Security Improvement on an Anonymous Fair Exchange E-commerce Protocol

Nay Chi Htun, and Khin Khat Khat Kyaw

Abstract—An anonymous fair exchange e-commerce protocol was proposed by Indrakshi Ray and Indrajit Ray from University of Michigan-Dearborn [1]. This protocol satisfy five features: (1) fairness, (2) Offline TTP, (3) no manual dispute resolution, (4) item-correctness, (5) anonymity. But this protocol has security weakness. An Outsider can compromise and modify the information of Customer and Merchant. Moreover, the contents of some messages can increase the communication overhead. Therefore, the paper makes a security-enhancement over the protocol and reduces the numbers of contents in some messages.

Keywords—e-commerce, anonymous, offline TTP, fairness, security

I. INTRODUCTION

NOWADAYS, the technology has much improved and widespread utilization of World Wide Web, e-commerce plays a vital role for every country all over the world. Many electronic items such as software, music, the account number are sent via Internet everyday. So many ecommerce protocols created by great researchers become important for developing ecommerce. An e-commerce protocol should have the following properties.

Security: Security is the most important property for exchanging items via Internet. Only the intended parties must receive the intended items. Besides, the exchanged items must also be real. None can modify or change the items.

Fairness: Fairness is also one of the most important properties of e-commerce protocols. A protocol can be said as “fair” on condition that after performing that protocol, all members must have the same chance and same authority to influence another member. Fair exchange is usually performed with Trusted Third Party (TTP). TTP is the third party whom believed by both parties. Without TTP, the actual fairness cannot be obtained. Depending on the level of TTP involvement, a protocol can be described in two types: online-TTP and offline-TTP. With online-TTP, every exchange step of the protocol must be noticed by TTP. With offline-TTP, TTP is necessary only when some unnatural behaviors occur.

Item-correctness: Item-correctness is also important for exchanging parties. In some cases, merchant advertises an item with its features on a web page. A customer satisfies the item and tries to buy this item. After the customer had paid, the merchant sent the low-quality product that is not same as one he advertises. Good e-commerce protocols must cover this undesirable fact.

Anonymity: Anonymity is another property of e-commerce protocols. With anonymity, parties involved in the exchange process do not revealed their identities. So merchant does not know who buys his product. Similarly, customer does not know who sells the product.

An e-commerce protocol should satisfy at least two properties: security and fairness. The protocol in [1] satisfies three properties: fairness, item-correctness and anonymity of customer. But it does not satisfy the most important property: Security. So the paper makes a security-improvement over the protocol.

The paper is organized as follow. The original protocol proposed by Indrakshi Ray and Indrajit Ray is described and analyzed in section 2. The proposed protocol is presented and analyzed in section 3. In section 4, the paper is concluded.

II. AN ANONYMOUS FAIR EXCHANGE PROTOCOL

In this section, an anonymous fair exchange protocol with off-line TTP introduced in [1] is briefly described. The notations are described as follow.

C, M, and TP are Customer, Merchant and Third Party
CB and MB: Customer’s Bank and Merchant’s Bank
Cacc: Customer’s bank account with CB
Macc: Merchant’s bank account with MB
m: Product the customer is purchasing
PO: Purchase order used to order product m
Ti: Transaction involving purchase of m
Apriv, Apub: A’s private and public keys
Apriv, Apub: A’s private and public keys used only in Ti
Bpriv, Bpub: Common private and public keys for banks
A→B: X: A sends X to B
[X, K]: Encryption of X with key K
CC(X): Cryptographic checksum of X
K1: Key given to The TP by M
K1-1: Decrypting key of K1 held by third party
K2: Key that is compatible with K1
K2-1: Decrypting key corresponding to K2
r: Random number chosen by merchant for Ti
r-1: Multiplicative inverse of r modulo N2
P: Payment token used for paying for the product
MTI: money transfer instruction
M registers itself with TP by sending m, its description with the cost, and the key pair (K1, K1-1) to TP. TP encrypts the
product with $K_1$ and advertises it on the web. When C wants to buy m, he sends PO to M. M replies by encrypted m and encrypted his account. Then C asks CB to generate P and send back him. Next C forwards P to M. M sends P to MB. MB responds M with acknowledgement when $M_{acct}$ is incremented. Finally, M sends $K_2^{-1}$ to C to decrypt m.

A. Preface
- M registers with TP, by sending the product m, its description with the cost, and the key pair, $(K_1, K_1^{-1})$ to TP.
- M generates a public/private key pair, $(M_{ipub}, M_{ipriv})$, and provides the public key, $M_{ipub}$, to TP.
- C gets [m, $K_1$] and $M_{ipub}$ from TP.
- C generates a public/private key pair, $(C_{ipub}, C_{ipriv})$ for Ti.
- All banks share a common public, private key pair $(B_{cpub}, B_{cprv})$.

B. Main Protocol

Message1: $C \rightarrow M$: [PO, [CC(PO), C_{ipriv}], [C_{ipub}, M_{ipub}]]
- PO includes the product that C wants to buy, the Price, the pseudo identities of C and M, and other necessary information.

Message2.1: $M \rightarrow C$: [Abort, $M_{ipriv}$]
- Or

Message2.2: $M \rightarrow C$: [CC(PO), $M_{ipriv}$], [m.r, $K_1$]×$K_2$, [CC([m.r, $K_1$]×$K_2$), $M_{ipub}$], [K1×$K_2$], [CC([m.r, $K_1$]×$K_2$), $M_{ipub}$], [CC([m.r, $K_1$]×$K_2$), $M_{ipub}$], [CC([m.r, $K_1$]×$K_2$), $M_{ipub}$]
- MTI contains the amount of money to transfer, $C_{acct}$ and [M_{acct}, MB_{pub}]

Message3.1: $C \rightarrow CB$: [[MTI, C_{ipriv}], CB_{pub}]
- CB asks TP to generate P and sends it to C. Instead, if M claims that he did not received the product in message3, he forwards the message to C. Then C first uses his signature to verify message4. If there is no problem, CB generates P and sends it to MB. MB asks C to generate message5. If C receives message5, he sends message6. If M receives abort message in message5, he aborts the transaction. Otherwise, M sends C’s forwarded message with MB’s public key and forwards to MB.

Message7: $M \rightarrow CB$: [K1×$K_2$], [CC([m.r, $K_1$]×$K_2$), $M_{ipub}$]
- Finally, C uses $K_2^{-1}$ to decrypt [m.r, $K_1$] and he gets m.r mod $N_2$. C then multiplies this with r^{-1} and extracts m.

C. Recovery Protocol

In recovery protocol, C does not need to complain to TP because he sends the product decryption key only if he gets the money. For C, the event that M does not give product decryption key even if he paid the cost can exist. For this case, C needs to run the recovery protocol. C sends the signed checksums (signatures) received from M and payment token (P) to TP. TP then verifies P from any bank and asks M to send product decryption key to him. During a certain amount of time, if he receives product decryption key from M, then he forwards it to C. Instead, if M claims that he did not received P, then TP sends P to M. If M does not reply during a predetermined amount of time, TP sends $K_1^{-1}$ to C. C then can decrypt [m, $K_1$] with $K_1^{-1}$ and can get m.

D. Analysis of the Protocol

According to the protocol, C verifies the correctness of the item with cross validation theory in receiving message 1. So the protocol ensures item correctness. According to main and recovery transactions, it can be clearly seen that true fairness can be given by the protocol. TP involves only when dispute occurs and it is not necessary manual dispute resolution process. However, the protocol has security weak points.

Message 1 consists of three parts. The first part is PO. PO is not encrypted with any key. Here, the intruder can easily learn PO. The second part is checksum of PO encrypted with his private key. Here, the intruder knows PO so that he computes checksums of PO, encrypted with his private key and replaces the second part with his created part. Similarly he can replace the third part. He can get $M_{ipub}$ by downloading from TP. So he decrypts his public key with $M_{ipub}$ and replaces the third part with his created parts. Then he sends the whole message to M pretending to be C. When M replies with message 2.2, he forwards the message to C. Then C performs message3 and 5.1 and CB performs 4.1. Similarly, M performs message 6 and MB performs message 7. When M generates message8, he uses intruder’s public key to encrypt the product decryption key according to the cross validation theory. For the positive case, C encrypts MTI with his private key for authentication. Then this information is encrypted with CB’s public key and sent to CB.

In message4, if there is no problem, CB generates P and encrypts it with common private key of banks. Next, CB encrypts this information with C’s public key and sends back to C. Otherwise, CB replies failure message to C.

In message 5, for the positive case, C encrypts CB’s message with M’s public key and forwards to M. For the negative case, C sends abort message to M.

In message6, if M receives abort message in message5, he aborts the transaction. Otherwise, M encrypts C’s forwarded message with MB’s public key and forwards to MB.

In message7, after MB credits to M’s account, he replies acknowledgement to M.

In message8, M sends r^{-1} and the key to decrypt the product ($K_2^{-1}$) that is encrypted with C’s public key, his signature on them. r^{-1} is the inverse of r modulo $N_2$.

Finally, C uses $K_2^{-1}$ to decrypt [m.r, $K_1$] and he gets m.r mod $N_2$. C then multiplies this with r^{-1} and extracts m.
key. So, eventually, the intruder can decrypt the product and he buys the product with the money of C. This type of attack is known as man in the middle attack.

E. Attack Trace

Message 1: \( C \rightarrow M: \text{PO}, [\text{CC(PO),C}_{\text{iprv}}, [\text{C}_{\text{ipub}}, \text{M}_{\text{ipub}}] \)

Intruder gets, compromises and imitates Message 1.

Attack 1: \( I \rightarrow M: \text{PO}, [\text{CC(PO),I}_{\text{iprv}}, I_{\text{ipub}}, \text{M}_{\text{ipub}}] \)

Message 2.1: \( M \rightarrow C: [\text{Abort}, \text{M}_{\text{iprv}}] \)

Message 2.2: \( M \rightarrow I: [\text{CC(PO),M}_{\text{iprv}}, [\text{m.r.K1} \times K2], [\text{CC(m.r.K1} \times K2), M_{\text{iprv}}, \text{[r.K1]}, [\text{CC(r.K1)}], M_{\text{iprv}}, [\text{M}_{\text{acct}}, \text{MB}_{\text{pub}}], [\text{CC}([\text{M}_{\text{acct}}, \text{MB}_{\text{pub}}]), \text{M}_{\text{iprv}]} \)

Attack 2: \( I \rightarrow C: [\text{CC(PO),M}_{\text{iprv}}, [\text{m.r.K1} \times K2], [\text{CC(m.r.K1} \times K2), M_{\text{iprv}}, \text{[r.K1]}, [\text{CC(r.K1)}], M_{\text{iprv}}, [\text{M}_{\text{acct}}, \text{MB}_{\text{pub}}], [\text{CC}([\text{M}_{\text{acct}}, \text{MB}_{\text{pub}}]), \text{M}_{\text{iprv}]} \)

Message 3: \( C \rightarrow CB: [[\text{MTI}, C_{\text{iprv}}], \text{C}_{\text{ipub}}, \text{M}_{\text{ipub}}] \)

\( \text{MTI} \) contains the amount of money to transfer, \( \text{M}_{\text{acct}} \) and \( [\text{Macct,MB}_{\text{pub}}] \)

Message 4.1: \( CB \rightarrow C: [[\text{P,B}_{\text{iprv}}], \text{M}_{\text{ipub}}] \)

\( P \) includes the amount of money to be credited, the encrypted M’s account to be credited and a nonce to prevent replay attack.

Or

Message 4.2: \( CB \rightarrow C: [\text{Failure, C}_{\text{ipub}}] \)

Message 5.1: \( C \rightarrow M: [[\text{P,B}_{\text{iprv}}], \text{M}_{\text{ipub}}] \)

Message 5.2: \( C \rightarrow M: [[\text{Abort}, C_{\text{ipub}}] \)

Message 6: \( C \rightarrow MB: [[\text{P,B}_{\text{ipub}}], \text{M}_{\text{ipub}}] \)

Message 7: \( MB \rightarrow M: [\text{ack,MB}_{\text{ipub}}] \)

Message 8: \( M \rightarrow C: [[k_2^{-1}, r^{-1}], M_{\text{iprv}}], C_{\text{ipub}}] \)

The improved protocol modified three messages: message 1, 2.2 and 8, of the main protocol.

Message 1 consists of two contents: \( [\text{PO}, C_{\text{iprv}}] \), PO encrypted with C’s private key for data origin authentication, and \( C_{\text{ipub}} \), C’s public key used for current transaction. These two contents are encrypted with M’s public key for current transaction, \( M_{\text{ipub}} \). Later M can decrypt the message with his private key and use C’s public key to verify the origin of PO.

Message 2.2 contains four parts: \( [\text{PO}, M_{\text{iprv}}] \), PO encrypted with M’s private key that is to prove that he actually receives C’s real message, \( [\text{m.r.K1} \times K2] \), encrypted \( m.r \), \( [r.K1] \), encrypted \( r \) and \( [\text{M}_{\text{acct}}, \text{MB}_{\text{pub}}] \), the encrypted M’s bank account to be credited. These four contents are encrypted with M’s public key, \( C_{\text{ipub}} \).

Message 8 consists of \([k_2^{-1}, r^{-1}]\), product decryption key and inverse of \( r \) modulo \( N_2 \) that are used by C to extract \( m \). They are encrypted with M’s private key, \( M_{\text{iprv}} \), to ensure data origin and source authentication. The information is next encrypted with C’s public key, \( C_{\text{ipub}} \).

In the modified protocol, the use of checksum is cancelled to save the computation and communication overhead. The aim of using checksum is for authentication and evidences. Instead, private key encryption is used as the signature for authentication and evidences.

C. Recovery Protocol

The recovery protocol is similar to the original one. Without using checksums, C sends the signed data received from M and payment token (P) to TP to run the recovery protocol.

D. Analysis of the Protocol

The modified protocol can recover the security weakness of the old one.

In the original protocol, message 1 is sent without encrypting. So the intruder can easily learn the contents of the message.

In modified protocol, message 1 is encrypted with M’s public key before sending. So only M can learn the contents of the message. If the intruder gets the message, he cannot learn the message. So he cannot compromise, modify and change the
contents of the message. Encrypting with M’s public key is able to give data integrity and confidentiality properties. Moreover, message 1 of modified protocol deletes the use of checksums to reduce the cost. Here, the original properties of the old one still remains.

In original protocol, message 2 is also sent without encrypting. So the intruder can get the knowledge about the contents of the message. Here, it is noticed the intruder gets the knowledge about message 2 as much as C can.

In modified protocol, message 2 is encrypted with C’s public key. That’s why, only C gets the content of message. If the intruder sees the message, he cannot know anything about the message due to the data integrity and confidentiality properties of modified protocol. Here, the cost of message 2 is also reduced by eliminating signed checksums.

Message 8 of the modified protocol is as safe as that of original one. But it saves the cost of message by removing checksums.

**IV. CONCLUSION**

E-commerce protocols are most important for improving e-commerce applications. Good-quality e-commerce protocols must be proposed by the researchers although everything is not perfect. As a consequence, more and more users begin to trust on the e-commerce applications. The protocol was proposed by Indrakshi Ray and Indrajit Ray is the protocol that satisfies five good features. But it has weakness in security of the message contents. The paper overcomes the security weak points of the original protocol. Moreover the paper reduces the computation and communication overhead by removing signed checksums.

**ACKNOWLEDGMENT**

We foremost thanks go to Professor Dr. Aung Win, the Principal of the Technology of University in Yatanarpon Cyber City, for welcoming our research and giving a hand for us. Next, we would like to thank Professor Dr. Soe Soe Khaing, the Head of the Department of Information and Communication Technology in our university, for giving a chance to fulfill my goal. Moreover, we also wish to thank to the other members of our department for encouraging us and offering guidelines about our research. Besides, we also thanks Indrakshi Ray and Indrajit Ray from University of Michigan-Dearborn for their idea of the original protocol. Finally, our thanks go to our families and friends for all the love and kindness they give us.
REFERENCES


