A Secure Model in Agent-Based Marketplace

Ying-Hong Wang
Department of Computer Science &
Information Engineering
Tamkang University, Tamshui, Taiwan
inhon@mail.tku.edu.tw

Chen-An Wang
Department of Computer Science &
Information Engineering
Tamkang University, Tamshui, Taiwan
689190212@s89.tku.edu.tw

Abstract

Due to the popularity of broadband network and World Wide Web, network service advances more completely. E-Commerce is much emphasized by degrees. In spite of lots of network companies suffer deficits, E-Commerce still attracts numerous enterprises to invest in.

But consumers have no confidence for electronic transaction, the main reason is security problem. They fret about the data would be stolen, or their accounts would be usurped. Thus the most influential facility is security model. And in the security model, the basic model is “authentication”. If there is no sturdy authentication, anyone can masquerade others’ identities. The major objective of this paper is to propose an agent-based E-Commerce environment and to set up a secure E-marketplace authentication mechanism. In this mechanism, there are some issues are be researched. They include Agent, Mobile Agent, Aglets, Digital Signature Algorithm, Public Key Infrastructure (PKI).

Key word: Agent, Mobile Agent, E-Commerce , aglets, signature, Authenticate

1.Introduction

With the popularization of Internet and World Wide Web, there is no geographical limit to the development of E-Commerce. Web Sites help that display products and take orders are orders are becoming common for many types of business. However, Such Web sites are still designed for interactive use by humans and do not yet support automated electronic commerce among computers.

E-Commerce can help Customers and Companies or enterprises to trade through Internet. Companies or Enterprises can trade in merchandise with customers on Internet without periodical and geographic limitations. Marketplaces that connect buyers and sellers are up and running in many product categories, and are creating value by making trading more efficient and possibly even effective than traditional channel. It is obvious that these Electronic marketplaces that occur on the Internet are different from traditional, physical markets. Speed, cost, and flexibility have become top priorities. But there are still some issues of E-commerce on Internet.

First, how to reduce the network load and trade quickly is one of the E-Commerce issues. Because time is money, all companies hope that transaction can complete quickly. When the network loads heavily, many customers can’t shop in E-marketplace quickly. When network is off-line, it maybe led to wrong transaction for buyers and sellers. Security is another issues that buyers and sellers care. When there is no secure mechanism in E-Marketplaces, it is no attractive to customers.

Agent technique has been used to help buyers and sellers to act on E-marketplaces on behalf of users. When the users are disconnected, the agents are still automated on Internet on behalf of their clients. Mobile Agents can transport themselves from a host to another host in a network. . This is a very interesting concept that becomes even more attractive when the agents are no longer bound to the host where they begin execution. There are some advantages of mobile agent technique are applied in E-Commerce [1]:

- They reduce the network load
- They overcome network latency
- They encapsulate protocol
- They execute asynchronously and autonomously
- They adapt dynamically
- They are naturally heterogeneous
- They are robust and fault-tolerant

The major objective of this research is to propose agent technologies to set up the applications of E-commerce and to design a secure model for E-marketplace based on agents and mobile agents. In this mechanism, there are some issues are be researched. They include Agent, Mobile Agent, Aglets, Digital Signature Algorithm, and Public Key Infrastructure (PKI).

The reminder of this paper is organized as follows. In Section 2,we describe the related works that include some researches of E-commerce based on agents and mobile agents, and some secure mechanisms on Internet. In section 3,we present the security threats and security requirement of mobile agents. In section 4, aglets that agent platform and the platform architecture of E-marketplace are discussed. The secure model is shown in section 5.the last part of this paper is the conclusion and future work.

2.Related works

A. Cryptography

(1) Symmetric Cipher:

A symmetric cipher uses the same key for encryption and decryption (as opposed to a public-key or asymmetric cipher). When the sender transfer the ciphertext encrypted by the key to the receiver, the receiver need to use the same key for decryption. This key needs to be maintained confidential that others don't know. The advantage of this technique is to encrypt and decrypt rapidly and the drawback is how to transfer the key securely from the sender to the receiver. The symmetric cipher is shown in figure 2.1.

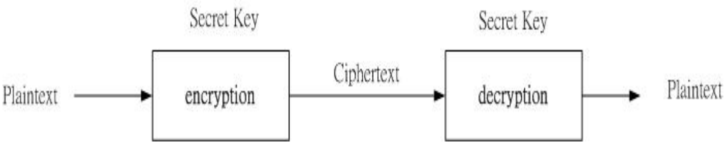

Figure2.1 Symmetric cipher

(2) Asymmetric Cipher

An asymmetric cipher uses the different key for encryption and decryption. The pair of keys is created together. The information encrypted by the public key can only decrypt by the relative private key. The advantage of this technique is to overcome the drawback of the symmetric cipher and the drawback is that encryption and decryption is slower than the symmetric cipher. The asymmetric cipher is shown in figure 2.2.

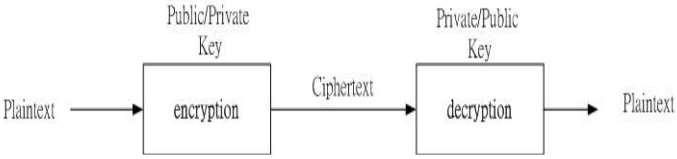

Figure2.2 Asymmetric cipher

B. Digital Signature

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

A digital signature that can be attached to an electronically transmitted message that uniquely identifies the sender. Like a written signature, the purpose of a digital signature is to guarantee that the individual sending the message really is who he or she claims to be. Digital signatures are especially important for electronic commerce and are a key component of most authentication schemes. The algorithm of digital signature is shown in figure 2.3.

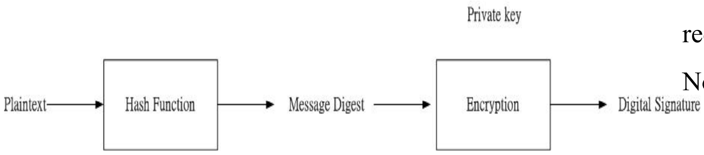

Figure2.3 Digital signature algorithm

3.Security threat and security requirement

Thread to security generally fall into three main classes: disclosure of information, denial of service, and corruption of information [7]. In this paper, we use the components of an agent system to categorize the threats as a way to identify the possible source and target of an attack. Four threat categories are classified in table 3.1: threats resulting from an agent attacking an agent platform, an agent platform attacking an agent, an agent attacking another agent on the agent platform, and other entities attacking the agent system.

Threats source and target	Categories of Threads

Agent-to-Platform	Masquerading;
	Denial of Service;
	Unauthorized Access;

Agent-to-Agent	Masquerade;
	Denial of Service;
	Repudiation;
	Unauthorized Access;

Platform-to-Agent	Masquerade;
	Denial of Service;
	Eavesdropping;
	Alteration;

Other-to-Platform	Masquerade;
	Unauthorized Access;
	Denial of Service;
	Copy and Replay;

Table 3.1 Security threats

The users of agent and mobile agent frameworks applied in E-commerce have four main security requirements: authentication, confidentially, integrity, and Non-repudiation.

- Authentication

Agents must be able to authenticate their identity to platform and other agents, while platforms must be able to authenticate their identity to agents and other platforms. An agent accessing publicly advertised product prices may not be required to authenticate itself, but if this agent decide to purchase any of these products the agent must be able to authenticate itself before the transaction is completed. Similarly, buyer agent will require some proof of seller agent's claimed identity. Both buyer agent and seller agent may require the agent platform to authenticate itself before they visit the platform.

- Confidentially

Any private data stored on a platform or carried by an agent must remain confidential. Agent frameworks must be able to ensure that their communications remain confidential. Mobile agents may also want to keep their location confidential. Mobile agents may communicate through a proxy whose location is publicly known if the agents conceal their presence on a platform.

- Integrity

The agent platform must protect agents from unauthorized modification of their code, state, and data and ensure that only authorized agents or processes carry out any modification of shared data. The agent itself cannot prevent a malicious agent platform from tempering with its code, state, or data, but the agent can take measure to detect this tampering.

- Non-repudiation

In an electronic transaction, there is the possibility that one of the users later denies either the terms of the deal, or even that the communication took place at all. In order to adding non-repudiation, the customer must gets a proof that the order has been sent and received correctly, and the web shop gets a proof that the customer is the originator of a particular message at a particular time. Non-repudiation always needs to depend on the use of a trusted third party.

4. Framework of E-Marketplace

There are four types of server in the proposed architecture for *e*-marketplace, they are: 1) Coordinator Server, 2) Marketplace, 3) Buyer Agent Server, and 4) Seller Server. Each server includes several agents and mobile agents (see Figure 4.2). They are described as follows[8][12]:

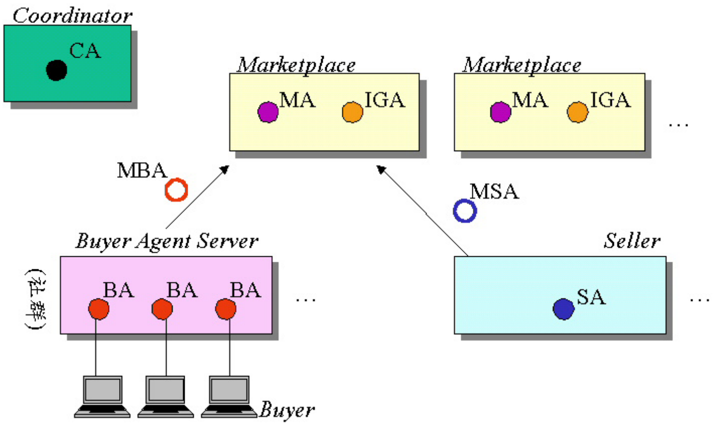

Figure 4.2 The architecture of electronic commerce environment

1) Coordinator Server

Coordinator Server is an environment where there is a Coordinator Agent (CA). The CA is a static agent and manages its EC domain. CA has several abilities: 1) initials an EC domain, 2) monitors Marketplaces, Buyer Agent Servers and Seller Agents, 3) manages Marketplaces, Buyer Agent Servers and Seller Agents, 4) provides the functions of register and authentic query, and 5) cooperates with other CA.

2) Marketplace

Marketplace is a platform that supports the transaction facilities for mobile agent of sellers and buyers. There are two kinds of static Agents and two kinds of Mobile Agent in the Marketplace:

a) Management Agent (MA)

MA is a static Agent in the Marketplace. It has two abilities: 1) manages the registration of Mobile Agents when they enter into this Marketplace, 2) manages the activities of agents in this Marketplace.

b) Information Gathering Agent (IGA)

IGA is a static Agent in the Marketplace. IGA will gather the related information in the Marketplace. They include the records of transaction, the information of the productions, the requirements of customers and so on.

c) Mobile Buyer Agent (MBA)

MBA stands for the buyer, moves from one Marketplace to another Marketplace and trades with Mobile Seller Agent.

d) Mobile Seller Agent (MSA)

MSA stands for the seller, moves from one Marketplace to another Marketplace and trades with MBA.

3) Buyer Agent Server

The Buyer Agent Sever provides the web interface that lets users via browser to control agent to carry the e-commerce activation out. The Buyer Agent Server is managed by the Buyer Server Management Agent (BSMA). The BSMA will produce Buyer Agent (BA) for each user to serve its homologous user. BA will produce Mobile Buyer Agent (MBA) according to the requirements of the user. It stands for the user to go to every marketplace to make bargains.

There are several elements in Buyer Agent Server. They are:

a). Http Agent (HttpA)

HttpA provides the Web interface, let users can use all service of the Buyer Agent Server with web browser.

b). The Buyer Server Management Agent (BSMA)

The BSMA is the manager of this Buyer Agent Server. BSMA has several abilities: 1) according the user's requirement of the user to create a Buyer Agent, 2) manages and monitors all Agents in the Buyer Agent Server and 3) provides the functions of registration and authentic query.

c). Buyer Agent (BA)

One BA serves a specific user. BA can create MBA according the requirement of the user. BA also manages MBAs that execute missions in Marketplaces.

d). Mobile Buyer Agent (MBA)

MBA is created by BA and migrate to marketplaces. It stands for user to collect the information of interesting productions.

e). User DB

User DB stores the profiles and information of users.

f). Agent DB

Agent DB is managed by BSMA and stores the information of agents in the Buyer Agent Server.

4) Seller Server

Each company, which wants to join this e-marketplace, should build a Seller Server. There are two main Agents in a Seller Server, include:

a). Seller Agent (SA)

SA has two main abilities: 1) manages Seller Server, 2) creates Mobile Seller Agents and dispatches them to Marketplaces for selling productions.

b). Mobile Seller Agent (MSA)

MBA moves from one Marketplace to another Marketplace and executes missions that are assigned by SA.

The table 4.1 is the comparison of agents in this architecture:

	Server	Stationary/ Mobile	Creator
Coordinator Agent	Coordinator Server	Stationary	
Buyer Server Manage Agent	Buyer Agent Server	Stationary	Coordinator Agent
Manager Agent	Marketplace Server	Stationary	Coordinator Agent
Buyer Agent	Buyer Agent Server	Stationary	Buyer Server Manage Agent
Seller Agent	Seller Server	Stationary	Coordinator Agent
Mobile Buyer Agent	Buyer Agent Server	Mobile	Buyer Agent
Mobile Seller Agent	Seller Server	Mobile	Seller Agent

Table 4.1 Comparison of agents

5. Secure model

In this section, we will describe the secure model that includes the mechanisms of registration and authentication.

5.1 The mechanism of registration for mobile agents

When we set up a domain, CA is created first, then CA create the other agent that include SA, BSMA, Ma, and IGA in this domain. CA stores the information of these agents into CA's database and dispatch them to their server. But BA is created by BSMA, MBA is created by BA , and MSA is created by SA, so CA doesn't have their related information. In this paper, we propose a mechanism of registration for BA, MBA, and MSA.

- BA registers with CA: When BSMA creates BA, BSMA store the information of BA and register with CA by means of transferring the information of BA. The information of BA for registration include identifier, its owner, and public key…etc.
- MBA registers with CA: When BA creates MBA, BA transfer the information of MBA to BSMA.BSMA store the information and register MBA with CA by means of transferring the information of MBA. The information of MBA for registration include identifier, its owner, Creation Time and Lifetime…etc.
- MSA registers with CA: When SA creates MBA, SA store the information of MSA and register MSA with CA by means of transferring the information of MSA. The information of MBA for registration include identifier, its owner, Creation Time and Lifetime…etc.

Any CA owns the information of all agents in the same domain and the information of CAs in partnership with it. When the agent request the information of marketplace in other domain, BA request CA in same domain to send a request of offering the information of the marketplace to CA that owns this marketplace.

5.2The mechanism of authentication for mobile agents

5.2.1 The information of authentication of agents

We divide the information of authentication of agents into five parts.

- CA: CA owns the information and public key of CA in partnership with it and the information of all agents in the same domain.

- BA: BA generates a pair of key.
- MBA: MBA owns the digital signature of MBA's identity and agent code. It's presented in Figure 5.1.
- MA: MA generates a pair of key.
- MSA: MSA owns the digital signature of MSA's identity and agent code.

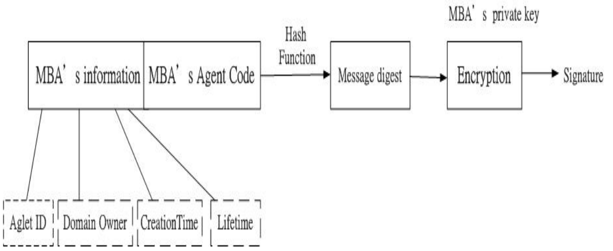

Figure 5.1 MBA's digital signature

5.2.2 MBA request itinerary

After MBA registers at CA, MBA will be dispatched to the Marketplace to request service and trade according to the demand of user. First, MBA request the information of Marketplace from BSMA, BSMA forward the request to CA , BSMA's domain owner. CA refers to its database and look for suitable marketplaces. When CA, BSMA's domain owner, finds no information, it requests the information from other CAs and send back the information.

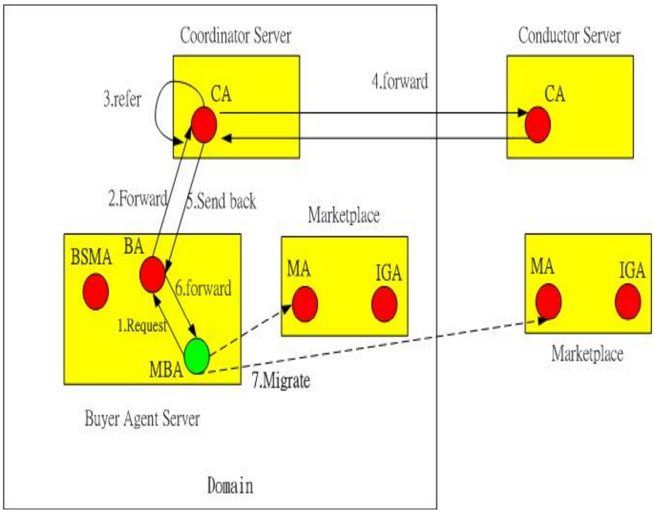

Figure5.2 MBA request the itinerary from CA

When SA wants to sell merchandise, it creates MSA and registers MSA at CA. CA requests the information of suitable marketplaces. When CA finds no information, it requests the information from other CAs and send back the information to MSA.

5.2.3 Preparation before agents is dispatched

After MBA registers at CA, it requests the itinerary from CA according to the demand of user. Before it leaves Buyer Agent Server to the first marketplace to request services, some preparations must be done.

- MBA leaves Buyer Agent Server to Marketplace

1. BA looks for MA's public key from the database, if it have no MA's public key, it requests MA's certificate from CA, BA's domain owner. When MA belongs to the different domain from BA, CA, BA's domain owner, request MA's certificate from CA, MA's domain owner.
2. BA generates a random number C_0,and uses its public key to encode C_0.
3. The encrypted C_0 is stored in MBA.
4. BA notifies CA of MBA's migration, CA and BA record the information that BA will be dispatched to which marketplace.
5. MBA dispatches to marketplace.

- MBA leaves marketplace-k to marketplace-k+1

1. MA-k generates two random numbers R_{1k} and R_{2k}.
2. MA-k generates a key seed S_k from Ck and R_{1k} . It generates new random number C_{k+1} from S_k and R_{2k}.
3. MA-k uses MBA's public key to encode R_{1k} and R_{2k} and stores the Encrypted R_{1k} and R_{2k} in MBA.
4. If MA-k has no MA-k+1's public key, MA-k

request MA-k+1's certificate from CA, MA-k's domain owner. When Ma-k+1 doesn't belong to this domain, CA, MA-k's domain owner, request MA-k+1's certificate from CA, MA-k+1's domain owner.

5. MBA starts migrate.

5.2.4 the process of authentication

When MBA migrates to marketplace, authentication will be done before it request services. The process of authentication is following:

- MBA migrates to marketplace in the same domain(See figure 5.3)

1. After MBA migrates to marketplace, it request authentication from MA

2. MA requests MBA's certificate from CA that MBA belongs to.

3. MA identifies MBA's certificate.

4. MA obtains MBA's public key from MBA's certificate, and identifies MBA's digital Signature.

5. CA notifies BA of MBA's migration.

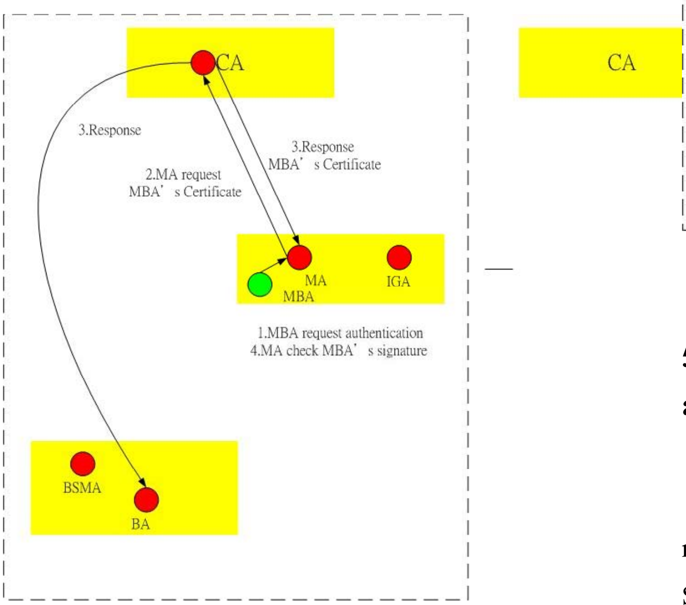

Figure 5.3 MA and MBA belong to the same domain

- MBA migrates to marketplace in the different domain (See figure 5.3)

1. After MBA migrates to marketplace, it request authentication from MA
2. MA requests MBA's certificate from MBA's CA.
3. Because MA is not trusted by MBA's CA, MBA's CA issues MBA's certificate for MA's CA and MA's CA issues the certificate of MBA's CA.
4. MA obtains certificate chaining

   (1) The certificate of MA's CA that MBA's CA issues

   (2) MA's certificate that MA's CA issues
5. MA identifies certificates
6. MA obtains MBA's public key from MBA's certificate, and identifies MBA's digital signature.
7. CA notifies BA of MBA's migration.

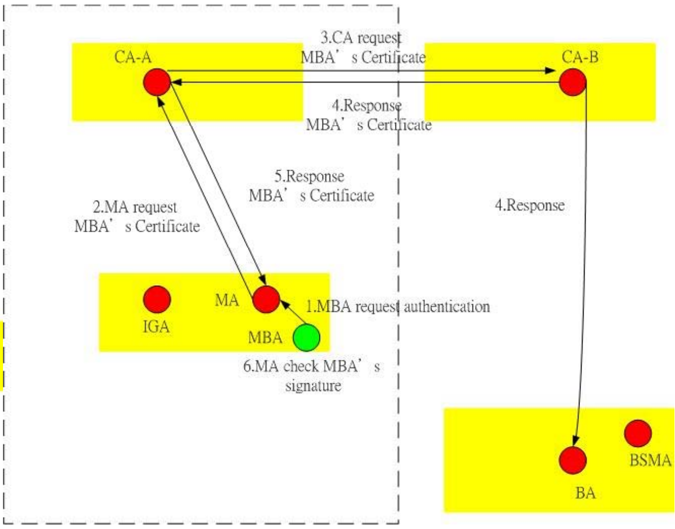

Figure 5.4 MBA and MA belong to the different domain

5.3 The protection of Data integrity and confidentiality

Before MBA migrates to marketplace, it generates a random number C_0. MBA stores C_0 in Buyer Agent Server and encrypts C_0 with MA's public key. C_0 is transferred with MBA.

After MBA arrive in marketplace, MA identifies

MBA and check MBA's digital signature. After authentication succeeds, MA encrypts C_0 with MA's private key and generates two random numbers ($R1_1$, $R2_1$). MBA generate a key seed S_1 using C_0 and R_1 by means of a one-way hash function (see Figure 5.5). In this paper, we use SHA-1 as one-way hash function, so S_1 is 160bits. We use the last 64 bits as session key K_{S-1}.

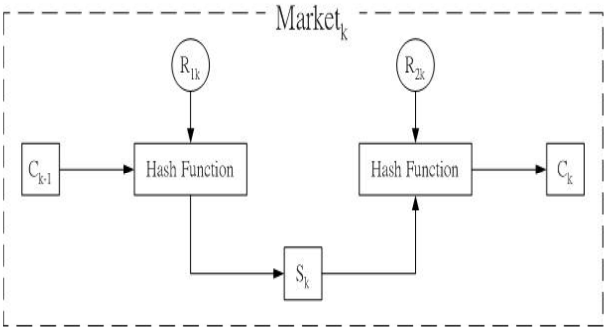

Figure 5.5 One-way hash functIon

When MBA collect the data from marketplaces, MA signs the collected data in order to ensure its non-repudiation and integrity, and encrypts the data and digital signature with the session key in order to ensure its confidentiality.

When MBA will migrate to next marketplace, MA generates next random number C_1 using S_1 and $R2_1$. MA encrypts $R1_1$ and $R2_1$ with MBA's public key and encrypts C_1 with next MA's public key.

When MBA will leave Marketplace-k to Marketplace-k+1,MBA encrypts C_k with MA-k+1's public key, then replaces origin random number C_{k-1} and migrates with MBA.

When MBA migrates to Marketplace-k+1,MA-k+1 identifies MBA. If authentication succeeds,MA-k+1 decrypts C_k with Ma-k+1's private key and generates two new random numbers $R1_{k+1}$ and $R2_{k+1}$.Ma-k+1 generates new key seed S_{k+1} Using C_k and $R1_{k+1}$ and use the last 64 bits of S_{k+1} as session key K_{S-k+1}.

When MBA come back to Buyer Agent Server, MBA decrypts all R1 and R2 that all Servers in itinerary generate. MBA generates key seed S_1 using C_0 and $R1_1$ and use the last 64 bits of S_1 as session key K_{S-1}.MBA decrypts the data of Marketplace-1 with K_{S-1} and generates C_1 using S_1 and $R2_1$. When MBA will decrypts the data of marketplace-k, MBA generates key seed S_k and use the last 64 bits as session key K_{S-k}. MBA decrypts the data of Marketplace-k with K_{S-k} and generates C_k using Sk and $R2_k$.After all data is decrypted, MBA identifies all digital signature of all data .

6.Conclusion and future works

The major objective of this research thesis is to propose an agent-based E-Commerce environment and to set up a secure E-marketplace authentication mechanism. This paper proposes the following:

1. It proposes a mechanism of registration. All agents can register at CA, the domain administrator, and can look for the information of other agents.
2. It proposes a mechanism of authentication. Marketplace can authenticate all incoming agents, avoid malicious agents cause damage to marketplace.
3. MA serves as trusted third party and signs all data that trade in marketplace in order to ensure its non-repudiation.
4. It provides the protection of integrity and confidentiality. All sellers and buyers can't know his competitors' bid and modify their bid.
5. BA and MBA record MBA's itinerary in order to avoid the attack that platform-to-agent.

In the future, we not only improve this mobile agent-based E-Commerce platform but also do more research on secure model.

- marketplace

We can design a mechanism of load balancing. When a agent migrates to marketplace, if this marketplace has too many agents and load heavily, the marketplace migrates the agent to another marketplace that load lightly.

Besides, how to generate personal profiles for all customers and how to make the shopping suggestion to customers is our future works. As for the mechanism of auction, how to design multiple auctions is a difficult problem.

- Secure model

So far, this paper proposes a secure model in order to provide secure protection, but system performance will be reduced. In the future, we can divide the functions of agents in Coordinator Server and Marketplace into many functions. We can use Certificate Authority for generation and issue of certificate in order to reduce the load in CA.

Reference

[1]Danny B.Lange, Mitsuru Oshima， “Programming and Deploying Java^{TM} Mobile Agents with aglets^{TM},” Addison-Wesley

[2]O. M. Ba-Rukab and M. M. Shahsavari, "Agent-Host Mutual Authentication," IEEE SoutheastCON '99, Lexington, KY (1999)

[3]Jonathan Knudsen, “Java cryptography” , O’reilly & Associates Inc

[4]William Stallings ， “Cryptography and Network Security: Principles and Practice,” Prentice hall ,INC

[5]Wayne Jansen, Tom Karygiannis , “NIST Special Publication 800-19: Mobile Agent Security”, National Institute of Standards and Technology, August 1999

[6]Gunter Karjoth, Danny B. Lange, and Mitsuru Oshima, “A Security Model for Aglets”, in IEEE Internet Computing, Vol. 1, No. 4, July/August 1997

[7]R. Kalakota, A. B. Whinston, “Frontiers of Electronic Commerce”, Addison-Wesley

[8]Ying-Hong Wang, Chen-An Wang, Wen-Nan Wang, and An-Cheng Cheng, “Mobile Agents over e-business,” Accepted by CATA-2002, San Francisco, California USA

[9]A. Corradi, R. Montanari, and C. Stefanelli, “Mobile agents protection in the Internet environment,”in *The 23rd Annual International Computer Software and Applications Conference(COMPSAC ’99)*, pp. 80–85, 1999.

[10]Neuenhofen, K. and Thompson, M. 1998. “A secure marketplace for mobile java agents”. in Proceedings of the second international conference on Autonomous Agents, Minneapolis MN USA (May 1998), pp. 212~218.

[11]Jongyoul Park, Dong-Ik Lee, Hyung-Hyo Lee, “Data Protection in Mobile Agents; one-time key based approach”, IEEE ISADS 01, pp.411-418, March 2001.

[12]Ying-Hong Wang, Hua-Chien Chen, and Shih-Wei Kao, Mobile Agent-Based Platform Supports to e_Market Place, Proceeding of The Seventh International Conference on Distributed Multimedia System (DMS2001), Sep. 2001,pp9~16

[13] IBM Aglet Home Page; http://www.trl.ibm.co.jp/aglets

[14] Aglet Research Group of NCKU; http://turtle.ee.ncku.edu.tw/