Development of Indicators for Information Security Level Assessment of VoIP Service Providers

Seokung Yoon[1], Haeryong Park[1] and Hyeong Seon Yoo[2]
[1] Korea Internet Security Center, Korea Internet & Security Agency
IT Venture Tower, Jungdaero 135, Songpa, Seoul, Korea, 138-950
[e-mail: seokung@kisa.or.kr, hrpark@kisa.or.kr]
[2] Computer and Information Engineering, Inha University
100 Inharo, Namgu, Incheon, Korea, 402-751
[e-mail: hsyoo@inha.ac.kr]
*Corresponding author: Hyeong Seon Yoo

Abstract

VoIP (Voice over Internet Protocol) is a technology of transmitting and receiving voice and data over the Internet network. As the telecommunication industry is moving toward All-IP environment with growth of broadband Internet, the technology is becoming more important. Although the early VoIP services failed to gain popularity because of problems such as low QoS (Quality of Service) and inability to receive calls as the phone number could not be assigned, they are currently established as the alternative service to the conventional wired telephone due to low costs and active marketing by carriers. However, VoIP is vulnerable to eavesdropping and DDoS (Distributed Denial of Service) attack due to its nature of using the Internet. To counter the VoIP security threats efficiently, it is necessary to develop the criterion or the model for estimating the information security level of VoIP service providers. In this study, we developed reasonable security indicators through questionnaire study and statistical approach. To achieve this, we made use of 50 items from VoIP security checklists and verified the suitability and validity of the assessed items through Multiple Regression Analysis (MRA) using SPSS 18.0. As a result, we drew 23 indicators and calculate the weight of each indicators using Analytic Hierarchy Process (AHP). The proposed indicators in this study will provide feasible and reliable data to the individual and enterprise VoIP users as well as the reference data for VoIP service providers to establish the information security policy.

***Keywords*: VoIP, MRA, AHP**

A preliminary version of this paper was presented at APIC-IST 2013 and was selected as an outstanding paper. This research was supported by Inha University Research Grant.

http://dx.doi.org/10.3837/tiis.2014.02.0018

1. Introduction

The VoIP service is one of the social media based Internet telephony service that uses IP based packet type voice transfer technology. It is growing as the communication industry technology continuous to advance based on All-IP with growth of broadband Internet network. Despite its low fee, the VoIP service failed to gain popularity because of low QoS, inability to receive calls as the phone number could not be assigned and inadequate accessibility. However, it has become the leading convergence technology in the broadcasting/communication market due to increasing subscribers and expanding market as the service based operators entered the market, cost-saving in long distance and international phone calls, and improving network efficiency as the voice and data are transferred over a network (IP nework) [1]. A report forecasted that the total market size of VoIP equipments for corporation was KRW 240 billion in 2012 and is predicted to be KRW 285 billion in 2016 [2].

Although interest on VoIP service is increasing in Korea, more security threats against VoIP and security incidents have also been reported. Therefore, it is important to prepare and carry out the security policy to create the safe usage environment of VoIP. However, there were no indicators that required VoIP service providers to measure their information security level. Consequently, they are having difficulty establishing their security policy and they are potentially exposed to numerous security threats.

In this study, we developed reasonable security indicators through questionnaire study and statistical approach. To achieve this, we made use of 50 items from VoIP security checklists. Then, we verified the suitability and validity of the assessed items through Multiple Regression Analysis (MRA) using SPSS 18.0. As a result, we drew 27 indicators and calculate the weight of each indicators using Analytic Hierarchy Process (AHP). The proposed indicators will provide feasible and reliable data to the individual and corporate VoIP users as well as the reference data for VoIP service providers to establish the information security policy.

We present in Section 2 some related work. Section 3 looks into the research method and Section 4 describes result of the analysis. Lastly, Section 5 discusses the study result, implication and future study direction.

2. Related Work

2.1 Security Issues in VoIP

Since VoIP technology delivers service over an IP network, it is vulnerable to attacks related with IP. Accoring to the VoIP security guideline [3], attacks can be classified into four types.

First is the DoS attack. DoS is a type of attack that monopolizes the system resources to disable the original functionality. It can interrupt the operation of VoIP service or even shut it down. Its leading examples include the flooding attack, which send a large volume of message in a specific period to shown the VoIP service or degrading the call quality and BYE message attack or CANCEL message attack which terminate the active calls by force.

The second attack is the session interception. It is a method of stealing the privilege from users or using it illegally. Since it changes the route of the voice data of the active call to wiretap all messages of the participating host and intercept the session data, users' registration data can also be leaked.

Third is eavesdropping. It is the act of illegally listening to another user's call without consent. In the VoIP service environment, calls between the users can be wiretapped using the vulnerability of the system or terminal. The easiest way is to collect the packets through the ARP poisoning attack in the same LAN environment. Collected packets contain the call establishing message packet, voice RTP packet, user authentication data packet, etc., and the voice RTP packet can be analyzed to wiretap the call.

Fourth is VoIP spam. VoIP spam takes advantage of relatively low Internet cost and utilizes the spam generation automation tool to activate the phone service to a large number of users. When such VoIP spam increases, it can violate privacy and degrade reliability of VoIP service.

2.2 VoIP Security Checklists

It is necessary for VoIP service providers to establish security policies and check security act continuously. To achieve this, there is an urgent need for an institutional stanard to assess VoIP service providers information security level. Also, it is important to check their service periodically based on the standard and to remove the security threats according to the result. Korea Communication Committee (KCC) and Korea Information & Security Agency (KISA) enacted VoIP security guideline together security experts from government, laboratory, academy and industrial world. It contains VoIP security checklists seperated by three categories: technical, managerial, and physical as shown in **Table 1**. To get 50 items, we carried out literature research and Delphi surveys three times targeting thirty VoIP security experts and professors. The Delphi survey is a effective method when it is impossible to make decision making based on objective and accurate information. It gathers the opinions of experts and makes decision through consensus of expert opinions [4]. Yoon et al analyzed the factor of VoIP security checklists using AHP [5].

2.3 AHP

AHP developed by Saaty in 1970 could help effective decision making to simplify the procedures [13]. AHP also provides a comprehensive method by considering quantitative factors and qualitative factors simultaneously based on evaluators' consistent decision through pairwise comparison [14]. AHP could measure the reliability of questionnaire response based on consistency ratio (CR). The consistency of data and weight of each factores are considered meaningful when the value of CR is less than 0.1 [13, 15]. With these characteristics, AHP is widly used to decide the importance of security indicators. In this paper, AHP is used to decide the weight of each indicators.

3. Research Method

This study verifies the suitability and validity of the assessed items through hierarchy and objective method of survey of VoIP service providers and security experts.

First, this study selected 50 items from VoIP security checklists. Before SMR, we performed Delphi surveys for considering the independence of indicators under VoIP service environment.

Second, we organized 50 items into a hierarchy and conducted the first survey of 100 VoIP service providers and security experts. Then, internal consistency analysis and step-by-step multiple regression analysis (SMR) were performed to reduce the assessed items from 50 to 23.

Third, Anlaytic Hierachy Process (AHP) was applied to calculate the weight factor for each assessed item.

Table 1. VoIP security checklists (50 items)

Classification		Item	Literature Research
Technical Inspection	Network Security	9	VoIP Security Guideline [3] Samarati and Vimercati [6] Gordon and Loeb [7] NIST [8] Bodin et al. [9]
	Terminal Security	5	
	VoIP Equipment Security	7	
	User Information Protection	2	
Managerial Inspection	Security Organization Setup and Operation	5	Information Security Check Service Manual [10] Falk & Fries [11] Akhil [12]
	Security Planning Establishment and Management	6	
	Manpower Security	5	
	User Information Protection	1	
	Response to Incident	1	
	Security Measures Inspection	1	
	IT Asset Management	2	
Physical Inspection	Entry/Exit and Access Control	2	VoIP Security Guideline [3] Gordon and Loeb [7] NIST [8] Bodin et al. [9]
	Accessory Equipment and Facility Operation	1	
	Etc	3	

4. Analysis Result

4.1 MRA Result

To verify reliability, the composite scale reliability index (CSRI), which is similar to Cronbach's Alpha was calculated. If CSRI value is 0.7 or higher, the variable measurement is considered to be internally consistent [16]. Since CSRI values of all variables are 0.7 or higher, measured indicators of this study are considered to be reliable. Reliability and validity of the measured indicators were verified by the analysis of the measurement model. Using the model, significance test of each indicator in the multiple regression analysis was performed to verify the hypothesis. VoIP service provider inspection indicators adopted for information security indicators to be used in multiple regression analysis were 10 technical protective measures, 10 managerial protective measures, and 3 physical protective as shown in **Table 2**. The 27 dropped indicators are also shown in **Table 3**.

Table 2. Adopted items after SMR (23 items)

Classification		Contents
Technical	Network Security	Is the integrated management system of VoIP security equipment?
		Is the technology to detect the malicious attack on users and VoIP network applied?
		Are the technical measures to prevent eavesdropping in the LAN/WAN zone applied?
		Is the spam response system to respond to VoIP spam deployed?
	Terminal Security	Can the users change the ID/PW of the terminal?
		Does the system provide encryption of the signaling and media data?
		When an administrator logs in remotely, is encryption or login channel protective technology applied?
		Is the blacklist function to block the spam in the terminal provided?
	User Information Protection	Is the security technology applied to prevent information leakage during storing or transfer of the personal information?
		Is the technology to control access to personal information DB and processing system applied?
Managerial Inspection	Security Organization Setup and Operation	Is a Chief Information Security Officer (CISO) assigned?
		Is a coordinator assigned for each area of information security duty?
	Security Planning Establishment and Management	Is the information security policy containing the goal, scope, and responsibility of information security established?
		Is the plan approved by management?
		Is the current year's information security action plan containing the budget and schedule based on the policy?
		Was the action plan approved by management and does the CISO checks the progress semi-annually?
	Manpower Security	Is the PR campaign carried out so that employees would be aware of the information security?
		When consigning the IT operation to a third party, are reflected in the security contract or SLA?
	IT Asset Management	Is the VoIP network schematic diagram generated and revised when there have been changes?
		Is the VoIP equipment and facility lists (including the usage and location) generated and managed?
Physical Inspection	Entry/Exit and Access Control	Is the locking system installed so that unauthorized people cannot enter?
		Are the entrance/exit records kept for at least one month?
	Accessory Equipment and Facility Operation	Is the backup equipment and facility installed and operated to provide the VoIP service continuously when there is the power interruption or line problem?

Table 3. Dropped items after SMR (27 items)

Classification		Contents
Technical	Network Security	Is the system to monitor and manage the VoIP traffic operated?
		Is there a bypass route considering emergency situation?
		Is the technology to respond to DoS/DDoS attack applied to ensure service availability?
		Are the voice and data network physically or logically separated?
		Is the access by the unauthorized VoIP terminal and equipment blocked?
	Terminal Security	Are the firmware and applications of the terminal regularly updated?
	VoIP Equipment Security	Are the installation of backdoor and hacking agent and activation of unneeded service checked?
		Is the access control technology of personal information DB and processing system applied?
		Do the VoIP switching systems apply the authentication mechanism to authenticate the users and terminals?
		Is the default passwords of the administrator changed immediately? Are the changed passwords difficult to infer?
		Are the logs of administrator, system, and abnormal activities kept and regularly inspected?
		Are the security patches of the equipment regularly updated?
		Is the encryption of voice and data provided?
Managerial Inspection	Security Organization Setup and Operation	Is the information security organization consisting of information security officer, information security manager, and information security coordinator operated?
		Is the organization staffed with people who can yield the emergency measure authority in the case of accident?
		Is the manager overseeing the information security duty assigned?
	Security Planning Establishment and Management	Is the information security practical guidance specifying the detailed methods and procedures of managerial, technical and physical protective measures of information and communication equipment and facility established?
		Was the practical guide approved by the CISO, and is it revised when there are the changes like the legislation or replacement of equipment?

	Manpower Security	Is the access privilege to the accounts and records immediately removed when an employee is transferred or retired?
		Are the members of information security protection organization and employees regularly trained regarding information security?
		Is the security pledge demanded when a third party employee is involved in the work?
	User Protection	Are the users continuously provided of information concerning accident warning, security vulnerability and etc.?
	Response to Accident	Is the response plan to accident containing the accident definition and scope, response system, response method and procedure, and so on established and executed?
	Inspection	Does the information security officer inspect the information security status according to the guide each year?
Physical Inspection	Others	Does the VoIP service provider's security policy include the case of using the software or Web interface for VoIP system management?
		Is the stored information safely deleted when the medium containing the important information is disposed?
		When disposing the storage unit containing the important information such as the user's personal information, is the recorded information completely deleted and confirmed to be unrecoverable before the unit is physically disposed?

4.2 AHP result

Based on hierarchy tree as shown in **Fig. 1**, we calculated the weight of each indicators through questionnaire survey. The questionnaire survey is carried out targeting 15 security experts during one month (2012.9~2012.10). The 15 security experts consist of 10 VoIP service carriers and 5 security consultants. They not only have an impressive academic and business background but they have an ability to influence decision making for VoIP service.

After questionnaire survey, we collected 15 answer sheets and selected 13 answer sheets after calculating the CR value of each answer sheet. And we calulated weight of indicators using geometic mean with 13 answer sheets. We analyzed the CR value of merged data using Expert Choice 2000, especially analysis function for group determination. The CR value was 0.02 and we verified that the response was within the level of significance [17]. When we synthesized all elements using Expert Choice, we obtained the relative importance shown in **Fig. 2**. Considering technical, managerial and physical aspects, 'locking system for access control' and 'integrated management system of VoIP security equipment' are relatively important among indicators. It means that specialists for information security are highly considered as key factors for constructing a secure VoIP environment.

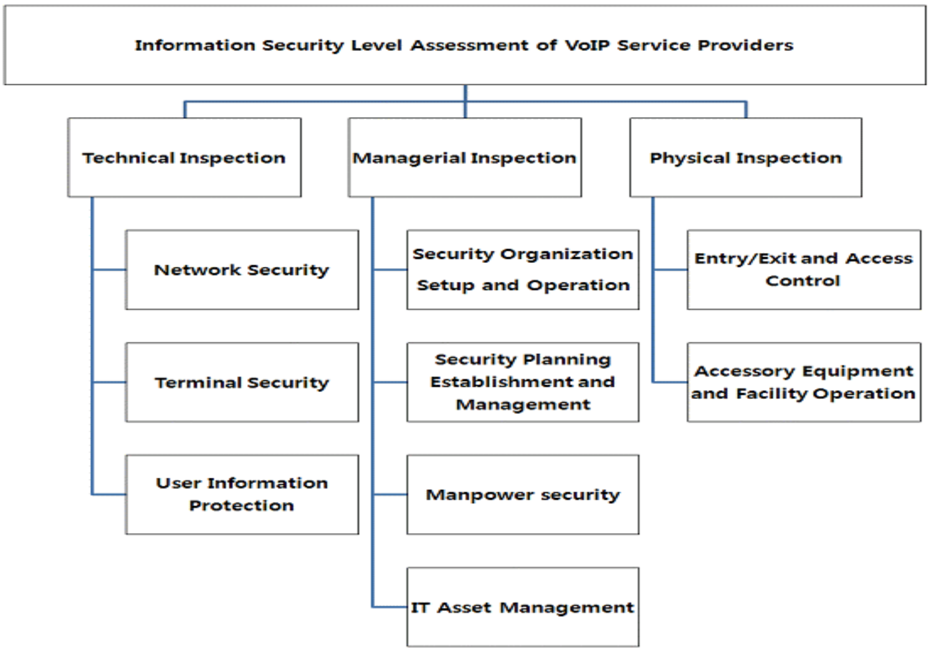
Information Security Level Assessment of VoIP Service Providers
Technical Inspection
Managerial Inspection
Physical Inspection
Network Security
Terminal Security
User Information Protection
Security Organization Setup and Operation
Security Planning Establishment and Management
Manpower security
IT Asset Management
Entry/Exit and Access Control
Accessory Equipment and Facility Operation

Fig. 1. A hierarchy tree for Information Security Level Assessment for VoIP service providers

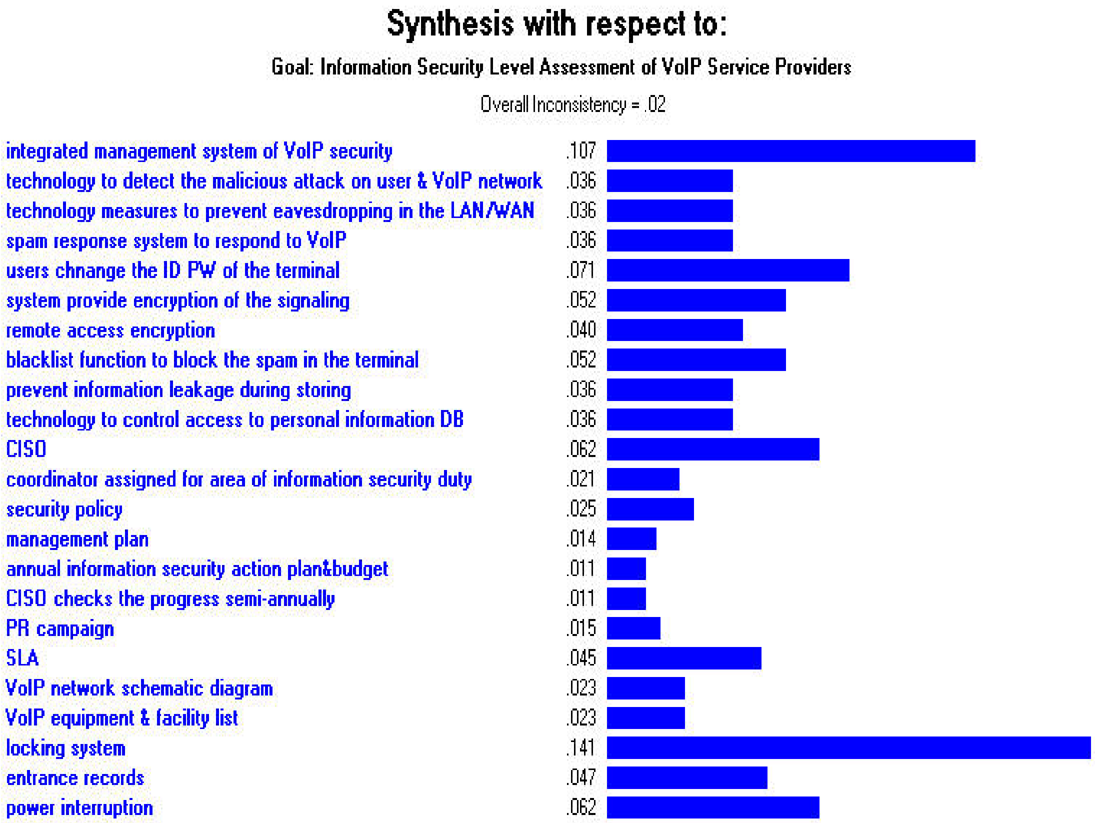

Fig. 2. Synthesis for the problem of Information Security Level Assessment of VoIP Service Providers

Table 4 shows the priority orders of indicators regarding opinions of VoIP security experts. In terms of the weight factor for each indicator, Network Security, Terminal Security, and User Information Protection were the highest for technical inspection indicators respectively.

Security Organization Setup and Operation, Security Planning Establishment and Management, Manpower Security and IT Asset Management were the highest for managerial protective measure respectively. Entry/Exit and Access Control and Accessory Equipment and Facility Operation were the highest for physical protective measure respectively.

In case of technical inspection, an indicator - Is the integrated management system of VoIP security equipment? - is the highest order among indicators. It means that it is important to operate the integrated management system such as ESM for preventing incidents targeting VoIP. In the case of managerial inspection, an indicator - Is a Chief Information Security Officer (CISO) assigned? – is highest the order among indicators. It means that the will of top management is important to establish and operate the security policy. In the case of physical inspection, an indicator - Is the locking system installed so that unauthorized people cannot enter? - is the highest order among indicators. It means that it is important to detect and block the unauthorized person for preventing VoIP facilities. This indicator is also the hightest order between all indicators.

Table 4. The analysis result of priority order between indicators

Classification		Indicators	Priority Order (Classification)	Priority Order (All)
Technical Inspection (0.500)	**Network Security (0.429)**	Is the integrated management system of VoIP security equipment? (0.500)	**0.215 (1)**	0.107 (2)
		Is the technology to detect the malicious attack on users and VoIP network applied? (0.167)	0.072 (6)	0.036 (11)
		Are the technical measures to prevent eavesdropping in the LAN/WAN zone applied? (0.167)	0.072 (6)	0.036 (11)
		Is the spam response system to respond to VoIP spam deployed? (0.167)	0.072 (6)	0.036 (11)
	Terminal Security (0.429)	Can the users change the ID/PW of the terminal? (0.330)	0.142 (2)	0.071 (3)
		Does the system provide encryption of the signaling and media data? (0.241)	0.103 (3)	0.052 (6)
		When an administrator logs in remotely, is encryption or login channel protective technology applied? (0.188)	0.081 (5)	0.040 (10)
		Is the blacklist function to block the spam in the terminal provided? (0.241)	0.103 (3)	0.052 (6)
	User Information Protection (0.142)	Is the security technology applied to prevent information leakage during storing or transfer of the personal information? (0.500)	0.071 (9)	0.036 (11)
		Is the technology to control access to personal information DB and processing system applied? (0.500)	0.071 (9)	0.036 (11)

Managerial Inspection (0.250)	**Security Organization Setup and Operation (0.330)**	Is a Chief Information Security Officer (CISO) assigned? (0.750)	**0.248 (1)**	0.062 (4)
		Is a coordinator assigned for each area of information security duty? (0.250)	0.083 (4)	0.021 (19)
	Security Planning Establishment and Management (0.241)	Is the information security policy containing the goal, scope, and responsibility of information security established? (0.409)	0.099 (3)	0.025 (16)
		Is the plan approved by management? (0.241)	0.058 (6)	0.014 (21)
		Is the current year's information security action plan containing the budget and schedule based on the policy? (0.175)	0.042 (7)	**0.011 (22)**
		Was the action plan approved by management and does the CISO checks the progress semi-annually? (0.175)	0.042 (7)	**0.011 (22)**
	Manpower Security (0.241)	Is the PR campaign (distribution of information security practical guide, etc.) carried out so that employees would be aware of the information security? (0.250)	0.060 (5)	0.015 (20)
		When consigning the IT operation to a third party, are reflected in the security contract or SLA? (0.750)	0.181 (2)	0.045 (9)
	IT Asset Management (0.188)	Is the VoIP network schematic diagram generated and revised when there have been changes? (0.500)	0.094 (9)	0.023 (17)
		Is the VoIP equipment and facility list (including the usage and location) generated and managed? (0.500)	0.094 (9)	0.023 (17)
Physical Inspection (0.250)	**Entry/Exit and Access Control (0.750)**	Is the locking system installed so that unauthorized people cannot enter? (0.750)	**0.563 (1)**	**0.141 (1)**
		Are the entrance/exit records kept for at least one month? (0.250)	0.188 (3)	0.047 (8)
	Accessory Equipment and Facility Operation (0.250)	Is the backup equipment and facility installed and operated to provide the VoIP service continuously when there is the power interruption or line problem? (1.000)	0.250 (2)	0.062 (4)

5. Conclusions

This study selected 50 items, organized them into a hierarchy, and verified suitability and validity of evaluated items using the objective method of survey of service providers and security experts. And then we drew 23 indicators and calculated the weight of each indicators using Analytic Hierarchy Process (AHP).

To summary the result, it is important for VoIP security to operate the integrated management system, assign Chief Information Security Officer (CISO), and install the locking system for preventing the unauthorized people.

Since VoIP service uses the existing IP environment, it is vulnerable to various security problems of the IP environment. Leakage of confidential information through eavesdropping of the call is particularly one of the critical security issues, and it requires special protection. To do so, application of VoIP security protocol is essential. The number of users of VoIP service is expected to rapidly increase in the future because of its low cost and the proliferation of various types of devices supporting VoIP. For such increasing VoIP service users, not only must the security measures of existing vulnerabilities of VoIP services be developed but also the security technologies to cope with newly appearing attacks.

In future study, the validity of the study result needs to be improved by conducting face-to-face interview or exploratory research such as observation in parallel, and then comparing the results.

References

[1] D. Kim, "Analysis of Game Theoretical Effect of Internet Telephone (VoIP) Quality Assurance Policy and Number Transfer Policy," Business Research, Vol. 38, No. 1, pp. 35~49, 2009.

[2] IDC Korea, http://www.idckorea.com/product/Getdoc.asp?idx=544&field=PressRelease.

[3] Korea Communication Commission and Korea Internet & Security Agency, "VoIP Security Guideline," 2007.

[4] Turoff, M. "The policy delphi. In the delphi method: Techniques and applications," 2002.

[5] S. Yoon, H. Park, and H. Yoo, "Factor Analysis of VoIP Security Checklists using AHP," Journal of the Korea Institute of Information Security & Cryptology, Vol. 22, No. 5, pp.1115~1122, 2012.

[6] P. Samarati and S. Vimercati, "Access control: Policies, Models, Mechanisms", Lecture Notes in Computer Science, vol. 2171, no. 137, 2001.

[7] L.A. Gordon and M.P. Loeb, "The economics of Information Security Investment," ACM Transactions on Information and System Security, vol. 5, no. 4, pp.438-457, Nov. 2002. Article(CrossRef Link)

[8] D. Richard Kuhn, Thomas J. Walsh, Steffen Fries, "Special Publication 800-58: Security Considerations for Voice Over IP Systems," National Institute of Standards and Technology, Jan 2005

[9] L.D. Bodin, L.A. Gordon and M.P. Loeb, "Evaluating Information Security Investments Using the Analytic Hierarchy Process," Communications of the ACM, vol 48, pp. 79-83, Feb, 2005. Article (CrossRef Link)

[10] Korea Communication Commission and Korea Internet & Security Agency, "Information Security Check Service Manual," 2012.

[11] Rainer Falk and Steffen Fries, "Security Governance for Enterprise VoIP Communication," Emerging Security Information, Systems and Technologies (SECURWARE), pp 279-286, 2008.

[12] A.B., Cisco IP Telephony Security Framework, Cisco Press, 2012.

[13] T.L. Saaty, The Analytic Hierarchy Process, McGraw Hill, New York, 1980

[14] H. Jung, "A study on importance on Evaluation Index of Personal Information security using AHP," J Korean Data Anal Soc vol.12 no.3 (B) (Jun. 2010) pp.1499-1510, 2010.

[15] T.L. Saaty and G.V. Luis, "Diagnosis with Dependent Symptoms: Bayes Theorem and the Analytic Hierarchy Process," Operation Research, Vol. 46, No. 4, pp491-502, 1998. Article (CrossRef Link)

[16] Fornell, C., Larcker, D.F., Journal of Marketing Research, VOL.18 NO.1 pp39-50, 1981.

[17] H. Kong, T. Kim, J. Kim, "An analysis on effects of information security investments: a BSC perspective," Journal of Intelligent Manufacturing, Vol. 23, No. 4, pp.941-953, 2010. Article (CrossRef Link)

Seokung Yoon received his Bachelors degree in Industrial Automation Engineering in 1998 from Inha University and his Masters degree in Computer Science and Engineering from Inha University in 2003. Since August 2006, Mr. Yoon is a general researcher at KISA (Korea Internet & Security Agency). His current research interests include security of IT convergence services and applications.

Haeryong Park received his BS degree in Mathematics from Chonnam National University, Korea, in 1999. In 2001, he received his MS degree in Mathematics from Seoul National University, Korea. In 2006, he received his PhD degree in Information Security from Chonnam National University, Korea. He is a manager of Information Security Technology Team at Korea Internet & Security Agency (KISA). His current research interests include the design and analysis of cryptographic algorithm and the security of IT convergence services..

Hyeong Seon Yoo received his Bachelors degree in Mechanical Engineering in 1974 from Inha University and his Ph.D from Ghent University, Belgium in 1983. Dr. Yoo is a professor in the school of Computer science and information technology at Inha University. His research interests include computer securities, applied cryptography and scientific computations.