Journal of Computer and System Sciences 81 (2015) 615–631

Contents lists available at ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

Fair signature exchange via delegation on ubiquitous networks

Q. Shi [a,*], N. Zhang [b], M. Merabti [a]

[a] School of Computing & Mathematical Sciences, Liverpool John Moores University, Byrom Street, Liverpool L3 3AF, UK
[b] School of Computer Science, The University of Manchester, Oxford Road, Manchester M13 9PL, UK

ARTICLE INFO

Article history:
Received 17 December 2010
Received in revised form 11 September 2012
Accepted 24 October 2014
Available online 6 November 2014

Keywords:
Ubiquitous computing
Fair exchange
Signature
Communication protocol

ABSTRACT

This paper addresses the issue of autonomous fair signature exchange in emerging ubiquitous (u-) commerce systems, which require that the exchange task be delegated to authorised devices for its autonomous and secure execution. Relevant existing work is either inefficient or ineffective in dealing with such delegated exchange. To rectify this situation, this paper aims to propose an effective, efficient and secure solution to the delegated exchange to support the important autonomy feature offered by u-commerce systems. The proposed work includes a novel approach to symmetric-key based verifiable proxy encryption to make the exchange delegation flexible, efficient and simple to implement on resource-limited devices commonly used in u-commerce systems. This approach is then applied to design a new exchange protocol. An analysis of the protocol is also provided to confirm its security and fairness. Moreover, a comparison with related work is presented to demonstrate its much better efficiency and simplicity.

1. Introduction

The advance of ubiquitous computing technology enables everyday objects such as refrigerators and toasters to be augmented with information processing capabilities to offer ubiquitous network platforms on which to build smart integrated applications and services. This opens up great opportunities for pressing current electronic or mobile (*e*/*m*-) commerce technologies forward to provide seamless and intelligent business services from anywhere at anytime, which is also called ubiquitous (u-) commerce. While u-commerce greatly enhances the quality of life for individuals and families, its systems typically involve distributed and autonomous operations running on much open, dynamic and resource-diversified ubiquitous networks. These features are making the system security protection very challenging. Without proper security assurance, the wide acceptance and deployment of u-commerce would not become reality.

One of the important security challenges for u-commerce systems is about how to fulfil fair signature exchange. Such exchange means that two parties (e.g. individuals, companies or systems) can exchange their valuable digital signatures for agreed commercial transactions such as contract signing over networks without one party being disadvantaged by the other during the exchange process. More specifically, the fairness requires that either each party, or neither of them, can get the expected signature from the other party at the end of the exchange, which is also referred to as strong fairness [1]. This requirement is essential for preventing one party from deceptively gaining business or financial advantages over the other.

To conduct a fair signature exchange, the existing work normally simplifies the exchange settings by assuming that decision making responsibilities for the exchange rest with the parties involved in the exchange and trusted computing

* Corresponding author. Fax: +44(0) 151 207 4594.
E-mail addresses: Q.Shi@ljmu.ac.uk (Q. Shi), ning.zhang@manchester.ac.uk (N. Zhang), M.Merabti@ljmu.ac.uk (M. Merabti).

http://dx.doi.org/10.1016/j.jcss.2014.11.001
0022-0000/

devices are employed to execute the exchange. This simplification leads to a more focused issue of how to exchange the agreed signatures fairly without concerns about the environment in which the exchange is conducted. Accordingly the solutions developed under such assumptions are applicable to less intelligent e/m-commerce systems with fairly static exchange scenarios and settings.

However, emerging u-commerce systems are posing new challenges to fair signature exchange owing to their more complex features such as high autonomy, distributability and heterogeneity. To illustrate such features, we present the following example about a potential u-commerce setting for a user Alice and her smart home, which is derived from the example given in [20]:

- Alice is informed at work that her request for changing to a more rewarding job within her organisation has been granted. She is delighted with the news, and decides to invite her parents for dinner in her house in the evening to tell them the good news at the dinner table.
- She uses her smart phone to prepare a list of groceries needed for the dinner and sends it to her home manager—a software agent running on one of her home computing devices.
- The home manager responds to the request by initiating the following tasks:
  - Checks the RFID (radio frequency identification) enabled fridge and cupboards in the kitchen in reference to the received grocery list to decide what to buy, asks price quotations from nearby supermarkets, and sends a purchase order to the supermarket, offering the best deal, for home delivery in the afternoon;
  - Inspects the networked heating facilities fuelled by either solar power or gas controlled by a "pay as you go" meter, finds that the fuel supply is insufficient to keep the house warm due to cold weather, and thus decides to buy additional credits on-line from a gas supplier to top up the gas meter.
- Alice arrives at home after work, prepares the dinner with the delivered groceries, and shares the good news and nice meal with her parents in the warm house.

This application scenario involves the following signature exchanges:

(1) Alice's payment authorisation signature on the grocery order is exchanged for the supermarket's signature on a digital receipt for the paid groceries;
(2) Alice's payment authorisation signature on the gas credit purchase is exchanged for the gas supplier's signature on a digital ticket of the purchased credits.

Clearly, the above example demonstrates that Alice's home system is autonomous in deciding what, from whom, when and how purchases should be made with regard to given policies or requests. In this case, it is crucial for Alice to delegate the signature generation and exchange to her agent–home manager. Otherwise, she would have to make herself available for signing signatures when they are required, as she often does not know beforehand what to sign, e.g. the gas credit purchase mentioned above. This would seriously hinder the system's efficiency and effectiveness, especially when a signature is needed but Alice is unavailable to sign it.

Additionally, the system makes use of heterogeneous computing facilities ranging from small microprocessors embedded in devices such as a gas meter to a big home computer. The system operations are highly distributed among home appliances, mobile devices and the Internet for collaborative smart decision-making and autonomous execution. Clearly these capabilities are essential for the provision of smart services, which are much more beneficial to users than those offered by the existing e/m commerce applications. However, such benefit also brings complication into the u-commerce system. Particularly, its operations are much more open, dynamic, inter-operative and autonomous. This does not match the assumptions mentioned earlier for the development of existing signature exchange solutions, as exchange decision is no longer directly made by a user and computing devices used for the exchange could be vulnerable to security attacks. Consequently the existing solutions are either ineffective or inefficient to properly handle signature exchange in u-commerce settings, as will be discussed further later. Hence more research is needed to devise more suitable solutions.

The focus of this paper is on how to delegate the signature exchange task to an autonomous agent(s) and ensure the exchange fairness and security, which are essential for the exchange in u-commerce settings. So far, a large number of protocols have been developed for fair exchange [1–5,7,8,14,18–20,22–25]. Nevertheless, they are hardly intended for the emerging autonomous exchange scenarios of u-commerce. These protocols are mainly based on verifiable signature encryption to achieve the exchange fairness. They can be divided into two categories in terms of the types of encryption. The majority of the protocols fall in the first category that employs public-key based verifiable signature encryption (e.g. [2–5]). The other category comprises the protocols built on symmetric-key based verifiable signature encryption (e.g. [19,20,25]).

The public-key based verifiable signature encryption allows its task to be delegated to a chosen agent(s), namely, it is applicable to u-commerce systems. The reason for this is that a public key is used to verifiably encrypt a signature, so the public key can be directly given to the agent for performing the signature encryption. However, the symmetric-key based verifiable signature encryption is unsuitable for its direct delegation to a chosen agent, i.e., it is not directly applicable to u-commerce systems. Since a secret key is employed for a verifiable symmetric encryption of a signature in this case, the delegation of the encryption task to a chosen agent would require directly assigning the secret key to the agent. This