Mobile Agent Protection and Verification in the Internet Environment

Ying-Hong Wang, Ching-Lin Wang, and Liao, Cheng-Horng
Department of Computer Science & Information Engineering
Tamkang University, Tamshui, Taipei County, Taiwan
inhon@mail.tku.edu.tw, clwang@cs.tku.edu.tw, 791190092@s91.tku.edu.tw

Abstract

For Mobile Agent, it can only be performed under trusted environment if there is no proper security. It can not be performed in the Internet due to the high risks. There are too many security issues in Internet. For example, some malicious servers or programs which attack or steal our server or original data. Hence, this paper proposes a mobile agent application of E-commerce system and some authentication mechanisms for the system that include authentication of the legality of servers in E-commerce, authentication of the legality of mobile agents, and the verification of attacks on servers and mobile agents.

By applying mobile agent and encryption/ decryption technologies, this paper will introduce how coordinator server establishes authentication mechanisms, and the authentication between servers, as well as how coordinator server verifies that each server is attacked or not? Meanwhile, this paper also introduces the authentication between: (1) buyer/ seller and server, (2) mobile agent and server, as well as the verification of attacks on mobile agent.

Finally, this paper focuses on protecting and verifying the data that are collected by mobile agent, to ensure the data's integrity, authentication, non-repudiation, confidentiality and availability, so as to achieve the targets of data security mechanism.

Keywords: Agent, Mobile Agent, Electronic Commerce, Authentication Mechanism, Verification Mechanism.

1. Introduction

The rapidly increased global Internet users and the popularized using of World Wide Web have resulted in a gradually developing of Internet based E-commerce. In view of Internet's easy to access, convenience virtue and huge potential users, lots of enterprises have involved in this high technology field and invested in E-commerce software and equipment, to acquire niche and business opportunity.

The key point for allowing the practical application of E-commerce is security issue. As Internet is under open environment, attackers will utilize any malicious servers or programs to invade our server or original data. Hence we have to ensure every server and program is executed under secured protection, and they won't be threaten by malicious servers or programs.

The main idea for this paper is to initiate secured E-commerce on Internet. We propose a mobile agent based E-commerce system and some authentication mechanisms for the system, which includes authentication of the legality of servers in E-commerce. We introduce how coordinator server establishes authentication mechanism, and the authentication between servers, as well as how coordinator server verifies that each server is attacked or not? Meanwhile, we also introduce the authentication between: (1) buyer/ seller and server, (2) mobile agent and server, as well as the verification of attacks on mobile agent. Finally, this paper focuses on protecting and verifying the data that are collected by mobile agent, to achieve the targets of data security mechanism.

This paper is organized as follows: Section 2 describes the related works. Section 3 presents the architecture of mobile agent system. Section 4 proposes the authentication and the verification between servers. And section 5 proposes the protection and the authentication mechanism between mobile agent and servers. The verification mechanism for data collected by mobile agent in section 6. The last part of this paper is our conclusion and future works.

2. Related works

Mobile Agent is an emerging research topic in these years. Agent is a software which represents the behaviors of the users in the world of the computer networks. There are some mobile agent's fundamental characteristics, which are following [1]:

- Reactive
- Autonomous

0-7695-2216-5/04 $20.00 © 2004 IEEE

- Object-oriented
- Communicative
- Mobile
- Learning
- Believable

To spread out the advantages of mobile agent, many people are devoted themselves in developing mobile agent application environment. For example, Aglets, Voyager, Odyssey, Concordia, ARA, Mole, Agent TCL, TACOMA and SHIP-MAI. Here we will introduce four of the common use application environment: Aglets, Voyager, Odyssey and Concordia [2]:

- Aglet system is nicely accommodated to the Internet Environment; it is robust and it is the most widely used system.
- Voyager provides unique concept of serialization and mobility of objects and allows quick and easy creating of sophisticated network applications.
- Odyssey is more distributed systems oriented than other mobile agent systems but brings a new dimension to the programming.
- Concordia system provides modularity, security and enables remote administration that makes it suitable for enterprise systems.

Michael S. Greenberg, Jennifer C. Byington and David G. Harper addressed in their co-made paper, attack categories for mobile agent include [3]:

- Damage
- Denial of Service
- Breach of Privacy or Theft
- Harassment
- Social Engineering
- Triggered Attack
- Compound Attack

Many security problems happened in un- security execution, so we here conclude four dimensions for protecting mobile agent [4]:

- Protecting server, to deny un-authenticated mobile agent for access.
- Protecting server, to avoid attack by malicious mobile agent.
- Protecting mobile agent, to avoid attack by other mobile agent.
- Protecting mobile agent, to avoid attack by malicious server.

Through the interactive coordination of the above mechanisms, mobile agent can then operate under security environment. However, the performing works of mobile agent are dispatched by users. The mobile agent itself can represents the user, then the work that it performs also needs to keep privacy. Hence the security issue should be taken into consideration.

3. The Architecture of E-commerce System

This section is focusing on establish an E-commerce environment to enable buyer and seller for inquiry and transaction. Thus, this paper will base on the E-commerce system which developed by our laboratory [5], to adjust and expand related function on this system.

3.1 E-commerce System Platform

Under this architecture, the major servers are Coordinator Server, Database Server, Marketplace Server, Buyer Server and Seller Server. (see Figure 3.1)

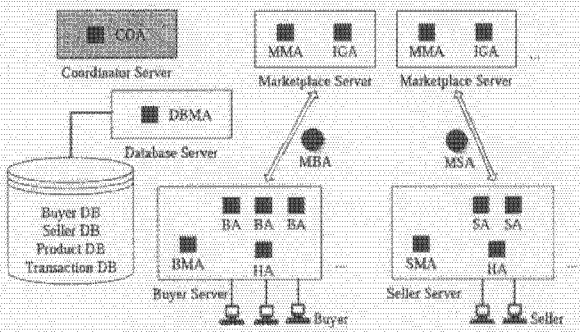

Figure 3.1 The Architecture of E-commerce System Platform

Every server has different functions, is responsible for related service, and each server will be differentiated between monitoring and management according to the correspondent hierarchical relationship.

3.2 Role Play and Positioning for Servers

There is a Coordinator Agent (COA) in Coordinator Server that is in charge of the initiating and establishes for entire E-Commerce system platform, which includes Database Server, Marketplace Server, Buyer Server and Seller Server. It manages every server's execution status, provides authentication mechanisms for each server and mobile agent, monitors entire system status, and coordinates with other domain's coordinator server, as well as verifying the authenticity of Public Key with Certificate Authority (CA).

There is a Database Management Agent (DBMA) in Database Server that in charge of the needed database, which includes every server, agent, mobile agent, buyer, seller, products and transaction. DBMA is responsible for access control of entire database, the access can be proceeded only if the Coordinator Server authorized

There are two mobile agents in Marketplace Server, they are Marketplace Management Agent (MMA) and

Information Gathering Agent (IGA). Through MMA and IGA, e.g. products enquiry data collection or products transaction, this server can provide buyers and sellers a security E-marketplace. MMA is for managing all agents in Marketplace Server, which includes IGA, Mobile Buyer Agent (MBA) and Mobile Seller Agent (MSA), as well as bilateral authentication between MBA and MSA. While IGA is responsible for collecting the enquired information or transaction information which is delivered by MBA or MSA, IGA proceeds the Data Mining on database.

There are four agents in Buyer/ Seller Server. they are Buyer/ Seller Management Agent (BMA/ SMA), Buyer/ Seller Agent (BA/ SA), HTTP Agent (HA) and Mobile Buyer/ Seller Agent (MBA/ MSA). This Server provide buyer/ seller a security operating platform, proceed E-commerce by using Browser. BMA/ SMA is responsible for managing all agents in entire Buyer/ Seller Server. It also authenticates, monitors and records all data from mobile agents, and generates BA/ SA according to HA that buyer's/ seller's needs. BA/ SA is responsible for serving buyers/ sellers and every buyer/ seller will be given a correspondent BA/ SA. Meanwhile, BA/ SA will generates MBA/ MSA according to buyer's/ seller's needs, and BA/ SA will also control MBA/ MSA which is outside the Buyer/ Seller Server. HA is responsible for providing a web page interface, which enables buyer/ seller to login and setup related data by using browser, and as instructed by HA, BA/ SA will dispatch MBA/ MSA to Marketplace Server to collect/ maintain data or proceed transaction.

4. Authentication and Verification Mechanism Between Servers

While the E-Commerce system platform starts to operate, its major Coordinator Server will play the role as this domain's private certificate authority, and it will establish Database Server, Marketplace Server, Buyer Server and Seller Server in sequence. To prevent the servers from malicious attacks during the whole processing, this section will introduce how Coordinator Server establish authentication mechanism, and the authentication between servers, as well as how to verify each server if it has been attacked or not.

4.1 Coordinator Server and Database/ Marketplace/ Buyer/ Seller Servers

- Initial Startup

When Coordinator Server establish Database/ Marketplace/ Buyer/ Seller Servers, it also computes the specific servers with Hash Function to generate Digest, which will be stored in Coordinator Server, and then produce and set of public key and private key of asymmetric key to Database/ Marketplace/ Buyer/ Seller Servers for authentication.

- Database/ Marketplace/ Buyer/ Seller Servers Operation

Coordinator Server requests Database/ Marketplace/ Buyer/ Seller Servers to compute Hash Function by themselves to generate Digest for a period of time. This Digest will be sent back to Coordinator Server by using Coordinator's Public Key to encrypt. After receiving it, the Coordinator Server will use its own Private Key to decrypt, and compare to the original Digest. If these two Digests are same, that presents the Database/ Marketplace/ Buyer/ Seller servers are in normal operation; in case they are different, that represents the Database/ Marketplace/ Buyer/ Seller servers have been attacked, then Coordinator Server can force to terminate Database/ Marketplace/ Buyer/ Seller servers, to restart new Database/ Marketplace/ Buyer/ Seller Servers. (see Figure 4.1)

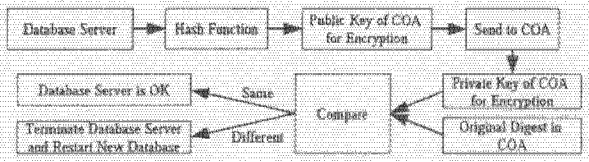

Figure 4.1 Coordinator Server and Database Server for Verification

4.2 Database Server and Marketplace/ Buyer/ Seller Servers

When Marketplace/ Buyer/ Seller Servers need to online to Database Server for the products transaction/ buyer's/ seller's data, it needs to be authenticated by Coordinator Server, to access database.

First of all, Marketplace/ Buyer/ Seller Servers will send out their own digital certificate to Database Server, which will inquire Coordinator Sever the authenticity of this digital certificate when it receives, then Coordinator Server will compare the information on digital certificate. If the authentication is successful, Coordinator Server will ask Database Server to authorize Marketplace/ Buyer/ Seller Servers to access; if not, then the access will be denied.

5. Protection and Authentication Mechanism for Mobile Agent

When the E-commerce system platform normally operated, the Buyer Server and Seller Server will provide related services to Buyer and Seller. However, during inquiry and transaction, it is important to prevent legal servers from attacking by malicious

mobile agents, or vice versa. In this section, we will introduce the authentication between (1) Buyer and Buyer Server, (2) Seller and Seller Server, (3) Mobile Agent and Servers, as well as the verification of attacks on mobile agent.

5.1 Buyer/ Seller and Buyer/ Seller Sever

When Buyer/ Seller connects to Buyer/ Seller Server, i.e. direct communication with MA/ SA, the Buyer/ Seller can use the following ways to login:

- Login by Account and Password

Traditionally, it's the most useful way for identification and authority control, but the function is limited and not secured. When Buyer/ Seller input account and password, HA will send the data to BMA/ SMA, then BMA/ SMA go further to inquire for Database Server to compare if the account and password is matched or not. If it does, then Buyer/ Seller can login, and there will be a BA/ SA for Buyer/ Seller uses; it is not matched, then the login will be denied.

- Login by Digital Certificate

The digital certificate is the best identification tool, just like an electronic ID, it provides more solid security than traditional account and password system. Especially, it can ensure Buyer's/ Seller's identity to provide better protection during the transaction process. When Buyer/ Seller sends their own digital certificate to HA, it will forward the data to BMA/ SMA, then BMA/ SMA will ask Coordinator Server to confirm with Certificate Authority the authenticity of this digital certificate. If it's successful, then it will notify BMA/ SMA to let this Buyer/ Seller in; if not, then the login will be denied.

5.2 MBA/ MSA and Buyer/ Seller Server

5.2.1 How to establish authentication mechanism for MBA/ BSA

If MA/ SA needs to establish MBA/ MSA while serving Buyer/ Seller, it can use the following steps to generate MBA/ MSA: (see Figure 5.1)

- BA/ SA will ask BMA/ SMA for providing temporary public key and private key of asymmetric key.
- BMA/ SMA can not provide the key by itself, it needs to ask Coordinator Server to provide temporary public key and private key of asymmetric key.
- After Coordinator Server provides the keys, it will conduct the 1st encryption by using its own private key, then use public key of Buyer/ Seller Server to do the 2nd encryption. By doing so, it can be transmitted to BMA/ SMA safely.
- When BMA/ SMA receives the above, it will use its own private key to decrypt the 1st encryption, then use public key of Coordinator Server to decrypt the 2nd encryption, to well protect the keys' security.
- After that, BMA/ SMA provides the set of keys to BA/ SA, then BA/ SA will generate MBA/ MSA for identification.
- Although MBA/ MSA is moving and executing in remote servers, its own private key is taken care by BA/ SA, the key is not movable, to avoid stolen by malicious server.

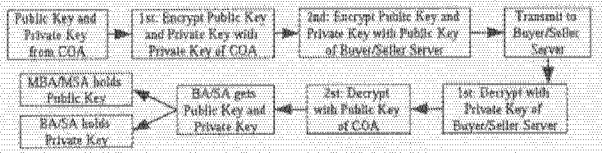

Figure 5.1 Establish authentication mechanism for MBA/BSA

5.2.2 Mechanism for how Buyer/ Seller Server authenticate MBA/ MSA

When MBA/ MSA finishes its work and returns, Buyer/ Seller Server needs to authenticate the identity of MBA/ MSA, if it's the original one. Listed below the authentication steps:

- When BA/ SA generates MBA/ MSA, BA/ SA will base on the identity and code to compute MBA/ MSA with Hash Function for generating Digest, which will be stored in BA/ SA.
- When MBA/ MSA requests to return, BA/ SA will ask this MBA/ MSA to compute Hash Function with its own identity and code for generating Digest. Then the Digest will be encrypted by its own public key and send back to BA/ SA. When BA/ SA receives it, that can be decrypted by MBA's/ MSA's private key, and then compare the Digest with original one. If they are the same, then it means MBA/ MSA is normally operated without any attacks; if they are different, that means MBA/ MSA has been attacked, the BA/ SA will refuse its return.

5.2.3 Mechanism for how MBA/ MSA authenticate Buyer/ Seller Server

When MBA/ MSA has been authorized to return to Buyer/ Seller server, MBA/ MSA can inquire to Coordinator Server if the Buyer/ Seller Server is legal. If yes, MBA/ MSA can return to the Buyer/ Seller Server, then it transmits the execution result to Buyer/ Seller. If not, or the Buyer/ Seller Server is re-established because of being attacked, the Coordinator Server will keep the execution result temporarily, and

turn in it to the original Buyer/ Seller when they are re-login.

5.3 MBA and Marketplace Server

When MBA is going to Marketplace Server, this Server has to authenticate MBA's identity for login; on the contrary, MBA also needs to authenticate if the Marketplace Server is a legal server, to secure its own safety. The following two points will explain how they conduct the mutual authentication.

5.3.1 Mechanism for how Marketplace Server authenticate MBA

When MBA is going to Marketplace Server, BA will send MBA's digital certificate to MMA. When MMA receives, it will inquire to Coordinator Server about the authenticity of this digital certificate. If the identification is successful, it will reply BMA to let MBA to migrate and login; if not, the migration and login will be denied.

Similarly, if MBA wants to migrate from one Marketplace Server to another one, MBA will call BA to conduct authentication. First of all, BA will send this MBA's digital certificate to MMA. When receives, MMA will inquire to Coordinator Server for the authenticity of this digital certificate. If the identification is successful, it will reply BMA to let MBA to migrate and login; if not, then the migration and login will be denied.

5.3.2 Mechanism for how MBA authenticates Marketplace Server

When MBA has been authorized to login Marketplace Server, BA will ask Marketplace Server to provide its digital certificate. When receives, BA will inquire to Coordinator Server for the authenticity of this digital certificate. If the identification is successful, it will allow MBA to migrate and login Marketplace Server; if not, the migration and login will be denied.

Similarly, if MBA wants to migrate from one Marketplace Server to another one, MBA will call BA to conduct the authentication. BA will ask the another Marketplace Server to provide its digital certificate. When receives, BA will inquire to Coordinator Server for the authenticity of this digital certificate. If the identification is successful, the it will let the MBA to migrate and login to another Marketplace Server; if not, the migration and login will be denied.

6. Data Verification Mechanism for MBA

This section will introduce a data verification mechanism, to enable buyers to determine the authenticity of data, and ensure the data is having Integrity, Authentication, Non-repudiation, Confidentiality and Availability, to achieve the targets of data security mechanism.

When BA establish MBA, it not only provides related authentication data, but also provides data verification mechanism. The steps are as follows:

- When MBA is in No. i Marketplace Server (see Figure 6.1)
  - When MBA is in No. i Marketplace Server, this Marketplace Server will have a variable randomly, then compute this variable with Hash Function to generate Digest Ci.
  - This No. i Marketplace Server will get the first 64-bit of Ci to act as secret key (CCi) of symmetric key, then use this CCi to encrypt the data (Di), that is obtained from No. i Marketplace Server, into DDi. (To achieve the Confidentiality of the data Di)
  - This No. i Marketplace Server will use MBA's Public Key to encrypt CCi into BBi. (To achieve the Confidentiality of Secret Key)
  - This No. i Marketplace Server lets data (Di) to use Hash Function to generate Digest (Hi), then uses No. i Marketplace Server's Private Key to encrypt it, to produce Digital Signature (Si) for No. i Marketplace Server. (To achieve the Non-repudiation of No. i Marketplace Server)
  - Finally, MBA, with the previous data plus the No. i Marketplace Server's data, will go further to next Marketplace Server together with {BB_1, DD_1, S_1. BB_2, DD_2, S_2. ..... BBi, DDi, Si}.
  - When MA visited No. n Marketplace Server, it will bring together {BB_1, DD_1, S_1. BB_2, DD_2, S_2. ... BBn, DDn, Sn} to return to Buyer Server.

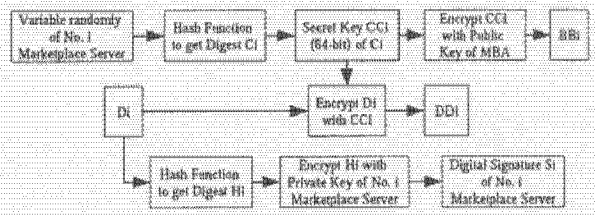

Figure 6.1 MBA is in No. i Marketplace Server

- When MBA returns to Buyer Server (see Figure 6.2)
  - When MBA return to Buyer Server, it will turn in all the collected data to BA.

- BA will take out the data in order, from 1st Marketplace Server {BB1, DD1, S1}, 2nd Marketplace Server {BB2, DD2, S2} to Nth Marketplace Server {BBn, DDn, Sn}, to conduct decryption and verficiation.
- BA takes out the No. i Marketplace Server's data {BBi, DDi, Si}, and then uses MBA's Private Key to decrypt BBi into CCi.
- BA uses CCi to decrypt DDi , to restore to the data (Di) of No. i Marketplace Server.
- BA will then take out the data (Di), and use Hash Function to generate Digest (Vi).
- BA will also take out Digital Dignature (Si) of No. i Marketplace Server, and use Public Key of No. i Marketplace Server to obtain the original Digest (Hi).
- Then, BA will compare Vi and Hi. If they are the same, it presents that the data (Di) has not been forged, which also proves the data was sent out by No. i Marketplace Server. If Vi and Hi are different, it means Di has been forged or it is unable to prove the data was sent out by No. i Marketplace Server.

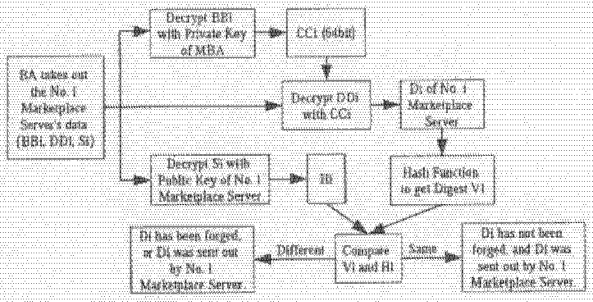

Figure 6.2 MBA returns to Buyer Server

7. Conclusion and Future works

By using the electronic network market, which is made up by mobile agent and security technologies, this paper proposes a secured electronic trading environment. There are some contributions for this paper. They are following:

- This paper proposes a mobile agent based E-commerce system, and formulate each server's role play and position.
- To prevent servers from malicious attacks, this paper illustrates how coordinator server establishes authentication mechanism, and the authentication between servers, as well as how Coordinator Server verifies that each server is attacked or not?
- To prevent legal server from attacking by malicious mobile agents or vice versa, this paper also introduce the authentication between (1) buyer and Buyer Server, (2) seller and Seller Server, (3) mobile agent and servers, as well as the verification of attacks on mobile agent.
- For the data collected by mobile agent, this paper provides a data verification mechanism, for buyers to determine the authenticity of these data, to achieve the targets of data security mechanism.

Limitation for this paper, the entire system is emphasizing E-commerce Security as top priority, during the research, we use many different security mechanisms alternatively, which may bring about some limitation as follows:

- The network transmission volumes are enlarged between servers.
- The workload for servers is heavier because of agent's authentication.
- It wastes times due to the various ways for encryption and decryption on mobile agents.

This paper proposes some security mechanisms, but there are still some targets to be achieved in the future, such as: (1) For system platform: Marketplace Server can distribute some mobile agents to other Marketplace Servers for reducing the load. And Coordinator Server should be subdivided into several Coordinator Servers for balancing the workload. (2) For mobile agents: Buyers can dispatch several mobile agents at the same time for avoiding repeated work. And mobile agents can achieve bargaining/negotiation mechanism. (3) For security mechanism: To raise the efficiency for entire system and give consideration to the security are important in the future works.

References

[1] Danny B. Lange, Mitsuru Oshima, "Programming and Deploying Java Mobile Agents with Aglet", Addison-Wesley

[2] Damir Horvat, Dragana Cvetkovic, Veljko Milutinovic, Petar Kocociv, Vlada Kovacevic, "Mobile Agents and Java Mobile Agents Toolkits", System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on Jan 4~7, 2000, Pages: 3090~3099

[3] Michael S. Greenberg, Jennifer C. Byington, David G. Harper, "Mobile agents and security", IEEE Communications Magazine, Vol. 36, Pages: 76~85, July 1998

[4] F. Hohl, "A model of attacks malicious hosts against mobile agents", in 4th Workshop on Mobile Object Systems: Secure Internet Mobile Computations, 1998

[5] Ying-Hong Wang, Hua-Chieh Chen, 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, Pages: 9~16