[13] Industrial Network Team, "Windows Device Driver Programming", SamYangBook, Korea, **(2000)**, pp. 571-578.

Authors

Jong Kyung Baek[1]

2010. 2. : Soongsil University Graduate School of Information Science Department of Information Security (Master of Engineering)

2011. 3. ~ present : Soongsil University Graduate School Department of Computer Science (Ph. D. Course)

< Significant area of interest >

Information Security, Information Network, Cryptography.

Jae Pyo Park [2]

1998. 8. : Soongsil University Graduate School Department of Computer Science (Master of Engineering)

2004. 8. : Soongsil University Graduate School Department of Computer Science (Doctor of Engineering)

2008. 9. ~ 2009. 8. : Soongsil University Institute of Information and Media Technology Full-time researcher

2010. 3. ~ present : Soongsil University Graduate School of Information Science Professor

< Significant area of interest >

Information Security, Information Network, Digital Forensics, Cryptography.