Computers and Electrical Engineering 49 (2016) 198–206

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

An Unlinkable Anonymous Payment Scheme based on near field communication ☆

Jia Ning Luo [a], Ming Hour Yang [b,*], Szu-Yin Huang [b]

[a] Dept. of Information and Telecommunications Engineering, Ming Chuan University, Taiwan
[b] Dept. of Computer and Information and Computer Engineering, Chuan Yuan Christian University, Taiwan

ARTICLE INFO

Article history:
Received 8 September 2014
Received in revised form 11 August 2015
Accepted 11 August 2015
Available online 19 September 2015

Keywords:
Unlinkability
Anonymity
Mobile payment

ABSTRACT

A number of mobile payment studies have been proposed in recently years. Most of the schemes are largely focused on transaction security, not on users' privacy. In this paper, we propose an Unlinkable Anonymous Payment Scheme to provide a secure and anonymous mobile commerce environment. In the proposed protocol, a user applies an anonymous virtual credit card from a trusted service manager. The sensitive information of the applied credit card is stored in the secure elements of user's mobile device. Our proposed protocol ensures various imperative security properties such as anonymity, unlinkability, and non-repudiation etc.

1. Introduction

With the rapid development of wireless communication, users can perform electronic payment on their mobile devices such as smartphones. Mobile devices have high computing and communication ability, and large storage; therefore, money transfer services are shifting from traditional methods (such as pay on arrival, ATM transfer, or credit cards) to mobile devices. For consumers, it is much more convenient to use smartphones instead of traditional computers in mobile commerce activities. In 1982, Chaum [2] proposed the concept of anonymous payment. Since then, more and more mobile payment schemes have been proposed. Chen et al. [4] propose a payment scheme that is based on 3G/UMTS security services. Toorani and Beheshti [20] propose a small amount payment scheme based on short message service (SMS).

Near field communication (NFC) is a short-range wireless communication technology that enables communication between two devices in close proximity to each other (e.g., within 10 cm). NFC devices have a higher degree of security because both sniffing communications and man-in-the-middle attacks are then harder if not impossible to accomplish. In recent years, NFC technology is being increasingly considered as a solution for contactless mobile payment services.

Saeed and Pourghomi [19] integrate NFC into mobile transaction by using Global System for Mobile Communications (GSM) authentication. Kumari et al. [15] propose anonymous withdrawal and payment in small amount transactions. In Martínez-Peláez et al.'s scheme, a customer's identity is kept anonymous. This scheme prevents double spending and forgery attacks. As the banks keep customers' transaction records, they may breach their privacy. Molloy et al. [16] propose a virtual credit card mechanism that utilizes a dynamic virtual credit card number to mitigate the loss in card theft. The virtual credit card accounts are derived from a user's existing physical credit card account. Grønli et al. [12] propose architecture to

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. W-H Hsieh.

* Corresponding author.
E-mail addresses: deer@mail.mcu.edu.tw (J.N. Luo), mhyang@cycu.edu.tw (M.H. Yang), Kobebryand76@gmail.com (S.-Y. Huang).

http://dx.doi.org/10.1016/j.compeleceng.2015.08.007
0045-7906/

support the concept of mobile wallet. The most well-known NFC mobile payment applications include Google Wallet and Apple pays, which are all based on the EMV standard. EMV is a technical standard for smart payment cards, which stands for Europay, MasterCard, and Visa, the three companies which originally created the standard [10].

However, these schemes are largely focused on transaction security, not on users' anonymity. In this paper, we propose an NFC-Based Unlinkable Anonymous Payment Scheme. In our scheme, sensitive data such as users' real identities and the encrypted keys are stored in the trusted element (the secure element) of a Mobile Trusted Module (MTM) [7,10,11]. The host applications on the mobile phone should be verified by the remote attestation services. The users have to open a financial bank account to get a virtual bank account identifier. Then the users apply for an anonymous transaction account from the TSM, which will issue an EMV-compatible virtual credit card that has limited valid time and credits. The card will be stored in the smartphone's secure elements. If the card expires or if the virtual account's balance reaches the limits, the users must apply for another virtual bank account and a new virtual credit card.

The main contributions of our scheme include convenience, anonymity, unlinkability, and non-repudiation.

- Convenience: users can simply take their NFC phones for transactions. Traditional credit cards are not required.
- Anonymity: the user's real identity is hide. Except the bank, no entities in the payment procedure can determine the users' real identity.
- Unlinkability: unlinkability is also called strong anonymity. In our scheme, merchants can only retrieve a temporary virtual credit card's information of a user. The adversary cannot trace the mobile phone by using interactions with the phone. Even though TSM has users' payment information, it can only track to their anonymous virtual accounts. The information of users' real identities will not be revealed to TSM. As for the issuing bank, it is unable to know their transaction records.
- Non-repudiation: in our scheme, all the messages of registration, transactions, and card issuance are signed to guarantee non-repudiation.

The rest of the paper is organized as follows. Section 2 describes our propose anonymous scheme. Section 3 analyses our scheme's security strength by using the common security attack models. Section 4 then compares our protocol with other related studies. Finally, Section 5 presents our conclusions.

2. An Unlinkable Anonymous Payment Scheme based on near field communication

Our propose anonymous payment scheme consists of four phases: (1) registration; (2) anonymous virtual bank account generation phase; (3). anonymous transaction account generation phase; and (4) virtual credit card generation phase. The following introduces the roles in our system:

1. Bank: it provides accounts for users.
2. Trusted Service Manager (TSM): TSM is a trusted third party (TTP) that provides services and management of anonymous credit cards; requests payment from and verifies anonymous authority with banks; and provides transaction services.
3. Host: it is the execution environment in an NFC-enabled mobile phone. In the mobile phone, an application issued from the service provider is responsible for the payment process.
4. Secure element (SE): SE is a secure storage in an NFC-enabled mobile phone.
5. Merchant (M): denotes a merchant in a mobile transaction.

The four phases of our scheme are described as follow:

1. Registration phase: At this stage, the system generates parameters that are required for the payment process.
2. Anonymous virtual bank account generation phase: A user applies for an anonymous account to be used for payment from his bank.
3. Anonymous transaction account generation phase: A user takes his virtual bank account identifier to the TSM to create a transaction account. After the TSM verifies the user's allowed credits with his bank, it issues a service account to him.
4. Virtual credit card generation phase: A user requests a temporary virtual credit card from the TSM and stores it into the SE.

2.1. Notations

Table 1 lists the notations used in our scheme.

2.2. Registration phase

When a user opens a bank account with a valid identification document and commits to his attributes and public key, the bank issues a certificate $CERT_U^B$ corresponding to the user's public key PK_U. The bank generates a shared key $K_{B,U}$ between the