Appl. Math. Inf. Sci. 6 No. 1S pp. 209S-220S (2012)

Applied Mathematics & Information Sciences
An International Journal

@ 2012 NSP
Natural Sciences Publishing Cor.

A Study on Security Management Service System for Wireless Network Environment

Daeseob Lee[1] and Dongho Won[1*1]
[1]School of Information and Communication Engineering, Sungkyunkwan University, Suwon, Korea
Email Address: dhwon@security.re.kr

Received: Received May 02, 2011; Revised July 25, 2011; Accepted September 12, 2011
Published online: 1 January 2012

Abstract: Cyber attacks against public communications networks are getting more complicated and varied. Sometimes, one country could make systematic attacks at a national level against another country to steal its confidential information and intellectual property. Therefore, the issue of cyber attacks is now regarded as a new major threat to national security. Moreover, with the rapid growth of smart phone, the interest on the security management service system for wireless network has increased significantly. The conventional way of operating individual information security systems such as IDS and IPS may not be sufficient to cope with those attacks committed by highly-motivated attackers with significant resources. Therefore, we require the security management services system which provides attack detection, analysis and response on a real-time. In this paper, we provide major threats to the wireless network and how the responses to these threats are made. Moreover, we suggest an improved security management service system for wireless network environment.

Keywords: Security management service system, Wireless network, Monitoring, Smart phone

1 Introduction

Recently, along with the popularization of wireless mobile devices such as smart phones or tablet PC's, the cases connecting to wireless network using these devices are increasing. Currently, the wireless mobile communication devices usually connect to the network using 3G or 4G (LTE: Long-Term Evolution) network provided by mobile carriers to be connected using Wireless LAN at the Wireless AP(Access Point) installed by mobile carrier or individual. While the wireless network was restrictively used at department stores, some laboratories and corporate environment with frequent change of inner structure, the demand on wireless network became increased from the appearance of smart phones and tablet PC's. Accordingly, the mobile carriers are currently expanding wireless network environment based on schools and public institutions in order to promote an uninterrupted use of wireless network and prevent the overload of data network. Thus, various problems that did not occur in the existing wired network are being created as the wireless network environment and wireless devices are widely spread. In other words, the leak of important internal network information to the outside could be blocked effectively because client-server, server-server and client-client were connected through wired network under existing wired network environment. However, the possibility of leaking important confidential information to the outside became higher because the mobile communication device can be connected to external network through 3G

[1] **Corresponding Author: Dongho Won, dhwon@security.re.kr**

data network or wireless network under wireless network environment.

Therefore, the necessity of security management service system on wireless network as well as the existing wired network environment became greater. In order to cope effectively with security threats from the activation of wireless network, it is important to set up a security service management system detecting, analyzing and coping with the leak of important internal data and cyber attacks real-time. Therefore, this paper analyze security threats on the communication environments that include wireless network to examine a security management service system for effective and systematic performance of security management service systems under such environment.

The organization of this paper is as follows; In Section 2, we analyze the security requirements for security management service system. Section 3, we describe the security threat on wireless network environment. Then, we provide the state-of-the-art of security management service system in Section 4. In Section 5, we describe the problems of security management service system. We suggest the wireless network security management service system framework in Section 6. Finally, we conclude the research in Section 7.

2 Security Requirements for Security Management Service System

Smart phones are providing internet calls, e-mail, mobile games and data communication, etc in addition to the cellular phone function that was provided by existing feature phones. Accordingly, various services for smart phones are being created and the wireless traffic usage is also getting increased. Thus, the amount of data traffic estimated by mobile carriers is being exceeded along with the rapid increase of mobile data usage. Therefore, various problems such as data communication not operating well in densely populated areas even during ordinary times are being raised.

The mobile carriers ended up forming a wireless network environment using wireless LAN technology as a plan to accommodate it became difficult to accommodate the rapidly increasing mobile traffic just with mobile communication network. The wireless LAN does not require payment of spectrum fees or transmission permits because the public frequency band is used while having characteristics of being appropriate for short-term installation because the price of wireless AP is inexpensive. Moreover, at the position of users, there is an advantage of being able to use the service with faster speed and inexpensive rates than the existing mobile communication network. Due to such advantage of wireless LAN, the competitive spread of wireless LAN by mobile carriers took place with competition since first half of 2010 and about 70,000 Wi-Fi zones are set up to be operated in our country as the result [1]. Meanwhile, the cases of installing wireless LAN even at homes is increasing due to the sale of inexpensive wireless routers along with extended spreading of internet phones provided with a wireless router. Moreover, the environment for convenient use of wireless LAN is formed throughout the country such as expanding the wireless LAN access facilities in order to provide convenience for customers even at public facilities including banks, hotels, restaurants and airports.

The used environment of wireless LAN can be mainly classified into commercial wireless network, home wireless network and corporate wireless network. A commercial wireless LAN is a wireless network area installed by mobile carrier to be used after performing device authentication through USIM (Universal subscriber identity module), MAC (Media Access Control) or ID/password. While home wireless LAN environment has many cases of being installed by purchasing an AP at random by an individual, an unauthorized access is possible because there are many cases of using the initial settings as it is in general and carries the problem that the leak of information may occur through the wireless device using the corresponding AP. Finally, the corporate wireless network is a wireless LAN environment set up for improving work efficiency within the company and the cases of building up this network is increasing as the introduction of smart office and smart work is being spread recently. If wireless connection to corporate network is possible, it carries a problem that the possibility of accessing by detouring security devices of wired network because a systematic management on contact point and accessing devices is not easy unlike the existing wired network. In this paper, a method for making more efficient and systematic security management service system possible will be researched by blocking the leak of important information from government • public institutions or within companies and relating with the existing wired network. Therefore, the details will be described focused on wireless LAN environment of public institution and corporations.

Many corporate enterprises and government organizations are taking advantage of the productivity-boosting and cost-saving benefits of 802.11 wireless LANs. However, in today's growing concern over cyber terrorism, some government organizations can be critical of using wireless LANs because of vulnerabilities. Therefore, many companies are trying to work with government and public safety organizations to secure and optimize wireless LANs by:

- Identifying security risks, such as rogue access points and unencrypted traffic
- Monitoring the network in real-time to identify impending threats, such as unknown stations scanning the network and the use of network probing tools
- Detecting and preventing intruders by quickly identifying attacks and eliminating the threats
- Enforcing corporate WLAN policy to maximize security and performance and providing fault diagnostics and performance monitoring to aid network management

Federal, state, and local agencies are relied on for critical public services and are also looking for ways to improve services as well as increase security of both people and assets. A reliable network allows government agencies to extend mobile enterprise tools to government workers and improves workflow efficiency. The suite of wireless network solutions ensure that when vital operations are at stake, wireless agility enables successful outcomes.

The Department of Defense issued a wireless directive, Number 8100.2 on April 14, 2004. This directive establishes policy and assigns responsibilities for the use of commercial wireless devices, services, and technologies in the DoD Global Information Grid. Recognizing the security threats that unsecured wireless networks pose to interconnected systems, the Directive spells out policies for deploying secure wireless networks, and requires monitoring of those wireless networks for compliance. To ensure the requirements of Directive 8100.2, we require the intrusion detection, and auditing to maintain network compliance with DoD policy. The Department of Defense (DoD) Directive Number 8100.2 was issued on April 14, 2004. The Directive covers the use of commercial wireless devices, services, and technologies in the DoD Global Information Grid (GIG). The Directive spells out policies for deploying secure wireless networks, and requires monitoring of those wireless networks for compliance. Additionally, the Directive states that wireless networks are banned from use in certain areas, and it covers policies for banned and authorized wireless networks. The Directive is effective immediately. Table 1 shows the wireless related security requirements of Directive 8100.2.

Section	*Security Requirement*	*Description*
4.1.1	Monitoring for Strong Authentication	*Section 4.1.1 of the directives mandates that all commercial wireless devices connected to the DoD global information grid need to use strong authentication*
4.1.2	Monitoring for Strong Encryption	*Section 4.1.2 requires strong encryption (FIPS 140-2 compliant) for all unclassified communication between wireless devices*
4.1.4	Mitigation of Denial of Service and other Disruptions	*Section 4.1.4 mandates the measures be taken to mitigate denial of service attacks including interference from friendly sources.*
4.2 & 4.3	Banning Wireless Devices in Designated Areas/Monitoring	*Section 4.2 & 4.3 of the Directive bans wireless devices from areas where classified information is discussed, processed, stored or transmitted.*
4.5	Active Monitoring of Unauthorized Access of DoD IS	*Section 4.5, the DoD Components shall actively screen for wireless devices. Active electromagnetic sensing at the DoD or contractor premises to detect/prevent unauthorized access of DoD ISs shall be performed to ensure compliance*

Table 1. Wireless related Security Requirement of Directive 8100.2

3 Security Threat on Wireless Network Environment

The wireless network is convenient in that it can be easily accessed even without the communication line of wired network. However, the threat of wiretapping increases at the same time. In other

words, an attacker with malicious intentions is able to easily gain the transmitted data without a separate operation on the communication line. Therefore, the situation is that public institutions and some corporations are restricting the use of wireless LAN. In this manner, a steady research is necessary for improving security under wireless LAN environment because the wireless LAN technology has various types of vulnerabilities. At the same time, the wireless LAN carries the problem of having difficulty in finding the physical location of attacker because the intrusion log is not saved and the attack by an attacker with malicious intentions is possible from any location where wireless communication is reached on the top of enabling detoured intrusion on the existing security system due to its nature [8]. Therefore, the security threats that may occur under wireless network environment using wireless LAN are summarized as follows.

Threat	Problem	Threatening Factor
Rouge AP (Installation of illegal AP within the company)	•Used by connecting unauthorized wireless AP in the wired network within the company (institution) without the permission of security administrator •Illegal installation of unauthorized AP by malicious user	•Intrusion of wired network is possible by detouring the firewall of company (institution) wired network or different security solutions using unauthorized AP
Mis-Configuration AP (An AP violating company policy)	•The use of AP that has not applied security policy due to the mistake of administrator •Change of security policy on unauthorized AP by a malicious user	•The intrusion of internal network by a malicious user is possible using an AP which is in violation of security policy
Tapping (Packet monitoring)	•Absence of encryption policy on the wireless interval at the AP	•A malicious user taps on the details of communication
Service denial attack	•Vulnerable to DoS attack due to structural cause of allocating resources when authentication is requested by a malicious attacker	•Possible to disable the wireless LAN service by indiscriminate authentication request by a malicious attacker
Unauthorized access (Illegal access of company AP)	•A malicious unauthorized user from the outside accesses to a normal authorized AP within the company	•Possible to intrude the company network without authentication process in case of open system authentication methods connecting to AP without password or certificate •Able to access various authentication methods applied for wireless LAN security (WEP, pre-shared key or WPA, etc) by hacking
Mis-Association (Access of external AP/service)	•An authorized user using internal network is able to access to external AP of nearby area	•An authorized user may leak confidential data of internal network by connecting to the external AP
Ad-Hoc Connection (Sharing of wireless network)	•Configuration of network among wireless users without going through the wireless AP using AD-Hoc communication which is a function provided by wireless LAN card	•An authorized user leaks data to external network using Ad-Hoc communication after saving internal data to a laptop •A hacker disguises as available free wireless LAN to decoy a user and leaks internal data as network connection is made with hacker in case the user attempts to access
Honeypot AP/Evil Twin (Theft of company AP service ID)	•SSID is an ID of wireless network and can be configured as same SSID intentionally or unintentionally	•The company user gets to access determining as proper authorized AP when there is attack such as Honeypot AP and leaks internal data of accessed authorized user
MAC Spoofing (Theft of user MAC hardware address)	•Sending AP MAC information by Beacon information sent periodically from wireless LAN AP	•Hacking Beacon information transmitting to AP using software based hacking tool •Taking internal data after causing access of authorized user by stealing MAC address to configure a dual AP

Table.2 Security Threats on Wireless Network Environment

As examined above, various attack threats exist under wireless network environment. Therefore, the management on wireless network must be performed systematically in order to protect the important confidential information of government agencies and companies from being leaked to the

outside. It is natural that the possibility of internal confidential information being leaked to outside gets higher in case the management on wireless network is not performed systematically [15].

4 State-of-the-Art of Security Management Service System

4.1 Definition of Security management service system

Cyber attacks are all forms of actions including theft, forgery or interfering with availability of information stored in the information system or communicated using information network while hacking, e-mail bomb, e-mail with hidden hacking program, service failure, Trojan horse, logic bomb, worm, trapdoor or sniffing, etc are being used as attack methods. Cyber attack detection is an action of finding out the cyber attack attempts such as sudden increase or decrease of total traffic on the network, hacking attempt to steal information and distribution of malicious hacking programs in advance using security management service system to detect conditions such as worm virus, DNS normal operation status and disconnection, delay or error of homepage. It also includes the action of finding security vulnerabilities so that the managed computer network is not abused as intermediate point of hacking [3].

The detection and analysis in security management service system stands for the action of identifying the attacker information, attack time and attack method, etc by gathering log information related to latest hacking technology and invaded computer network after detecting hacking attempts such as abuse of intermediate point, distribution of hacking mails, forgery of homepage and theft of information data.

Moreover, the counteraction from the management service stands for the action of notifying the fact of hacking to the agency that has suffered from the damage, promptly providing a specialized technology so that the damaged system can be operated normally using attacker information and vulnerability information identified at the analyzing stage as well as preventing the same intrusions in advance by developing detection technology on same hacking attacks based on hacking tools and hacking methods used for the attack.

Currently, the security management service system is performing detection, analysis and actions in various forms depending on the technological standard or security management service system know-how of each security management service system center. Therefore, the definition on security management service system can be considered by classifying into the security management service system of narrow sense and security management service system of broad sense depending on the range of performing the details of security management service system operations. The "security management service system of narrow sense" means only the activity of detecting cyber attacks through the monitoring on network traffic while the "security management service system of broad sense" could be considered as the concept which also includes detection, analysis and action. Therefore, this thesis considers the security management service system of computer network as the concept of security management service system of broad sense to be defined as "a series of activities to detect, analyze and take actions on various cyber attacks or threatening activities toward information system or information network to prevent loss of resources or invasion of information on them in advance [4]".

4.2 Foreign Security Management Service System Status [3][7]

4.2.1 United States

The United States is devoting active research and effort on the level of homeland security strategy to prepare for cyber terrors since the September 11 attacks. Currently, the security management service system operations such as monitoring of cyber threat symptoms on the computer network of United States federal government agencies is being performed by US-CERT under NCSD (National Cyber Security Division) within DHS (Department of Homeland Security).

4.2.1.1 NCSD

This agency was established in June, 2003 based on Homeland Security Presidential Directive (HSPD-7) and operating US-CERT is in operation under this agency. It is known to be under development of a system to identify the hidden status on hacking codes within network packets at this time because the ability is quite lacking in detecting hackings although 24 hour security management service system is performed by installing harmful traffic monitoring system (Einstein) at 15 main agencies among about 500 agencies within the United States. It also issues cyber threat alerts, evaluates vulnerabilities on federal government information network and has

real-time information sharing system maintained with CIA, Department of Justice or Department of Defense through CIIMG (Cyber Interagency Incident Management Group) security portal site.

Recently, as the accident of computer system information on main government institutions being exposed had occurred frequently due to the attack of hackers assumed to be foreign spies from China, etc, the Department of Homeland Security has newly established "National Cyber Security Center (NCSC)" (March, 2008) to be operated as a general government department organization supervising computer system and internet security of all federal government institutions such as monitoring cyber terror and managing hacking vulnerability information on the computer systems of federal government agencies under cooperation of FBI, NSA and Department of Defense. It is also performing Cyber Storm every two years in order to check the ability to cope with cyber attacks on the important national assets.

4.2.1.2 National Security Agency (NSA)

This agency has installed TOC (Threat Operation Center) for the purpose of protecting information system of storing and communicating important national secrets such as partial national defense network at IA and information network used by information agencies.

4.2.1.3 Department of Defense (DOD)

This agency has installed JTF-CNO (Joint task Force- Computer Network Operation directly under tactical commander to be monitoring information, performance of mission and cyber attacks with US armed forces stationed throughout the world based on national defense CERT (DISA: Defense Information System Agency). DISA is gathering cyber attack information and performing counteractions by monitoring existence of viruses or hacking attacks as it operates a situation room of 15~20 people 24 hours a day.

4.2.2 England

England is performing similar duties as security management service system at the CESG Incident Response Team (GovCertUK) of CPNI (Centre for the Protection of National Infrastructure). Incident Response Team stands for The UK Government's Computer Emergency Response Team and performs the function of minimizing computer related attacks and the following aftermath on government system which is one of CESG's missions. To make this possible, it is considering a comprehensive safety measures by identifying various forms of attacks and gathering case related information while issuing alert according to the level of cyber threat and performing by establishing various issue of advice and guidelines.

4.2.3 Russia

At the FAPSI under Federal Security Bureau (FSB) is conducting 24 hour monitoring on the internet network of government institutions. It is performing coping activities and attacker track down activities such as notifying the information security center which belongs under same organization, investigation of accidents on damaged PC or improvement on vulnerabilities, etc after detecting and analyzing cyber threatening symptoms. FAPSI is performing filtering and remote control on the internet traffic by installing a hardware device called SORM on the internet network through an ISP company.

4.2.4 Japan

Japan is monitoring on cyber threatening symptoms such as hacking or worm virus 24 hours a day on central government ministries since January, 2009 at the cabinet secretariat information protection center established based on the Rules related to the Installation of Information Security Centers" (by the decision of prime minister) in April of 2005 while performing the duty of providing support on the corresponding ministry by analyzing attacker information, attack time and attack method, etc on the detected threats.

5 Problems of Current Security Management Service System

Since the commercial service on the internet had started targeting the public since June of 1994, the cyber threat factors are being increased by as much as government or public institutions have gradually adopted the internet to be utilized for work. This was because the important work related data stored in the computer became target of theft for hackers as government or public institutions have used one computer for work and for internet at the same time. An example of this could be the cyber intrusion on all government or public institutions detected and handled at the national cyber safety center in 2007 being a total of 7,588 cases which is nearly two times the increased that the 4,286 cases of 2006. Such cyber attack is expected to be increased each day by gradually getting advanced and intelligent. Also, the form of its attack is threatening the safety of computer network as it became changed to attacks for the purpose of stealing internal information or DDoS attack interfering with normal services from attacks of simply showing off and

even demand money. Also in the diplomatic problems between countries, the attacks for the purpose of stealing national secrets or advanced technology of competing country is increasing while the trend is developing up to the phase of information warfare between countries by establishing a hacking unit for organized attacks.

If we examine the realities on preparation of cyber information warfare between countries, China is operating professional hacking organization with scale of about 6,000 people in People's Liberation Bureau while the United States is consolidating cyber security even more by pointing out Chinese government as the background as the cases of hackers intruding the Department of Defense and main government institution websites to leak confidential documents occurred frequently since 2001. While it was known to establish a virtual attack system to prepare for cyber warfare recently, there was a time when US Air Force had expressed that it would train as cyber attack crack unit such as disturbing the communication system of enemy or destroying data packets by newly establishing cyber headquarters organized by formation of 4 units until October of 2008. This is the part getting even more attention because the fact that US government can assume preemptive strike was openly suggested by turning away from being consistent as defense centered with the cyber warfare.

The security management service system operations on government or public institutions of our country was performed independently by each institution starting with financial ISAC installed by Korea Financial Telecommunications & Clearings Institute in December, 2002 for security management service system on 18 banks on the market and the National Cyber Security Center was launched in February, 2004 from the opportunity of internet crisis in January 25, 2003 to perform the function of general security management service center on national level targeting government or public institutions.

Currently as of December, 2008, there are security management service system centers by each field established by each central administrative agencies and unit security management service system centers under operation by each individual agency including the National Cyber Security Center for the security management service system centers of our country.

The National Cyber Security Center is maintaining 24 hour cyber attack information detection, general analysis and coping system considering characteristics, priority and security system operation environment of computer network at each agency in order to perform a security management service system operations on a country-wide level targeting main national information networks after being established within the National Intelligence Service in February, 2004 based on "National Cyber Security Management Rules (Presidential Instruction No. 141)". The alerts are issued by levels such as attention, caution, alert or severe considering far reaching effects of cyber attack or scale of damage for systematic actions and preparations on cyber attacks. Also, while the latest security management service technology is developed to be utilized for security management service system operations to cope effectively with advanced cyber attacks, this technology is also supported to other security management service system centers. The security management service system center by each field is performing duties of detecting and blocking cyber attacks targeting the independent computer network of central administrative agencies or its affiliated agencies while the unit The security management service system centers are performing The security management service system duties on the independent computer network of the corresponding agency. Although security management service system center continues to be extended and established by each agency, it carries the following problems.

First, the defense system on the level of national security and protecting national interest on cyber space is lacking. While each security management service system center is detecting and blocking cyber attacks on cyber space unlike the defense system on physical space by army, navy or air force, most of these are remaining at the level of detecting simple cyber attacks such as worms or viruses to be insufficient for detecting and blocking hacking attacks invading national security or national interest such as advanced defense industry secrets or core technology of the nation.

Second, most security management service system center are lacking exclusive security management service system organizations and specialized workers while the situation is that they are lacking in the ability to detect, analyze and cope with cyber attacks because there are even institutions that are not performing 24 hour security management service system duties.

Third, there are cases of same invasions recurring in other agencies as the information that

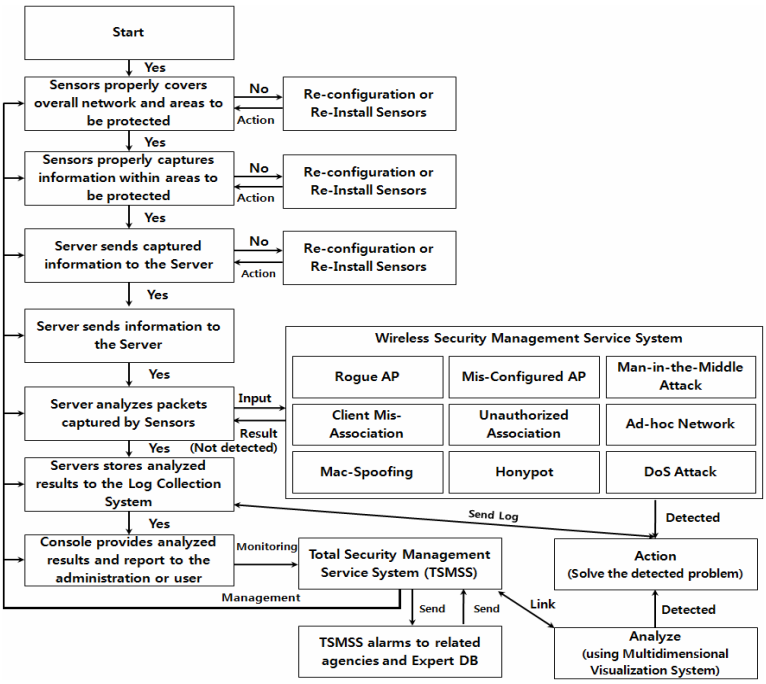

Fig.1 Proposed Wireless Security Management Service Procedures

can be shared are not shared by each other due to lack of cooperation between security management service system centers as well as the sharing of security management service system information being difficult as the performed type or method, technological standard and security management service system scale, etc are different by each security management service system center.

Fourth, each agency is somewhat going through difficulty in performing security management service system activities because there is no clear legal basis followed by performance of security management service system activities. Therefore, the situation is that it is necessary to setup up a security management service system for national computer network that can effectively detect, analyze and cope with cyber attacks on a national level in the policy oriented perspective.

6 Proposal of Wireless Network Security Management Service System Framework

In order to building up a secure security management service system in wireless network environment which is going through a rapid increasing recently, the security threats on wireless network environment must be clearly identified to consider the method to solve problems in various angles in the aspects of technology, management and policy.

Figure 1 shows proposed wireless network security management service system procedure. We can prevent the data leakage from organization using radio spectrum. It tell us the presence of unauthorized, rogue access points and the use of wireless attack tools. The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a rogue access point is detected.

The proposed framework requires fully distributed sensors and server to analyze the captured by sensors. Sensors contain antennas and radios that scan the wireless spectrum for packets and are installed throughout areas to be protected. Also, Server analyzes the packet captured by sensors. This framework related with various securities system techniques. In this section, we explain the detail elements to make secure wireless network environments.

6.1 Intelligent Type Wireless Network Security Management Service System Framework

The security management service system performed until now has many limitations in resources, information, time and technology. In other words, while a skilled expert on the corresponding field is required in addition to the devices for analysis, detection and counteraction in order to building up a safe security management service system, there is much difficulty because

there are few of these experts and they are high class workers. At the same time, while the access authority on IP location information on the attacker is required for detecting and analyzing intrusions, the access is limited. Also, the time required for taking action is gradually increasing as the attacks are becoming complicated and diversified while having the characteristics of having difficulty in coping effectively within the limited time to cope with attacks [9].

Therefore, it is necessary to adopt an intelligent type system in order to detect attacks with highest performance under situation of having many limitations in resource, information, time and technology. An intelligent type system helps to make fast decision making possible on information security cases by connecting internal system and external data to analyze the correlation between these systems.

6.2 Wireless Security Management Service System

In order to block security threats on the wireless network, a system for providing security on the wireless network is required. The wireless LAN security can be mainly classified into two types. One is the section related to wireless LAN authentication and the other is building up a security system called Wireless Intrusion Detection System (WIDS) or Wireless Intrusion Protection System (WIPS) [1][10].

WIDS/WIPS is able to prevent hacker intrusions and leak of internal corporate information from using illegal AP as the one that has extended the security function provided by the existing firewall of wired network and the VPN security system. It also gets to prevent security accidents by blocking connection with improper AP and client in and out of the corporation causing security vulnerabilities. WIPS includes various forms of systems implemented in a form of hardware, firmware or software as a system providing support to raise stability of wireless LAN and perform integrated management by detecting and preventing the access of unauthorized wireless devices automatically by steadily monitoring the wireless LAN Operated in a specific organization.

WIPS provides the function of detecting and blocking intrusion attempts using illegal AP or user's devices, Ad-Hoc connection and MAC modulation attacks, etc within the range of wireless AP used in the exposed wireless network.

WIPS can be mainly configured as two system types of centralization type and decentralization type. The centralization WIPS means the type which performs centralized processing by sending all wireless data gathered from WIPS sensor to the server and the decentralization type WIPS is the structure in which the security policy of WIPS server is applied to the WIPS sensor so that the sensor performs filtering and attack detection/block functions on wireless traffic directly according to the security policy.

WIPS server and sensor may exist in different hardware from each other or can be running in same hardware. Especially, the sensor can exist independently from AP or can be configured as combined from with AP. WIPS server must be located at a physically safe environment and must be accessed only by the administrator. The administrator may perform security management and audit report management, etc by accessing WIPS server with local or remote connection. The security function of safe route/channel configurations must be provided in order to protect the data transmitted between administrator and WIPS server or between WIPS server and WIPS sensor while the data sent or received can be user data. Also, a time synchronization feature must be provided in order to secure the validity of time on the audit data created real time.

6.3 The Linked Model Method with Existing Security Management Service System

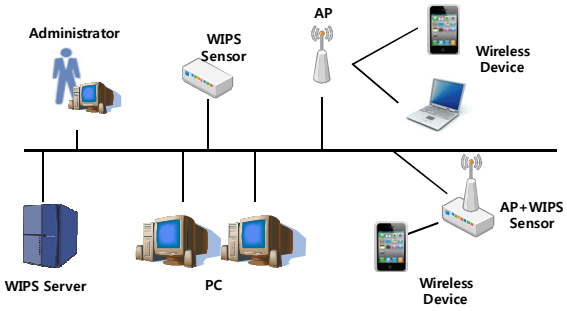

Fig.2 Wireless Network Environment

Currently, the internet environment is very complicated and diverse while DDoS attack method also continues to evolve using the vulnerability of action system. First of all, the current security management service system method is coping with attacks based on device. Therefore, the actions on new attacks are inadequate from device centered defense system configuration and the complexity of operation gets increased by being installed without considering the relationship with existing security devices. Also, the current DDos attack coping

method is block centered. When the threshold value configured in the device is exceeded, the availability gets invaded by blocking the access of normal users in sequence. In addition, it is difficult to actively cope with new attacks as the coping system is set up based on known attacks and carries the problem of not being able to distinguish normal users and attackers when the signature is missing [11].

In order to solve these problems, an IP reputation policy using QoS can be utilized. This is a service method of providing selective blocks according to availability by evaluating the IP reputation after gathering IP information connecting to the system at ordinary times and gathering IP on this normal user. This is a method to guarantee availability of normal users and while the attack packets pass through backbone sector router or boundary sector router, the effective packet blocks are made possible without invading the availability of normal user that had occurred in the past while detecting DDoS attacks through DDoS devices [2].

Moreover, the abnormal behavior detection technique can be utilized in detecting malicious behaviors after preparing normal behavior pattern of normal user or abnormal behavior as profile under normal conditions.

However, the security management service system on wireless network is unable to solve problems on all vulnerabilities with technological actions. Therefore, multilateral actions in physical and administrative aspects are necessary.

In other words, the wireless network must be properly managed by an integrated security management system in case the use of wireless network is authorized by combining with the wired network within the organization [14]. In other words, the wireless routers must be controlled by security management service system along with existing MPLS, IPS, IDS, Firewall, VPN, server security and DB security. While the information leaked to the outside must be blocked effectively by adopting network separation policy defined in advance by the organization in a security management service system, the wireless network carries the problem of being able to detour the security system without going through the wired network. Therefore, the installation of unauthorized devices must be removed by detecting illegal AP's on wireless LAN sections in order to solve this problem while the physical control and interfering frequency on corresponding zone can be utilized with CCTV in case the physical control on AP at the boundary of internal and external organization is difficult. Also, the 3G data network must apply MDM (Mobile Device Management) system because the detection on leak of information through wireless network security management service system is difficult [12].

6.4 Wireless Network Data Correlation Analysis, Detection and Action Method System

As cyber attacks are getting intelligent / advanced each day, the detection and analysis • action on them are getting difficult. If we look into the cases of recent cyber attack invasions, the detection is not easy and also takes a lot of time in the analysis because new attack methods are mixed up in addition to the previously known attack methods. Although the defense on the vulnerability is possible if the vulnerability open to public gets removed in case of previously known attacks, the steady monitoring by accident analysis expert and long period of research on this are necessary in case of new attach methods. However, there are many difficulties on the level of actual counteraction because the condition of being able to analyze for long period of time cannot be formed. Therefore, it would be proper to have normal behavior pattern of normal user or abnormal behavior under normal times to utilize the abnormal behavior detection method during monitoring.

Most of all, the application of multilateral detection method and coping system are necessary because the extent and influence of damages are quite high if the important confidential information of the nation or corporation can be leaked to the outside through the wireless network which is not properly managed at this time. The following has indicated the data correlation analysis, detection and action method for performing security management service system more effectively on the wired and wireless integrated network [1].

6.5 The Multidimensional Visualization Plan of Wire/Wireless Integrated Security Management Service System Technology

To cope with constantly changing security threats, it is necessary to develop functions such as setting up the policy of extracting important information related to the outbreak of new threats by performing multidimensional analysis on the data gathered on attacks. This can make instant actions possible when abnormal symptoms occur. Thus, there is an advantage of being able to minimize the damages with prompt action after checking additional threats by performing integrated analysis on internet status and intrusion data detected and gathered through the security management service system. At this time,

the data gathered to the security management service system requires the function of refining and summarizing the abnormal symptom detection results along with the function of analyzing the relationship to cope effectively by creating the

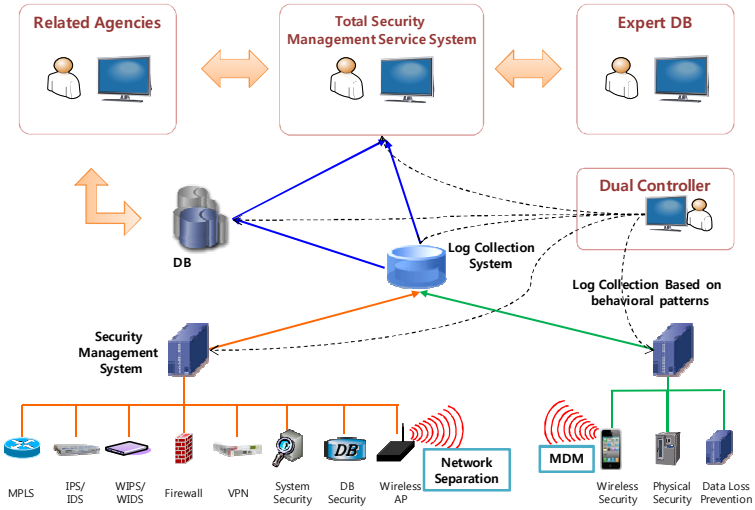

Fig.3 Security Management Service System Framework

results reacting up to hundreds thousands of cases per each unit system. According to the intrusion correspondence team of Korea Internet & Security Agency, the related data is gathered with more than 350,000 cases of e-mail spam trap and more than 60,000 cases on threat management system based on one day. Therefore, an analysis method that can visualize by selectively extracting the significant information among numerous gathered data is required [13].

The thing to consider while implementing such multidimensional visualization is as follows. First of all, the operation stability must be considered while connecting between the existing system and newly developed system. Only the valid data among mass quantity of data gathered to the security management service system should be sorted out and gathered while having only the minimum effect on the operated system. Also, the preparation of a standard for consistency of input information and accuracy of analysis information is necessary. It must be able to accommodate both existing retained information and additional information of the future while it is necessary to define the standard data format to enable integrated analysis.

7 Conclusion

In order to fundamentally block the leak of important data within government and public institutions or corporations, the internet and work computer network must be separated. While the current network separation business is focused on the separation of wired network, the issue of wireless security has become an essential and indispensable situation for the security management service system on wireless network to protect the important assets of organization in the security of entire organization because the wireless access using smart phones is possible at any time and place under the current situation in which smart phones are widespread. In other words, the real-time analysis of wireless traffic and wireless network security management service system on leak of data and external threatening behaviors through wireless network would be necessary. That is because the separation of the network on internet and work can become meaningless if the wireless network can be used by internal user or external wireless threats exist even if the wired network separation is accomplished successfully. Actually, it is difficult for public institutions to identify whether an internal user is using wireless network with laptop or wireless device even if the use of wireless network is restricted. Also, it is more than possible for internal users to access the external network just with one illegal router at the internal network and the reality is that the installation of inexpensive wireless router is often taking place due to user convenience including service companies in the work-site operations. The items checked when the security management service system company diagnoses vulnerability mainly includes whether intrusion from outside to inside is possible, whether

going out from the inside is easy, how many illegal routers there are and how much service availability is guaranteed without freezing the work system due to DoS attack while using wireless infrastructure. Currently, it is difficult to solve this problem only with technology related plans while the security at policy related perspective through management effect of the organization along with legal and systematic improvement would have to take place at the same time.

Acknowledgements

This research was supported by the MKE(The Ministry of Knowledge Economy), Korea, under the "ITRC" support program supervised by the NIPA(National IT Industry Promotion Agency) (NIPA-2011-C1090-1001-0004).

References

[1] Tarek S. Sobh, "Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art," Computer Standards & Interfaces, Volume 28, Issue 6, pp. 670-694, September 2006.

[2] R.F. DeMara, A.J. Rocke, "Mitigation of network tampering using dynamic dispatch of mobile agents," Computers and Security, vol. 23, pp.31-42, 2004.

[3] G.Shipley, Chapter 12 "Intrusion Detection Systems (IDSs)," in Shelley Johnston Markunday, Maximum Security:A Hacker's Guide To Protecting Your Internet Site And Network, third edition, Sams Pyblisher, Indiana, 2001.

[4] N. Ye, Q. Chen, "Profile-based information fusion for intrusion detection," Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, 2001, pp. 227– 230.

[5] R.A. Kemmerer, G. Vigna, "Intrusion detection: a brief history and overview," Reliable Software Group, Computer Science Department, University of California Santa Barbara, Supplement to Computer Security and Privacy (2002) 27–30.

[6] S.H. Oh, W.S. Lee, "An anomaly intrusion detection method by clustering normal user behavior," Computers & Security 22 (7) (2003) 596–612.

[7] J. Mirkovic, G. Prier, P. Reiher, "Attacking DDoS at the source," Proceedings of ICNP 2002, Paris, France, 2002, pp. 312–321.

[8] R.R. Talpade, G. Kim, S. Khurana, "NOMAD: Traffic-based network monitoring framework for anomaly detection", Proceedings of the Fourth IEEE Symposium on Computers and Communications, 1998.

[9] J. Yang, P. Ning, X. Wang, S. Jajodia, "CARDS: a distributed system for detecting coordinated attacks," in: Sihan Qing, J.H.P. Elof (Eds.), Proceedings of IFIP TC11 Sixteenth Annual Working Conference on Information Security (SEC 2000), Kluwer Academic Publishers, 2000.

[10] J.B.D. Cabrera, L. Lewis, X. Qin, W. Lee, R. Prasanth, K. Ravichandran, B. Mehra, "Proactive detection of distributed denial of service attacks using MIB traffic variables—a feasibility study," Proceedings of the 7th IFIP/IEEE International Symposium on Integrated Network Management, Seattle, WA, May 14–18, 2001.

[11] Y. Huang, J.M. Pullen, "Countering denial of service attacks using congestion triggered packet sampling and filtering," Proceedings of the 10th International Conference on Computer Communications and Networks, 2001.

[12] S. Han, S. Cho, "Detecting intrusion with rule-based integration of multiple models, "Computers & Security 22 (7) (2003) 613– 623.

[13] Donghwi Shin, Kwangwoo Lee, Dongho Won, "Malware Variant Detection and Classification using Control Flow Graph," Proc. of ICHIT 2011, International Conference on Convergence and Hybrid Information Technology 2011, Springer-Verlag, Daejeon, Korea, September 22-24, 2011, pp.180-187.

[14] Kwangwoo Lee, Changbin Lee, Namje Park, Seungjoo Kim and Dongho Won, "An Analysis of Multi-Function Peripheral with a Digital Forensics Perspective", Proc. of CNSI 2011, International Conference on Computers, Networks, Systems, and Industrial Engineering, Jeju Island, May 23-25, 2011, pp.252-257.

[15] Kwangwoo Lee, Dongho Won, and Seungjoo Kim, "A Secure and Efficient E-Will System Based on PKI," Information - An International Interdisciplinary Journal, International Information Institute, Volume 14, No.7, July 2011, pp.2187-2206.

Deaseob Lee is a Ph.D. student in the School of Information and Communication Engineering at Sungkyunkwan University. His current research interests are in the area of information security and assurance. Contact him at dslee@security.re.kr

Dongho Won received his B.E., M.E., and Ph.D. degrees from Sungkyunkwan University in 1976, 1978, and 1988, respectively. After working at the Electronics & Telecommunications Research Institute (ETRI) from 1978 to 1980, he joined Sungkyunkwan University in 1982, where he is currently a Professor of the School of Information and Communication Engineering. His interests are cryptology and information security. He was the president of the Korea Institute of Information Security & Cryptology (KIISC) in 2002. He is the corresponding author. Contact him at dhwon@security.re.kr