IJCSC International Journal of Computer Science and Communication Vol. 3, No. 1, January-June 2012, pp. 207-210

NOVEL APPROACH FOR SECURING MOBILE AGENT SYSTEMS

Chandrakant Sharma, Apekshit Sharma

[1,2]Assistant Professor, IBB Group of Colleges, Ranpur, Kota,Rajasthan, [1]*E-mail: cksmca@gmail.com* [2]*E-mail: apxit21@gmail.com*

ABSTRACT

The term "agent" is gaining popularity nowadays. Its meaning depends on the context in which it is used. Commonly it is defined as an independent software program which runs on behalf of a network user. Mobile Agents are special kind of agents that have an extra ability to travel to multiple locations in the network[6]. As they travel, they perform work on behalf of the user, such as collecting information or delivering requests. This mobility feature greatly enhances the productivity of each computing element in the network and creates a uniquely powerful computing environment well suited to a number of tasks. Yet, these systems are not being used fully because many security problems need to be solved. The lack of a feasible agent security model seriously hinders the adoption of the agent paradigm. Security, especially the attacks performed by hosts to the visiting mobile agents (the malicious hosts problem), is a major obstacle that prevents mobile agent technology from being widely adopted. The secure execution of a mobile agent is a very important design issue in building a mobile agent system. This paper provides a review of a number of security models for mobile agents.

Keywords: Mobile Agent, platform, threat.

1. INTRODUCTION

A Mobile Agent is specialized in that in addition to being an independent program executing on behalf of a network user, it can travel to multiple locations in the network [2]. The agent platform provides the computational environment in which an agent operates. The platform from which an agent originates is referred to as the home platform, and normally is the most trusted environment for an agent. Mobility allows an agent to move, or hop, among agent platforms as shown in Fig.1. As it travels, it performs work on behalf of the user, such as collecting information or delivering requests. This mobility greatly enhances the productivity of each computing element in the network and creates a uniquely powerful computing environment well suited to a number of tasks[7]. Agents are independent pieces of software capable of acting autonomously in response to input from their environment.

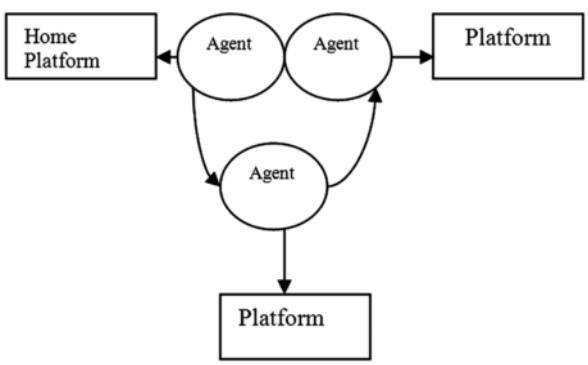

Figure 1: Agent System Model

Mobile agents are very useful for developing distributed applications but these systems are not used that freely and easily due to the inherent security problems associated with them [8]. Mobile agents simply offer a greater opportunity for abuse and misuse, broadening the scale of threats significantly. Four threat categories are identified: threats stemming from an agent attacking an agent platform, an agent platform attacking an agent, an agent attacking another agent on the agent platform, and other entities attacking the agent system. Many commercial and research Mobile Agent Security architectures have been implemented and many are still under development. In this paper some of the security architectures are discussed and reviewed.

2. MOBILE AGENT SECURITY POLICIES

Before getting into the details of security architecture one must fully understand that when dealing with mobile agents what should be the security policies that agents and host must support. In this section certain security policies are discussed. As in conventional distributed systems one of the most important requirement is **isolation** - that user programs and agents must be protected from each other, and the host must be protected from agents. An agent moves in a variety of networks or we can say it moves in a number of heterogeneous networks during its lifetime. The owner of the agent can have different levels of trust in each host. An agent must therefore be **adaptable** to the environment in which it runs. This means that it must be programmed to respond to the differing trust levels of the hosts that it visits, and to adapt its defenses accordingly. Another important

requirement is **survivability** i.e., the agent should be capable of surviving from attacks. This means being able to replicate an agent and send the replicas on different routes. A further security property is **believability**[1]. This means that there must be a way to verify the information furnished by an agent.

3. SECURITY MODELS FOR MOBILE AGENTS SYSTEMS

3.1 POM - Police Office Model [3]

The POM model focuses on the malicious host problem in which the host attacks the visiting agent [5, 6]. The main concept behind this model is that it separates the mobile agent into two parts the master part, which is security critical and the slave part which is security free part. This model is similar to the police office system in the real world. Police Office (PO) is introduced in each predefined region. The PO is a special host belonging to each region, it supervises all the hosts inside a region and every PO is assumed to be honest at any time, it never attacks any mobile agents. Region refers to group of hosts which have relatively high connection speed to each other and low connection speed to the hosts outside the region. Regions can not be overlapped.

According to the POM model whenever a Mobile agent wants to visit a new host, i.e., the mobile agent's running environment has to follow some steps which are the basis of POM model. The model has also conceptually refined Mobile agent by dividing it into the *master* part and the *slave* part.

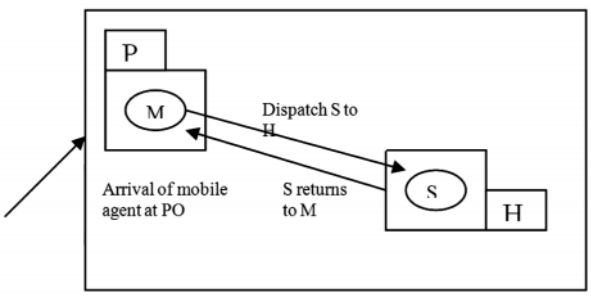

Figure 2: POM Steps for Mobile Agent Moving to a Host

The master part is security-critical while the slave part is security-free. Moreover, the slave part is designed to be capable of only migrating between the host and PO. Now, suppose a mobile agent with master part *M* and slave part *S* has to visit a host *H* whose *PO* is *P*. Then, first the mobile agent will arrive at *P*, on reaching at *P*, *M* becomes active and sends *S* to *H* to perform security free actions such as data gathering. After completing its work *S* returns to *P* with its work result. *M* performs some security critical actions on *P* using the results on *S*. After that depending on the work *M* sends another *S* to *H* or moves to the next host.

3.2 SFM (Secured Floating Market) Model. [9]

The SFM models focuses on solving the problems that are associated with the agents while their execution i.e., when they migrate from one server to the other these problems are agent controllability, resource restriction and security. In SFM, a computer called market provides mobile agents with some resources, such as high speed CPU, large storage space, special devices, etc. These resources are opened to mobile agents. This model can realize a execution style that both a server agent and a user agent make interaction as traveling through the network together, called Floating Market. SFM Model is composed of agents, markets, Market Managers, Location Management Servers, Local Authenticators and a Global Authenticator. In network services agents should be adaptable to a variety of requests issued by their users. Since an agent cannot be capable of handling all the requests, thus agent controllability is required. In this model an agent has some control parameters which indicate the permissible range of the ability of each ability , which are set appropriately by the user to make the agent adaptable to its request. Agents face two kinds of restrictions during their execution. First is *location restrictions*, which is the restrictions with the amount of information about location of resources and agents. Second is, *Capacity restrictions which* are the restrictions related to the processing ability or the load of each resource. SFM Model loosens these restrictions by using of Market Managers and Location Management Servers. An agent can get information about other agents and markets from a local Market Manager. For the purpose of resource restriction, in SFM model agent migration is also divided into two type *agent initiate migration* and *market initiate migration*. In agent initiate migration an agent sends a migration request to the local Market Manager. The Market Manager forwards this request to the Location Management Server of the area. The Location Management Server checks its data to find suitable candidate, it doesn't finds one then it forwards the request to other Location Management Servers to find a suitable candidate. The Location Management Server sends back the information (ID, location, etc.) of candidate market to the Market Manager. The Market Manager forwards this information to the agent and the agent migrates to the destination. In the market initiate migration the Market Manager selects an agent that it request to migrate according to some criteria and then it selects a candidate market as a destination. The Market Manager asks a Market Manager of the candidate market if it can accept agents. If it cannot find acceptable market in the area, Market Manager will look for it from other areas via Location Management Servers. The Market Manager sends the agent the request of migration and the information (ID, location, etc.) of the alternate market. The agent migrates to the alternate market. In SFM, security is guaranteed by using *enclosure of personal information*,

resource access limitation and *authentication*. Personal information is enclosed according to the value of an enclosure parameter. Resource access limitations are classified in some levels, and a suitable level is selected according to services. When an agent arrives at a market, the market refers the requirement of the incoming agent, which consists of amount of requirement resources, lifetime and so on. If this requirement is acceptable for the market, it allows the agent to access its resources. SFM Model uses two level authentications, global authentication and local authentication. Global authentication is used for only significant services which require a high reliability for authentication. If an agent does not require global authentication, all authentication of the agent are executed by local authentication. Local authentication applies extended GMAP (Global Mobile Authentication Protocol) [4], a protocol for the authentication of mobile users. GMAP introduces the mobile server which checks the user identification upon receiving a connection request from the mobile user and executes the third party authentication based on Kerberos[5].

SFM Model is implemented using ASDK (Aglets Software Development Kit). ASDK is a development tool of Aglets, and agents are described by Java for evaluation[11].

3.3 SECMAP [10]

SECMAP proposes a new agent model named as the shielded agent model for security purposes. A shielded agent is a highly encapsulated software component that ensures complete isolation against unauthorized access of any type. SECMAP provides secure agent communication and migration facilities as well, and maintains security policy information to examine agent actions and to prevent undesired/unauthorized activity. The system ensures protection of different agents and system components by enforcing security policies for various agent activities and continuously monitors and reports on the execution of an agent from its creation to its completion. A Secure Mobile Agent Server (SMAS) resident on each node presents a secure execution environment on which new agents may be created or to which agents may be dispatched. A SMAS may operate in three modes according to the functionality it exhibits: standard mode(SM-SMAS), master browser mode (MB-SMAS) for maintaining name location directory of all currently active agents, or security manager mode(SM-SMAS) for authentication purposes. A SECMAP agent's code and state information are kept encrypted during its life time using Data Encryption Standard (DES) algorithm. SECMAP employs a policy based authorization mechanism to permit or restrict agents to carry out certain classes of actions Two types of policies are defined: Agent policies that defines the rights of an agent and host policies that determine restrictions on access to the host resources by the agents. When agent transfer completes, its new location information is updated on MB-SMAS automatically so that any new message destined to this agent is redirected to the correct SMAS. Agent communication is secured by transforming encrypted message content through SSL. All communication that is carried out between SMAS engines to complete the transfer of the agent is encrypted through SSL.

4. OBSERVATIONS

By reviewing the above models discussed in section 3.1 to 3.3 the author has observed some important points about these models which are shown in Table 1.

Table 1
Comparison of the Three Models

Property	*POM*	*SFM*	*SECMAP*
Agent to Platform Attack	Not secured	Highly Secured	Moderately Secured
Agent to Agent attack	Moderately Secured	Not secured	Not secured
Platform to Agent Attack	Highly Secured	Not secured	Moderately Secured
Computational Overhead	Very little	Large	Less than SFM
Any Bottleneck	Yes	No	Yes
Network utilization	Moderate	Optimum	Moderate

5. CONCLUSION

In this paper the security problems associated with mobile agents are addressed by making a deep study of three existing mobile security models. These models are reviewed by the authors and a comparative study of these models is done for various issues like agent to platform attack, Platform to Agent Attack, Computational Overhead and Network utilization.

REFERENCES

[1] A Security Framework for a Mobile Agent System Ciar´an Bryce, Proceedings of the 6th European Symposium on Research in Computer Security (ESORICS 2000), Toulouse, France.

[2] Mobile Agent Computing, A White Paper.

[3] POM - A Mobile Agent Security Model against Malicious Hosts Xudong Guan, Yiling Yang, Jinyuan You Dept. of

Computer Science and Ens., Shanghai Jiaotong University, 200030.

[4] A. Takubo, M. Ishikawa, T. Watanabe, M. Soga and T. Mizuno, "User Authentication in Mobile Computing Environment", *IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences*, **E80-A,(7)**, pp. 1288-1298, 1997.

[5] J. Kohl, B. Neuman, "The Kerberos Network Authentication Service(V5)", rfc1510, Oct. 1993.

[6] D.C. Chess, C. Harrison, A. Kershenbaum, "Mobile Agents: Are They a Good Idea?", *IBM Research Report*, 1995.

[7] J.E. White, "Telescript Technology: Mobile Agents", *General Magic White Paper*, 1995.

[8] F.G. McCabe and K.L. Clark, "April - Agent Process Interaction Language", In M.J. Wooldridge and N.R. Jennings, editors, *Intelligent Agents - Proceedings of the 1994 Workshop on Agent Theories, Architectures, and Languages*, Springer-Verlag, Heidelberg, Germany, 1995.

[9] A Model of Mobile Agent Services Enhanced for Resource Restrictions and Security Tomoya Taka Tadanori Mizuno Takashi Watanabe Shizuoka University.

[10] An Overview of SECMAP Secure Mobile Agent Platform Suat Ugurlu, Nadia Erdogan.Publisher Springer Berlin / Heidelberg ISSN 0302-9743 (Print) 1611-3349 (Online).

[11] D. B. Lange and D. T. Chang, "IBM Aglets Workbench White Paper", 1996.