A Study on Real-time Cooperation Protect System Against Hacking Attacks of WiBro Service

Dea-Woo Park, *Member, KIMICS*

Abstract— **U.S. Obama government is submit a motion to consider cyber attacks on State as a war. 7.7DDoS attack in Korea in 2009 and 3.4 DDoS attacks 2011, the country can be considered about cyber attacks. China hackers access a third country, bypassing South Korea IP by hacking the e-commerce sites with fake account, that incident was damaging finance. In this paper, for WiBro service, DDoS attacks, hackers, security incidents and vulnerabilities to the analysis. From hacker's attack, WiBro service's prognostic relevance by analyzing symptoms and attacks, in real time, Divide Red, Orange, Yellow, Green belonging to the risk rating. For hackers to create a blacklist, to defend against attacks in real-time air-conditioning system is the study of security. WiBro networks for incident tracking and detection after the packets through the national incident response should contribute to the development of technology.**

Index Terms— **WiBro Service, Hacking, Vulnerability, DDoS, Blacklist, Real-time Cooperation Protect System**

I. INTRODUCTION

WIBRO(Wireless Broadband) service is a 4G Standard with LTE(Long Term Evolution). 3GPP LTE is a standard in the mobile phone network technology tree that produced the GSM/EDGE and UMTS/HSPA network technologies. WiBro service with the latest high-speed Internet and phone services are being linked in South Korea. With the proliferation of smart phones and even the domestic WiBro network services market by 2011 is expected to reach 5 million people.

The U.S. government was initiative a new bill for strengthen cyber security. Enhance penalties for cyber crimes and other crimes and equate them is that the content contained. In addition to the core infrastructure, the minimum penalty for any hacking attempt has decided to establish. The U.S. Department of Defense Operational Domain considered a cyber space land, air, sea, space that is similar to the operational areas were considered.

Manuscript received July 21, 2011; revised August 8, 2011; accepted August 10, 2011.

Dea-Woo Park is with the Department of IT Application Technology, Hoseo Graduate School of Venture, 1463-10, Seocho 3-dong, Seocho-gu, Seoul, South Korea (Email: prof1@paran.com)

In case of cyber attack of Korea, in 25th February 2009, auction users 10.81 million people was leaked their personal information by hacking. In addition, 7 July 2009 and other major intelligence agencies and financial institutions in the Blue House Internet site, a DDoS attack by hackers [1] is paralyzed by, SQL Injection attacks, XSS attacks and the many Web [2] had. March 4, 2011 in DDoS attacks and cyber terrorism, cyber attacks, cyber security on a national level, the importance of research and the security is.

DDoS attacks on the WiBro network services, if carried out, and connected to a network communications system can bring about the communications failure.

But attached to the WiBro network and communications systems, the lack of comprehensive real-time security defense systems in real time by attacking a DDoS attack is difficult to respond.

For the protection of DDoS attacks in real time incident response center and the remote attacker to make attacks on the event information causes a rapid real-time analysis is difficult as a result it is difficult to defend. For the defense of DDoS attacks in real time incident response center and the remote attacker to make attacks on the event information causes a rapid real-time analysis is difficult as a result it is difficult to defend[3].

To defend against DDoS attacks and tracing the Victim Server [4] and the associated network DDoS attacks in real time and related early warning network system to be delivered to and through the coordination of real-time defense system should be organic.

That is causing DDoS attacks Zombie PC [5], as well as the course of transit camp forged IP addresses [6] to use a blacklist to determine the location of a remote hacker [7] raised, and real-time protection by modifying the security policy If you do not build systems, hackers are developing new types of cyber attacks are expected to make a DDoS attack.

In this paper, a DDoS attack, intelligent, diversified, WiBro network equipment and security equipment for the study and, DDoS attacks carried out in real-time analysis of events from the remote control to determine the whereabouts of the hackers Blacklist raised, Modify Security Policy to build a real-time defense system is to study.

II. RELATED WORKS

2.1. Cyber attack cases and DDoS attacks

Hybrid types of cyber attacks gradually, intelligent, larger, and the result of the attack target of infringement damages to individuals and businesses is being enlarged [8]. Table 1 shows the incident is a major status.

TABLE 1
STATUS OF MAIN INCIDENT

Date	Status of Main Incident
25/Jan/2003	In 1.25 Internet chaos, worldwide 75,000 computers and over 8800 Korean computers infected by the 'Slammer worm' virus.
05/Feb/2009	Disclosure of 10,810,000 Auction Users individual Information by Hacking
07/Jul/2009	The Blue House and other major institutions and some portal websites down by DDoS attack
04/Mar/2011	To The Blue House, Daum, if their time changes earlier than attack and infection time , damage to the hard disk

2.2. WiBro Service

WiBro (**Wi**reless **Bro**adband) is a wireless broadband Internet technology developed by the South Korean telecoms industry. WiBro is the South Korean service name for IEEE 802.16e (mobile WiMAX) international standard. WiBro services using next-generation mobile communication technology, high-speed mobile internet anytime, anywhere on the road a Web search, as well as e-mail, multimedia, videoconferencing, Internet telephony services including Internet information and content available Mobile 2.0 service [9] should include. Table 2 shows Comparison with other Mobile Internet Access methods.

TABLE 2
COMPARISON OF MOBILE INTERNET ACCESS METHODS

Standard	Family	Primary Use	Radio Tech	Downlink (Mbit/s)	Uplink (Mbit/s)
WiBro	802.16e	Mobile Internet	MIMO-SOFDMA	128	56
LTE	UMTS/ 4GSM	General 4G	OFDMA/ MIMO/ SC-FDMA	100	50
Wi-Fi	802.11 (11n)	Mobile Internet	OFDM/ MIMO	300 or 600	

As an international standard IEEE 802.16e Handoff to support the mobility and Sleep Mode feature is available. In addition, to maximize power-saving features of the terminal and the area between Base Stations in a stable multicast / broadcast service to provide the MBS (Multicast & Broadcast Service) and Idle Mode feature, call forwarding services, considering the Paging feature, and provides faster handover for FBSS (Fast Base Station Switching) feature and has been reflected in standard. In addition, to improve the performance of the system for multi-antenna technology, AAS (Adaptive Antenna System) and MIMO (Multiple-Input Multiple-Output) and a number of suggestions were adopted. In recent years, improved the way Channel Coding with LDPC technology adoption also provides various functions [10].

2.3. Security System Technique of WiBro Network

WiBro network security monitoring, and the simplicity in the form of security policies across the network is expanding into the security control area.

Security Management System Security Device only a single direction of the development not just IT infrastructure, applications, transactions, business-oriented integrated management of the [11].

WiBro network security products Firewall, IDS (Intrusion Detection System), IPS (Intrusion Prevention System), VPN (Virtual Private Network) to the security of a dedicated unit DPI (Deep Packet Inspection) technology is based on. In recent years, firewalls, antivirus software, such as content filtering and spam filtering capabilities that are integrated into one package, integrated security system, UTM (Unified Threat Management) has evolved into.

The WiBro network management targets and the existing traffic control devices in the range shown in Table 2 include SMS (System Management System), NMS (Network Management System), ESM (Enterprise Security Management) [12], and two representative, the current ESM equipment, the NMS / SMS, with the main features of the absorption and TMS (Threat Management System) and UTM (Unified Threat Management) that such connections are becoming integrated security network system.

III. ANALYSIS OF A HACKING ATTACK ON THE WIBRO SERVICE

3.1. DDoS Attack and hacking Analysis of WiBro service

WiBro equipped mobile devices to configure the network using the WiBro service to a PC using an Internet service that targets the DDoS attacks were shown in Figure 2.

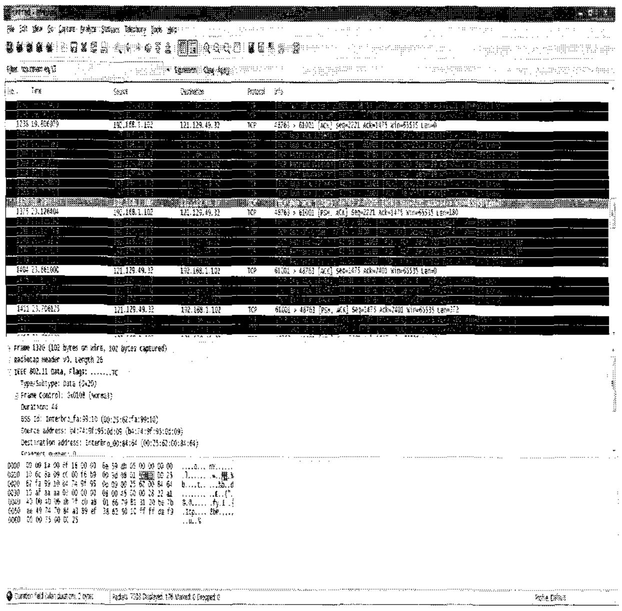


Fig. 1. Packet capture in victim system

TCP SYN Flooding / DRDoS and about 150,000 in a second thread form of the session to attack the target system, resulting in the goal WiBro system was down. IP Fragment, in the attack packet about 1MB of attacks began around 1 minute and WiBro slow down the processing of the target system as the administrator of the resource consumption is impossible in normal use and eventually became Crash target system. Quiescent state of the system is moving faster than the system to deplete the availability of resources the system was halted[3].

In addition, ICMP / IGMP Flooding ICMP echo request/igmp-0 message in the attack were sent in bulk. Spoofing the source IP is a detecting for the ICMP Flooding and Bad ICMP echo request packet that is detected by the detection of IGMP was not.

Attacks of the system to process the packet on average, about 70% of CPU resources consumed, and the drop in the level of the target system, the kernel and did not leave a log[3].

3.2. Personal Information hacking attack Analysis of on the WiBro service

Wibro Messenger to communicate with the Internet network, the vulnerability of personal information, as Figure 1, Shows scanning the contents of the packets through the analysis has been found.

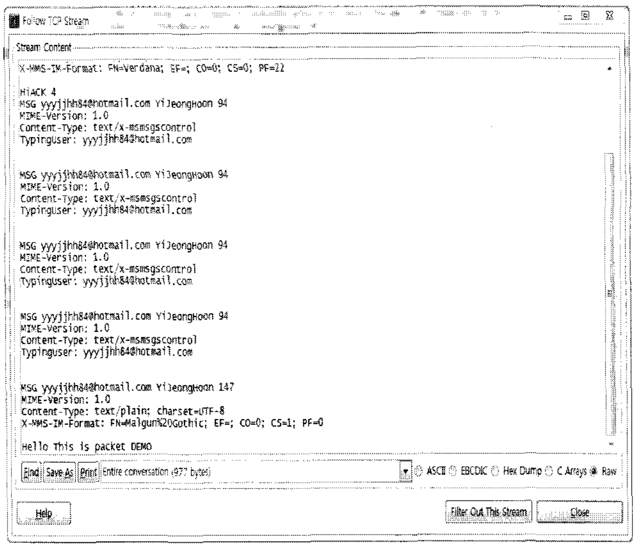


Fig. 2. Vulnerability of Personal Information

Wibro network using hacking tools on the user's authentication key tapping, hacked authentication key to log on as a user of the WiBro network, integrated monitoring, using hacking tools A company connected to the wireless AP can monitor the user's information. Hacking tools of the social security number and address of connected users, phone numbers and other sensitive information can be hijacked by the way, the ability to verify the information by the Internet has.

Hackers in the laboratory in the vicinity of the WiBro search for a specific company, the Company shall determine in writing the name of the wireless AP. Made of the same name, and the wireless AP to lure users to access. Users can easily be connected to the wireless AP is a fake. At this point the user to enter a site address, the hacker may have access to the site will be created. User login and password to enter a fake, this information will be stored on the hacker's computer.

IV. REAL-TIME SECURITY AND COOPERATION SYSTEM CONFIGURATION ABOUT WIBRO SERVICE

4.1. Process configuration of real-time security and cooperation system

WiBro service, hacker attacks and external network security for the eco-system with a process for real-time security and cooperation systems is shown in Figure 4.

WiBro service network and external information in the system, identifier, IP information, browser information, local information, such as dynamic IP address to gather information. Information stored on the Web and the WAS server, running on the server through the information gathering and writing log records and statistics, such as the blacklist.

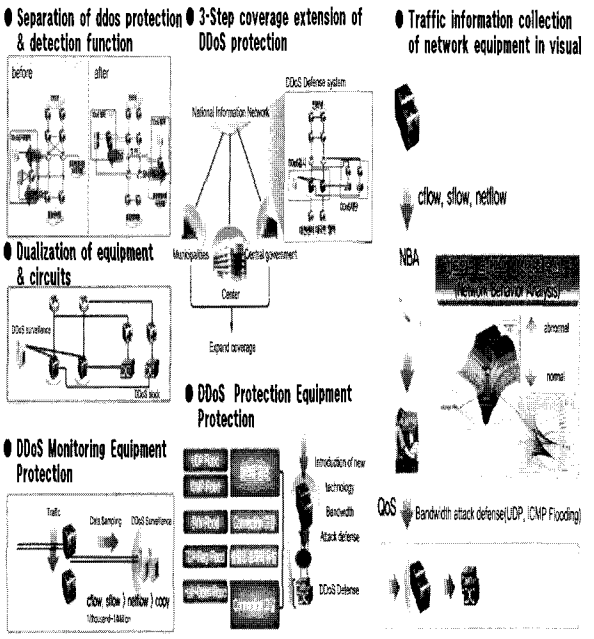


Fig. 3. Process of real-time cooperation protect system configuration

In WiBro service attack, and cooperation systems for real-time security of the collected visitor IP, port, service, Application to collect information, statistics and information collected through the analysis of possible threats to the analysis of pre-capture, Red, Orange, Yellow Risk in real time by dividing the propagation and defense. Yellow risk grade for WiBro service, real-time analysis and more, Red risk grade for WiBro service is to respond before the incident while performing real-time, packet analysis, and related agencies for the security system, security policy and defense programs, etc. propagation in real time and updates.

4.2. Function analysis of real-time security and cooperation system

To configure real-time security and cooperation systems require the following features.

■ The source of hacker attacks / host site / blacklist generation search technology, such as zombie PC is secure. Potential source of attack / host site / zombie PC-related data collection / normalization / search / store, the spread of malicious code, secure and real-time inspection and monitoring of the path through the execution of malicious code analysis of the situation, with a per-property correlation analysis of network security situation is should.

■ Real-time attack, incident response professionals to share information between the framework will be built. Between countries, between regions, by administrative area of information sharing and cooperation based on information modeling framework, real-time attack, a standard data model for sharing of information is needed.

■ Information sharing framework based data interchange format and transfer protocol is needed. Collection of information on the incident / normalization / search / store, share, and the object of attack, information technology, information exchange types of attacks, national standards, to deliver a secure connection based on the information is necessary to establish protocols.

■ Information sharing framework is based integrated security control system. Between attacks, security event and network event information of an attack linked technology, real-time attack information systems integration and conformance for sharing, potential areas of application development and management to define and should be piloted.

4.3. Network configuration of real-time security cooperation system

Shown in Figure 3 with WiBro service is installed between the Internet and internal networks have Firewall and VPN, DMZ security cooperation, including in the packet capture server to install the system.

Firewall Internal Network on the inside and the manager module installs the application.

4.4. Traceback configuration of real-time security and cooperation system

For WiBro service, SQL Injection attacks, XSS attacks, such as in the case of most Web as shown in Figure 5 for the Web visitor Real IP acquired the security and cooperation systems using toxic post treatments were tracking configuration.

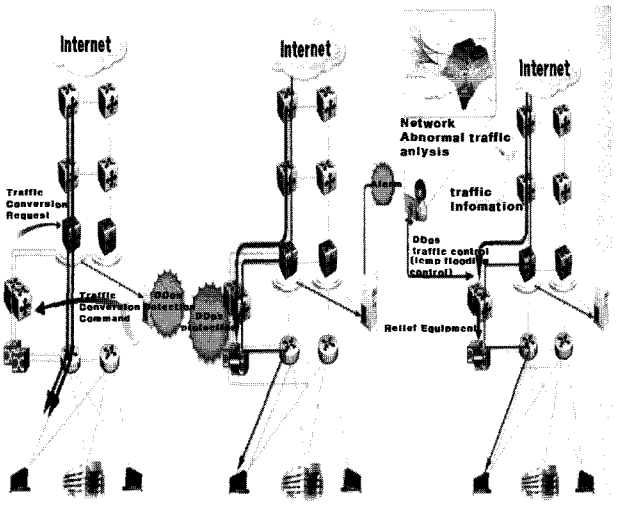


Fig. 4. Network configuration of real-time cooperation protect system

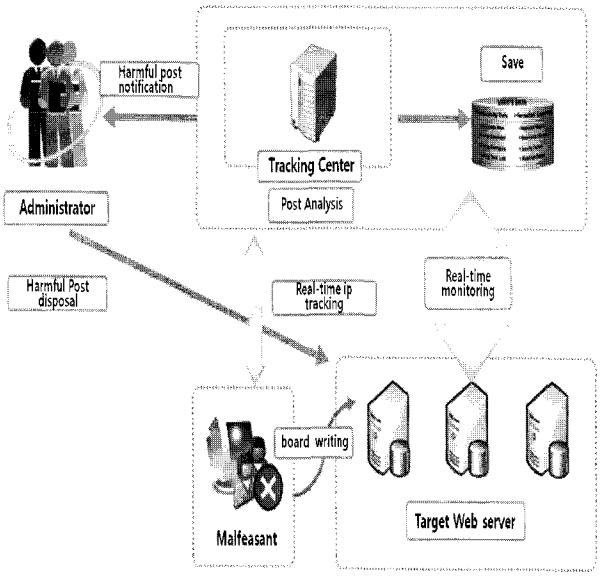


Fig. 5. Configuration of real-time cooperation protect system Tracking

Agent of web pages and bulletin boards to install the tracking system to track the Real IP, detect and trace Writing on the board.

V. CONCLUSIONS

For WiBro service, hacker attacks and attacks on the precursor symptoms correlate and analyze real-time cooperation protect system. To counteract this through WiBro service is installed between the Internet and internal networks have Firewall and VPN, DMZ security cooperation, including in the packet capture server, install the system and statistical analysis of collected information and threats that may occur throughout the pre-Analysis to capture, Red, Orange, Yellow, Blue dividing Risk Transfer and defending in real time, real-time security cooperation through the response of the system configuration process and obtained web splice Real IP for security and cooperation systems using toxic post treatments Traceback Configuration was.

For the future research, include real-time security cooperation through WiBro service uses a system of Red, Orange, Yellow and divided by the risk rating on the security policy accordingly agency details and real-time response by the security guidelines and manuals on research need.

ACKNOWLEDGMENT

" This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(grant number: 2011-0005784)".

REFERENCES

[1] Ashley Chonka, Jaipal Singh, Wanlei Zhou, "Chaos Theory Based Detection against Network Mimicking DDoS Attacks", IEEE Communications Letters, Vol. 13 No. 9, pp. 717-719, September 2009.

[2] K. K. Mookhey, "Nilesh Burghate, Detection of SQL Injection and Cross-site Scripting Attacks",http://www.securityfocus.com/infocus/1768

[3] Dea-Woo Park, "A Study on Hacking Attacks and Real-time Security Cooperation System of WiBro Service", Korea Institute of Maritime Information and Communication Sciences, Vol. 4 No. 1, pp. 6-9, June 2011.

[4] Dea-Woo Park, Jung-Man Seo, "TCP / IP attacks, security measures for the study, " Korea Institute of Computer and Information, Volume 10 No. 5, pp.217-226, November 2005.

[5] Sung-Ho Ahn, Chang-Gu Kang, Young-Rak Choi, "Agent DDoS attack response mechanisms and through cooperation, "

[6] "Reducing the Energy Consumption of Ether net with Adaptive Link Rate(ALR)", Cham ara Gunaratne, IEEE Transaction on computers, Vol. 57, No. 4, 2008.

[7] In-Hee Lee, Dea-Woo Park, "spam and Vulnerability attack to VoIP and security for the Study", Korea Computer and Information Science, Volume 14 No. 2, pp.215-224, December 2006.

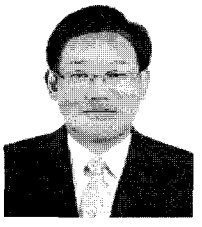
[8] Jung-Ho Choi, "cyber-terrorism, and South Korea support the direction of the transition", Defence and Security Conference, pp.155-172, April 2008.

[9] T Yamakami, T ACCESS, "MobileWeb 2.0: Lessons from Web 2.0 and Past Mobile Internet Development," Multimedia and Ubiquitous Engineering, 2007.

[10] A Raniwala, T Chiueh, "Architecture and algorithms for an IEEE 802.11-based multi-channel wireless mesh network," IEEE Computer and Communications Societies, Proceedings IEEE, 24th Annual Join, INFOCOM 2005.

[11] Dea-Woo Park, Seung-Lin Im, "the hacker's attack, intrusion prevention system for the study of intelligent connection", Korea Institute of Computer and Information, Volume 11, No. 2, pp.351-360, May 2006.

[12] Yeon-Seo Jung, Gul-Woo Ryu, Jong-Su Jang, "ESM technology trends for network security", ETRI, 2001.



Dea-Woo Park is an Adjunct Professor of IT Application Science Department at the Hoseo Graduate School of VENTURE, South Korea. Dr. Park received the B.S. degree in computer science from the Soongsil University in 1995. And he received the M.S. degree in 1998. He received the Ph.D. degree from the computer science department of the Soongsil University in 2004. Dr. Park has worked as the Head of Researcher and Developer Laboratories at Magiccastle co., LTD. His research interests are Hacking, Forensic, Information Security of Computer and Networks, Smartphone and Mobile Communication Security.