International Journal of Security and Its Applications
Vol.8, No.2 (2014), pp.145-156
http://dx.doi.org/10.14257/ijsia.2014.8.2.15

A Practical Decision-Making Model for Security Products Preference

SungJin Kim[1], JunYoung Son[1,2], SeungHun Nam[1*] and ChaeHo Lim[1]

[1]*Korea Advanced Institute of Science and Technology(KAIST)*
[2] *Korea Institute of Nuclear Safety(KINS)*
r3dzon3, jyson13, nam1202, chlim@kaist.ac.kr

Abstract

As many users of electronic devices have demanded security functions for their devices, many security products have been recently developed and released. Only a few products, unfortunately, are selected by users and most of products are disappeared. The kinds and demand-side market of electronic devices have been dramatically increased. And potential users consider various factors when they purchase security products. However, until now, security products have been developed in no consideration of user's selection features with effective evident criteria and that's the reason why most of products are disappeared. Thus this study explores the key factors and preference tendencies that are essentially deliberated when users choose security products. This study provides a decision-making model for software developers, users and market strategist. Also this paper proposes the assessment matrix for measuring the factor level to form the criteria which can be utilized in a security product market.

Keywords: *Security products, User preference factors, Potential user, Decision-making algorithm, Decision-making key factors*

1. Introduction

The preference for security products has been changed in accordance with increased electronic devices and requirements for security [1]. The security product supplier requires data considered the assessment of the potential user preference. It is essentially important for us to find out their preference criteria. There are many assessment criteria related to the security product. Most researches are focusing on evaluation for performance or usability only [2, 5] and the other factors are ignored. To know what are required for users to purchase security products, this study provides test sets and scenarios which can be adopted. There are two groups such as security knowledgeable group and non-knowledgeable group for the survey because we assumed that people have different flavors about selecting products based on security knowledge. Also there might be big different preferences between groups. With the differences on two groups, this study makes three main design goals. This study shows how various purchase factors there are and explore what can be key factors among them. Finally this study suggests a decision-making model and assessment matrix [8].

2. Related Work

In real world, security incidents are frequently mentioned on media and security is considered as a one of priorities in daily life. To resolve the security problems, companies have purchased proper security products to keep security levels reasonably. In previous studies, they have only focused on security performance and usability [3]

[*] The first three authors are contributed equally to this works

ISSN: 1738-9976 IJSIA

[9]. That is, those are considered as factors which lead users to purchase. However it needs to consider various factors including two factors mentioned, and it requires to know how each factors affect for users to purchase. Furthermore, before spending money on a security product, decision-makers want to know that all decision factors are justifiably evaluated.

2.1. Performance Evaluation Standard

In case of performance evaluation, many countries have standardized criteria for security evaluation in their own way such as TCSEC in USA, ITSEC in Europe and CTCPEC in Canada respectively and have integrated it into common criteria. The purpose of this evaluation is to give reliability on security products in terms of performance and products development. Main factors in this evaluation are identification, authentication, reliable channel, user security, resource utilization, security function, privacy, communication in functional requirements for eavesdrop protection, self-security and communication security [6].

2.2. Usability

Usability is attribution on quality that assesses how easy user interface is to use. The word "usability" means the methods to improve ease-to-use in design process [4]. Usability is defined by five quality components: learnability in accomplishment, efficiency in productivity, memorability in proficiency, errors rectification in recovery, and satisfaction in usage. In brief, the definition means that usability requirements are based on measures of users performing tasks with the product to be developed.

2.3. Existing Assessment Schemes

There are many kinds of assessment schemes based on performance: IETF Performance Test Standard, KISA Security Evaluation, Tolly Group, ICSA Labs, VeriTest, NSS. These are focusing on the criteria of the factors based on performance evaluation.

2.3.1. IFTF Performance Test Standard

Standard of information security system performance test proposed by the IETF were established as follows. As evaluation method (RFC 2544) of network interoperability, it exhibits performance test method about throughput, latency and packet loss rate in order to evaluate network device, and presents other test method (RFC 3511) about forwarding, connectivity and filtering in order to evaluate Firewall.

2.3.2. KISA Security Evaluation

As security evaluation methods of information security system, security evaluation of IPS evaluates user data protection, identification and authentication, security management and self-protection. And it evaluates assessment control for data protection, data certification and assessment flow control. Security evaluation of certification evaluates user attribute process, certification and feedback-protection.

2.3.3. Tolly Group Security Evaluation

Tolly Group's evaluation conducts performance test of information communication device. Information security system conducts performance test of anti-virus, firewall, IPS and VPN.

Firewall performance test is divided into network performance and security performance. Network performance evaluates throughput, latency and traffic detection.

2.3.4. ICSA Labs

ICSA is a certification agency which conducts performance test of information security system such as anti-virus, firewall, IPS and VPN. ICSA performance test evaluates reliable authentication, safely remote management, interoperability and firewall module [7].

2.3.5. VeriTest

VeriTest holds the research institute in many countries and has hundreds of experts of performance support. VeriTest performance test is divided into anti-virus and device of web security. Performance test of anti-virus evaluates functionality, performance and user acceptance testing and availability.

2.3.6. NSS Labs

NSS Labs is rating agency which conducts performance test of information security system. This agency evaluates security products such as firewall, IPS, VPN and UTM objectively. NSS Labs gives the product which passed all of performance standard certification mark. Thus, NSS Labs is known for good performance evaluation.

2.4. TCO

Total Cost of Ownership, or TCO, of any information security product purchase consists of more than simply the direct costs of acquisition and maintenance. Advanced flexibility to add new protection capabilities is a fundamental requirement for internet security. The potential cost of a lack of flexibility can show up either as a need for a continuous upgrade of an inflexible solution or, worse, as a security breach due to a lack of protection for a newly discovered exploit [9].

3. Survey Mdeling

Many security products that are unaccompanied by user purchase review emerge in the market, and it leads to concentrate on purchase decision about better security solution. This research helps us a better understanding of the factors influencing purchase decision, and to seek the differences among two different user groups with respect to security knowledge. Generally, the security knowledge influences on applicable ways alternatively in personal or company usage purpose.

The objectives of this study are three goals. First of all, it is aimed to determine the factors influencing security product purchase decision, and the findings are to provide the base factors of product development. Maybe, the basic development of product should be originally distinct between two groups (security knowledge and now-knowledge group) because of key factor's difference. Secondly, it is intended to find out whether there are differences among purchase patterns and utilizes it in marketing strategies and tactics relating to the information given to the factors influencing purchase.[8] Thirdly, we will propose a new model, and in advance, it informs you of that how new security product affects in market before launching.

In the first part of the questionnaire, the potential users are asked whether they have security knowledge and purchase experience or not, and then those who gave

demographic questions are allowed to continue to the rest of survey. We classified the base of the information into two groups: knowledge group and non-knowledge group.

Then, they are asked for following questions as you have switched security products or suppliers, who had switched, are asked to state the reason of why they switched from a previous one and how often you did. If not, the reason why they haven't switched. This question included overall dissatisfaction from the previous one, and reasons other than dissatisfaction to make prominent key factors. In addition, we asked whether you buy a domestic product if the price is lower than global brand and local support is well organized. If possible, which conditions you affects. One of the objectives of this study was to investigate the factors that influence security product purchase decisions. Otherwise, for that purpose, a list of features was stated in the questionnaires, which were gathered from the analysis of previous studies as well as personal interviews with the experts from the sector. The purchasers were asked which factors they consider important elements when they were purchasing security products. They choose key factors among the factor list, and make an order. Then we used a 10-point Likert-scale that is comprised of percent values in order to measure the factors influencing consumers' purchase decisions. Namely, on a scale of 1 to 10 priorities, we requested to define it, being total 100% important weight values. Hence, individual purchasers should make total 100% out of 10 key factors they choose. In addition, each factors lead to a series of small factors, and request same ways to allocate score in order and weight value every factor compartment.

4. Evaluation

This study is about purchase decision on security products such as F/W, IDS/IPS and Anti-virus program. To understand users' attitude towards factors influencing purchase decisions, we performed an empirical study targeting 150 potential users. In order to ensure the validity and accuracy of the questionnaire, we divided potential users into two groups: expert and non-expert on security. This survey mainly focuses on purchasing influence factors from each group. The main purpose of this study is to find important factors which affect to purchase of security product based on users' knowledge degree. To design the questionnaire, this study classified it with three parts. The first part is about the basic conditions of users including their genders, ages, education, security knowledge, security career period, occupation, enterprise size, purchasing experience and purchased product types. Second part is to choose the influencing factors in order of priority when they buy a security product. Each factor in here has detailed factors. The last part is to judge priority of detailed factors by personal comparison. Finally this study asked several questions about switching security products experience and preference between local and global product.

In this survey, 150 questionnaires are distributed and 134 copies are finally collected. We got 120 valid copies from a double check on collected questionnaires since 14 copies were considered as unusable in consequence. The validity ration is 80%. This survey reaches the almost expected goal and the results are consistent with the facts. However, the result of two group is totally different with the other (each other). The following data analysis is based on the 120 valid copies. Of the 120 respondents, approximately 10% were female whereas 90% were male. This result reflected the gender status of working area in security, but not much influence a purchase decision. The age structure of the participants of this survey was as follows: 31.5% of them was between 22-29 year old, 30.2% was between 30-39, 30.8% was between 40-45, and

finally 7.5% was 46 and above. The education level of the respondents was college or above as expected; 84.4% were university graduates or students, and 15.6% had a MA or Ph.D. degree. And 89% of users in this survey have experienced the purchasing of more than 1 time, and they purchased it by same or similar manner. The participants were supposed to decide order of priority on demographic questions and weight values among 84 detailed factors in Table 1.

Table 1. The Factors for Purchasing the Security Product

Factor [# of factors]	**Detailed Factors**
Performance [18]	Efficiency (in response time) / Latency, Packet Loss Rate, Efficiency (in H/W resource usage), Throughput & Data Transfer Rate, Concurrent Session Number, Protocol Support Specification, H/W Specification, Scalability, Integration & Correlation, Deployment Feasibility (including new technology), Protection Capabilities, Detection Rate /Filtering, User Security Functionality, Identification /Authentication, Local / Remote Access Control, Self-Security, Privacy, Cryptography
Monitoring [4]	Real-time Monitoring/Analysis, Analysis Capability, (Integrated) Event Management, Exception Handling, Audit & Log, Report & Statistics Search
Service Consistency [6]	Avoidance of Down/Failure, High Availability (Dualization) & In-line mode, Update/Upgrade Cycle, Reliability (Self Recovery) / (Failure) Data Recovery / Recovery Capabilities, Malfunction Prevention / Operation Safety, Easy Backup
Usability [16]	(Integrated Console) UI & GUI / Control Screen, Intuitive Visibility & First Impressions, Ease of Use, Localization (including Local Language or Language Translation), Customizing, Learnability (in accomplishment), Productivity (in efficiency), Operability (Operation Management), Proficiency in Memorability, Repair-Errors Rectification, Satisfaction or Likeability in Usage, Help (Menu), Documentation, Standardization in Development, Information Providing, Understandability
Management Aspects [3]	Portability-Management Capabilities / Easy Installation / Un-installation / Easy Eradication / Deletion, Compatibility, Data Consistency & Substitutability /Versatility
Reasonable Price [6]	Actual Acquisition Costs, Maintenance Fee, Annual License Fee, Operating Cost, Opportunity Cost, Incident Recovery Cost
Personal Relation [2]	Recommendation by Relatives & Friends, Domestic Product Purchase (by nationalism or preference just in flavor)
Brand Reputation [9]	Commercial Credits (or Reputation / Awareness), Market Share (Distribution Rate & Use Rate), CC & Credential Certificates, Intellectual Property Right (or Patent), Media Public Relations & Advertisement, Revenue for Product Sales, Sales References, Product Winner / Prizes, Business Credit Rate & Status
Customer Service [6]	Maintenance (Vendor Support Capability) / Benefit of Quality Support, Product Information Providing (information opening & easy understanding) / Easy Information Acquisition Access, Technical Transfer, Quality Warranty, Available Engineers Numbers, Endurance (for consistent support)
Law Regulation [1]	Compliance of Law (Satisfaction of Security Law & Regulation)

In a recent study, we examined factors influencing in purchase behavior, and found that security solution purchasing have a more positive attitude towards performance and brand reputation rather than price and customer service. Figure 1 shows performance, brand reputation and service consistency are important factors for knowledgeable group when they purchase products.

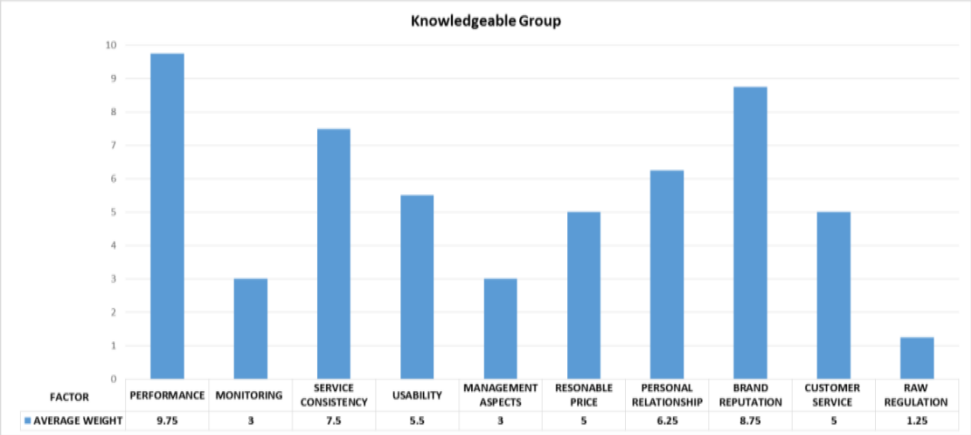

Figure 1. The Surveyed Factors for Purchasing Security Products by Knowledgeable Group

Figure 1 illustrated the distribution of factors by the respondents of the survey. In other words, the frequency of key factors used by the respondents can be summarized as follows: 9.75 performances, 8.75 brand reputations, 7.5 service consistencies, 6.25 personal relationships and 5.5 usability based on 10. It means that 97.5% of respondents chose a performance at most important factor and 87.5% of them chose a brand reputation in 2nd key factor.

Hence, the high-factor demand affects an enterprise's product decision, which is fundamentally the basic consideration for an enterprise choosing the security product. And that is also the marketing strategy and tactics for security developers and sales managers. However, security products are even far away from these circumstances. Security developers don't design well at the beginning phase and not planned as well in this aspect. Accordingly, the plan in development must focus on the user's flavor. Additionally, an enterprise's marketing should take the consumer as the core. By studying the influencing factors of consumer behaviors, the enterprise can identify the user demand, enhance the factors that promote their purchasing, and change unfavorable factors, taking the satisfaction of them as the start point and ultimate goal of marketing behaviors. Only by providing high-quality performance products, by increasing brand values, by satisfying unstop service, by maintain relationships between decision-makers and providers, by elevating usability needs, a product provider can earn more consumers, and decision-makers will gradually accept your selling approach. Accordingly, which kind of factors are the key ones affecting their purchasing, and how to affect their minds and behaviors, and as forming a theoretical proposal, we can effectively promote their purpose [10]. On the other hand, Figure 2 shows non-knowledgeable group considers reasonable price, performance, usability and service consistency as important purchase factors. Especially service consistency purchasers had worried about conflict or collision with other software. The result of the survey is followed below.

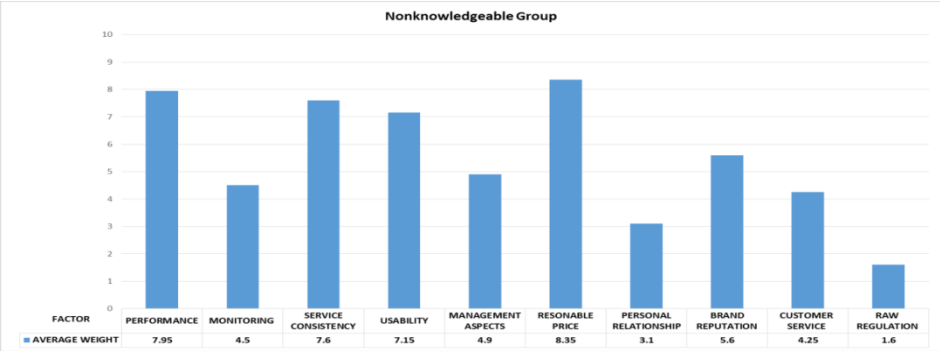

Figure 2. The Surveyed Factors for Purchasing Security Products by Non-Knowledgeable Group

Besides, Understanding the user attitudes of two different groups plays an important role when implementing marketing and development strategies in effective and feasible reaction to client retention. Furthermore, it is also crucial to understand whether there are differences among these groups in terms of the factors affecting their future purchases as purchasing same manner. From two graphs, the characteristics of user's non-knowledge on the product also affect to purchase with the competitive price as core impact factors. The results show that the pleasure of purchasing is originated from which factors, and have a great influence on the purchasing intention of users. This introduces the individual characteristics of purchasers, including security knowledge, price, usability and so on. The results also show the purchase difference between two groups on novel concepts to build new model, and effectively explain the intention of applying the needs. To build a conceptual analysis model for influencing factors of purchasing and performs an empirical analysis based on date of offline/online survey. The research emphasizes the pattern of various factors on purchasing activities, including economical features, quality characteristics, and personal flavors except demographic/geographic factor. We also introduce the new predictable diffusion model of the security solution in security market before releasing its product beforehand with arithmetic formula. This model generates a large positive effect on actual behaviors by a direct and indirect way. It can decrease risk significantly before launching the security product, which can produce a huge repressive effect on actual behaviors. The purchasing behavior patterns have very conventional time to time.

5. Assessment Modeling

An alternate approach is to find detailed factor from the subset of factors to extract comparably meaningful results. Each point values represent detailed factors and are calculated by multiplying the value of priority for factor, weighted value of factor and weighted value of detailed factor. Figure 3 demonstrated that several factors were at high value, while the rest of them showed up trivial. And 65% of detailed factors influence less in purchasing decision. It was also noteworthy to mention that all the features of 35 % listed in the survey were considered important by the respondents since some features of both performance and personal relationship were highest impacts such as H/W specification, throughput, concurrent session, packet loss rate in behalf of performance and recommendation of relatives or friends in retailer's marketing.

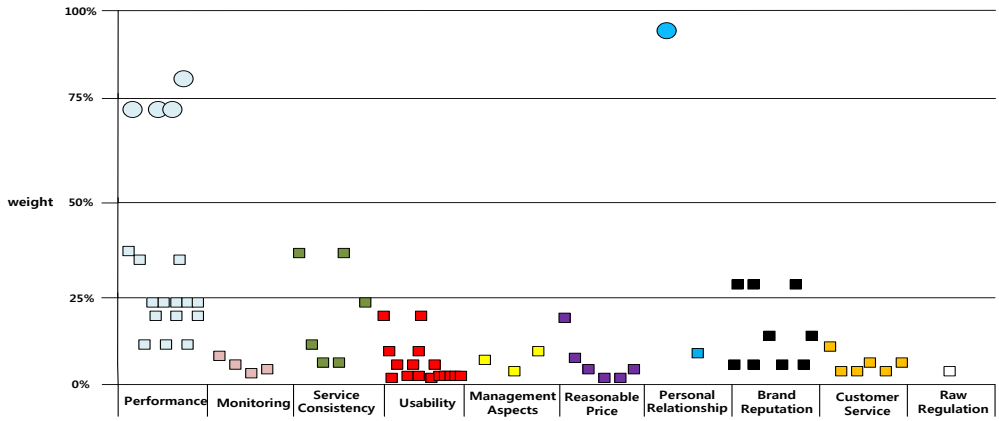

Figure 3. The Surveyed Factors for Purchasing Security Products by Non-Knowledgeable Group

The formulas to analyze Figure 3 to make user select the best security product are following (1). M_s is sum of the high selected preference factors for analyzing on Figure 3. To select the best security products, W_n represents the n-th value of priority for factor. This element builds that the more preferred factor can be weighted. F_n is the weighted value for factors to make the values standard number, from 10 to 1. And S_n is the weighted value of user's preference for detailed factors. M_{ave} is the average of the M_s. The higher M_{ave} value has, the more users purchase. The criteria for considering how many factors are included to produce the product will be selected by decision making model. In decision making model, M_{ave} is the indicator how well the criteria is decided.

$$M_s = \sum_{n=1}^{n_c} W_n \times F_n \times S_n, \; M_{ave} = \frac{M_s}{n_c}. \qquad (1)$$

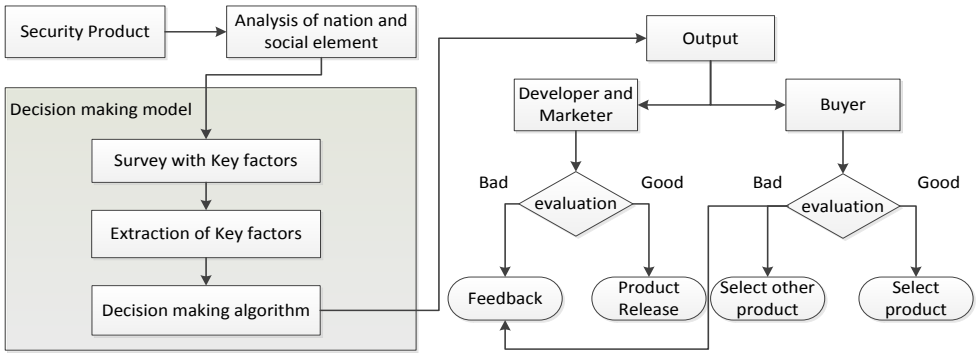

Figure 4. Decision Making Model

This study proposes effective decision making model. This decision making model, shown in Figure 4, focuses on the factors which affect purchasing security product. Decision making model includes survey, key factor extraction and decision making algorithm. Through this model, user, developer and marketer are able to decide their opinion rationally. Especially developer can find that which factors locate high priority and develop security products in consideration of user's preference tendencies. The

questionnaires also indicate different aspects in terms of the product selection that participants want to purchase. In Table 2, many users chose a foreign product in Firewall rather than domestic ones. It was because the products they chose were suitable with their prerequisites such as high performance and consistency. Normally, if Firewall has a lack of reliability to support business contingency, it is really serious. Downtime is increased and business is downed. Accordingly, they need a product related to high performance and business reliability.

Table 2. Key Factors based on Product Selection Preference

Product	Firewall	IDS/IPS	Web F/W
Purchaser Preference	Foreign Product	Domestic Product	Both of Foreign / Domestic Product
2013' Market Share	Foreign Product Preference	Domestic Product Preference	Both is very competitive
Main Issues for Purchase	High Performance, Consistency	Detection Rate, Local Support	High Performance, Local Support
Purchase Reasons	excellent performance, global brand reputation, good service consistency	good performance, good brand reputation, strong personal relation, excellent usability, strong local support, good service consistency	excellent performance or good performance, strong local support or good service consistency

In reality, many foreign products showed high qualities in BMT (Bench Mark Test). However, in behalf of IDS, participants also desire a strong local support like rule updates. Hence, even if a domestic product is less qualified in performance, participants want strong relation with maintainer to assist the product. Besides, web firewall coexists in performance and easy accessibility to the local support. The product that satisfies two conditions will be selected by purchaser. From the reasons, both of domestic and foreign products are selected at similar rate.

6. Conclusion

Studies on users' purchasing behaviors are useful in security field. It is important for both groups, knowledgeable and non-knowledgeable group, to recognize differences of product purchase decision factors. This issue is related with users' preferences on purchase/upgrade/change security products and that is important for product producers. This study is limited for security field to adopt and for the factors influencing user's purchase decisions in this market. This methodology, however, can be widely used in decision-making. The result in this survey proves that purchasing factors determines user's actual behaviors to purchase the security products they want. The main driving factors for knowledgeable group are the performance, brand reputation, nonstop service of inner security. On the other hand, price and usability are main factor for non-knowledgeable group. And this paper explores a number of techniques that can be used to measure value for purchasing decision within security products. This study proposes new decision-making methodology for decision-makers, marketers and developers respectively to suggest direction and strategy on security. Developers should develop security products with consideration on view differences between knowledgeable group and non-knowledgeable group. Also marketers should do marketing recognizing what main factors to buy products are. This study suggests quantitative criteria to measure security product value. There is no standard technique for quantitatively measuring

security product value, and those criteria might have different direction because different culture and social effect decides different purchase factor. Thus this paper suggests standard evaluation model and algorithm which can be adopted for various nations. The features should be emphasized on security product development and strategy of security market. It is important to recognize what main purchase factors are and how to overcome weakness points that security industry has because purchase preferences is related to security industry.

References

[1] P. An Wang, "Information Security Knowledge and Behavior: An Adapted Model of Technology Acceptance", (ICETC), **(2010)**.
[2] P. An Wang, "Assessment of Cyber security Knowledge and Behavior: An Anti-phishing Scenario", International Conference on Internet Monitoring and Protection (ICIMP), **(2013)**.
[3] P. An Wang and E. Nyshadham, "Knowledge of Onli-ne Security Risks and Consumer Decision Making: An Experimental Study", (HICSS), **(2011)**.
[4] Nielsen Norman Group, http://nngroup.com/articles/usab-ility-101-introduction-to-usability/.
[5] S. M. Furnell, P. Bryant and A. D. Phippen, "Assessing the security perceptions of personal Internet users", Computers & Security, vol. 26, no. 5, **(2007)**, pp. 410-417.
[6] M. M. Eloff and S. H. von Solms, "Information Security Management: An approach to combine process certification and product evaluation", Computer & Security, vol. 19, no. 8, **(2000)**.
[7] L. Birdwell, http://www.ontrack.co.uk/special/ICSAlabs_VirusSurvey2004.pdf.
[8] J. Bau and J. C. Mitchell, "Security Modeling and Analysis", Security & Privacy, IEEE, **(2011)**.
[9] Check Point Software Technologies Ltd.: The Seven Key Factors for Internet Security TCO, **(2003)**.
[10] S. Kim, J. Son, S. Nam and C. Lim, "An Effective Analysis Model following the selection criteria on the preference for Security Product", (ASTL-series / SERSC), **(2013)**.

Authors

Sung Jin Kim is currently a PhD student at KAIST. He received the BS and MS in computer science from Ohio State University and Sogang University respectively. His current research interests include various security issues such as malware, early warning system, forensic, big data analysis, risk analysis, and protection system.

Jun Young Son is now an Engineering Staff of the KINS (Korea Institute of Nuclear Safety). He received the BS degree from Kyungpook National University, Daegu, Korea, and the MS degree from the University of Science and Technology (UST), Daejeon, Korea. And He is in course of Doctor Degree in KAIST(Korea Advanced Institute of Science and Technology), Daejeon, Korea. He has been involved in studies on mobile and wireless communication field since 2007. And He has been involved in system and cyber security & cryptography field and developed a security chip since 2009. His current research interests are the cyber security of nuclear power plant Instrument & control system and SCADA systems, embedded system, wireless & mobile communication.

Seung Hun Nam is received the Bachelor's degree from Dongguk University in seoul, major in information communication engineering. He is currently a graduate student of the Dept. of Computer Science at Korea Advanced Institute of Science and Technology. His research interests are multimedia forensics and multimedia security.

Chae Ho Lim is a professor at KAIST from 2010. He received his PhD in Computer Science from Hongik University in 2001. He received my MS and BS degrees in Computer Science from Konkuk University and Hongik University in 1990 and 1986. His research areas are various security fields such as ISMS, risk analysis, malware detection and security policies.