Computers and Electrical Engineering 000 (2016) 1–18

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

A lightweight two-gateway based payment protocol ensuring accountability and unlinkable anonymity with dynamic identity

Venkatasamy Sureshkumar[a,*], R. Anitha[a], N. Rajamanickam[a], Ruhul Amin[b]

[a] Department of Applied Mathematics and Computational Sciences, PSG College of Technology, Coimbatore-641004, India
[b] Department of Computer Science and Engineering, Thapar University, Patiala-147004, India

ARTICLE INFO

Article history:
Received 23 December 2015
Revised 25 July 2016
Accepted 25 July 2016
Available online xxx

Keywords:
Accountability
Anonymity
Payment protocol
Payment gateway
CPSA
Strand space

ABSTRACT

In the current scenario, mobile web payment provides a standard platform to the Internet users for online digital goods shopping. Though the majority of online transactions use single gateway, there is a need for multi-gateway, due to insufficient balance in a customer's account in a specific bank. There are a few payment protocols which support a transaction using multiple cards, but they too have some limitations like cards should be of the same bank and the process should be based on independent transactions. This paper proposes an efficient payment protocol that is used for making online transactions via two gateways for purchasing digital goods to overcome the above mentioned limitations. The proposed protocol is simulated using the automated tool Cryptographic Protocol Shape Analyzer (CPSA) and it satisfies accountability, anonymity and atomicity properties. Formal proof of correctness is provided using the strand space model. The protocol is then compared with the state-of-the-art protocols in terms of different security features and computational overhead. Results show that our protocol achieves better performance than other protocols.

1. Introduction

Online shopping has been increasing exponentially in the recent days. The main idea behind online shopping of digital goods is to order the goods and make the payment using a payment protocol with user anonymity [1,2]. This user anonymity is preserved by using dynamic identity (ID), that needs to be updated at the end of each transaction [3,4]. The online shopping is usually performed through portable devices such as iPads, tablets, smartphones etc., which have lower power, limited storage, and less computational capacity compared to desktop computers [5,6]. Therefore, it is highly desirable to use, lightweight payment protocols in portable devices and the usage of the Public Key Infrastructure (PKI) in these protocols is not advisable. Symmetric key operations as well as hash functions are the most lightweight operations in the field of cryptography [7].

A payment protocol has to satisfy many properties and one such important property is accountability. Formally, "Accountability is the property whereby the association of a unique originator with an object or action can be proved to a

* Corresponding author. Fax: +914222573833.
E-mail address: sand@amc.psgtech.ac.in (V. Sureshkumar).

http://dx.doi.org/10.1016/j.compeleceng.2016.07.014
0045-7906/

third party" [8]. The payment protocol may lead to several disputes without accountability property. Authentication provides origination of the message and confirms the sender of the message [9–11]. Hence, accountability could be achieved via authentication. Customer anonymity, which is another property to be satisfied in online transactions, can be obtained by means of the two primitives, untraceability and unlinkability [5]. A payment protocol satisfies untraceability property, when an attacker is unable to distinguish a particular customer from a group of customers. A payment protocol is said to satisfy unlinkability property, when the sent messages are not associated with the sender and receiver [12]. Thus, if the payment protocol is unlinkable, an attacker cannot identify the customer and his account in the specific bank. Therefore, unlinkability is a stronger notion of anonymity [13].

Let us consider a situation in which a customer uses two different bank cards for the online payment. If the total cost of the product is more than the balance in a single bank, then the customer tends to use the second card also to make the payment. In this case, the customer is unable to make the payment through the normal payment system. This scenario requires an efficient payment protocol for the online payment system, where the customer can pay the required amount through two gateways.

1.1. Related work

This section presents some of the existing payment protocols, and briefs their working mechanisms. The popular SET protocol, which is proposed by VISA and MasterCard consists of many phases such as purchase order, card inquiry, authorization, payment initialization and payment capture [14]. Customer's bank details and purchase order details are concealed from the merchant and the bank respectively. But this protocol requires all the parties to have certificates for their public keys. Bellare et al. [15] introduced a collection of protocols $-iKP$ $(i = 1, 2, 3)$ for secure online payment which is designed based on a public key cryptosystem. Merchant, customer and payment gateway are the protocol entities in iKP. The following protocols $1KP$, $2KP$ and $3KP$ stand apart in the aspect of the number of protocol entities maintaining their individual public key pairs and the scheme with more key pairs achieves better security [15]. Supakorn Kungpisdan [16] introduced a secure payment protocol using symmetric key cryptosystem. In this protocol, the secret information (card details, pin number, etc.) are not disclosed at the time of transaction. The protocol consists of several entities such as client, merchant, issuer, acquirer and payment gateway. Moreover, this protocol is composed of two subprotocols, merchant registration protocol and payment protocol. The client executes the merchant registration protocol to register himself with merchant and then he executes the payment protocol to make the payment. Isaac-Camara [17] designed a payment protocol using public key infrastructure for the restricted connectivity environment in mobile commerce. Fun et al. [18] introduced Mobile Network Operator (MNO) based lightweight payment protocol using symmetric keys for mobile environments which provides customer anonymity. Isaac-Zeadally [19] proposed a payment gateway centric model based anonymous payment protocol which is used in mobile devices. In this scheme, there is no direct communication between the client and the merchant and in each communication cycle, the merchant and the client contact through the payment gateway. Later, Yang-Lin [1] pointed out that Isaac-Zeadally mechanism does not provide fairness and non-repudiation requirements on the client side. Further, it is noted that their scheme used a redundant symmetric key between the client and the merchant. This key is not essential as all the messages are transmitted through the payment gateway and thus causes a key management problem and increases the computation and communication costs in the cloud environment. The schemes in [14,15,17] are based on the public key cryptography and hence, they are not applicable for lightweight payment devices, whereas the schemes in [16,18,19] are designed based on the Symmetric Key Infrastructure (SKI) and therefore are used in lightweight payment devices. However, in these schemes [16,18,19], there is no facility of making payment through two gateways. The customer anonymity is achieved by the issuer bank by creating user IDs and sending them in bulk, due to which the future sessions can be compromised.

A system provided in [20] supports two cards from the same bank (gift card) for making payment for a single item. Each payment has only one funding source and has to be fully supported by a single bank. However, it will not cover the terms of the purchase protection program at that point. A payment mechanism in [21] permits to use two cards from different banks with the exception of the cards being MasterCard/Visa/American Express cards only. These card services follow 3-D secure protocol. This protocol is designed for a single payment, but the organisation uses two different individual transactions which do not affect each other to complete the original payment. Accountability issues are caused when one transaction commits and the other transaction fails due to network problem. So the customer is unable to start a fresh transaction for buying products or services. In order to overcome these shortcomings, an efficient payment protocol is needed.

A Light Weight Two Gateway (LWTG) payment protocol has been proposed in [22] for not only making payment for a single item using two cards from different banks, but also for using a dynamic ID to provide customer anonymity. Further, the LWTG protocol overcomes the issues faced by the existing protocols, which use the mechanism of bulk posting of the customers ID from the issuer bank.

In this paper, the LWTG payment protocol is enhanced to satisfy the atomicity property, by including suitable subprotocols and commitment phase. A nested transaction is developed where the original transaction commits only if the two inner transactions are committed successfully. Otherwise, the whole nested transaction rolls back and the committed product can be used to resolve accountability issue. The customer can also start a fresh transaction for buying digital goods.

Please cite this article as: V. Sureshkumar et al., A lightweight two-gateway based payment protocol ensuring accountability and unlinkable anonymity with dynamic identity, Computers and Electrical Engineering (2016), http://dx.doi.org/10.1016/j.compeleceng.2016.07.014