A Practical Approach of Fairness in E-procurement

Debajyoti Konar, Presidency University, India
Chandan Mazumdar, Jadavpur University, India

ABSTRACT

In this paper the authors present a practical approach of fairness in E-procurement. A generalized model of E-procurement is also presented here, which includes both E-contracting and E-trading. The model also proposes the generalized methodologies to develop E-procurement protocols that ensure fairness in true sense without using an additional trusted third party. They conclude this paper by indicating the area of applicability for their model.

Keywords: E-Contracting, E-Procurement, Fairness, Graduate Secret Release (GSR) Fair Exchange Protocol, Information Security

1. INTRODUCTION

In this new scenario of E-commerce, procurement is shifted to E-procurement for low cost and high efficiency. Since transactions in such businesses transcend the boundaries of states and countries, it may become difficult to trace maliciously behaving transacting parties. Moreover, since transactions are made over public channels such as the world-wide web, information security becomes a major barrier to the success of such E-commerce transactions. This situation leads to major research efforts on information security services, viz., confidentiality, integrity, availability, authentication, and non-repudiation. Among these, non-repudiation is a security service that creates, collects validates and maintains the cryptographic evidences to support settlement of possible dispute among the transacting parties. The transacting parties will have more confidence in taking part in E-procurement with the provision of non-repudiation service. Two or more parties involving in a commercial transaction can identify their activities as a sequence of message exchanges, or in short a protocol. During these exchanges in the protocol, a non-repudiation service protects all transacting parties from false denial of having been involved in the transaction.

The fairness of these protocols is the way that guarantees that either all the parties obtained what they want or none do. The issue of fairness is becoming increasingly important in fast growing scenario of E-commerce. The current proliferation of on-line auction venues, E-shopping malls and other similar sites makes it difficult for a user to establish the credibility of a counter party in a commercial transaction

DOI: 10.4018/jisp.2012070105
on the internet. So *E-procurement protocols* are required to provide mutual guarantees to the protocol participants and ensure fairness. As a result, fairness of e-procurement protocols has become an important field of research.

A common approach to ensure fairness is to include a Trusted Third Party (TTP) in the transactions, in *Inline, Online, or Offline* mode. In many of these TTP-based protocols, some important application specific properties are maintained. But, the subscription to and maintenance of such TTPs are costly. In a second approach, instead of using a TTP, Secrets are released gradually resulting in so-called Graduate Secret Release (GSR) protocols. But, most of such protocols fail to provide application specific properties. The challenge is to develop GSR protocols with acceptable fairness for e-commerce activities, which satisfy the application specific properties. Availability of E-payment systems and online banking coupled with the popularity and rising demand of e-procurement, provides the motivation of this research.

**2. PREVIOUS WORK**

In this section we discuss briefly some related work in providing fair-exchange in E-commerce. In previous works, trusted third party (TTP) is used in most of the fair exchange protocols either in offline mode or in online mode. By using the third party in off-line mode, the optimistic fair exchange protocols have a considerable contribution in the field of fair exchanges in E-commerce. There are some GSR protocols for fair exchange in which the participants increase the probability of fair exchange gradually over several rounds of message exchanges.

The idea of using a trusted third party in on-line mode to obtain non-repudiation of origin and delivery of an email message was proposed by Deng, Gong, Lazar, and Wang (1996) and Zhou and Gollmann (Sandholm & Lesser, 1996). In essence, these protocols are similar. An E-Payment Protocol to Realize Fair- Exchange by Zhang, Mayes, and Markantonakis (2004) has been designed to provide a user centric m-payment solution over internet by ensuring fair exchange, customer’s anonymity and implementing an embedded biometric authentication framework for high security requirement. Without using any financial institution, the protocol engages seven principal participants, viz, Payment Applet in the SIM Card (PA), Mobile Phone (MP), Bio-Applet in the SIM Card (BA), Merchant’s Application (MA), Trusted Third Party (TP), Delivery Cabinet (DC), and Mobile Operator (MO). Using an on-line trusted third party the protocol involves twelve message exchanges. The protocol proposes the sensitive information, viz., user’s private key etc are to be stored in SIM card and non-repudiation of the origin (NRO) for the request and response is achieved by digital signatures using the sender’s private keys. The protocol has no conflict with customer’s anonymity property. The correctness of the product is assured by theory of cross validation within this protocol. But maintaining on-line third party makes the protocol costly in implementation and use.

There are several fair exchange protocols that use third party in offline mode, when it is required and hence they are optimistic fair exchange protocol. These protocols are designed either to sign a contract or to purchase a digital product. An Optimistic Contract Signing Protocol (Asokan, Shoup, & Waidner, 1998) has been designed to provide a service to Originator and Responder for obtaining each other’s commitment on a previously agreed. The protocol consists of three interdependent sub-protocols, viz., Exchange sub-protocol, Abort sub-protocol and Resolve sub-protocol. This asynchronous protocol, in essence, a fair exchange protocol involves three participating parties, viz., originator (O), Responder (R) and trusted third party (T). As it is a contract signing protocol, the protocol does not consider the anonymity property for any transacting party and also the correctness of the text property. On the other hand there are some effective works to provide the fair exchange protocols for purchasing of digital
Mobile Worms and Viruses
www.igi-global.com/chapter/mobile-worms-and-viruses/114378?camid=4v1a