16th Bled eCommerce Conference

eTransformation

Bled, Slovenia, June 9 – 11, 2003

A secure electronic Murabaha transaction

Mansour A. Al-Meaither

Information Security Group, Royal Holloway, University of London,
Egham, Surrey, TW20 0EX, UK.
Phone: +44 1784 444150, Fax: +44 1784 430766
M.Al-meaither@rhul.ac.uk

Chris J. Mitchell

Information Security Group, Royal Holloway, University of London,
Egham, Surrey, TW20 0EX, UK.
Phone: +44 1784 443423, Fax: +44 1784 430766
C.Mitchell@rhul.ac.uk

Mansour A. Al-Meaither, Chris J. Mitchell

Abstract

Conventional credit card transactions are not consistent with Islamic principles, as exemplified by the Islamic banking system and the 'Murabaha sale'. Thus, if Islamic principles are to be applied to e-commerce, where credit card transactions are the norm, a new and secure electronic payment process is required. In this paper we present a method for secure electronic Murabaha transactions. After introducing the notion of Murabaha sale within the Islamic banking framework, we describe a general model for a secure electronic Murabaha transaction, and then consider the associated security risks. Security requirements are then identified for a secure electronic Murabaha transaction. We then present the Secure Electronic Murabaha Transaction (SEMT), designed to address the identified security requirements. Finally, we analyse how the proposed protocol matches the identified security requirements.

1. Introduction

The emergence of the Internet has led to the development of new electronic commerce (e-commerce) protocols that seek to reduce both the cost of buying goods as well as the merchant's cost of selling. One of the most important enablers of an e-commerce transaction is the secure Internet payment. Although several e-payment protocols have been proposed, e.g. SET [5], no protocol has to date been proposed to allow electronic sales based on Islamic banking principles.

One of the key concepts of the Islamic economic system is the prohibition of payment and receipt of interest on deposits and loans. Instead, it encourages the sharing of profits and losses among parties to any business transaction. It is thought that this will ensure the de-linking of economic gains from risk-taking. The notion of interest as a reward for delaying consumption is rejected in Islam, on the grounds that people can only be rewarded for their efforts, not for mere waiting.

Modern banking systems were introduced into the Muslim countries in the late 19th century. Many Muslims confined their involvement with these banks to transaction activities such as current accounts and money transfers. Borrowing from banks was strictly avoided in order to avoid dealing in interest, which is prohibited in Islam.

Islamic banks offer financial instruments that are consistent with Islamic religious beliefs. According to Islamic law, the mode of finance should emphasize profit and loss sharing. One of the most widely used transactions in Islamic banking is Murabaha [2].

Although it is difficult to obtain exact figures on the size of the Islamic financial sector, it is nevertheless experiencing strong growth. According to [3], the assets of Islamic banks grew from $5 billion in 1985 to a level of over $100 billion in the late nineties. While conventional banks guarantee the capital and rate of return, the Islamic banking system, working on the principle of profit and loss sharing, cannot, by definition, guarantee any fixed rate of return on deposits.

Islamic law puts many restrictions on contracts to attain maximal justice in a financial transaction, minimise the potential for legal disputes, and build a healthy and stable financial and economic system [1]. Hasanin [2] notes that Murabaha is the most frequently used mode of contract by Islamic banks, accounting for 90 percent of all financing provided by some Islamic banks.

2. Murabaha Sale

Sale is defined in Islamic law as the exchange of a thing of value by another thing of value with mutual consent. Islamic jurisprudence has specified that the subject of sale must be in the ownership of the seller at the time of sale. What the seller does not own, cannot be sold. If something is sold before acquiring ownership, the sale is void.

Islamic banks have devised a number of products based on the religious beliefs associated with risk and profit sharing. Murabaha sale is one of the most commonly used forms of financing provided by Islamic banks. The Islamic bank purchases the goods and then re-sells them to a buyer at a mark-up, as agreed to by both parties.

Murabaha is an Arabic term that means profit and is a type of trust trading. Financially, it means cost plus profit sale, but, in Islamic law, it refers to a particular kind of sale [2].

Islamic financial institutions now use Murabaha sale as a mode of financing. A customer wishing to purchase goods requests the financial institution to purchase these items on his behalf and then sell them to him with a certain amount of profit agreed upon added to the initial cost. The basic component of Murabaha is that the seller discloses the actual cost he has incurred in acquiring the goods, and then adds some profit thereon.

With Murabaha the financial institution buys the goods on behalf of the client and resells them at a mark-up, but in the period up to the resale the bank has title to the goods, and hence a legal responsibility.

2.1 Rules Governing a Murabaha Sale

The validity of a Murabaha transaction depends on certain conditions, which should be properly observed to make the transaction acceptable in Islamic law. In order to understand these conditions correctly, one should appreciate that Murabaha is a sale that has its own implications, and that all the basic ingredients of a valid sale should be present in Murabaha. The rules that govern this principle, as stated by [2], are as follows.

- The two sale contracts, one through which the financial institution acquires the commodity and the other through which it sells it to the buyer, should be separate and real transactions.
- The financial institution must own the commodity before it is sold to the buyer. It is essential to the validity of the Murabaha transaction that the buyer must be aware of the original price, including the costs necessary to obtain the commodity and the profit. This is because Murabaha is a sale with a mark-up, and if the buyer did not know the basic price then the sale is void.

- Both parties, i.e. the financial institution and the buyer, have to agree on the profit for the financial institution from the sale, where the sum of the cost and profit is equal to the selling price charged by the financial institution.
- Murabaha is valid only where the exact cost of a commodity can be ascertained. If the exact cost cannot be ascertained, the commodity cannot be sold on a Murabaha basis.
- It is also necessary for the validity of Murabaha that the commodity is purchased from a third party. The purchase of the commodity from the client on a "buy back" agreement is not allowed in Islamic law. Murabaha based on a "buy back" agreement would be nothing more than an interest-based transaction.

Unless these conditions are fully observed, a Murabaha transaction becomes invalid under Islamic law.

3. Electronic Murabaha Transaction Payment Model

In this section, we describe our model of an electronic Murabaha transaction. The model identifies the entities involved and includes a brief description of their interactions.

3.1 Entities involved

An electronic Murabaha transaction involves interactions between three parties: the buyer, the merchant and the provider. Their roles are straightforward.

- **Buyer:** This is the entity that wishes to buy goods from a merchant, but does not have the cash immediately available to complete the transaction.
- **Merchant:** This is the entity that offers the goods which the buyer wishes to purchase.
- **Provider:** This is a financial institution that acts as an intermediary between the buyer and the merchant. It undertakes the purchase of commodities as specified by a buyer, and then resells them on Murabaha to him for the cost price plus a margin of profit agreed upon previously by the two parties. It does not make a purchase unless the buyer requests it and makes a prior promise to purchase.

Trust is a critical issue in payment systems. In our model, we assume that both the buyer and the merchant trust the provider. This trust is explicit as both the buyer and the merchant have a formally established agreement with the provider that defines the trust and liability relationship, while we do not assume trust between the buyer and the merchant.

3.2 Interactions

In the proposed electronic Murabaha transaction model, the buyer shopping at an Internet merchant site first chooses to pay using Murabaha through a specified provider. The merchant redirects the buyer to the provider to complete the purchase on his behalf. If the provider chooses to proceed with sale, he will calculate his profit, and sends a promise to sell the goods to the buyer once they have been bought. In return, the buyer promises the provider to buy the goods on Murabaha sale for the cost of the goods plus the agreed upon profit. This promise is not binding on either the buyer or the provider, and is not an actual sale. It is just a promise to effect a sale in future on the basis of Murabaha. At this stage the relationship between the provider and the buyer is that of a promisor and a promisee.

Based on the goods description supplied to the provider, he communicates with the merchant Internet site and completes the purchase of the goods. The provider is in a better position to obtain payment discounts from the merchant, who in most cases will prefer dealing with a provider as the merchant will receive payment more quickly and with less risk.

Once the purchase of the goods is settled between the provider and the merchant, the provider notifies the buyer of completion of the purchase. Now, the buyer sends his payment authorisation to buy the goods from the provider on Murabaha.

4. Security requirements for an electronic Murabaha transaction

In order to understand how to make an electronic Murabaha transaction secure, we will start by identifying the risks in the internet environment and the resulting security requirements for all the participants in such a transaction.

4.1 Security Risks

The most likely motive for any attack on an electronic Murabaha transaction would be financial gain. This could be accomplished by creating fraudulent electronic representations of the payment instruction that are accepted as genuine by the provider, or by stealing data from the buyer. If successful this would cause financial loss to the participants and financial gain to the attacker. Alternatively, an attack on an electronic Murabaha transaction might be motivated not by financial gain but by a desire to disrupt a particular system and/or cause losses to one or more of the legitimate parties. The primary areas of vulnerability in an electronic Murabaha transaction system are the computers used in the system, and the messages transmitted between the participants [6].

4.1.1 Unauthorised access to data in computers

An attacker might gain access to a buyer computer and fraudulently utilize the data stored on the computer. For example, insertion of a malicious program into a buyer's computer might enable the attacker to copy or modify payment instructions. Such unauthorised use of buyer payment instructions might only be detected after the buyer received an account statement from the provider, by which time the attacker may already have obtained the desired financial benefit.

4.1.2 Alteration of messages

An attacker could attempt to delete messages, replay messages, or substitute an altered message for a valid one. Critical data in a message, such as the price, could be changed and the message then retransmitted to its intended recipient. Messages authorising the sale could be copied and replayed to the provider in an attempt to repeat transactions on behalf of the buyer.

4.1.3 Impersonation

An attacker with access to the network between the buyer's web browser and the merchant server can take advantage of this access to read and rewrite traffic. Imagine a buyer communicating with a merchant server. The attacker, monitoring communications between the buyer and merchant site, watches for an HTTP redirect to the Provider. In the scheme described below, the merchant site is required to perform this redirection at the beginning of an electronic Murabaha transaction. Seeing this redirection, the attacker intercepts the packet and rewrites the URL in the redirection to a previously established bogus Provider server. This server then acts as a proxy between the buyer and the Provider, and between the buyer and merchant site, impersonating the Provider service to the buyer and vice versa while rewriting all URLs and HTTP redirects to force traffic through the proxy. An attacker could thereby obtain the buyer's payment details and subsequently use them fraudulently.

4.1.4 Repudiation of transaction

Fraud could also be attempted through repudiation of transactions. For example, a buyer could deny that he had authorised a particular Murabaha transaction which has previously been performed. This could cause losses to the provider.

4.1.5 Unauthorised disclosure of data

An interceptor of transaction messages between a genuine buyer and a provider could learn the identity of the buyer, as well as details of the transaction (e.g. price, nature of goods, etc.). In some circumstances this would be an undesirable breach of user privacy.

4.1.6 Denial of service

The distributed nature of an electronic Murabaha transaction makes it vulnerable to denial of service attacks. Obviously, as the usefulness of a system like this increases in proportion to the number of merchants who support the payment method, the effects of a denial of service attack on a provider are potentially severe.

4.2 Security requirements

We next identify what security services are required to combat the threats identified in the previous section.

4.2.1 Confidentiality

Confidentiality for information exchanged between the electronic Murabaha transaction participants is needed. This is especially important in an internet environment where information may travel through network segments that are not necessarily trusted [6]. This security service can be sub-divided into the following.

1. The buyer needs to keep his personal data and payment details secret from outsiders. A non-authorised user should not have access to the transaction details. Moreover, the identity of the buyer must remain anonymous to the merchant.
2. The provider needs to be sure that his transaction information, e.g. pricing, is protected from outsiders.

4.2.2 Authentication

Authentication provides guarantees regarding the identity of the originator of an action [6]. This security service can be sub-divided into the following:

1. The buyer needs assurance that he is being redirected to a genuine provider. Otherwise he might be paying an attacker.
2. The provider needs to authenticate the buyer to prove that he is the legitimate source of the payment instruction received.

4.2.3 Integrity

Integrity ensures that information is not altered by unauthorised persons during transmission, without detection by electronic Murabaha transaction participants [6]. This security service can be sub-divided into the following.

1. The buyer must be aware of the original price of the goods and the amount of profit the provider is charging him before buying the goods.
2. The buyer requires a proof that the provider owns the goods being offered.
3. The provider must be in possession of a proof that the buyer has authorised the payment for the goods using Murabaha sale.
4. No attacker can authorise a false payment on behalf of a buyer.
5. The buyer payment authorisation must be protected against alteration, or any alteration must be detectable.

5. The SEMT Protocol

We now describe the proposed Secure Electronic Murabaha Transaction (SEMT) protocol in detail. SEMT consists of four phases: the *Transaction request phase*, in which the buyer finds goods he wishes to buy at an Internet merchant site, and decides to use Murabaha to pay for the goods; the *Promising phase*, invoked by the provider, wherein the provider promises to sell the buyer the goods he is interested in, while the buyer promises to buy the goods from the provider, once the provider has ownership; the *Purchase phase*, invoked by the provider, wherein he buys the goods requested by the buyer from the merchant, and the *Murabaha phase*, invoked by the provider, wherein the buyer validates the provider's ownership of the goods offered and sends authorisation to the provider to buy the goods at the agreed price.

Initial registration of both buyer and merchant to the provider is necessary. The public keys (encryption and signature verification) of both entities are certified by the provider. Moreover, merchant and buyer receive the public key (encryption and signature verification) certificates of the provider. The registration process is outside the scope of SEMT.

5.1 Notation

Table 1 lists the notation used in the description of the SEMT protocol. Note that in this table, as throughout, || is used to denote concatenation of data items.

Table 1: Notation used in the protocol descriptions

NOTATION	DESCRIPTION
A	The Acquirer.
Account_Number	The Buyer account number with the provider.
Cert_{PK_X}	A certificate for the public encryption key of entity X (i.e. PK_X), issued by the Provider.
Cert_{V_X}	A certificate for the signature verification key of entity X (i.e. V_X) issued by the Provider.
$E_K(D)$	The symmetric encryption of data D using secret key K.
$e_{PK_X}(D)$	The asymmetric encryption of data D using the public key of entity X (PK_X).
$\mathrm{ENV}_X(M)$	The digital envelope on message M intended for recipient X, equal to $E_K(M) \| e_{PK_X}(K)$, where K is a randomly chosen secret session key.
Expiry	Expiry date of the merchant quotation.
ID_X	A string of bits that uniquely identifies entity X within the domain of application of the protocol.
Items	Details of the goods, e.g. quantity, description.
M	The Merchant.
Merchant_URL	The Merchant Internet address.

Murabaha_Price	The price paid to the Provider for the goods by the Buyer, which must equal the cost to the Provider plus an agreed profit.
P	The Provider.
PK_X	The public encryption key of entity X.
Price	The price of the goods asked by the merchant.
Quote_ID	An identifier that uniquely identifies a quotation.
R_i	Random nonce, $i = 1, 2, 3, \ldots$
S_X	The private signature key of entity X.
$S_{S_X}(M)$	The signature on message M computed using the private signature key of entity X. We assume that M can be recovered from the signature; if not, then the notation implies that a copy of M is sent with the signature.
T	Date/Time stamp.
Trans_ID	This is an identifier chosen by the provider which uniquely identifies the context.
V_X	The public signature verification key of entity X.

The SEMT protocol makes use of the concept of a 'digital envelope' for data confidentiality, which combines symmetric and asymmetric encryption. The sender of a message requiring confidentiality protection first generates a random ('one time') secret key for use with a symmetric encryption algorithm. This key is then used with the symmetric algorithm to encrypt the message. The secret key is then encrypted with the public asymmetric encryption key of the intended recipient, and the digital envelope then consists of the concatenation of the asymmetrically encrypted random secret key, with the symmetrically encrypted message.

5.2 SEMT Protocol Description

We now describe the operation of the four phases of the protocol in detail. We start by listing the requirements for use of the protocol.

5.2.1 Specific requirements

In order to execute the protocol, the following requirements must be satisfied by the SEMT participants.

1. Each participant X must have two asymmetric key pairs: one pair used for encryption and decryption and the other (S_X, V_X) used for the creation and verification of digital signatures. This requirement applies not only to buyers and merchants but also to the Provider.
2. Every buyer has authentic copies of the provider public encryption key PK_P and the provider public signature verification key V_P.
3. The buyer, the merchant and the provider must be using the same public key encryption scheme and the same digital signature scheme, see for example, [4].

5.2.2 Transaction request phase

This phase begins when a buyer, shopping at an Internet merchant site, indicates that he wishes to make a specific purchase using SEMT through a specified provider. In return, the merchant prepares and signs a quotation to be presented to the provider to complete the sale of the specified goods on behalf of the buyer.

The quotation prepared by the Merchant contains data related to the goods being offered, such as the specified goods information ('*items*'), price, validity of the quotation ('*expiry*') and address of the merchant web site ('Merchant_URL'). Additionally, the merchant includes in the quotation his identifier ID_M, the provider identifier ID_P, the time T the quotation was prepared and a quotation identifier ('Quote_ID'). The combination of ID_M, ID_P, T and Quote_ID is used later by

the provider to uniquely identify this quotation. In order to protect the quotation contents from eavesdroppers, it is encrypted in a digital envelope constructed using PK_P, the public encryption key of the provider, an authentic copy of which is possessed by every merchant.

After preparing the quotation, the merchant redirects the buyer to the provider with the above quotation included in the query string of the redirect message, along with the merchant's signature verification public key certificate Cert_{V_M}.

In summary, the following steps are performed.

1. $B \rightarrow M$: Request to pay using SEMT through P.
2. M: Generate 'quotation' as
$$S_{S_M}(ID_M \,||\, ID_P \,||\, T \,||\, \text{Quote\_ID} \,||\, \text{items} \,||\, \text{price} \,||\, \text{expiry} \,||\, \text{Merchant\_URL}).$$
3. Set query string to
$$ID_M \,||\, ID_P \,||\, T \,||\, \text{Quote\_ID} \,||\, \mathrm{Env}_P(\text{quotation}) \,||\, \mathrm{Cert}_{V_M},$$
4. $M \rightarrow B$: Redirect B to P.

5.2.3 Promising phase

This three-step phase starts every time a buyer is redirected from an Internet merchant site to a provider. After receiving the quotation prepared in the transaction request phase and successfully decrypting and then verifying the merchant's signature, the provider starts to negotiate with the buyer to assert his willingness to buy the goods specified in the previous phase.

When the buyer is redirected to the provider, the query string is also sent to the provider. After extracting ID_M, ID_P, T and 'Quote_ID', the provider makes sure that there is no previously processed quotation with the same information. Then, using his private key, the Provider first decrypts the encrypted quotation. If successful, he uses the merchant signature verification certificate Cert_{V_M} sent in the query string to verify the merchant's signature on the quotation to ensure that the quotation has not been altered by an adversary.

1. P: Decrypt and verify 'quotation',

If the quotation verified successfully, the expiry date is still valid and the provider chooses to proceed with the sale, he will calculate his profit ('*Profit*'), and then generate and send a *Promise-To-Sell* message to the buyer that contains:
$ID_P||ID_B||$Trans_ID$||T||$items$||$Cost$||$Profit$||$Due_Date.

In addition to his identifier ID_P and the buyer identifier ID_B, the provider includes in the message a transaction identifier ('Trans_ID') to identify the context, the time the *Promise-To-Sell* was created T, the specified goods information ('*items*'), the buying cost of the goods ('*Cost*'), the profit requested by him ('Profit') and the date the provider expects the buyer payment ('*Due Date*'). The inclusion of the profit requested by the provider ('*Profit*') in this message is to satisfy the conditions set out in 2.1. Finally, the message is signed and encrypted by the provider and sent to the buyer. This message promises the buyer that the provider will sell the requested goods to the buyer, once bought from the merchant:

2. $$P \rightarrow B : \mathrm{Env}_B(S_{S_P}(Promise\text{-}To\text{-}Sell)),$$

After receiving the message in step 2 and successfully decrypting and then verifying the provider signature, the buyer will check that the goods promised by the provider ('items') are the requested goods. Also, the buyer will check that both the profit ('Profit') and the due date ('Due_Date') offered by the provider are acceptable to him. If the buyer chooses to proceed with sale, then he has to promise the provider that he will buy the goods once the provider has the ownership of the goods. This is achieved by generating a *Promise-To-Buy* message which contains the same information received earlier in step 2 from the provider, i.e. *Promise-To-Buy* = ($ID_B||ID_P||$Trans_ID$||T||$items$||$Cost$||$Profit$||$Due_Date).
T here represents the time that the buyer created his *Promise-To-Buy*. Then, the buyer signs and encrypts the *Promise-to-Buy* message and sends it, along with its signature verification certificate, to the provider. The *Promise-To-Buy* message is encrypted to protect the contents against eavesdroppers:

3. $$B \rightarrow P : \mathrm{Env}_P(S_{S_B}(Promise\text{-}To\text{-}Buy)) \,||\, \mathrm{Cert}_{V_B}.$$

5.2.4 Purchase phase

When the Provider receives the *Promise-To-Buy* message from the buyer, he decrypts it and then verifies the buyer signature to ascertain the integrity of the received message.

Assuming that the provider is using the SET protocol to submit payment to the merchant, the provider generates a SET protocol *Pay-Request* message based on the goods description ('*items*') contained in *Promise-To-Buy* received from the buyer. The provider send this message to the merchant web site address ('Merchant URL') specified previously in the *Transaction request* phase.

1. *P→M*: *Pay-Request,*

The merchant uses the Pay-Request message to produce a SET protocol *Auth-Request* message asking authorisation from the acquirer. Note that a SET protocol option must be set to make the *Auth-Request* / *Auth-Response* message exchange result in the actual transfer of money, i.e. simultaneous authorisation and capture.

2. *M→A*: *Auth-Request,*

The Acquirer goes through the financial network to obtain payment authorisation. If successful, it generates and digitally signs a SET protocol authorisation response message Auth-Response, indicating success or failure and the actual captured amount.

3. *A→M*: *Auth-Response,*

The Merchant obtains the authorisation response message Auth-Response and verifies the Acquirer's signature. The Merchant then gen erates and digitally signs a SET protocol *Pay-Response* message and transmits it to the provider:

4. *M→P*: *Pay-Response,*

In order to give the buyer evidence that the provider has bought the goods, the provider must forward the response message *Pay-Response* received from the merchant to the buyer:

5. $P \rightarrow B: \mathrm{Env}_B(S_{S_P}(ID_P \parallel ID_B \parallel \mathrm{Trans\_ID} \parallel \mathrm{items} \parallel Pay\text{-}Response))$.

This message will be used to convince the buyer to complete the next phase. The buyer can see if the acquirer has authorised the payment since it is indicated in the data fields *AuthStatus* and *CapStatus* within the *Pay-Response*.

Whilst the Purchase phase described above is based on SET, other methods of Internet payment could easily be used to complete the transaction. SET has been used here primarily for the purposes of illustration.

5.2.5 Murabaha phase

Once the buyer receives the message sent in step 5 of the Purchase phase, he decrypts and then verifies the merchant signature. The buyer retrieves *AuthStatus* and *CapStatus* from the *Pay-Response*, and validates that the acquirer has authorised the payment, i.e. the provider has bought the goods. If convinced, the buyer will send his payment authorisation to the provider using the following *Murabaha-Payment* message:

B→P:

$$\mathrm{Env}_P(S_{S_B}(ID_B \parallel ID_P \parallel \mathrm{Account\_Number} \parallel \mathrm{Trans\_ID} \parallel T \parallel \mathrm{items} \parallel \mathrm{Murabaha\_Price} \parallel \mathrm{Due\_Date}))$$

6. Security analysis

In this section, we examine to what extent the generic security requirements outlined in section 4.2 are met by the SEMT protocol.

SEMT is similar to the traditional SET protocol in that it provides confidentiality and integrity for payment information using public key cryptography. Moreover, it uses digital signatures to authenticate all parties involved in the payment process. However, there are two differences. The first is that the buyer does not submit his payment information through the merchant as in SET. The second difference is that SEMT involves two separate transactions, one between the provider and the merchant, and the other between the buyer and the provider. On the other hand, SEMT is similar to 3-D Secure [7] in that the issuer must be involved in every

transaction. However, 3-D Secure does not require the buyer to have a digital certificate. Instead SSL is used to secure communication between the cardholder and the merchant.

6.1 Confidentiality

All transaction information (e.g. pricing and payment details) in SEMT is encrypted. An attacker cannot recover messages exchanged between a buyer and the provider because all messages are encrypted before transmission. An advantage of SEMT is that the buyer does not need to send any private information via the merchant, unlike in conventional e-commerce schemes where a credit card number is sent to a merchant protected using SSL/TLS. This avoids any concerns regarding the ability of the merchant to store buyer private information in a secure manner. Moreover, this keeps the identity of the buyer anonymous to the merchant, since the buyer need not reveal his identity to anyone but the provider.

6.2 Authentication

Authentication in SEMT is accomplished using digital signatures and public key certificates [4]. An attacker cannot impersonate another participant except by stealing that participant's private signature key.

1. The Buyer needs to authenticate the provider: This requirement is met, because the buyer can verify the signature received in the *Promise-To-Sell* message of the Promising phase, using the provider signature verification key found in his certificate.
2. The provider needs to authenticate the buyer: This requirement is met, because the provider can verify the buyer signature received in the *Promise-To-Buy* message of the Promising phase, using the buyer signature verification key.

6.3 Integrity

Integrity in the secure electronic Murabaha transaction is accomplished using digital signatures. Signing a message with the sender's private key provides evidence that the message content has not been altered or destroyed, accidentally or with malicious intent, since it was signed.

1. *The buyer must be aware of the goods original price and the amount of profit the provider is charging him before buying the goods*: This requirement is met, because the buyer signs the original price *Cost*, and the amount of profit the provider is adding, the *Profit*, is included in the *Promise-To-Buy* message sent to the provider.
2. *The buyer requires evidence that the provider owns the goods being offered*: This requirement is met, because the buyer can verify the merchant signature on the *Pay-Response* message of the transaction phase, and that *AuthStatus* and *CapStatus* are set.
3. *The provider need a proof that the buyer has authorised the payment for the goods using Murabaha sale*: This requirement is met, because the buyer signs the *Murabaha-Payment* message in the Murabaha phase, and the Provider can verify the buyer signature using the buyer's signature verification key V_B.
4. *No attacker can authorise a false payment on behalf of a buyer*: Buyer authorisation is achieved by sending the buyer account number signed within the *Murabaha-Payment* message of the payment phase, and no one but the buyer has the private key necessary to create the required signature. The only way this can be attacked is by stealing the buyer private signature key. Adding a user PIN can provide some defence in the event that the buyer's signature key is compromised.
5. *The buyer payment authorisation must be protected against alteration, or any alteration must be detectable*: This requirement is met, because the payment authorisation supplied by the buyer to the provider during the Murabaha phase must be signed by the buyer.

7 Conclusions

In this paper, we have proposed the Secure Electronic Murabaha Transaction (SEMT) protocol that provides a secure Murabaha sale service on the Internet. We described the protocol in detail, and explained how it meets the identified security requirements. In future work, we intend to modify SEMT to support sales over wireless networks. Other possible future work includes investigating the possibility of porting other sales models based on Islamic banking to the Internet.

References

[1] Mahmoud Amin El-Gamal. A basic guide to contemporary Islamic banking and finance, 2000. http://www.ruf.rice.edu/~elgamal/files/primer.pdf.

[2] Fayad Hasanin. Murabaha Sale in Islamic Banks. The International Institute of Islamic Thought, Herndon, VA, U.S.A, 1996. ISBN 977-5224-23-3.

[3] Zamir Iqbal and Abbas Mirakhor. Progress and challenges of Islamic banking. Thunderbird International Business Review, 41(4–5):381–405, 1999.

[4] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone. Handbook of applied cryptography. CRC Press, 1997.

[5] SET. The SET Standard Book 1 Business Description, version 1.0 edition, 1997.

[6] M. H. Sherif. Protocols for Secure Electronic commerce. CRC Press, 2000.

[7] VISA. 3-D secure system overview, 2002. http://international.visa.com/fb/paytech/secure/main.jsp.