Modeling of a Human Decision-Making Process with Prospect Theory

Dongmin Shin[1], Hokyoung Ryu[2], Namhun Kim[3], and Jieun Kim[4]

[1] Department of Information and Industrial Engineering, Hanyang University, Ansan, Korea
[2] Department of Industrial Engineering, Hanyang University, Seoul, Korea
[3] School of Design and Human Engineering,
Ulsan National Institute of Science and Technology, Ulsan, Republic of Korea
[4] Innovation Design Engineering, School of Design, Royal College of Art, England
{Dmshin,hryu}@hanyang.ac.kr,
nhkim@unist.ac.kr, jieun.kim@network.rca.ac.uk

Abstract. The aim of the present study is to examine what rationality conditions are ignored and why it happens when users have more than one dimension in conflict, such as *perceived security* and *usability* in the online banking use experience. In a controlled experiment, thirty subjects used two different online banking authentication interfaces: a fingerprint interface and a normal four-step interface, in a reverse order. The empirical findings revealed that a different combination of rationality conditions was employed based on a change from effortless interaction (e.g., the fingerprint) to effortful interaction (e.g., the four-step logon system) or vice versa. We also provided some design implications for HCI practitioners, and proposed a new approach to evaluate user experiences as there are benefits and drawbacks mixed in user interface design.

Keywords: Prospect theory, Decision making, Perceived security, rational ignorance, user experience.

1 Introduction

HCI practitioners and designers often encounter two or more design factors in conflict. For instance, the aesthetic aspect of design and its relationships to other design dimensions, such as usability and usefulness, have gained significant attention in the design community (e.g., [7]), in particular, when these two or three aspects cannot be in parallel. Recent, the relationship between usability and its privacy concern has also become a focus in social media design (e.g., Facebook). In a similar vein, the friction between user's security and usability in online banking system design has been much in the foreground (e.g., [3,6]). In certain cases, it is necessary, for the purpose of security, to include behavior that is complex. Conversely, it is also possible to weaken the security of a system by simplifying or automating certain elements, which usually improve usability. These mixed interpretations imply that a certain level of in-security (or "un-usability") in a system is inevitable for usability (or security). Online banking users seem to accept a certain level of insecure system for the sake of usability, and vice versa.

P.L.P. Rau (Ed.): CCD/HCII 2013, Part I, LNCS 8023, pp. 459–466, 2013.

However, we do not respond blankly to in-secure or un-usable system. Every such decision involves balancing the uncertain rewards of actions against the potential losses. In particular, many private identity data for enhancing security, this propensity is influenced by the potential rewards of risk taking, and perceptions of the risk are influenced by one's own (or others) experience (or belief) of losses. Hence, unless there is no experience on this matter, people tend to have the propensity to take risks. Several empirical studies, surveys and anecdotal evidences supported this account, emphasizing an apparent dichotomy between perception on security and their actual behavior. In detail, many online banking users are willing to trade security for convenience or bargain the release of personal information in exchange for relatively small gain or benefit such as usability [1,6]. Herley [4] goes further on this, arguing that users rationally reject security advice, because the burden of complying with security procedures often outweighs any gain in protection, because it would be a future benefit rather than an instant reward. Marked interesting is a vast body of economic and psychological literature has already identified several forms of psychological deviations from rationality that affect such irrational decision-making [3,5]. However, HCI designers or practitioners have lacked for applying them to take account of user experience as yet.

A key to the present study is to see an online banking use experience from such psychological deviations that make offset users' rationality conditions, and how they might stand in assessing individual's user experience.

2 Kahneman and Tversky's Prospect Theory and Evaluating User Experience

When people make every judgment, it is virtually impossible to take all variables into account at once. They have certain cognitive limits, such as computational capacity, memory, incomplete information and so forth. This makes them quick decisions using various heuristics, e.g., "good enough" heuristic, which will serve as one of the reference points in the following comparison. In support of Kahneman and Tversky [5]'s prospect theory, many empirical studies have demonstrated an idiosyncrasy between losses and gains in uncertain circumstances.

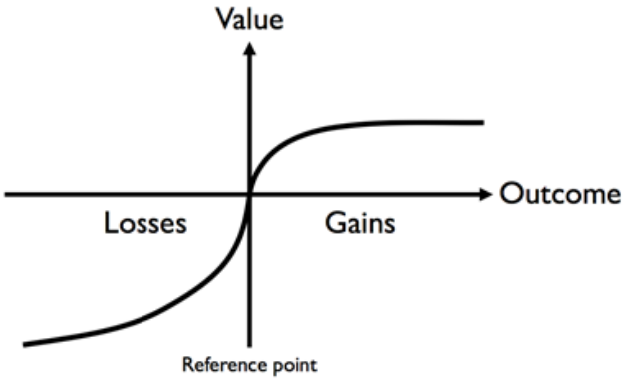

Fig. 1. The Value Function Proposed in Prospect Theory [5]

As depicted in Figure 1, Kahneman and Tversky [5] described the asymmetric valuation of gains and losses, concave for gains and convex for losses, where in general, losses are weighed heavier than gains of the same absolute value. Thus, people are prone to have loss aversion and there is relatively a diminishing sensitivity for higher absolute deviations in gains. One important consequence of loss aversion is the endowment effect and the status quo bias (ibid.). The endowment effect means people are less likely to give up the old benefit against a new one unless it is alarmingly acceptable. This implies that our innate bounded rationality limits our ability to acquire, memorize, perceive and process all relevant information, and it makes us rely on several very simplified mental models, approximate strategies and heuristics. These also suggest that HCI practitioners need to replace theoretical quantitative approaches with descriptive qualitative evaluations, to assess user experiences.

In this context, we carried out an empirical study of online banking system use, which inevitably have two conflicting rationality conditions (i.e., usability vs. security), in which people would assess the loss and gain with a contingent trade-off.

3 An Empirical Study: Online Banking System Design

The experimental setting in the present study deliberately involved two mixed rationality conditions to be used by the participants: security and usability. In so doing, two types of online banking authentication interface were developed: a fingerprint logon (single-step), and an authentication by entering four different personal identity data. It is assumed that each interface has a different level of usability and perceived security. The experiment was to examine changes in user's rationality conditions when they used both, but in a reverse order (i.e., one group used the fingerprint interface first and then the four-step logon, and the other used them in the other way round).

3.1 Method

Participants. Thirty students (15 males, 15 females) in a tertiary institution voluntarily participated in the study, all of whom had no prior experience with any fingerprint systems. We presented them with a simulated online banking system equipped the two ways of authentication (see Figure 2). Half of the participants first used the fingerprint logon system (Figure 2b), and then the four-step logon system (Figure 2a), which included id, password, date of birth, and email address registered by themselves before the experiment (hereafter this is called as Condition I). The other half used both too, but in the reverse order (Condition II).

Apparatus/Procedure/Design. Prior to the experiment, all participants needed to register their fingerprints. In the main experiment, they only needed to scan their index fingertip on the fingerprint reader, which virtually simulates a single-step logon process. Once they used each online banking authentication system and performed several transaction with the two interfaces, all of them rated the two statements on a five-point Likert scale, respectively: "It was easy for me to use the online banking system''; "I would feel totally secure to use the online banking system''. At the end of the experiment, the participants were asked to choose one of them for their preference.

Fig. 2. The four-step (left) and fingerprint (right)

4 Results

Figure 3 showed the tally of preferences of the two interfaces. In Condition I, when participants used the fingerprint first, they seemed to show significant preference of the fingerprint logon interface over the four-step authentication (i.e., 12 of 15 chose fingerprint for their preference). By comparison, the participants in Condition II showed no difference in preference. A chi-square test of this contingency supported this interpretation (p-value ≈ 0.05).

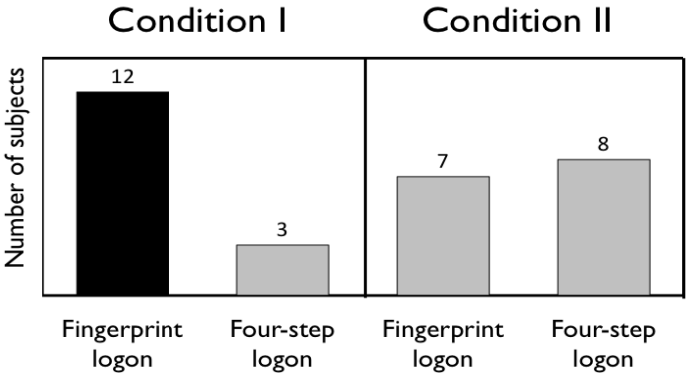

Fig. 3. Preference of the two interfaces

Table 1 detailed the changes in their rationality conditions (security and usability) for the two authentication systems. The subjects who used the fingerprint first (Condition I) seemed to positively rate the perceived security of the four-step logon system (mean 4.20 → 4.53, d'=+0.33), although they poorly rated its usability (mean 4.40 → 2.60, d'=−1.80). That is, the participants in Condition I highly ranked the benefits of the fingerprint interface in terms of the vivid usability dimension, which also implies the rational ignorance on perceived security (this is interesting that our participants did not see the smaller gain of the four-step interface in terms of security).

Table 1. Mean scale ratings (standard deviation)

Condition/Order		Security	Usability
Condition I	1. Fingerprint	4.20 (0.56)	4.40 (0.74)
	2. Four-step	4.53 (0.52)	2.60 (0.63)
	d'	**+0.33**	**−1.80**
Condition II	1. Four-step	4.27 (0.59)	3.93(0.59)
	2. Fingerprint	4.60 (0.51)	4.87 (0.35)
	d'	**+0.33**	**+0.94**

Conversely, with the participants who first used the four-step logon system (Condition II), the fingerprint logon interface was perceived as being more secure (mean 4.27 → 4.60, d'=+0.33), positively shifting the ratings of security. Likewise, they rated the usability of the fingerprint highly (mean 3.93 → 4.87, d'=+0.94). Thus, the sample participants developed their rationality conditions of the fingerprint system in a mixed way based on both usability and security.

5 Discussion

Although statistical comparisons of the two conditions are inappropriate due largely to the order of the systems exposed to our sample population, this trial does demonstrate that the rationality conditions are quite different. We tried to interpret these phenomena according to the systematic psychological deviations from rationality that might affect individual decision-making, and how this understanding can help HCI practitioners to design novel user experiences.

5.1 Loss-Aversion and Rational Ignorance: Condition I

In Condition I, the conversion from the fingerprint logon (effortless interaction) to the four-step logon system (effortful interaction) would make our participants to perceive both gain and loss. From the perspective of gain, only minor increment (+0.33) was observed in security. However, the loss is much greater than the gain (-1.80) in terms of usability. Thanks to this inconsistent prospect, many users would take loss-aversion decision if there are no clear mental models of the gain given. That is the reason behind why the fingerprint interface was preferred by our participants (see Figure 3). The shaded area in Figure 4 confirmed that the motivation of loss has a greater impact than the motivation of gain does, in making a decision on their preference. In particular, even though the four-step interface seems to be more secure than the fingerprint

interface, it can be seen that our subjects consider the gains in security negligible. It might be due to the fact that security is an abstract and future value, which might not be authentic, as people have no such mental models to highly weigh the gain. This consequently demonstrated 'rational ignorance' regarding security, which is in line with Herley's study [4].

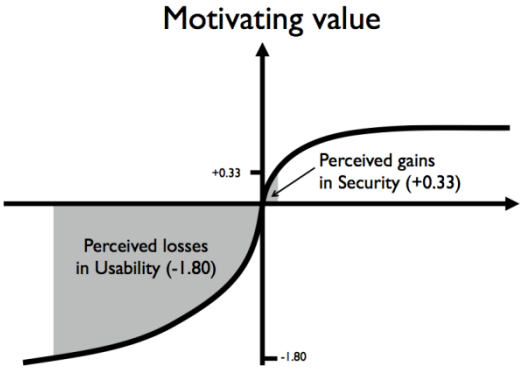

Fig. 4. A comparison of motivational value and the prospect theory of analysis of relationships between perceived security and its usability in Condition 1

5.2 Endowment Effect and Rational Ignorance: Condition II

Condition II can be rather distinctively interpreted. The fingerprint interface was positively rated than the four-step interface in both dimensions. There are extra gains in terms of both security (+0.33) and usability (+0.94) (See Figure 5). However, on the contrary to Condition I, only half of the participants preferred the fingerprint logon experience. This seems to be irrational, because even though the fingerprint use experience was highly rated in both dimensions, our participants did not show any preference to the interface. This interpretation is relevant to user experience change from effortless interaction (e.g., the fingerprint) to effortful interaction (e.g., the four-step logon).

Put it simply, when he or she needs to adopt a new interaction style, she needs to learn the new interaction with effort. Of course, because she is accustomed to the old system, she does not want to use further efforts to adopt the new interaction. Hence, when she needs to adopt the new interaction style, it is highly associated with the decision under risk. If the perceived risk is greater than gain expected, she would be reluctant to take the risk. Otherwise, she will take the new interaction style. That said, our participants in Condition II seem to show risk-aversion thanks to the gains (0.33 for security and 0.96 for usability) from the change negligible and do not mind the complicated logon procedure. This is much in line with endowment effect [3,5] which means that people tend to place a higher value on objects, concepts, and beliefs they already own (in Condition II, the four-step logon user experience) relative to new ones they do not (in Condition I, the fingerprint interface). This case also seems to demonstrate rational ignorance on the extra gains from both security and usability.

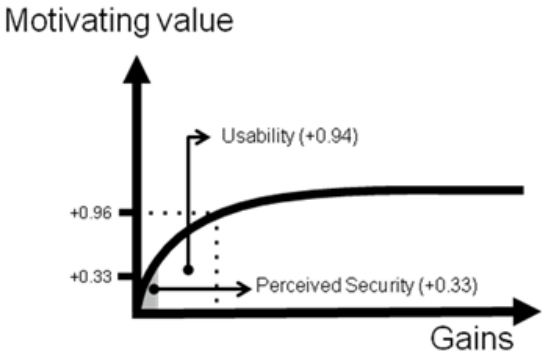

Fig. 5. A comparison of motivational value and the prospect theory of analysis of relationships between the perceived security and usability in condition II

6 Implications for User Experience Design

Experience design is getting tricky due to the fact that individual's decision-making varies depending on their prior experience that is also subjective. In addition, the systematic psychological deviations resulting from loss-aversion and endowment effect [3,5] would cause irrational or biased behaviors that might be quite different from what the designer has originally thought of. Behind this approach, it can be seen that the designer wrongly assumes that users do not possess a set of pre-defined preferences for every contingency of user experience. However, our experiment showed that it is more likely that user's preferences are constructed in the process of making a choice or judgment. That being said, the context and procedures involved in making choices or judgments influence the preferences or preferred experience that are implied by the elicited response. In practical terms, this means that behavior is likely to vary across situations that HCI practitioners might have considered as identical. An evaluation dimension, which is unequivocal in theory, might produce different outcomes if its exposing sequence (in our experimental scope) against other evaluation dimensions influences the evaluation outcome.

For instance, in Condition I, when there is a potential gain in security (even this is an abstract value) by the four-step logon system compared to the guaranteed loss of making the poor-usability decision (this is a concrete value), the twelve users (see Figure 3) would not be much inclined to take the risk (i.e., prefer the fingerprint interface to the four-step one). This means that these users might have status quo bias, and how this bias would be associated with experience design is in urgent need of further investigation by HCI designers. Similarly, in Condition II, the eight users who did not prefer the fingerprint interface, though they saw the gains of the interface, cannot be interpreted by conventional HCI evaluation methods. In this regard, the results imply that users might subjectively perceive both loss and gain although both of them are objectively measured, and their contingent trade-off is much susceptible to rational ignorance, consequently affects what would be shadowed. However, if a clear mental model of gain or loss is sufficiently given, the prospect of the risk can be

re-calculated; then people would re-assess the loss and gain with more rational contingent trade-off. Hence, in experience design, it is first to determine what gains or losses of a design dimension might be rationally ignored by users.

7 Conclusions and Future Works

Based on theoretical principles and empirical findings above, we are currently working toward developing a framework for modeling rationality conditions of user experience. Our preliminary data showed that security and usability attitudes are complex but are also compatible with the explanation that loss aversion and the diminishing sensitivity of a higher absolute value (so that people have rational ignorance on the higher absolute value - status quo) could lead to underestimate security and overestimate usability. In conclusion, we do not support a linear model of user experience to describe individual preference, though we acknowledge that the current experimental setting is somewhat arbitrary and not perfect to pinpoint what user experience would be disclosed by the experimental setting. A further work on individual's biased behavior and the experimental validation are still needed.

Acknowledgments. This work was supported by the National Research Foundation of Korea (NRF, 2011-0028992) grant and Agency for Defense Development.

References

1. Davinson, N., Sillence, E.: It won't happen to me: promoting secure behavior among Internet users. Computers in Human Behavior 26(6), 1739–1747 (2010)
2. Gilovich, T., Griffin, D.W., Kahneman, D.: Heuristics and Biases: The psychology of intuitive. Cambridge University Press (2002)
3. Gunson, N., Marshall, D., Morton, H., Jack, M.: User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. Computers & Security 30(4), 208–220 (2011)
4. Herley, C.: So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. In: Proc. New Security Paradigms Workshop (2009)
5. Kahneman, D., Tversky, A.: Prospect theory: An analysis of decision under risk. Econometrica 47(2), 263–291 (1979)
6. Mannan, M., Oorschot, P.C.: Security and usability: the gap in real-world online banking. In: Proc. New Security Paradigms Workshop, pp. 1–14 (2007)
7. Tractinsky, N., Katz, A.S., Ikar, D.: What is beautiful is usable. Interacting with Computers 13, 127–145 (2000)