Secure and Optimized Mobile Based Merchant Payment Protocol using Signcryption

Shaik Shakeel Ahamad, Institute for Development and Research in Banking Technology and University of Hyderabad, India

V. N. Sastry, Institute for Development and Research in Banking Technology and University of Hyderabad, India

Siba K. Udgata, Institute for Development and Research in Banking Technology and University of Hyderabad, India

ABSTRACT

The authors propose a Secure and Optimized Mobile based Merchant Payment (SOMMP) Protocol using Signcryption scheme with Forward Secrecy (SFS) based on elliptic curve which consumes less computational and communication cost. In SOMMP client sends message in the form of TransCertC (Transaction Certificate) which is a X.509 SLC (X.509 Short Lived Certificate) thereby reducing the client interactions with the engaging parties thereby reducing the consumption of resources (from Client’s perspective) which are very scarce in Resource Constrained Devices like Mobile Phones. In SOMMP protocol WSLC (WPKI Short Lived Certificate) eliminates the need of certificates validation and removes the hurdle of PKI thereby reducing storage space, communication cost and computational cost. Their proposed SOMMP ensures Authentication, Integrity, Confidentiality and Non Repudiation, achieves Identity protection from merchant and Eavesdropper, achieves Transaction privacy from Eavesdropper and Payment Gateway, achieves Payment Secrecy, Order Secrecy, forward secrecy, and prevents Double Spending, Overspending and Money laundering. In addition to these SOMMP withstands Replay, Man in the Middle and Impersonation attacks. The security properties of the proposed SOMMP protocol have been verified using BAN Logic, AVISPA and Scyther Tools and presented with results.

Keywords: Automated Validation of Internet Security Protocols and Applications (AVISPA) Tool and Scyther Tool, Burrows-Abadi-Needham Logic, Secure and Optimized Mobile Based Merchant Payment (SOMMP), Signcryption Scheme with Forward Secrecy (SFS), Transaction Certificate (TransCertC), X.509 Short Lived Certificate (X.509SLC)

1. INTRODUCTION

In this paper we propose a Secure and Optimized Mobile based Merchant Payment (SOMMP) Protocol using Signcryption scheme with Forward Secrecy (SFS) based on elliptic curve which consumes less computational and communication cost. Signcryption Scheme with forward secrecy (SFS) based on Elliptic curve combines digital signature and encryption func-
tions (Hwang et al., 2005). This scheme takes lower computation and communication cost to provide security functions. SFS not only provides message confidentiality, authentication, integrity, unforgeability, and non-repudiation, but also forward secrecy for message confidentiality and public verification. In this scheme, the judge can verify sender’s signature directly without the sender’s private key when dispute occurs. This scheme can be applied to mobile communication environment more efficiently because of the low computation and communication cost.

We consider the following scenario in Mobile based Merchant payments. A Client tries to buy goods/services from merchant through a communication network i.e., internet and the client’s platform is mobile phone equipped with UICC as secure element which is tamper resistant. Client cannot tamper the inner working of UICC because of its tamper resistant nature of the UICC, the communication channel between UICC and mobile phone is secure and reliable. The communication channel among the engaged entities in our proposed protocol SOMMP is unreliable which is prone to attacks.

In our proposed SOMMP protocol client sends message in the form of TransCertC (Transaction Certificate) which is a X.509 SLC (X.509 Short Lived Certificate) thereby reducing the number of client interactions among the engaging parties (i.e. reducing the consumption of resources from Client’s perspective which are very scarce in Resource Constrained Devices like Mobile Phones). Our proposed Mobile Payment protocol (SOMMP) can be used in both Remote mobile payments & Proximity Mobile Payments (i.e., at Point Of Sale). In SOMMP protocol WSLC (WPKI Short Lived Certificate) eliminates the need of certificates validation and removes the hurdle of PKI thereby reducing storage space, communication cost and computational cost.

2. RELATED WORK

Mobile Payment Protocols proposed (Téllez & Sierra, 2007a, 2007b, 2007c; Téllez et al., 2006a, 2006b, 2008) are suitable for scenarios with communication restrictions (Téllez & Sierra, 2007c; Téllez et al., 2006a) employs symmetric-key operations and (Téllez & Sierra, 2007a, 2007b; Téllez et al., 2006b, 2008) protocols employs Digital Signature with Message Recovery using Self-Certified public keys schemes based on RSA. Our proposed SOMMP protocol is suitable for scenarios with/without communication restrictions.

2.1 Gaps Found in Related Work

a) Protocols proposed (Téllez & Sierra, 2007c; Téllez et al., 2006a) employs symmetric-key operations and (Téllez & Sierra, 2007a, 2007b; Téllez et al., 2006b, 2008) employs Digital Signature with Message Recovery using Self-Certified public keys schemes based on RSA (which consumes more computational and communication cost compared with ECC).

b) The no of Client interactions with other engaged parties are more.

c) Protocols proposed (Téllez & Sierra, J. 2007a, 2007b, 2007c; Téllez et al., 2006a, 2006b, 2008) do not ensure forward secrecy and Public Verification.

d) In Téllez and Sierra (2007a, 2007b, 2007c) and Téllez et al. (2006a, 2006b) protocols every Client C needs to register itself with merchant in merchant registration protocol thereby consuming lot of resources.

e) Téllez and Sierra (2007c) and Téllez et al. (2006a) protocols does not ensure non repudiation.

f) Téllez and Sierra (2007a, 2007b) and Téllez et al. (2006b) protocols cannot withstand Replay attack, Impersonation attack, and MITM attack. Téllez et al. (2008) protocol cannot withstand MITM attack.

g) Merchant communicating Payment Gateway is not realistic in Téllez and Sierra (2007a, 2007b) and Téllez et al. (2006b, 2008)

h) Security protocols are error prone and are not easy to identify errors and prove their correctness. Mobile Payment Protocols proposed by Tellez et.al. were not verified