Decision Support Systems 53 (2012) 1–11

Contents lists available at SciVerse ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

Security versus convenience? An experimental study of user misperceptions of wireless internet service quality

Byung Cho Kim [a], Yong Wan Park [b,*]

[a] Graduate School of Management of Technology, Sogang University, Seoul 121-742, Korea
[b] Department of Marketing, Pamplin College of Business, Virginia Tech, Blacksburg, VA 24061, USA

ARTICLE INFO

Article history:
Received 23 March 2010
Received in revised form 26 May 2011
Accepted 21 August 2011
Available online 26 August 2011

Keywords:
Information security
Security/convenience tradeoff
Security engineering
Inference making

ABSTRACT

This paper demonstrates that consumers make incorrect inferences about security/convenience tradeoff. We find the evidence that consumers tend to infer unobservable security quality from observable convenience and that their inferences are not always correct. In four studies, we examine user perceptions of wireless Internet service quality, with an aim to understand consumers' irrational choice of a dominated product over a dominant option. Our results indicate that consumers make inference in security from convenience using a zero-sum heuristic and that they believe in improving security in return for losing convenience. In a choice setting, we empirically show that security perception, as well as convenience, influences consumers' product choices, contradicting the common view of existing literature that convenience is the sole driver of consumer choice. Our findings show that spontaneous and extensive education of consumers about security makes a modest impact on their inference making.

1. Introduction

As the Internet becomes a crucial part of our lives, more companies use the Internet for business, resulting in the transmission of large amounts of data including countless online transactions. Accordingly, security becomes a critical success factor for online business and electronic commerce. The Obama administration has put a priority on securing cyber space and digital infrastructure, as has been seen in the government's recent cyber security efforts, including creation of a top position charged with protecting online security [10]. Microsoft has been committed to making a joint industry–government effort to fight against security threats. Despite these efforts made by both the government and the industry sectors, cyber security still remains poor in quality. According to 2008 CSI Computer Crime and Security Survey, computer viruses were identified as the most frequent security incidents which occurred at almost half (49%) of the respondents' organizations, followed by insider abuse (44%) and theft of laptops or other mobile devices (42%).

While the technical problems have been argued to be the main contributors to poor security, some researchers have a different view. They believe that the problem lies in the economic and behavioral aspect of security. Existing studies with economic perspectives mainly focus on firm-side security issues such as the effect of security breach announcements on market value [6,33]. Other researchers have established theoretical foundations that explain consumer-side causes of poor security. The literature on consumer-side security identifies lack of appreciation of secure and safe systems and the low demand for security to be the main contributors to poor network security [25]. Recently, researchers have paid more attention to psychological aspects of security that may explain consumers' insufficient incentive for security. D'Arcy et al. examined the impact of user awareness of security countermeasures on the misuse of information systems and found that the network users' poor security awareness and their misuse of technology result in poor cyber security [11]. Ng et al. identified the factors that influence a user to practice computer security grounded on a model adapted from the healthcare literature [26].

In this paper, we study the psychological aspect of security from a different angle. We investigate how consumers make inferences about unobservable security quality from observable convenience of information goods and services and how consumers' perceived quality affects their choices. We then examine the impact of educating consumers about security on their inference making process. Finally, we discuss the managerial and policy implications of consumers' perception about security/convenience tradeoff.

Security and convenience are two distinct quality dimensions based on which consumers evaluate information goods, as stated in Bill Gates' famous memo[1] [15]. It is widely believed that there is a tradeoff between security and convenience, that is, enhanced security in return for increased inconvenience. For example, since 9/11, as a process

* Corresponding author.
E-mail addresses: kkbbcc@gmail.com (B.C. Kim), ywpark@vt.edu (Y.W. Park).

[1] "We've done a terrific job at that, but all those great features won't matter unless customers trust our software. So now, when we face a choice between adding features and resolving security issues, we need to choose security."

0167-9236/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.dss.2011.08.006

required to increase airport security, every traveler in the United States has experienced a painful and inconvenient security check from simple metal detection to privacy-invasive full body scanners. While this security/convenience tradeoff generally holds for most cases of physical security, advanced technology sometimes achieve enhanced security without losing much convenience for some information goods. One example is Hypertext Transfer Protocol Secure (HTTPS) which is a combination of the Hypertext Transfer Protocol with the Secure Sockets Layer/Transport Layer Security (SSL/TLS). The operators who want to create a secure channel over an insecure network such as online banking sites provide an HTTPS connection which significantly improves security without even being noticed by most users. A secure virtual private network (VPN) can be another example. A secure VPN provides better security by using encryption based on cryptographic tunneling protocols. All users need to do is click once to turn on the VPN. In most cases, these secure options are offered to users at no additional cost, but providers often struggle with low level of usage unless these secure options are made to be the only available choice.

Grounded on well-established theory in psychology and marketing literature about inference making process, we test our premise that consumers have a tendency to make incorrect inferences about security quality from convenience features. We argue that consumers are in favor of enhancing security in return for losing convenience even though advanced technology could improve both security and convenience without requiring any additional cost for certain information goods and services as in the aforementioned examples. Our study is motivated by consumers' irrational product choice, which is often observed in the information goods market. That is, even when one product is superior to another in both convenience and security dimensions and both are provided at the same price, some consumers choose a dominated product over a dominant option. This phenomenon cannot be explained by existing studies. In this paper, we aim to provide a theory that explains why consumers may prefer a dominated product to a dominant one grounded on the literature of psychology and marketing.

In four studies, with a focus on wireless Internet service, we investigate how consumers make inferences about two different quality dimensions of information goods and services: security and convenience. In Study 1, with a between-subjects design, we find that consumers underestimate security quality of a dominant product (i.e., an option with better security and better convenience), but they calibrate their perception when additional information is presented. Surprisingly, there is no difference in convenience rating between a dominant product and a dominated one. In Study 2, we present descriptions of both products to consumers concurrently (i.e., within-subjects design) and ask them to rate security and convenience. The study shows that the dominant product's security rating is lower and its convenience rating is higher than that of the dominated option. We observe the same pattern even when the product description clearly states that security of the dominant option is enhanced. The results support our argument that consumers incorrectly infer unobservable security quality from observable convenience feature by using compensatory inference. In Study 3, we extend our argument to the choice setting. Our findings indicate that consumers' perception of both security and convenience drives their choice. Consistent with the previous two studies, their misperceived security quality leads to the consumers' choice of the dominated product while correctly perceived convenience drives their choice of the dominant one. Interestingly, we found no significant impact of consumer knowledge about technology on their choice. In Study 4, we investigate whether educating consumers is effective in terms of correcting consumers' misperception of security quality. It turns out that spontaneous and extensive education about security makes an impact on consumers' inference making process. Although the impact is marginal, providing detailed description of security aspect of the product at the time of choice may be an effective way to have them make a rational choice of the product.

The present paper makes contributions to the literature in the following ways. First, our study extends compensatory inference to IT product category. The characteristics of IT products are different from traditional product categories, so the value parity could be violated by advanced technology, which explains why a dominant product and a dominated option co-exist in the IT product market. Second, we find the evidence that consumers make inferences about security quality from convenience because convenience is observable but security is not. Even when consumers compare a dominant product with a dominated option, their preferences are affected by security/convenience tradeoff. Consumers' misperception of security quality would dampen motivations of information goods providers to enhance the security of their products. Third, our results show that both security and convenience drive consumer choice, which contradicts the general view of the existing studies in computer science and software engineering that only confirms the effect of convenience. The validated impact of security perception, combined with the incorrect perception of security/convenience tradeoff provides explanation for consumers' irrational choice behavior.

Our findings have practical implications for information goods providers and policy makers. First, our results imply that there may exist an optimal level of convenience, which may signal sound security to consumers. Thus, the optimal strategy may be to offer a certain level of procedural complexity instead of perfect convenience which may mislead consumers. Second, not only enhancing security quality but also educating consumers about security so that they correctly perceive and appreciate improved security is a key success factor for business. Finally, from a policy perspective, setting minimum security quality standards would be desirable for certain information goods or subsidizing providers who educate consumers about security may be a welfare-enhancing strategy in the sense that information providers can be better motivated for security development.

This paper is organized as follows. In the next section, we review the literature, followed by a theoretical background based on consumers' inference making. Then we present a series of four studies and our findings, followed by general discussion. Finally, we provide managerial implications of our findings.

2. Literature review

While a large volume of literature has exclusively studied information security from a technological perspective, a growing body of literature is looking at information security problems through an economic lens. Anderson argues that failure in providing individual users with the incentive for security leads to poor security [1]. For example, Internet users are concerned only about protecting their machines, not the entire network that can be harmed by exploitation of individual personal computers with insufficient protection. August and Tunca examine individual users' incentive under costly patching and investigate different security patch management policies in the presence of negative network externalities [3]. Their results indicate that subsidy-based patching is better than mandatory patching. Kannan and Telang investigate whether markets in vulnerabilities can work better than intermediaries like CERT [21]. They find that CERT brings higher social surplus than the unregulated market. Arora et al. model the optimal timing of vulnerability disclosure and show that the vendor's disclosure timing affects both patching speed and quality [2]. Cavusoglu et al. examine the impact of vulnerability disclosure on firms' performance and find that announcements of security breaches hurt the market value of the breached firms [6]. Cavusoglu et al. investigate how vulnerabilities should be disclosed in order to minimize social loss [7]. They find that the disclosure of vulnerability without ensuring patch release may not be socially beneficial. Telang and Wattal show that vulnerability disclosure negatively affects the market value of software vendors and that vendors' failure to provide timely patches makes situations even worse [33]. Zhao et al. examine the efficiency of