Enhancement of Usability of Information Security Systems

Gwang-Il Ju
Dept. of Scienct and Technology Cyber Security Center
Korea Institute of Science and Technology Information
Daejeon, Korea
e-mail: kiju@kisti.re.kr

Hark-Soo Park
Dept. of Scienct and Technology Cyber Security Center
Korea Institute of Science and Technology Information
Daejeon, Korea
e-mail: hspark@kisti.re.kr

***Abstract*—An information security system can be divided into the administrator mode and the user mode, in terms of its interface. This research can provide a way to achieve effective results in terms of compliance with security policies through division. In this paper, we propose a human-centric security system which is based on user-centered security (User eXperience) interface. In particular, this study divides the user layer by profiling using the UX methodology's personalization method. Based on this, we apply the information security system on a scenario-by-scene basis, and prepare the factors that could cause difficulties in advance. The information security system was able to confirm the increase of the management level in terms of security policy compliance at the user side, resulting in insight from various HCI (Human Computer Interaction)s standpoints. This can lead to meaningful results that future users can reference in information security systems that they can directly control.**

Keywords- Usability; Compliance; Information Security System.

I. INTRODUCTION

With the performance improvement in computing infrastructure and the increase in its complexity, there have been numerous studies on how to solve the difficulties users face in HCI (Human Computer Interaction) and the need for a solution to the complexity from the perspective of the human factor. A security system officer needs to pursue user-personal security and help users feel comfortable with security. According to the 'Psychology of Security for the Home Computer User' released at the IEEE Symposium [1], the current approach to security is not appropriate because it overlooks the ease of use. In addition, the paper 'The Weakest Link Revisited [2]' written on IEEE Security & Privacy read that the weakest point from a corporate security standpoint is the user. In other words, making security more convenient for users can significantly upgrade a corporate security level.

In this way, information security is approaching the service concept for user's efficient business performance from the aspect of enterprise business. This study aims to present the direction of an effective information security system by analyzing the result when the user improves usability through information security as a service concept.

II. RELATED WORK

In terms of a study on HCI approach from the perspective of information security, the NIST [3] has developed a framework which can reduce user errors in a control system from the usability standpoint. The framework provides a common language and mechanism for organizations to: (1) describe current cybersecurity status; (2) describe their target state for cybersecurity; (3) identify and prioritize opportunities for improvement within the context of risk management; (4) assess progress towards the target state; (5) foster communications among internal and external stakeholders.

L. Jean Camp [4] suggested the privacy and mental model for security (Figure 1). This model is used for the effective communication regarding the environmental aspects of risks and is operated to handle misinterpretations for complicated risks. It cannot take care of everything, but can help users have a better understanding using a certain model. It is applicable to physical security, medical infections, criminal behavior, economics failure and warfare.

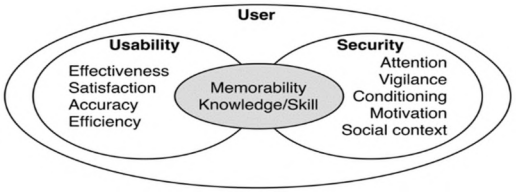

Figure 1. Security-Usability Threat Model

HCI security has evolved in a way to strengthen the usability of user application from the perspective of information security. Ronald [5] proposed the Security-usability Threat Model (Figure 1) in consideration of HCI extension in security. This study attempted to discuss its application which can reinforce the usability of a security system based on the HCI user methodology.

D. D. Woods [6] studied information processing by humans in HCI and applied it to system design with a goal of maximizing productivity. It applied organizational information security policy through profiling techniques based on demographic characteristics. This study aimes at classifying users through demographic profiling and then categorizing the effects of information security policy.

 ISBN: 978-1-61208-661-3

In this study, we construct a map by grouping users through user profile and interviewing the subjects, and analyzing key points where users can experience difficulties based on them. Based on this, we formulate the problems that users face and draw the conclusion that a more user friendly information system is needed by applying the solution system.

III. METHOD

A. Information System Profiling

This study attempted to apply the HCI approach based on the diagnosis of the parts which would be handled by users in person in the past from the perspective of user interface in a security system. In particular, it analyzes security system services through profiling and journey maps which can specify target users in terms of user experience.

One obvious approach to synthesizing usability engineering and securing systems is to apply established procedures for enhancing usability to developing on existing secure systems. Techniques for enhancing the usability of software cover a wide range of fields and sophistication [8].

Contextual Design [9] uses in-depth studies of potential users' work habits and needs to determine initial product goals.

Contextual Inquiry [9] provides usability testing on a deployed product, where real users using the system in their daily chores allow observers to record this use.

This study performs a classification through user profiling before launching a case study and then categorizes the type of security users. 'K' is a professional IT research agency in which most users have a high level of knowledge about IT. The age range varied widely. Then, the data was divided into age and amount of information in a 2X2 format and profiled. TABLE I divides the users into the understanding of occupation and IT and the tendency of each. Through this, we aim to utilize the users more sophisticatedly to track the direction they pursue.

TABLE I. INFORMATION SECURITY USER PROFILING

Type	Age	IT Understanding	Security Observance Tendency
Type A	Researcher in his/her 30s	Fast approach to new technology (early adopter), quick to keep pace with current IT trends, with a high level of IT knowledge	Strong resistance against security policy, but no disagreement regarding institutional security policy
Type B	Administrator in his/her 30s	Repetitive tasks, source of a large amount of information	High observance of information security policy
Type C	Researcher in his/her 40-50s	Relatively poor understanding of IT	Hard to apply it to security policy due to multiple work experiences
Type D	Administrator in his/her 40-50s	Very poor understanding of IT	Hard to apply it to security policy due to multiple work experiences

B. Information System Journey Map

A journey map [7] (Figure 2) has been widely used in diverse fields as an analysis technique of user behavior along with scenario mapping. To derive user pain points, it is executed in the following procedure.

While there is no standardized approach or methodology for customer journey mapping, a survey of current practitioners and an evaluation of surrounding literature revealed four universal traits: (1) a team-oriented execution, (2) a highly visual, nonlinear nature, (3) the use of touch-points, and (4) an emphasis on real customers and consumers.

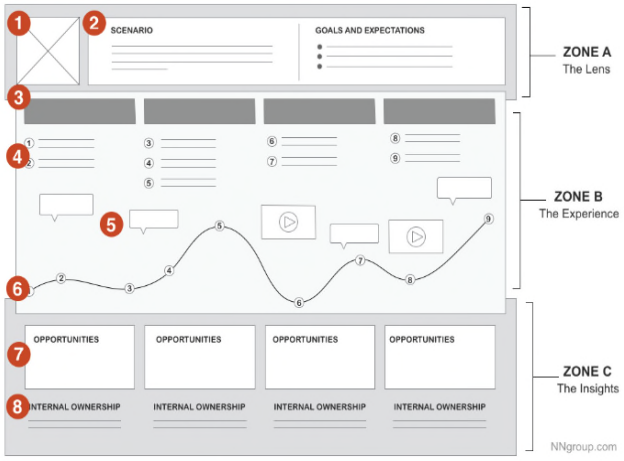

Figure 2. Journey Map (NN Group)

In this study, we made an IS Journey map for the security system (Figure 3) based on the NN group map. As a result, based on interviews with users, we found a point where we can identify their difficulties.

Figure 3. IS Journey Map (for Security System)

C. Change of institutional Security Policy to Journey Map

'K' agency has performed security management in terms of managerial security and technical security. From the perspective of technical security, a centralized security check solution had been applied. In 2015, however, such

policy improved in a way for users to be able to check security indicators in person [10]. This change is significant in two aspects: i) performance improvement after the replacement of old facilities, ii) shift of a security system, allowing a user to control the system in person. See TABLE II.

TABLE II. SECURITY INSPECTION SOLUTIONS

Category	Previous	Now
Manufacturer	'N'	'C'
Year Introduced	2009	2015
Feature	Centralized	User check

Such security policy indicators were applied, focusing on the matters which are directly or indirectly checked by the government bureau during the security inspection period, and the details are in TABLE III.

TABLE III. INFORMATION SECURITY INDICATORS BY CATEGORY

No.	Description
1	Windows login account password
2	Screensaver password
3	Time of screensaver activation (min.)
4	Anti-virus installed
5	Firewalls set
6	Shared folder set
7	Shared folder password
8	Windows security update
9	Local system set
10	Conditions of the unused ActiveX

'K' agency's security policy is organized in a top-down structure in which national and government-led security policies are collectively delivered from the top to the bottom. Therefore, the agencies at the bottom are always under the influence of those on top. To increase the flexibility of institutional security policies, a separate guideline has been prepared to guide the users.

Users were positioned, as shown in Figure 4, to check PC security vulnerability. First, vulnerability was assessed through scores (out of 100 points). It was designed for a central manager to set a target score and make users reach the goal.

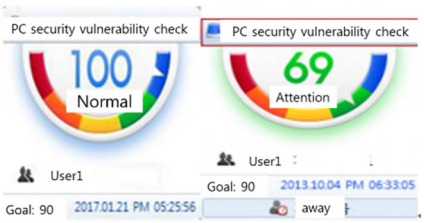

Figure 4. Check on PC Security Vulnerability by Scores

In addition, the level of PC security vulnerability was classified by color to draw more attention from users. The indicators in each sector were designed to be fixed in person and applied as shown in Figure 4. In the case of interface security, which is simply a change of screen, there is a case of studying an efficient method for real-time monitoring of security control [11]. However, below we show examples of user-centered actual measurement and performance.

IV. EXPERIMENTAL RESULTS

According to the application of a new security system, the security policy of 'K' agency has brought the following results in comparison to conventional policies (out of 100 points). While a security level (scores) was low in conventional systems, the related indicators have improved as stated in TABLE IV through the improvement of a security system and provision of user-centered security services.

Score acquisition status was classified by the integration score before (2015), the application year (2016), and the operation (2017) for 1 year after application of security system.

TABLE IV. ACQUISITIONS BY SECURITY INDICATOR

Level	**Before**	Apply	**After**
1	76	77	86
2	45	94	98
3*	47	98	99
4	71	99	99
5	88	98	99
6	79	94	98
7*	79	98	99
8	77	100	100
9*	87	91	91
10	56	65	77
Mean	70.5	91.4	94.6

 ISBN: 978-1-61208-661-3

After the replacement of the security system, the scores improved for most indicators. Until now, the policies have gradually improved. According to the significantly improved indicators, compliance rates have increased, focusing on the indicators which can be applied by users in person after simple settings such as 'screen saver setting'. Then, most indicators were close to a perfect score. Finally, complete content and organizational editing is done before formatting.

The reason why the new system can acquire high scores is that the integration score (Figure 4) can be checked directly, and the user has provided convenience for confirming and taking security measures directly.

Based on the findings above, the following results were obtained:

1) An easy-to-execute security policy was applied with the application of policies by security of user group (profiling).
2) Compliance rates increased after a shift from the conventional centralized policy transferred from a little understanding of security policies to a way for users to check them in person.
3) The difficulties in applying security policies through a journey map were supported in man-to-man format to make them applied more easily.

A security system gains significant improvements after analyzing user experience factors from a security service perspective and applying profiling and user journey map as a way of service methodology. As a result, it was able to derive the following implications on the endpoint of future security systems:

1) Realization of efficient security policies through classification of major risks and vulnerability factors in a collective application of security policies by a policy indicator
2) Shift from the conventional centralized security policy transfer to user-centered security service
3) Better understanding of users with the application of service methodology.

V. CONCLUSION

With the recent increase in security breaches due to the vulnerability of user security, the importance of internal security control aside from an outside attack has become increasingly important [12]. Therefore, this study attempted to derive the applications of a more efficient security system through a better understanding of the users from a security service perspective and service-methodology approach. Escaping from conventional studies which focused on how to reduce user errors from a human factor perspective, this study discussed a way to increase the understanding of end-users.

As a result, it is anticipated that the study results would be useful in analyzing the end users' intention to observe security policies and establish a turning point with the intention to reduce a security system manager's workload. In this paper, we propose to expand the scope of research into a more specific security system by establishing a larger scale and a standard in future research although it is limited in the subject and scale of user profiling. In addition, there might be further studies on the extension of a study scope with more types of specific security systems (user vaccination) or a behavioral analysis on the users' security awareness to provide customized security services by user.

ACKNOWLEDGMENT

This research was supported by Korea Institute of Science and Technology Information (KISTI).

REFERENCES

[1] B. Payne and W. Edwards, "A Brief Introduction to Usable Security", IEEE Computer Society, May, 2008, doi: 10.1109/MIC.2008.50

[2] I. Arce, "The Weakest Link Revisited", IEEE Security & Privacy, April, pp.72-76, 2003, doi: 10.1109/MSECP.2003.1193216

[3] NIST, "Discussion Draft of the Preliminary Cybersecurity Framework", Aug. 2013

[4] L. Camp, "Mental models of privacy and security", IEEE Society on Social Implications of Technology, Vol 28(3), Sep. 2009, doi: 10.1109/MTS.2009.934142

[5] R. Kainda, I. Flechais, and A.W. Roscoe, "Security and Usability:Analysis and Evaluation", International Conference on Availability , Reliability and Security, Feb. 2010, doi: 10.1109/ARES.2010.77

[6] D. D. Woods and E. M. Roth, "Cognitive Engineering: Human Problem Solving with Tools", Human Factors: The Journal of the Human Factors and Ergonomics Society, pp.415-430, 1988

[7] Nielsen Norman Group, "Customer Journey Map", https://www.nngroup.com/articles/customer-journey-mapping/

[8] S. Faily, J. Lyle, Ivan, and A. Simpson, "Usability and security by design: a case study in research and development", Internet Society NDSS symposium, Feb 2015

[9] D. Wixcon, K. Holzblatt, and S. Knox, "Contextual Design: An Emergent View of System Design", in CHI'90 Conference Proceedings, April pp.329-336, 1990

[10] G. Ju, J. Park, W. Heo, J. Gil, and H. Park, "A Study of the Factors Influencing Information Security Policy Compliance", Advanced Multimedia and Ubiquitous Engineering, May, pp. 720-728, 2017

[11] J. Park, S. Kim, S. Ahn, C. Lim, and K. Kim, "A Study on Interface Security Enhancement", KIPS Transactions on Computer and Communication Systems, Vol. 4, pp.171-176, 2015

[12] Ponemon Institute, "Risky Business: How Company Insiders Put High Value Information at Risk", June 2016

 ISBN: 978-1-61208-661-3