Security Architecture for On-Line Mutual Funds Trading With Multiple Mobile Agents

Nirmala C R nirmala_cr@hotmail.com
Asst. Professor /Department of CS &E
Bapuji Institute of Engineering & Technology
Davangere, 577004, India

Dr.V.Ramaswamy researchwork04@yahoo.com
Professor & Head, Computer Science & Engineering
S B M J C E
Bangalore, India

Abstract

In this paper we propose a security architecture for the transaction procedure of On-Line Mutual Fund Trading system which is implemented using multi mobile agents that helps an individual, who is a kind of Do It yourself investor to invest her/his money in mutual funds online. Here, we modify, design and implement the global standard which provides security for transaction processing in E-Commerce i.e. Secure Electronic Transactions (SET). This eliminates the fraud that normally occurs during money transaction on-line. Modified SET protocol provides authentication of the participants, non-repudiation, data integrity and confidentiality. These features give a guarantee of security during payment procedure. The system is implemented on Aglets Framework - ASDK2.0.2 which is Mobile Agent Development platform and using java programming language. The issues of security and performance are analyzed.

Keywords: Secure Electronic Transaction, User Agent1(UA1), User Mobile Agent1(UMA1), MFC Super Market, Banker Agent.

1. INTRODUCTION

Increasingly, people are dependent on computer networks and Internet to access and pay for goods and services with Electronic Money. E-money or digital cash is merely an electronic representation of funds. The primary function of e-cash or e-money is to facilitate transaction on the network. E-money is a necessary innovation in the financial markets. Where money is involved, fraud occurs by one or the other means. There must be a way to avoid such fraudulence. Hence we have come up with a complete security system for On-Line Mutual Funds Trading system by incorporating mobile agents and modified secure electronic transaction protocol. Our system is an E-commerce application, in which user can buy mutual funds online. This system is also implemented using mobile agent. The system has four interconnected modules namely user module, Mutual Funds Company Super Market module , Internet banking and Payment module and Share and stock market module.

The modifications that we have made to the original SET protocol is different from participants in SET, the card holder, merchant, acquirer and issuer. The main participants here are the Investor (I), The MFC Super Market (M), the IBP (P) and the certificate Authority (CA), which is trusted to issue X.509v3 public-key certificate for the participants. The IBP acts as a financial institution with which the Super market and the investor establish their accounts for processing payment On-Line. Each of these participants may possess two kinds of key certificates one for key exchange which is used for encryption and decryption operations, and the other for creation and verification of digital signature.

1.1 Secure Electronic Transaction

SET aims at achieving secure, cost-effective, on-line transactions that will satisfy market demand in the development of a single, open industry specification. VISA and MASTER CARD have jointly developed the SET protocol which is an application layer protocol. It is a method to secure payment card transaction over the open networks.

1) SET Business Requirements :These requirements specify the following aspects
    i. Provide confidentiality of payment and order information.
    ii. Ensure the integrity of all transmitted data
    iii. Provide authentication that a cardholder is a legitimate user of a credit card account
    iv. Provide authentication that a merchant can accept credit card transactions through its relationship with a financial institution
    v. Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction
    vi. Create a protocol that neither depends on transport security mechanisms nor prevents their use
    vii. Facilitate and encourage interoperability among software and network providers
2) Confidentiality: all messages encrypted
3) Trust: all parties must have digital certificates
4) Privacy: information made available only when and where necessary

1.2 Security Architecture of SET

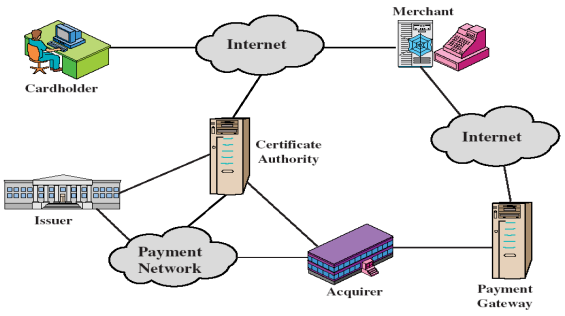

FIGURE 1: Security Architecture of SET

SET changes the way in which participants in the payment system interact. In face-to-face retail transaction or a mail order transaction, the electronic processing of the transaction begins with the merchant or the acquirer. Here the electronic transaction begins with the card holder. The other participant is Issuer, a financial institution which establishes an account for a card holder and issues the payment card. A merchant offers goods for sale or provides a service in exchange for payment. An acquirer is the financial institution that establishes an account with a merchant and processes payment card authorizations and payments. A payment gateway is a device operated by an acquirer or designated third party which processes merchant payment messages.

The encryption systems used by the SET Symmetric Key Encryption System

FIGURE 2: Symmetric Key Encryption

Here same key is used for both encryption and decryption. Examples are DES, 3DES and AES.

Public Key Encryption System

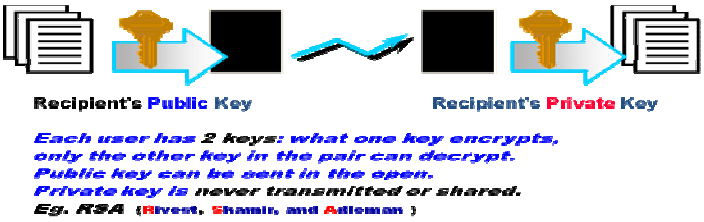

FIGURE 3: Public Key Encryption System

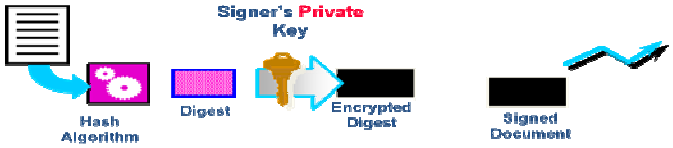

FIGURE 4 : Generating Dual Signature

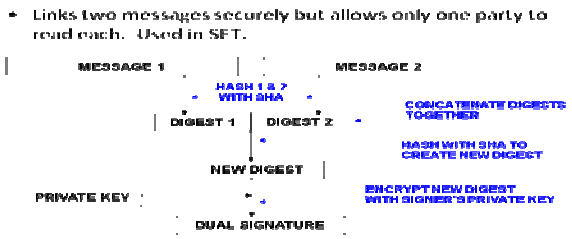

FIGURE 5: Dual Signatures

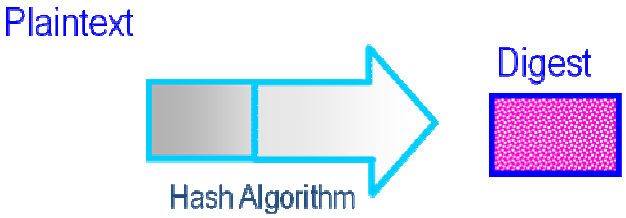

FIGURE 6: Generating Message Digest Using SHA-1

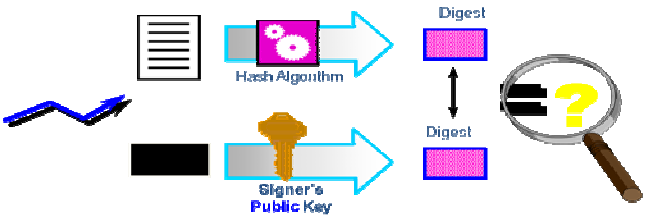

FIGURE 7: Verifying the Digital Signature.

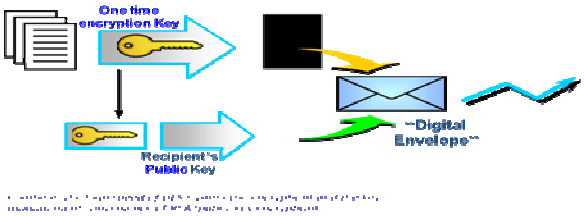

FIGURE 8: Generation of Digital envelop

1.3 Modified Secure Electronic Transaction Architecture

The modified Secure Electronic Transaction has the following architecture.

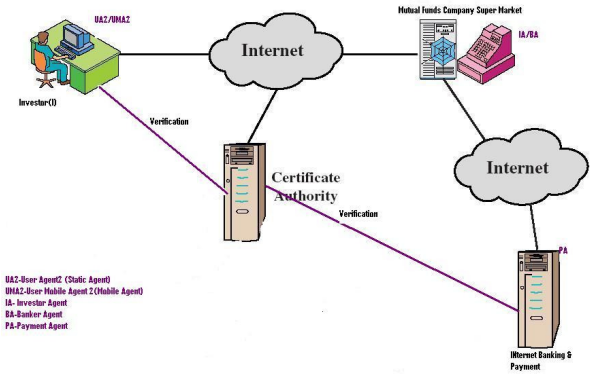

FIGURE 9: Modified SET Architecture

The participants in this architecture are Investor (I), Mutual Funds Company Super Market (M) and Internet Banking and Payment (B). The working process is given below. Consider an individual user who wishes to purchase mutual funds online.

- The user makes use of UA1 and UMA1, browses for the mutual funds and decides to purchase mutual funds.
- Now the second pair of agents at the client system UA2 and UMA2 dispatches encrypted dually signed order and payment information to MFC super market.
- Super market's Investor agent forwards payment Information to Banker Agent.
- Banker Agent in turn transfers the request to Payment Agent at IBP for payment authorization.
- The Investor Agent completes the order.

- Investor agent captures the transaction
- Notification is done to user/client

2. Applications of Modified SET and Multi Mobile Agents

Some of the notations used with the system are as follows.

$ENCk[M]$: encrypt message M with key k

KRi : IA's private Key

Kran: Random signature key generated by IA

Kub: IBP's Public key

Ds : Dual signature

$DS = ENCKRi[H(H(PI) \| H(OI))]$

PI: Confirmed Payment Information

OI: Selected Funds (Order Information)

Cert(x): X's certificate authorized by CA

ID: Transaction Identification

Following steps demonstrate how mobile agents and modified SET together work for securing a transaction of payment in case of user wants to purchase mutual funds online.

1. Investor creates UA2. This UA2 in turn creates UMA2 and fills it with funds selection form in which selected mutual funds are described in detail. The funds selection form later will be used as mutual fund order information (OI). UMA2 then transfers the request to investor agent of super market for performing the task of payment.

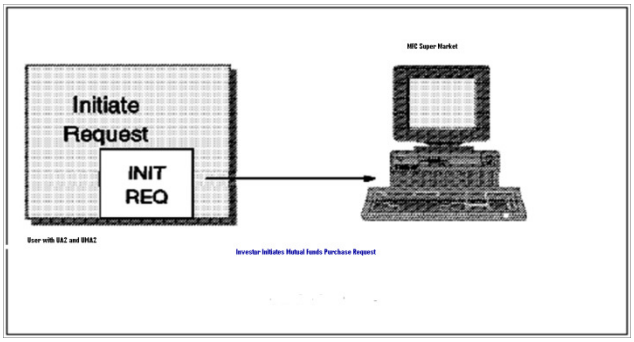

FIGURE 10: Investor Initiating the Purchase request

2. Investor agent who receives OI from UMA2 simply transfers this message to Banker Agent. BA in turn check the investors account balance. If there is sufficient balance, no money from IBP is required. The confirmation message is sent back to mobile agent to inform the investor and process the investor's portfolio management based on the request. Otherwise, the banker agent will assign a unique transaction identifier to the message and then pass its own signature certificate cert (M) and the IBP's key exchange certificate cert (IBP) along with the transaction ID to UMA2. UMA2 verifies super markets and IBP's certificate by tracing through the certificate authorities. It then holds them to be used later during the purchasing process. UA2 continues to create the approved selection form together with its payment.

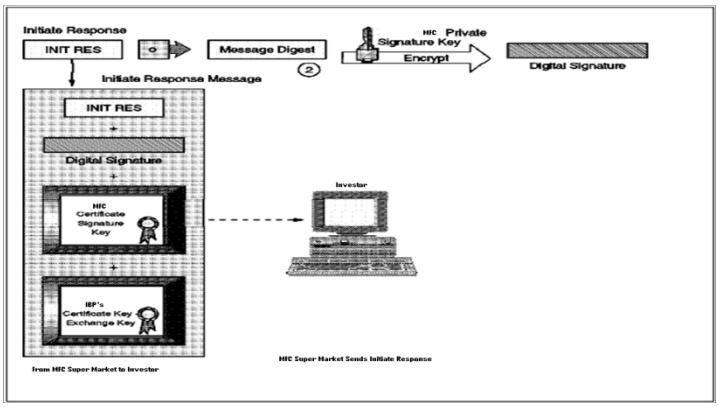

FIGURE 11: Super Market Initiating Response

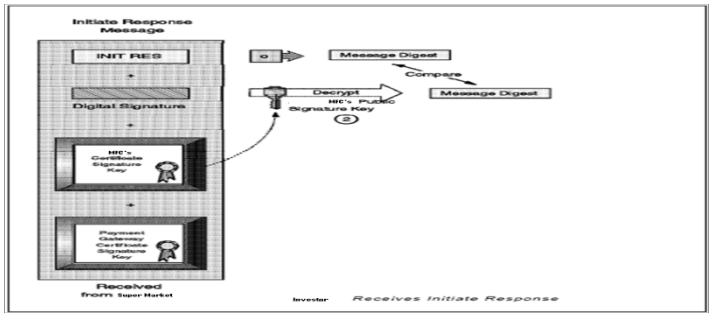

FIGURE 12 : Purchase Request.

3. UA2 dually signs on the two parts of the message (OI and PI) to generate dual signature. OI is the selected mutual fund and PI is the payment information. It then generates a random symmetric encryption key (Kran) and uses it to encrypt the dual signed payment information. Next, UA2 encrypts the PI as well as Kran into a digital envelop using Kub. Finally, UA2 transmits the whole message to UMA2 together with its certificate cert (I). UMA2 is dispatched to IA/BA at the super market.
4.

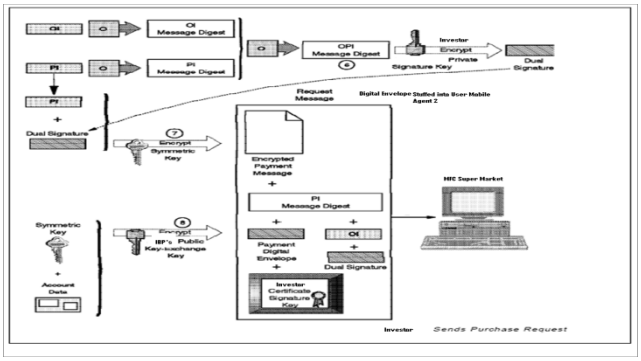

FIGURE 13: Creating and Sending the Digital Envelope

5. Banker Agent verifies the investor's certificate and the dual signature on the first part and then forwards the digital envelope to IBP for autherization. If the authorization response from IBP indicates that the transaction is approved, then the Banker Agent persues the service stated in the request form and at the same time generates the purchase complete message back to UMA2.

6. When UA2 retracts the UMA2 and recieves the message from super market, it verifies the super market signature certificate by traversing the trust ed CAs. It uses super market's public key to check the MFC's digital signature. If everything is correct, it takes necessary action.

In this sytem, most payment and redeem process are done by the mobile agents. The user agent need not be online all the time as defined by the SET protocol.

3. Analysis and Evaluation

The purpose of this work is to implement a secure payment procedure which provides security, confidentiality and data integrity during on-line purchasing of mutual funds. We will discuss some of the security and performance issues, advantages and disadvantages of the system.

3.1 Security Issues

System implementation is based on SET protocol specification with little modifications. Instead of card number, PAN number is used for authentication. Here, all the confidential actions such as signing, authentication, key generation and encryption are performed in the investor's computer (In SET it is done by the card holder). During transaction procedure, sensitive messages are encrypted using secret key. This can be decrypted using the entities which have the public key and read the messages. Finally, the transaction will be completed on IBP in a secured manner.

Note that in [7] MA has to compose OI, PI and generate random symmetric key while residing at the merchant server. This is a very dangerous operation since there is no highly secured way to protect MA from malicious hosts[10]. True there are approaches[11] using Hiding Encrypted Functions (HEF) which can build a secure mobile agent[9] that is capable of producing digital signature. But there is no clear, evidence to show that key materializing can be generated securely at remote server. Therefore, we place the key generation part in step 6 on UA and not on MA for providing secure transaction.

3.2 Performance

The major pit fall to an effective mutual fund transaction is the complexity of payment during the whole procedure. It delays the responses from the investors and thus brings the true compromise to this kind of business. How to make it more concise to pay becomes the crux of adapting proposed system to the real environment. The payment system in the real world is still a real bank based on off-line scheme.

In the system we have attempted to implement, while selecting a mutual fund, he or she can trigger Apriori Agent which does the auto selection of mutual funds. This saves time for user in searching and selecting mutual funds which match the investor profile at that instance. It also makes the choices more suitable to the investor.

In the transaction procedure, the investor payment from her/his online checking account, which is the account in the virtual bank (IBP) along with the certificates from the trusted CA. If it is a real deal, then money is transferred from real bank to IBP for which real bank gives security.

In this work, we have provided security only for transaction procedure. We would like to provide security for all agents and agents servers from malicious hosts and malicious agents using an inter IBP secure transaction and message exchange protocols, the system can be used under International scenario or in the larger perspective.

Beyond meeting the fundamental security and performance requirements, the system shall also have the following potential improvements.

Scalability

The proposed system can also be scaled to an international environment. Let us imagine such a scenario: in the near future where we can have an online network purchase and payment system

around the world. There are many IBPs running at different levels, and different MFCs and investors from all over the world. The investors in one country can search for the MFCs from another country, and pay for her investment from an IBP from the third country, in which she has registered. Compared with the traditional system, the larger the application scenario, the more efficient the transaction.

Practicability
The whole system we describe here is a mutual fund system in the IBP environment. In fact, with the IBPs as the international financial service in the near future, we can also implement other transaction systems by referring to our online payment scheme.

Mobility
More and more mobile users are taking the convenience of mobile network. For example, the WAP users can enjoy great benefits from this system. Only with the mini-browser on her hand-phone, the investor can browse the investment information easily. Because the message exchanged online in this system is limited, with only a few clicks, the investor can finish the transaction assisted by MA in several minutes anywhere anytime via air.

Applicability
In this paper, we proposed a transaction scheme based on SET. It is fully compatible to the original SET. From the investor's point of view, she needs not to make any modification to her SET related software except embedding an agent that executes the investment functions. She may complete the whole transaction in a few steps without knowing the transaction details. This feature enables investors to provide uniform payment method to both online purchase and online investment on mutual funds with only one electronic IBP account, which improves the applicability of the proposed system.

4. Conclusion and Future Work

In this paper, we have analysed, implemented, designed and modified the secure electronic transaction protocol for our system "Multiple Mobile Agents for online Mutual funds trading". This provides security in the form of authentication, data integration, non repudiation etc. This makes the investors to perform transaction without fear of losing their confidential information.

5. REFERENCES

1. Daniel Minoli and Emma Minoli "Web Commerce Technology Handbbok –Secure Electronic Transaction" –Tata McGraw-Hill Edition, 1999: ISBN:0-07-463742-8

2. Nirmala C R and Dr. V Ramaswamy "*Multiple Mobile Agent Architecture for On-Line Mutual Funds Trading*" – in the proceedings of IEEE -2nd International Conference on "E-Learning, E-Business, Enterprise Information Systems, and E-Government (EEEE 2010),. Volume No1. IEEE Catalogue Number: CFP1047I-PRT: ISBN: 978-1-4244-7689-3, pp. 243-246. Luoyang, China ,2010

3. Tieyan Li & Yan Jiang Yang *"Secure Mobile Agent Mediated System for Online Mutual Fund Trading"*

4. Krishna,V., Ramesh,V., *"Portfolio Management Using Cyberagents*." IEEE international Conference on Systems, Man, and Cybernetics, 1998.

5. VISA INTERNATIONAL, and MASTERCARD INTERNATIONAL. "*Secure Electronic Transaction (SET) Specification.*" Version 1.0, May 1997.

6. Artur Romao and Miguel Mira de Silva. ``*An Agent-Based Secure Internet Payment System for Mobile Computing"*, Trends in Distributed Systems'98. Electronic Commerce, Hamberg, German, LNCS, June 3-5, 1998.

7. G.Vigna (Ed.). *Mobile Agents and Security*. Springer Verlag, LNCS 1419, 1998.

8. P. Kotzanikolaou et. al, "*Secure Transactions with Mobile Agents in Hostile Environments"*, LNCS1841, proceeding of 5th Australasian Conference, ACISP 2000, Brisbane, Australia, July 2000.

9. Sander,Tomas; Tschudin,Christian: *On Software Protection via Function Hiding*. Submitted to the 2nd International Workshop on Information Hiding, Dec 1998. http://www.icsi.berkeley.edu/~sander/publications/hiding.ps