ISBN: 978-972-8924-66-9 © 2008 IADIS

A REVIEW OF CURRENT ONLINE PAYMENT SYSTEMS RELATED TO SECURITY AND TRUST SOLUTIONS

Thair Al-Dala'in, Suhuai Luo, Peter Summons
School of DCIT, Newcastle University
Newcastle, Callaghan NSW 2308, AUSTRALIA

ABSTRACT

This paper presents a review of current online payment systems in relation to security and trust solutions. These are examined to determine their underlying assumptions, as well as their strengths and weaknesses. A new electronic payment system model based on a personal mobile device and existing electronic payment models is proposed. The model focuses on trust to enhance the feeling of security in the use of credit cards for online payment systems. Mobile personal trust devices are 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. One of the advantages of the proposed scheme is that the trust mechanism does not require a trust merchant to act as an intermediary between customers and the acquirer. Therefore, customers will send their information without concern of personal disclosure, or of the possibility of misuse of their secure information by the merchant.

KEYWORDS

Trust, security, e-payment, e-commerce.

1. INTRODUCTION

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. Therefore, customers need a system to guarantee that the other party will not abuse their confidential information, such as their credit card details and financial details. Merchants also need guarantees that they will receive payment for the goods delivered.

In current e-payment systems, where a payment is made with a credit card or a debit card, the SSL/TLS (Secure Socket Layers / Transport Layer Security) protocol has become a standard to protect the electronic transaction against 'eavesdroppers' during transmission over the internet. However, any internet payment system has to satisfy four fundamental security requirements (Zoran 2005):

- Confidentiality (privacy): ensuring that authorized parties can only access information.
- Data Integrity: ensuring that information cannot be altered or tampered with.
- Authentication: offering 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.

The two major factors influencing 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. Many security and trust solutions have been proposed in the past to deal with these factors. The following section indicates some of the existing security and trust mechanisms for e-payment systems, especially those which consider the use of a mobile device in their structure. Section 2 also examines how those mechanisms work, and discusses their advantages and disadvantages. Section 3 introduces the proposed model design and system architecture. Finally, Section 4 presents the paper's conclusions.

2. RESEARCH BACKGROUND

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 peoples' 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.

Recently, some studies have emphasised definitions to distinguish between security and trust mechanisms. For example, Rasmussen and Jansson (Lars & Sverker 1996) 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. (Kreyer, Pousttchi & Turowski 2002) 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" (Linck, Pousttchi & Wiedemann 2006; Pousttch, G & Wiedemann 2007). 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 following sections review recent research on security, followed by research on trust solutions.

2.1 Security Solutions

In general, the information sent over the Internet usually uses TCP/IP (Transmission Control Protocol / Internet Protocol). The information is divided into sequentially numbered 'packets' with error control data attached. SSL or TLS 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 (Vorapranee & Chris 2002b). 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.

Although SSL/TLS is currently popular and is used for e-commerce, there are still some challenges and problems for its acceptance in credit card payments. As mentioned, one of these problems is that, while SSL solves the problem of transmitting secure information between the customer and the merchant, it does not help with the rest of the transaction. For example, in SSL credit card transactions it is still possible for a merchant to steal a customer's card numbers. Another problem with SSL-based payment systems, is that the customer does not provide cardholder authentication (Vorapranee & Chris 2002a).

Another approach 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 (Sherif et al. 1998). There are also a number of drawbacks to using the SET Protocol and it 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 in their PC to handle SET transactions. Also, business banks must have established agreements with companies that will manage the bank's payment gateway. Furthermore, participating merchants must have an account opened at the business bank that is capable to receive their SET transactions (Zoran 2005). Moreover, SET requires a PKI and using public key cryptographic techniques is costly in terms of computational overhead and performance. As a result, the security benefits that come from the implementation of SET may not be sufficient to bring about its adoption (Levi & Koc 2001).

In order to reduce these deficiencies of SSL, there has been considerable research proposing a combination of SSL with other protocols. Vorapranee et al. (Vorapranee & Chris 2002b) proposed a protocol that provided cardholder authentication through EMV PIN (Europay MasterCard Visa - Personal Identification Number) verification to enhance the security of existing internet payment methods that relied on SSL/TLS for their transaction security. The PIN is associated with the physical integrated circuit on the card and so, without the correct PIN, the card will not work and, no transaction can be made. This scheme

reduces the online authorization overhead because the integrated circuit on the card allows some decisions to be made offline. On the other hand, a weakness in this proposal is that the protocol relies on the cardholder system integrity. Moreover, confidentiality of the card's details is not provided as the cryptograms making up the card details are transmitted over the Internet and so may be intercepted.

A proposal by Joris et al. (Joris, Bart & Joos 2001) tried to enhance the security of e-payment systems by combining the features of SSL/TLS with the Global System for Mobile communications (GSM). When a customer has completed their purchase request using the SSL/TLS secure channel they receive a confirmation via this same secure channel, as well as on their mobile phone. Therefore, the customer can double-check the merchant's identity, the contents of their purchase, and also the amount of money to be paid. The merchant can rely on the GSM network to ensure they receive an authenticated payment from the customer (via the network operator later on). Moreover, customers cannot cheat by requesting their network operator to deduct a smaller amount of money than originally requested by the merchant, as the merchant would notice the smaller amount of money and not send a receipt. Indeed, the purpose of this model is to use GSM as an extension to the internet to provide security and functionality. It assumes the customer's personal mobile phone can be considered as being solely for individual use by the customer. The model cannot protect mobile phones from unauthorized access in case of the phone is stolen or lost. Moreover, this model requires some additional software on the customer's personal computer and there has to be a connection between the mobile phone and the personal computer in case the customer wants to digitally sign the information regarding their authenticity. Furthermore, the relation between the merchant and the customer's mobile phone relies on short message service (SMS) that can only contain a limited number of characters.

The payment protocol proposed by Vorapranee et al. (Vorapranee & Chris 2002a) 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. This requires a prior agreement between the issuer and the mobile phone service provider so that the issuer can use the services of the mobile phone service provider as an Authentication Center.

It is clearly notable from a security solutions perspective that the main objective of these solutions is to provide mechanisms for customer and merchant protection. These solutions are chiefly based on traditional security techniques such as cryptography based mechanisms. However, most of these solutions do not have the ability to satisfy all the security requirements. These models do not use security requirements as an assistant device to anticipate vender behaviour for security decision enhancement. Hence the customer's protection level cannot be pre-determined. For example, while the customers can initiate security protocols with a particular merchant, they may not have any knowledge of possible malicious behaviours of this merchant, such as the merchant providing misleading information, using 'fake' websites, or initiating 'phishing' attacks.

2.2 Trust Solutions

A number of trust models have been proposed in e-commerce; such as the mathematical trust model (Zhongwei & Zhen 2006); reputation models (Audun et al. 2007); and computational trust models (Sabater & Sierra 2005). Zhang et al (Zhongwei & Zhen 2006) 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 a 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. The same type of model is being considered for e-commerce development and deployment within China (Wang, Zhang & Zhang 2006).

Yang et al (Yang et al. 2006) developed a web trust profiling framework (W3TF) that attempted to enhance customer confidence by evaluating the trust, and the transitivity of trust, on web-based services in a heterogeneous web environment. To create an approach to trust assessment, W3TF focused on a combination of using existing trust systems such as PKI, translating identifying trust attributes that take from customer perceptions into trust metadata, and using Web technology to extract some trust information from Web-documents in form of metadata. The W3TF framework dealt with the technical trust issues but did not address issues of Web accessibility (W3C 2007). Moreover, as there are no standards for metadata

information offered for metadata contained in Web documents, the extraction of hidden trust information is a very complex task, as is the assignment trust values to a trust attribute in trust metadata.

Reputation models have also been used as method to enhance trust in e-commerce environments and so help customers make decisions about who to trust in the future. Organisations 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. Ildemaro and Araujo (Ildemaro 2005) proposed three methods to support trust in e-commerce by focusing on privacy issues in web stores and merchant sites. Their proposals included approaches to handle the privacy of customer data. These were: the development of legislation; the use of mechanisms for user self determination; and the implementation of regulation through corporate practice. Attention to trust in e-commerce website interfaces is enhanced by providing information about the organisation's products, its privacy policy, company address, contact persons and third party seals of approval (Jeffrey Sam 2003).

As indicated earlier, the trust models examined above have been proposed to solve specific trust issues in e-commerce environments without considering the relationship between security and trust. A trust and reputation model largely relies on customer feedback and focuses only on evaluating and establishing a trust relationship without consideration of the security requirements in their design. It was identified that customer trust in these models is influenced by customer evaluation from the amount of experience customers have and the degree of associated satisfaction. However, these mechanisms do not guarantee protection for customers and customers may therefore misinterpret cues which may be misleading. Furthermore, in reputation models, it is possible that some users may provide false feedback to intentionally raise the reputation of a service.

3. PROPOSED MODEL

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 2. This is achieved by changing the traditional electronic payment transaction processes between customers and merchants through the use of mobile personal devices, where the devices participation in the payment processes gives customers the feeling of being in control of the payment process. The proposed trust mechanism does not require a trust merchant to act as an intermediary between customers and the acquirer. So, customers will send their information without the worry of disclosure or misuse of their confidential personal information by the merchant. Figure 1 illustrates the proposed e-payment system. It shows the principal participants in the new payment model as the Customer, the Merchant, a Personal Mobile Device, a Third Party (Acquirer), the customer's bank and the merchant's bank. In the proposed model, every customer establishes a contractual relation with an issuer (or an acquirer acting for the issuer) who provides the customer with a credit card in the form of a small application toolkit in the SIM (subscriber identity module) card of the customer's mobile phone. This is done securely off-line by the issuer. 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. Incidentally, the customer knows that the purchase will be done through the trusted third party and so will not feel reluctant about being involved in the e-payment transaction.

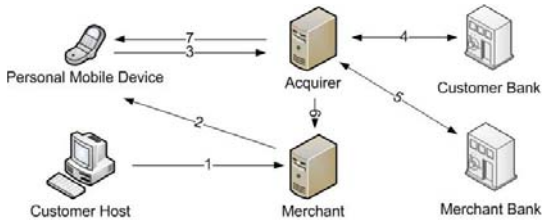

Figure 1. Proposed electronic payment system

The system uses a personal computer as the interface between the cardholder and the merchant. A personal mobile device is used as the interface between the merchant and the cardholder and between the cardholder and the acquirer. Interfaces to the merchant from customer use SSL/TLS and interfaces from the merchant to the customer's mobile device use GSM to satisfy the security requirements of the customer and the merchant. The merchant requires secure communication with the customer's mobile device is achieved by establishing secure end-to-end communication between an application on the customer's SIM and the internet service provider by secure packets implemented over SMS or unstructured supplementary services data (USSD) (Kadhiwal & Zulfiquar 2007). 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. The merchant sends a purchase confirmation and information to the customer's mobile device. This 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. The customer authorizes the payment transaction by entering a personal PIN in their mobile device. After this 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. 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 for as the customer is concerned).

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. If successful, the acquirer then decrypts the received data to obtain the payment information and goes through the financial network to obtain the payment authorization. The acquirer informs the customer's bank to transfer the payment to the merchant's account in the merchant's bank from the customer's account, and the customer bank notifies the acquirer that the payment has been transferred. The merchant's bank sends a message to inform the acquirer that the customer has paid for the goods. Finally, the acquirer sends a confirmation message to both the merchant and the customer's personal mobile device to inform them of the success or failure of the payment. 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 sends a notification message to the customer's mobile device and releases the goods/service to the customer. Any other communications between the parties remain unchanged with the existing financial network acting as a gateway between the parties.

The proposed model has more advantages compared with a conventional e-payment system. Some customers may be unfamiliar with the trust solutions used by a website, for example trust evaluation or a trusted signature. A false website might counterfeit these and so customers may be the victim of a 'phishing' attack. On the other hand, in the proposed model the customers trust their mobile because they know that the device is authorized by a trusted third party who is responsible for any kind of fraud that may occur. Moreover, this model has additional advantages in that it combines the personal computer with a personal mobile device and uses existing infrastructure and technologies to minimise the extra cost of a new e-payment method. While the SIM does initially require additional software from the issuer, this solution provides mobility which is not possible in the conventional solutions where software has to be installed in any PC participating in a transaction, as in the SET case (section 2.1). The use of a mobile phone and SIM can offer a more economical, secure, and more mobile solution than conventional e-payment systems. Using any available personal computer in the navigation phase is more comfortable than using only a mobile phone, with limited navigation and display capability, for the entire transaction.

4. CONCLUSION

This paper has presented a review of current online payment systems related to security and trust solutions and demonstrated the lack of comprehensive research to support the integration of security solutions with

trust solutions for electronic payment systems. Current approaches to electronic payment systems were examined to determine their underlying assumptions, as well as their strengths and weaknesses.

As the current mechanisms cannot offer prior knowledge of possible malicious behaviours by the merchant, the question was raised as to how the belief in a payment systems 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, 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 personal mobile device and existing electronic payment models was proposed. The steps of a proposed study to develop such a system were also outlined. 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 that may help to increase trust in online shopping.

REFERENCES

Audun J. et al, 2007. A Survey of Trust and Reputation Systems for Online Service Provision, *Decis. Support Syst.*, Vol. 43, No. 2, pp 618-644.

Ildemaro, A., 2005. Privacy Mechanisms Supporting the Building of Trust in E-Commerce, *Proceedings of the 21st International Conference on Data Engineering Workshops*. IEEE Computer Society.

Jeffrey Sam, S., 2003, *The Effect of Web Interface Features on Consumer Online Shopping Intentions*.

Joris, C. et al, 2001, Combining World Wide Web and Wireless Security, *Proceedings of the IFIP TC11 WG11.4 First Annual Working Conference on Network Security: Advances in Network and Distributed Systems Security*. Kluwer, B.V., pp 153-172.

Kadhiwal, S and Zulfiquar, AUS, 2007. *Analysis of Mobile Payment Security Measures and Different Standards*, Computer Fraud & Security, Vol. 2007, No. 6, pp 12-16.

Kreyer, N. et al, 2002. Standardized Payment Procedures as Key Enabling Factor for Mobile Commerce, *University Library of Munich*, Germany.

Lars, R. and Sverker, J., 1996. Simulated Social Control for Secure Internet Commerce, *Proceedings of the 1996 Workshop on New Security Paradigms*. Lake Arrowhead, California, United States, pp. 18-25.

Levi, A. and Koc, CK., 2001. CONSEPP: CONvenient and Secure Electronic Payment Protocol Based on X9.59, *Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual*. pp. 286-295.

Linck, K, Pousttchi, K & Wiedemann, DG 2006, Security Issues in Mobile Payment from the Customer Viewpoint, University Library of Munich, Germany.

Pousttch, K. et al, 2007. What Influences Consumers' Intention to Use Mobile Payments?, University of Augsburg, Germany.

Sabater, J and Sierra, C., 2005. *Review on Computational Trust and Reputation Models*, Artificial Intelligence Review, Vol. 24, No. 1, pp 33-60.

Sherif, MH. et al, 1998. SET and SSL: electronic payments on the Internet. *Third IEEE Symposium on Computers and Communications, 1998. ISCC '98. Proceedings*. pp. 353-358.

Vorapranee, K. and Chris, JM., 2002a. Using GSM to Enhance E-commerce Security, *Proceedings of the 2nd International Workshop on Mobile Commerce*, Atlanta, Georgia, USA, pp.75-81.

Vorapranee, Ks. and Chris, JM., 2002b. Using EMV Cards to Protect E-commerce Transactions, *Proceedings of the Third International Conference on E-Commerce and Web Technologies*. Springer-Verlag, pp. 388-399.

W3C 2007, Web Accessibility Initiative (WAI), viewed http://www.w3.org/WAI.

Wang, Z. et al, 2006. *Towards Enhancing Trust on Chinese E-Commerce*, Frontiers of WWW Research and Development - APWeb 2006, pp. 331-342.

Yang, Y. et al, 2006. *W3 Trust-Profiling Framework (W3TF) to Assess Trust and Transitivity of Trust of Web-Based Services in a Heterogeneous Web Environment*, Frontiers of WWW Research and Development - APWeb 2006, pp. 367-378.

Zhongwei, Z. and Zhen, W., 2006. Assessing and Assuring Trust in E-Commerce Systems, *Proceedings of the International Conference on Computational Inteligence for Modelling Control and Automation and International Conference on Intelligent Agents Web Technologies and International Commerce*. IEEE Computer Society.

Zoran, D., 2005. IPS - Secure Internet Payment System, *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05) - Volume I - Volume 01*. IEEE Computer Society. pp. 425-430.