Using a Mobile Device to Enhance Customer Trust in the Security of Remote Transactions

Thair Al-Dala’in, Suhuai Luo and Peter Summons
School of Design, Communication and Information Technology
The University of Newcastle, Callaghan NSW 2308, AUSTRALIA
Email: Thair.Al-Dalain, Suhuai.Luo, Peter.Summons@newcastle.edu.au

Abstract

This paper presents a new scheme for online payment systems based on a mobile personal device and existing debit/credit card electronic payment protocols. The model focuses on trust to enhance the feeling of security in the use of debit/credit cards for online payment systems. A mobile personal device is used to control the payment process of customers in a transaction so as to give them the feeling of being in control of the payment process. The new model provides a way in which customer trust in controlling e-payment systems can be established, so that customers can trustfully participate in electronic commerce. We provide guidelines on how the trust of mobile devices can be applied to achieve mutual improvements between security and trust. Moreover, the model requirements are identified, and an analysis of these requirements against trust and security requirements in transactions is discussed.

1. Introduction

Electronic commerce (e-commerce) has been growing at an exponential rate in recent years and has become an essential tool for financial services. Many of the customers who have purchased goods using the internet have felt reluctant about electronic payment (e-payment) transactions, usually when entering their credit card number [1]. However, “consumers, and more generally, the recipients of services, may feel that they are in an unclear and vague situation with few guarantees as to the level of protection afforded and they may therefore be unwilling to conclude on-line contracts and exploit new opportunities” [2]. Therefore, customers need a system to guarantee that the other party will not misuse their confidential information, such as their credit card details and financial details.

In general, current e-payment systems consist of four parties, namely, a customer, a merchant, an acquirer and an issuer. With reference to Figure 1, a customer makes a payment, using a card issued by a bank (the issuer) that has a contractual relationship with the card, for something purchased from a merchant. In order to provide a payment service, each merchant has to establish a contractual relationship with an acquirer organization. The acquirer is a financial institution which has a financial network with the issuer. The merchant attaches the payment order that is received from the customer, to the payment request, and sends the information to the acquirer to obtain online authorization of the payment. If the acquirer grants authorization, the merchant provides the required service/goods and then reclaims the payment from the acquirer [3].

Trust one of the most important factors necessary to usage of e-payment systems in e-commerce. The first thing customers usually think of in relation to trust is the question of security in electronic transactions. However, any internet payment system has to satisfy four fundamental security requirements [4]:

- Confidentiality (privacy): ensuring that information can only be accessed by authorized parties.
• Data Integrity: ensuring that information cannot be altered or tampered with.
• Authentication: providing the ability to determine the sender’s and the recipient’s identity.
• Non-repudiation: ensuring that parties cannot deny that a message was actually received.

With the popularity and availability of mobile devices such as, mobile phones, PDA’s (personal digital assistant), and laptop computers, these devices have become effective for managing payment and banking transactions by providing security and convenience advantages. The use of the Global System for Mobile communications (GSM) in e-commerce has been proposed by [3; 4], and Bottoni et al. [1] showed that mobile devices fulfill the security requirements and thus can be used as a personal trusted device.

This paper is organized as follows: Section 2 discusses the related work of existing security and trust mechanisms for e-payment systems, especially those which consider the use of a mobile personal device. Section 3 discusses the security and trust in e-payment systems. Section 4 introduces the proposed model design, model components, model requirements and analysis the proposed model requirements against security and trust requirements. Finally, Section 5 presents the paper’s conclusions.

2. Related work

A number of trust and security solutions have been proposed for e-commerce transactions. However, these involve solutions for security and for trust systems considered independent of each other. The SSL or TLS is currently popular and is used to protect the information during transactions. These protocols use the Public Key Infrastructure (PKI) mechanisms and digital certificates to ensure customer privacy and authentication for the merchant. Therefore, credit card details can be sent safely with SSL/TLS. However, once the details reach the merchant server they are vulnerable to outsiders ‘hacking’ into the server, or to the merchant misusing them. Therefore, the SSL/TLS solves the problem of transmitting the information between the customer and the merchant, while it does not help with the rest of the transaction [5].

Another protocol that has been developed by Visa and MasterCard, namely the Secure Electronic Transaction (SET) protocol, uses PKI for privacy, and digital certificates to authenticate a merchant, a customer and a bank. The SET Protocol has not been widely adopted for use. One of the most important obstacles to SET implementation is that the protocol is very complex and confusing for its users. The customer must install additional software to handle SET transactions. As a result, the security benefits that come from the implementation of SET may not be sufficient to bring about its adoption [6].

Due to the currently popular use of SSL/TLS protocol, there has been considerable research proposing a combination of SSL/TLS with other protocols. A proposal by Joris et al. [7] tried to enhance the security of e-payment systems by combining the features of SSL/TLS with GSM. The merchant can rely on the GSM network to ensure they receive an authenticated payment from the customer (via the network operator later on). The purpose of this model is to use GSM as an extension to the internet to provide security and functionality. The payment protocol proposed by Vorapranee et al. [8] is focused on eliminating the possible security risk of storing debit/credit card details at the merchant’s server. The protocol provides user authentication and card detail confidentiality based on GSM data confidentiality.

On the other hand, a number of trust models have been proposed in e-commerce; such as the mathematical trust model; reputation models; and computational trust models. Zhang et al [9] proposed a computational model ERS2G based on user’s attitudes, opinions and motivations, that attempted to improve the trust level, and to provide some insight for customers of e-commerce. They proposed a model based on the idea of reputation aggregation in Role Play Games. Their model combines the concepts of a reputation system and the mathematical trust model by using a representation of the customer’s direct experience, customer evaluations and recommendations, digital credentials, and also certificates and system guarantees, to provide a metric for the trust level.

Reputation models have also been used as method to enhance trust in e-commerce environments and help customers make decisions about who to trust in the future. Organizations such as eBay and BizRate have used aggregated feedback from many of their customers to enhance the trust of potential future customers in them. However, these systems still encounter significant challenges. For instance, feedback can be erased if merchants change their name, and a dishonest participant can use this to build a new business and lose their bad reputation. Another challenge to these types of systems is the reliability of, or the possibility of bias in, the feedback provided. For example, customers may not be willing to provide any feedback other than negative feedback.

In summary, there are a limited number of researchers who have tried to connect trust with security solutions, especially for e-payment systems [10], and most researchers agree regarding the
importance of trust solutions to the security solutions [11]. Moreover, trust has been shown to be important but not sufficient, just as security is important but not sufficient, for building trust and security in e-commerce systems so as to convince consumers that it is safe to use their credit cards in online shopping. In order to address these issues it is important to ask how customer trust in the security model can be developed. Any new work in this area should also be capable, in a physical or practical way, of providing evidence to the customer to satisfy their need.

3. Security and trust

The two major factors influencing trust in remote card transactions in e-payment systems are the security of card details in the transmission to merchants and the customers’ trust in internet merchants. Several questions can be raised concerning the security requirements of the electronic transaction: Who is the party I am doing business with and is he really who he claims to be? Will the transaction data be altered during its transmission over the internet? Can unauthorized parties read my personal information while it is transmitted over the internet? Can the other party deny having received my payment order? It is essential to answer these questions in order to provide customer with trust in electronic transactions. At the same time, customers in general have a tendency to engage in the transaction by means of the most easy to use mechanisms, rather than complicated but more secure mechanisms.

Although security mechanisms are important in order to protect resources and e-commerce transactions from malicious users, they cannot protect people from those who offer services (the merchants) providing incorrect or misleading information. Therefore, trust is the main factor in determining people’s acceptance of e-commerce businesses. Even if a system is totally secure, people may not use it if they do not trust it for some reason, or if they do not fully understand the security mechanisms used. Indeed, it is important to mention that current mechanisms for both security and trust are based on individual bodies of research and that little of that research considers combining security solutions with trust solutions [10]. Thus, security mechanisms may very well produce a system that works efficiently but it does not guarantee that the system will be trusted and used.

Recently, some studies have emphasized definitions to distinguish between the two mechanisms. For example, Rasmussen and Jansson [12] used the term ‘hard security’ and ‘soft security’ to show the difference between traditional security mechanisms, like authentication and access control, and what they called ‘social control’ mechanisms in general, of which trust and reputation systems are examples. Also, Kreyer et al. [13] have used the term ‘objective security’ and ‘subjective security’ to distinguish between the two dimensions of security. They defined objective security as “a concrete technical characteristic, given, when a certain technological solution responds to all of five security objectives: confidentiality, authentication, integrity, authorization and non-repudiation”. Subjective security is defined as the acceptance of mobile payment as “the degree to which a person believes that using a particular mobile payment procedure would be secure” [14].

4. Using a mobile device for e-payment

In this section, the proposed model is described. In the model, a consumer is required to have a GSM mobile phone with a Subscriber Identity Module (SIM). The SIM card has software installed by an authorizer and this acts as a “credit card” that is recognized by the authorizer. However, the mobile phone does need some special capabilities, as described below. This section also describes the model components, the model requirements and the transaction processing procedure.

4.1. Model components

We introduce a new practical trust mechanism designed to enhance the feeling of security in the use of credit cards in online payment transactions, and to satisfy the fundamental security requirements outlined in Section 1. This is achieved by changing the traditional electronic payment transaction processes between customers and merchants through the use of a mobile personal device, where the device participation in the payment processes gives customers the feeling of being in control of the payment process. Six principal participants are involved in the new e-payment model. These are the Customer, the Merchant, a Mobile Personal Device, a Trusted Third Party (Acquirer), the customer’s bank and the merchant’s bank. Figure 2 illustrates the proposed payment system components.
4.2. Model requirements

The purpose of the model is to simplify the payment procedure, to reduce risk, and to protect customer data, as well as enhancing customer’s trust. It is based on a mobile personal device that is an intermediary between the customer and the other parties involved in the transaction, instead of merchant being the intermediary as in current e-payment systems. Thus, customers will send their information without the worry of disclosure or misuse of their confidential personal information by the merchant. In order to satisfy the security and trust requirements in the proposed model, first we will indicate these requirements from our model’s perspective. These requirements state that with trust management, an improved customer protection level can be assured.

Requirement 1 (Authentication): It must be impossible for a customer’s credit card to be used by other people.

Requirement 2 (Non-repudiation): A customer might need to have proof that the acquirer authorized the transaction. (That is, proof that the merchant who has received payment will deliver the goods).

Requirement 3 (Trustworthiness): A customer does not need proof that the merchant is trusted (That is the responsibility of the acquirer to verify that the merchant is accredited at some known trusted third party).

Requirement 4 (Privacy): A customer might require privacy of payment information. That is, no one but the customer and the acquirer can know the payment information.

Requirement 5 (Integrity): A customer may want anonymity when transmitting personal information between their personal computer and the merchant’s server to protect from ‘eavesdroppers’. The customer also needs proof that merchant will not steal his card details.

Requirement 6 (Integrity and Non-repudiation): The merchant may need proof that no one can alter the transmitted payment information from the customer’s mobile device and that no one can deny his payment.

Requirement 7 (Integrity and Authentication): When the acquirer authorizes a payment to a particular merchant, the acquirer must have proof that the merchant has requested this payment.

Requirement 8 (Authorization): The acquirer obtains a payment authorization of the payment from a financial network with the customer’s bank if and only if both customer and merchant have agreed upon the payment.

4.3. Analysis of security and trust in the model transactions

In this section we argue that the payment transactions in the proposed model fulfill the security and trust requirements that were mentioned in the previous section. The following steps illustrate the interactions between the parties in the proposed model that take place in the payment phase (see Figure 2).

In the proposed model, every customer establishes a contractual relation with an acquirer who provides the customer with a credit card in the form of a small application toolkit in the SIM card of the customer’s mobile phone. This is done securely off-line by the acquirer. The customer can then use it in the e-payment system. Also the customer’s mobile device has to be authorized by the acquirer (or by a trusted third party) to receive the acquirer’s certificate.

The system uses a personal computer as the interface between the cardholder and the merchant in the proposed model. A mobile personal device is used as the interface between the merchant and the cardholder and between the cardholder and the acquirer.

1- To make a purchase a cardholder uses a personal computer to send the necessary information to the merchant (including details such as the selected service’s description and the customer’s mobile number) but without any credit card details. Therefore, the information that is transmitted to the merchant is not sensitive and this satisfies requirement 3. Privacy protection for the customer/merchant can be provided using a secure SSL/TLS channel as is normally the case for internet transactions; this is related to requirement 5.

2- The merchant sends a purchase confirmation and the information that has been digitally signed by the merchant to the customer’s mobile device. This information includes details such as a transaction number, the merchant bank ID, the merchant’s ID and
the amount of money to be paid. The merchant stores details of the transaction in their transaction database. According to our assumptions and to satisfy requirement 6, in messages between the customer’s mobile device and both merchant and acquirer, the connection requires secure communication with the customer’s mobile device. This is achieved by establishing secure end-to-end communication between an application on the customer’s SIM and the internet service provider using secure packets implemented over SMS, or unstructured supplementary services data (USSD), if the mobile personal device is a GSM, UMTS or WAP cell phone [15]. Furthermore, the merchant sends the acquirer the payment information via the customer’s mobile device and this information is digitally signed under a trusted third party’s public key. Therefore, no one can alter this information unless they have the private key.

3- The customer authorizes the payment transaction by entering a personal PIN in their mobile device according to requirement 1. Therefore, no one can complete the payment process except the person who has both the personal mobile device and the PIN at the same time. Moreover, if an attacker has stolen the personal mobile device, he/she will not be able to complete the payment process as the attacker still needs the PIN. After the customer enters a personal PIN successfully the customer’s mobile device can then act on behalf of the cardholder and plays the role of the customer in the payment transaction with the acquirer, by sending the validated message received from the merchant, plus customer information such as the customer’s bank ID and customer’s bank account details to the acquirer. The personal trusted device encrypts all these details with the acquirer’s public key and this satisfies requirement 4. In these processes the customer does not need to ensure that the merchant is trusted because in the proposed model the merchant does not act as an intermediary and the information that is transmitted to the merchant is not sensitive (as far as the customer is concerned). Incidentally, the customer knows that the purchase will be done through the trusted third party and knows that it is the responsibility of the acquirer to verify that the merchant is accredited by a known trusted third party. The customer will then not feel reluctant about being involved in the e-payment transaction, and this satisfies requirement 2.

4- To satisfy requirement 7, when the acquirer receives the payment order message from the customer it verifies the digital signatures of both the customer and the merchant in order to ensure their authenticity. For requirement 8, the acquirer will go through a financial network if and only if that message from the merchant has been digitally signed by the customer using his mobile device. That means the customer has authorized the payment transaction and agrees to transfer the payment to the merchant. If successful, the acquirer then decrypts the received data to obtain the payment information and goes through the financial network to obtain payment authorization. The acquirer informs the customer’s bank to reserve the payment to the merchant, and the customer bank notifies the acquirer that the payment has been reserved for the merchant in order to transfer it to the merchant’s account in the merchant’s bank if the acquirer requests that later on.

5- The acquirer sends a confirmation message to both the merchant and the customer’s mobile device to inform them of the success or failure of reserving the payment.

6- When the customer and the merchant receive these response messages from the acquirer, both of them check the digital signature of the message to ensure that it comes from the acquirer. In addition, the merchant checks the transaction number and timestamp to ensure that the receipt message corresponds to the original transaction stored in their transaction database. If all of these processes are completed successfully, the merchant then releases the service/goods to the customer and sends two notification messages. The first message is to the acquirer to inform it that the goods/service have been released to the customer. When the acquirer receives this message, it verifies the digital signature of the merchant to ensure its authenticity. The second message is to the customer’s mobile device to inform the customer that the service/goods have been released. Therefore, the customer can use the service. In the case of the purchase are goods, the customer can collect them from the merchant shop or from the merchant’s deliverer. In the two previous cases, the merchant, or the merchant’s deliverer, verifies the merchant’s signature from the merchant’s message that informed the customer that the goods had been released. If the signature is valid, the merchant delivers the goods.

7- When the acquirer receives the merchant’s message for releasing the service/goods to the customer then the acquirer can inform the customer’s bank to transfer the reserved money to the merchant’s bank, and then the customer’s bank informs the acquirer that the payment has been transferred to the merchant’s account in the merchant’s bank. If the process fails at some stage such as if the merchant does not inform the acquirer to release the service/goods to the customer after a period of time, then the acquirer informs the customer’s bank to cancel the money being held.
8. When the merchant’s bank receives the payment, it sends a confirmation message to inform the acquirer that the customer has paid for the goods.
9. When the acquirer receives the message from the merchant’s bank, it informs the merchant that the customer has paid for the goods.

We note that crucial messages from both customers and merchants are digitally signed. This means that there is no need for the customer and merchant to trust each other; they just only need to trust the use of the correct public keys, which should be ensured by the certificates that are issued by a trusted Certification Authority (CA). In the case of a dispute, they can verify the digital signature of both customers and merchants by a Judge.

5. Conclusion

As the current mechanisms cannot offer prior knowledge of possible malicious behaviors by the merchant, the question was raised as to how the belief in a payment system security can be improved so as to facilitate customer’s trust in the system, and hence make them more willing to engage in future e-commerce transactions without concerns about the trust-worthiness of the merchant.

In a partial answer to this question, this paper has presented a new practical trust scheme to enhance the feeling of security of the use of an e-payment system and to satisfy the security requirements by using a mobile device and existing electronic payment protocols. The development of such a system will be the focus of future research as it is seen as a crucial step towards customer acceptance of e-payment systems and to increase trust in online shopping.

6. References