Information Sciences 345 (2016) 143–155

Contents lists available at ScienceDirect

Information Sciences

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

Accountable mobile E-commerce scheme via identity-based plaintext-checkable encryption

Jinguang Han[a,*], Ye Yang[b], Xinyi Huang[c,f], Tsz Hon Yuen[d], Jiguo Li[e], Jie Cao[b]

[a] Jiangsu Provincial Key Laboratory of E-Business, Nanjing University of Finance and Economics, Nanjing, Jiangsu 210003, China
[b] College of Information Engineering, Nanjing University of Finance and Economics, Nanjing, Jiangsu 210003, China
[c] Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, Fuzhou, Fujian 350117, China
[d] Shield Lab, Huawei International Pte Ltd, 20 Science Park Road, #02-06/10, Teletech Park, Singapore Science Park II, Singapore 117674
[e] College of Computer and Information, Hohai University, Nanjing, Jiangsu 211100, China
[f] Nanjing University of Information Science and Technology, Nanjing, Jiangsu 210044, China

ARTICLE INFO

Article history:
Received 31 March 2015
Revised 9 September 2015
Accepted 22 January 2016
Available online 1 February 2016

Keywords:
Privacy
Accountability
Identity-based system
Plaintext-checkable encryption
Mobile E-commerce

ABSTRACT

In mobile e-commerce systems, users conduct transactions using wireless or Internet-based devices, such as mobile phones and tablets. It is different from traditional e-commerce systems relying on workstations or desktops, which is usually used in a fixed location. Recently, privacy and accountability have become users' primary concerns in mobile e-commerce applications. In this paper, a novel mobile e-commerce scheme is developed to address the fundamental requirements. We *first* propose an identity-based plaintext-checkable encryption (IBPCE) scheme where anyone can check whether a ciphertext is the encryption of a plaintext under a specific identity without knowing the secret key. Furthermore, the proposed IBPCE scheme is incorporated into the mobile e-commerce scenario, which results in an accountable mobile e-commerce (AMEC) scheme. Our proposed AMEC scheme has several superior features: (1) Users can register to the e-commerce system by using their mobile identities, such as mobile phone numbers; (2) The transactions between a buyer and a vendor are encrypted; (3) If there is a dispute, an offline adjudicator can identify who is dishonest by checking the encrypted transactions. We evaluate the proposed scheme and confirm that the new scheme can effectively balance the need for privacy and accountability.

1. Introduction

The increasing advances in electronic commerce or e-commerce enable people to conduct more and more transactions on the Internet. It brings us with a new trading model and affects the global economy. Meanwhile, it also promotes the development of information technology and all economic branches. E-commerce companies are creating tremendous online services and exploiting the opportunities provided by the Internet. However, one of the disadvantages in traditional e-commerce schemes is the fixed location restriction by workstations or computers [1]. This limits the use of e-commerce.

* Corresponding author. Tel.: +86 25 83494883; fax: +86 25 83494883.
E-mail addresses: jghan22@gmail.com (J. Han), yangye6365@163.com (Y. Yang), xyhuang81@gmail.com (X. Huang), Yuen.Tsz.Hon@huawei.com (T.H. Yuen), ljg1688@163.com (J. Li), caojie690929@163.com (J. Cao).

http://dx.doi.org/10.1016/j.ins.2016.01.045
0020-0255/

The advent of wireless network, such as 4G wireless network [19,21,33,36] and Wi-Fi [9,15,22,40] enables users to access the Internet anytime and anywhere. To facilitate transactions, wireless network has been exploited in e-commerce. This is called mobile e-commerce (m-commerce) or mobile e-business (m-business) [17,26,42]. In m-commerce schemes, a user can use his electronic identity to register, such as mobile phone number and e-mail address. Then, he can use his mobile phone or tablets to conduct transactions anywhere, without the limitation of locations.

Since its introduction, m-commerce has attracted lots of attentions. M-commerce schemes with distinctive features were proposed [35,39,41]. Ngai and Gunasekaran [30] reviewed m-commerce schemes and classified them into five types: wireless user infrastructure, wireless network infrastructure, mobile middleware, m-commerce cases applications and m-commerce theory and research.

Wireless communication is a very complicated communication environment where end-to-end security should be provided [32]. To achieve this goal, public-key encryption [2,13,14] has been exploited. Lin et al. [24] proposed a mobile payment architecture for wireless mobile network. This scheme was based on identity-based encryption (IBE) and can provide end-to-end security.

In m-commerce schemes, two of the most concerned issues are privacy and accountability. Although privacy issues have been addressed extensively [17,37,38], accountability has not been focused. However, accountability is an important property of m-commerce as it can guarantee that a dishonest user can be identified when there is a dispute.

In a traditional public-key encryption scheme, it is difficult to check whether a ciphertext is the encryption of a message under a public key when the secret key is unknown. To resolve this problem, Canard et al. [6] proposed a plaintext-checkable encryption (PCE) scheme. In their scheme, given a plaintext and a public key, anyone can check whether a ciphertext is the encryption of the plaintext under the public key. So, a dishonest sender can be identified without knowing the receiver's secret key if he sends an incorrect ciphertext to the receiver. Hence, a PCE scheme can provide not only confidentiality but also accountability.

1.1. Our contributions

In this paper, we first proposed an identity-based plaintext-checkable encryption (IBPCE) scheme where anyone can verify whether a ciphertext is the encryption of a plaintext under an identity if the plaintext and the identity are provided. This scheme is fully secure in the standard model. To the best of our knowledge, it is the *first* time that an IBPCE scheme is proposed and proven secure.

Then, we propose an accountable mobile e-commerce (AMEC) scheme by exploiting the proposed IBPCE scheme into the mobile e-commerce scenario. In our scheme, users' identities can be arbitrary strings, such as mobile phone number and e-mail address. The transactions between a buyer and a vendor are encrypted. In case of dispute, an offline adjudicator can identify who is dishonest by checking the encrypted transaction records. Hence, our scheme is an ideal primitive to balance the need for privacy and accountability. We also implement our scheme in the PBC library [25].

1.2. Paper organization

The remainder of this paper is organized as follows. The related work is introduced in Section 2. In Section 3, we introduce the preliminaries which are used throughout this paper. We propose an IBPCE in Section 4. In Section 5, an AMEC scheme is proposed and implemented. We prove the security of the proposed IBPCE in Section 6. Finally, Section 7 concludes this paper.

2. Related work

In this section, we introduce the related work.

2.1. Identity-based encryption

To avoid verifying the public-key certificates used in public-key infrastructure (PKI), Shamir [34] introduced the definition of identity-based encryption (IBE). IBE is a public-key encryption system where users' public keys can be any arbitrary string, such as IP address and e-mail address, and the secret keys are generated by a trusted party called private key generator (PKG). Boneh and Franklin [5] first proposed a secure and practical IBE scheme using bilinear groups. This scheme was proven to be secure in the random oracle model [4]. As mentioned in [7], a scheme which is secure in random oracle model does not necessarily imply that it is secure in the standard model. Subsequently, Canetti, Halevi and Kat [8] proposed an IBE scheme which was proven without using the random oracle, but in a weak model called the selective-ID model. Waters [43] and Gentry [16] proposed two efficient and practical IBE schemes which are fully secure in the standard model.

2.2. Plaintext-checkable encryption

Canard et al. [6] proposed a plaintext-checkable encryption (PCE) scheme which is universally possible to check whether a ciphertext is the encryption of a plaintext under a public key if the plaintext and the public key are publicly known.