Electronic Commerce Research and Applications 9 (2010) 84–95

Contents lists available at ScienceDirect

Electronic Commerce Research and Applications

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

An empirical study of customers' perceptions of security and trust in e-payment systems

Changsu Kim [a,1], Wang Tao [a,2], Namchul Shin [b,*], Ki-Soo Kim [a,2]

[a] School of Business, Yeungnam University, 241-1, Dae-dong, Gyeongsan-si, Gyeongsangbuk-do, 712-749, South Korea
[b] Department of Information Systems, Seidenberg School of Computer Science and Information Systems, Pace University, 163 William Street, New York, NY 10038, United States

ARTICLE INFO

Article history:
Received 2 May 2008
Received in revised form 31 January 2009
Accepted 28 April 2009
Available online 23 June 2009

Keywords:
e-Payment systems (EPS)
EPS use
Electronic commerce
Security
Trust

ABSTRACT

It is commonly believed that good security improves trust, and that the perceptions of good security and trust will ultimately increase the use of electronic commerce. In fact, customers' perceptions of the security of e-payment systems have become a major factor in the evolution of electronic commerce in markets. In this paper, we examine issues related to e-payment security from the viewpoint of customers. This study proposes a conceptual model that delineates the determinants of consumers' perceived security and perceived trust, as well as the effects of perceived security and perceived trust on the use of e-payment systems. To test the model, structural equation modeling is employed to analyze data collected from 219 respondents in Korea. This research provides a theoretical foundation for academics and also practical guidelines for service providers in dealing with the security aspects of e-payment systems.

1. Introduction

Electronic commerce (EC) is built upon e-payment systems (EPS). As EC becomes a major component of business operations for many companies, e-payment has become one of the most critical issues for successful business and financial services (Hsieh 2001, Peha and Khamitov 2004, Stroborn et al. 2004, Linck et al. 2006, Cotteleer et al. 2007, Kousaridas et al. 2008).

In comparison to the traditional payment methods, e-payment techniques have several favorable characteristics, including security, reliability, scalability, anonymity, acceptability, privacy, efficiency, and convenience (Chou et al. 2004, Stroborn et al. 2004, Tsiakis and Sthephanides 2005, Linck et al. 2006, Cotteleer et al. 2007, Kousaridas et al. 2008). EPS have gained recognition and have been deployed throughout the world. Countries such as France, the US, and the UK have fully developed systems, while regions such as the Asia–Pacific rim provide the growth impetus to the industry.

Our research uses Korea as the site of the empirical investigation because the supporting infrastructure required for the EPS development has been put in place. Korea has aggressively pursued the development of IT and networks and created a world-class IT infrastructure (Au and Kauffman 2008). Since the mid-1990s, the Korean government has enforced a number of policies for spreading and promoting EC. As a result of these focused investments, Korea now boasts a world-class infrastructure for EC. According to the annual report of EC published by the Korea Ministry of Commerce in 2007, the total EC market size in Korea was USD 507.42 billion with a growth of 34.6% compared to the previous year. Meanwhile, Korea also has one of the highest per-capita usage statistics for the Internet; the number of Internet users was 34,430,000 (or 75.5% of the population aged six or older) and continues to rise. In the meantime, online shopping and transactions have become a normal part of life for average consumers.

The e-commerce market in Korea is expected to double annually in the next five years. Since Korea is the world's second-fastest-growing IT market, EPS will play an important role in executing wide-ranging activities and actively confronting changing economic conditions. In fact, many EPS brands such as Easycash, Easypaydirect, Inipay, iCash, eGate, eCredit, Smartpay, mypay.net, Payplus, and Paymatics have been established in the recent years.

While good EPS have a number of advantages over the traditional payment methods, they must be free of security breaches (Hegarty et al. 2003, Linck et al. 2006). The Gartner Group reports that 95% of customers are somewhat concerned about privacy or security when using credit cards on the Internet; Harris interactive also reports that six in ten respondents fear credit card theft. A key factor for the success of EPS is security, a requirement that is becoming even more crucial in the current global EC environment

* Corresponding author. Tel.: +1 212 346 1067; fax: +1 212 346 1863.
E-mail addresses: c.kim@ynu.ac.kr (C. Kim), w.tao@ynu.ac.kr (W. Tao), nshin@pace.edu (N. Shin), k.kim@ynu.ac.kr (K.-S. Kim).
[1] Tel.: +82 53 810 2752; fax: +82 53 810 4652.
[2] Tel.: +82 53 810 3213; fax: +82 53 810 4652.

1567-4223/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.elerap.2009.04.014

(Herzberg 2003, Stroborn et al. 2004, Peha and Khamitov 2004, Tsiakis and Sthephanides 2005, Linck et al. 2006, Cotteleer et al. 2007). Transactions in EC can occur without any prior human contact or established interpersonal relationships. Stories about EC security threats from the media or interpersonal networks can undermine trust in EPS and cause people to fall back on the interpersonal trust that arises in human-to-human interactions. Generally, security is a set of procedures, mechanisms, and computer programs for authenticating the source of information and guaranteeing the process (Theodosios and George 2005, Linck et al. 2006). Although extant literature extensively addresses technical details of security and trust in EPS from the perspective of merchants or EPS service providers, consumers' perceptions of the security of EPS have not been well addressed and empirical studies are lacking in this area (Linck et al. 2006).

A number of e-payment systems have recently emerged on the Internet. Although various security measures and mechanisms have been designed for these EPS, many security problems still remain (Hsieh 2001, Chou et al. 2004, Dai and Grundy 2007, Kousaridas et al. 2008). Hence, there is a growing need to minimize the risks associated with e-payment transaction processes (Tsiakis and Sthephanides 2005). Since the majority of users of EPS are relatively unfamiliar with the technical details of EPS, they tend to evaluate the security level of EPS on the basis of their experience with user-interfaces. Thus, to attract and retain e-payment users, it is vital to enhance consumers' perceptions of security and to maintain customers' trust during e-payment transactions (Chellappa and Pavlou 2002, Stroborn et al. 2004, Tsiakis and Sthephanides 2005, Linck et al. 2006, Kousaridas et al. 2008). The principal objective of this research is to empirically examine, from the viewpoint of consumers, the determinants that affect consumers' perceptions of security and trust, as well as the effects of perceived security and perceived trust on the use of EPS.

In the next section, we review the EPS that currently exist in B2C and C2C EC and examine prior research on security and trust issues in EPS. Section 3 develops an exploratory conceptual model of consumers' perceived security and perceived trust in the use of EPS, and presents research hypotheses and constructs. We outline research methodology and results in Section 4. Conclusions and research implications are provided in Section 5.

2. Theoretical background

2.1. Electronic payment systems

When EC created the need for e-payment services, traditional cash-based and account-based payment instruments were used as a model. Simultaneously, new intermediaries such as PayPal succeeded in fulfilling some of the new needs of online merchants and consumers (Dahlberg et al. 2008).

e-Payment is defined here as the transfer of an electronic value of payment from a payer to a payee through an e-payment mechanism. e-Payment services exist as web-based user-interfaces that allow customers to remotely access and manage their bank accounts and transactions (Weir et al. 2006, Lim 2008).

International banking statistics from the Bank of International Settlements and the European Central Bank show that the popular payment instruments used for the payment of day-to-day purchases include cash, checks, debit cards, and credit cards. In general, EPS can be classified into five categories (Lawrence et al. 2002, Guan and Hua 2003, Abrazhevich 2004, Dai and Grundy 2007, Schneider 2007), which are listed below.

1. Electronic-cash: transactions are settled via the exchange of electronic currency.
2. Pre-paid card: customers use a pre-paid card for a specified amount by making an entry of the unique card number on merchant sites. The value of the card is decreased by the amount paid to the merchant.
3. Credit cards: a server authenticates consumers and verifies with the bank whether adequate funds are available prior to purchase; charges are posted against a customer's account; and the customer is billed later for the charges and pays the balance of the account to the bank.
4. Debit cards: a customer maintains a positive balance in the account, and money is deducted from the account when a debit transaction is performed.
5. Electronic checks: an institution electronically settles transactions between the buyer's bank and the seller's bank in the form of an electronic check.

Electronic-cash, pre-paid cards, credit cards, and debit cards are widely used in B2C and C2C EC (Theodosios and George 2005), as shown in Fig. 1. This study focuses on these four types of EPS.

2.2. Electronic payment systems in B2C and C2C EC

2.2.1. Electronic cash

Electronic cash is a method of payment in which a unique identification number is associated with a specific amount of money. Electronic cash is often referred to as e-cash or cyber cash (Jewson 2001, Wright 2002, Stalder 2002, Chou et al. 2004). This method was developed as an alternative to the use of credit cards for Internet purchases of goods or services. For using this payment system, customers purchase electronic digital-cash from the issuing company (Abrazhevich 2004). The cash may then be transferred through computers or other telecommunications channels (Hsieh 2001). The digital-cash method involves a single organization for the issuance and redemption of cash. The low cost characteristic of electronic cash makes it one of the most promising methods

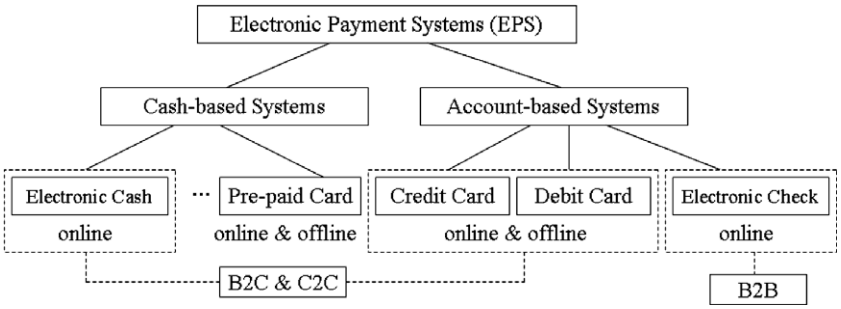

Fig. 1. Classification of electronic payment systems.

for micro-payment (Panurach 1996, Lawrence et al. 2002, Wright 2002, Kim et al. 2006).

2.2.2. Pre-paid card

Pre-paid cards are issued for a particular value by a particular merchant and are frequently used in store transactions. The card can be given as a gift or just used as a convenient way of making purchases. Ease of use and convenience are the primary reasons for consumers to use this card. The pre-paid card is also favorable for merchants because customers tend to spend more freely when using it (Kniberg 2002).

2.2.3. Credit card

Credit card payments originate from offline credit card mechanisms (Lawrence et al. 2002). Credit cards are the most frequently used form of e-payment (Hsieh 2001, Chou et al. 2004). Two important issues associated with the credit card method are security (Stroborn et al. 2004) and privacy, since consumers' transaction records can be tracked through their credit cards (Laudon and Traver 2001). The credit card method involves an irreducibly complex transaction-structure (Hsieh 2001, Wright 2002). Compared to other EPS, it is not appropriate for small-value transactions, i.e., transactions involving less than a dollar (Kalakota and Whinston 1996).

2.2.4. Debit card

Debit card is one of the most widely used systems for e-payment. The debit card method combines the features of the Automatic Teller Machine (ATM) card with Internet banking. When customers pay with a debit card, money is automatically deducted from their bank accounts. In contrast with credit cards, the expended money comes directly from a bank account. Many banks issue a debit card that can be used in places where credit cards are not accepted. When users pay with a debit card, the payment is processed as a debit transaction (Abrazhevich 2004).

2.2.5. Summary

Pre-paid cards, credit cards, and debit cards are the most frequently utilized e-payment methods in B2C and C2C EC, whereas the electronic-cash method operates as a complement to them. Each e-payment technique performs an important function in EC transactions. The electronic-cash method is appropriate for small-value transactions while the pre-paid cards, credit cards, and debit cards can be employed for most types of transaction, although small-value transactions can be disproportionately costly. Since no single e-payment system clearly predominates in EC transactions, each e-payment system can operate as a complement to the others. For micro-payment systems, efficiency and speed are the most important factors. Security issues are also of concern for small-value e-payment transactions. For large-value transactions, security is the most critical issue, and the use of encryption and other security mechanisms should be accordingly considered in order to reduce e-payment transaction risks.

2.3. Review of the literature on security and trust issues in EPS

In order to identify the factors that affect consumers' perceived security and perceived trust in the use of EPS in B2C and C2C EC, this section reviews the relevant literature and provides a conceptual foundation.

Since the Internet is an open network with no direct human control over individual transactions, the technical infrastructure that supports EC and EPS must be resistant to security attacks. Technical protections that are devised to reduce this kind of risk need to be taken into consideration before the problem of consumer trust is addressed. Kalakota and Whinston (1997) assess some of the issues associated with the security of EPS. They note that EPS should be hardened against security breaches, and that the vulnerability of EPS should be carefully considered. The security of e-payment transactions depends on a number of factors, such as systems factors, i.e., technical infrastructure and implementation (Laudon and Traver 2001, Linck et al. 2006), transaction factors, i.e., secure payment in accordance with specific and well-defined rules (Hwang et al. 2007, Lim 2008), and legal factors, i.e., a legal framework for electronic transactions (Peha and Khamitov 2004). Reviewing existing security technologies for EPS, including encryption and authentication techniques, Slyke and Belanger (2003) conclude that a secure e-payment system should provide security against fraudulent activities and must protect the privacy of consumers. Finally, Romdhane (2005) addresses the importance of security evaluation for EPS and argues that a secure e-payment system must exhibit the following two components: (1) integrity, which encompasses authentication, fraud prevention, and privacy; and (2) divisibility, transferability, duplicate spending prevention, payment confidentiality, payment anonymity, and payer traceability.

Transaction procedures in EPS have also been discussed at length in prior literature (e.g. Linck et al. 2006, Hwang et al. 2007, Kousaridas et al. 2008). The procedures in e-payment solutions differ from the ones in the traditional payment solutions because the transaction infrastructures are fundamentally different from each other; this may engender a range of new security issues, including concerns over unauthorized use and transaction status (Linck et al. 2006, Hwang et al. 2007, Lim 2008). Although an e-payment system has the advantage of overcoming time and space constraints when compared to the traditional offline transactions, consumers' perceptions of security and the trust they place in systems are of paramount importance for increasing the use of these systems (Linck et al. 2006, Kousaridas et al. 2008). Laudon and Traver (2001) argue that sophisticated procedures and process interactions should be developed in EPS to deal with security requirements. Lawrence et al. (2002) also suggest that refined process interactions in EPS can eliminate consumers' fears over security issues associated with the use of EPS.

Posting security statements in e-payment sites is another important step (e.g. Mukherjee and Nath 2003, Cotteleer et al. 2007, Lim 2008); the term, "security statements", refers to the information provided to consumers for EPS operations and security solutions. However, few studies address the importance of security statements in EPS. Miyazaki and Fernandez (2000) argue that security-related statements that are posted on websites are likely to increase the chances of consumers' purchasing and paying over the Internet. The rationale supporting this proposition has its basis in the concept of information asymmetry and the role that it plays in decision-making. Information asymmetry refers to situations in which one of the parties involved in a transaction does not have access to all the information needed for decision-making (Akerlof 1970). This has been recognized as one of the major problems in EPS. According to Mukherjee and Nath (2003), the extent of information asymmetry (i.e. security statements not provided to customers) should influence customer's perceptions of security and trust in EPS. Friedman et al. (2002) also suggest that the statements of security features, statements of data protection and privacy, security-policy statements, and other descriptive contents concerning safety precautions help users construct more accurate interpretations of what a secure e-payment system means.

Consumers are extremely sensitive to the risks involved in personal privacy and information security. A great deal of prior empirical research has focused on the technical details of protection, such as privacy and integrity, which are critical for consumers' use of EPS (Tsiakis and Sthephanides 2005, Linck et al. 2006, Hwang et al. 2007, Kousaridas et al. 2008). However, transaction

procedures for authentication, confirmation, and modification are also important in EPS (Tsiakis and Sthephanides 2005, Linck et al. 2006, Hwang et al. 2007, Kousaridas et al. 2008). The availability, accessibility, and comprehensibility of security statements are also important for e-payment transactions (Mukherjee and Nath 2003, Cotteleer et al. 2007, Lim 2008). All three of these dimensions should be considered in the design of secure EPS.

Based on this review of the literature, we can categorize the factors that influence consumers' perceptions of security and trust in the use of EPS into three areas: security statements; transaction procedures; and technical protections (Fig. 2). As described earlier, security statements refer to the information provided to consumers in association with EPS operation and security solutions. Technical protections refer to specific and technical mechanisms to protect consumers' transaction security. Transaction procedures refer to the steps that are designed to facilitate the actions of consumers and eliminate their security fears.

3. Research model and hypotheses

3.1. Research model

Little empirical research has been undertaken on the direct relationship between consumers' perceived security and perceived trust in EPS. A notable exception is the study of Chellappa and Pavlou (2002). They conclude that online transactions are subject to multiple security threats and propose that consumers' trust in online transactions is influenced by their perceived security. They test these propositions and demonstrate a significant, positive relationship between consumers' perception of the security of online transactions and their trust in these transactions. Theodosios and George (2005) argue that e-payment service providers must take into account trust and security as important determinants of consumers' use of EPS.

Empirical research on security issues, which is based on the viewpoint of consumers, is problematic because theoretical concepts of security are very abstract. To address this issue, we develop a survey questionnaire by adopting the security survey framework proposed by Linck et al. (2006). They focus on the security issues influencing customers' participation in a mobile payment procedure and classify the security concept into two dimensions: objective security and subjective security. This research borrows their notion of objective and subjective security dimensions. In the objective dimension, we regard security measures as the concrete solutions in EPS that respond to all security concerns, including technical protections, transaction procedures, and security statements. However, average customers find it difficult to objectively evaluate the security solutions of EPS (Egger and Abrazhevich 2001); most of them evaluate the security of EPS based on their immediate interface with the system. Consumers' subjective evaluations of security have no effect on objective security measures, whereas the level of objective security measures influences consumers' subjective evaluations of security (Linck et al. 2006).

This study tests a research model of consumers' EPS use, which is influenced by both consumers' perceptions of security and trust. We integrate consumers' perceived security and perceived trust into the research model by assuming that both security and trust are important concerns for consumers during an e-payment transaction. If an e-payment system does not adequately provide a secure transaction environment, consumers will treat the system with suspicion, which may erode consumers' trust and eventually their use of the system (Guan and Hua 2003, Mukherjee and Nath 2003, Linck et al. 2006, Kousaridas et al. 2008). Fig. 3 summarizes our research model, based on the research hypotheses developed.

While some of the EPS security factors identified in this model have been presented in previous studies, our research model identifies new antecedents that are considered important to consumers' perceptions of security and trust, in addition to incorporating both perceived security and perceived trust. As shown in the model, technical protections, transaction procedures, and security statements are the principal factors for consumers' perceptions of security and trust in the utilization of EPS. These three factors are directly responsible for determining whether or not a consumer would consider an e-payment system to be secure and whether or not a consumer would have trust in EPS.

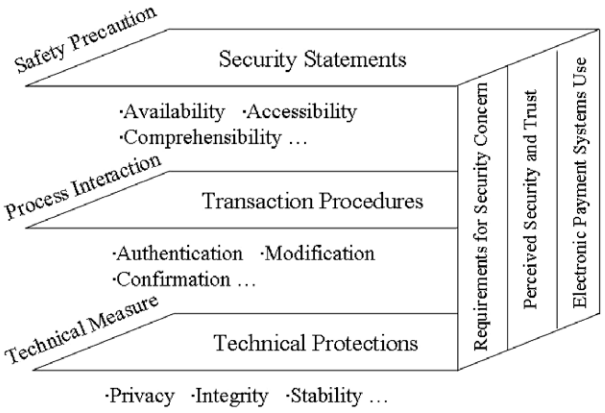

Fig. 2. Diagram of factors that influence perceived security and perceived trust in EPS use.

3.2. Research hypotheses

3.2.1. Technical protections in EPS

Technical protections are generally considered to be the foundation of EPS security. A series of specific technical mechanisms are utilized to ensure payment security during the transaction process on the Internet (Slyke and Belanger 2003, Linck et al. 2006,

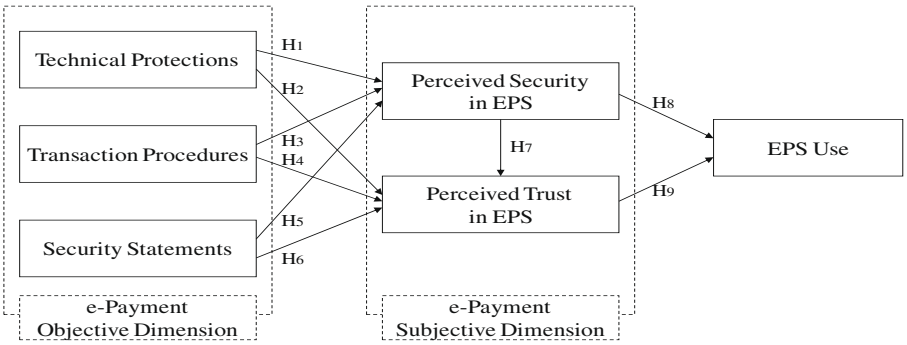

Fig. 3. The model of perceived security and perceived trust in EPS use.

Kousaridas et al. 2008). In association with this concept, Chellappa and Pavlou (2002) assert that perceived security and perceived trust will be favorably influenced by technical protections, including privacy, integrity, and stability. If an e-payment system can offer a guarantee regarding privacy, integrity, and stability, then the level of consumers' perceived security and perceived trust in EPS can be enhanced (Romdhane 2005, Tsiakis and Sthephanides 2005, Hwang et al. 2007). Accordingly, we hypothesize that technical protections are likely to exert a positive impact on consumers' perceptions of both security and trust.

Hypothesis 1. Technical protections are positively associated with consumers' perceived security in EPS.

Hypothesis 2. Technical protections are positively associated with consumers' perceived trust in EPS.

3.2.2. Transaction procedures in EPS

The primary objective of transaction procedures is to facilitate consumers' use of EPS and to eliminate their concerns about the security of EPS (Lawrence et al. 2002). To fulfill consumers' security requirements, well-defined EPS procedures should be prepared (Hwang et al. 2007). Typically, three principal procedures are deployed during the transaction process: (1) authenticating each participant prior to the transaction; (2) providing consumers with several separate steps toward the completion of the e-payment transaction; and (3) sending an acknowledgement after each transaction to assure consumers that the e-payment system has successfully executed the task (Tsiakis and Sthephanides 2005, Hwang et al. 2007). We hypothesize that transaction procedures exert a positive effect on both perceived security and perceived trust in EPS.

Hypothesis 3. Transaction procedures are positively associated with consumers' perceived security in EPS.

Hypothesis 4. Transaction procedures are positively associated with consumers' perceived trust in EPS.

3.2.3. Security statements in EPS

According to the report of Mukherjee and Nath (2003), security statements on EPS websites are a crucial factor influencing consumers' trust in online activities. By informing and reassuring consumers regarding the security of their payment options, it will be possible to influence consumers' perceptions of security and trust in EPS (Lim 2008). If normal consumers remain unaware of the level of security that is inherent to their transactions, they will be reluctant to engage in e-payments (Hegarty et al. 2003, Lim 2008). Consumers' decisions to use any e-payment system will be considerably influenced by the quality of security statements available to them. This notion is bolstered by the results reported by Miyazaki and Fernandez (2000), who, as noted earlier, argue that security-related statements that are posted on websites are likely to increase the chances of consumer purchase over the Internet. We hypothesize that security statements exert a positive effect on both consumers' perceived security and perceived trust in EPS.

Hypothesis 5. Security statements are positively associated with consumers' perceived security in EPS.

Hypothesis 6. Security statements are positively associated with consumers' perceived trust in EPS.

3.2.4. Perceived security in EPS

Perceived security refers to the customer's subjective evaluation of the e-payment system's security (Linck et al. 2006). Since consumers possess different experiences and expectations, they may adopt different attitudes towards the security of online transactions. This is true even if e-payment systems provide assurances with regard to all aspects of consumer's security requirements (Stroborn et al. 2004). If the level of perceived security in an e-payment transaction is too low, consumers are unlikely to participate in the transaction until solutions are implemented to allay their fears (Tsiakis and Sthephanides 2005). Indeed, some studies show that consumers' perceptions of security associated with e-payment dominates their decisions to use EPS. Security and trustworthiness are the main concerns for customers who use EPS, and they are closely related to each other (Guan and Hua 2003, Peha and Khamitov 2004, Linck et al. 2006). Thus, we propose two hypotheses regarding the role of perceived security in relation to consumer's perceived trust and EPS use.

Hypothesis 7. Perceived security in EPS is positively associated with consumers' perceived trust in EPS.

Hypothesis 8. Perceived security in EPS is positively associated with consumers' use of EPS.

3.2.5. Perceived trust in EPS

Consumers' perceived trust in EPS is defined as consumers' belief that e-payment transactions will be processed in accordance with their expectations (Tsiakis and Sthephanides 2005, Mallat 2007). Consumers can make a rational decision based on the knowledge of possible rewards for trusting and not trusting. Trust enables higher gains while distrust avoids potential losses (Linck et al. 2006, Kousaridas et al. 2008). Consumers' attitudes toward EPS are associated with their perceptions of the systems' security. In other words, consumer perceptions of security-enforcement principles augment their beliefs in security, and hence contribute to their perceptions of trust for electronic transactions. Kniberg (2002) argues that "users and merchants are more likely to use an insecure payment system from a trusted company than a secure payment system from an untrusted company (p. 60)". This is consistent with the findings of the previous studies (Tsiakis and Sthephanides 2005, Mallat 2007), which suggest that trust is more important than security. Without customer trust, it would be extremely difficult for an EPS to gain widespread usage. Thus, we hypothesize that consumers' perceived trust in EPS influences the use of EPS.

Hypothesis 9. Perceived trust in EPS is positively associated with consumers' use of EPS.

3.3. Measurement

This section describes the measurement of the three principal variables that affect consumers' perceptions of EPS security and trust.

3.3.1. Measurement of technical protections

This research measures technical protections by using the following three categories: privacy; integrity; and confidentiality (Friedman et al. 2002, Tsiakis and Sthephanides 2005, Hwang et al. 2007). A privacy-protection mechanism can assure consumers that their personal information, such as names, addresses, and contact details, will not be released to other parties (Wright 2002, Peha and Khamitov 2004). Consumers would like to ensure that the information provided to merchants during an e-payment process cannot be used by other parties (Slyke and Belanger 2003, Chou et al. 2004). These technical protections can be achieved by certain specific policies, including standardization as

to the manner in which consumers' information is utilized, stored, and securely protected (Pilioura 2001). Some consumers are reluctant to use EPS, simply because they fear that their personal details can be misused on the Internet (Kalakota and Whinston 1997, Wright 2002). Integrity measures the security of payment information both during and after a payment process (Romdhane 2005). Integrity mechanisms ensure that other parties do not intercept or alter e-payment information (Tsiakis and Sthephanides 2005, Hwang et al. 2007, Kousaridas et al. 2008). This can be achieved via the use of encryption mechanisms, including Secure Sockets Layer (SSL) and Secure Electronic Transaction (SET) technologies (Slyke and Belanger 2003, Dahlberg et al. 2008). Consumers typically require that the integrity of e-payment information is ensured and that the amount of payment and other data remain unchanged (Laudon and Traver 2001). This mechanism influences consumers' perceptions of security and trust in EPS use. Finally, confidentiality refers to the prevention of unauthorized parties from capturing, interpreting, or understanding data. Confidentiality performs a crucial function in gaining consumers' confidence in EPS. There are a variety of factors that may affect the confidentiality of electronic transactions, including e-payment software, e-payment databases, e-payment system platforms, and power supply (Kalakota and Whinston 1997). Additionally, technical protection of establishing authentication of parties, such as the two-factor authentication, is also important for confidentiality. The use of two different factors as opposed to one factor delivers a higher level of authentication assurance (Friedman et al. 2002, Tsiakis and Sthephanides 2005).

3.3.2. Measurement of transaction procedures

This research measures transaction procedures by using the following three factors: authentication; modification; and confirmation. Authentication is the procedure by which the identity of participants is verified through their identity and password before they participate in an e-payment system (Tsiakis and Sthephanides 2005, Hwang et al. 2007). Although authentication offers an initial procedure for preventing illegal intrusions, it is subject to a number of risks that arise from the open nature of the Internet. Authentication is a visible procedure that is directly related to payment security, and thus influences consumers' perceptions of security and trust (Laudon and Traver 2001, Tsiakis and Sthephanides 2005, Kousaridas et al. 2008). Modification is the procedure by which consumers cancel or modify their payment amount or method prior to the completion of the final stage of the payment process. The provision of such an option can also give consumers a perception of confidence and reassurance that they have control over their payment transactions until the finalization stage (Laudon and Traver 2001). Confirmation is the procedure by which consumers can be assured that their payments have been received by merchants (Linck et al. 2006). In this procedure, merchants send an acknowledgement by using mobile phone messages, emails, faxes, etc. The provision of acknowledgement information regarding a payment affects consumers' perceptions of security and trust in EPS use (Romdhane 2005).

3.3.3. Measurement of security statements

This research measures security statements through three factors: availability; accessibility; and comprehensibility. First, availability refers to the information that supports consumers' use of an e-payment system (Mukherjee and Nath 2003). Consumers require knowledge regarding what options and functions are provided by EPS. Insufficient statements can be an obstacle to consumers' use of EPS (Lim 2008). Therefore, a well-designed e-payment system should provide general statements concerning the technical description and functionality of EPS, namely, (1) functions and options within an e-payment, (2) explanations as to how to use an e-payment function, and (3) advice on how to prevent defaults on an e-payment system (Miyazaki and Fernandez 2000, Tsiakis and Sthephanides 2005, Lim 2008). In addition to information that allows customers to distinguish between trustworthy and non-trustworthy merchants, other information could also be provided by EPS. For instance, a reputation system can affect merchants' trustworthiness, and can encourage consumers to use EPS. Second, accessibility refers to the convenience with which consumers can locate statements that concern the security aspects of EPS (Wright 2002, Hegarty et al. 2003). Consumers should not need to exert any special or extraordinary efforts to locate security statements. They should be made available either on the e-payment webpage or on other linked webpages. Thus, a well-designed e-payment system should make it relatively easy for customers to locate security statements (Cotteleer et al. 2007). Finally, comprehensibility refers to the manner in which security statements are provided to the consumers (Linck et al. 2006). The security statements should be explicit and simple enough for an average consumer to comprehend easily. They should also attract consumers' attention when customers make an e-payment transaction (Mukherjee and Nath 2003). Accordingly, a well-designed e-payment system should have the following characteristics: (1) the statements should be comprehensive and explicit and (2) the statements should attract consumers' attention (Hsieh 2001, Cotteleer et al. 2007).

4. Data analysis and results

4.1. Methodology

Measurement assessments are used to validate our model. Following recommendations of prior studies for developing and validating measurement instruments (Hair et al. 1998, Novak et al. 2000, Bollen and Long 1993), our study conducts a three-stage procedure. The first stage is conducted through a review of the relevant literature and corresponding scales (Gefen et al. 2000). In stage two, a set of sample items is generated for each construct and assessed for the reliability and content validity (Joreskog and Sorbom 1993, Kline 1998). In stage three, we proceed with an extensive confirmatory analysis for EPS by testing and validating the refined scales for the reliability and construct validity. We also verify convergent validity and the goodness-of-fit of our research model.

4.2. Survey administration

This research uses Korea as the site of the empirical investigation. The reason is that we have found EC to be more active and successful in Korea, compared to other countries; hence, Korea is an appropriate site for our study on the use of EPS.

This research carried out a two-stage survey to test research hypotheses. First, prior to the conduct of a formal survey, a pretest was carried out to validate the initial version of the survey questionnaire. The samples for the pretest were obtained from the business school of a university located in Korea. The sample comprised approximately 30 undergraduates and graduate students, all of whom had no specific technical background in EPS, but had used EPS before. Some questions that respondents failed to clearly understand were revised. Two IS professors were asked to review the questions to improve the construct validity. The results from the pretest study led to the final version of the survey questionnaire. The respondents rate the questionnaire items by the extent to which they agreed with each statement. Each questionnaire item was scored on a five-point Likert scale (1 = strongly disagree; 2 = disagree; 3 = neutral; 4 = agree; and 5 = strongly agree). The questionnaire contained a few nominally scaled background ques-

tions. These questions sought information on demographics, Internet use, online purchases, payment methods used, etc.

A structured, paper-based questionnaire was used in a formal survey, which was conducted to evaluate the proposed model and to validate the proposed set of interrelationships that were associated with consumers' perceptions of security and trust in the use of EPS. The survey was conducted with participants on a large scale through a 40-item questionnaire. The questionnaire has six sections: technical protections, transaction protections, security statements, perceived security in EPS, perceived trust in EPS, and EPS use. A total of 1260 questionnaires were distributed between October 2007 and January 2008. The printed questionnaires were distributed through the mail, personal visits, and email to people who were working in diverse industries and social institutions, including schools, universities, offices, research institutes, and companies that were drawn at random in Korea. After distributing survey questionnaires, we asked the recipients for their email addresses or telephone numbers in order to increase the response rate by making a call and sending an email to the participants who could not complete the survey. To refine the measures and to assess their reliability and validity, the survey was conducted with strict guidelines. Each participant was requested to carefully complete the questionnaire. Participants were instructed to assess the degree of their faith in technical protections, transaction procedures, security statements, perceived security, perceived trust, and EPS use, which they would expect from a prospective e-payment with particular online merchants.

Altogether, 335 questionnaires were collected by mail, personal visits, and email. Forty-four questionnaires were eliminated due to invalid answers or a lack of experience in the use of EPS, leaving 291 questionnaires for our empirical analysis (a response rate of 23.1%). Our sample comprised 56.4% male and 43.6% female respondents. Most respondents were experienced users of EPS. In terms of age, 11.2% of participants were between 11 and 19 years, 47.9% between 20 and 25 years, 22.8% between 26 and 30 years, and 18.1% older than 30 years. 72.2% of the participants were using the Internet for more than an hour a day. 50.5% of the respondents reported that they engaged in more than two online purchases per month. The value of products purchased online was between $1000 and $10,000. The most frequently utilized EPS were credit cards, fund deliveries, and virtual accounts.

The composition of the sample could potentially limit the generalization of the results because over 80% of participants were aged 30 or below (Peterson 2001). However, young and middle-aged users of EPS represent a significant portion of the user population in Korea. According to Lin and Lu (2000), the results obtained from the analysis of this type of sample can still reflect true phenomena and provide significant outcomes because young and middle-aged users are the most important strata of the user population, and because ultimately, these users will be the most active consumers in EC in the near future. Thus, the sample can be regarded as being representative of the whole population of users of EPS in Korea.

4.3. Reliability and validity tests

4.3.1. Validity test

Factor analysis identifies the underlying structure within a set of observed variables (Miyazaki and Fernandez 2000). SPSS (Statistical Package for the Social Sciences) software was used in the assessment of validity. We assessed the construct validity by identifying the concepts of perceived security and perceived trust. In addition, factor scores were derived from the identified components from the formal survey questionnaire.

An exploratory factor analysis is initially conducted with rotations to detect the significance of the hypothesized factors (convergence validity). All Eigen values are set to greater than one, and the items are reduced to their principal constructs. Finally, a principal component analysis is used as the extraction method for confirmatory factor analysis with varimax rotation.

Table 1
KMO value and Bartlett's test.

Kaiser–Meyer–Olkin measure of sampling adequacy		.866
Bartlett's test of sphericity	Approximate Chi-square	3572.301
	Degrees of freedom	406
	Significance	.000

Twenty-nine survey items in the questionnaire were relevant to factor analysis. To determine the underlying structure, the correlation matrix was initially examined to determine how appropriate it was for factor analysis. The KMO (Kaiser–Meyer–Olkin) values for each of the 29 survey items exceeded 0.45. In addition, the value of the test statistic for sphericity on the basis of a Chi-squared transformation of the determinant of the correlation matrix was large (0.866), and the associated significance level was extremely small (0.000). As shown in Table 1, we concluded that the data were approximately multivariate normal data. Furthermore, the correlation matrix contained sufficient covariation for factoring.

To determine that technical protections, transaction procedures, security statements, perceived security, perceived trust, and EPS use are separate variables, a confirmatory factor analysis was conducted through SPSS. The initial component solution was rotated by using the varimax procedure, with components whose Eigen values were greater than one, which is the criterion for factor retention. Based on the Scree test and the Eigen values that were greater than one, six factors were accepted as interpretable factors. These factors accounted for 60.01% of the variance. Table 2 shows the results of our factor analysis.

Table 2
Rotated component matrix.

Items	Component					
	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5	Factor 6
TECH4	.800					
TECH5	.731					
TECH2	.706					
TECH6	.662					
TECH1	.658					
TECH3	.575					
PROC4		.827				
PROC5		.768				
PROC6		.710				
PROC3		.679				
PROC2		.657				
PROC1		.629				
TRUS4			.836			
TRUS3			.795			
TRUS2			.740			
TRUS1			.682			
STAT1				.782		
STAT2				.742		
STAT4				.689		
STAT5				.620		
STAT3				.609		
STAT6				.494		
SECU2					.745	
SECU4					.725	
SECU1					.708	
SECU3					.620	
USE2						.827
USE1						.815
USE3						.706
Eigen values	3.550	3.324	3.103	2.887	2.342	2.199
% Of Variance	12.240	11.463	10.699	9.955	8.077	7.581
Cumulative %	12.240	23.703	34.402	44.357	52.434	60.015

Table 3
Reliability coefficient test.

Scales	Number of items	Alpha	Mean	Standard deviation
Technical protections	6	0.8493	4.32	0.63
Transaction procedures	6	0.8211	4.27	0.43
Security statements	6	0.7717	4,37	0.47
Perceived security	4	0.7502	4.23	0.48
Perceived trust	4	0.8737	4,33	0.62
EPS use	3	0.7727	4.21	0.45

Note: $n = 294$.

4.3.2. Reliability test

Reliability is determined by Cronbach's alpha, a popular method for measuring reliability (Mukherjee and Nath 2003). Nunnally (1978) suggests that for any research at its early stage, a reliability score or alpha that is 0.60 or above is sufficient. As shown in Table 3, the reliability scores of all the constructs were found to exceed the threshold set by Nunnally; all measures demonstrated good levels of reliability (greater than 0.70). The perceived trust scale achieved the largest reliability of 0.8737.

4.4. Structural equation modeling

As suggested in the literature (Bollen and Long 1993, Joreskog and Sorbom 1993, Kline 1998), the model fit is assessed by such indices as the Comparative Fit Index (CFI), the Goodness of Fit Index (GFI; Hair et al. 2003), the Normed Fit Index (NFI), and the Root Mean Square Error of Approximation (RMSEA; Steiger 1990). The Comparative Fit Index is an index of overall fit (Gerbing et al. 1993). The Goodness of Fit Index measures the fit of a model compared to other models (Hair et al. 2003). The Normed Fit Index measures the proportion by which a model is improved in terms of the fit, when compared to the base model (Hair et al. 2003). The RMSEA provides information in terms of the discrepancy for the degrees of freedom for a model (Steiger 1990). The accepted thresholds for GFI, RFI, NFI, and CFI are 0.90; RMSEA is recommended to be at most 0.05, and acceptable up to 0.08 (Gefen et al. 2000).

The correctness of the research model was tested by using structural equation modeling techniques with AMOS 6.0. The Chi-square statistic of the model was 686.546 with 368° of freedom, thus indicating a good fit with the model (a ratio of less than 3). However, since the Chi-square test is very sensitive to the sample size, we employed a number of other indices to further test the model fit. As shown in Table 4, all the indices – RMR, GFI, AGFI, CFI, NFI, RFI, IFI, and RMSEA – are at acceptable levels. Overall, the results showed that our model provides a valid framework for the measurement of consumers' perceived security and perceived trust in EPS.

4.5. Hypotheses-path testing

This section presents the statistical results of the measurement-validation and hypothesis testing. The effects of technical protections, transaction protections, and security statements on consumers' perceptions of security and trust in EPS were assessed through AMOS 6.0. Our empirical results are shown in Table 5.

As shown in Table 5, the effects of technical protections and security statements on consumers' perceived security in EPS were significant ($\beta_{TECH} = 0.360$, $t = 7.058$, $p < 0.01$ and $\beta_{STAT} = 0.251$, $t = 2.814$, $p < 0.01$).[3] Hence, Hypothesis 1 (H_1) and Hypothesis 5 (H_5) are strongly supported by the results. In contrast, the effect of transaction procedures on consumers' perceived security was not significant ($\beta_{PROC} = -0.069$, $t = -1.637$, $p = 0.102$), showing that transaction procedures do not act as an antecedent of consumers' perceived security in EPS. Hence, Hypothesis 3 (H_3) is not supported.

Our results indicate that technical protections ($\beta_{TECH} = 0.404$, $t = 4.968$, $p < 0.01$) and perceived security in EPS ($\beta_{SECU} = 0.419$, $t = 3.012$, $p < 0.01$) are strongly associated with consumers' perceived trust in EPS. Thus, Hypothesis 2 (H_2) and Hypothesis 7 (H_7) are supported. On the other hand, the effects of security statements ($\beta_{STAT} = 0.154$, $t = 1.239$, $p = 0.215$) and transaction procedures on consumers' perceived trust ($\beta_{PROC} = 0.072$, $t = 1.189$, $p = 0.235$) were not significant; thus, Hypothesis 4 (H_4) and Hypothesis 6 (H_6) are not supported.

Our results also show that consumers' perceived trust in EPS exerts a substantial effect on consumers' EPS use ($\beta_{TRUS} = 0.297$, $t = 3.835$, $p < 0.01$), thus validating Hypothesis 9 (H_9). Finally, the impact of consumers' perceived security in EPS is positively associated ($\beta_{SECU} = 0.276$, $t = 1.814$, $p < 0.05$) with consumers' EPS use, thus supporting Hypothesis 8 (H_8).

Overall, the path coefficients of H_1, H_2, H_5, H_7, and H_9 were significant at a level of $p < 0.01$, thereby indicating support for these hypotheses. The path coefficient of H_8 was significant at a level of $p < 0.05$, thus indicating support for the eighth hypothesis. Hypotheses 3, 4, and 6 are not supported.

Fig. 4 shows a summary of our results for each hypothesis in the research model. The significance of the estimates is indicated by a solid line. As shown in Fig. 4, consumers' perceived security in EPS use is determined by technical protections and security statements. It is also apparent that perceived security and perceived trust are significant factors that influence consumers' EPS use. Additionally, there is a significant impact of perceived security on perceived trust.

5. Conclusion and implications

This paper examines security issues in the context of EPS from the viewpoint of consumers. Our research proposes a research model that delineates the determinants of consumers' perceived security and perceived trust, as well as the effects of perceived security and perceived trust on EPS use. Our findings show that both technical protections and security statements are significant factors for improving consumers' perceived security. Consumers' perceived security is positively related to consumers' perceived trust and EPS use. Finally, consumers' perceived trust also has a positive impact on EPS use. The results are consistent with the findings of the previous research (Culnan and Armstrong, 1999, Miyazaki and Fernandez 2000).

This study finds no evidence of a statistically significant relationship between the quality of transaction procedures and consumers' perceived security or perceived trust in EPS use. The magnitudes of the estimates are quite small, and thus do not support Hypothesis 3 (H_3) and Hypothesis 4 (H_4). These results are not consistent with the results of the study conducted by Laudon and Traver (2001), Romdhane (2005). One possible explanation is that complex procedures, such as fussy authentication and log-in procedures, erode consumers' convenience in using certain e-payment systems. The inconvenience consumers experience in the transaction procedures might degrade consumers' valuation of the security and the trustworthiness of the e-payment system. Thus, e-payment service providers may have to provide consumers with not only secure procedure but also convenient procedures for e-payment systems.

This study provides important theoretical and practical contributions to the area of security and trust in EPS. This research develops a theoretical model of consumers' perceived security and perceived trust, including their roles in the use of EPS. It helps to explain the direct relationships between perceived security, perceived trust, and EPS use. Our results clearly delineate the role of

[3] Some survey items to measure technical protections were not based on real data (i.e. actual implementation of technical protections), but on users' perceptions. That might positively influence the relationship between technical protections and perceived security (and trust) in EPS.

Table 4
Indices of fit and comments for model analysis.

Indices in SEM analysis	Default model	Data fitting of the model
Chi-square/degrees of freedom ratio	686.546/368 = 1.865	Good fit (should be less than 3)
RMR (root mean square residual)	0.080	Good fit (should be less than 0.08)
GFI (Goodness of Fit Index)	0.858	Not a good fit (should be greater than 0.90)
AGFI (Adjusted GFI)	0.832	Good fit (should be greater than 0.80)
NFI (Normed Fit Index)	0.815	Not a good fit (should be greater than 0.90)
RFI (Relative Fit Index)	0.796	Not a good fit (should be greater than 0.90)
IFI (Incremental Fit Index)	0.905	Good fit (should be greater than 0.90)
CFI (Comparative Fit Index)	0.903	Good fit (should be greater than 0.90)
RMSEA (Room Mean Square Error Approximation)	0.055	Good fit (should be less than 0.08)

Table 5
Hypotheses-testing of the research model.

Hypothesized path	Estimate	Standard error	*T*	*p*-Value
Transaction procedures → perceived security in EPS	−.069	.042	−1.637	.102
Technical protections → perceived security in EPS	.360	.051	7.058	.000**
Security statements → perceived security in EPS	.251	.089	2.814	.005**
Transaction procedures → perceived trust in EPS	.072	.061	1.189	.235
Technical protections → perceived trust in EPS	.404	.081	4.968	.000**
Security statements → perceived trust in EPS	.154	.124	1.239	.215
Perceived security in EPS → perceived trust in EPS	.419	.139	3.012	.003**
Perceived security in EPS → EPS use	.276	.152	1.814	.010*
Perceived trust in EPS → EPS use	.297	.077	3.835	.000**

* $p < 0.05$.
** $p < 0.01$.

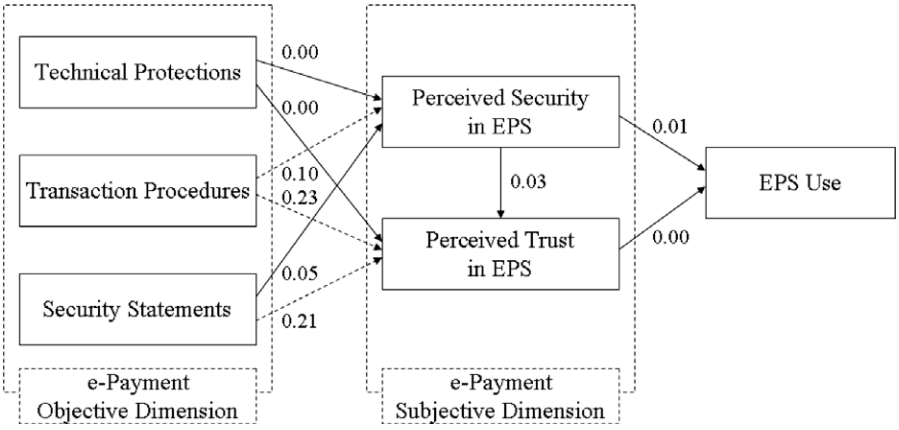

Fig. 4. Output path diagram of the research model.

consumers' perceived security in building the trust of consumers and the positive impact of both perceived security and perceived trust on EPS use. The effects of both technical protections and security statements on consumers' perceptions of security and trust are also validated. Consumers' perceived security and perceived trust are essential concepts in our understanding of consumers' use of EPS. This research is consistent with previous claims that both perceived security and perceived trust perform a crucial function in promoting consumers' EPS use. By presenting an empirically devised set of security issues in EPS in B2C and C2C EC, this research can serve as a basis for the selection of appropriate indicators for further empirical research.

This study suggests that mere introduction of e-payment services is not going to be sufficient to attract consumers to B2C and C2C EC. e-Payment service providers should allay the security concerns of consumers and promote customers' belief in the trustworthiness of services. Some e-payment service providers merely concentrate on technical protections and ignore the importance of security statements in the system. Others hold the notion of "more is better" or "as detailed as possible" on procedural design, based on the objective dimension of security, which seems to be reasonable in terms of obtaining consumers' confidence in EPS. However, from the subjective viewpoint of consumers, this practice ignores the ease of use in operation and thus, can be counterproductive. It is of prime importance for e-payment service providers to develop systems that are deemed as secure on both objective and subjective levels. Thus, management needs to focus on the promotion of these beliefs among consumers when designing security systems.

This study is not free from limitations. First, although the research comes up with some significant findings from the viewpoint of consumers, it does not include all the factors that affect consumers' use of EPS. For example, factors, such as specific e-payment functions, and social and individual factors can be taken into consideration in future research. Special attention should also be paid to human factors, management, education, awareness, and other non-technology factors in order to prevent security risks. For example, to fight against identity theft, education can play a role in increasing consumers' awareness for keeping personal data secure in the physical and virtual worlds. Second, all the participants

in the samples in our research had experience in EPS use. Pre-interaction factors, such as brand reputation, advice, or experience from trusted sources of information (e.g. word of mouth and traditional media), were not considered in our research model. It would be interesting for further research to focus on other factors that give more detailed information on security and trust in EPS. Third, the use of a particular e-payment method is likely to influence the sample respondents in their answers. In our research, credit and debit cards accounted for more than 90% of EPS usage in the samples. Although credit and debit cards entail similar procedures to other e-payment methods, the dominance of these two modes of payment necessitates a careful interpretation of our results. Fourth, the sample employed for our empirical analysis was collected from Korean consumers. The issues associated with e-payment are widely recognized in countries with more advanced EC settings. Thus, it would be interesting to compare the results of this study to those of studies that are conducted through samples collected from other countries. Considering these limitations, our research constitutes an important stepping-stone for future research in different national settings in which it involves an investigation of the factors that influence e-payment security and trust.

Acknowledgments

This research was supported by grants awarded from Yeungnam University in 2007. The authors would like to thank the referees for their helpful comments and suggestions for improvement on a previous version of this paper.

Appendix A. Survey questionnaire

Survey items for transaction procedures in EPS.

Questionnaire items	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
EPS always call for user name and password when you log-in					
Various measures are provided by EPS to authenticate					
The site offers you an opportunity to change any of payment information before completing the final stage of the payment process					
The site provides a step to verify a payment before the finalization of the actual payment					
The site typically displays a summary of the payment information (cost, payee...) and the final payment amount					
A confirmation is sent to you through one of several available methods (online, email, etc.) to assure you that the payment has in fact been received					

Survey items for technical protections in EPS.

Questionnaire items	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Your personal information, such as contact details or payment details, has never been stolen because of using EPS					
Your personal information has not been released to other third parties by EPS service providers for any other purposes					
The payment amount or transaction data displayed on EPS is always accurate					
You think that the EPS transaction data transferred over the Internet is securely protected					
Payment services are always available at any time in a day					
Temporary or sudden errors frequently occur during EPS transaction					

Survey items for security statements in EPS.

Questionnaire items	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
The site offers detailed explanations as to how to review, cancel modify or record a payment					
The site provides security statements on security-policy, contact information under emergency, technical descriptions and functionalities of the EPS					
You do not need to make any special or extraordinary efforts to find security-related statements					
Your concerns on security issues can be easily found from frequently asked questions (FAQ) or a help section					
Security-related statements are drafted in an easily understandable way and largely free from technical words					
The security-related statements are drafted in a wording that attracts your attention					

Appendix A (*continued*)

Survey items for perceived security in EPS.

Questionnaire items	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
I perceive EPS as secure					
I perceive the information relating to user and EPS transactions as secure					
The information I provided in previous EPS is helpful for secure payment transactions					
I do not fear hacker invasions into EPS					

Survey items for perceived trust in EPS.

Questionnaire items	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
I trust each participant, such as seller and buyer, involved in EPS					
I trust the security mechanisms of EPS					
I trust EPS services					
I trust the information provided during the EPS process					

Survey items for the extent of EPS use.

Questionnaire items	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
I use EPS more often than others					
I am using currently and will continue to use EPS					
I believe EPS use will increase					

References

Abrazhevich, D. *Electronic Payment Systems: A User-Centered Perspective and Interaction Design*. Technische Universiteit Eindhoven, Eindhoven, 2004, 24–26.

Akerlof, G. The market for lemons: quality uncertainty and the market mechanism. *Quarterly Journal of Economics*, 1970, 488–500.

Au, Y. A., and Kauffman, R. J. The economics of mobile payments; understanding stakeholder issues for an Emerginh financial technology application. *Electronic Commerce Research and Applications*, 7, 2008, 141–164.

Bollen, K. A., and Long, J. S. *Testing Structural Equation Models*. Sage, Thousand Oaks, CA, 1993.

Chellappa, R., and Pavlou, P. Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management*, 15, 5, 2002, 358–368.

Chou, Y., Lee, C., and Chung, J. Understanding M-commerce payment systems through the analytic hierarchy process. *Journal of Business Research*, 57, 2004, 1423–1430.

Cotteleer, M. J., Cotteleer, C. A., and Prochnow, A. Cutting checks: challenges and choices in B2B e-payments. *Communications of the ACM*, 50, 6, June 2007, 56–61.

Culnan, M. J., and Armstrong, P. K. Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. *Organization Science*, 10, 1999, 104–115.

Dahlberg, T. et al. Past, present and future of mobile payments research: a literature review. *Electronic Commerce Research and Applications*, 7, 2008, 65–181.

Dai, X., and Grundy, J. NetPay: an off-line, decentralized micro-payment system for thin-client applications. *Electronic Commerce Research and Applications*, 6, 2007, 91–101.

e-Business in Korea. Ministry of Commerce, Industry and Energy, 2007. www.mocie.go.kr.

Egger, F. N., and Abrazhevich, D. Security and trust: taking care of the human factor. *Electronic Payment Systems Observatory Newsletter*, Vol. 9. (September 2001). Available at http://epso.jrc.es/newsletter/vol09/6.html. Accessed June 06, 2008.

Friedman, B., Hurley, D., Howe, D. C., Felten, E. and Nissenbaum, H. Users' conceptions of web security: a comparative study. In *Proceedings of the CHI 2002: Changing the World, Changing Ourselves*, April 20–25, 2002, ACM Press, Minnesota, USA.

Gefen, D., Straub, D. W., and Boudreau, M. C. Structural equation modeling and regression: guidelines for research practice. *Communications of the Association for Information Systems*, 6, Article 7, 2000, 1–30.

Gerbing, D. W., Anderson, J. C., and Carlo, M. Evaluation of goodness-of-fit indices for structural equations models. *Sociological Methods and Research*, 21, 2, 1993, 132–160.

Guan, S., and Hua, F. A multi-agent architecture for electronic payment. *International Journal of Information Technology and Decision Making*, 2, 3, 2003, 497–522.

Hair, J. F., Anderson, R. E., Tatham, R. L., and Black, W. C. *Multivariate Data Analysis*, 5th edition. Pearson Education, India, 2003.

Hegarty, J. et al. A trust model for consumer internet shopping. *International Journal of Electronic Commerce*, 6, 1, 2003, 75–91.

Herzberg, A. Payments and banking with mobile personal devices. *Communications of the ACM*, 46, 2003, 53–58.

Hsieh, C. E-commerce payment systems: critical issues and management strategies. *Human Systems Management*, 20, 2001, 131–138.

Hwang, R., Shiau, S., and Jan, D. A new mobile payment scheme for roaming services. *Electronic Commerce Research and Applications*, 6, 2007, 184–191.

Jewson, R. e-Payments: credit cards on the Internet, *White Paper*, 2001, 1–7. Available at <www.aconite.net>. Accessed January 04, 2009.

Joreskog, K. G., and Sorbom, D. *LISREL 8: Structural Equation Modeling with the SIMPLIS Command Language: Scientific International Software*. Chicago, IL, 1993.

Kalakota, R., and Whinston, A. B. *Frontiers of Electronic Commerce*. Addison Wesley Publishing, 1996.

Kalakota, R., and Whinston, A. B. *Readings in Electronic Commerce*. Addison Wesley Publishing, 1997.

Kim, J. B., Kim, H., and Lee, W. An empirical study on settlement risks of payment and settlement system in Korea. *Journal of Financial Investigation (Korean)*, 10, 2006, 1–178.

Kline, R. B. *Principles and Practice of Structural Equation Modeling*. The Guilford Press, New York, NY, 1998.

Kniberg, H. *What Makes a Micropayment Solution Succeed*. Masters thesis, Institution for Applied Information Technology, Stockholm, Sweden, 2002.

Kousaridas, A., Parissis, G., and Apostolopoulos, T. An open financial services architecture based on the use of intelligent mobile devices. *Electronic Commerce Research and Applications*, 7, 2008, 232–246.

Laudon, K. C., and Traver, C. G. *E-Commerce: Business, Technology, Society*. Addison Wesley Publishing, 2001.

Lawrence, E., Newton, S., Corbitt, B., Braithwaite, R., and Parker, C. *Technology of Internet Business*. John Wiley and Sons Australia Publishing, 2002.

Lim, A. S. Inter-consortia battles in mobile payments standardisation. *Electronic Commerce Research and Application*, 7, 2008, 202–213.

Lin, J., and Lu, H. Towards an understanding of the behavioural intention to use a website. *International Journal of Information Management*, 20, 2000, 197–208.

Linck, K., Pousttchi, K., Wiedemann, D. G. Security issues in mobile payment from the customer viewpoint. In *Proceedings of the 14th European Conference on Information Systems (ECIS 2006)*, Goteborg, Schweden, 2006, 1–11.

Mallat, N. Exploring consumer adoption of mobile payments – a qualitative study. *Journal of Strategic Information Systems*, 16, 2007, 413–432.

Miyazaki, J., and Fernandez, K. The antecedents and consequences of trust in online-purchase decisions. *Journal of Interactive Marketing*, 16, 2, 2000, 47–63.

Mukherjee, A., and Nath, P. A model of trust in online relationship banking. *International Journal of Bank Marketing*, 21, 1, 2003, 5–15.

Novak, T. P., Huffman, D. L., and Yung, Y. F. Measuring the customer experience in online environments: a structural modeling approach. *Marketing Science*, 19, 1, 2000, 22-40.

Nunnally, J. C. *Psychometric Theory*. McGraw-Hill, New York, 1978, pp. 23–45.

Panurach, P. Money in electronic commerce: digital cash, electronic fund transfer, and Ecash. *Communications of the ACM*, 39, 6, June 1996, 45–50.

Peha, J. M., and Khamitov, I. M. PayCash: a secure efficient internet payment system. *Electronic Commerce Research and Applications*, 3, 2004, 381–388.

Peterson, R. A. On the use of college students in social science research: insights a second-order meta-analysis. *Journal of Consumer Research*, 28, December, 2001, 450–461.

Pilioura, T. Electronic payment systems on open computer networks: a survey. *Computer and Information Science Publications Collection*, 2001, 197–227.

Romdhane, C. Security implications of electronic commerce: a survey of consumers and businesses. *Internet Research: Electronic Networking Applications and Policy*, 9, 5, 2005, 372–382.

Schneider, G. *Electronic Commerce*. Thomson Course Technology, Canada, 2007.

Slyke, C. V., and Belanger, F. *E-Business Technologies: Supporting the Net-Enhanced Organization*. John Wiley and Sons Inc., 2003.

Stalder, F. Failures and successes: notes on the development of electronic cash. *The Information Society*, 18, 2002, 209–219.

Steiger, J. H. Structural model evaluation and modification: an interval estimation approach. *Multivariate Behavior Research*, 25, 1990, 173–180.

Stroborn, K., Heitmann, A., Leibold, K., and Frank, G. Internet payments in Germany: a classificatory framework and empirical evidence. *Journal of Business Research*, 57, 2004, 1431–1437.

Theodosios, T., and George, S. Concept of security and trust in electronic payments. *Computers and Security*, 2005, 10–15.

Tsiakis, T., Sthephanides, G. The concept of security and trust in electronic payments. *Computers and Security*, 24, 2005, 10–15.

Weir, C. S., Anderson, J. N., and Jack, M. A. On the role of metaphor and language in design of third party payments in eBanking: usability and quality. *International Journal of Human-Computer Studies*, 64, 8, 2006, 70–784.

Wright, D. Comparative evaluation of electronic payment systems. *INFOR*, 40, 1, February 2002, 71–85.