European Journal of Scientific Research
ISSN 1450-216X Vol.51 No.3 (2011), pp.321-331

http://www.eurojournals.com/ejsr.htm

An Enhanced Mobile Agent Security Protocol

P. Marikkannu
Department of Information Technology, Anna University of Technology, Coimbatore, India
E-mail: pmarikkannu@gmail.com
Tel: +91-9444813225

J.J. Adri Jovin
Department of Information Technology, Anna University of Technology, Coimbatore, India
E-mail: adrijovin@yahoo.co.in
Tel: +91-9994797284

T. Purusothaman
Department of CSE & IT, Government College of Technology, Coimbatore, India
E-mail: purushgct@yahoo.com
Tel: +91-9842279020

Abstract

Mobile agent technology is one of the most advancing technologies in the world of computers with the property of mobility of the code from one location to another. Usually these mobile agents are used in a distributed environment, which possess hosts or systems in a distributed manner, to collect and to process the data obtained from various hosts and to provide the required result. Though code mobility possesses a number of advantages, it is prone to security attacks also. The external malicious entity may attack either the data possessed by the mobile agent or the mobile agent itself. A lot of algorithms have been proposed to cope with the security attacks present. However, a technique which may be immune to one type of attack may not be immune to some other type of attack. In this paper, we propose a protocol which would provide an integrated solution for the various types of attacks. The protocol uses the combination of three techniques to overcome most of the security attacks. In the protocol, we use trip markers, digital signatures and encryption techniques to make the mobile agent immune to most types of security threats. The results obtained on experimentation shows a good progress in the security aspects compared to most other techniques that are being used, in terms of security.

Keywords: Agent based intelligent systems, Malicious Identification, Mobile Agents, Security protocol

1. Introduction

Mobile agent technology is one of the most advanced technologies which introduce the concept of code mobility. The mobility of the code facilitates various tasks to be performed in an effective manner. Mobile agents prove to be more efficient in the case of usage in a distributed environment where data from various systems may be needed to perform a particular task. This also poses a threat over the entire system that the mobile code may be prone to malicious attacks. The malicious attacks

may either manipulate the data or increase the network traffic or misguide the mobile agent to some other location. Hence mobile agent security plays an important role in the mobile agent system. The security may be provided either to the mobile agent or agent platform. In our work, we propose a mobile agent security protocol which provides security to the mobile agent by protecting it from various types of attacks. A combination of techniques has been used to make this protocol an efficient one. We use trip marking to overcome these replay attacks, digital signature to provide the service of authenticity and authorization and finally the Malicious Identification police, to check whether any malicious attacks have been done over the mobile agent. The theoretical implications show that the mobile agent is theoretically secure. From the experimental point of view, it has been found that the protocol provides security to the mobile agent which makes it resistant to most known types of attacks.

2. Background

2.1. Mobile Agent

Mobile Agent paradigm is an extension to distributed computing paradigm. A mobile agent is a program that can migrate from a starting host to many other hosts in a network of heterogeneous computer systems and fulfill a task specified by its owner. A mobile agent is capable of performing a task on behalf of a user. It possesses various properties to make it suitable to be used in various tasks involving intelligence. Also it can communicate and interact with the neighboring or other mobile agents. The advantages of using a mobile agent in a distributed environment are

- Lowered network traffic
- Autonomous behavior
- Reduced network delay

Mobile agents, as a team are capable of performing tasks which need a synchronized approach. These abilities of the mobile agent make it more suitable to be used in various real time tasks. As they work in behalf of a user, they could also be assigned various real time tasks which may be booking a ticket or performing an online monitoring or similar tasks.

2.2. Mobile Agent Security

Ever since the emergence of mobile agent technology, the threats to mobile agents have also emerged. To overcome the various threats various algorithms have been proposed. However security of the mobile agent has been a challenging task for the past few decades. The various types of attacks that have been categorized so far are

- Agent to platform
- Agent to Agent
- Platform to Agent and
- Other to Agent platform

The various attacks that have been specifically identified are

- Masquerading
- Denial of service
- Unauthorized access
- Repudiation
- Eavesdropping
- Alteration and
- Replay attacks

In this work, we mainly focus on the security of the mobile agent which would possibly avoid the Agent to Agent Attack, Platform to Agent Attack and Others to Agent attacks.

2. Previous Research

There are numerous works that have been proposed to provide mobile agent with security. In this part, a few works are being analysed and the inference made from them is scripted.

Venkatesan et al (2010), proposes a model of policy based malicious identification police which helps to identify the malicious agents by means of the extended Root canal Algorithm (XRC). The model is based on the policy files or the definition files that are present within the system. This model overcomes the drawbacks of the simple MIP which works based on the principle of signature based Intrusion Detection System. Moreover, the system uses an Attack Identification Scanner which would help the system to check whether any attack have been made over the mobile agent or the mobile agent is subjected to any sort of attack. This model also compromises of techniques to identify any new types of attack by means of lexical analysis and similar methods. However, the attack code detection strategy is not well defined. Though the model maintains the integrity of the mobile agent, it couldn't provide a better solution against replay attacks and non-repudiation. This model serves to act similar to an anti-virus that is being used in a system.

The model proposed by Pierre and Benachenhou (2006) aims at providing a better security to the mobile agent by means of maintaining a reference clone of the mobile agent in a secure severe where no attacks are possible. The model is based on the assumptions that the network is divided into regions and agent communication is conducted through an authenticated channel. Though this model may be found to be more secure, it adds an overhead in the network. This model is immune to masquerading, Denial of Service, Eavesdropping and Alteration. For each mobile agent generated in the system, a reference clone is being created and transmitted to the secure server. Practically, this increases the traffic of the network. Also the assumptions that are made in this system are highly not practical because no private secure channels may be used for agent transport. In case, if any such channel is being used, it does not necessitate the usage of this method itself. Therefore, this model could be considered a theoretical one and may not have much consideration in a practical aspect.

Xuan Hong (2009) proposes a proxy signature protocol which mainly focuses on the non-repudiation attack. This protocol satisfies the various aspects like verifiability, unforgeability, secrecy, undeniability and identifiability which are mainly concerned with non-repudiation attacks. This method uses a digital signature to assure authenticity. Though this method is more successful with non-repudiation attacks, it couldn't prove itself to be efficient in case of other types of attacks. Therefore, this technique couldn't be considered so efficient for a secure transaction of data to be done. This technique doesn't assure most other secure services and the issues related to it. However this technique is provably efficient in case of identifying a host or the origin of a mobile agent.

Ametller (2004) proposes a system in which the agent code is protected by means of a public decrypting function, agent authentication and some other classical protection mechanism. This method of protecting the mobile agent may be efficient against classical threats. Attacks to overcome the techniques used in this system have been identified in the recent period and hence, this method couldn't be used in case of the modern mobile agent systems.

In our work, we propose a model to enhance the security mechanisms in the existing works.

4. Proposed Solution

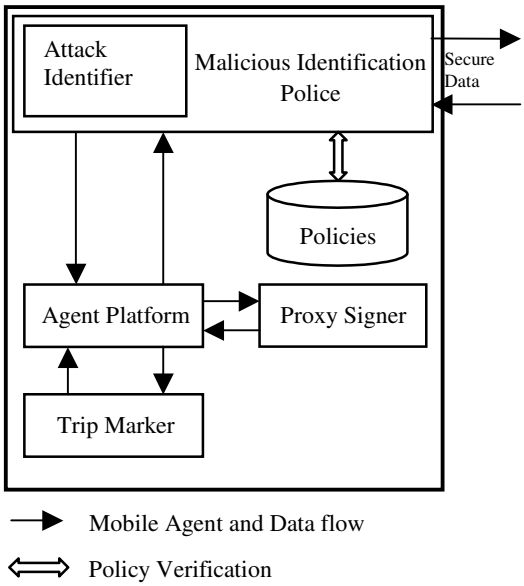
Figure 1 shows the architecture of the system. The various components of the system are as follows.

- Agent Platform
- Trip Marker
- Proxy Signer
- Malicious Identification Police

4.1. Agent Platform

The agent platform is one which is responsible for the creation of the mobile agent. The mobile agent that is created is subjected to the various processes in the model. The secure mobile agent is sent to the various parts of the system for further processing.

Figure 1: System Architecture



4.2. Tripmarker

The trip marker appends the trip mark data to the mobile agent. The trip marker sets an expiry times and a counter for the mobile agent. It is also responsible for checking and resetting the expiry time of the mobile agent as well as decrementing the counter for the mobile agent. This would be helpful to overcome the external replay attacks.

4.3. Proxy Signer

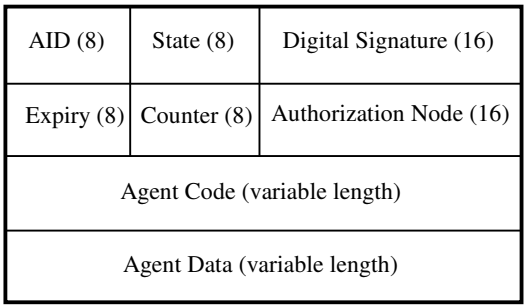
The proxy signer is responsible for signing the mobile agent as well the data. This is used to assure the authentication service of the system as a whole. The proxy signer uses a sequence of processes to perform the signing process more secure.

4.4. Malicious Identification Police

The Malicious Identification Police contains an inbuilt Attack Identifier which helps to detect any sort of attack that has been made over the mobile agent during the time of transportation from one host to another. Moreover, it uses various policies to check whether a mobile agent is authorized to access a resource or not. The policy files are maintained in a database. This also decides whether a mobile agent needs to be transmitted from the system. It encrypts and transmits the mobile agent along with the data.

5. Agent Format

Figure 2: Secure Mobile Agent Format



The figure 2 shows the format of the mobile agent that is being used in this protocol. The mobile agent format contains the following fields:

- Agent Identifier (AID)
- State
- Digital Signature
- Expiry
- Counter
- Authorization Node
- Agent code
- Data

5.1. Agent Identifier

The agent identifier is the one which uniquely distinguishes the mobile agent. It is an 8 bit field which is being occupied by a unique number with respected to the system.

5.2. State

The state field represents the state of the agent. The agent may be active or passive or may get dispatched or retracted. This field could be directly accessed by the agent platform. It is also an 8 bit field.

5.3. Digital Signature

The digital signature is appended to the mobile agent by means of the proxy signer. The proxy signer may use any means of signing. This part ensures the authentication services. The size of this field is 16 bits.

5.4. Expiry Timer

The expiry time is set by the trip marker which sets a time stamp which contains the maximum time limit for which the mobile agent must be alive. It is an 8 bit field.

5.5. Counter

The counter contains the number of itineraries the mobile agent could make to its maximum. Once this filed becomes zero, the mobile agent reaches its destination or gets destroyed. The counter is also an 8 bit field.

5.6. Authorization Node

The authorization node is the creation of the Malicious Identification Police. The node contains details of the privileges of the mobile agent which indicates to which resources the mobile agent could have access. This is a 16 bit field.

5.7. Agent Code

Agent code is the actual code that the mobile agent is made of. It is the source code which is programmed to move from one host to another. The size of this field is variable and depends on the design of the system.

5.8. Agent Data

The data field is also a variable one which would contain the data the agent needs to carry inorder to perform a task.

6. Proxy Signing

These are various methods to perform digital signing over the data. One such technique is the proxy signing technique which involves a sequence of steps.

Consider the original signer id I_A and the proxy signers or the platforms involved in signing $I_{p1}, I_{p2}, ..., I_{pn}$, a combiner C, secure one way hash function $H(.)$ and the message warrant m_w which is used to record I_A. Two random prime numbers p_0, q_0 are chosen by I_A.

$$p_0 = 2p_0' + 1$$

$$q_0 = 2q_0' + 1$$

where p_0', q_0' are prime numbers.

Let, $N_0 = p_0.q_0$ and $M_0 = p_0'.q_0'$

where M_0 is of the order of Q_{N0}. Q_N is the subgroup of squares in Z_N^* which is in order

$$M = [(p-1)(q-1)]/4$$

We use the RSA algorithm and so the agent with identity I_A computes the RSA exponents e_0 and d_0 where,

$$e_0.d_0 \equiv 1 \bmod M_0$$

Now, the private key is (d_0, M_0) and the public key is (N_0, e_0). In general,

$$N_i = p_i q_i$$

$$\phi N_i = (p_i - 1).(q_1 - 1)$$

$$e_i d_i = 1 \bmod \phi(N_1)$$

and d_i becomes the private key, (N_i, e_i) becomes the public key. Consider the threshold proxy key of I_A as

$$D \equiv d_0.H(m_W) \bmod M_0$$

I_A shares the signing key D among n proxy signers.

I_A sets $a_{A0} = D$ and chooses a_{Ai} at random from

$\{0,1,.....,M_0 - 1\}$ for $1 \le i \le t$

which defines $t-1$ degree polynomials.

$$f(x) = a_{A0} + a_{A1}x + ... + a_{At-1}x^{t-1} \bmod M_0$$

The partial proxy signature key $K_i = f(i) \bmod N_0$ for each proxy signer I_{pi} and is computed by I_{A0}.

The validation is performed by computing the proof.

I_{A0} chooses randomly $N \in Q_{N0}$ for $1 \le i \le n$

$v_i = v^{ki} \in Q_{N0}$

I_{A0} makes $(v_1, v_2 \ldots\ldots\ldots\ldots, v_t)$ public. Coming to the part of proxy signature generation

$x = H(m, m_w)$ and $\Delta = n!$

Each proxy signer uses its partial proxy signing key K_i to sign the partial signature.

$x_i = x^{2\Delta, k_i} \in Q_{N0}$

I_{Ai} computes the proxy signature $(\Delta\sigma_i, \sigma_i)$

$\Delta\sigma_i = [x_i / N_i], \sigma_i = x_i^{d_i} \bmod N_i$

The proof of correctness could be done as follows

$$\log_{x=x^{4\Delta}} x_i^2 = \log_{v.v_i} v_i$$

chooses $r \in \{0,1,\ldots\ldots\ldots 2^{|N_0|+2L_1} - 1\}$ where L_1 is the secondary security parameter. The function then computes

$$v' = v^r$$

$$x' = \tilde{x}^r$$

$$c = H'(v, \tilde{x}, v_i, x_i^2, v, x'), z = k_i C + r$$

The proof of correctness is given as (z, c) and the final partial proxy signature is given as $(i, \Delta\sigma_i, \sigma_i, x)$.

While considering the final part of the signature, we move on to combining. C is the proxy signature combines which is a signer who do not own any secret parameters.as soon as the combines receives $(i, \Delta\sigma_i, \sigma_i, c, z)$ if recovers the partial signature by

$x_i = (\Delta\sigma_i, N_i) + (\sigma_i^e \bmod N_i)$

To calculate the proof of correctness, the following is done

$$C = H'(v, \tilde{x}, v_i, x_i^2, v^z v_i^{-c}, \tilde{x}^z x_i^{-2c})$$

Suppose, all the proxy signatures are correct and valid, then the corresponding signer set is

$S = \{i_1, i_2, \ldots\ldots\ldots, i_t\} C \{1,2,\ldots\ldots\ldots n\}$

and the signature share is given as

$$\lambda_{ij}^s = \frac{\Delta\pi_{j' \in S \setminus \{j\}} (i - j')}{\Delta\pi_{j \in S \setminus \{j\}} (j - j')} \in Z$$

Proxy signature of the message which is confirmed to m_w is given as

$$w = x_{i1}^{2\lambda_0^3, i_1} \ldots\ldots\ldots\ldots\ldots x_{it}^{2\lambda_0^3, i_t} \bmod N_0$$

Using the standard Lagrangian formula

$$\Delta.f(i) = \sum_{j \in s} \lambda_{ij}^3 . f(j) \bmod M_0$$

since $x_{ij}^2 = x^{4\Delta k_{ij}}$

we have $w^{e_0} = x^{4\Delta^2 . H(m_w)} \bmod N_0$

since $\gcd(4\Delta^2, e_0) = 1$

$$y^{e_0} = x^{H(m_w)}$$

(i.e) $y^{e0} = H(m, m_w)^{H(m_w)}$

using a standard algorithm

$$y = w^a x^b$$

where a and b are integers such that $4\Delta^2 a + e_0 b = 1$

which is obtained from the extended Euclidean algorithm on $4\Delta^2$ and e_0. The proxy signing involves the steps above for the digital signing process to be successful.

7. Process

Initially the mobile agent is generated by the agent platform and the data it needs to carry is also allocated by the agent platform. The mobile agent is subjected to encapsulation when it gets off a system and is decapsulated when it enters the system. The encapsulation and decapsulation are defined below. host_agent represents the agent originating from the host and remote_agent represents the agent originating from a remote host.

7.1. Encapsulation

READ host_agent
APPEND expiry_time AND loop_counter
APPEND digital_signature
APPEND authorization_node
DECIDE transmit (host_data)
ENCRYPT AND TRANSMIT (host_data)

7.2. Decapsulation

READ remote_agent
DECRYPT remote_agent
VERIFY authorization_node
SCAN remote_agent
IF malicious
DESTROY remote_agent
ELSE
VERIFY digital_signature
IF valid
VERIFY expiry_timer AND loop_counter
DECREMENT loop_counter
ELSE
DESTROY (remote_agent)
ENDIF
ENDIF

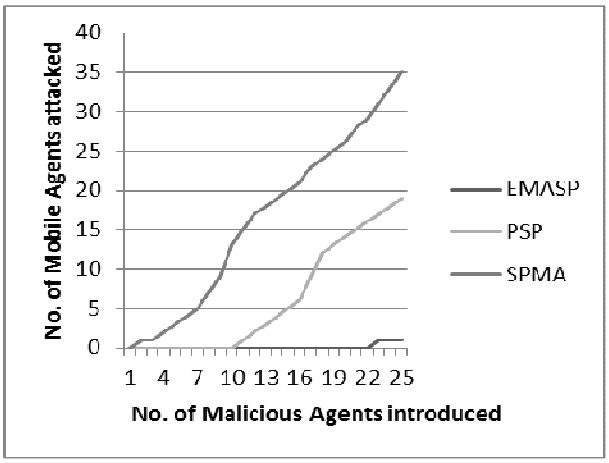
Once the mobile agent along with the data is initialized, the trip marker appends the expiry time and counter to the entire packet. Along with that, the proxy signer appends the digital signature over the mobile agent, at the time of creation contains an identity and a state. When the mobile agent along with the trip marking data and digital signature is about to leave the system, the Malicious Identification Police appends the authorization details inorder to provide privileges to the mobile agent to access the various resources in the foreign platform. Once all these processes are complete, the mobile agent is allowed to be transmitted through the network.

Similarly, when a mobile agent enters the system, the Attack Identifier verifies it whether the mobile agent have been subjected to any sort of attack. When the mobile agent is not attacked by any

malicious objects, it is allowed to access the resources inside the agent platform as per the details inside the authorization node. Further the digital signature is being checked to verify whether the mobile agent is an authenticated one. The trip marker checks the expiry times for the time stamp value and the counter values. The counter value is decremented for each itinerary for the mobile agent. Each time the mobile agent wishes to access a resource the authorization node is checked to verify whether the mobile agent has the privilege to access the particular.

8. Experimental Results

Figure 3: Malicious Agent vs Mobile Agent Failure



Two types of mobile agent systems are designed using Aglets 2.0.1 in a Network containing 20 systems with Intel Dual Core processor functioning in Windows XP operating system. The systems are separated into two groups each containing 10 systems. The mobile agents are made to transfer from one system to another to perform some operations. The mobile agents carry data with them. Malicious agents which would attack the mobile agents in various methods are introduced inside the network. In Figure 3 EMASP refers to the Enhanced Mobile Agent Security Protocol, PSP refers to the Proxy Signature Protocol and SPMA refers to the Self Protected Mobile Agents. A comparison between the three schemes is shown in Figure 3.

The system is made to function using the schemes shown above. With the introduction of different malicious agents, it is found that the Enhanced Mobile Agent Security Protocol is immune to most types of attacks compared to the Proxy Signature Protocol and the Self Protected Mobile Agent Scheme.

9. Analysis

9.1. Authentication

The protocol is designed such that it doesn't compromise with the security services. The digital signature and the Agent Identifier contribute to the authentication service. The Agent Identifier gives recognition to the mobile agent and the digital signature confirms the origin of the mobile agent there by contributing to the authentication service.

9.2. Access Control

Access control is another security service which need to be concentrated in any security model. Any system designed must provide the access control service. The authorization node present in our

protocol is the main tool to provide this service. It contains all the privilege definition which controls the access towards a resource.

9.3. Confidentiality

The security protocol provides an encryption scheme by which the data is encrypted. Encryption scheme protects the data from being viewed by other users which ensures confidentiality of the data.

9.4. Integrity

The protocol also provides a sophisticated integrity measure by not allowing any other malicious agents to access to the data by means of the encryption technique which it uses before transmittance of the data.

9.5. Non-repudiation

The protocol provides the non-repudiation service by means of the digital signature. The digital signature ensures the origin of the mobile agent, thereby avoids any sort of attack which poses repudiation towards the agent or the data.

9.6 .Masquerading

The protocol is efficiently designed to overcome the masquerading attack. Each agent is provided with a unique agent identifier which distinguishes itself from other mobile agents in the system. Therefore no other mobile agent in the system could have the same identifier, thereby making the system immune to Masquerading.

9.7. Replay Attacks

The protocol is designed especially in concentration with replay attacks. The tripmarker used in the system facilitates the protocol to encounter replay attacks. The value in the counter and the expiry time field decides the further itineration of the mobile agent. In case if it is found to be invalid, then the mobile agent is destroyed or marked to be malicious.

10. Conclusion and Future Work

In this work, we have developed a protocol which is immune to most types of known attacks. The protocol uses the techniques of trip marking, digital signing and Malicious Identification Police to overcome the most types of attacks. From the experimental point of view, it has been found that the mobile agents in this system are more immune to attacks while compared to the systems which are implemented in an ordinary environment.

In future, this work could be extended by optimizing the processes involved in the security mechanism thereby reducing the time to encapsulate and decapsulate the mobile agent and data. Also, new techniques could be included inside the protocol to improve the efficiency of the protocol.

References

[1] Venkatesan et al., 2010. “Advanced Mobile Agent Security Models for Code integrity and Malicious Availability Check”, *Journal of Network Computer Application*.

[2] Lofti Benachenhou, Samuel Pierre, 2006. “Protection of a Mobile Agent with a Reference Clone”. *Computer Communications*, pp. 268–278.

[3] Xuan Hong, 2009. “Efficient threshold proxy signature protocol for mobile agents”. *Information Sciences*, pp. 4243- 4248.

[4] J.Ametller, S.Robles, J.A.Ortega- Ruiz, 2004 “Self-protected Mobile Agents”, *Proceedings of AAMAS ‘04*.

[5] Lu Ma, Jeffrey J.P. Tsai, 2006. *Security Modeling and Analysis of Mobile Agent Systems*, Imperial College Press.

[6] Oshima Mitsuru, Danny Lange, 2002. Programming and Deploying Java Mobile Agents with Aglets, Addison-Wesley.

[7] Peter Braun, Wilhelm Rossak, 2005. Mobile Agents: Basic Concepts, Mobility Models and the Tracy Toolkit. Morgan Kaufmann Publishers.

[8] http://www.trl.ibm.com/aglets