Imposing fairness in electronic commerce

Using Trusted Third Party for electronic product delivery

Fahad A. ALQAHTANI
Software Technology Research Laboratory
De Montfort University,Leicester,United Kingdom

Abstract

In the recent years, electronic commerce has gained much importance. Traditional commerce is slowly being replace with e-commerce and more people tend to prefer doing their shopping online. One of the main reasons for this attraction is the convenience the e-commerce provides. Customers can choose from a lot of different merchants at the convenience of their homes or while traveling by avoiding the hassle and stress f traditional shopping. However, e-commerce has lots of challenges. One key challenge is trust as transactions take place across territories and there are various legal & regulatory issues that govern these transactions. Various protocols and underlying e-commerce technologies help in the provision of this trust. One way to establish trust is to ensure fair exchange. Thus the aim of this research is to propose a protocol that provides fair exchange to the transacting parties by making use of a Trusted Third Party.

Keywords—Trust; electronic commerce; fair exchange; Trusted Third Party

1. Introduction

Boston Consulting Group recently did a study on electronic commerce trends and found out that UK is one of the most internet savvy markets that contribute to around 8.3% economy with a total worth of £121 billion that accounts to almost 13.5% of the total sales. The study also indicates that this would go up to 23% by 2016. Nearly 32 million people in Great Britain (which accounts to 66% adults) have used electronic commerce technologies to buy products and services online. [1]

Thus the main idea of the research is to propose an electronic commerce protocol which will ensure that both the transacting parties remain honest while enabling efficient and smooth exchange of information (including payment related information), digital goods and/or services online. Furthermore, the protocol also ensures that the identities of the customers are kept as secret thus providing complete anonymity during the transactions. The research also aims at designing a protocol that would provide automated dispute resolution with the help of the third party.

The research aims at implementing a prototype for the proposed protocol, thoroughly evaluating it against different criteria and model checking the protocol to ensure the logic is correct and validating the protocol to make sure that the core functionality proposed by the protocol holds good and that it satisfies all the key properties. The research proposes to implement the protocol in order to ensure that the designed protocol is ready for use in the real-world and to prove that it is not just a research-based, theoretical design but a robust, fully deployable model.

2. Background

According to Ray [2], a fair exchange protocol is defined as *"a protocol that ensures that no player in an electronic commerce transaction can gain an advantage over the other player by misbehaving, misinterpreting or by prematurely aborting the protocol."* It describes that fairness is achieved in an electronic exchange when at the end of the business transaction, each of the transacting parties fulfils its obligations and receives the item expected or none of the transacting parties involved gets anything.

Asokan [3] defines fair exchange as a system *"that does not discriminate against a correctly behaving player. As long as a player is behaving correctly, a fair system should ensure that other players will not gain any advantage over correctly behaving players."*

There are various protocols that offer fair exchange. There are, however, many drawbacks that could be spotted. For example, Boa's protocol [4] offers fair exchange using an offline TTP. The disadvantage of this protocol is its complexity. Similarly, Ray's protocol [5] provision of anonymous and failure resilient fair exchange is another key protocol in the fair exchange arena. It is an optimistic protocol and invokes the Trusted Third Party only when it is absolutely necessary i.e. an offline TTP. It does not however provide a true fair exchange and the usage of pseudo-identifiers makes it a bottle neck to run this protocol. The next protocol that is key is the practical fair exchange protocol for anonymous purchase and physical delivery by Zhang et al [6]. This protocol provides an effective and efficient way and provides means to support fair document exchange over the internet for electronic commerce transactions by making use of RSA signatures. However, the disadvantage of this protocol is that it becomes very cumbersome to manage the keys efficiently.

In short, the element of trust plays a major role in e-commerce and encompasses many aspects including fairness, anonymity, data protection and privacy. The diagram below explains these elements of trust.

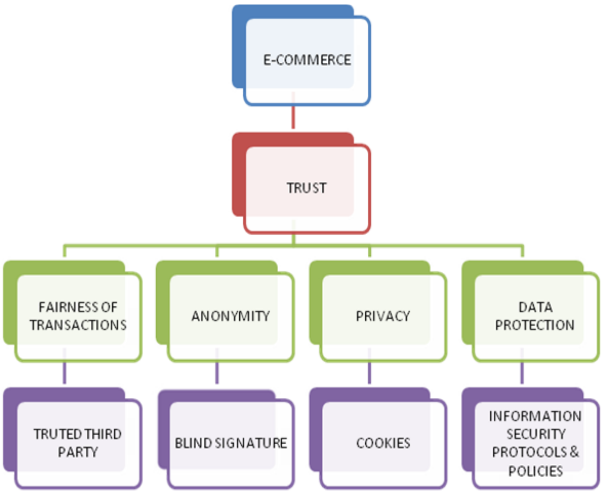

Figure 1: Elements of Trust in E-commerce

3. Proposed protocol aims

The main objective of this research is to propose an efficient and effective protocol for electronic commerce transactions that provide both anonymity and fair exchange. The protocol is based on three other protocols that provide the same features namely Ray et al's anonymous and failure resilient fair-exchange electronic commerce protocol, Zhang et al's Efficient Protocol for Anonymous and Fair Exchange and . Though these protocols have achieved both the above mentioned characteristics of anonymity and fair exchange, there are inherent problems that these protocols have as discussed in the earlier chapters. The protocol also makes use of an online Trusted Third Party to mediate between the transacting parties and also for any dispute resolution purposes. The protocol is also aims at providing fair exchange throughout all phases of an electronic commerce transaction. The protocol proposed hence has the following success criteria:

1. Fair Exchange: The key goal is to ensure true fair exchange where either both the parties or none of the parties gets the goods at the end of the transaction. This ensures that honest parties are not being punished because of the deeds of the dishonest party.
2. Anonymity: Using blind signature concept, the protocol ensures that the customers' identities are kept secret thus providing privacy. This is achieved by using the concept of blind cash.
3. Trusted Third Party: The protocol ensures that the TTP is entirely trusted and not a semi-trusted Third Party that has the ability to masquerade as another party or alter or read messages in anyway.
4. Single Payment Token: The efficiency of the protocol is increased as the payment made is done using a single token rather than multiple tokens with the same denomination.
5. Simplicity: The protocol makes use of symmetric key cryptography wherever possible for example, encryption and decryption of messages to ensure that it is simple and also reduces any computational bottlenecks and key management overheads.

3.1 Abbreviations,Acronyms and Notations

1. Merchant: Merchants are entities (individual or corporate) that have digital products to sell. This entity has the authorization to advertise its intention to sell such goods online from the producer of the online products. Merchants, in return for sale of the digital products, take cash (in the form of electronic cash) from the customer which is then redeemed at the Merchant's bank. In the protocol, Merchant is represented by the letter M.

2. Customer: Customers are entities (individual or corporate) that require digital products sold by the merchant. Customers verify the authenticity of the products using a Trusted Third Party and purchase the online product in exchange for electronic cash that is withdrawn from the Bank. Where the transaction has not been carried out as required, the Customer can initiate arbitration process. In the protocol, Customer is represented by the letter C.

3. Bank: Helps withdrawal and redemption of electronic cash to the Merchant and Customer. The bank is also responsible for verifying details when requested by the Trusted Third Party. In the protocol, Bank is represented by the letter B.

4. Trusted Third Party: Refers to an individual or corporate that helps mediating the electronic commerce transaction. It is an entity trusted by both the Customer and the Merchant. In the protocol, it is represented as TTP.

5. Certificate Authority: Refers to an individual or corporate that is responsible for issuing, verifying and revoking certificates and is represented in the protocol as CA.

6. Producer: Producers are entities (individual or corporate) that create and own digital contents and have the digital copyrights over the products. The producer gives permission to the merchants to sell these products online to customers requiring those. In the protocol, Producer is represented by the letter P.

3.2 Protocol Assumptions

The proposed electronic commerce protocol assumes the following and aims at achieving fair exchange and customer

anonymity. First and foremost, the protocol assumes that a secure communication channel has already been established and will continue to remain secure throughout the electronic commerce transaction. Hence it does not deal with Transport Layer Security. Secondly, the protocol does not dictate who the Trusted Third Party would be. It assumes that the customer and the merchant would have mutually agreed on who the TTP would be and hence not be involved in the selection process.
The other assumptions include:

1. The trusted third party (TTP) is semi-trusted and hence is used only to validate the authenticity of the merchant to the customer and vice-versa. It therefore makes use of TTP heavily in the initial stages while trust is being established.

2. The Trusted Third Party (TTP) cannot read or modify messages sent.

3. The Trusted Third Party will not collude with any other party

4. All parties involved in the protocol will behave rationally

5. The protocol would avoid any replay attacks by making use of cryptographic mechanism such as Digital signature and the messages are time stamped. Time stamps can also be made use in case of dispute resolution.

6. The protocol also assumes that a resilient connection is present between all parties involved namely the customer, merchant and the Trusted Third Party. This means that all messages that are sent are relayed appropriately to the appropriate recipients.

7. With regards to payment, the protocol makes use of digital cash and any double payment is are dealt with and refunded to the customer by the appropriate payment authority.

8. The protocol also assumes that all the transacting parties make use of the same cryptographic mechanisms for all purposes including encryption, decryption, signing messages and hashing.

3.3 Protocol Steps

This section of the document aims at providing a gist of the steps involved in the protocol. In summary, the following are the key stages in the proposed protocol. It describes the messages sent between all parties involved in the protocol process.
Step 1: The merchant gets approval to sell the digital contents from the producer (P), who owns the digital copyrights for the product
Step 2: The merchant, on receiving the go ahead from the producer to sell the products, now gets the digital contents verified by a certificate authority (CA). The CA verifies the identity of the merchant and issues a certificate that is digitally signed.
Step 3: The merchant uploads the product details online to his website to attract potential customers. Along with the product details, the merchant also uploads the certificate received by the certification authority to help enhance the perception of trust.
Step 4: The interested customer now views the product and verifies the digital signature and gets to understand the authenticity of the merchant.
Step 5: The customer withdraws cash (electronic cash) from the bank.
Step 6: The bank issues the electronic cash to the customer
Step 7: The customer, after viewing the digital products available for purchase contacts the Trusted Third Party (TTP) with a hashed, time-stamped and encrypted Electronic Cash. It is encrypted to ensure that the TTP cannot read it, time-stamped to avoid any replay attacks and hashed to protect the integrity of the file and avoid any file tampering.
Step 8: The Trusted Third Party (TTP) verifies the hash and now sends the same to the merchant. This allows the merchant to trust that the customer is indeed genuine and will definitely pay on receipt of products being delivered.
Step 9: The merchant now contacts the Trusted Third Party (TTP) with hashed, time-stamped and encrypted digital product. The product is encrypted to avoid any misuse by intruders or the Trusted Third Party and hashed to be able to verify if tampered.
Step 10: The Third party now verifies this and sends the same to the Customer
Step 11: Merchant and the customer now directly send each other the hash to verify.
Step 12: Each of them verify the hash individually and exchange private keys
Step 13: Merchant requests the Trusted Third Party to send the electronic cash that the customer sent earlier.
Step 14: The Trusted Third Party sends the encrypted cash to the merchant who then decrypts the same using the key exchanged in step 12
Step 15: The Customer requests the Third Party to send the digital product that the merchant sent
Step 16: The Trusted Third Party sends the encrypted product to the customer who then decrypts using the keys exchanged in step12
Step 17: Merchant sends request to the bank to redeem the cash

3.4 Dispute Resolution

At the end of an electronic commerce transaction, just like a traditional commerce transaction there might be disputes that need to be resolved. Unlike traditional commerce, however, the disputes are varied in nature and dispute handling and resolution is a lot different in an electronic commerce scenario.

With specific reference to the proposed Imposing Fairness and Anonymity protocol, after the completion of the transaction between the Merchant (M) and Customer (C), there are four different scenarios that are likely to occur from the point of view of the Customer (C). These scenarios are as follows:

Customer receiving the correct digital products that he/she ordered for

Customer did not receive the correct digital products

Customer received the correct digital products but the product(s) were defective or not according to the specification

Customer did not receive the product at all

The protocol aims at achieving the first output and that is the most desired outcome of the protocol, which is smooth facilitation of the transaction and guaranteeing fair exchange.

Similarly, from the point of view of the Merchant (M), there are three key outcomes that are most likely to occur. These outcomes are as follows:

The Merchant receiving the correct payment for the digital product(s) sold.

The Merchant receiving incorrect payment for the digital product(s) sold.

The Merchant not receiving the payment for the digital product(s) sold.

Again, the protocol aims at achieving the first outcome as that is the most desired one. If however, for any reason the second or the third output occurs, then there is a dispute. Incorrect product refers to the digital product that was not requested by the customer or more specifically a product that does not match the product description given by the merchant. Similarly, incorrect payment refers to the sum of money that does not match the Merchant's price mentioned or more specifically payment that is not exactly what the Merchant advertised and requested. In such cases, dispute resolution plays a major role in identifying the cause of the dispute and provides a means to resolve the issue.

The aim of this sub-section is to discuss in detail the various possibilities that might arise at the end of the electronic commerce transaction and points out to scenarios where there might be issues or disputes. The protocol, however, does not involve or discuss about the mechanism that needs to be used or the steps to be followed when there is a dispute. It is assumed that the aggrieved party in the transaction will take appropriate measures in order to be indemnified.

Table 1: Dispute-Resolution Scenarios

Customer	Merchant	Outcome
Receive the correct product	Receive the correct payment	No Dispute
Receive the correct product	Receive incorrect payment	Dispute raised by the Merchant
Receive the correct product	Does not receive the payment	Dispute raised by the Merchant
Receive incorrect product	Receive correct payment	Dispute raised by the Customer
Receive incorrect product	Receive incorrect payment	Dispute raised either by the customer or the merchant
Receive incorrect product	Does not receive the payment	Dispute raised either by the customer or the merchant
Receive correct product but defective	Receive correct payment	Dispute raised by the customer
Receive correct product but defective	Receive incorrect payment	Dispute raised either by the customer or the merchant
Receive correct product but defective	Does not receive the payment	Dispute raised either by the customer or the merchant

As seen above, there are totally twelve possibilities where the dispute might arise. From the above table it can be noted that if both the parties the customer and the merchant receive the products then there is no dispute.

Similarly, during the electronic commerce transaction, there are various possibilities where disputes might occur. The below table identifies the possibilities where the transacting parties might be dishonest and the scenarios which might lead to a dispute.

4. Research contribution

1. The protocol ensures that the TTP is entirely trustworthy and cannot read messages or masquerade.
2. The protocol will not proceed if one or more parties try to be dishonest. It also avoids any collusion.
3. The protocol is effective and efficient. It satisfies all the success criteria mentioned.
4. By making use of anonymous electronic cash, it provides 100% customer anonymity.
5. It is practical and simple with very less messages.
6. It provides payment security by preventing forging and double-spending.
7. It offers built-in dispute resolution

5. Conclusion and future works

The protocol is designed in such a way where the number of disputes that might arise would also be very much minimal. This is because, neither of the transacting parties namely the Customer and the Merchant would get the digital product or electronic cash before they send the electronic cash or the digital product respectively. The trusted third party will only forward the items to the appropriate entities after receiving items from both the parties. Also, in case of certificates and signatures, both the Merchant and the Customer can verify the correctness of this before sending the digital product or the electronic cash respectively. This is because to forge a signature the private key of the other party needs to be known. For example, if the customer wants to forge a signature on the electronic cash, then the customer would need to know the private key of the bank that would be used to sign the electronic cash. Therefore, the question of incorrect or forged signature is impossibility in this case.

It can also be found that there is a significant reduction in the number of actual messages between the customer and the merchant (which is restricted to two messages while they exchange the private decryption keys). The usage of an inline trusted third party is advantageous as the TTP does not need to be online full time. The trusted third party is not involved in the key exchange process as well and this reduces the overhead on the trusted third party and also makes it more secure. Similarly, in case of disputes (all possible scenarios are clearly shown and discussed by the protocol), the number of messages required to resolve the issues are limited.

The protocol assumes that all channels used for the purposes of telecommunication are secure and this is the basis on which the protocol is able to ensure fair exchange and anonymity. Any failure in securing the communication channel is not a part of the protocol and the protocol does not also describe any fail safe mechanisms or fault tolerant techniques that could be adopted for the purposes of securing the communication channel. Hence this is not within the scope of the protocol. Therefore, this area could be worked on in future development of the protocol.

References

1. New Media Trend Watch, 2013: Ecommerce accessed at: http://www.newmediatrendwatch.com/markets-by-country/18-uk/150-ecommerce
2. I Ray & I Ray, 2002: Fair Exchange in Electronic commerce, ACM SIGecom Exchange
3. Asokan et al, 1997: "Optimistic protocols for fair exchange," in Proceedings of the 4thACM Conference on Computer and Communications Security
4. F. Bao, R.H. Deng and W. Mao, “Efficient and practical fair exchange protocols with off-line TTP”, Proceedings of the IEEE Symposium on Security and Privacy, pp. 77-85, Oakland, California, USA, 1998.
5. Ray, I. Ray and N. Natarajan, “An anonymous and failure resilient fair-exchange electronic commerce protocol”, Decision Support Systems, Vol. 39, No. 3, pp. 267-292, 2005.
6. Zhang et al, “A Practical Fair Exchange E-payment protocol for anonymous purchase and physical delivery”, IEEE conference on System & Application, 2006
7. D Chaum, 1983: “Blind Signature for Untraceable Payment”, Proceedings of Eurorypto’82, pp. 199-203, Plenum press, New York, 1983.