Improving Security Policies in Mobile Agent Based Systems

*Jaspreet Kaur, **Prof. Jasbir Singh Saini
Guru Nanak Dev Engineering College, Ludhiana

Abstract
With the development of network technology and the extensive use of e-commerce, the traditional e-commerce processes and its supported technology were faced with challenges. Traditional information retrieval systems have several shortcomings in common, such as delaying in information updating, costing additional host and network resources, and so on. The promise of mobile agent technology is becoming highly attractive. We approach to apply the mobile multi-agent technology to information retrieval in order to build a brand-new system. Although the mobile agent technology advantages information retrieval systems and features such as reducing network load, without continuous network connections and easy to support services, it also brings several new negative problems. The most serious one is the security problem because of agent's mobility and initiative. In this paper, we firstly analyze the drawbacks of current information retrieval systems, and then describe how to employ the mobile multi-agent technology to the information retrieval system to improve its performance. What we discuss mainly in this paper is the security problems of the information retrieval system based on mobile agent (IRSMA). We analyze threats to the security of the new system, study out the security policies, and at last establish a robust and secure architecture name MASA (Mobile Agent Security Architecture), which can effectively protect our system, and also adapt to other network application based on mobile agent because of its generality. For implementing the data safe transmission in Internet, a safe transmission mechanism which base on RSA and DES algorithm is put forward.
Keywords- RSA; DES; digital abstract; safe transmission; information retrieval; mobile agent; agent; e-commerce; security; Java.

I. INTRODUCTION

With the rapid development of e-commerce, its security issues were particularly notable and the traditional Client / Server (C / S) computing model has been unable to meet the actual needs of network application, distributed computing is increasingly becoming one of the critical study in computing technology field nowadays. As an emerging distributed computing model, Mobile Agent has many merits such as reducing network load, overcoming network latency, supporting for mobile clients and cross-platform implementation, robustness and fault tolerance [1]. It can migrate from one host to another automatically on the network to complete the assignments given by the owner of Mobile Agent, such as searching, filtering and collecting information, etc, or even e-commerce activities on behalf of users [2]. E-commerce based on Mobile Agent has the intelligence, dynamic and mobility, which have brought new ideas and excellent features to distributed computing. However, because its procedures were implemented on the host for freedom movement and complete autonomy, it also brings a lot of problem of traditional security fields of e-commerce [3].

For implementing the data safe transmission in Internet, a safe transmission mechanism which base on RSA and DES algorithm is put forward. The mechanism makes full use of advantage of DES and RSA. Because encryption speed of DES algorithm is faster than RSA algorithm for long plaintext, and RSA algorithm distribute key safely and easily. Date encryption security of DES algorithm is far higher. This mechanism realizes the confidentiality, completeness, authentication and non-repudiation. It is an effective method to resolve the problem of safe transmission in Internet. Internet is an open system which faces to public, it must confront many safe problems. The problems include network attack, hacker intruding, interception and tampering of network information which lead huge threat to Internet. Information security becomes a hot problem which is concerned by our society.

This paper puts forward a safe mechanism of data transmission to tackle the security problem of information which is transmitted in Internet. The mechanism includes many properties that are confidentiality, completeness, authentication of identity, and non-repudiation. It bases DES algorithm and RSA algorithm.

II. SYMMETRIC ENCRYPTION ALGORITHM-DES ALGORITHM

A. DES Algorithm

DES (Data Encryption Standard) algorithm is a traditional encryption technology. It developments in 20th century 70's and it was adopted by American government in November, 1976. Encryption and decryption of this algorithm are equivalence. The algorithm is open, but the key do not release. The security of System depends on the secrecy of the key.

DES algorithm synthetically makes use of many cryptography technologies which include replacement, alternation and data input. It is a product cryptogram. Plaintext is divided into many blocks when encryption begins. Each block has 64 bits and the length of key is 64 bits. The valid length is 56 bits and the rest 8 bits are used for parity checking.

First, 64 bits data is divided into two parts after initial replacement. Each part includes 32 bits. Then iterative process began. Right half 32 bits are extended to 48 bits. The result exclusive or with 48 bits sub-key which is got from 64 bits keys. The result is compressed as 32 bits through s

box. After replacement, the 32 bits data exclusive or with left 32 bit data which is got from the beginning of replacement. Right half part of the new round is got. At the same time, the result is regard as the parameter of new round [4].

After 16 round replacements, a new 64 bits data is generated. There is one step we must pay attention to. The two results of last round do not exchange. The encryption and decryption can use the same algorithm through this process. To the last, the 64 bits result needs an inverse replacement. The 64 bits cipher text is got.

B. The Shortage and Improvement of DES

Although DES is a safe encryption algorithm, the security issues of DES exist. First, the length of DES key is too short, because it includes 64 bits. Second, the weak links of DES are the protection and distribution of the key. Once the key lose, the whole system becomes worthless. Third, all the calculation of DES is linear besides the calculation of S box.

Because the key of DES has some shortage, triple DES algorithm is brought up. The length of key lengthens to 112 bits. This method performs three times encryption by using two different keys. Supposing two different keys are K1 and K2. K1 performs DES encryption and K2 decrypts the result of step one. Using K1 encrypt the result of step two. When encryption is performed, encryption algorithm and decryption algorithm exchange. The sequence of keys does not exchange. The specific process is expressed by figure1.

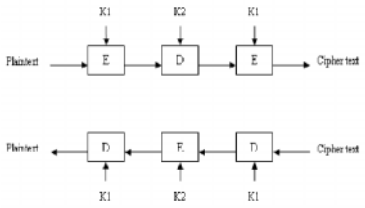

Figure 1. The process of DES

III. PUBLIC KEY ALGORITHM-RSA ALGORITHM

Public key algorithm is also called asymmetric key algorithm. The basic thought of public key algorithm is that the key is divided into two parts. One is encryption key and the other is decryption key. Encryption key can not be got from decryption key and vice versa. Because

public key is open and private key keep secret, RSA algorithm overcomes difficult of key distribution. RSA encryption process is showed as figure 2.

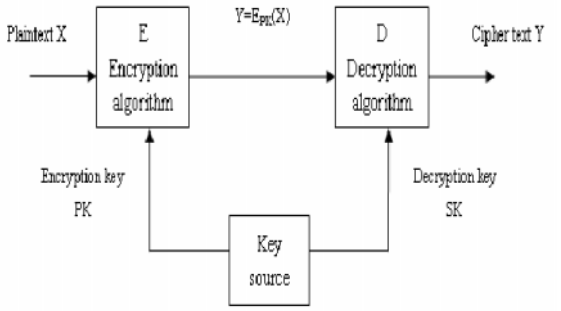

Figure 2. The process of RSA.

The principle of RSA algorithm is that: according to number theory, it is easy to finds two big prime number, but the factorization of the two prime numbers is hard. In this theory, every customer has two keys. They are encryption key PK = (e , n) and decryption key SK = (d , n) . Customer opens public key. Each person who wants to transmit information can use the key. However, customer keeps private key to decrypt the information. Here, n is the product of two big prime number p and q (the bits of p and q which are decimal number extend 100). e and d satisfy certain relation. When e and n are known, d can not be got. The specific content of algorithm is showed as below [5].

A. Encryption and Decryption Algorithm

Assuming integer X expresses plaintext and integer Y expresses cipher text. The operation of encryption is that

Encryption: $Y = X^{e} \bmod n$ (1)

The operation of decryption is that

Decryption: $X = Y^{d} \bmod n$ (2)

B. Key Generation and Calculation of Relevant Parameter

1) Calculating n. Customer selects two big prime number p and q. The value of n can be got by the equation n = p * q . n is the mode number of RSA algorithm. Plaintext must be expressed by a number which is smaller than n. In practice, n is long number which includes a few hundreds of bits.

2) Calculating φ (n) . Customer calculates the Euler function

$$\varphi(n) = (p-1) * (q-1) \qquad (3)$$

φ (n) is defined as the number which is smaller than n and primes to n.

3) Choosing e. Customer chooses a number e which prime to φ (n) from [0,φ (n) − 1] as open encryption index.

4) Calculating d. Customer calculates the d which satisfies the follow equation.

$$e * d = 1 \bmod \varphi(n) \qquad (4)$$

5) Public key PK = (e, n) and private key SK = (d , n) are got through calculating.

IV. MODEL OF DATA SAFE TRANSMISSION BASED ON RSA AND DES

Digital signature can achieve following three points: receiver could check the signature of message which is sent by dispatcher. Dispatcher can not deny the signature of message. Receiver can not fake the signature. Encryption transmission process of digital signature is showed as figure 3.

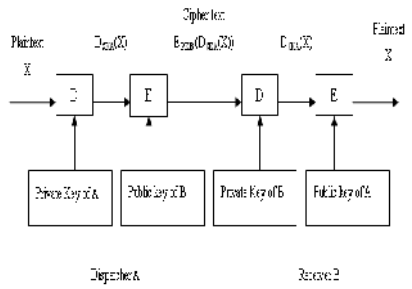

Figure 3. The process of digital signature.

Dispatcher A uses his private key (SKA) encrypt the signature. The result is encrypted by public key (PKB) of receiver to protect the security of safe transmission. After the message is transmitted in network, receiver uses his private key decrypt the signature which is sent by dispatcher. At the same time, receiver uses public key (PKA) of dispatcher to verify the signature.

DES and RSA represent symmetrical and asymmetrical encryption algorithm respectively. Because the mechanism is different, they have their own merit and shortcoming. The comparison is showed as below:

1) In aspect of security, DES and RSA algorithm have strong security. The methods which break the algorithm in short time do not exist.

2) In aspect of encryption speed, the velocity of DES is faster than RSA algorithm. Because the length of DES has 56 bits, software can enhance the speed. The calculation process of RSA algorithm has many steps such as power and mod of big integer with many bits. The speed of RSA is slower than DES. In crowed network, it is not suitable to encrypt long plaintext.

3) In aspect of key management, RSA algorithm is better than DES algorithm. Because public key is opened to outside and private key is kept by holders. The update of key is easily. However, DES needs to allocate key pair. The update of key is hard. DES generates and keeps different key. At the same time, the transmission of key in networks is hard to guarantee [6].

RSA algorithm can realize data signature and authentication. It is better than DES. RSA achieve the reliability, completeness, and non-repudiation of data transmission. Structural drawing of data safe transmission is showed as figure 4. The concrete step is illustrated as figure 4.

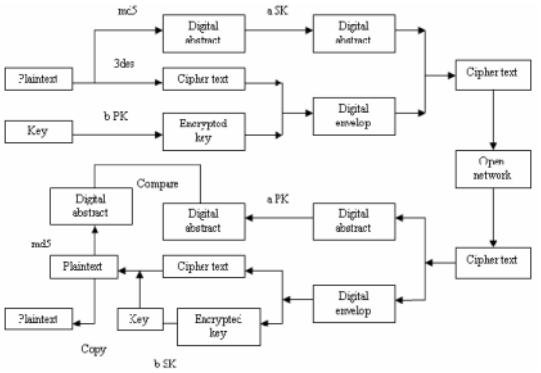

Figure 4. The structure drawing of data safe transmission.

1) First, dispatcher and receiver generate key pair (public key and private key) according to RSA. They open the public key to sign the digital abstract and verify the signature. Public key also encrypts and decrypts the symmetrical key.

2) The plaintext which dispatcher wants to send is generated digital abstract with 128 bits according to algorithm. The digital abstract is encrypted by private key from dispatcher. Then digital signature is generated to guarantee the reliability and non-repudiation during transmission.

3) Key pair of triple DES is generated in receiver. Then it encrypts the plaintext. Using public key of receiver encrypt symmetrical key pair.

4) Symmetrical key and plaintext which are encrypted by dispatcher are sent to receiver through open network. Encrypted digital abstract is dispatched too.

5) Receiver uses their own private key to encrypt symmetrical key pair, after getting the information from dispatcher. Then receiver uses symmetrical key decrypt message which is encrypted by dispatcher. At the same time, plaintext is copied.

6) Public key of dispatcher encrypts digital abstract. The digital abstract which is from dispatcher and calculated abstract which is from plaintext are compared. If the results are same, the transmission is safe. If the results are different, the message is tampered.

V. E-COMMERCE SECURITY MODEL BASED ON MOBILE AGENT

Figure 5 shows a trusted third party based on the security e-commerce model of Mobile Agent, it designs for the security threats, which comes from malicious main host to agent. Workflow of model is as follow:

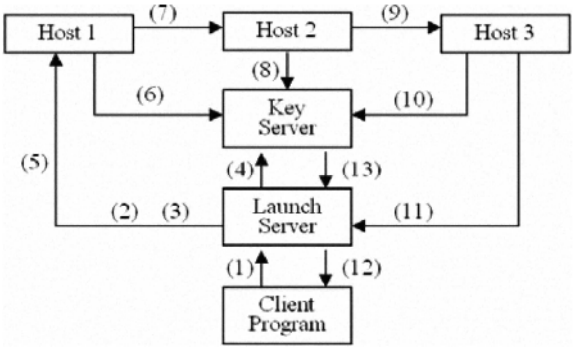

Fig. 5 Flowchart of secure e-commerce model

(1) Client Program based on user input, gives Launch Server query request.

(2) Launch Server generates an agent object, the query is initialized, sets agent's access route.

(3) Launch Server generates a pair of keys for the agent.

(4) Launch Server signs the query request, and registers the public key of agent on the Key Server.

(5) Launch Server sends agent to the network.

(6) The Database Server of Host 1 obtain agent public key from Key Server, and verity the agent queries. Then, the search agent may check the information, and use their private key sign the query results and encrypt public key of agent.

(7) Agent migrates to Host 2.

(8) Database Server of Host 2 performs the same operation in step 6.

(9) Agent migrates to the next Host 3 of access route.

(10) The Database Server of Host 3 performs the same operation in step 6.

(11) Agent returns to Launch Server.

(12) Launch Server decrypts query results, and verifies the signature of query results, then checks whether access routes change, calculates finally, reporting the best solution to the client.

(13) Launch Server deletes public key, which completes tasks on the Key Server.

VI. MODEL ANALYSIS AND TEST

This is a security model based on the public key encryption system; each agent and the host have a pair of keys for encryption and decryption. Agent and the host can encrypt or give digital signature to carry data of agent, in order to achieve protection of the transaction data (such as commodity prices, the number and query results, etc.) In this security model, it uses Key Server to facilitate management of agent's public key. Before Launch Server sends query agent, queries are signed by the agent's private key, and registers agent's public key on the Key Server. Database Server of business obtains agent public key from querying the Key Server, it can verify the source of queries to prevent the agent was pretended. In addition, query results of Database Server use its own private key sign, using agent public key encrypt. on the one hand, to prevent others reading or tampering with query results, ensure Launch Sever that only those with private key of agent read the query results; on the other hand, Launch Server obtains merchant public key via Key Server to verify the source of query results, to prevent other businesses posing as a

certain business return a false query result. This will solve the agents' and merchants' authentication problem in the system.

In this model, the system's information security can be ensure through the following mechanism: the use of authorized access, resource control, auditing and other security mechanisms to protect Key Server on; the use of RSA algorithm to encrypt and sign the information. The complexity of breaking RSA encryption system depends on the length of the key, the longer key is, the harder it will be broken, the higher security of the system become. Under the present circumstances, 128bits key length can assure the data's safety. A longer key can be used to encrypt the information and signatures in the future.

To assess the performance of the model, the host agent was tested the round-trip time of information inquiries, which visit three businesses for different sizes (such as the different volume and conditions of query goods). The results showed that agents' round-trip time and agents' query size are linear incremental relationship. This is mainly due to the introduction of the RSA encryption system, each query request and query result must be encrypted and decrypted, and it takes some time. The longer the key is, the more obvious time-consuming become. It also simulates malicious host's attacks, and changes the agent's query information and query results, the test revealed that agent's round-trip time is longer than the time which never suffers from attacks, indicating agent's round-trip time can be used as an indicator of whether agent being attacked.

VII. CONCLUSION

Mobile Agent is a major technology of e-commerce system in the future; the article explores security issues in details on e-commerce system based on Mobile Agent and gives a viable security model. With the continuous resolution of these security issues, it is believed that e-commerce system based on Mobile Agent will continue to be refined, promoting the development of e-commerce further.

Data safe transmission bases on triple DES and RSA algorithm. It makes use of the advantage of DES which has the high encryption speed for plaintext. It also develops the merit of RSA which manages the key easily. This mechanism realizes the confidentiality, completeness,

authentication and non-repudiation. It is an effective method to resolve the problem of safe transmission in Internet.

REFERENCES

[I] RuLin Lu. Knowledge Science and Computational Science rMJ Tsinghua University Press 2003.0 I (In Chinese)

[2]White,lE.,Telescript technology:the foundation for the electronic marketplaee. White Paper,General Magic Inc.,Mountatin View,CA,1994.

[3] Qi Lin,Jianwei Zhang. Mobile Agent Security on MaliciousHost [J]. Computer Engineering,2002,(6): 118 - 120. (In Chinese)

[4] H. G. Zhang, Y. Z. Liu, "Evolution password and DES evolution research," Chinese Journal of Computer, vol 12, no. 2, pp. 1678-1684, September 2003.

[5] B.Yang, Modern Cryptography[M], Beijing: Tsinghua University Press, 2006.

[6] B. Jiang, "Synthesized encryption plan of DES and RSA," Micro-Computer Science, vol 23, no. 6, pp. 52-54, March 2006.

[7] W. Li, T. Zhao, w. Zang, "Summary-based information retrieval model", Jounal of Software, vol. 19 no.9, pp. 2329-2338, September 2008.

[8] X. Xu, R. Wany, "The Agent-based information retrieval model with multi-weight ranking algorithm", Journal of Electronics & Information Technology, vol. 30 no.2, pp. 482-485, February 2008.

[9] S. Gui, L. Li, Z. Peng, "Network information retrieval method based on information resource catalog system", Geomatics and Information Science of Wuhan University, vol. 33 no.! I, pp. 1202-1205, November 2008.

[10] http://en.wikipedia.orglwiki/InformationJetrieval

[11] A. Heydon, M. Najork, "Mercator: A scalable, extensible Web crawler", World Wide Web, vol. 2 no.4, pp. 219-229, April 1999.

[12] W. Yang, R. Dai, X. Cui, "Model for Internet news force evaluation based on information retrieval technologies", Journal of Software, vol. 20 no.9, pp. 2397-2406, September 2009,

[13] S. Brin, L.page, "The anatomy of a large-scale hypertexual web search engine", in Proceedings of the WWW Conference, Brisbane, Australia, April 1998, pp. 107-117.

[14] S. P. Wang, Y. M. Wang, "Digital signature scheme based on DES and RSA," Journal of Software, vol 14, no. 1, pp. 146-150, June 2003.

[15] Douglas R. Stinson, Cryptography Theory and Practice[M], Beijing: Publishing House of Electronics Industry, 2002.

[16] K. C. Lu, Computer Cryptography-data Confidentiality and Security in Computer Network, Beijing: Tsinghua University Press, 2000.

[17] Y. X. Xu, Java Security Program Example, Beijing: Tsinghua University Press, 2003.

[18] Jianxun Lin, Renfa Li, ShenSheng Zhang.The Issues of Mobile Agent and Safety[J]. Computer Engineering and Applications 2000.07,27-30(In Chinese)

[19] Tomas Sander,Christian F Tschudin.Protecting Mobile Agent against Mulicious Hosts.In: G..Vigna(Ed.),4 Mobile Agent and Security,Lecture Notes im Computer ScienceI419,Springer,Berlin:1988:44 - 46

[20] Xiang Tan, Yuqing Gu, Chongming Bao. Mbile Agent System Security Research [J]. Computer Research and Development,2003,Vol. 40 No. 7,984 - 993(In Chinese)