International Journal of Latest Engineering and Management Research (IJLEMR)
ISSN: 2455-4847
www.ijlemr.com || Volume 02 - Issue 05 || May 2017 || PP. 12-17

Research on Security Problem and Countermeasure of Mobile Agent System

Lin DeShu

（College of Computer Science, Yangtze University, Jingzhou Hubei, 434023, China）

Abstract: In recent years, the rapid development of the Internet technology has greatly changed the way people deal with information. In the past, mainly used in the field of scientific research and send and receive e-mail Intemet, has been fancy to many businesses, has become an important platform for e-commerce, thus promoting the mobile agent technology for further research and application. The most important feature of a mobile agent is that it is mobile and can be moved autonomously over a network from one host to another. This flexibility makes mobile agent technology has many advantages, but also faces security problems. Mobile Agent technology security threats mainly from malicious agents, may also come from a malicious host. In this paper, the author puts forward a series of countermeasures to solve the security problem in the two aspects of mobile agent technology.

Key words: Mobile agent; malicious host; security threat

Agent mobility will bring a lot of uncertain factors, in order to make MA widely accepted, successfully applied to business (such as e-commerce), and we must solve the MA's security issues. MA's security problem is the bottleneck of successful application of MA, which is the most important and complicated problem in mobile agent system.

1. Mobile Agent features bring security issues

Mobile Agent is a special agent with mobility. The behavior of the mobile agent includes Agent movement, task execution and communication. Because the mobile agent can autonomously move from one host to another on the network, it has many new and flexible features compared to the traditional software architecture based on the Client / Server model, and has many advantages [1]. It is these new features that make the mobile agent system also have a lot of new security issues. Here we discuss the security issues that arise from the characteristics of mobile agents.

1.1Agent implementation

Often, Agent needs to be implemented in some environments, such as hosts, agents, and so on. This gives us a question, in the end where the implementation of access controls operations. As the Agent needs to enter the implementation of the host, Agent need to prevent malicious host attacks, the same, the host also need to prevent malicious Agent attacks. This makes the security problem of the Agent system a very complicated problem.

1.2 Environment

The meaning of the term "environment" depends on the application and is of broad meaning. For example: it can be the implementation of the Agent's Internet or host. If an Agent's environment is limited by the host that executes the agent, then special security measures are not needed.

1.3Autonomy

The combination of autonomy and other features of Agent can lead to serious security problems [2].

Autonomy is not a characteristic of Agent, and many existing systems also have this attribute. For example: network worms have autonomy. It can let the worm in the case of non-human interaction and efficient transmission. We can learn from the teachings of network worms to solve the problems caused by Agent autonomy.

1.4 Communication

From a security perspective, social behavior in many attributes is an interesting attribute [3]. The social attribute of Agent means that Agent can communicate with other agents and people. As Agent needs to be protected from communication with the execution environment, Agent needs to be protected when communicating with other agents and people. The attributes that need to be protected during communication are: Confidentiality: Ensure that the information used for communication can not be accessed by an unauthorized entity. Data integrity: Ensure that the information used for communication can not be operated by an unauthorized entity without being detected. Source Proof: Ensure that the communication information is from the host that made the communication request. Effectiveness: Ensure that the communication information arrives at its receiving place in a timely manner. In general, security issues are related to cost issues [4]. The above mentioned solutions to protect these attributes need to take up additional computing resources and communication resources. A number of security protocols and security mechanisms have been proposed for security issues with communications. These protocols and mechanisms can meet the requirements for protecting the authenticity, confidentiality and data integrity of communications.

1.5 Reasonableness, accuracy and goodwill

These properties seem to be safe, but to the next level, these attributes are too abstract and can not consider their specific security issues. From a security perspective, these attributes mean that the agent behaves well and does not perform malicious operations. If we want to achieve this goal, it will cause a lot of system redundancy, these redundancy will make the system becomes useless. Of course, assuming that the Agent can run honestly in any environment, such a system is valuable. However, if there is no strict control and the only authorization, it is impossible for the mobile agent system to ensure that the Agent can run honestly in any environment. Now, people have put forward some restrictions on the implementation of malicious agents Agent method. These methods ensure that only information from a reliable source can be executed and that Agent is responsible for its actions. Mobile Agent these features, making the mobile agent system in addition to the traditional security issues, there are some new security threats. Therefore, the mobile agent system to solve the traditional security issues, based on the need to study and design new methods to resist new security threats.

2. Mobile Agent system security threats

In recent years, the application of mobile agent system based on the vigorous development, therefore, mobile agent system security issues are increasingly getting people's attention. According to the characteristics of mobile agent system, its security threats can be divided into four cases:

2.1 malicious agent attacks Agent platform

Moving the Age claw system requires an Agent platform to receive and execute Agent. An external non-local Agent has two main ways to attack: one is to visit the Agent platform in the illegal access to information, the second is a devastating way to access the legitimate access to information. The first attack is due to the lack of appropriate access control mechanism or a relatively weak authentication strategy. Due to the lack of strong access control mechanism and authentication strategy, some malicious agents can disguise themselves as trusted agents into the Age gate t platform. If this happens, the information residing on the Agent platform is compromised or tampered with. In addition to confidential data, these leaked or tampered

information may also include the platform's instruction code. Depending on the access level, some Agent VII can completely shut down or terminate the operation of the Agent platform. If the constraint mechanism of the resource is not well established, even if no illegal access rights are obtained, an agent can deny the Agent platform to service other agents by consuming computing resources. In addition, Agent can publish meaningless service requests to interfere with the operation of the Agent platform.

2.2 Malicious agent platform attack agent

An Agent platform can easily isolate and capture an Agent and attack the Agent by extracting its information, destroying or modifying its code and state, rejecting its service request, simply reinitializing the Agent, or terminating its operation to attack Agent [5] The A simple example is to extract the electronic money directly from the agent. An Agent is very susceptible to the Agent platform. The Agent platform can destroy an agent by incorrectly responding to a request, a service request, an external communication, or a delay agent until its task is no longer valid. Even more, the Agent platform can subtlety modify Agent by fully analyzing the Agent and reverse engineering the Agent design. Agent platform on the Agent to modify and destroy is a very hidden and terrible attack. Because it can fundamentally change the behavior of agents (e.g., turning a trusted agent into a malicious agent) and influencing the accuracy of the calculation (e.g., changing the collected information to produce incorrect results).

2.3 malicious agents attack other Agent

An agent can attack other agents by some common methods. These attacks include forgery of transactions, eavesdropping conversations or interference with other Agent activities. For example, a malicious agent can incorrectly respond to a request received from a target agent or deny a legitimate transaction. But also can be used as a media to collect information about the target agent or use the platform services to eavesdrop on the platform of the message. If the control mechanism of the Agent platform is weak or there is no control mechanism at all, the Agent can acquire or modify the data or code of other agents. You can also interfere with the operation of the agent by activating the agent's common method (for example, trying to get the buffer overflow, reset the initial state, etc.). Even if the Agent platform has a very reliable control mechanism, Agent can also attempt to send messages to other agents to influence the communication capability of Agent.

2.4 other entities attack Agent system

Even if the local Agent and Agent platforms are assumed to be secure, other entities inside or outside the Agent framework will attempt to destroy the Agent system. Common methods have to attack the internal communication between agents and agents through camouflage or interception. For example, in an agent-to-agent or platform-to-platform protocol layer, an entity may obtain information by tapping a message from the target agent or Agent platform. A malicious entity may intercept agents from the middle to modify, replace their contents, or simply resend the conversation to attempt to break the synchronization or integrity of the Agent framework. In addition, the use of the available network interface to deny the service is also a possible form of attack.

3. Mobile agent communication security measures

Mobile agent communication security measures can be solved using encryption algorithms and digital signatures. In the TCP / IP protocol based on the communication network can also use SSL (Secure Socket Layer) protocol to ensure the safe transmission of data network.

3.1 Mobile agent security measures using AES encryption

In the mobile agent system encryption algorithm can be used AES (Advanced Encryption Standard), this algorithm is also known as Rijndael encryption method. AES is the National Institute of Standards and

Technology NIST aims to replace the DES and proposed a new encryption standard. AES encryption algorithm using symmetric block cipher system, the key length support for 128,192,256, packet length 128, the algorithm should be easy to achieve a variety of hardware and software.

Here we can accord different levels of information security, the use of different lengths of the key to achieve, as shown in Table 1. The classification here not only takes into account the security requirements of the data, but also the hardware cost of the network and the implementation. In the actual operation, we use the 128-bit key length for data communication in the wireless network.

Table 1 encryption level classification table

Data on security requirements	Applications	Key length
Higher	Personal information, bank data, business confidential information and so on	256
medium	Contact information, telephone number, address	192
general	Wireless network information, non-private information	128
No request	For example: public announcement information	not use encryption

3.2 through the AES encryption algorithm to achieve the process

The AES block cipher accepts a 128-bit plaintext and generates a 128-bit cipher under the control of a 128,192,256 key. The specific operation is a set of steps called rounds, where the number of turns may be 9, 11, 13 (depending on the key length). A AES operation has four steps: 1.SubBytes 2.ShiftRows 3.MixColumns 4.AddRoundKey [6-7].

(1) SubBytes function

The function SubBytes step is the only step in the AES algorithm that uses a nonlinear blend, and each of the 16 bytes is mapped in parallel as a new byte. The SubBytes function is executed as shown in Figure 1.

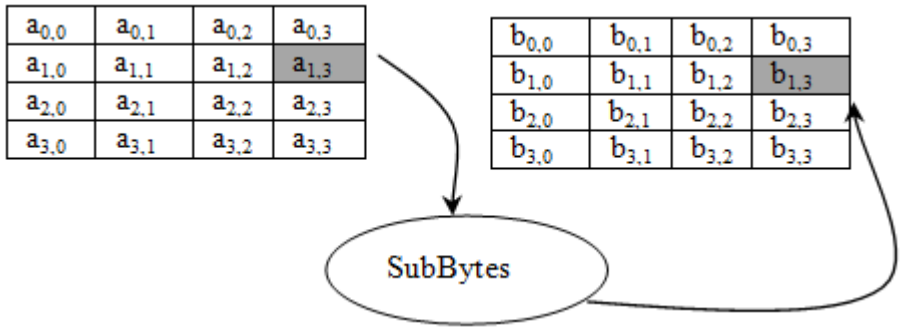

Figure 1 SubBytes function execution diagram

(2) ShiftRows function

The function of the ShiftRows function is to move 0, 1, 2, and 3 bits to each of the lines in the state data. This state transformation is easier to implement. The ShiftRows function is executed as shown in Figure 2, where ROLi represents the right shift i bit.

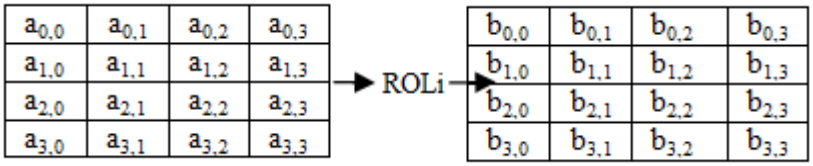

Figure 2 ShiftRows function execution diagram

(3) MixColumns function

The main function of the MixColumns function is to perform a column transformation on the encryption process. The operation is to multiply a matrix by a matrix of the matrix of the state matrix to obtain a new matrix. The repeated operation yields a new state matrix data. The MixColumns function is executed as shown in Figure 3.

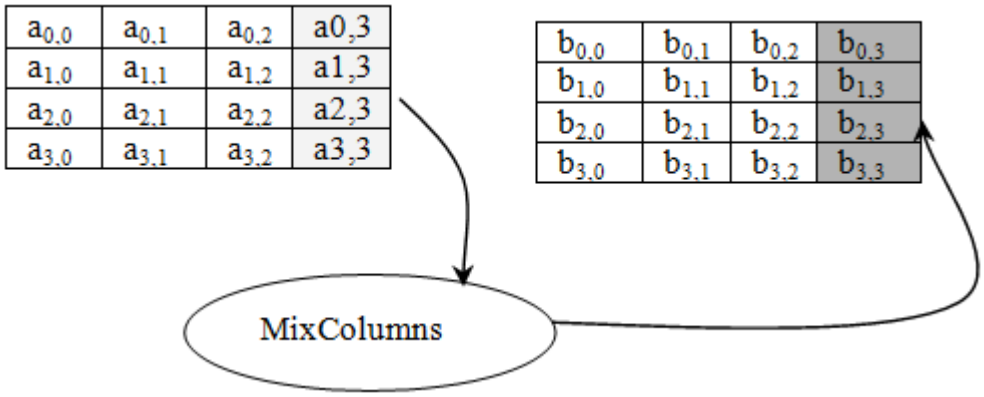

Figure 3 MixColumns function execution diagram

(4) AddRoundKey function

The function of the AddRoundKey function is to get the new state data from the key and the state data, as shown in Figure 4.

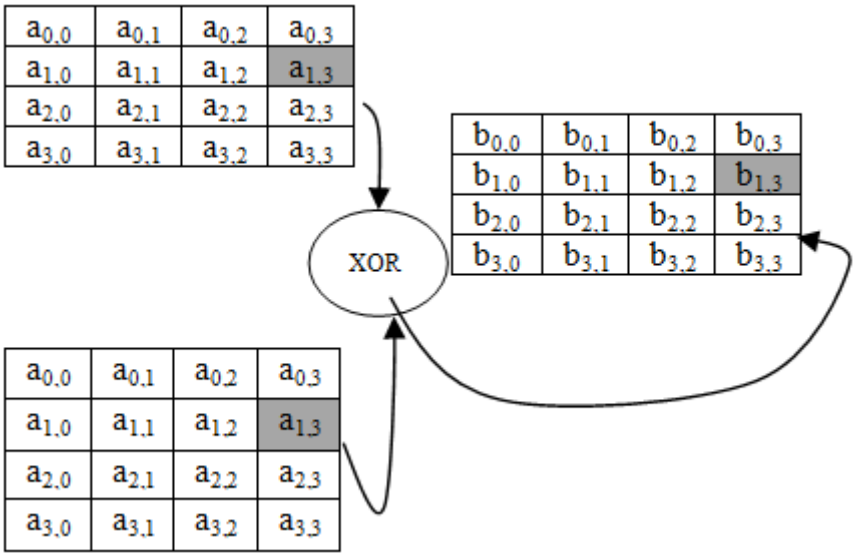

Figure 4 AddRoundKey function execution diagram

4. concluding remarks

With the continuous development of mobile Agetn technology, mobile agent system security issues more and more people's attention. Because its security problems have seriously hindered the application of mobile agent technology in practice. This paper focuses on the security threats that exist in the mobile agent system and the security countermeasures for these security threats.

References

[1]. Mobile Agents for Distributed and Heterogeneous Information Retrieval [J]. Subrata Das, Kurt Shuster, Curt Wu, Igor Levit. Information Retrieval. 2005 (3)

[2]. Performance Monitoring of Remote Websites Using Mobile Agents [J]. Wen-Kui Chang, Min-Hsiang Chuang. Software Quality Journal. 2004 (2)

[3]. A Security Architecture for Mobile Agent Based Applications [J]. V. Varadharajan, D. Foster. World Wide Web. 2003 (1)

[4]. A kind of security fault-tolerant mechanism of mobile agent system [J]. LIU Tian-tian.Computer Engineering. 2005 (18)

[5]. malicious host on the Mobile Agent security solutions [J]. Wang Dayong, Mei Zhihong, Jin Weidong. Journal of Southwest Jiaotong University. 2005 (04)

[6]. A mechanism for mobile Agent data protection [J]. TAN Xiang, GU Yuqing, BAO Chongming. Journal of Software 2005 (03)

[7]. Mobile Agent Security Detection Protocol Research [J] .Lihao Jun, Qiu Feiyue, Wang Liping. Computer Engineering and Applications. 2005 (08)