Appl. Math. Inf. Sci. 6 No. 1S pp. 249-255S (2012)

Applied Mathematics & Information Sciences
An International Journal

E-commerce Client-side System Security: The Government Regulation Issue in Korea

Min Hong[1] and Eunjin Kim[2*]
[1]Department of Computer Software Engineering, Soonchunhyang University, Korea
Email Address:mhong@sch.ac.kr
[2]Department of International Industrial Information, Kyonggi University, Korea
Email Address:ejkim777@kgu.ac.kr

Received: Received May 02, 2011; Revised July 25, 2011; Accepted September 12, 2011
Published online: 1 January 2012

Abstract: As criminal activities that target the client-side system of e-commerce increase, client-side system security becomes an issue of government regulation in Korea. To enhance client-side system security, the Korean government requires e-commerce firms to provide client-side security mechanisms to consumers and to force consumers to install such security programs. In this study, we investigate whether such government policy is desirable. With an analytical model, we show that such policy benefits e-commerce firms. Besides, it is shown that firms have an incentive to invest more for client-side system security mechanisms under such policy. However, the policy is shown to worsen consumer welfare with depriving consumers an option not to deploy inconvenient security mechanisms. Still, such policy is socially desirable under the condition where the security breaches incur relatively high costs to e-commerce firms.

Keywords: Government policy, e-commerce, client-side system security

1Introduction

Information security is the protection against security threats that are defined as a circumstance, condition, or event with the potential to cause economic hardship to data or network resources in the form of destruction, disclosure, modification of data, denial of service, fraud, waste, and/or abuse (Kalakota and Whinston, 1996; Belanger et al., 2002). Nowadays, security threats have become more and more important to e-commerce firms. In 2008, the private information of 10 million customers of Internet Auction, which is eBay's South Korea unit, was leaked through hacking attacks. This private information included IDs, passwords, and social security numbers. In 2010, Shinsegae, one of the biggest Korean retailers, issued a statement of apology after data on 3.3 million customers was stolen from its online shopping mall. In 2011, Nate and Cyworld, two major Korean online community sites, announced that the private information of their 35 million users had been hacked. This is currently known as the worst security breach occurred in Korea. Now, users of Nate and Cyworld are making their efforts to file lawsuits against the two sites over the leakage of their private information. As shown in these cases, security related crimes expose e-commerce firms and consumers to a greater security

* **Corresponding Author: Eunjin Kim, ejkim777@kgu.ac.kr**

risk which can incur financial and non-financial losses (Singh, 2007).

To reduce risks to be exposed to security related crimes, e-commerce firms have deployed many security measures. Such security measures include the technological solutions for encryption and authentication – the application of a mathematical algorithm to a message in order to scramble that message, which makes it difficult to view the information without an authorized key, and technological solutions for protection – such as firewall technologies to prevent unauthorized attacks or intrusions (Belanger et al., 2002; Chellappa and Pavlou, 2002). In deploying security measures, it has been known that e-commerce firms have for the most part focused on the security of the server side and on network security (McCullagh and Caelli, 2005). This makes criminals to concentrate more of their crime activity upon the client side system of e-commerce, which remains relatively weak (McCullagh and Caelli, 2005). For the most part, criminal activities that target client side system of e-commerce have taken the form of phishing scams, trojan horse software, and spyware software (McCullagh and Caelli, 2005; Singh, 2007).

In Korea, a serious security breach of Internet banking occurred in 2005 by attacks on the client side of the system (Singh, 2007). A 20 year old hacker attached hacking software to a message he planted on a community Internet site. A victim clicked on it and inadvertently downloaded a key stroke logging program that enabled the hacker to gain the passwords and security codes for the victim's bank account. Using the victim's information, the hacker stole 50 million won (approximately 5 million US dollars) from the victim's account. After the incident, the Korean government enhanced regulation regarding the security of the client-side system of e-commerce (Ministry of Information and Communication of the government of South Korea, 2005; Kim et al., 2010).

However, as e-commerce firms enhance client-side system security and forcing consumers to install security plugins or to deploy security mechanisms, they also inconvenience consumers (Kim et al., 2010). It has been noted that downloading security plugins takes a fair amount of time (Kim and Jung, 2010). Besides, recent survey results show that even though 58.3% of respondents said that the most important reason they prefer Korean Internet banking services was "I feel more secure," more than 30% of respondents answered that the most significant reason that they feel uncomfortable using the Korean banking services was that the system is complicated and slow (Kim et al., 2010). Hence, Kim et al. (2010) insisted that even though such security plugins can improve the level of security, a more user-friendly system should only recommend security plugins and allow users to decide whether or not to install them.

While government regulations regarding client side system security are still under debate, there has been no theoretical analysis to the best of our knowledge. In this study, we investigate the impact of such regulations on e-commerce firms, consumers, and the society as a whole. With an analytical model, we show that such policy benefits e-commerce firms. Besides, it is shown that firms have an incentive to invest more for client-side system security mechanisms under such policy. However, the policy is shown to worsen consumer welfare with depriving consumers an option not to deploy inconvenient security mechanisms. Still, such policy is socially desirable under the condition where the security breaches incur relatively high costs to e-commerce firms.

The rest of the paper is organized as follows. In section 2, we present a review of the literature. We describe the model in Section 3. We then analyze the model and discuss our findings in Section 4. We conclude our research in the final section.

2 Literature Review

Internet has changed the way of making transactions. Consumers' intention to have online transactions has long been studied from several perspectives. Research on consumer attitude showed that there are several factors predetermining a consumer's attitude towards online transactions such as a person's demographic, motivation and prior experience of computers and new technology (Laforet and Li, 2005). Karjaluoto et al. (2002) found that highly educated, young and wealthy people with good knowledge of computers tend to conduct more online transactions. This phenomenon has been well known as the digital divide. To bridging such divide, governments in many countries have made continuous efforts.

As the digital divide has been bridged and the Internet penetration rate has increased, more and more people have conducted online transactions. However, at the same time, privacy and security breaches have increased. It is shown that information security perceived by consumers has significant influence on the level of trust perceived (Flavian and Guinaliu, 2006). Trust – which is

defined as a willingness to rely on an exchange partner in whom one has confidence – is further known to influence consumers' reluctance to have online transactions (Belanger et al., 2002). Hence, maintaining high level information security is important to promote consumers to have online transactions.

To maintain certain level of information security, many countries have enforced a number of policies for privacy and security protection (Wu et al., 2011). Especially, among countries, Korea has had some unique policies regarding client-side system security (Kim et al., 2010). From 1999, the Korean government has mandated all encrypted online financial transactions to be based on electronic signatures enabled through a public-key infrastructure that only works with plugins (Kim et al., 2010). Besides, other security plugins for firewall and keystroke encryption have been further required to be installed (Ministry of Information and Communication of the government of South Korea, 2005). However, such plugin installation is known to inconvenience consumers (Kim et al., 2010; Kim and Jung, 2010).

Previous research on the technology acceptance model showed that perceived ease of use has significant impact on users' intention to have online transaction (Pavlou, 2003). Hence, we can infer that such regulation dismotivates people to have online transaction. Based on the online user survey result, Kim et al. (2010) also showed that such regulation is not desirable for consumers. However, the effects of such regulation on e-commerce firms and on the society as a whole were not shown in the previous studies. Besides, the theoretical framework that allows us to analyze the overall impact of such regulation was not suggested. In this study, we intend to fill this void with developing a theoretical model for the comprehensive analysis of the effects of such government regulation.

3The Model

It is assumed that an e-commerce firm gets a benefit, the average amount of which is a, from serving a consumer online. However, if a security breach occurs for a consumer's account due to criminal activity targeting the client-side system, it incurs cost c to an e-commerce firm on average, which includes financial and non-financial costs such as loss of reputation. An e-commerce firm can reduce the probability of the occurrence of such security breaches through investing in and providing security plugins or mechanisms to consumers for the client side system. We assume that the investment cost $f(s)$ is an increasing, continuous function of the quality of security plugins or mechanisms, s, where the marginal investment cost is increasing in quality s. That is, $f(0)=0, df(s)/ds \geq 0, d^2 f(s)/ds^2 > 0$. For simplicity, we assume $f(s)=s^2$.

In the market, there exist consumers who consider using the e-commerce firm and the total number of consumers is normalized as 1. We assume that a consumer gets a benefit, the average amount of which is b, from using services of the e-commerce firm. However, if a consumer is exposed to a security breach due to criminal activity targeting the client-side system, such a security breach incurs cost k on average to a consumer. When a consumer uses services of an e-commerce firm without installing the security plugins or deploying the security mechanisms provided by an e-commerce firm, he or she will be exposed to a security breach with probability α. The probability of a consumer to be exposed to a security breach due to criminal activity targeting the client-side system is affected by the amount of skills and knowledge that a consumer has regarding how the Internet operates, how to set the browser's privacy and security options, how to recognize phishing emails and spoof web sites, how to limit surreptitious gathering of personal information and behavior patterns, and how to clean the computer system from parasite applications, viruses and worms (Cullen, 2008). While a consumer who has sufficient knowledge and skills is expected to have a low probability to be exposed to a security breach, a consumer who lacks such knowledge is expected to be exposed to a security breach with higher probability. It is assumed that α, the probability that a consumer is exposed to a security breach, is uniformly distributed on the interval [0, 1].

The probability of a consumer to be exposed to a security breach can be reduced with a consumer installing security plugins or deploying security mechanisms provided by an e-commerce firm. The higher the quality of security plugins or mechanisms, the lower the probability of a consumer to be exposed to a security breach. We assume that the probability of a consumer to be exposed to a security breach when a consumer installs the security plugins or deploys the security mechanisms is a function of the α and the quality of security plugins or mechanisms, s. The probability of a consumer to be exposed to a security breach when one installs the security plugins or deploys the security mechanisms, $g(\alpha, s)$

is a decreasing, continuous function of s, where the marginal impact on the decrease in the probability is decreasing in quality s. That is,
$g(\alpha,0)=\alpha, \partial g(\alpha,s)/\partial s \le 0, \partial^2 g(\alpha,s)/\partial s^2 > 0$.
For simplicity of the analysis, we assume $g(\alpha,s)=\frac{\alpha}{s+1}$.

Even though a consumer can expect to lower the probability of being exposed to a security breach with installing the security plugins or deploying the security mechanisms, installing such security plugins or deploying the mechanisms incurs inconvenience costs to a consumer. As an e-commerce firm tries to provide higher security level with higher quality security plugins or mechanisms, it might require more time to download plugins or lock consumers into a particular platform, and hence incurs more inconvenience to consumers. It is assumed that the inconvenience cost for a consumer when installing plugins or deploying the mechanisms is rs where r is coefficient.

To investigate the effect of the government regulation that forces consumers to deploy security mechanisms for client side system security on e-commerce firms, consumers, and the society as a whole, we compare the following two cases. Case 1 is forcing consumers to install or deploy security measures, and case 2 is allowing consumers to determine whether or not to install or deploy security measures. In either case, if an e-commerce firm sets s to 0, it becomes a case of not investing in and not providing security plugins or mechanisms. Hence, in our model setting, an e-commerce firm only needs to choose among the two cases that provide a higher profit at the level of s^* (where $0 \le s^*$) that maximizes the profit.

4 Analysis

Case 1)

When $r>0$, the utility that a consumer can get from using e-commerce services with the security plugins or deploying the security mechanisms is

$$U_{I|r>0} = b - rs - \frac{\alpha}{s+1}k$$

A consumer chooses to use e-commerce services when $U_{I|r>0} \ge 0$. From the utility function, we can derive as

$$n_{case1|r>0} = \min\{\max\{\frac{(b-rs)(s+1)}{k}, 0\}, 1\}$$

Profit of an e-commerce firm is

$$\pi_{case1|r>0} = n_{case1|r>0}a - c\int_0^{n_{case1|r>0}} \frac{\alpha}{s+1} d\alpha - s^2 \quad (1)$$

The consumer surplus in this case is derived as

$$CS_{case1|r>0} = \int_0^{n_{case1|r>0}} (b - rs - \frac{\alpha}{s+1}k) d\alpha \quad (2)$$

The social welfare is

$$SW_{case1|r>0} = CS_{case1|r>0} + \pi_{case1|r>0} \quad (3)$$

Case 2)

In this case, a consumer can determine whether or not to install the security plugins or to deploy the security mechanisms when a consumer uses e-commerce services. If a consumer installs the security plugins or deploys the security mechanisms, the utility is

$$U_{I|r>0} = b - rs - \frac{\alpha}{s+1}k$$

If a consumer chooses not to, the utility is $U_N = b - \alpha k$. A consumer chooses to install the security plugins or to deploy the security mechanisms if $U_{I|r>0} \ge U_N$ and $U_{I|r>0} \ge 0$. A consumer chooses not to when using e-commerce services if $U_{I|r>0} < U_N$ and $U_N \ge 0$. Hence, when $s \le \frac{b-r}{r}$ satisfies, consumers whose α is under the condition $\frac{1}{k}(r+rs) \le \alpha \le \frac{(b-rs)(s+1)}{k}$ choose to install the security plugins or to deploy the security mechanisms. Consumers whose α satisfies the conditions $\alpha < \frac{1}{k}(r+rs)$ choose not to install or deploy them. When $s > \frac{b-r}{r}$, no consumers who choose to use e-commerce services install or deploy them. Therefore, only the consumers whose $\alpha < \frac{b}{k}$ use e-commerce services without installing or deploying them.

Hence, we can derive the demand as

$$n_{case2|r>0} = \min\{\frac{(b-rs)(s+1)}{k}, 1\} \quad \text{when } 0 \le s \le \frac{b-r}{r}$$

where $b > r$.

Profit of an e-commerce firm is

$$\pi_{case2|r>0} = n_{case2|r>0}a - c\int_0^{\frac{1}{k}(r+rs)} \alpha d\alpha - c\int_{\frac{1}{k}(r+rs)}^{\min\{\frac{(b-rs)(s+1)}{k},1\}} \frac{\alpha}{s+1} d\alpha - s^2 \quad (4)$$

Consumer surplus is derived as

$$CS_{case1|r>0} = \int_0^{\frac{1}{k}(r+rs)} (b - \alpha k) d\alpha - \int_{\frac{1}{k}(r+rs)}^{\min\{\frac{(b-rs)(s+1)}{k},1\}} (b - rs - \frac{\alpha}{s+1}k) d\alpha \quad (5)$$

When $s > \frac{b-r}{r}$ where $b > r$ or when $s \ge 0$ where $b \le r$, we can derive the demand as $n_{case2|r>0} = \frac{b}{k}$.

Profit of an e-commerce firm is

$$\pi_{case2|r>0} = n_{case2|r>0}a - c\int_0^{n_{case2|r>0}} \alpha d\alpha - s^2 \quad (6)$$

Consumer surplus is derived as

$$CS_{case2|r>0} = \int_0^{n_{case2|r>0}} (b-\alpha k)d\alpha \quad (7)$$

The social welfare is

$$SW_{case2|r>0} = CS_{case2|r>0} + \pi_{case2|r>0} \quad (8)$$

Proposition 1. An e-commerce firm can generate larger profit with the government regulation that forces consumers to install the security plugins or to deploy the security mechanisms.

Proof. $\pi_{case1|r>0} - \pi_{case2|r>0} \geq 0$ for all possible $s\ (\geq 0)$.

Since installing the security plugins or deploying the security mechanisms incurs inconvenience to consumers, smaller number of consumers will use e-commerce services if they are forced to deploy security mechanisms for the client side system security. Hence, if an e-commerce firm only considers the number of consumers that the firm can attract, it could be better to allow consumers to choose not to deploy client side system security mechanisms. However, when such an option is allowed as in case 2, not all consumers who use e-commerce services install the security plugins or deploy the security mechanisms. This makes consumers who do not choose to install or deploy security mechanisms to be exposed to a security breach with higher probability. As shown in our results, this further incurs more loss to an e-commerce firm. Hence, from an e-commerce firm's perspective, it is better with the government policy that forces consumers to install security plugins or to deploy security mechanisms.

Proposition 2. Consumer surplus is smaller with the government regulation that forces consumers to install the security plugins or to deploy the security mechanisms.

Proof. $CS_{case1|r>0} - CS_{case2|r>0} \leq 0$ for all possible $s\ (\geq 0)$.

Unlike an e-commerce firm, it is shown that consumers are worse off when they are forced to install security plugins or to deploy security mechanisms than the case when they are allowed to not install or deploy them. Hence, the government policy that forces consumers to install or deploy security mechanisms is not desirable for consumers.

Proposition 3. If $c \geq k$ (if $c < k$), social welfare is larger (smaller) with the government regulation that forces consumers to install the security plugins or to deploy the security mechanisms.

Proof. For all possible $s\ (\geq 0)$,

$$SW_{case1|r>0} - SW_{case2|r>0} \geq 0 \text{ if } c \geq k.$$

As shown in proposition 1 and 2, while the government policy that forces consumers to install the security plugins or to deploy the security mechanisms benefits e-commerce firms, it worsens consumer surplus. Then, is such policy socially desirable or not? Our result shows that when the cost incurred by a security breach and imposed upon an e-commerce firm is higher than the cost imposed upon a consumer, forcing the consumers to install the security plugins or to deploy the security mechanisms is socially desirable.

Proposition 4. With the government regulation that forces consumers to install the security plugins or to deploy the security mechanisms, an e-commerce firm maintains a higher quality level of security plugins or mechanisms for the client side system security.

Proof. For all possible $s\ (\geq 0)$,

$$\frac{d\pi_{case1|r>0}}{ds} - \frac{d\pi_{case2|r>0}}{ds} \geq 0.$$

As shown in Proposition 1, with the given quality level of security plugins or mechanisms, an e-commerce firm can expect larger profits when forcing consumers to install the plugins or to deploy the mechanisms compared to the case when not forcing them. Hence, when an e-commerce firm can force consumers to deploy security mechanisms, an e-commerce firm can expect larger increases in profits with additional investment in security plugins or mechanisms. Hence, the government policy that forces consumers to install the security plugins or to deploy the security mechanisms promotes e-commerce firms to invest more for the security mechanisms for the client side system.

Proposition 5. An e-commerce firm does not maintain socially desirable quality level of security plugins or mechanisms for the client side system security even with the government regulation that forces consumers to install the security plugins or to deploy the security mechanisms.

Proof. For case 1, $\frac{d\pi_{case1|r>0}}{ds} - \frac{dSW_{case1|r>0}}{ds} \geq 0$ when $r \geq \frac{b}{2}$, or when $r < \frac{b}{2}$ and $s^*_{case1|r>0} \geq \frac{1}{3r}(b-2r)$. Under such conditions, an e-commerce firm over-invests compared to the socially desirable level. When $r < \frac{b}{2}$ and $s^*_{case1|r>0} < \frac{1}{3r}(b-2r)$, $\frac{d\pi_{case1|r>0}}{ds} - \frac{dSW_{case1|r>0}}{ds} < 0$. If such a condition satisfies, an e-commerce firm under-invests compared to the socially desirable level. Such a condition is satisfied when r is small so that

$r < \min\{\frac{b}{2}, \frac{2k}{a}, \frac{1}{a}(\frac{1}{2}\sqrt{16abk+16k^2+a^2b^2}-\frac{1}{2}ab-2k),$
$\frac{1}{c}(ak-\frac{1}{2}bc+\frac{1}{2}\sqrt{8ck^2-4abck+b^2c^2+4a^2k^2})$

Otherwise, when r is not small, an e-commerce firm over-invests compared to the socially desirable level.

For Case 2, $\frac{d\pi_{case2|r>0}}{ds}-\frac{dSW_{case2|r>0}}{ds}\geq 0$ when $s^*_{case2|r>0}\geq\frac{1}{3r}(b-r)$. If such a condition satisfies, an e-commerce firm over-invests compared to the socially desirable level. When $s^*_{case2|r>0}<\frac{1}{3r}(b-r)$, $\frac{d\pi_{case2|r>0}}{ds}-\frac{dSW_{case2|r>0}}{ds}<0$. That is, an e-commerce firm under-invests compared to the socially desirable level. Such a condition is satisfied if $r<\frac{2k}{a}$. When $r\geq\frac{2k}{a}$, an e-commerce firm over-invests.

An e-commerce firm does not fully consider the consumer benefit and cost of installing the security plugins or deploying the security mechanisms in determining its level of investment in the security plugins or mechanisms. Our results show that when consumer inconvenience cost is high, the consumer cost of installing or deploying security measures is not fully considered by an e-commerce firm. Therefore, an e-commerce firm over-invests compared to the socially desirable level. When the consumer inconvenience cost is low, an e-commerce firm does not fully consider the consumer benefit and makes an underinvestment in security mechanisms. Since an e-commerce firm intends to under-invest or over-invest compared to the socially desirable level, a government might need to become involved to force an e-commerce firm to invest at the socially desirable level.

5Conclusion

As security threats targeting the client-side system of e-commerce increase, security on the client-side system gains importance. Especially in Korea, the government strongly requires consumers to deploy security protection measures for the client-side system. However, deploying such measures incurs inconvenience to customers.

In this study, we show that consumers are always better when they are allowed to decide whether or not to install such security plugins or to deploy certain security mechanisms. Unlike Korea, many other countries allow consumers to decide in deploying client-side security measures. Our result shows that these countries can make consumers better off. However, allowing consumers to decide is not always socially desirable. The government needs to consider both consumers and firms and to maximize the overall welfare. Our result shows that forcing consumers to install or to deploy security measures is socially desirable when the security breaches incur relatively high cost to e-commerce firms compared to consumers. Still, there is an issue to solve. In the real world context, calculation of the cost imposed on consumers and firms is not easy. For the calculation, it is needed to verify who is responsible for the occurrence of the security breaches. Besides, since the stolen personal information is often used in unpredicted manner, it is hard to expect how much consumer costs will be incurred. Hence, the appropriate calculation measure is required in optimizing the policy.

Our result also shows that firms have an incentive to invest more for client-side system security mechanism under the government policy that enforces consumers to install security plugins. Still, to make firms to invest in client-side system security mechanism to the socially desirable level, further government involvement is desirable.

Regardless of our contribution, there are some limitations of our research. There exist other factors not considered in this study. Regarding regulations for information privacy, which are closely related to information security issues, previous studies have shown that the amount of government involvement is related to the cultural values and individual information privacy concerns (Milberg et al., 1995; Milberg et al., 2000). Hence, we can expect that other various factors impact on information security policies and regulations of e-commerce firms and governments. Therefore, further empirical research is desired to enhance or complement our results.

References

[1] Belanger, F., Hiller, J. S. and Smith, W. J., Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes, *Journal of Strategic Information Systems*. 11 (2002) 245-270.

[2] Boritz, J. E., No, W. G. and Sundarraj, R. P., Internet Privacy in E-Commerce: Framework, Review, and Opportunities for Future Research, *Proceedings of the 41st Hawaii International Conference on System Sciences*. 7-10 January 2008, Waikoloa, Big Island, HI, USA, 2008.

[3] Chellappa, R. K. and Pavlou, P. A., Perceived Information Security, Financial Liability and Consumer Trust in

Electronic Commerce Transaction, *Logistic Information Management*, 15 (2002) 358-368.

[4] Chen, H. and Corriveau, J., Security Testing and Compliance for Online Banking in Real-World, *Proceedings of the International MultiConference of Engineers and Computer Scientists.*2009 Vol I, IMECS 2009, March 18 -20, 2009, Hong Kong , 2009.

[5] Cullen, R., Citizens' concerns about the privacy of personal information held by government: A comparative study, Japan and New Zealand, *Proceedings of the 41st Hawaii International Conference on System Sciences*. 7-10 January 2008, Waikoloa, Big Island, HI, USA, 2008.

[6] Flavian, C. and Guinaliu, M., Consumer Trust, Perceived Security and Privacy Policy, *Industrial Management & Data Systems*. 106, 5 (2006) 601-620.

[7] Kalakota, R. and Whinston, A.B., Frontiers of electronic Commerce, *Addison-Wesley*. MA., 1996.

[8] Karjaluoto, H., Mattila, M. and Pento, T., Factors underlying attitude formation towards online banking in Finland, *International Journal of Banking Marketing*. 20, 6 (2002) 261-72.

[9] Kim, H., Huh, J. H. and Anderson, R., On the Security of Internet Banking in South Korea, Technical Report RR-10-01, *University of Oxford Computing Laboratory*. 2010.

[10] Kim, C. and Jung, J., Online Security, at a Rather Lofty Price, *Joongangdaily*. March 24, 2010, which is available at http://joongangdaily.joins.com/article/view.asp?aid=2918231

[11] Korea Financial Telecommunications & Clearing Institute. Internet banking in the U.S. and Japan, 2010 which is available at http://www.kftc.or.kr/data/data_view.jsp?seq=5191&p=1&category=research&searchKey=&searchVal=#.

[12] Laforet, S. and Li, X., Consumers' attitudes towards online and mobile banking in China, *International Journal of Bank Marketing*. 23, 5 (2005) 362 – 380.

[13] McCullagh, A. and Caelli, W., Who Goes There? Internet Banking: A Matter of Risk and Reward, Information Security and Privacy, 3574/2005, *Springer Berlin, Heidelberg*. 2005.

[14] Milberg, S.J., Burke, S.J., Smith, H.J. and Kallman, E.A., Values, Personal Information Privacy and Regulatory Approaches, *Communications of the ACM*. 38(1995)65-74.

[15] Milberg, S. J., Smith, H. J. and Burke, S. J., Information Privacy: Corporate Management and National Regulation, *Organization Science*. 11 (2000) 35-57.

[16] Ministry of Information and Communication of the government of South Korea. Public Report on the Electronic Transaction Safety Countermeasures, 2005, which is available athttp://www.eprivacy.or.kr

[17] Pavlou, P. A., Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model, *International Journal of Electronic Commerce*. 7, 3 (2003) 69-103.

[18] Singh, N., Online Frauds in Banks with Phishing, *Journal of Internet Banking and Commerce*. 12, 2 (2007) 1-27.

[19] Tan, M. and Teo, T.S.H., Factors Influencing the Adoption of Internet Banking, *Journal of the Association for Information Systems*. 1, 5 (2000) 1-42.

[20] The Bank of Korea, Report on the Internet Banking Use in South Korea for the first quarter of 2010, 2010, which is available at http://www.bok.or.kr/contents/total/ko/boardView.action?menuNaviId=559&boardBean.brdid=70440&boardBean.menuid=559

[21] Wu, Y., Lau, T., Atkin, D. and Lin, C.A., A comparative study of online privacy regulations in the U.S. and China, *Telecommunications Policy*. 35 (2011) 603-616.

Min Hong is an assistant professor at Soonchunhyang University, Korea. He received his PhD in Bioinformatics from University of Colorado at Denver. His research interests include computer simulation and bioinformatics.

Eunjin Kim is the corresponding author. She is an assistant professor at Kyonggi University, Korea. She received her BS, MS and PhD in Management Engineering from Korea Advanced Institute of Science and Technology (KAIST). Her current research interests include economic analysis of digital content, information systems and effects of the digital divide.