SECURITY SCHEME FOR MOBILE AGENT SYSTEM IN E-COMMERCE SCENARIO

Rajwinder Singh and A.K.Sarje

Deptt. of Electronics and Computer Engineering

Indian Institute of Technology Roorkee,

Roorkee – 247667, India.

rwsingh@yahoo.com

ABSTRACT

Mobile agents are software program that can autonomously migrate from a platform to another platform to accomplish their tasks and it is believed that they will play an important role in future e-commerce system, offering higher flexibility and improved performance. In spite of those benefits from mobile agent system, security in mobile agent system is especially hard to achieve when a mobile agent is executed on remote platform that may behave maliciously or mobile agent may behave maliciously on the remote platform. There has been a lot of work done in the area of mobile agent's security. Recently, Bae et al. proposed a security scheme for mobile agent system using an IDENTITY- BASED digital signature scheme and claimed that their scheme provided complete security to mobile agent system.

However, in this paper, we show that their security scheme still suffers from some security weakness such as man in middle attack and previous agent platform can forge the signature. And then we further propose a new security scheme for secure mobile agent system that solves the weakness of their protocol using dynamic generated partial multi signature with message flexibility and provides the security services such as mutual authentication, confidentiality, integrity, non-repudiation and the prevention of replay and exclude attack. The propose scheme is suitable and practical for protecting mobile agent from malicious platform in e-commerce scenario over the Internet.

KEY WORDS

Mobile Agent, malicious platform, multi-signature scheme

SECURITY SCHEME FOR MOBILE AGENT SYSTEM IN E-COMMERCE SCENARIO

1 INTRODUCTION

Mobile agents are software programs that can autonomously migrate from platform to platform to accomplish their goals in computer networks [1]. The mobile agents are executed locally on remote hosts to perform their task and return to the end-user to report their results. The main advantages of the mobile agent paradigm lie in its ability to move the client code and computation to remote server resources; reducing network traffic and to overcome network latencies [2]. Thus a mobile agent offers a new computing paradigm for distributed application development due to combination of autonomy and mobility characteristics. There are several application areas of mobile agent systems such as information searching and retrieval, network management and e-commerce. However, it is difficult to find commercial distributed applications using a mobile agent. Since a real distributed environment is an open network, it is very vulnerable to a variety of security attacks. Despite the benefits of mobile agent paradigm, they pose new threats to security as stated in [3,5] and could classify into two areas.

- Threats to agent platform from malicious agents.
- Threats to agent from malicious agent platforms

Many researchers have been worked to solve the mobile agent's security in above areas [4]. Since the first problem is similar to the one that already existed with Java and ActiveX technologies in which the host has to run software coming from untrusted sources.

Second problem is harder than the first one because the mobile agent is executed on the remote agent platform that has no direct control over the remote platform by the agent owner and more vulnerable to attacks by remote agent platform if platform is malicious since during its execution the remote platform is able to access the agent's code, data and state. [5]

Recently, Bae et al [6] proposed a security scheme to solve the security issues for mobile agent system by using the digital multi-signature [7] and identity-based key distribution scheme [8]. But their protocol has some security weaknesses; i.e., their protocol is vulnerable to man-in-the-middle attack and the previous agent platform can forge the multi-signature.

In this paper, we discuss the security weaknesses of Bae et al. security scheme. Next we propose a security scheme for protecting mobile agent system. To solve the weaknesses of their protocol and strengthen the security of the mobile agent system, we apply dynamic generated partial multi-signature scheme with message flexibility [9] to our scheme. Our scheme provides the mutual authentication, confidentiality of the mobile agent's execution results, the non-repudiation, and the prevention of replay attack and exclude attack. In this paper we consider a shopping scenario in which a mobile agent searches the best price of the item.

The paper is organised as follows. In next section 2, we explain the notations used in this paper. The security scheme of Bae et al. and their security weakness are briefly describes in section 3 and 4 respectively. In section 5, we present the proposed scheme for mobile agent security in e-commerce scenario. In section 6, we analyze the security of our proposed scheme. Finally, we present our conclusion.

2 NOTATIONS

Model and cryptography notations used in the paper are same as in [6] and defined as follows.

AP_i	The ith agent platform $(0 \le i \le n)$ on migration path of mobile agent
AP_0	Agent home platform

AMC	Trusted agent management center
Id_i	Identity information of AP_i
A_ name	A name of mobile agent (or agent)
A_code	An executable code of mobile agent
A_ exe_ $results_i$	Execution results of mobile agent at the agent platform AP_i
A_ exe_ results	All execution results of mobile agent at the every agent platform
A_ sign	A multi-signature for $A\_exe\_results_i$
MA	A mobile agent, a set of {A_ name, A_ code, A_ exe_results, A_sign}
$Cert_{A:}$	A's certificate
p and q	Large primes with p= 2q+1
g	A generator $g \in z_p^*$ has order of q
x_i	A secret key of AP_i
y_i	A public key of AP_i, $yi = g^{xi} \pmod p$
h	A strong one-way hash function
$sk_{A, B:}$	A session key between A and B
E_k	An encryption function with key k
$time_i$	Timestamp made by APi
"||"	Concatenation.
$AP_i \rightarrow AP_n : M$	The agent platform AP_i sends the message M to the agent platform AP_n

3 SECURITY SCHEME OF BAE ET AL.

We first describe the Bae et al security scheme presented in [6]. Their scheme employed Okamoto-Ohta multi signature scheme based on Fiat-Shamir Scheme [7] and identity based key distribution scheme [8] to solve the security issues for mobile agent system. In their scheme, secure communication is obtained by using one-time password between hosts for each section through Identity-based key distribution rather than maintaining a public key directory. It generates multi-signature on the mobile code and verifies results of the previous step when migrating to next server. Then, the executable code and resulting data can be protected and unauthorized tampering can be detected in real time. Moreover, malicious disposal of agent and unauthorized copying can be detected by monitoring the migration condition of agent at the agent management center.

The scheme is composed of five phases that are Registration (agent platform registration and key distribution), CreateAgent, ExecuteAgent, TransferAgent and AuditAgent.

In the registration phase, all agent platforms (AP_i ($0 \le i \le n$)) should be registered at AMC in order to execute service to mobile agent system and AMC generates session key using ID upon request of registration from agent platform and distributes it to the agent platform using the smart card.

In CreateAgent phase, the agent is created at agent home AP_o with the path information and generates the session key with AMC using Diffie-Hellman key exchange scheme [10].

Then, AP_0 sends an encrypted agent code and path information to AMC as below

$$AP_0 \rightarrow AMC: \; E_{sk_{0,AMC}}(MA, time_0)$$

The AP_0 generates the session key with AP_1 using Diffie-Hellman key exchange scheme and also generates the multi signature on the execution result of the agent using Okamoto-Ohta multi signature scheme. Then APo sends the encrypted data to AP_1

$$AP_0 \rightarrow AP1: E_{sk_{0,1}}(MA, time_0)$$

In the ExecuteAgent phase, when an agent migrates to $AP_{i+1,}$ the platform treats this agent as one thread, executes the agent, makes a log_i and renews the result

$$Log_i = E_{k_{i,AMC}}(A\_exe\_results_i, time_i)$$

$$A\_exe\_results_i = A\_exe\_result_{i-1} \| log_i$$

Then AP_i generates a multi-signature on the execution results $A\_exe\_result_i$ of the agent using Okamoto-Ohta multi signature scheme.

In the TransferAgent phase, the agent migrates from agent platform to agent platform whenever the agent has made requests. The session key $E_{k_{i,i+1}}$ between agent platforms (AP_i and AP_{i+1}) is generated and session key $E_{k_{i+1,AMC}}$ is between AP_{i+1} and AMC is also generated. The AP_i transmits the sign for result of execution and agent code to AP_{i+1}

$$AP_i \rightarrow AP_{i+1}: E_{sk_{i,i+1}}(MA, time_i)$$

And then AP_{i+1} can verify the signature written by the previous AP_i. If the verification is correct, AP_{i+1} execute this agent. Otherwise AP_{i+1} reports to the AMC.

In the AuditAgent phase, the AMC knows the migration path and according to $AP_0 \rightarrow AP_1$: $E_{sk_{0,1}}(MA, time_0)$ and also know session key shared with AP_i whenever agent migrates. Hence the AMC decrypts all the execution result of the agent that travels according to planned path and arrives at AMC after signature verification. And then AMC encrypts the execution result with the session key $k_{H,\ AMC}$ and transmits it to agent home. Finally agent reports to home and terminates execution.

4 SECURITY ANALYSIS BAE ET AL. SECURITY SCHEME

In this section, we present the security weakness on the Bae et al. security scheme. There are two security weaknesses in the Kim-Chung protocol. First, their scheme is vulnerable to intruder-in-the-middle attack [11], because it uses the unauthenticated Diffie-Hellman key exchange as the method of session key generation in the CreatAgent phase, the ExecuteAgent phase and the TransferAgent phase. The man-in-the-middle attack on this protocol is as follows. AP_i and AP_j have secret random values R_i and R_j, respectively. An illegal adversary creates R'_i and R'_j. The adversary intercepts AP_i's exponential value g^{R_i} and replaces it with $g^{R'_i}$. He also intercepts AP_j's exponential value g^{R_j} and replaces it with $g^{R'_j}$. AP_i forms session key $k_{i,\ j} = g^{R_i R'_j}$, while AP_j forms session key $k_{j,\ i} = g^{R'_i R_j}$. The adversary is able to compute both these keys. When AP_i sends a message encrypted under $k_{i,j}$ to AP_j , the adversary deciphers it, re-enciphers under $k_{j,i}$, and forwards it to AP_j . Similarly the adversary deciphers messages encrypted by AP_j under $k_{j,i}$, and re-enciphers them under $k_{i,j}$. Both AP_i and AP_j believe that they communicate securely, while the adversary reads all messages. Therefore, the adversary can know the agent code, the path information and the execution results of the agent which should be protected from unauthorized user. Since the adversary can be other agent platforms, other agent platforms can know all execution results of the agent in the previous agent platforms. Therefore, this protocol does not provide a confidentiality of execution results.

Secondly since each agent platform AP_i generates the multi-signature on a different $A\_exe\_results_i$ using Okamoto-Ohta multi-signature scheme without message fexibility; i.e., the message flexibility means that a message does not need to be fixed beforehand, the previous signer can forge the multi-signature as follows. After the previous signer AP_j ($1 \leq j \leq\cdot i$) intercepts the multi-signature transmitted from AP_i to AP_{i+1}, AP_j changes her own execution results and re-signs on the changed execution results and sends the forged multi-signature to AP_{i+1}.

5 PROPOSED SECURITY SCHEME FOR MOBILE AGENT

In this section, we propose a security scheme for the secure mobile agent system that solves the weaknesses of Bae et al. security scheme and provides the mutual authentication, confidentiality, the non-repudiation, and the prevention of replay attack and exclude attack. In our protocol, each agent platform efficiently generates partial multi- signature on execution results of the mobile agent using dynamic generated partial multi-signature scheme that has the feature of the message flexibility. So, unlike Bae et al. scheme, the previous agent platform cannot forge the multi-signature in this scheme. And it also protects the mobile agent's code and execution results from unauthorized entity using encryption function. The proposed security scheme has five phases such as agent platform registration phase, mobile agent creation phase, mobile agent execution phase, mobile agent migration phase and mobile agent arrival phase.

5.1 Agent platform Registration Phase

All agent platform and agent home must register at the AMC before access the service of mobile agent system. The protocol between all agent platforms AP_i and AMC for registration and to obtain the session key between them using KEA key exchange algorithms [12] is as follows

1. AP_i sends a request message $request_i$ and $cert_i$ to the AMC.
2. AMC sends $cert_{AMC}$ to the AP_i and register them at AMC.
3. Session key $sk_{AMC,\,i}$ are established between each AP_i and AMC using KEA protocol.

5.2 Mobile Agent Creation Phase

The protocol for mobile agent creation at agent home AP_o as follows:

1. The mobile agent is created at AP_o and the result is $A\_exe\_result_0$.

2. Generates the partial multisignature (s_o, r_o) on the result of mobile agent creation $A\_exe\_result_0$ to ensure that AP_o created that mobile agent as follows:

- AP_o selects a random number $k_o \in Z_q^*$
- AP_o computes $Ro = y_o^{k_0} \bmod p$

$$r_o = (h\,(A\_exe\_result_0 \,||\, Id_o))^{-1}.\, R_o \bmod q$$

$$s_o = (x_0 r_o + y_1).k_0^{-1} \bmod q$$

3 Session key $sk_{0,1}$ is generated between AP_o and AP_1 using KEA key exchange algorithm.

4. Now, AP_o generated $E_{sk_{0,1}}(MA, time_0)$ and $E_{sk_{0,AMC}}(MA, time_0)$. After initialization the agent immigrates with the information (Id0, r_o, s_o, $E_{sk\ 0,1}(MA, time_0)$) to AP_1 and (Id_0, ro, so, $E_{sk\ 0,AMC}$ (MA, $time_0$)) to AMC.

5.3 Mobile Agent Execution Phase

When a mobile agent migrates to AP_{i+1} , a platform treats this as one thread. The protocol for mobile agent execution at platform AP_{i+1} as s follows

1. AP_{i+1} executes the mobile agent and then it makes a log_i and renews the A_exe_results.

$$log_i = E_{sk_{i,AMC}}(A\_exe\_results_i, time_i)$$

$$A\_exe\_results_{i,} = A\_exe\_results_{i-1} \,||\, log_i$$

At this stage, the results of the execution must be protected from other agent platforms and this can be done with the help of private key of the AP_i.

2 APi generates the partial multisignature on $A\_exe\_results_i$ to ensure that the AP_i executes the mobile agent and make the results $A\_exe\_results_i$ as

- AP_i selects a random number $k_i \in Z_p^*$
- AP_i computes $R_i = y_0^{k_i} \bmod p$,

$$r_i = (h\ (A\_exe\_results_i \,||\, Id_i))^{-1}.\ R_i \bmod q$$

$$s_i = (x_i\ r_i + y_{i+1}).k_0^{-1} \bmod q$$

The last platform AP_n uses the partial multisignature from AP_{n-1} to compute the final multisignature and indicates as the next destination the initial signer platform as:

$$S_n = (x_n\ r_n + y_o).k_n^{-1} \bmod q$$

5.4 Mobile Agent Migration Phase

The protocol for mobile agent migration from platform AP_i to AP_{i+1} as follows:

1. Session key $sk_{i,\ i+1}$ is established between AP_i and AP_{i+1} using KEA protocol when a mobile agent is migrated from AP_i to AP_{i+1}.
2. The AP_i sends the partial multisignature for the results of execution and encrypted agent code $Esk_{i,i+1}(MA, time_i)$ to AP_{i+1} .

5.5 Mobile agent Arrival Phase

When a mobile agent reaches at agent home platform, it calculates

- For i= n, n-1, ----2, $Ri' = y_o^{s_i^{-1}.y_{i+1}}.y_i^{x_o r_i s_i^{-1}} \bmod p$, and $Ti = Ri'.r_i^{-1} \bmod q$ by using AP_i's public key y_i and verifies $r_{i-1}=T_i$. $(h\ (A\_exe\_results\ ||Idi))^{-1} \bmod q$
- For i=1, $Ri' = g^{s_i^{-1}.y_2}.y_0^{x_o r_i s_i^{-1}} \bmod p$, and $Ti' = Ri'.r_j^{-1} \bmod q$ and verifies $Ti' = (h\ (A\_exe\_results_1\ ||Id_1))$

Now, the agent home platform verifies the signatures provided by each new platform and decrypts the result. If signature verification fails, the agent platform must report the AMC for further action i.e. either got the information from the AMC for rechecking the signature or again executes the agent.

6 SECURITY ANALYSIS OF THE PROPOSED SECURITY SCHEME

In this section we analyze the security of the proposed scheme. The proposed scheme uses the dynamic generated partial multi-signature with message flexibility. With the proposed scheme, the agent home platform creates the mobile agent and signs the result and then forwards this to the next platform. Each new platform can modify the results and sign the result. The order of platform to be visited need not be specified in advance but may be generated dynamically. The verification process shows who signed with modified result and the order of platforms visited. Also since the execution result and results of the mobile agent are protected by the encryption function, it is very useful and practical in protecting the mobile agent from malicious platform in the E-commerce over the Internet to find the best price of the products.

The proposed security scheme provides the basic security service like the mutual authentication, confidentiality, non-repudiation, prevention of replay and excludes attack, protection of private key of the agent home platform and solves the weakness of the Bae et al security scheme as follows:

- **Mutual Authentication:** Since the proposed security scheme establishes the session key between two-agent platforms, so anyone who does not know the private key corresponding to public key of the certificate cannot compute the session key. Hence the mutual authentication is provided between two-agent platforms.
- **Confidentiality of the agent code and data:** Since the private key of the agent home platform is used in the mobile agent creation phase, no other platform knows the result

except agent home platform AP_0 and achieve the confidentiality security service on agent code and data.

- **Integrity of agent code and data:** Since the mobile agent is encrypted with the next platform session key and send this information to next platform as well as AMC and next platform can verify the integrities of agent code and data through the verification process. If any incorrectness is detected, this is being reported immediately to the AMC.
- **Protection of result obtained at each platform:** Since the agent home platform's public key is included in the first step of signature generation. After the agent is dispatched to collect information, each new platform generates the partial signature and encrypts the information. If any verifier, except the agent home platform and the platform that provides the information, wants to verify and decrypts the information, it must get the private key of the agent home original platform or of the platform that provides the information.
- **Prevention of replay attack:** Since each agent platform uses different timestamp and random number in proposed scheme, the unauthorized entity cannot succeed in the replay attack.
- **Prevention of exclude attack:** Since the public key of next platform is added in the generation of the partial multisignature so that verification of the signing order of platform agent visits will be fixed after agent return back to the agent home platform.

Also the proposed scheme solves the weakness of the Bae et at as follows. First, since our security scheme uses the authenticated key exchange protocol KEA in the session key generation, unauthorized entity who does not know the communicating agent platform's private key cannot perform the intruder-in-the-middle attack. Second, we use the dynamically generated multi-signature scheme with message flexibility. So, the previous agent platform cannot forge the multi-signature by using the verification of signing order.

7 CONCLUSION

In this paper, we briefly reviewed the Bae et al security scheme for mobile agent system and shown that there scheme suffered from the man in middle attack, and previous agent platform forged the multisiganture and exclude attack

We further proposed a security scheme for the mobile agent system that solves the security weakness of Bae et al security scheme. We applied the KEA key exchange algorithm and dynamically generated partial multisignature with message flexibility to provides the mutual authentication, confidentially, integrity non-repudiation, prevention of replay attack and exclude attack and cannot forged the multisiganture by previous agent platform The proposed scheme is suitable and practical for protecting mobile agent and agent platform in the e-commerce over Internet.

REFERENCES

1. A. Fuggetta, G. P. Picco, and G.Vigna. "Understanding Code Mobility," IEEE Transactions on Software Engineering, vol. 24, no. 5, pp. 342-361,2000.
2. D. B. Lange, M. Oshima, "Seven Good Reasons for Mobile Agents," Communications of the ACM, Vol.42 (3), pp.88-89, March 1999.
3. W. Jansen and T. Karygiannis ," Mobile Agent Security," National Institute of Standards and Technology, Special Publication 800-19, August 1999.
4. N. Borselius, "Mobile agent security," Electronics & Communication Engineering IEE Journal, October 2002, Volume 14, no 5, pp 211-218, London, UK.

5. Fritz Hohl, “ A Model of Attacks of Malicious Hosts Against Mobile Agents”, in Proc. ECOOP Workshop on Distributed Object Security and 4th Workshop on Mobile Object Systems: Secure Internet Mobile Computations, pp 105 – 120, INRIA, France, 1998.
6. Y. Bae, S. Kim and I. Chung, “A Secure Mobile Agent System Applying Identity-Based Digital Signature Scheme," in Proc. Of the International Conference on Security and Management, SAM '03, June 23 - 26, 2003, Las Vegas, Nevada, USA, Volume 2. CSREA Press 2003, ISBN 1-932415-17-3
7. T. Okamoto and K. Ohta, “A Digital Multisignature Scheme based on the Fiat-Shamir Scheme," in Proc. ASIACRYPT'91, Advances in Cryptology{LNCS 739, Springer-Verlag, pp.139-148, 1991.
8. A. Shamir, “Identity-based Cryptosystem and Signature Scheme," in Proc. of CRYPTO '84, Advances in Cryptology, Springer-Verlag, LNCS , 196, pp.47-57, 1985.
9. S. Mitomi and A. Miyaji, \A General Model of Multisignature Schemes with Message Flexibility, Order Flexibility, and Order Verifiability," IEICE Transaction on Fundamentals, Vol.E84-A, No.10, pp.2488-2499, 2001.
10. W. Diffie and M. Hellman, “New Directions in Cryptography”, IEEE Transaction on .Information Theory, IT-22(6), pp. 644-654, November 1976.
11. A.J. Menezes, P.C. Oorschot and S.A. Vanstone, *Handbook of Applied Cryptography*, CRC, 1997.
12. National Security Agency, “SKIPJACK and KEA Algorithm Specification," Version 2.0, May 29, 1998.