Available online at www.sciencedirect.com

ScienceDirect

Computer Communications 30 (2007) 1697–1712

computer communications

www.elsevier.com/locate/comcom

Improving authentication of remote card transactions with mobile personal trusted devices

Andrea Bottoni, Gianluca Dini *

Dipartimento di Ingegneria dell'Informazione: Elettronica, Informatica, Telecomunicazioni, University of Pisa, Via Diotisalvi 2, 56100 Pisa, Italy

Received 21 May 2006; received in revised form 5 February 2007; accepted 6 February 2007
Available online 16 February 2007

Abstract

Credit card transactions are a popular and diffused means of payment over the network. Unfortunately, current technology does not allow us to technically solve disputes that may arise in such transactions. Thus these disputes are often solved on legal and administrative basis. In these cases, responsibility is not necessarily allocated fairly and the problems of managing the resulting risks have proven to be an impediment to the growth of electronic commerce.

In this paper we present a protocol for credit card transactions over the network that uses personal trusted devices (e.g., a cellphone or a PDA) to improve the technical management of disputes and permit a more fairly allocation of risks between customer and merchant. The protocol also defines a practical trade off between the security properties of these devices and the resource limitations deriving from their form factor. Furthermore, by means of formal methods, we specify the security requirements of a personal trusted device and analyse the security properties of the protocol. Finally, we argue that a cellphone practically fulfills the above security requirements and thus can be used as a personal trusted device.

Keywords: Security; Authentication; e-Payment; Trusted device

1. Introduction

Remote card transactions are credit card transactions in which cardholder and merchant "meet over the network". Remote card transactions are a popular and diffused means of payment over the network [54].

In remote card transactions, the incidence of risk is quite different from that where the card is presented by the customer to the merchant. Bohm et al. provided a very deep and precise analysis [7]. Briefly, in a remote card transaction no voucher is signed and the customer only provides the merchant with information apparent from the face of the card. The ability to provide the card information does not depend on the possession of the card. In fact, such an information is available to anyone through whose hands the card has passed during earlier transactions. It follows that there is very little impediment to fraud either by the cardholder falsely repudiating a genuine transaction or by an impostor using the card details without authority. If the cardholder repudiates a remote card transaction, the bank has no basis on which to charge the cardholder's account. Faced with apparently unmanageable risks of this kind, banks have adopted the approach requiring the merchant to carry the risk. Thus, if the cardholder repudiates a remote card transaction for which there is no voucher signed by the cardholder, the bank makes a "chargeback", i.e., obtains reimbursement from the merchant of anything paid to the merchant in respect of the transaction. The merchant is in practice unable to transfer the risk to anyone else, since he is unlikely to be able to prove who initiated the transaction.

Although simple, this liability regime has important implications. The greatest risk to the merchant arises from the provision of online services. Although online services

[*] Corresponding author. Tel.: +39 050 2217 549; fax: +39 050 2217 600.
E-mail addresses: a.bottoni@iet.unipi.it (A. Bottoni), g.dini@iet.unipi.it (G. Dini).

0140-3664/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2007.02.006

have been provided for long, they have expanded greatly with the commercialization of the Internet. Provision of online services is one of the most effective uses of the Internet for electronic commerce. Small and medium enterprises are among those which can derive the greatest benefit from access over the Internet, but can least afford exposure to the risks which remote card transactions place on merchants. Therefore, the problem of managing the resulting risks for the merchant may well prove to be an impediment to the growth of electronic commerce in online services.

Technological solutions have been proposed to improve the security of remote card transactions. The most relevant are *Secure Socket Layer*, SSL [27], and *Secure Electronic Transactions*, SET [45]. In remote card transactions carried out using a web browser to connect to the merchant, it is possible to establish a secure connection so that the information is delivered in encrypted form using protocols such as SSL or TLS [13]. This procedure is widely followed and provides protection against interception of the card information in transit. However, it cannot affect the widely availability of the card information from other sources, and cannot provide evidence that the supplier of the card information is authorised by the cardholder. Thus it does not materially reduce the merchant's risk [7,54].

Secure Electronic Transactions (SET) is a standard promulgated by Visa and Mastercard. SET allows a merchant to check whether the bank will accept the cardholder's authority as genuine. The intent is to remove the risk from the merchant, or at least reduce it. SET has not gained acceptance perhaps because it is over elaborate and its implementation is burdensome and expensive [54]. Apart from that, there is a subtle point about its security model that is central to this paper. SET improves the merchant's exposure to risk of chargeback by precluding a cardholder from repudiating a SET transaction which appears to have been authorised by that cardholder. However, this gives rise to an unacceptable shift of the risk from the merchant to the customer. In fact, the risk of the customer of losing control of the means of authorising a SET transaction, namely information stored in electronic form, is very different from the risk of losing a plastic card. The current version of SET was designed for common desktop PCs as typical user terminals, and with the Internet as the transport network. PCs are unlikely to meet any serious security requirement for several reasons [7,41]. In such an environment, the customer is exposed to the risk of his private key being compromised without the means of detecting the compromise until the fraudulent use becomes evident. A sophisticated attack might leave no evidence and the customer would be thus left in a weak position to resist an assertion of the bank that the remote card transaction was correctly authorised.

In this paper, we present a protocol to improve authentication of remote card transactions by means of personal trusted devices. The main objective of the protocol is to shift the risk to a more balanced position between the merchant and the customer. Improving authentication consists in providing non-repudiable proof of transaction authorization both from the customer and the merchant. These proofs make it possible to improve the technical solution of disputes. In the authorization process, the personal trusted device plays a crucial role as it allows the customer to generate his strong proof and, at the same time, reduces the risk that he can lose control of the means of authorising a payment transaction.

More in detail, the paper makes the following contributions.

- First, it shows that the overall security of an electronic payment system can be greatly increased by means of a personal trusted device. In particular, the use of such a kind of device makes it possible to improve the way to solve disputes in a technical way.
- Second, the electronic payment protocol takes into account both the security limitations of conventional user computers (e.g., home/office PCs) and the resource limitations of personal trusted devices (small screen and keyboard), and defines a practical trade-off between security and usability. A PC is used to browse and select goods, whereas a personal device is used to authorize a payment transaction. In order to issue such an authorization the customer has only to read a few information items on the device screen, enter a PIN, and press just a few buttons.
- Third, by using a formal method, namely an extended version of the BAN logic [9,1], we state the trust requirements of the personal device. So far, these requirements have been informally stated [40]. To the best of our knowledge, ours is the first effort to formalize them.
- Fourth, we exploit the formal framework to highlight the security limitations of a conventional, "open", PC-based system, with or without smart cards, and to argue that a GSM/UMTS cellphone can be practically considered a personal trusted device as long as it is part of the "closed" GSM/UMTS application framework. The use of cellphones in e-commerce has been suggested by many [5,10,12,26,33–35,44,46,49,50]. In this paper we give a theoretical and architectural basis to this statement.

The paper is organized as follows. In Section 2, we briefly introduce the payment model based on credit cards. The proposed electronic payment system has the objective to interface with the pre-existing credit card payment systems without changing them. In Section 3, we specify the basic security requirements the proposed electronic payment system is required to fulfill. In Section 4, we present the electronic payment system. In Section 5, we make a security analysis of the proposed payment protocol. In this activity we will use a variation of the BAN logic [9]. In Section 6, we discuss the electronic payment protocol. Finally, in Section 7, we make conclusive remarks.