International Journal of Engineering Research and Development
e-ISSN: 2278-067X, **p**-ISSN: 2278-800X, www.ijerd.com
Volume 7, Issue 4 (May 2013), PP. 85-89

Review of Security Issues for Mobile Agent Technology

Rajesh Kumar[1], Yashpal Singh[2], S Niranjan[3]
[1]Research Scholar, Department of Electronics & Communication Engineering, Mewar University, Rajasthan.
[2]Research Scholar, Department of Computer Science & Engineering, Mewar University, Rajasthan.
[3]Professor, Department of Computer Science & Information Technology , PDM College of Technology & Management , Bahadurgarh, Jhajjar, Haryana.

Abstract:- In the recent time the computer systems have evolved from monolithic computing device to much complex client-server environment. Mobile-agent paradigm is one such technology. It has numerous application where it can be beneficial, to name a few areas where the mobile-agents have potential deployment are database search, distributed systems and e-commerce. This technology has given a new direction to networking. Because of mobility of mobile agent, the security problems becomes more complicated and have become a bottleneck for development and maintenance of mobile agent technology especially in security sensitive applications such as e-commerce, military application scientific applications etc. This paper discusses about the mobile-agent, architecture of mobile agent, what are the various security issues that should be resolve for better performance, that can affect the transmission and reception of information. In last, in this paper we discuss the counter measures for above mentioned security issues for better performance of the mobile agent technology.
Keywords:- Authentication, Cryptography, access control, trust management, privacy, and signature schemes, DOS (Denial of Service), Intrusion detection, FIPA (Foundation for Intelligent and Physical Agent).

I. INTRODUCTION

A mobile agent is a software program with mobility which can be sent out from a computer in to a network and roam among the computer nodes in the network. It can be executed on those computers to finish its task on behalf of its owner. The transferring of a mobile agent state facilities it in working automatically to travel between one or more remote computer [3]. The key Characteristics of the mobile agent paradigm are that any host in the network is allowed a high degree of flexibility to possess any mixture of know-how, resources and processors. Its processing capabilities can be combined with local resources. Knowhow (in the mobile agent) is available throughout the network. Since, the mobile agent has many salient merits, so it has attracted tremendous attention in last few years and become a promising direction in distributed computing and processing as well as high performance network area. In mobile agents, the mobile code generated by one party transfers and execute in an environment controlled by another party so several security issues arises in various mobile agent computing [4].

II. AGENT

Most obvious definition of an Agent in real world is something who acts on the behalf of somebody. They are given some goals and they try to achieve these goals according to their intelligence [1]. In order to achieve these goals they communicate and interact with other agents, they exchange information and take back the results to the user. The agents may be stationary or mobile able to move from one host to another [2]. There are various agents these are as follows Software Agents, Autonomous Agents, Intelligent Agents, Adaptive Agents, Mobile Agents, Coordinate Agents, broker agent, manager agent, facilitator agent etc

Mobile Agent

The mobile agent can be thought of as a software program which travels from one platform to another in order to get its work done, during this process it carries its state and data with itself and resume its execution from the state it had left on the previous platform [5]. The reason for using mobility is the improved performance which can be achieved by moving the agent closer to the new host, where it can use services locally.

Architecture Of Mobile Agent

The architecture gives the structure of the system which consists of some components, their individual functionalities and their inter relationship with each other. The basic architecture of the mobile agent can be thought of as a client sends out an agent who travels the network visiting servers in order to perform some required action.

The architecture consists of [5]:

• **Agent Manager:** The agent manger has few responsibilities as it [6]

- ❖ Sends agents to and receives agents from remote hosts.
- ❖ Prepares agents for transport by serializing the agent.
- ❖ Reconstructs received agents and creates the agents execution context.

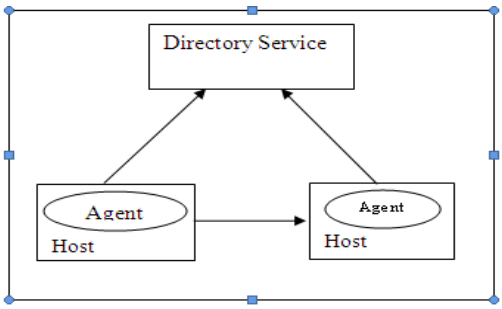

Figure 1

• **Security Manager:** The responsibilities of security manager are:

- ❖ Authenticates agents before allowing execution.
- ❖ Automatically invoked when the agents tries to use any system resource or tries for any unauthorized activity.
- ❖ Protects the host and agent from unauthorized access.

• **Inter-agent Communication:** It allows the agents to communicate through message passing mechanism. Till now all those agent system which follow FIPA (Foundation for Intelligent and Physical Agent) standards [3] are able to exchange messages as they follow a standard format for sending and receiving messages. Inter communication is still an issue among heterogeneous agent system.

• **Directory Manager:** Lists names and addresses of services and agents. Fig.1 shows the agent first migrates to remote container and registers itself to the Directory Services.

Language: The architecture of a mobile agent system describes the flow of information among the various components of the system. The language used for the efficient transfer of data and provides the developer with the tools to efficiently implements the system. Most current agent systems are implemented on top of the Java Virtual Machine (JVM), which provides object serialization and basic mechanism to implement weak mobility.

III. SECURITY ISSUES

Internet has become the main revolutionary medium for expanding business and as Internet is expanding, more and more companies in corporate world want to take full advantage of it[7]. The major security threats are given as follows:

1) Authentication: It means that correct identity is known to communicating partner.
Authentication of user: the user needs to authenticate himself to a given server. Public-key encryption or a password can be used for this purpose.

Authentication of host: before a server starts to communicate with another server or client, it needs to know with whom it is communicating.

Authentication of code: before executing an incoming agent, the host needs to know who created the agent. Digital signatures are typically used for this purpose

Authentication of agent: before executing an incoming agent, the server needs to know who is responsible for this agent or who its owner is.

The agents can decide if external security is required or not. Agent handles host security using public key cryptography for authentication and secure execution environment for authorization. It has three components in its security architecture (Fig 2) encryption Subsystem a language-dependent enforcement module, and a language-independent policy module [1].When an incoming agent arrives, the server of the receiving machine verifies the agent's digital signature, and then either accepts or rejects the agent after checking against the server's current access list. If the server accepts the agent, it records the identity of the agent's owner, starts up an execution environment for the agent, and resumes agent execution [1].
When an agent requests access to a resource, the enforcement module forwards the request to the appropriate resource manager. The resource manager, which is just a stationary agent, implements a security policy that determines whether the access request should be approved or denied. The security module then enforces the decision. This approach provides a clean separation between security policy and mechanism, with the same resource managers making security decisions for all agents, regardless of their implementation language[10].

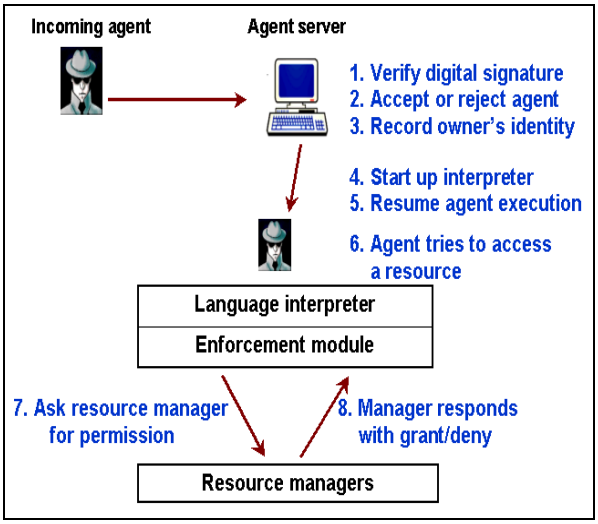

Fig. 2 the components of the Mobile Agents security architecture.

Digital signature By using a public-key cryptography entity, message can be sent securely, but the question remains: how can the receiving machine make sure that the agent is really from the sending machine, and not an impersonator? Digital signature can solve this problem. It serves as a means of confirming the authenticity of an agent. Typically the code signer is either the creator of the agent, or the user of the agent. Digital signatures benefit greatly from the availability of a public key Infrastructure.
For example, if machine A wants to send an agent to machine B, the state image is signed with A's private key, and encrypted with B's public key, and sent to machine B, when the agent arrives at B, B uses its private key to decrypt the state image, and uses A's public key to decrypt the result. If B can successfully finish the two steps then B can ensure that the agent is from A, because only A can use A's private key to sign a message. Here, we assume B knows the correct public key of A.

2) Confidentiality: Ensures certain information is never disclosed to unauthorized entities. An agent may carry confidential information that should be readable only by intended server or agent. Such information should be kept secret form other servers and agents.

3) Eavesdropping: Eavesdropping threat involves the monitoring and interception of the secret information which is being communicated between authenticated hosts. In the case of malicious host problem, where an agent is executing on the remote host and the host has every chance to monitor each instruction executed by the agent. This becomes more serious problem in case of malicious host. If the host gets access to agent code, it can expose proprietary algorithm, private information, negotiation strategies or some secret information of the agent.

4) Alteration: Alteration attack is extended attack of eavesdropping threat that we have mentioned above. If the agent is executing on malicious host it is exposing its code and data. A malicious host can change the data or the behavior of the agent. This type of Security of Mobile Agents attack can be detected by having the agent signed by original author. If an agent is moving to several hosts on its literary and one or more hosts turned out to be malicious, then this kind of attack is nearly impossible to track down in the end as the agent has undergone numerous changes of its data or code. Alteration includes modification of data, state and code. Modification

can't be prevented but it should be possible for another agent or platform to detect unauthorized modifications. It is typically prevented by using the digital signatures but they are use only for code and static data. The original author can digitally signed agent's code and read only data. Signature can't be used to detect malicious modifications to dynamic data modified at different host .

5) Masquerade: An agent platform can masquerade itself as another platform, to make itself appear to be an authenticated one, to a mobile agent. It may attract the agent to come and make it execute so that malicious host can extract sensitive information. These kinds of malicious platforms can harm both the agents and the platform whose identity they have assumed. These types of masquerading platform can give rise to the other attacks like eavesdropping and alteration.

6) Denial of Service: This kind of attack occurs when an agent comes to a host to produce some results by utilizing the resources of the host. Now a malicious host can ignore the agent request, may introduce delays or it may not allow the agent to execute at all. This kind of attack may give rise to deadlock condition or unnecessary long delays when multiple agents are dependent on each other's result. Among all the security services, authentication is probably the most complex and important issue in MANETs since it is the bootstrap of the whole security system. Without knowing exactly who you are talking with, it is worthless to protect your data from being read or altered.

7**) Availability**: Availability means the normal service provision in face of all kinds of attacks.

8) Non-repudiation: Ensures that the origin of a message cannot deny having sent the message [7].

9) Auditing: Auditing service records security-related activities of an agent for later inspection.

IV. COUNTER MEASURES

We will first try to avoid the problem, if not, and then we will see how to handle them from those proposed solutions.

5.1 Hardware-based Security: Hardware-based security is the most effective approach but it is not feasible enough. This approach requires installing a secure hardware on each node where a mobile agent can migrate to and execute. This is again meant for the small network where such procedures are possible.

5.2 Encryption-based: Another approach is to use mobile cryptography techniques. Symmetric cryptography is well suited for those mobile agents which need to send the results back to its owner. It gives security to eavesdropping and alteration attacks performed to the agents on remote host. Here similar techniques authorization and authentication are also mentioned by M.Farmer, J. Guttman, and V. Swarup [8].

5.3 Computed with encrypted functions: Sander and Tschudin have proposed a method whereby an agent platform can execute a program embodying an enciphered function without being able to discern the original function [9]. It says that a function can be encrypted in such a way that they can still be implemented as programs. The resulting program can be understandable by processor but processor will still not understand the program's function.

CONCLUSION

In this paper we have discussed about the mobile-agents, its security issues. Mobile agent system is a very promising paradigm; it has shown its presence in many applications like distributed networking, e-commerce applications. There are numerous advantages of using the mobile agent paradigm rather than conventional paradigm such as client-server based technologies. In one way it provides the abstraction to networking. The benefits of mobile-agent technology cannot be exploited fully until all the security issues are properly addressed. It still does not address the problem of denial of service. Also obfuscation technique affects the performance of the code as it may change the whole layout of the program structure.

REFERENCES

[1]. Object Management Group, NEEDAM MA, Agent Technology Green Paper 1 Sept 2010, PP. 8-11
[2]. Hyacinth S. Nwana, "Software Agents: An Overview", Intelligent systems Research, Advanced Applications & Technology Department, Ipswich, Suffolk U.K. Cambridge University Press 2011.
[3]. The Foundation for Intelligent Physical Agents (FIPA), http://www.fipa.org/.
[4]. James Odell, "Objects and Agents: How Do They Differ?". 2010

[5]. Danny B.Lange and Mitsuru Oshima, "Programming and Developing Java Mobile Agents with Aglets". (Addison Wesley publication). Reprint 2012
[6]. Luca Ferrari, "The Aglets 2.0.2 User's Manual", October 2011.
[7]. General Magic Inc. Odyssey http://www.genmagic.com/agents.
[8]. William M.Farmer, Joshua D. Guttman, and Vipin Swarup, "Security for Mobile Agents: Authentication and State Appraisal", pp. 5-11, European Symposium on Research in Computer Security (ESORICS).
[9]. T. Sander and C. F. Tschudin, "Protecting Mobile Agents Against Malicious Hosts". G. Vigna, editor, Mobile Agents and Security, volume 1419 of LNCS, pp. 44–60. Springer-Verlag, June 1998.