A secure and efficient mobile banking scheme based on certificateless cryptography

Abstract. Providing the security requirements (authenticity, integrity, confidentiality and non-repudiation) all together in mobile banking has remained a problematic issue for both banks and their customers. The Public Key Infrastructure (PKI) has been thought of as a solution to provide secure mobile services, but generally the PKI suffers the two problems of scalability and certificate management. Despite the identity-based cryptography addressing these two issues, it could not offer a true non-repudiation solution, due to the key escrow problem. In this paper, we propose a fully secure certificateless and GPRS based mobile banking scheme. Within this scheme only the key generating center has a certificate to prove its identity. Both a client and a bank's web-server uses the identity of each other to obtain the public key of each other from the key generating center via secure channels. Then, each party computes a shared secret symmetric key without any interaction. By using this shared secret key the client can encrypt his username and password (which are decrypted and verified at the bank's web-server side) to access his banking account and carry out banking transactions.

Keywords: Security Requirements, Mobile Banking, Certificateless Cryptography, Pairing.

1 Introduction

Mobile banking is a way for a bank's customer to access banking services on his/her cell phone to perform bank transactions. It makes life of customer easier by being able to access his/her accounts anytime anywhere. From the side of bank, it reduces time and effort costs at the different bank branches. Quality services mobile banking does bring more customers to the bank and makes it competent to the other banks[2].

Banks enable customers to access their banking accounts through one of four technologies. These technologies are the interactive voice response, the short messaging service, the wireless access protocol and the stand-alone mobile application clients. In each case, the customer's serious fraud about mobile banking is "How safe is it to use mobile banking?". The customer wants to guarantee that no one else will impersonate his identity to perform banking transactions on his/her banking accounts.

On the other hand, mobile networks can be connected to the Internet via gateways. The wireless application protocol (WAP) is used to connect a mobile or any WAP device to the WAP gateway. Then the TCP/IP protocol is used to transmit the data from the WAP gateway to the web server. Mobile networks have some weaknesses which reduces the trust in the mobile banking. Mobile banking systems are struggling with the task of authenticating a user's identity and also that mobile networks do not have the same or equivalent security layers the Internet sites do. This makes the touching points of mobile banking easier for criminals to gain access to and being capable of infiltrating an unsuspecting bystander's mobile banking account [4].

Therefore, the main bank fraud is "Is he the customer who claims that he is?". Also, the bank wants to guarantee that the customer will not deny a transaction that he has performed using mobile banking. Both the bank and the customer would like to be sure that the bank has performed the exact transaction that the customer has performed[2].

Public Key Infrastructure (PKI) has been thought of as the most practical solution for the problem of mobile banking security. Based on this thought, many mobile banking systems based on PKI have been proposed (see for example [5], [6],[10] and [14]). Generally, the PKI suffers two problems: scalability and certificate management[1]. The identity-based cryptography [7] came to address these two problems, but could not offer true non-repudiation due to the key escrow problem [1],[3]. However, few researchers introduced solutions to the problem of the security of mobile banking based on the identity based cryptography. For example Zhao and Aggarwal [13] proposed an end-to-end secure messaging in mobile networks based on identity-based cryptography. A very similar work was proposed by Parasad et. al in [8] in which a secure end-to-end messaging in mobile networks based on identity based cryptography was introduced.

The certificateless cryptography is considered a cross between PKI and identity based cryptography. It provides a solution to the non-repudiation problem, where the trusted third party is unable to impersonate the user. In many secure mobile banking research articles, the certificateless signatures have been considered (see for example [9], [11] and [12]). But to the best of our knowledge, no secure mobile banking scheme based on certificateless cryptography has been proposed up to now.

In this paper, we propose an efficient and fully-secured mobile banking scheme based on certificateless cryptography with only one certificate to autherize the KGC. When the client mobile requests the banking service from the bank's web-server, both the mobile client and the bank's web-server can be securely connected to the KGC using the SSL protocol from where they can obtain the public key of each other and their own partial private keys. Then each of them can generate a common secure symmetric key using a bilinear pairing without any direct interaction between them. By using this secret key, the client can encrypt his username and password and send them to the web-server (which are decrypted and verified at the service provider's side) to access his banking accounts and doing the banking transactions.

The rest of this paper has been organized as follows. Section 2 gives backgrounds about mobile banking technologies. In Section 3, we introduce the concept of certificateless public key cryptography. In Section 4, we introduce the proposed secure mobile banking scheme using certificateless cryptography. Section 5 concludes the paper.