International Journal of Smart Home
Vol.7, No.5 (2013), pp.135-144
http://dx.doi.org/10.14257/ijsh.2013.7.5.14

Design and Analysis of Client Control System Using DNS Control Firewall

Bong-Hyun Kim[1] and Young-Gil Park[2]

[1]*Department of Computer Engineering, Kyungnam University*
[2]*Department of Multimedia Engineering, Hanbat National University*
hyun1004@kyungnam.ac.kr, yppark@atek21.com

Abstract

In this paper, the client control system designed for infringement blocking system development. In order words, infected with harmful files on your computer by using a user-centered information systems development and security through the design of a control system using DNS control firewall client access to the site randomly for acts that can block the under solving techniques. Design of the client control system was classified as Dynamic intrusion prevention system module design, Embedded domain name service system module design, Interlocking DNS service module design and Cert & Analysis module design. Finally, through simulation, an average of 14% was measured by abnormal packet ratio.

Keywords: *Client Control, DNS Server, Dynamic Intrusion Prevention Module, Embedded DNS Module, Interlocking DNS Module, Cert & Analysis Module*

1. Introduction

Current cyber hacking and privacy spill continues and a variety of information and communication technologies to the development of a security breach, accident and attack methods evolve further. KISA reported 18,937 cases damages for malicious code and hacking incidents received 18,126 cases are being investigated in the year 2012 in November according to November 2012 Internet attack trends and analysis monthly[1]. A web site to access concealed malicious code when the user directly by typing the URL in the web browser to search for information, or induction of malicious code, such as security breaches occur through the use of the web hard, the first user can be preventable through DNS control access to the web site[2, 3].

Therefore, in this paper, the client control system designed for infringement blocking system development. In order words, infected with harmful files on your computer by using a user-centered information systems development and security through the design of a control system using DNS control firewall client access to the site randomly for acts that can block the underlying solving techniques.

Shown in Figure 1 infringement blocking DNS server module is applied as proposed solutions to the internal DNS IP information requested user information and real-time information of the request passed to the DNS control firewall policy settings and automatically check for normal access procedure sallow access to the normal[4]. In addition, against illegal access to the defined DNS query access without blocking. Blocking the illegal access to information about the site, collect the security team and the CERT team passed to the analysis of the client control system has been designed with a sophisticated system can handle security technology.

ISSN: 1975-4094 IJSH

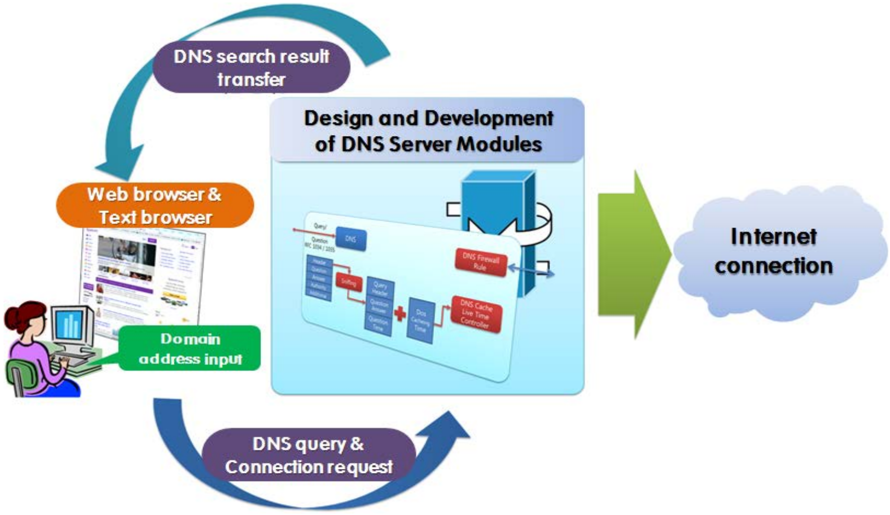
DNS search result transfer
Design and Development of DNS Server Modules
Web browser & Text browser
Domain address input
Internet connection
DNS query & Connection request

Figure 1. System Flow Chart

2. Infringement Incidents Status

Looking at the statistics on domestic security threats[5], as shown in Table 1, the last in November 2012 according to data from Internet Security Response Center received the year November 2012 hacking incidents of domestic handled 18,126 cases, damage reported malicious code 18,937 cases. As shown in Figure 2 and report[6], the number of hacking incidents received treatment since 2005 has reduced, but the damage reported malicious code since 2008 continue to increase.

Table 1. Monthly Infringement Incidents Receipt Processing Statistics (2012year)

type	2011 year	2012 year											total
		1	2	3	4	5	6	7	8	9	10	11	
Malignant code damage reporting	21,751	1,443	1,186	1,685	2,164	2,138	2,394	1,638	1,472	,1339	1,419	2,059	18,937
Hacking incident receipt processing	11,690	1,510	1,210	1,702	1,419	1,534	2,174	1,937	2,173	1,273	1,608	1,586	18,126
• Spam relay	3,727	429	395	474	621	693	598	485	434	400	812	668	6,009
• Phishing stopover	365	36	37	38	39	37	34	30	29	41	42	36	399
• Simple intrusion attempts	2,961	202	184	159	106	206	394	240	614	304	191	155	2,755
• Others hacking	2,783	233	307	415	515	488	796	1,000	1.013	431	440	355	5,993
• Homepage falsification	1,854	610	287	616	138	110	352	182	83	97	123	372	2,970
Malicious Bot infection rate	0.52%	0.6%	0.6%	0.6%	0.7%	0.7%	0.7%	0.6%	0.7%	0.7%	0.7%	0.8%	0.68%

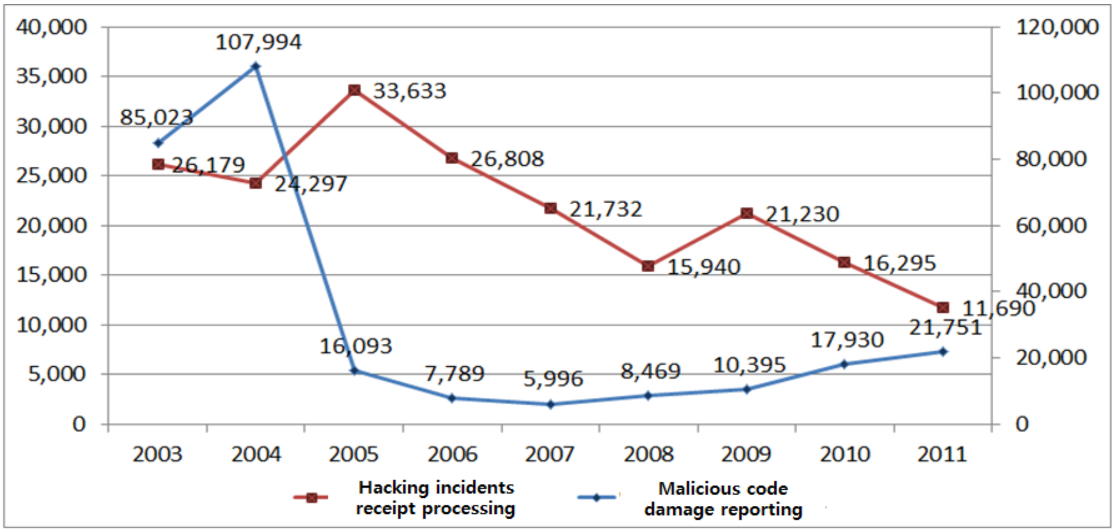

Figure 2. Security Infringement Incidents Processing Statistics (2003~2011year)

Look at overseas trends, security vendor McAfee according to the march 2012 quarter threats report [7] were aggregated URL worldwide in the third quarter of 2012, the threat of malware and phishing sites separated by the total number of 43,400,000 cases. This is an increase of 20% compared to the second quarter of 2012, and 23700000 represents the URL of the domain name than before up to 5% increase. In addition, domain handsome newly discovered threats URL monthly average 2,700,000 cases is the number of unique IP address, and 110,000 cases distinct domains, such as the threat of a new trend also was announced [8, 9]. Figure 3 and Figure 4 shows per month in 2012 newly discovered threats, the increasing rate of the URL and phishing sites.

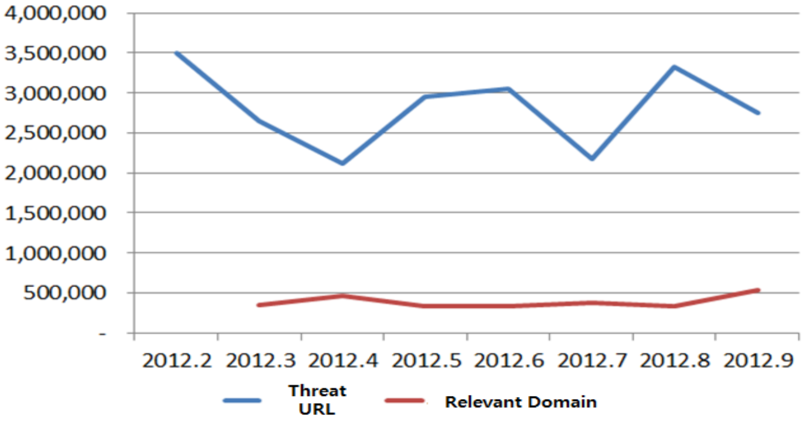

Figure 3. Monthly Discovered Threats URL Situation (2012year)

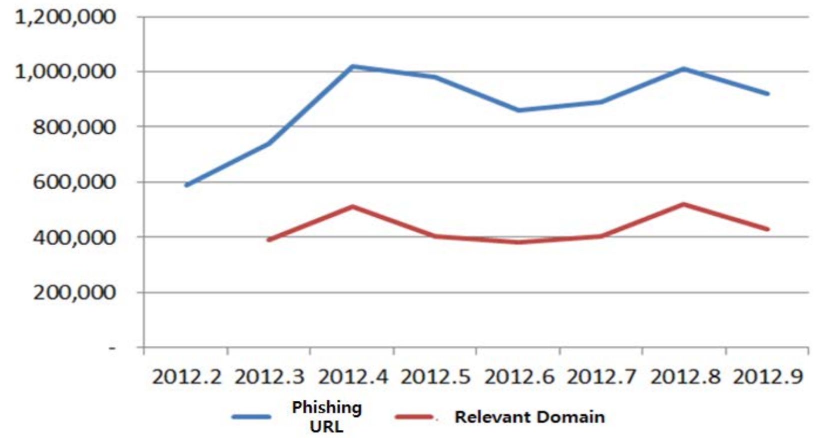

Figure 4. Monthly Discovered Phishing URL Situation (2012year)

Production of malicious code in recent years, additional attacks, disseminate very made it easier, variant exponentially more. Web site access these threats and malware infections accordingly customer information leaked confidential information leaked by a malicious hacking or industrial espionage, the company's internal staff, such as using a computer crime has skyrocketed[10, 11]. But specific threat cannot just to control the security system because it blocked breaches through the 100% perfect. In other words, the security system can allow open access path is required to work for only blocked infringement perfect difficult. In addition, through surveillance, detection, detect breaches through bypass techniques, such as intrusion detection IDS also widely known for obvious abnormal behavior patterns or detection because there is a limit [12-14].

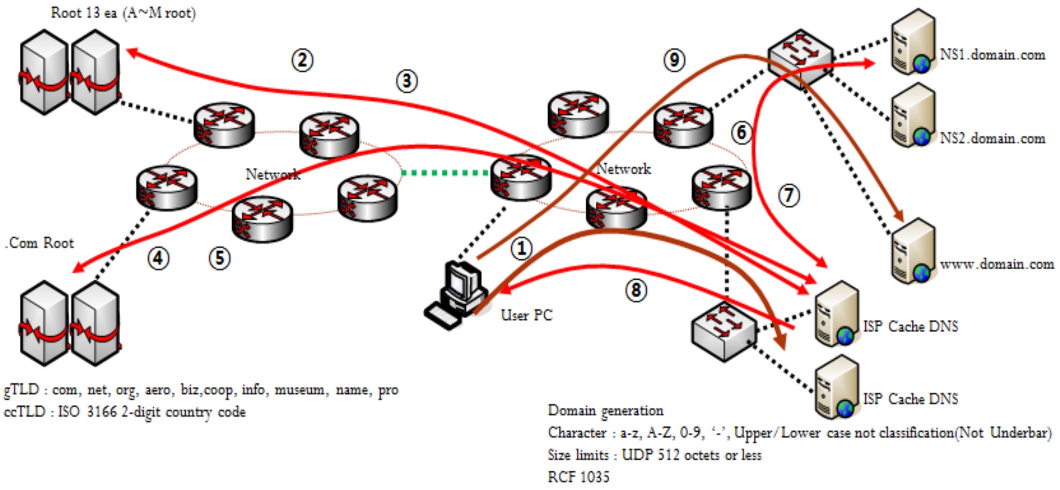
Root 13 ea (A~M root)
②
③
⑨
NS1.domain.com
NS2.domain.com
⑥
Network
Network
⑦
.Com Root
④
⑤
①
www.domain.com
⑧
User PC
ISP Cache DNS
ISP Cache DNS
gTLD : com, net, org, aero, biz,coop, info, museum, name, pro
ccTLD : ISO 3166 2-digit country code
Domain generation
Character : a-z, A-Z, 0-9, '-', Upper/Lower case not classification(Not Underbar)
Size limits : UDP 512 octets or less
RCF 1035

Figure 5. DNS Service Flow According to Client Request

Therefore, in order to fundamentally solve them is absolutely necessary to control the behavior-based user-centric form only. For this purpose, in this paper requested internal user of a reliable IP to DNS information internally defined and the results of the request, the information in real-time intrusion prevention system and passed to the device (DNS Control Firewall), we automatically set the policy, and the normal were allowed access to normal verification procedures for access to the normal. Moreover, block illegal access, and additional related information processing (information processing, analysis, and design) that can be used to handle system [15, 16].

3. Design and Analysis of DNS Control Firewall

In this paper, the client control system designed to develop the next-generation system of block infringing. In order words, the client control system designed using DNS reliability of the system control block for evolving and diverse security breaches in advance for block module. Design of the client control system was classified as Dynamic intrusion prevention system module design, embedded domain name service system module design, Interlocking DNS service module design and Cert & Analysis module design.

Design of client control system using DNS control firewall is normally Query information about the results of the DNS information Interlocking block is the core technology that allowed for the respondents performed.

Step 1: Dynamic intrusion prevention system module with the results of DNS requests generated and has a dynamic policy was generated during the destruction process for tracking the user's session through the process of being destroyed.

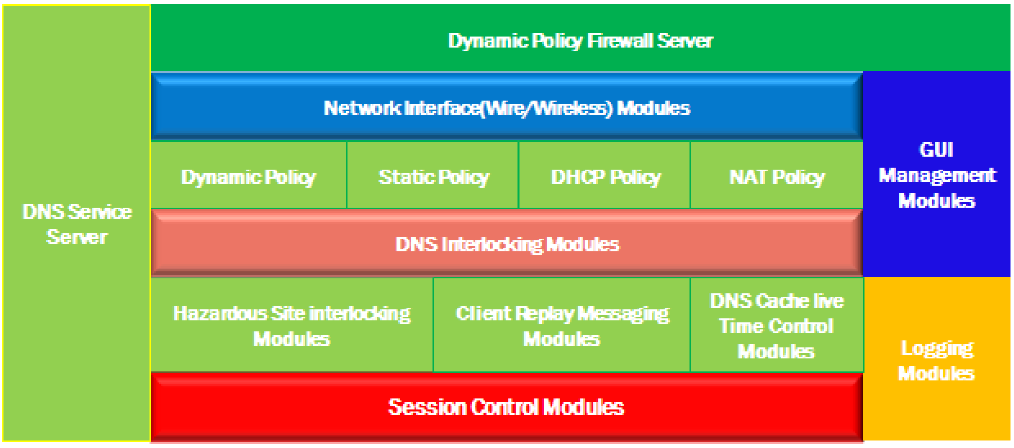
DNS Service Server
Dynamic Policy Firewall Server
Network Interface(Wire/Wireless) Modules
Dynamic Policy
Static Policy
DHCP Policy
NAT Policy
GUI Management Modules
DNS Interlocking Modules
Hazardous Site interlocking Modules
Client Replay Messaging Modules
DNS Cache live Time Control Modules
Logging Modules
Session Control Modules

Figure 6. Dynamic Intrusion Prevention System Module Diagram

Step 2: Embedded domain name service system module is own hardware resources to be occupied by the various services that are used by the operating system by removing all DNS service availability to ensure maximum.

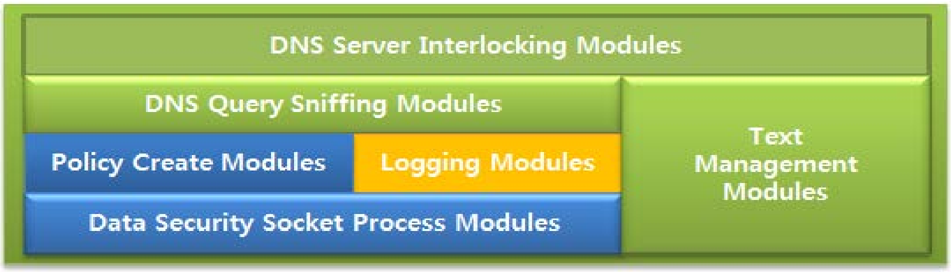
DNS Server Interlocking Modules
DNS Query Sniffing Modules
Policy Create Modules
Logging Modules
Data Security Socket Process Modules
Text Management Modules

Figure 7. Embedded Domain Name Service System Module Diagram

Step 3: Interlocking DNS service module is DNS query sniffing through the results for the normal requestor to determine the response. Next, Dynamic intrusion prevention system generate part of the policy to create policies to be applied to the system dynamic intrusion resulting value. Interlocking DNS service module is embedded server socket tunneling communication internally to DNS service system, and a dynamic intrusion prevention system design.

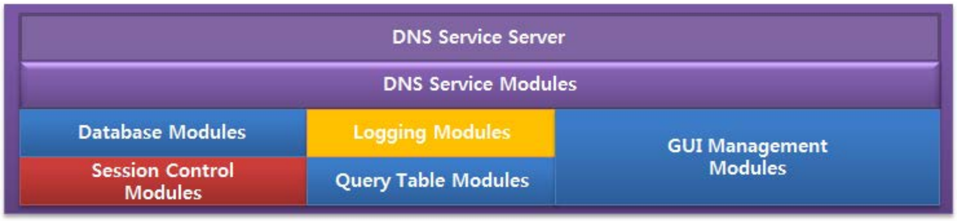

Figure 8. Interlocking DNS Service Module Diagram

Step 4: Cert & Analysis module is part of that development to take advantage of the resulting information processing to second as possible as a variety of information provide and information processing. Also, the system was developed to maintain the security of the latest design through the automatic update.

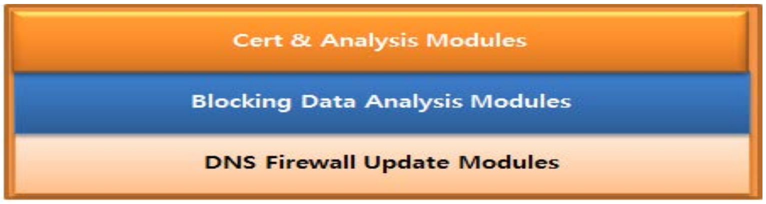

Figure 9. Cert and Analysis Module Diagram

Web site to access the user when using a browser to run for illegally planted illegally outside the browser is blocked through DNS server the configuration module design and apply, Inspection from a trusted primary DNS blocking. Requested internal user's trusted secondary DNS IP information on real-time information and request information automatically delivered to the device by DNS policy by setting your browser to block illegal. The normal browser for a normal approach can access the hack to block and prevent breaches expected in advance.

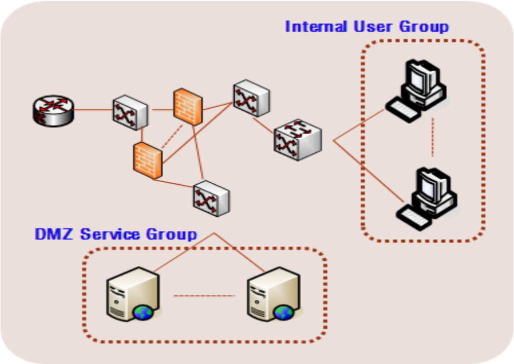

Figure 10. System Operating Diagram

Method designed in this paper, it is a form of integrated Domain Host to search method and Intrusion Prevention System unlike the solution of existing. Therefore, a variety of problems and worries of existing information security system fake phishing damage domain approach, disclosure of personal information by users unwittingly install the zombie damage and the secondary & tertiary infections damage due to harmful files utilizing protocols that are operating on existing development is intended to solve the problem.

In this paper, we designed that simulation was performed based on the DNS Control Firewall. As shown in the simulation results, it shows an average of 14% of abnormal packets. As a result, DNS information is proposed in this paper, the control method for linkage techniques is the way to solve fundamentals.

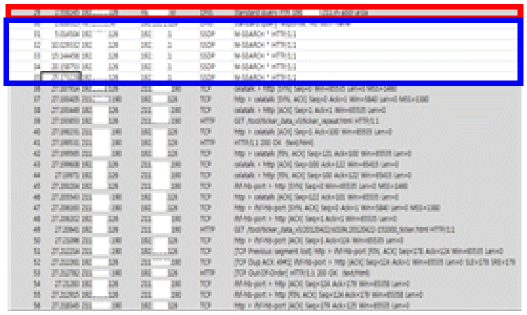

Figure 11. DNS Packet Data Collecting

Table 2. Packet Analysis Results

Acquisition time	Total packet	DNS query	DNS Normal response	DNS Abnormal response	Normal packet	Abnormal packet	Normal packet rate	Abnormal packet rate
1 min	90	10	6	4	66	11	73%	12%
5 min	570	2	2	0	491	75	86%	13%
10 min	1186	0	0	0	1015	171	86%	14%
15 min	1560	2	2	0	1315	243	84%	16%
20 min	2349	2	2	0	2032	315	87%	13%
Average	5755	16	12	4	4919	815	85%	14%

4. Conclusion

In this paper, the client control system designed for infringement blocking system development. In order words, infected with harmful files on your computer by using a user-centered information systems development and security through the design of a control system using DNS control firewall client access to the site randomly for acts that can block the underlying solving techniques.

For this purpose, the client control system design was classified as Dynamic intrusion prevention system module design, Embedded domain name service system module design, interlocking DNS service module design and Cert & Analysis module design. The future, the information security market, through various forms of user authentication, service access, and control method is applied in the form of market will be blocked with the proposed configuration of the DNS server modules are to be analyzed infringement of user-centered system to take advantage of the core technologies of the information security market.

Finally, in this paper, we designed simulation was performed based on the DNS Control Firewall. As shown in the simulation results, it show an average of 14% of abnormal packets. As a result, DNS information is proposed in this paper, the control method for linkage techniques is the way to solve fundamentals.

References

[1] Korean Internet & Security Agency, KISA Report, **(2012)**.

[2] B. G. Kyoun, “A study on the improvement of the computer security incident management”, Sungkyunkwan Univ. A Master's Degree Paper, **(2011)**.

[3] D. G. Song, “Hacking Infringement Accidents Analysis”, Ji&Son Publishers, Korea, **(2009)**.

[4] G. M. Pérez, F. G. Clemente and A. G. Skarmeta, “Managing semantic-aware policies in a distributed firewall scenario”, Internet Research, 10.1108/10662240710828049, vol. 17, no. 4, **(2007)**.

[5] KISA, Trends report monthly malicious code detection of concealed site, **(2012)**.

[6] KISA, Trends and analysis monthly of internet infringement accidents, **(2012)**.

[7] McAfee Threats Report: Third Quarter, **(2012)**.

[8] T. Ma, “On the Security of A Novel Elliptic Curve Dynamic Access Control System”, International Journal of Software and Its Applications, 10.1007/978-3-642-10240-0_1, vol. 3, no. 1, **(2009)**.

[9] P. El Khoury, P. Busnel, S. Giroux and K. Li, “Enforcing Security in Smart Homes using Security Patterns”, International Journal of Smart Home, http://www.sersc.org/journals/IJSH/vol3_no2_2009/5.pdf, vol. 3, no. 2, **(2009)**.

[10] F. Alkhateeb, A. M. Manasrah and A. R. Bsoul, “Bank Web Sites Phishing Detection and Notification System Based on Semantic Web Technologies”, International Journal of Software and Its Applications, http://www.sersc.org/journals/IJSIA/vol6_no4_2012/5.pdf, vol. 6, no. 4, **(2012)**.

[11] E. Hooper, “Efficient and Intelligent Network Infrastructure Protection Strategies for Complex Attacks, IDS Evasions, Insertions and Distributed Denial of Service”, International Journal of Software and Its Applications, http://www.sersc.org/journals/IJSIA/vol1_no1_2007/IJSIA-2007-01-01-03.pdf, vol. 1, no. 1, **(2007)**.

[12] M. Khairallah, “Security System Design and Implementation Guide: The Design and Implementation of Electronic Security Systems”, Butterworth-Heinemann http://www.bicsi.org/pdf/Regions/northeast/PhiladelphiaMarch2012/ESSsystemDesign_Mahoney_Faber.pdf, **(2005)**.

[13] H. S. Yoo, H. G. Park, I. H. Yoo and H. J. Kim, “A Study on Network Reliability Analysis for Information Security”, Journal of Korea Academia-Industrial cooperation Society, 10.5762/KAIS.2010.11.10.3935, vol. 11, no. 10, **(2010)**.

[14] D. Rountree, “Security for Microsoft Windows System Administrators: Introduction to Key Information Security Concepts”, Elsevier, **(2010)**.

[15] J. S. Kim and S. S. Shin, “Probabilistic Filtering Method for Efficient Sensor Network Security”, Journal of Korea Academia-Industrial cooperation Society, 10.5762/KAIS.2012.13.1.382, vol. 13, no. 1, **(2012)**.

[16] K. Chain, W. C. Kuo and J. C. Cheng, “An Improved Secure Anonymous Protocol for Distributed Computer Networks”, International Journal of Software and Its Applications, http://www.sersc.org/journals/IJSIA/vol6_no4_2012/13.pdf, vol. 6, no. 4, **(2012)**.

Authors

Bong-Hyun Kim received the B.S., M.S., and Ph.D. degrees from the Department of Computer Engineering of Hanbat National University, Daejeon, Korea, in 2000, 2002, and 2009, respectively. He is currently a professor in the Department of Computer Engineering, Kyungnam University, Korea. He is research interests include Bio-signals analysis, security system, USN applications, e-Commerce and u-Healthcare system.

Young-Gil Park received the B.S. degree from the Department of Computer Engineering, in 2007, M.S. degrees from the Department of Multimedia Engineering of Hanbat National University, Daejeon, Korea, in 2009, respectively. He is currently a representative director in the ATEK Information Technology Co., Ltd, Daejeon, Korea. He is research interests include security system, network security, USN applications.